paloalto
TECHDOCS

Administration du filtrage des URL avancé

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 21, 2023

Table of Contents

Bases du filtrage des URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

La technologie de filtrage des URL protège les utilisateurs des menaces Web en offrant un contrôle granulaire sur l'accès des utilisateurs et leur interaction avec le contenu sur Internet. Vous pouvez développer une politique de filtrage des URL qui limite l'accès aux sites en fonction des catégories d'URL, des utilisateurs et des groupes. Par exemple, vous pouvez bloquer l'accès aux sites connus pour héberger des logiciels malveillants et empêcher les utilisateurs finaux de saisir des informations d'identification d'entreprise sur des sites appartenant à certaines catégories.

Pour un contrôle granulaire de l'accès des utilisateurs aux catégories, vous pouvez créer un profil de filtrage des URL et définir l'accès au site pour les catégories d'URL prédéfinies et personnalisées ; puis appliquer le profil aux règles de politique de sécurité. Vous pouvez également utiliser des catégories d'URL comme critères de correspondance dans les règles de politique de sécurité. Pour obtenir une liste des façons dont un abonnement au filtrage des URL avancé peut répondre aux besoins de sécurité Web de votre organisation, consultez Cas pratiques du URL Filtering.

- Solution de filtrage des URL de Palo Alto Networks
- Prise en charge du filtrage des URL
- Catégorisation locale en ligne
- Fonctionnement du filtrage avancé des URL
- Profils de URL Filtering
- Catégories d'URL
- Cas pratiques du URL Filtering

Solution de filtrage des URL de Palo Alto Networks

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Le filtrage des URL avancé (précédé de filtrage des URL) est un service d'abonnement qui protège votre réseau et ses utilisateurs contre les menaces Web malveillantes et évasives, connues et inconnues. L'abonnement offre la même fonctionnalité que le filtrage des URL (contrôle granulaire du filtrage des URL, visibilité sur l'activité des utilisateurs sur le Web, application de la recherche sécurisée et prévention de l'hameçonnage d'informations d'identification), avec l'ajout d'une inspection complète du contenu Web à l'aide d'un moteur de sécurité Web en ligne basé sur l'apprentissage automatique. Le moteur de sécurité Web en ligne permet l'analyse et la catégorisation en temps réel des URL qui ne sont pas présentes dans PAN-DB, la base de données des URL basée sur le cloud de Palo Alto Networks. Le moteur détermine ensuite l'action entreprise par le pare-feu.

Le filtrage avancé des URL protège contre les URL malveillantes qui sont mises à jour ou introduites avant que PAN-DB ne les ait analysées et ajoutées à la base de données. Lorsque le filtrage d'URL avancé est activé, les demandes d'URL sont les suivantes :

- Analysées en temps réel à l'aide des modules de détection de filtrage des URL avancé basé sur le cloud. Cela s'ajoute à la comparaison des URL aux entrées dans PAN-DB. Le moteur de protection Web alimenté par ML détecte et bloque les sites Web malveillants que PAN-DB ne peut pas détecter.
- Inspecté pour détecter le hameçonnage et les JavaScript malveillants grâce à la catégorisation locale inline, une solution d'analyse basée sur un pare-feu, qui peut bloquer en temps réel les pages web malveillantes inconnues.

Les licences de filtrage des URL avancé sont prises en charge sur les pare-feu de nouvelle génération exécutant PAN-OS 9.1 et versions ultérieures. Vous pouvez gérer des fonctionnalités de filtrage des URL sur l'interface Web PAN-OS et Panorama, Prisma Access, et les plateformes Cloud NGFW. Cependant, certaines fonctionnalités de filtrage des URL ne sont pas disponibles sur chaque plateforme.

Si les exigences de sécurité réseau de votre entreprise interdisent aux pare-feu d'accéder directement à Internet, Palo Alto Networks fournit une solution de filtrage des URL hors ligne avec le cloud privé PAN-DB. Vous pouvez déployer un cloud privé PAN-DB sur un ou plusieurs appareils M-600 qui fonctionnent comme serveurs PAN-DB au sein de votre réseau ; cependant, le cloud privé ne prend en charge aucune des fonctionnalités d'analyse d'URL basées sur le cloud fournies par la solution de filtrage des URL avancé.

Abonnement au filtrage des URL hérité

Le filtrage des URL applique des règles de politique pour les sites Web stockés dans votre cache local ou PAN-DB. Lorsqu'un utilisateur demande un site Web, le pare-feu vérifie le cache local pour sa catégorie d'URL. Si le site Web n'est pas dans le cache, le pare-feu interroge PAN-DB pour décider quelle action appliquer. Par conséquent, les attaquants sont mieux à même de lancer des campagnes d’attaques de précision en utilisant des URL qui ne sont pas présentes dans la base de données basée sur le cloud.

Les détenteurs d’abonnements hérités peuvent continuer à utiliser leur déploiement de filtrage des URL jusqu’à la fin de la durée de la licence.

Prise en charge du filtrage des URL

Des fonctionnalités avancées de filtrage des URL sont disponibles sur les pare-feu de nouvelle génération (virtuels et locaux), Prisma Access (Managed by Strata Cloud Manager), Prisma Access (Managed by Panorama), Cloud NGFW pour AWS et Cloud NGFW pour Azure. Toutefois, les pare-feu de nouvelle génération et Cloud NGFW pour Azure nécessitent un abonnement de filtrage des URL avancé, tandis que tous les Prisma Access et Cloud NGFW pour les licences AWS incluent des fonctionnalités de filtrage des URL avancé.

La prise en charge des fonctionnalités dépend de la plate-forme et du type de licence de filtrage des URL. Les fonctionnalités qui ne sont disponibles qu'avec une licence de filtrage des URL avancé sont indiquées par un label Filtrage des URL avancé.

Le tableau suivant montre la compatibilité des fonctionnalités de filtrage des URL avancé avec chaque plate-forme de Palo Alto Networks qui prend en charge le filtrage des URL.

Fonctionnalité	Pris en charge sur						Remarques
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW pour AWS	Cloud NGFW pour Azure	
Catégorisation en ligne • Catégorisation locale en ligne (appelée Inline ML avant PAN-OS 10.2) • (Filtrage des URL avancé) Catégorisation en ligne du cloud	Oui	Oui	Oui	Oui	Oui	Oui	Non pris en charge sur l'appareil VM-50 ou VM50L

Fonctionnalité	Pris en charge sur						Remarques
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW pour AWS	Cloud NGFW pour Azure	
Catégories d'URL personnalisées	Oui	Oui	Oui	Oui	Oui	Oui	
Détection des informations d'identification de l'utilisateur	Oui	Oui	Oui	Oui	Oui	Oui	
Pages de réponse de filtrage des URL personnalisées	Oui	Oui	Oui	Oui	Oui	Oui	
Mise en œuvre de la recherche sécurisée • Bloquer les résultats de recherche lorsque la recherche sécurisée stricte est désactivée • Forcer une recherche sécurisée stricte	Oui	Oui	Oui	Oui	Oui	Oui	

Fonctionnalité	Pris en charge sur						Remarques
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW pour AWS	Cloud NGFW pour Azure	
Contrôle prioritaire sur l'URL par l'administrateur	Oui	Oui	Oui	Oui	Oui	Oui	
Inspection de l'établissement de liaison SSL/TLS	Oui	Oui	Oui	Oui	Oui	Oui	
Intégration avec l'isolation du navigateur distant (RBI)	Non	Non	Oui	Oui	Non	Non	
Consigner uniquement la page du conteneur (consigner uniquement la page visitée par l'utilisateur)	Non	Oui	Oui	Oui	Oui	Oui	

Catégorisation locale en ligne

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé ***Note :*** *Prisma Access les licences incluent les capacités Advanced URL Filtering.*

La catégorisation en ligne locale (anciennement connue sous le nom de ML en ligne) permet au plan de données du pare-feu d'appliquer l'apprentissage automatique (ML) sur les pages Web pour alerter les utilisateurs lorsque des variantes de phishing sont détectées tout en empêchant les variantes malveillantes d'exploits JavaScript de pénétrer dans votre réseau. La catégorisation locale inline analyse et détecte dynamiquement le contenu malveillant en évaluant divers détails des pages web à l'aide d'une série de modèles ML. Chaque modèle ML détecte les contenus malveillants en évaluant les détails des fichiers, y compris les champs et les modèles du décodeur, afin de formuler une classification et un verdict de haute probabilité, qui sont ensuite utilisés dans le cadre de votre politique de sécurité web plus large. Les URL classées comme malveillantes sont transmises à PAN-DB pour une analyse et une validation supplémentaires. En outre, vous pouvez également spécifier des exceptions d'URL pour exclure tout faux positif qui pourrait être rencontré. Cela vous permet de créer des règles plus granulaires pour vos profils afin de répondre à vos besoins spécifiques en matière de sécurité. Afin d'être au courant des dernières évolutions des menaces, les modèles Inline ML sont régulièrement mis à jour et ajoutés via des communiqués de contenu. Un abonnement actif au filtrage avancé des URL est requis pour configurer la catégorisation en ligne.

La protection ML en ligne peut également être activée pour détecter les fichiers PE (exécutables portables) malveillants, les fichiers ELF et MS Office, ainsi que les scripts PowerShell et shell en temps réel dans le cadre de la configuration de votre profil antivirus. Pour en savoir plus, reportez-vous à la section : Advanced Wildfire Inline ML.

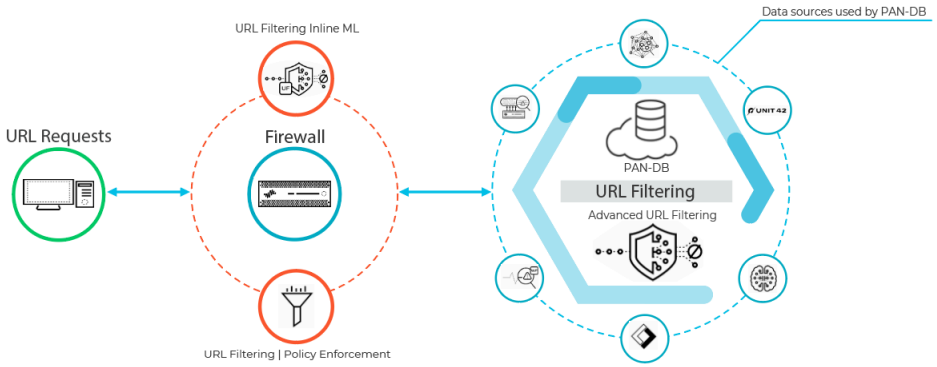
La catégorisation locale en ligne n'est pas prise en charge sur l'appareil virtuel VM-50 ou VM50L.

Fonctionnement du filtrage avancé des URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Le filtrage d'URL avancé classe les sites Web en fonction du contenu, des fonctionnalités et de la sécurité du site. Une URL peut avoir jusqu'à quatre catégories d'URL qui indiquent la probabilité que le site vous expose à des menaces. En tant que PAN-DB, la base de données d'URL de filtrage d'URL avancé, catégorise les sites, les pare-feu avec le filtrage d'URL avancé activé peuvent tirer parti de ces connaissances pour appliquer les stratégies de sécurité de votre organisation. En plus de la protection offerte par PAN-DB, le filtrage des URL avancé fournit une analyse en temps réel à l'aide de l'apprentissage automatique (ML) pour se défendre contre les menaces nouvelles et inconnues. Cela offre une protection contre les URL malveillantes qui sont mises à jour ou introduites avant que les bases de données de filtrage d'URL aient la possibilité d'analyser et d'ajouter le contenu, donnant aux attaquants une période ouverte à partir de laquelle ils peuvent lancer des campagnes d'attaque de précision. Le filtrage avancé des URL compense les lacunes de couverture inhérentes aux solutions de base de données en fournissant une analyse d'URL en temps réel par demande. Les modèles basés sur le ML utilisés par le filtrage des URL avancé ont été formés et sont continuellement mis à jour pour détecter diverses URL malveillantes, pages Web de hameçonnage et commandes et contrôle (C2).

Les sites Web qui indiquent la présence de certaines menaces avancées sont en outre traités via un système d'apprentissage profond en ligne basé sur le cloud, à l'aide de détecteurs et d'analyseurs qui complètent les modèles ML utilisés par le filtrage avancé d'URL. Les détecteurs d'apprentissage profond peuvent traiter des ensembles de données plus volumineux et mieux identifier les modèles et comportements malveillants complexes grâce à des réseaux neuronaux multicouches. Lorsque le filtrage d'URL avancé reçoit des données de réponse HTTP du pare-feu à la réception d'une requête Web suspecte, les données sont analysées plus en détail via les détecteurs d'apprentissage profond et fournissent une protection en ligne contre les attaques Web zero-day évasives. Cela inclut les sites Web masqués, dans lesquels le contenu des pages Web est récupéré subrepticement à partir de sites Web inconnus, cela peut inclure du contenu malveillant que les bases de données d'URL ne peuvent pas prendre en compte, des attaques en plusieurs étapes, des défis CAPTCHA et des URL à usage unique inédites. Étant donné que les sites Web malveillants évasifs sont dans un état de flux constant, les détecteurs et les analyseurs utilisés pour catégoriser les sites Web sont mis à jour et déployés automatiquement à mesure que les chercheurs en menaces de Palo Alto Networks améliorent la logique de détection, le tout sans que l'administrateur ait à télécharger les packages de mise à jour.



Lorsqu'un utilisateur demande une page Web, le pare-feu interroge les exceptions ajoutées par l'utilisateur et PAN-DB pour la catégorie de risque du site. PAN-DB utilise les informations d'URL de l'unité 42, WildFire, DNS passif, données de télémétrie Palo Alto Networks, données de la Cyber Threat Alliance, et applique divers analyseurs pour déterminer la catégorie. Si l'URL affiche des caractéristiques risquées ou malveillantes, les données utiles web sont aussi soumises à un filtrage d'URL avancé dans le cloud pour une analyse en temps réel et génère des données d'analyse supplémentaires. La catégorie de risque qui en résulte est ensuite récupérée par le pare-feu et est utilisée pour appliquer les règles d'accès Web en fonction de la configuration de votre politique. En outre, le pare-feu met en cache les informations de catégorisation du site pour les nouvelles entrées afin de permettre une récupération rapide des demandes ultérieures, tout en supprimant les URL auxquelles les utilisateurs n'ont pas accédé récemment afin de refléter avec précision le trafic de votre réseau. En outre, des contrôles intégrés aux requêtes PAN-DB dans le cloud garantissent que le pare-feu reçoit les dernières informations de catégorisation des URL. Si vous ne disposez pas d'une connectivité Internet ou d'une licence de filtrage d'URL active, aucune requête n'est adressée à PAN-DB.

Le pare-feu détermine la catégorie d'URL d'un site Web en la comparant aux entrées de 1) catégories d'URL personnalisées, 2) listes dynamiques externes (EDL) et 3) catégories d'URL prédéfinies, par ordre de priorité.

Les pare-feu configurés pour analyser les URL en temps réel à l'aide de l'apprentissage automatique sur le plan de données fournissent une couche de sécurité supplémentaire contre les sites web de hameçonnage et les exploitations JavaScript. Les modèles ML utilisés par la catégorisation locale en ligne identifient les variantes actuellement inconnues et futures des menaces basées sur des URL qui correspondent aux caractéristiques que Palo Alto Networks a identifiées comme malveillantes. Afin d'être au courant des dernières évolutions des menaces, les modèles ML de catégorisation inline locaux sont ajoutés ou mis à jour via des communiqués de contenu.

Lorsque que le pare-feu vérifie une URL auprès de PAN-DB, il cherche également des mises à jour critiques, notamment les URL qui, préalablement, étaient bénignes, mais qui sont désormais malveillantes.

Si vous pensez que PAN-DB a incorrectement catégorisé un site, vous pouvez soumettre une demande de modification dans votre navigateur via Test A Site ou directement à partir des journaux du pare-feu.

Le saviez-vous ?

Techniquement, le pare-feu met les URL en mémoire tampon sur le plan de gestion et le plan de données :

- *PAN-OS 9.0 et les versions ultérieures ne téléchargent pas les bases de données PAN-DB initiales. Au lieu, lors de l'activation de la licence de filtrage des URL, le pare-feu remplit le cache au fur et à mesure que les requêtes d'URL sont transmises.*
- *Le plan de gestion contient plus d'URL et communique directement avec PAN-DB Quand le pare-feu ne peut pas trouver la catégorie d'une URL dans sa mémoire tampon et effectue une recherche dans PAN-DB, il cache l'information de catégorie dans le plan de gestion. Le plan de gestion passe l'information au plan de données, qui la met aussi en mémoire tampon pour appliquer les politiques.*
- *Le plan de données contient moins d'URL et reçoit les informations du plan de gestion Une fois que le pare-feu a vérifié les listes d'exceptions de catégorie d'URL (catégories d'URL personnalisées et listes dynamiques externes) pour une URL, il recherche dans le plan de données. Si le pare-feu ne trouve pas l'URL dans le plan de données, il vérifie le plan de gestion et, si les informations de catégorie ne sont pas présentes, PAN-DB.*

Profils de URL Filtering

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Les profils de filtrage des URL définissent la manière dont le pare-feu gère le trafic vers des catégories d'URL spécifiques. Un profil de filtrage des URL est un ensemble de contrôles de filtrage des URL que vous appliquez à des règles de politique de sécurité individuelles qui autorisent l'accès à Internet. Vous pouvez configurer l'accès au site pour les catégories d'URL, autoriser ou interdire l'envoi d'informations d'identification utilisateur, activer l'application de la recherche sécurisée et divers autres paramètres. Pour appliquer les actions définies dans un profil de filtrage des URL, appliquez le profil aux règles de la politique de sécurité. Le pare-feu applique les actions du profil au trafic qui correspond à la règle de politique de sécurité (pour obtenir de plus amples renseignements, reportez-vous à la section Configuration du URL Filtering).

Le pare-feu est livré avec un profil par défaut qui bloque les catégories sujettes aux menaces, telles que les logiciels malveillants, l'hameçonnage et les contenus pour adultes. Vous pouvez utiliser le profil par défaut dans une règle de politique de sécurité, le cloner pour l'utiliser comme point de départ pour de nouveaux profils de filtrage des URL ou ajouter un nouveau profil de filtrage des URL. Vous pouvez personnaliser les profils de filtrage des URL nouvellement ajoutés et ajouter des listes de sites Web spécifiques qui devraient toujours être bloqués ou autorisés. Par exemple, vous pouvez bloquer la catégorie des réseaux sociaux, mais autoriser l'accès à des sites Web spécifiques de cette catégorie. Par défaut, l'accès au site pour toutes les catégories d'URL est défini sur autoriser lorsque vous créez un profil de filtrage des URL de base. Cela signifie que les utilisateurs pourront naviguer librement sur tous les sites et que le trafic n'est pas enregistré.

Créez un profil de filtrage des URL recommandé pour assurer la protection contre les URL qui ont été observées comme hébergeant des contenus malveillants ou d'exploitation.

Actions de politique du profil de filtrage des URL

Dans un profil de filtrage des URL, vous pouvez définir **l'accès au site** pour les catégories d'URL, autoriser ou interdire les **Soumissions d'informations d'identification de l'utilisateur** en fonction de la catégorie d'URL (par exemple, vous pouvez bloquer l'envoi d'informations d'identification de l'utilisateur à des sites à risque moyen et élevé), et activer l'application de la recherche sécurisée.

Action	Description
Accès au site	
alert (alerter)	Le site Web est autorisé et une entrée de journal est créée dans le journal de URL Filtering. *Définissez **alert (alerter)** comme Action des catégories ou du trafic que vous ne bloquez pas pour le journaliser ou obtenir une visibilité du trafic.*
allow (autoriser)	Le site Web est autorisé et aucune entrée de journal n'est créée. *Ne définissez pas **allow (autoriser)** comme Action des catégories ou du trafic que vous ne bloquez, car vous perdez la visibilité du trafic que vous ne journalisez pas. Optez plutôt pour l'option **alert (alerter)** comme Action des catégories ou du trafic que vous ne bloquez pas pour le journaliser ou obtenir une visibilité du trafic.*
block	Le site Web est bloqué, une page de réponse va s'afficher et l'utilisateur ne pourra pas continuer sa visite sur ce site Web. Une entrée de journal est créée dans le journal de filtrage des URL. Le blocage de l'accès au site pour une catégorie d'URL définit également les envois des informations d'identification de l'utilisateur pour cette catégorie d'URL sur block (bloquer).
continue (continuer)	Une page de réponse va s'afficher en indiquant que le site a été bloqué en raison de la politique de sécurité de l'entreprise, mais l'utilisateur pourra choisir de continuer sa visite sur ce site Web. L'action **continue (continuer)** est généralement utilisée pour les catégories qui sont considérées comme étant bénignes et permet d'améliorer l'expérience utilisateur en lui permettant de continuer s'il estime que le site n'a pas été correctement catégorisé. Le message de la page de réponse peut être personnalisé afin d'inclure des informations spécifiques à votre entreprise. Une entrée de journal est créée dans le journal de filtrage des URL.

Action	Description
	La page Continue (Continuer) ne s'affiche pas correctement sur les machines client configurées pour utiliser un serveur proxy.
override (contrôle prioritaire)	Une page de réponse va s'afficher en indiquant qu'un mot de passe est requis pour autoriser l'accès aux sites Web d'une catégorie donnée. Grâce à cette option, l'administrateur de sécurité ou l'employé du service de support doit fournir un mot de passe autorisant un accès temporaire à tous les sites Web d'une catégorie donnée. Une entrée de journal est créée dans le journal de URL Filtering. Reportez-vous à la section Autoriser l'accès par mot de passe à certains sites. Dans les versions antérieures. le contrôle prioritaire des catégories de URL Filtering plaçait l'application de la politique devant les catégories d'URL personnalisées. Dans le cadre de la mise à niveau vers PAN-OS 9.0, les contrôles prioritaires des catégories sont convertis en catégories d'URL personnalisées. L'application de la politique n'est plus prioritaire par rapport aux catégories d'URL personnalisées. Plutôt que l'action que vous avez définie pour le contrôle prioritaire des catégories dans les versions précédentes, la nouvelle catégorie d'URL personnalisée est appliquée par la règle de politique de sécurité disposant de l'action du profil de filtrage des URL la plus stricte. De la plus stricte à la moins stricte, les actions du profil de URL Filtering sont les suivantes : bloquer, appliquer un contrôle prioritaire, continuer, alerter et autoriser. Cela signifie que, si vous appliquiez des contrôles prioritaires sur les catégories d'URL avec l'action autoriser, il se peut que les contrôles prioritaires soient bloqués après être convertis à la catégories d'URL personnalisée dans PAN-OS 9.0. *La page Override (Remplacer) ne s'affiche pas correctement sur les machines client configurées pour utiliser un serveur proxy.*
none (aucun)	L'action **none (aucune)** s'applique uniquement aux catégories d'URL personnalisées. Sélectionner **none (aucune)** permet de s'assurer que, si plusieurs profils d'URL existent, la catégorie personnalisée n'affecte pas les autres profils. Par exemple, si vous possédez deux profils d'URL et que la catégorie d'URL personnalisée de l'un des profils est définie sur **block (bloquer)**, vous devez définir l'action sur

Action	Description
	none (aucun) si vous ne voulez pas que l'action de blocage s'applique à l'autre profil. De plus, pour supprimer une catégorie d'URL personnalisée, elle doit être définie sur **none (aucune)** dans un profil que vous utilisez.
Autorisations relatives aux informations d'identification de l'utilisateur *Ces paramètres exigent que vous* set up credential phishing prevention (Configuriez la prévention du hameçonnage des informations d'identification) *au préalable.*	
alert (alerter)	Permettez aux utilisateurs d'envoyer des informations d'identification professionnelles dans cette catégorie d'URL, mais générez un journal d'alerte de filtrage des URL chaque fois que cela se produit.
allow (par défaut)	Permettez aux utilisateurs d'envoyer des informations d'identification professionnelles dans cette catégorie d'URL.
block	Empêchez les utilisateurs d'envoyer des informations d'identification professionnelles dans cette catégorie. Une page de réponse anti-hameçonnage par défaut s'affiche pour les utilisateurs lorsqu'ils accèdent à des sites pour lesquels les envois d'informations d'identification professionnelles sont bloqués. Vous pouvez personnaliser la page de blocage qui s'affiche.
continue (continuer)	Affiche une page de réponse aux utilisateurs qui les invite à sélectionner Continuer pour saisir des informations d'identification afin d'accéder au site. Par défaut, la page de poursuite anti-hameçonnage s'affiche pour l'utilisateur lorsqu'il accède à des sites pour lesquels les envois d'informations d'identification sont déconseillés. Vous pouvez personnaliser la page de réponse pour mettre en garde les utilisateurs contre les tentatives d'hameçonnage ou la réutilisation de leurs identifiants sur d'autres sites Web, par exemple.

Catégories d'URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Palo Alto Networks classe les sites Web en fonction de leur contenu, de leurs fonctionnalités et de leur sécurité. Chaque catégorie d'URL correspond à un ensemble de caractéristiques utiles pour créer des règles de politique. Les URL auxquelles les utilisateurs de votre réseau ont accès sont ajoutées à la base de données de filtrage des URL de Palo Alto Networks, PAN-DB. PAN-DB attribue jusqu'à quatre catégories d'URL, y compris les catégories de risque (élevé, moyen et faible), à ces sites Web.

Les catégories d'URL permettent le filtrage par catégorie du trafic Web et le contrôle granulaire de la politique des sites. Vous pouvez configurer un profil de filtrage des URL pour définir l'accès au site pour les catégories d'URL et appliquer le profil aux règles de politique de sécurité qui autorisent le trafic vers Internet. Vous pouvez également utiliser les catégories d'URL comme critères de correspondance dans les règles de politique de sécurité pour vous assurer que ces règles s'appliquent uniquement aux sites Web dans les catégories spécifiées. Par exemple, vous pouvez configurer une règle de politique de décryptage qui empêche le décryptage du trafic vers la catégorie des services financiers.

Pour vérifier les catégories d'une URL spécifique, entrez l'URL dans Test A Site, notre moteur de recherche d'URL. Si vous pensez qu'une URL est incorrectement classée, soumettez une demande de modification de catégorie.

Catégories d'URL personnalisées

Vous pouvez créer une catégorie d'URL personnalisée pour exclure des sites Web particuliers de l'application basée sur la catégorie. Les catégories d'URL personnalisées peuvent être basées sur des URL spécifiques (Liste d'URL) ou d'autres catégories (Correspondance des catégories). Les catégories d'URL personnalisées de type de liste d'URL fonctionnent comme des listes de blocage et d'autorisation. Les catégories d'URL personnalisées de type Correspondance des catégories permettent une application ciblée pour les sites Web qui correspondent à toutes les catégories définies dans le cadre de la catégorie personnalisée.

Catégories d'URL prédéfinies

Le tableau suivant répertorie les catégories d'URL prédéfinies que PAN-DB utilise pour filtrer les URL. Certaines entrées décrivent des sites qui sont exclus de la catégorie. Catégories d'URL axées sur la sécurité décrit des catégories de risque qui ne sont pas attribuées à toutes les URL.

Catégorie d'URL	Description
Avortement	Sites qui se rapportent à des informations ou des groupes en faveur ou contre l'avortement, des détails concernant les procédures d'avortement, des forums d'aide ou de soutien pour ou contre l'avortement, ou des sites qui fournissent des informations sur les conséquences ou les effets de la poursuite (ou non) d'un avortement.
Drogues abusées	Sites qui font la promotion de l'abus de drogues légales et illégales, de l'utilisation et de la vente d'accessoires liés à la drogue, de la fabrication et/ou de la vente de drogues.
Adulte	Sites contenant du matériel sexuellement explicite, des médias (y compris du langage, des jeux ou des bandes dessinées), de l'art ou des produits, des groupes ou forums en ligne à caractère sexuellement explicite, et des sites qui font la promotion de services pour adultes, tels que des conférences vidéo ou téléphoniques, des services d'escorte et des clubs de strip-tease.
Alcool et tabac	Sites qui se rapportent à la vente, à la fabrication ou à la consommation d'alcool et/ou de produits du tabac et d'accessoires connexes. Comprend les sites liés aux cigarettes électroniques.
Intelligence artificielle	Sites Web qui utilisent des modèles d'apprentissage automatique et d'apprentissage profond, y compris de grands modèles linguistiques, pour fournir des services qui auraient généralement nécessité de l'intelligence humaine. Les services fournis incluent, sans s'y limiter, les services de chatbot, de productivité, de récapitulatif, de transcripteur, d'absence de code et de montage audio ou vidéo. L'accent est mis sur les sites Web hébergeant le service d'IA proprement dit, et non sur le contenu informatif de l'IA.
Enchères	Sites qui favorisent la vente de biens entre particuliers.

Catégorie d'URL	Description
	Les ventes aux enchères pour des donations sont classées dans la catégorie Société.
Affaires et économie	Sites ayant un contenu lié au marketing, à la gestion, à l'économie, à l'entrepreneuriat ou à la gestion d'une entreprise, y compris les éléments suivants : • Sites pour les entreprises de publicité et de marketing • Sites pour les services d'expédition, tels que fedex.com • Sites pour les fournisseurs de services téléphoniques, câblés et Internet • Sites pour sondages • Sites pour les chambres de commerce • Sites pour conférences* • *Les sites Web d'entreprises pourraient être classés en fonction de leur technologie au lieu de cette catégorie.* • ** Les sites liés aux conférences doivent être classés en fonction du contenu. Si le contenu d'un site n'est pas spécifique, il est classé dans la catégorie Affaires et économie.*
Commande et contrôle	Les URL et les domaines de commande et contrôle (C2) utilisés par les logiciels malveillants et/ou les systèmes compromis pour communiquer discrètement avec le serveur à distance d'un attaquant afin de recevoir des commandes malveillantes ou d'exfiltrer des données.
Informations sur les ordinateurs et Internet	Sites qui fournissent des informations générales sur les ordinateurs et Internet, y compris des sites sur les sujets suivants : • Informatique • Ingénierie • Matériel et pièces informatiques • Logiciels

Catégorie d'URL	Description
	• Sécurité • Programmation *La programmation peut avoir un certain chevauchement avec la catégorie Référence et recherche, mais la catégorie principale devrait être Informatique et Info Internet.*
Réseaux de distribution de contenu	Sites dont l'objectif principal est de fournir du contenu à des tiers tels que des publicités, des médias, des fichiers et des serveurs d'images.
Violation des droits d'auteur	Domaines dont le contenu est illégal, par exemple du contenu qui permet le téléchargement illégal de logiciels ou d'autres propriétés intellectuelles qui présente un risque de responsabilité éventuel. *Les sites qui fournissent des services d'échange de fichiers peer-to-peer ou des médias de streaming généraux appartiennent à leurs propres catégories respectives.*
Cryptomonnaie	Les sites Web qui font la promotion des cryptomonnaies, les sites Web de minage de cryptomonnaies (mais pas les mineurs de cryptomonnaies intégrés), les échanges et les fournisseurs de cryptomonnaies, et les sites Web qui gèrent les portefeuilles et les registres de cryptomonnaie. *Les sites référençant la cryptomonnaie ou les sites malveillants liés à la cryptomonnaie seront classés séparément. Par exemple, les sites qui expliquent le fonctionnement des cryptomonnaies et de la technologie blockchain relèvent de la rubrique Informatique et Info Internet.*
Rencontres	Sites offrant des services de rencontres en ligne, des conseils et d'autres annonces personnelles.

Catégorie d'URL	Description
	Les sites de rencontres qui proposent des salons de chat à caractère sexuel entrent dans la catégorie Adulte.
DNS dynamique	Les sites qui fournissent ou utilisent des services DNS dynamiques pour associer des noms de domaine à des adresses IP dynamiques. *DNS dynamique est souvent utilisé par les attaquants pour la communication de commande et de contrôle et d'autres fins malveillantes.*
Établissements d'enseignement	Sites officiels pour les écoles, collèges, universités, districts scolaires, cours en ligne et autres établissements d'enseignement. Comprend également des sites pour les académies de soutien scolaire. *Cette catégorie vise les établissements d'enseignement plus grands et établis tels que les écoles primaires, les écoles secondaires et les universités.*
DNS chiffré	Sites pour les fournisseurs de services de résolution DNS qui offrent sécurité et confidentialité aux utilisateurs finaux en cryptant les requêtes et réponses DNS à l'aide de protocoles tels que DNS sur HTTPS (DoH).
Spectacles et arts	Sites pour films, télévision, radio, vidéos, guides/outils de programmation, bandes dessinées, arts du spectacle, musées, galeries d'art ou bibliothèques. Comprend les sites suivants : • Divertissement • Actualités de l'industrie des célébrités et du divertissement • Romans • Cours de danse • Sites d'événements • Tatouage artistique
Extrémisme	Sites faisant la promotion du terrorisme, du racisme, du fascisme ou d'autres idéologies discriminant des gens ou des groupes d'origines ethniques, de religions

Catégorie d'URL	Description
	ou de convictions différentes. Dans certaines régions, les lois et règlements peuvent interdire l'accès aux sites extrémistes, et l'autorisation de l'accès peut présenter un risque de responsabilité. *Les sites Web qui abordent des avis politiques ou religieux controversés relèvent respectivement des catégories Philosophie et Plaidoyer politique et Religion.*
Services financiers	Sites Web contenant des renseignements ou des conseils financiers personnels, tels que les services bancaires en ligne, les prêts, les prêts hypothécaires, la gestion de dettes, les sociétés émettrices de cartes de crédit, les sociétés de change (FOREX) et les compagnies d'assurance. Exclut les sites liés à l'assurance maladie, aux marchés boursiers, au courtage ou aux services de trading.
Jeux d'argent	Sites Web de loterie ou de jeux d'argent qui facilitent l'échange d'argent réel ou virtuel. Comprend des sites connexes qui fournissent des informations, des tutoriels ou des conseils sur le jeu, comme la façon de parier. *Les sites Web d'entreprises pour les hôtels et les casinos qui ne permettent pas le jeu entrent dans la catégorie Voyage.*
Jeux	Sites qui offrent des jeux en ligne ou des téléchargements de jeux vidéo ou informatiques, des critiques de jeux, des conseils, des tricheries ou des publications et des médias connexes. Comprend les sites qui fournissent des instructions pour les jeux non électroniques, facilitent la vente ou le commerce de jeux de société, ou soutiennent ou hébergent des loteries et des cadeaux en ligne.
Gouvernement	Sites Web officiels pour les gouvernements locaux, étatiques et nationaux, ainsi que les agences, services ou lois connexes.

Catégorie d'URL	Description
	Les sites des bibliothèques publiques et des institutions militaires relèvent respectivement des catégories Référence et Recherche et Militaire.
Logiciel indésirable	Sites au contenu qui ne présente pas une menace directe pour la sécurité, mais qui affiche un autre comportement gênant et incite l'utilisateur final à accorder un accès à distance ou à effectuer d'autres actions non autorisées. Logiciel indésirable comprend les éléments suivants : • Sites détournés • Typosquattage de domaines qui ne présentent pas de comportement malveillant et qui ne sont pas la propriété du domaine ciblé • Sites avec roguewares, logiciels publicitaires ou autres applications non sollicitées, telles que les mineurs de cryptomonnaie intégrés, le clickjacking ou les pirates qui changent les éléments du navigateur Web • Sites à contenu illégal ou criminel
Piratage	Sites liés à l'accès ou à l'utilisation illégale ou douteuse d'équipements ou de logiciels de communication, y compris le développement et la distribution de tels programmes, des conseils pratiques ou des conseils qui peuvent entraîner la compromission des réseaux et des systèmes. Comprend également les sites qui facilitent le contournement des systèmes de licences et de droits numériques.
Santé et médecine	Sites contenant des informations sur la santé générale, des problèmes et des conseils, remèdes et traitements traditionnels et non traditionnels. Comprend également des sites pour diverses spécialités, pratiques et installations médicales (comme des gymnases et des clubs de fitness) ainsi que pour des professionnels. Les sites relatifs à l'assurance médicale et à la chirurgie esthétique sont également inclus.
Maison et jardin	Sites contenant des informations, des produits et des services concernant les réparations et l'entretien de

Catégorie d'URL	Description
	la maison, l'architecture, le design, la construction, la décoration et le jardinage.
Chasse et pêche	Sites qui fournissent des conseils ou des instructions de chasse et de pêche ou facilitent la vente d'équipements et d'accessoires connexes. *Les sites qui vendent principalement des armes à feu (même si elles sont utilisées pour la chasse) entrent dans la catégorie Armes.*
Contenu insuffisant	Les sites et les services qui présentent des pages de test, n'ont pas de contenu, fournissent un accès API non destiné à l'affichage de l'utilisateur final ou nécessitent une authentification sans afficher aucun autre contenu suggérant une catégorisation différente.
Communications Internet et téléphonie	Sites qui prennent en charge ou fournissent des services de chat vidéo, de messagerie instantanée ou de téléphonie.
Portails Internet	Sites qui servent de point de départ pour les utilisateurs, généralement en agrégeant un large éventail de contenus et de sujets.
Recherche d'emploi	Sites qui fournissent des offres d'emploi et des avis d'employeurs, des conseils et des astuces pour les entrevues, ou des services connexes pour les employeurs et les candidats potentiels.
Juridique	Sites qui fournissent des informations, des analyses ou des conseils concernant le droit, les services juridiques, les cabinets d'avocats ou d'autres questions juridiques connexes.
Logiciel malveillant	Sites contenant ou connus pour héberger du contenu malveillant, des exécutables, des scripts, des virus, des chevaux de Troie et du code.
Marijuana	Les sites qui discutent, encouragent, promeuvent, offrent, vendent, fournissent ou préconisent de toute autre manière l'utilisation, la culture, la fabrication ou la distribution de marijuana et de ses multiples pseudonymes, que ce soit à des fins récréatives ou

Catégorie d'URL	Description
	médicales. Inclut des sites avec des accessoires en lien avec la marijuana.
Militaire	Sites avec des informations ou commentaires concernant les branches militaires, le recrutement, les opérations actuelles ou passées, ou tout accessoire connexe. Comprend des sites pour les associations de militaires et d'anciens combattants.
Véhicules à moteur	Sites avec des informations relatives aux revues, à la vente, au commerce, à la modification, aux pièces et autres discussions connexes sur les automobiles, motocyclettes, bateaux, camions et véhicules récréatifs (VR).
Musique	Sites liés à la vente, la distribution ou l'information musicale. Comprend des sites Web pour les artistes musicaux, les groupes, les labels, les événements, les paroles et d'autres informations concernant l'industrie de la musique. Exclut les sites de streaming musical.
Domaines nouvellement enregistrés	Sites qui ont été enregistrés au cours des 32 derniers jours. Les domaines nouvellement enregistrés sont souvent générés volontairement ou par des algorithmes de génération de domaines et utilisés pour mener des activités malveillantes.
Actualité	Publications en ligne, agences de presse et autres sites Web qui regroupent l'actualité, la météo ou d'autres questions contemporaines. Comprend les éléments suivants : • Journaux • Stations de radio • Magazines • Podcasts • Programmes TV dédiés à l'actualité • Sites de bookmarking social, tels que reddit.com *Si le magazine ou le site d'information se concentre sur un sujet spécifique comme le sport, les voyages, la mode, il est classé en fonction du contenu dominant sur le site.*

Catégorie d'URL	Description
Non résolu	Cette catégorie indique que le site Web est introuvable dans la base de données de filtrage des URL locale et que le pare-feu n'a pas pu se connecter à la base de données sur le cloud pour vérifier la catégorie.
Nudité	Sites qui contiennent des représentations nues ou semi-nues du corps humain, indépendamment du contexte ou de l'intention, telles que des œuvres d'art. Comprend les sites nudistes ou naturistes contenant des images des participants.
Stockage et sauvegarde en ligne	Sites qui fournissent le stockage en ligne de fichiers gratuitement ou en tant que service. Comprend des sites de partage de photos.
Parqué	URL qui hébergent du contenu limité ou des publicités au clic, ce qui peut générer des revenus pour l'entité hôte, mais ne possède généralement pas de contenu utile pour les utilisateurs finaux. Comprend les domaines qui sont à vendre. *Les sites parqués à contenu adulte entrent dans la catégorie Adulte.*
Peer-to-peer	Sites qui fournissent un accès ou des clients pour le partage peer-to-peer de torrents, de programmes de téléchargement, de fichiers multimédias ou d'autres applications logicielles. Principalement applicable aux sites avec des capacités de téléchargement BitTorrent. Exclut les sites de partagiciels ou de logiciels gratuits.
Sites personnels et blogs	Sites Web personnels et blogs d'individus ou de groupes. Si ces sites ont un sujet dominant associé à une autre catégorie, ils seront classés avec les deux catégories.
Philosophie et plaidoyer politique	Sites contenant des informations, des points de vue ou des campagnes concernant des opinions philosophiques ou politiques.
Hameçonnage	Contenu Web qui tente secrètement de récolter des informations, telles que des identifiants de connexion, des informations de carte de crédit, des numéros de compte, des codes PIN et d'autres informations

Catégorie d'URL	Description
	d'identification personnelle (IIP), volontairement ou involontairement, auprès des victimes en utilisant des techniques d'ingénierie sociale. Inclut les arnaques à l'assistance technique et les logiciels de peur.
Adresses IP privées	Cette catégorie inclut les adresses IP définies dans la RFC 1918, 'Address Allocation for Private Intranets,' qui sont les suivantes : • 10.0.0.0 - 10.255.255.255 (préfixe 10/8) • 172.16.0.0 - 172.31.255.255 (préfixe 172.16/12) • 192.168.0.0 - 192.168.255.255 (préfixe 192.168/16) Il inclut également les domaines non enregistrés auprès du système DNS public (*.local et *.onion).
Contournement de proxy et anonymiseurs	Serveurs proxy et autres méthodes qui contournent le filtrage ou la surveillance des URL. *Les VPN dont l'utilisation se fait au niveau de l'entreprise entrent dans la catégorie Communication et Téléphonie Internet.*
Douteux	Sites Web contenant de l'humour de mauvais goût, des contenus offensants ciblant des groupes ou des individus spécifiques.
Ransomware	Sites connus pour héberger des ransomwares ou du trafic malveillant impliqué dans la conduite de campagnes de ransomwares qui menacent généralement de publier des données privées ou de maintenir l'accès à des données ou des systèmes spécifiques bloqués, généralement en les cryptant, jusqu'à ce que la rançon demandée soit payée. Inclut des URL qui fournissent des stealers, des wipers et des loaders connexes pouvant transporter des charges utiles de ransomwares.
Immobilier	Sites qui fournissent des informations sur les locations, les ventes et les conseils ou informations connexes, y compris des sites pour les éléments suivants : • Entreprises et agents immobiliers • Services de location • Listings (et ensembles)

Catégorie d'URL	Description
	• Amélioration immobilière • Associations de propriétaires • Groupes ou individus de gestion immobilière *Les sites pour les agents hypothécaires et de prêt entrent dans la catégorie Services financiers.*
Détection en temps réel (Filtrage des URL avancé uniquement)	URL qui ont été analysées et détectées par analyse en ligne en temps réel dans le cadre du filtrage avancé des URL.
Loisirs et passe-temps	Sites qui se composent d'informations, de forums, d'associations, de groupes ou de publications liés aux activités récréatives et aux loisirs. *Sites qui vendent des produits liés à des activités récréatives ou des passe-temps, tels que REI.com, entrent dans la catégorie Shopping.*
Référence et recherche	Sites qui fournissent des portails de référence, des documents ou des services personnels, professionnels ou universitaires, y compris des dictionnaires en ligne, des cartes, des almanachs, des informations de recensement, des bibliothèques, de la généalogie et des informations scientifiques. Comprend des sites pour ou liés aux éléments suivants : • Pages jaunes • Calendrier • Bibliothèques publiques • Instituts de recherche • Services de suivi des feux et des véhicules • Documents et dossiers relatifs à l'immobilier, au trafic, etc. (même lorsqu'ils appartiennent au gouvernement)
Religion	Sites contenant des informations sur diverses religions, activités ou événements connexes. Comprend des sites pour les organisations religieuses, les officiels religieux, les lieux de culte, la voyance, l'astrologie, les horoscopes et les accessoires religieux.

Catégorie d'URL	Description
	Les sites pour les écoles primaires ou secondaires privées affiliées à une organisation religieuse, comme les écoles catholiques, dont le programme est axé sur l'enseignement religieux général et les matières laïques, entrent dans la catégorie Établissements d'enseignement.
Activité de numérisation (Filtrage des URL avancé uniquement)	Campagnes menées par des adversaires qui peuvent être des indicateurs de compromission, ou des tentatives de mener des attaques ciblées ou de sonder les vulnérabilités existantes. Elles font habituellement partie des activités de reconnaissance menées par les adversaires.
Moteurs de recherche	Sites qui fournissent une interface de recherche à l'aide de mots-clés, d'expressions ou d'autres paramètres qui peuvent renvoyer des informations, des sites Web, des images ou des fichiers sous forme de résultats.
Éducation sexuelle	Sites qui fournissent des informations sur la reproduction, le développement sexuel, les pratiques sexuelles sans risque, les maladies sexuellement transmissibles, la contraception, des conseils pour une meilleure sexualité, ainsi que tout produit ou accessoire connexe. Comprend les sites Web de groupes, de forums ou d'organisations connexes.
Partagiciels et logiciels gratuits	Sites donnant accès gratuitement, ou contre des dons, à des logiciels, des économiseurs d'écran, des icônes, des fonds d'écran, des utilitaires, des sonneries, des thèmes ou des widgets. Inclut les projets open source.
Achats	Sites qui facilitent l'achat de biens et de services. Comprend les marchands en ligne, les sites des grands magasins, les magasins de détail, les catalogues et les outils d'agrégation ou de surveillance des prix. Les sites de cette catégorie devraient être des marchands en ligne qui vendent une variété d'articles (ou dont le but principal est la vente en ligne). *Un site Web pour une entreprise de produits cosmétiques qui autorise les achats en ligne entre dans la catégorie Produits cosmétiques.*

Catégorie d'URL	Description
Mise en réseau social	Les communautés d'utilisateurs ou les sites où les utilisateurs interagissent les uns avec les autres, publient des messages, des images ou communiquent avec des groupes de personnes. *Les sites, blogs ou forums personnels entrent dans la catégorie Sites et blogs personnels.*
Société	Sites ayant un contenu lié à la population en général ou à des questions qui touchent une grande variété de personnes, telles que la mode, la beauté, les groupes philanthropiques, les sociétés ou les enfants. Comprend les sites Web des restaurants. *Les sites Web d'entreprises liés à l'alimentation, comme Burger King, entrent dans la catégorie Affaires et économie.*
Sports	Sites contenant des informations sur les événements sportifs, les athlètes, les entraîneurs, les officiels, les équipes ou les organisations, les résultats sportifs, les horaires et les nouvelles connexes, ou tout accessoire connexe. Comprend des sites Web pour les sports de fantaisie et les ligues de sport virtuelles. *Les sites ayant pour but principal la vente d'articles de sport entrent dans la catégorie Shopping.*
Conseils et outils boursiers	Sites contenant des informations concernant le marché boursier, le commerce d'actions ou d'options, la gestion de portefeuille, les politiques d'investissement, les cotations ou les nouvelles connexes.
Diffusion multimédia en continu	Sites qui diffusent du contenu audio ou vidéo gratuitement ou à l'achat, y compris les stations de radio en ligne, les services de musique en streaming et l'archivage de podcasts.
Maillots de bain et sous-vêtements	Sites qui contiennent des informations ou des images concernant des maillots de bain, des vêtements intimes ou d'autres vêtements suggestifs

Catégorie d'URL	Description
Formations et outils	Sites qui proposent des services d'éducation et de formation en ligne et du matériel connexe. Comprend les auto-écoles ou les écoles de conduite, la formation en milieu de travail, les jeux, les applications, les outils éducatifs et les académies de tutorat.  *Les classes de compétences spécifiques sont classées en fonction de leur sujet. Par exemple, les sites Web pour les cours de musique entrent dans la catégorie Musique.*
Traduction	Sites qui fournissent des services de traduction, y compris les entrées utilisateur et les traductions d'URL. Ces sites peuvent également permettre aux utilisateurs de contourner le filtrage lorsque le contenu de la page cible est présenté dans le contexte de l'URL du traducteur.
Voyage	Sites qui fournissent des informations sur les voyages, tels que des conseils, des offres, des prix, des informations sur les destinations, le tourisme et les services connexes, tels que des outils de réservation ou de surveillance des prix. Comprend des sites Web pour les éléments suivants : • Attractions locales • Hôtels • Compagnies aériennes • Croisières • Casinos (si le site n'autorise pas le jeu en ligne) • Agences de voyages • Location de véhicules • Parkings
inconnue	Sites qui n'ont pas encore été identifiés par Palo Alto Networks.

Catégorie d'URL	Description
	Si la disponibilité de ce site est importante pour votre entreprise et que vous devez autoriser le trafic, demandez qu'une alerte soit envoyée en présence de sites inconnus, appliquez au trafic les profils de sécurité recommandés et renseignez-vous sur les alertes. *Les mises à jour en temps réel de PAN-DB prennent connaissance des sites inconnus après la première tentative d'accès à ces derniers. Les URL inconnues sont donc identifiées rapidement et deviennent des URL connues que le pare-feu peut gérer en fonction de la véritable catégorie d'URL.*
Armes	Sites qui gèrent les ventes ou proposent des avis, des descriptions ou des instructions concernant les armes, armures, gilets pare-balles et leur utilisation. *Les sites liés au tir à l'argile, aux stands de tir et au tir à l'arc sont classés dans la catégorie principale Armes et dans une catégorie secondaire Sports.*
Publicités Web	Sites avec publicités, médias, contenu et bannières. Comprend des pages pour s'abonner et se désabonner à des newsletters ou à des annonces.
Messagerie Web	Tout site Web qui donne accès à une boîte de réception de courrier électronique et la possibilité d'envoyer et de recevoir des e-mails. L'accent est mis sur les sites Web qui offrent un accès public gratuit ou payant à ces services.
Hébergement Web	Sites qui offrent des services d'hébergement gratuits ou payants pour des pages Web. Comprend des sites contenant des informations sur le développement Web, la publication, la promotion et d'autres méthodes d'augmentation du trafic.

Catégories d'URL axées sur la sécurité

PAN-DB évalue et attribue automatiquement une catégorie de risque (`risque élevé`, `risque moyen` et `risque faible`) aux URL qu'il n'a *pas* classées comme malveillantes ou qu'il *ne classe plus* comme malveillantes parce qu'elles n'affichent qu'une activité bénigne depuis au moins 30 jours. Chaque catégorie de risque possède des critères spécifiques qui doivent être satisfaits pour

qu'une URL reçoive une catégorie donnée. À mesure que le contenu du site change, la catégorie de risque et l'application des politiques s'adaptent dynamiquement.

Si PAN-DB détermine qu'une URL appartient à une catégorie d'URL malveillante, il n'assigne pas de catégorie de risque au site. Au lieu de cela, le pare-feu bloque automatiquement le site, car il présente un risque inacceptable pour la plupart des environnements.

Les adresses IP privées (et les hôtes) sont uniques à l'environnement hôte et sont invisibles pour PAN-DB. Par conséquent, Palo Alto Networks n'attribue pas de cote de risque aux sites de cette catégorie.

Les catégories d'URL axées sur la sécurité facilitent le décryptage ciblé et la mise en œuvre des politiques, contribuant à réduire votre surface d'attaque. Par exemple, vous pouvez bloquer l'accès des utilisateurs aux sites Web à risque élevé et moyen et aux domaines nouvellement enregistrés ou décrypter le trafic vers ces catégories si vous choisissez de les autoriser.

Le tableau suivant énumère les descriptions et les mesures par défaut et recommandées pour chaque catégorie de risque.

Vous ne pouvez pas soumettre une demande de changement pour des catégories d'URL axées sur la sécurité.

Catégorie d'URL	Description
À risque élevé	• Sites dont le modèle ML a identifié le domaine comme ayant des propriétés précédemment liées à des domaines malveillants connus ou ayant des signaux de faible réputation sur le Web. • Sites précédemment confirmés comme étant des sites malveillants, d'hameçonnage ou des sites de commande et contrôle (C2). • Sites associés à une activité malveillante confirmée ou qui partagent un domaine avec un site connu pour être malveillant. • Sites hébergés par un fournisseur de services Internet à toute épreuve • Domaines classés comme DDNS en raison de la présence d'une configuration DNS dynamique active. • Les sites hébergés sur des IP de ASN qui sont connus pour laisser passer le contenu malveillant.

Catégorie d'URL	Description
	• Site classé comme *inconnu*. *Ces sites demeurent à risque élevé jusqu'à ce que PAN-DB termine l'analyse et la catégorisation des sites.* • Les sites restent dans cette catégorie pendant au moins 30 jours. **Action de stratégie par défaut et recommandée : Alerter**
À risque modéré	• Les sites qui ont déjà été confirmés comme étant des sites malveillants, de hameçonnage ou C2 qui présentent uniquement des activités bénignes depuis au moins 30 jours. • Tous les sites de stockage sur le cloud (sites classés comme *stockage et sauvegarde* en ligne). • Adresses IP classées comme *inconnues*. *Ces adresses IP demeurent à risque moyen jusqu'à ce que PAN-DB termine l'analyse et la catégorisation des sites.* • Les sites restent dans cette catégorie pendant 60 jours supplémentaires. **Action de stratégie par défaut et recommandée : Alerter**
À risque faible	Sites qui ne sont pas à risque moyen ou élevé. Ces sites affichent une activité bénigne depuis au moins 90 jours. **Action de stratégie par défaut et recommandée : Autoriser**
Domaines nouvellement enregistrés	Identifie les sites qui ont été enregistrés au cours des 32 derniers jours. Il arrive fréquemment que les nouveaux domaines soient utilisés comme outils dans les campagnes malveillantes.

Catégorie d'URL	Description
	Les domaines nouvellement enregistrés sont souvent générés volontairement ou par les algorithmes de génération de domaines et sont utilisés pour mener des activités malveillantes. Il est recommandé de bloquer cette catégorie d'URL. **Action de stratégie par défaut : Alerter** **Action recommandée de la politique : Bloquer**

Catégories d'URL malveillantes

Nous vous recommandons fortement de bloquer les catégories d'URL suivantes, qui identifient les contenus et comportements malveillants ou d'exploitation.

- **commande et contrôle**
- **violation des droits d'auteur**
- **DNS dynamique**
- **extrémisme**
- **logiciel indésirable**
- **logiciel malveillant**
- **domaine nouvellement enregistré**
- **parqué**
- **phishing**
- **contournement de proxy et anonymiseurs**
- **douteux**
- **ransomware**
- **activité d'analyse**
- **inconnue**

Pour les catégories pour lesquelles vous optez pour une alerte, plutôt que le blocage, vous pouvez contrôler de manière stricte la façon dont les utilisateurs interagissent avec le contenu du site. Par exemple, donnez aux utilisateurs l'accès aux ressources dont ils ont besoin (comme les blogs des développeurs à des fins de recherche ou aux services de stockage cloud), mais prenez les précautions suivantes pour réduire l'exposition aux menaces Web :

- Suivez les meilleures pratiques antispyware, en matière de protection contre les vulnérabilités et de blocage des fichiers. Une mesure de protection consisterait à bloquer les téléchargements de types de fichiers dangereux et à bloquer le JavaScript obscurs pour les sites pour lesquels vous optez pour les alertes.
- Ciblez le déchiffrement en fonction de la catégorie d'URL. Le déchiffrement des sites à risque élevé et à risque modéré serait un bon commencement.

- Affichez une page de réponse aux utilisateurs lorsqu'ils visitent des sites à risque élevé et à risque modéré. Avisez-les que le site auquel ils tentent d'accéder est potentiellement malveillant, et informez-les des précautions à prendre s'ils décident de poursuivre leur consultation du site.
- Empêchez les attaques par hameçonnage en empêchant les utilisateurs de soumettre leurs informations d'identification d'entreprise à des sites y compris ceux qui sont considérés à risque élevé et à risque moyen.

Le tableau suivant répertorie les catégories que PAN-DB considère comme malveillantes *et* bloque par défaut, à l'exception des `adresses IP privées`. Les adresses IP privées (et les hôtes) sont uniques à l'environnement hôte et sont invisibles pour PAN-DB. Par conséquent, Palo Alto Networks n'attribue pas de cote de risque aux sites de cette catégorie.

Catégorie	Action par défaut
Commande et contrôle	Bloquer
Logiciel indésirable	
Logiciel malveillant	
Hameçonnage	
Ransomware	
Activité d'analyse	
Adresses IP privées	Autorisées (aucune action par défaut)

Cas pratiques du URL Filtering

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Il existe de nombreuses façons d'appliquer l'accès aux pages Web au-delà du simple blocage et de l'autorisation de certains sites. Par exemple, vous pouvez utiliser plusieurs catégories par URL pour autoriser les utilisateurs à accéder à un site, tout en bloquant certaines fonctions, comme la soumission des informations d'identification d'entreprise ou le téléchargement des fichiers. Vous pouvez également utiliser les catégories d'URL pour appliquer différents types de politiques, comme l'authentification, le décryptage, la QoS et la sécurité.

Lisez-en davantage sur les différentes façons de déployer URL filtering.

Contrôlez l'accès Web en fonction d'une catégorie d'URL

Vous pouvez créer un profil de filtrage des URL qui précise une action pour chaque catégorie d'URL et associer le profil à une règle de politique de sécurité. Le pare-feu applique la politique au trafic en fonction des paramètres définis dans le profil. Par exemple, pour bloquer tous les sites Web de jeux, vous configureriez l'action de blocage pour la catégorie *jeux* dans un profil de filtrage des URL. Ensuite, vous attacheriez le profil aux règles de politique de sécurité qui autorisent l'accès au Web.

URL Filtering de plusieurs catégories

Chaque URL peut compter un maximum de quatre catégories, y compris une catégorie de risque qui indique la probabilité que le site vous expose à des menaces. Des catégorisations d'URL plus granulaires signifient que vous pouvez passer à une approche qui dépasse le simple fait « de bloquer ou d'autoriser » l'accès Web. Vous pouvez plutôt contrôler l'interaction des utilisateurs avec le contenu en ligne qui, bien que nécessaire pour les affaires, est le plus à risque d'être utilisé dans le cadre d'une cyberattaque.

Par exemple, vous pourriez considérer que certaines catégories d'URL sont plus risquées pour votre organisation, mais vous pourriez hésiter à les bloquer immédiatement, car elles offrent des ressources ou des services précieux (comme des services de stockage dans le cloud ou des blogues). Vous pouvez maintenant autoriser les utilisateurs à visiter des sites qui correspondent à ces types de catégories tout en décryptant et inspectant le trafic et en appliquant l'accès en lecture seule au contenu.

Vous pouvez également définir une catégorie d'URL personnalisée en sélectionnant **Correspondance de catégorie** et en spécifiant deux ou plusieurs catégories PAN-DB dont la nouvelle catégorie sera composée. La création d'une catégorie personnalisée à partir de plusieurs catégories vous permet de cibler l'application pour un site Web ou une page qui correspond à toutes les catégories spécifiées dans l'objet de catégorie d'URL personnalisée.

Bloquez ou autorisez la soumission des informations d'identification d'entreprise en fonction de la catégorie d'URL

Prevent credential phishing(Évitez l'hameçonnage des identifiants) en activant la détection des soumissions d'informations d'identification d'entreprise aux sites par le pare-feu, puis contrôlez ces soumissions en fonction de la catégorie d'URL. Empêchez les utilisateurs d'envoyer des informations d'identification à des sites malveillants et non validés, avertissez-les contre la saisie d'informations d'identification professionnelles sur des sites inconnus ou contre la réutilisation d'informations d'identification professionnelles sur des sites hors travail, et autorisez explicitement les utilisateurs à envoyer leurs informations d'identification sur les sites de l'entreprise et les sites validés.

Application des paramètres de recherche sécurisée

De nombreux moteurs de recherche incluent un paramètre de recherche sécurisée qui filtre les images et vidéos réservées aux adultes dans les résultats de recherche. Vous pouvez activer le pare-feu pour bloquer des résultats de la recherche ou activer de manière transparente la recherche sécurisée pour les utilisateurs finaux qui n'utilisent pas les paramètres de recherche sécurisée les plus stricts. Le pare-feu peut appliquer la recherche sécurisée pour les moteurs de recherche suivants : Google, Yahoo, Bing, Yandex et YouTube. Voyez comment commencer à Mise en œuvre de la recherche sécurisée.

Autoriser l'accès par mot de passe à certains sites

Vous pouvez bloquer l'accès de la plupart des utilisateurs à un site, tout en permettant à certains utilisateurs d'y accéder. Consultez allow password access to certain sites (autoriser l'accès par mot de passe à certains sites).

Bloquez les téléchargements de fichiers à risque élevé de certaines catégories d'URL

Vous pouvez bloquer les téléchargements de fichiers à risque élevé de certaines catégories d'URL donnée en créant une règle de politique de sécurité et en y associant un profil de blocage de fichier.

Politiques d'application de sécurité, de déchiffrement, d'authentification et de QoS basées sur la catégorie d'URL

Vous pouvez appliquer différents types de politiques de pare-feu en fonction des catégories d'URL. Par exemple, si vous avez activé le décryptage, mais que vous souhaitez exclure certaines informations personnelles du décryptage. Dans ce cas, vous pourriez créer une règle de politique de décryptage qui exclut du décryptage les sites Web qui correspondent aux catégories d'URL *financial-services* et *health-and-medicine*. Dans un autre exemple, vous pourriez utiliser la catégorie d'URL *streaming-media* dans une politique de QoS pour appliquer des contrôles de bande passante à tous les sites Web qui correspondent à cette catégorie.

Le tableau suivant décrit les politiques qui acceptent des catégories d'URL comme critère de correspondance :

Type de politique	Description
Déchiffrement	Vous pouvez également utiliser les catégories d'URL pour introduire graduellement le déchiffrement, et pour exclure les catégories d'URL qui peuvent contenir des renseignements sensibles ou personnels du déchiffrement (comme les sites relatifs à des services financiers et à la santé et aux médicaments). Prévoyez de déchiffrer le trafic le plus à risque dans un premier temps (catégories d'URL les plus susceptibles de contenir du trafic malveillant, comme les jeux ou à risque élevé), puis d'en déchiffrer davantage lorsque vous acquérez de l'expérience. Vous pouvez éventuellement déchiffrer les catégories d'URL qui n'affectent pas votre entreprise dans un premier temps (si quelque chose ne se passe pas comme prévu, cela n'affecte pas l'entreprise), par exemple, de nouveaux flux d'informations. Dans les deux cas, déchiffrez quelques catégories d'URL, tenez compte des commentaires des utilisateurs, exécutez les rapports pour vous assurer que le déchiffrement fonctionne comme prévu, puis déchiffrez progressivement quelques catégories d'URL supplémentaires, etc. Planifiez de faire des exclusions de déchiffrement pour exclure les sites du déchiffrement, si vous ne pouvez les déchiffrer pour des raisons techniques ou parce que vous choisissez de ne pas les déchiffrer. *Le déchiffrement du trafic en fonction des catégories d'URL est une pratique recommandée pour le URL Filtering et le déchiffrement.*
Authentification	Pour vous assurer que les utilisateurs s'authentifient avant d'être autorisés à accéder à une catégorie spécifique, vous pouvez associer une catégorie d'URL comme critère de correspondance pour les règles de politique d'authentification.
QoS	Utilisez des catégories d'URL pour allouer des niveaux de débit à des catégories de sites Web spécifiques. Par exemple, vous pouvez autoriser la catégorie *streaming-media*, mais limiter le débit en ajoutant la catégorie d'URL à la règle de politique QoS.
Sécurité	Vous pouvez utiliser une catégorie d'URL comme critère de correspondance ou créer un profil de filtrage des

Type de politique	Description
	URL qui spécifie une action pour chaque catégorie et la rattacher à une règle de politique de sécurité.

Type de politique	Description

	Utilisation des catégories d'URL comme critères de correspondance vs. Application du profil de filtrage des URL à une règle de politique de sécurité
	• *Utilisez les catégories d'URL comme critères de correspondance dans les cas suivants :*
	  • *Pour créer une exception à l'application des catégories d'URL*
	  • *Pour attribuer une action particulière à une catégorie d'URL personnalisée ou prédéfinie. Par exemple, vous pouvez créer une règle de politique de sécurité qui autorise l'accès aux sites de la catégorie sites personnels et blogs.*
	• *Utilisez un profil de filtrage des URL dans les cas suivants :*
	  • *Pour enregistrer le trafic vers les catégories d'URL dans les journaux de filtrage des URL*
	  • *Pour spécifier des actions plus granulaires, telles qu'une alerte, sur le trafic pour une catégorie spécifique*
	  • *Pour configurer une page de réponse qui s'affiche lorsque les utilisateurs accèdent à un site Web bloqué ou bloqué-continuer.*
	Dans un profil de filtrage des URL, les actions spécifiées pour chaque catégorie d'URL s'appliquent uniquement au trafic destiné aux catégories spécifiées dans la règle de la politique de sécurité. Vous pouvez également appliquer un profil particulier à plusieurs règles.

Type de politique	Description
	Si, par exemple, le groupe de sécurité informatique de votre entreprise doit avoir accès à la catégorie *hacking*, mais que tous les autres utilisateurs ne doivent pas pouvoir y accéder, vous devez créer les règles suivantes : • Une règle de politique de sécurité qui autorise le groupe de sécurité informatique à accéder au contenu catégorisé en tant que *hacking*. La règle de politique de sécurité fait référence à la catégorie *hacking* dans l'onglet **Service/URL Category (Catégorie de service/d'URL)** et au groupe de sécurité informatique dans l'onglet **Users (Utilisateurs)**. • Une autre règle de politique de sécurité qui autorise un accès Web général pour tous les utilisateurs. Vous associez à cette règle un profil de filtrage des URL qui bloque la catégorie *piratage*. La politique autorisant l'accès au *piratage* doit être affichée avant celle bloquant le *piratage*. Ceci est dû au fait que la pare-feu évalue les règles de politique du haut vers le bas. Ainsi, lorsqu'un utilisateur qui fait partie du groupe de sécurité essaie d'accéder à un site de *hacking (piratage)*, le pare-feu évalue la règle de politique qui autorise l'accès en premier, puis accorde l'accès à l'utilisateur. Le pare-feu évalue les utilisateurs en les comparant à la règle d'accès Web générale qui bloque l'accès aux sites de *piratage*.

Configuration du URL Filtering

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Après vous être familiarisé avec les concepts de base du filtrage des URL, vous êtes prêt à commencer à utiliser le filtrage des URL. De l'activation d'une Advanced URL Filtering licence (le cas échéant) pour tester votre configuration, ce chapitre couvre ce dont vous avez besoin pour un déploiement efficace du filtrage des URL. Pour tirer le meilleur parti de votre déploiement, suivez les bonnes pratiques de filtrage des URL.

- Activer la licence de filtrage des URL avancé
- Premiers pas avec le URL Filtering
- Configuration du URL Filtering
- Configurer la catégorisation en ligne
- Exceptions de catégories d'URL
- Bonnes pratiques en matière de URL Filtering
- Tester la configuration du filtrage d'URL

Activation de la licence Advanced URL Filtering

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL FilteringLicence (ou une licence de filtrage des URL héritée) ***Remarques :*** • *Les licences de filtrage des URL héritées sont abandonnées, mais les licences héritées actives sont toujours prises en charge.* • *Les licences Prisma Access incluent les capacités Advanced URL Filtering.*

L'abonnement Advanced URL Filtering fournit une analyse des URL en temps réel et une prévention des logiciels malveillants. En plus de l'accès à PAN-DB, la base de données de filtrage des URL développée par Palo Alto Networks pour les recherches d'URL hautes performances, cela offre également une couverture contre les URL et les adresses IP malveillantes.

Les fonctionnalités Advanced URL Filtering sont disponibles sur les pare-feu de nouvelle génération (virtuels et sur site), Strata Cloud Manager, Prisma Access (Managed by Panorama)Cloud NGFW pour AWS et Cloud NGFW pour Azure. Cependant, les pare-feu de nouvelle génération et Cloud NGFW pour Azure nécessitent un abonnement Advanced URL Filtering, tandis que toutes les licences Prisma Access et Cloud NGFW pour AWS incluent des capacités Advanced URL Filtering.

Pour vérifier la compatibilité des fonctionnalités Advanced URL Filtering avec chaque plate-forme Palo Alto Networks prenant en charge le filtrage des URL, consultez Prise en charge du filtrage des URL.

- Strata Cloud Manager
- PAN-OS et Panorama

Activer la licence de filtrage des URL avancé (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

Basculez sur l'onglet **PAN-OS et Panorama** et suivez les instructions qui s'y trouvent pour l'activation de la licence.

Si vous utilisez Strata Cloud Manager :

❑ Validez votre licence de filtrage des URL.

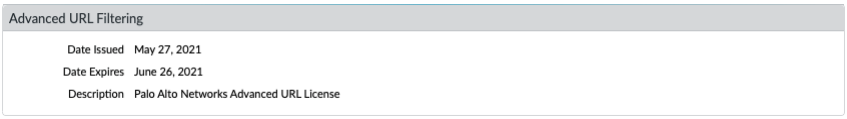
❑ Prise en main du filtrage des URL avancé.

Activer la licence de filtrage des URL avancé (PAN-OS et Panorama)

STEP 1 | Obtenir et installer une licence Advanced URL Filtering.

La licence Advanced URL Filtering inclut l'accès à PAN-DB ; si la licence expire, le pare-feu cesse d'effectuer toutes les fonctions de filtrage des URL, d'application de catégorie d'URL et de recherche d'URL dans le cloud. De plus, toutes les autres mises à jour basées sur le cloud ne fonctionneront pas tant que vous n'aurez pas installé une licence valide.

1. Sélectionnez **Périphérique** > **Licences**, puis, dans la section Gestion des licences, sélectionnez la méthode d'installation de la licence :
   - **Retrieve license keys from license server (Récupérer les clés de licence auprès du serveur de licences)**
   - **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)**
2. Confirmez que dans la section Advanced URL Filtering, le champ **Date d'expiration**, affiche une date valide.



Lorsque vous activez la licence Advanced URL Filtering, vos droits de licence pour PAN-DB et Advanced URL Filtering peuvent ne pas s'afficher correctement sur le pare-feu : il s'agit d'une anomalie d'affichage, pas d'un problème de licence, et cela n'affecte pas l'accès aux services. Vous pouvez mettre à jour les licences sur le pare-feu pour rectifier le problème d'affichage à l'aide de la commande CLI suivante : ***`request license fetch`***.

STEP 2 | Download and install the latest PAN-OS content release (Téléchargez et installez la dernière version du contenu PAN-OS). La version 8390-6607 et ultérieure du contenu des applications et menaces PAN-OS permet aux pare-feu fonctionnant sous PAN-OS 9.x et versions ultérieures d'identifier les URL qui ont été catégorisées à l'aide de la catégorie de détection en temps réel introduite avec x Advanced URL Filtering. Pour plus d'informations sur la mise à jour, reportez-vous aux Notes de mise à jour des applications et du contenu de menace. Vous pouvez également lire la section Notes de version pour les applications et menaces sur le portail d'assistance de Palo Alto Networks ou directement dans l'interface Web du pare-feu : sélectionnez **Périphérique** > **Mises à jour dynamiques** et ouvrez les Notes de version concernant une version de contenu donnée.

Suivez les Best Practices for Applications and Threats Content Updates (Meilleures pratiques pour les mises à jour du contenu de menace et des applications) *lors de la mise à jour vers la dernière version de contenu.*

STEP 3 | Planifiez le pare-feu pour télécharger les mises à jour dynamiques des applications et des menaces.

Une licence Threat Prevention est requise pour recevoir les mises à jour du contenu, notamment de l'antivirus, des applications et menaces.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Dans le champ Schedule (Programmer) de la section Applications and Threats (Applications et menaces), cliquez sur le lien **None (Aucune)** pour planifier des mises à jour périodiques.

   Vous ne pouvez planifier des mises à jour dynamiques que si le pare-feu dispose d'un accès direct à Internet. Si des mises à jour sont déjà planifiées dans une section, le texte du lien affiche les paramètres de la planification.

   Les mises à jour des applications et des menaces contiennent parfois des mises à jour pour le filtrage des URL liées à Mise en œuvre de la recherche sécurisée.

Étapes suivantes :

1. Configurer un profil de filtrage des URL pour définir les politiques d'utilisation du Web de votre organisation.
2. Testez votre configuration de filtrage des URL.

Premiers pas avec le URL Filtering

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering licence (ou une licence de filtrage des URL héritée) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

La première étape pour commencer à utiliser le filtrage des URL consiste à comprendre les modèles d'activité Web des utilisateurs de votre réseau.

Pour observer ces tendances en toute sécurité, nous vous recommandons ce qui suit :

- ❑ Évaluer les catégories d'URL prédéfinies de Palo Alto Networks.
- ❑ Entrez les URL dans notre moteur Test A Site pour voir comment PAN-DB les catégorise.
- ❑ Créez un profil de filtrage des URL (principalement) passif qui alerte sur la plupart des catégories. Lorsque vous sélectionnez le paramètre `alerte` pour une catégorie d'URL, le pare-feu consigne le trafic vers cette catégorie. Ensuite, vous pouvez voir les sites auxquels vos utilisateurs accèdent et décider de l'accès au site approprié pour les catégories d'URL et les sites spécifiques.

  L'envoi d'alertes sur toutes les activités Web peut créer un grand nombre de fichiers journaux. Par conséquent, vous ne souhaiterez peut-être le faire que dans le cadre d'un déploiement initial. À ce moment-là, vous pouvez également réduire les journaux de filtrage des URL en activant l'option ***Page de conteneur de journaux uniquement*** *dans le profil de filtrage des URL afin que seule la page principale qui correspond à la catégorie soit enregistrée, et non les pages ou les catégories suivantes qui peuvent être chargées dans la page conteneur.*
- ❑ Bloquer les catégories d'URL dont nous savons qu'elles sont mauvaises : logiciels malveillants, commande et contrôle et hameçonnage.

- Strata Cloud Manager
- PAN-OS et Panorama

Commencer avec Advanced URL Filtering (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

Basculez sur l'onglet ***PAN-OS et Panorama*** *et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Utiliser Test A Site pour vérifier comment PAN-DB catégorise un site Web spécifique.

Vous pouvez également utiliser la plateforme pour demander un changement de catégorisation pour tout site Web qui, selon vous, a été mal classé.

STEP 2 | Créez un profil passif de gestion des accès à l'URL qui *alerte* sur toutes les catégories.

Le pare-feu génère une entrée de journal de filtrage des URL pour les sites Web dans les catégories d'URL avec une action autre que *autoriser*.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès à l'URL**.
2. Sous Profils de gestion des accès à l'URL, sélectionnez la case située en regard du profil des meilleures pratiques, puis **clonez** le profil.

   Le profil cloné apparaît sous les profils portant le nom `best-practices-1`.
3. Sélectionnez le profil **best-practices-1** et renommez-le. Par exemple, renommez-le `url-monitoring`.

STEP 3 | **Alerte** sur toutes les catégories sauf les logiciels malveillants, les commandes et contrôles et le hameçonnage, qui devraient rester bloqués.

1. Sous **Contrôle d'accès**, sélectionnez toutes les catégories, puis excluez les `logiciels malveillants`, `les commandes et contrôle` et `le hameçonnage`.
2. Avec les catégories toujours en surbrillance, cliquez sur **Définir l'accès** et choisissez **Alerte**.
3. **Bloquez** l'accès aux `logiciels malveillants`, aux `commandes et contrôles` et `au hameçonnage` d'autres catégories d'URL dangereuses connues :
   - phishing
   - DNS dynamique
   - inconnue
   - extrémisme
   - violation des droits d'auteur
   - contournement de proxy et anonymiseurs
   - newly-registered-domain
   - logiciel indésirable
   - parqué
4. **Enregistrez** le profil.

STEP 4 | Appliquer le profil de gestion des accès à l'URL aux règles de politique de sécurité qui autorisent le trafic des clients de la zone de confiance vers Internet.

Un profil Gestion des accès à l'URL n'est actif que lorsqu'il est inclus dans un groupe de profils auquel une règle de politique de sécurité fait référence.

Suivez les étapes pour activer un profil Gestion des accès à l'URL (et tout profil de sécurité).

Assurez-vous que la `Zone Source` dans les règles de politique de sécurité auxquelles vous ajoutez des profils de gestion de l'accès aux URL est définie sur un réseau interne protégé.

STEP 5 | **Transmettre la configuration** pour valider la configuration.

STEP 6 | Vérifiez les journaux d'URL pour voir à quelles catégories de sites Web vos utilisateurs accèdent. Les sites bloqués sont également enregistrés.

Pour plus d'informations sur l'affichage des journaux et la génération de rapports, reportez-vous à la section Surveillance de l'activité Web.

Sélectionnez **Activité** > **Visionneuse de journaux** > **URL**. Les rapports de filtrage des URL vous donnent un aperçu de l'activité Web qui s'est produite sur une période de 24 heures.

STEP 7 | Étapes suivantes :

- Pour tout ce que vous n'autorisez pas ou ne bloquez pas, utilisez des catégories de risques pour rédiger une politique simple basée sur la sécurité des sites Web. PAN-DB classe chaque URL avec un niveau de risque (élevé, moyen et faible). Bien que le caractère malveillant des sites à risque élevé et modéré n'ait pas été confirmé, ils sont étroitement liés aux sites malveillants. Par exemple, ils peuvent se trouver sur le même domaine que des sites malveillants ou ont pu héberger du contenu malveillant jusqu'à tout récemment.

  Vous pouvez prendre des mesures préventives pour restreindre l'interaction de vos utilisateurs avec les sites à risque élevé, car, dans certaines situations, vous pourriez vouloir accorder à vos utilisateurs un accès à des sites qui pourraient également poser des problèmes de sécurité (par exemple, vous pourriez autoriser vos développeurs à utiliser des blogues de développeurs à des fins de recherche, même si les blogues font partie des catégories qui hébergent fréquemment des logiciels malveillants).
- Associez le filtrage des URL avec User-ID pour contrôler l'accès Web en fonction de l'organisation ou du département et pour bloquer l'envoi d'identifiants d'entreprise à des sites non approuvés :
  - Le filtrage des URL empêche le vol des identifiants en détectant l'envoi d'identifiants d'entreprise à des sites en fonction de la catégorie de site. Empêchez les utilisateurs d'envoyer des informations d'identification à des sites malveillants et non validés, avertissez-les contre la saisie d'informations d'identification professionnelles sur des sites inconnus ou avertissez-les contre la réutilisation d'informations d'identification professionnelles sur des sites hors travail, et autorisez explicitement les utilisateurs à envoyer leurs informations d'identification sur les sites de l'entreprise.
  - Ajoutez ou mettez à jour une règle de politique de sécurité avec le profil passif de gestion des accès à l'URL afin qu'elle s'applique à un groupe d'utilisateurs du département, par exemple, Marketing ou Ingénierie. Surveillez l'activité du département et obtenez des commentaires des membres du département pour comprendre les ressources Web qui sont essentielles au travail qu'ils effectuent.
- Considérez tous les façons d'exploiter le filtrage des URL pour réduire votre surface d'attaque. Par exemple, une école peut utiliser le filtrage des URL pour mettre en œuvre une recherche sécurisée stricte pour les étudiants. Ou, si vous avez un centre d'opérations de sécurité, vous pourriez donner seulement aux analystes des menaces un accès par mot de passe à des sites compromis ou dangereux pour la recherche.
- Suivez les bonnes pratiques de filtrage des URL.

Commencer avec Advanced URL Filtering (PAN-OS & Panorama)

STEP 1 | Utiliser Test A Site pour vérifier comment PAN-DB catégorise un site Web spécifique.

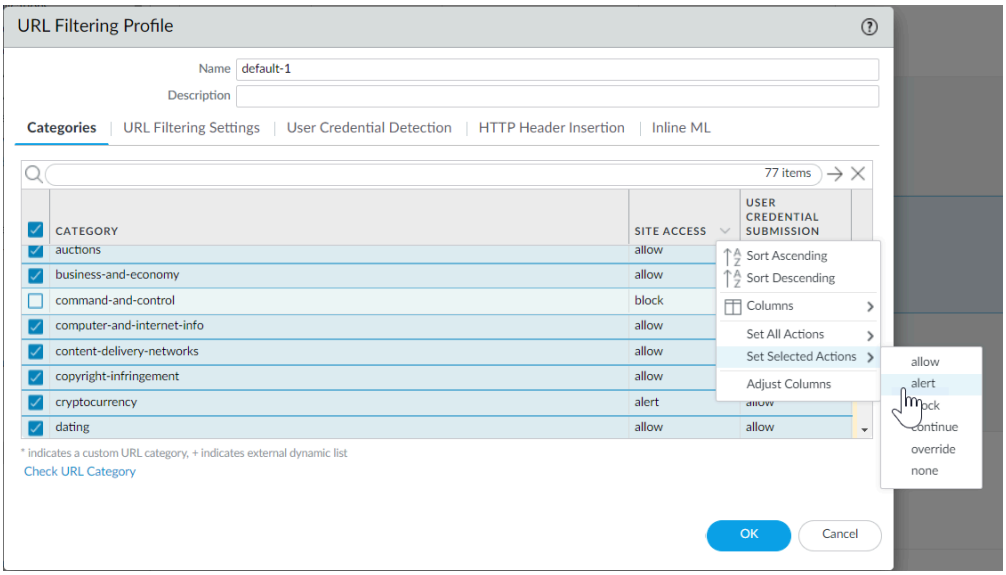
Vous pouvez également utiliser la plateforme pour demander un changement de catégorisation pour tout site Web qui, selon vous, a été mal classé.

STEP 2 | Créez un profil de filtrage des URL passif qui *alerte* sur toutes les catégories.

1. Sélectionnez **Objets** > **Profils de sécurité** > **Filtrage des URL**.
2. Sélectionnez le profil par défaut, puis cliquez sur **Cloner**. Le nouveau profil sera nommé **default-1 (default-1)**.
3. Sélectionnez le profil **défaut-1 (défaut-1)** et renommez-le. Par exemple, renommez-le Surveillance-URL.

STEP 3 | Configurez l'action sur **alert (alerter)** pour toutes les catégories, sauf pour les fichiers malveillants, la commande et contrôle et l'hameçonnage, qui doivent rester bloqués.

1. Dans la section qui répertorie toutes les catégories d'URL, sélectionnez toutes les catégories, puis désélectionnez les logiciels malveillants, la commande et le contrôle et le hameçonnage.
2. À droite de l'en-tête de la colonne *Action (Action)*, cliquez sur la flèche vers le bas, puis sélectionnez **Set Selected Actions (Paramétrer les actions sélectionnées)** et **alert (alerter)**.



3. **Block (Bloquez)** l'accès aux catégories d'URL dangereuses.

   Bloquez l'accès aux catégories d'URL suivantes : logiciels malveillants, phishing, DNS dynamiques, commandes et contrôles, extrémisme,violation des droits d'auteur, contournement des proxy et des anonymiseurs, domaine nouvellement enregistré, logiciel indésirable et URL en parking.

4. Cliquez sur **OK** pour enregistrer le profil.

STEP 4 | Appliquez le profil de filtrage des URL aux règles de politique de sécurité qui autorisent le trafic des clients de la zone de confiance vers Internet.

> *Assurez-vous que la `Zone Source` dans les règles de politique de sécurité auxquelles vous ajoutez des profils de gestion de l'accès aux URL est défini sur un réseau interne protégé.*

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**. Ensuite, sélectionnez une règle de politique de sécurité à modifier.
2. Dans l'onglet **Actions**, modifiez le paramètre de profil.
3. Pour le **Type de profil**, sélectionnez **Profils**. Une liste de profils apparaît.
4. Pour le profil de **filtrage des URL**, sélectionnez le profil que vous venez de créer.
5. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 5 | **Commit (Validez)** la configuration.

STEP 6 | Affichez les journaux de URL Filtering pour voir toutes les catégories de sites Web que consultent vos utilisateurs. Les catégories que vous avez décidé de bloquer sont également journalisées.

Pour plus d'informations sur l'affichage des journaux et la génération de rapports, reportez-vous à Surveillance de l'activité Web.

Sélectionnez **Surveiller** > **Journaux** > **Filtrage des URL**. Une entrée de journal sera créée pour tout site Web figurant dans la base de données de URL Filtering et dont la catégorie est configurée sur une action autre que **allow (autoriser)**. Les rapports de URL Filtering vous donnent un aperçu de l'activité Web qui s'est produite sur une période de 24 heures. (**Surveiller** > **Rapports**).

STEP 7 | Étapes suivantes :

- PAN-DB catégorise chaque URL avec un maximum de quatre catégories, et chaque URL comporte une catégorie de risque (élevé, modéré ou faible). Bien que le caractère malveillant des sites à risque élevé et modéré n'ait pas été confirmé, ils sont étroitement liés aux sites malveillants. Par exemple, ils peuvent se trouver sur le même domaine que des sites malveillants ou ont pu héberger du contenu malveillant jusqu'à tout récemment. Pour tout ce que vous n'autorisez pas ou bloquez, vous pouvez utiliser les catégories de risque pour rédiger des règles de politique simples basées sur la sécurité du site Web.

  Vous pouvez prendre des mesures préventives pour restreindre l'interaction de vos utilisateurs avec les sites à risque élevé, car, dans certaines situations, vous pourriez vouloir accorder à vos utilisateurs un accès à des sites qui pourraient également poser des problèmes de sécurité (par exemple, vous pourriez autoriser vos développeurs à utiliser des blogues de développeurs à des fins de recherche, même si les blogues font partie des catégories qui hébergent fréquemment des logiciels malveillants).
- Associez le filtrage des URL avec User-ID pour contrôler l'accès Web en fonction de l'organisation ou du département et pour bloquer l'envoi d'identifiants d'entreprise à des sites non approuvés :
  - Le filtrage des URL empêche le vol des identifiants en détectant l'envoi d'identifiants d'entreprise à des sites en fonction de la catégorie de site. Empêchez les utilisateurs

d'envoyer des informations d'identification à des sites malveillants et non validés, avertissez-les contre la saisie d'informations d'identification professionnelles sur des sites inconnus ou avertissez-les contre la réutilisation d'informations d'identification professionnelles sur des sites hors travail, et autorisez explicitement les utilisateurs à envoyer leurs informations d'identification sur les sites de l'entreprise.

  - Ajoutez ou mettez à jour une règle de politique de sécurité à l'aide du profil de URL Filtering passif, pour qu'elle s'applique à un groupe d'utilisateurs au sein d'un département, par exemple, le Marketing ou l'Ingénierie (**Politiques** > **Sécurité** > **Utilisateur**). Surveillez l'activité du département et recueillez les commentaires des membres du département pour comprendre les ressources Web qui sont essentielles à leur travail.

- Considérez tous les façons d'exploiter le filtrage des URL pour réduire votre surface d'attaque. Par exemple, une école peut utiliser le filtrage des URL pour mettre en œuvre une recherche sécurisée stricte pour les étudiants. Ou, si vous disposez d'un centre d'opérations de sécurité, vous pouvez ne donner aux analystes des menaces que l'accès par mot de passe à des sites compromis ou dangereux pour la recherche.
- Suivez les bonnes pratiques de filtrage des URL.

Configuration du URL Filtering

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Après avoir planifié votre déploiement de filtrage des URL, vous devez avoir une compréhension de base des types de sites Web auxquels vos utilisateurs accèdent. Utilisez ces informations pour créer un profil de filtrage des URL qui définit la manière dont le pare-feu gère le trafic vers des catégories d'URL spécifiques. Vous pouvez également restreindre les sites sur lesquels les utilisateurs peuvent soumettre des informations d'identification d'entreprise ou appliquer une recherche sécurisée stricte. Pour activer ces paramètres, appliquez le profil de filtrage des URL aux règles de politique de sécurité qui autorisent l'accès au Web.

- Strata Cloud Manager
- PAN-OS et Panorama

Configuration du filtrage des URL (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

Basculez sur l'onglet ***PAN-OS et Panorama*** *et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

Le filtrage des URL est appelé *Gestion de l'accès à l'URL* dans Strata Cloud Manager

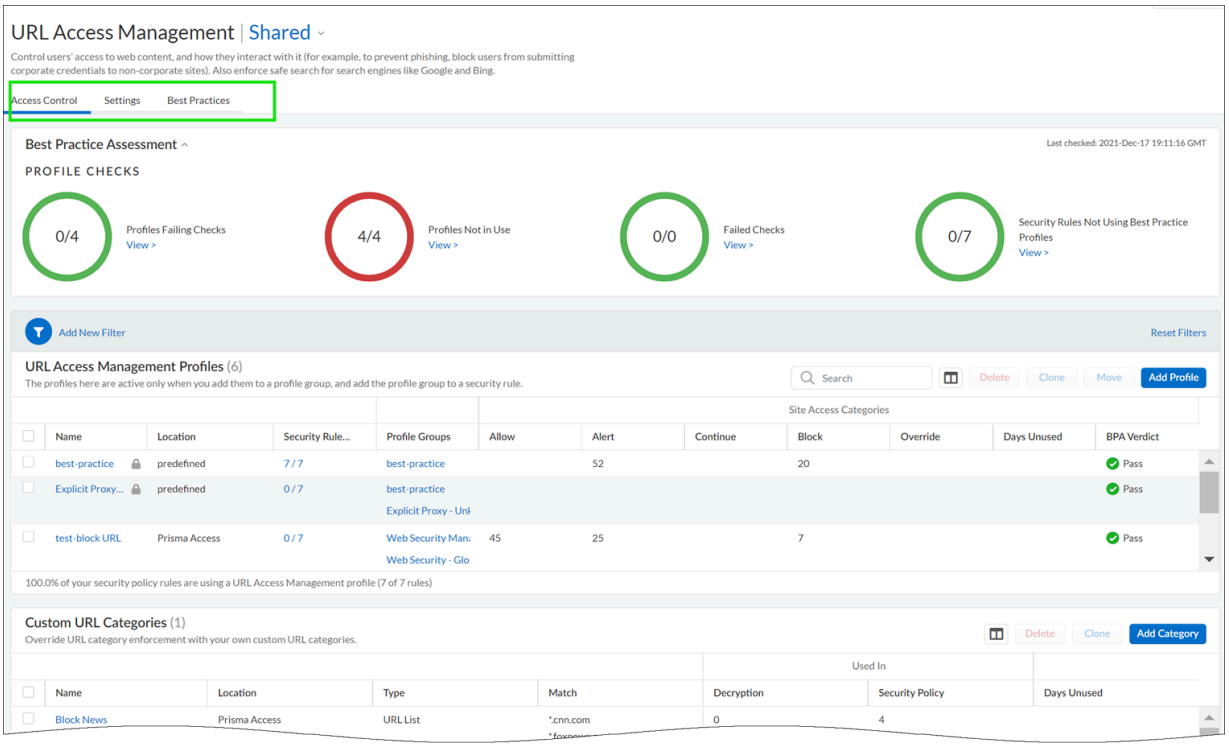
STEP 1 | Vérifiez que votre abonnement Prisma Access couvre le filtrage des URL avancé.

- Allez à Gérer > Configuration du service > Vue d'ensemble > Licences pour confirmer ce qui est inclus avec votre abonnement.

STEP 2 | Explorez le tableau de bord de la gestion des accès à l'URL.

Allez à **Gérer** > **Configuration** > **Services de sécurité** > **Gestion de l'accès à l'URL**.

Déplacez-vous entre les onglets **Contrôle d'accès**, **Paramètres** et **Bonnes pratiques** pour explorer les fonctionnalités de filtrage des URL disponibles.



STEP 3 | Examinez et personnalisez les paramètres généraux de filtrage des URL.

Sur le tableau de bord, allez à **Paramètres** pour voir les paramètres de filtrage des URL par défaut qui s'appliquent à l'ensemble de votre environnement Prisma Access, notamment :

- Paramètres de recherche et de délai de filtrage des URL
- Filtrage des URL remplace certains administrateurs
- Pages de réponse de filtrage des URL
- Paramètres d'isolation du navigateur distant (RBI)

Ajouter automatiquement des jetons de fin aux URL dans une catégorie d'URL personnalisée ou une liste dynamique externe

(PAN-OS 10.1 et versions antérieures) Si vous ajoutez des URL à des catégories d'URL personnalisée ou des listes dynamiques externes (EDL) de type liste d'URL et n'ajoutez pas de barre oblique de fin (/), vous pouvez bloquer ou autoriser plus d'URL que prévu. Par exemple, entrer ***`example.com`*** *au lieu de* ***`example.com/`*** *développe les URL correspondantes vers example.com.website.info ou example.com.br. Prisma Access peut automatiquement ajouter une barre oblique de fin aux URL dans les catégories d'URL personnalisée ou EDL de sorte que, si vous entrez* ***`example.com`****, Prisma Access le traite comme il traiterait* ***`example.com/`*** *et ne considère que ce domaine et ses sous-répertoires correspondent. Allez dans* ***Paramètres*** *>* ***Paramètres généraux*** *et activez l'option* ***Ajouter un jeton de fin aux entrées****.*

(PAN-OS 10.2 et versions ultérieures)Prisma Access ajoute automatiquement une barre oblique de fin aux entrées de domaine.

Vous pouvez personnaliser ces paramètres pour chaque type de déploiement (utilisateurs mobiles, réseaux distants ou connexions de service).

STEP 4 | Créez un profil de gestion de l'accès à l'URL.

Dans le tableau de bord Gestion de l'accès à l'URL, **Ajoutez un profil** et continuez à spécifier les paramètres d'accès Web :

- **Contrôle d'accès** Affiche les catégories et les listes d'URL pour lesquelles vous pouvez définir l'accès Web et la politique d'utilisation. Par défaut, les autorisations **Site Access**

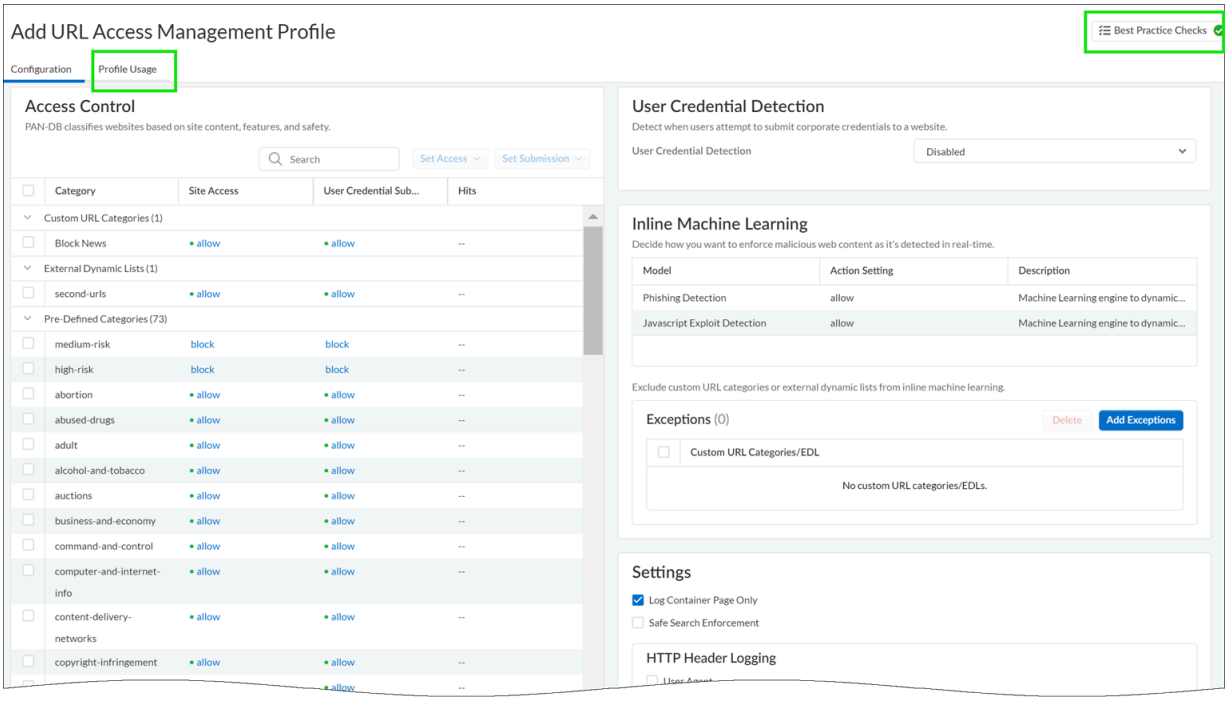
(Accès au site) et **User Credential Submission (Envoi des informations d'identification de l'utilisateur)** pour toutes les catégories sont définies sur **Allow (Autoriser)**.

- Pour chaque catégorie d'URL, configurez la **Détection des identifiants d'utilisateur** afin que les utilisateurs puissent soumettre des identifiants uniquement aux sites appartenant à des catégories d'URL spécifiées.
- Activez **Mise en œuvre de la recherche sécurisée** pour imposer un filtrage de recherche strict sécurisé.
- Activez **Consigner la page de conteneur uniquement** pour enregistrer uniquement les URL qui correspondent au type de contenu spécifié.
- L'activation de la **journalisation de l'en-tête HTTP** fournit une visibilité des attributs inclus dans la requête HTTP envoyée à un serveur.
- Utilisez la **catégorisation en ligne d'URL avancée** pour activer et configurer l'analyse des pages Web en temps réel et gérer les exceptions d'URL.
  - **Activer la catégorisation** locale inline : permet une analyse en temps réel du trafic URL à l'aide de modèles d'apprentissage automatique basés sur un pare-feu, afin de détecter et d'empêcher les variantes de phishing malveillantes et les exploits JavaScript d'entrer dans votre réseau.
  - **Activer la catégorisation Inline** dans le cloud : permet l'analyse en temps réel des URL en transférant le contenu suspect des pages Web vers le cloud pour une analyse supplémentaire, à l'aide de détecteurs basés sur l'apprentissage automatique qui complètent les moteurs d'analyse utilisés par le ML en ligne local.

- Vous pouvez définir des **exceptions** d'URL pour des sites Web spécifiques pour exclure des actions d'apprentissage automatique en ligne.

Notez que :

- Les vérifications des meilleures pratiques sont intégrées au profil pour vous donner une évaluation en direct de votre configuration.
- Une fois que vous avez terminé d'activer un profil, vous pouvez examiner l'utilisation du profil pour voir si des règles de politique de sécurité font référence au profil.



STEP 5 | Appliquez le profil Gestion des accès URL à une règle de politique de sécurité.

Un profil Gestion des accès URL n'est actif que lorsqu'il est inclus dans un groupe de profils auquel une règle de politique de sécurité fait référence.

Suivez les étapes pour activer un profil Gestion de l'accès à l'URL (et tout profil de sécurité). Assurez-vous de **Transmettre la configuration**

Configuration du filtrage des URL (PAN-OS et Panorama)

STEP 1 | Créez un profil de URL Filtering.

Configurez un Profil de filtrage des URL suivant les meilleures pratiques pour assurer une protection contre les URL qui ont été signalées comme hébergeant du contenu malveillant ou à risque.

Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **URL Filtering (Filtrage des URL)** et **Add (Ajouter)** ou modifiez un profil de filtrage des URL.

STEP 2 | Définir l'accès au site pour chaque catégorie d'URL.

Sélectionnez **Categories (Catégories)**, puis définissez l'accès aux sites pour chaque catégorie d'URL :

- **allow (autorise)** le trafic destiné pour cette catégorie d'URL, le trafic autorisé n'est pas journalisé
- Sélectionnez **alert (alerter)** afin d'avoir une visibilité des sites auxquels vos utilisateurs accèdent. Le trafic correspondant est autorisé, mais un journal de URL filtering est généré pour journaliser les situations où un utilisateur accède à un site appartenant à cette catégorie.
- Sélectionnez **block (bloquer)** pour refuser l'accès au trafic correspondant à la catégorie et pour activer la journalisation du trafic bloqué.
- Sélectionnez **continue (continuer)** et une page d'avertissement s'affichera et demandera aux utilisateurs de cliquer sur **Continue (Continuer)** pour accéder à un site appartenant à cette catégorie.
- Pour n'autoriser l'accès que si les utilisateurs fournissent un mot de passe configuré, sélectionnez **override (contrôle prioritaire)**. Pour obtenir de plus amples précisions sur ce paramètre, reportez-vous à la section Autoriser l'accès par mot de passe à certains sites.

STEP 3 | Configurez le profil de filtrage des URL afin qu'il détecte les saisies de noms d'utilisateurs d'entreprise valides sur des catégories d'URL autorisées.

Le pare-feu saute automatiquement la vérification de l'envoi des informations d'identification pour les APP-ID associés à des sites qui n'ont jamais hébergé de contenu malveillant ou de hameçonnage afin d'assurer un rendement optimal et un faible taux de faux positifs, et ce, même si vous activez les vérifications dans la catégorie correspondante. La liste des sites que le pare-feu ignorera lors de ses contrôles d'informations d'identification est mise à jour de manière automatique à travers les mises à jour d'applications et de menaces.

1. Sélectionnez **User Credential Detection (Détection des informations d'identification de l'utilisateur)**.
2. Sélectionnez l'une des methods to check for corporate credential submissions (Méthodes de vérification des saisies d'informations d'identification d'entreprise) sur les pages

web dans la liste déroulante**User Credential Detection (Détection des informations d'identification de l'utilisateur)** :

- **Use IP User Mapping (Utiliser le mappage des adresses IP aux utilisateurs)** : cherche des envois de noms d'utilisateur d'entreprise valides et vérifie que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Le pare-feu fait correspondre le nom d'utilisateur saisi à la table de mappage adresse IP / nom d'utilisateur. Vous pouvez utiliser n'importe laquelle des méthodes de mappage d'utilisateur décrites dans Map IP Addresses to Users (Mappage d'adresses IP à des utilisateurs).
- **Use Domain Credential Filter (Utiliser le filtrage par informations de domaine)** : Contrôle les saisies de noms d'utilisateurs d'entreprise et mots de passe valides et vérifie que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Pour obtenir des instructions sur la configuration d'un User-ID pour activer cette méthode, reportez-vous à la section Configuration de la Détection des informations d'identification avec l'agent User-ID Windows.
- **Use Group Mapping (Utiliser le mappage de groupe)** : contrôle les saisies de nom d'utilisateur valide basé sur la table de mappage d'utilisateurs à des groupes renseignée quand vous configurez le pare-feu pour le map users to groups (Mappage d'utilisateurs à des groupes).

  Avec le mappage de groupe, vous pouvez appliquer la détection des informations d'identification à **any (toute)** partie du répertoire, ou à un groupe spécifique, comme le département informatique qui aura accès à vos applications les plus sensibles.

  Cette méthode peut entrainer des faux positifs dans des environnements qui n'ont pas d'identifiants uniquement structurés, donc vous devriez n'utiliser cette méthode que pour protéger vos comptes utilisateurs les plus sensibles

3. Sélectionnez le **Degré de gravité d'enregistrement des détections de nom d'utilisateur valide** que le pare-feu utilise pour consigner la détection des saisies d'informations d'identification d'entreprise.

STEP 4 | Configurez le profil de filtrage des URL pour détecter le hameçonnage et le JavaScript malveillant en temps réel à l'aide de la catégorisation en ligne locale.

STEP 5 | Autorisez ou empêcher les utilisateurs de soumettre des informations d'identification d'entreprise à des sites, selon la catégorie d'URL afin d'prevent credential phishing (empêcher l'hameçonnage des informations d'identification).

> *Le pare-feu saute automatiquement la vérification de l'envoi des informations d'identification pour les APP-ID associés à des sites qui n'ont jamais hébergé de contenu malveillant ou de hameçonnage afin d'assurer un rendement optimal et un faible taux de faux positifs, et ce, même si vous activez les vérifications dans la catégorie correspondante. La liste des sites que le pare-feu ignorera lors de ses contrôles d'informations d'identification est mise à jour de manière automatique à travers les mises à jour d'applications et de menaces.*

1. Pour chaque catégorie d'URL à laquelle le **Site Access (Accès au site)** est autorisé, sélectionnez l'option **User Credential Submissions (Envoi des informations d'identification de l'utilisateur)** à appliquer :
   - **alert (alerter)** : autorise les utilisateurs à saisir des informations d'identification sur le site Web, mais génère un journal d'alerte de URL filtering chaque fois qu'un utilisateur saisit des informations d'identification sur les sites de cette catégorie d'URL.
   - **allow (autoriser)** (par défaut) – Autorise les utilisateurs à saisir des informations d'identification sur le site Web.
   - **bloquer** : affiche la page de blocage anti-hameçonnage pour empêcher les utilisateurs de saisir des informations d'identification sur le site Web.
   - **continuer**— Présente la page suivante anti-hameçonnage, qui oblige les utilisateurs à cliquer sur **Continuer** pour accéder au site.
2. Configurez le profil de filtrage des URL pour détecter les soumissions d'informations d'identification d'entreprise aux sites Web dans les catégories d'URL autorisées.

STEP 6 | Définissez des exceptions de catégorie d'URL pour spécifier les sites Web qui doivent toujours être bloqués ou autorisés, quelle que soit la catégorie d'URL.

Par exemple, pour réduire le nombre de journaux de filtrage URL, vous pouvez ajouter vos sites Internet à la liste d'autorisation, afin qu'aucun journal ne soit généré pour ces sites, ou s'il y a un site Internet qui est très utilisé et qui n'est pas en rapport avec le travail, vous pouvez ajouter ce site à la liste d'interdiction

Les actions de stratégie configurées pour les catégories d'URL personnalisées sont prioritaires sur les URL correspondantes dans les listes dynamiques externes.

Les éléments figurant dans la liste d'interdiction seront toujours bloqués, quelle que soit l'action attribuée à la catégorie associée, et les URL figurant dans la liste d'autorisation seront toujours autorisées.

Pour plus d'informations sur le format approprié et l'utilisation des caractères génériques, consultez les directives relatives aux exceptions de catégorie d'URL.

STEP 7 | Activer la mise en œuvre de la recherche sécurisée.

STEP 8 | Enregistrez uniquement la page visitée par un utilisateur pour les événements de filtrage des URL.

1. Sélectionnez **Paramètres de filtrage des URL** et activez **Enregistrez uniquement la page du conteneur** (par défaut) afin que le pare-feu enregistre uniquement la page principale qui correspond à la catégorie, et non les pages ou catégories suivantes qui se chargent dans la page du conteneur.
2. Pour activer la journalisation de toutes les pages/catégories, décochez la case **Log container page only (Page conteneur de journaux uniquement)**.

STEP 9 | Activez la Journalisation de l'en-tête HTTP pour un ou plusieurs des champs d'en-tête HTTP pris en charge.

Sélectionnez **URL Filtering Settings (Paramètres de URL Filtering)** et sélectionnez un ou plusieurs des champs suivants à journaliser :

- **User-Agent (Utilisateur-Agent)**
- **Référant**
- **X-Forwarded-For**

STEP 10 | Enregistrez le profil de filtrage des URL.

Cliquez sur **OK**.

STEP 11 | Appliquez le profil de filtrage des URL aux règles de politique de sécurité qui autorisent le trafic des clients de la zone de confiance vers Internet.

Assurez-vous que la `zone source` dans les règles de politique de sécurité auxquelles vous ajoutez des profils de filtrage des URL est définie sur un réseau interne protégé.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**. Ensuite, sélectionnez une règle de politique de sécurité à modifier.
2. Dans l'onglet **Actions**, modifiez le paramètre de profil.
3. Pour le **Type de profil**, sélectionnez **Profils**. Une liste de profils apparaît.
4. Pour le profil de **filtrage des URL**, sélectionnez le profil que vous venez de créer.
5. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 12 | **Commit (Validez)** la configuration.

STEP 13 | Testez votre configuration de filtrage des URL.

STEP 14 | (Meilleure pratique) Activez l'option **Suspendre la demande client pour la recherche de catégorie** pour bloquer les demandes client pendant que le pare-feu effectue des recherches de catégorie d'URL.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content ID**.
2. Sélectionnez **Garder en mémoire la demande du client pour la recherche de catégorie**.
3. **Commit (Validez)** vos modifications.

STEP 15 | Fixer le temps, en seconde, avant qu'une recherche de catégorie n'expire

1. Sélectionnez l'**icône de l'engrenage** > **Device (Périphérique)** > **Setup (Configuration)** > **Content ID (ID contenu)**.
2. Entrez un nombre pour le **délai d'expiration de la recherche de catégorie (sec)**.
3. Cliquez sur **OK**.
4. **Commit (Validez)** vos modifications.

Configurer la catégorisation en ligne

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering licence (ou une licence de filtrage des URL héritée) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Pour activer la catégorisation en ligne, associez un profil de filtrage d'URL configuré avec des paramètres de catégorisation en ligne à une règle de politique de sécurité (voir Configurer une politique de sécurité de base).

La catégorisation locale en ligne du filtrage d'URL n'est actuellement pas prise en charge sur le dispositif virtuel VM-50 ou VM50L.

- Strata Cloud Manager
- PAN-OS et Panorama

Configurer la catégorisation en ligne (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS et Panorama** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Mettez à jour ou créez un profil de gestion d'accès à l'URL.

1. Allez à **Gérer** > **Configuration** > **Services de sécurité** > **Gestion de l'accès à l'URL**.
2. Dans le tableau de bord Gestion de l'accès à l'URL, sélectionnez un profil de gestion de l'accès à l'URL ou **Ajoutez un profil**.

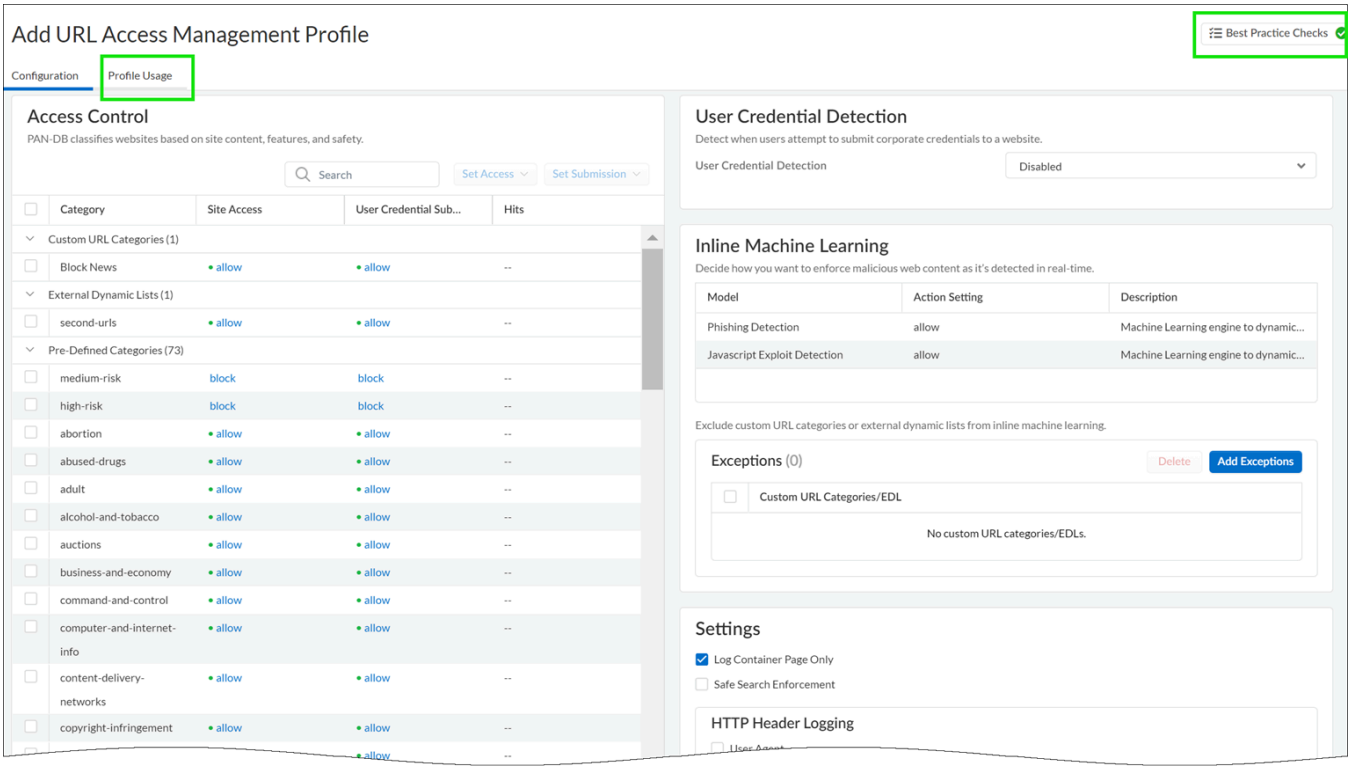
   Si vous créez un nouveau profil, configurez des paramètres dans le profil, tels que l'accès au site pour les catégories d'URL (**Contrôle d'accès**). Configurer le filtrage des URL (gestion du cloud) décrit les paramètres disponibles.
3. Sous **Catégorisation d'URL en ligne avancée**, sélectionnez un type de catégorisation en ligne.

   Les deux options permettent l'analyse des pages Web en temps réel et gèrent les exceptions d'URL.

   - **Activer la catégorisation Inline** dans le cloud : permet l'analyse en temps réel des URL en transférant le contenu suspect des pages Web vers le cloud pour une analyse

supplémentaire, à l'aide de détecteurs basés sur l'apprentissage automatique qui complètent les moteurs d'analyse utilisés par le ML en ligne local.

- **Activer la catégorisation** locale inline : permet une analyse en temps réel du trafic URL à l'aide de modèles d'apprentissage automatique basés sur un pare-feu, afin de détecter et d'empêcher les variantes de phishing malveillantes et les exploits JavaScript d'entrer dans votre réseau.
- Vous pouvez également définir des **exceptions** d'URL pour exclure des sites Web spécifiques des actions d'apprentissage automatique en ligne.



4. **Enregistrez** le profil.

STEP 2 | Appliquez le profil Gestion des accès URL à une règle de politique de sécurité.

Pour activer un profil de gestion des accès à l'URL (et tout profil de sécurité), ajoutez-le au `groupe de profils` et référencez-le dans une règle de politique de sécurité.

Configurer la catégorisation en ligne (PAN-OS et Panorama)

Dans PAN-OS 10.2, la fonctionnalité de filtrage des URL en ligne ML a été renommée Catégorisation en ligne. Par conséquent, la tâche PAN-OS 10.1 utilise l'expression Filtrage des URL en ligne ML, tandis que la tâche PAN-OS 10.2 et versions ultérieures utilise la catégorisation en ligne. Pour plus d'informations, consultez l'entrée de filtrage des URL en ligne ML dans Considérations relatives à la mise à niveau/rétrogradation de PAN-OS 10.2.

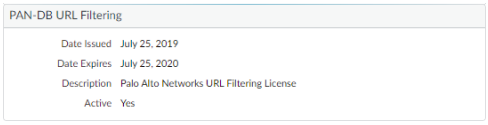
- PAN-OS 10.1
- PAN-OS 10.2 et versions ultérieures

Configurer la catégorisation en ligne (PAN-OS 10.1)

STEP 1 | Connectez-vous à l'interface Web PAN-OS.

STEP 2 | Vérifiez que vous disposez d'un abonnement actif de filtrage des URL hérité ou de filtrage des URL avancé.

Sélectionnez **Périphérique** > **Licences** et confirmez qu'une licence de filtrage des URL est disponible et n'a pas expiré.

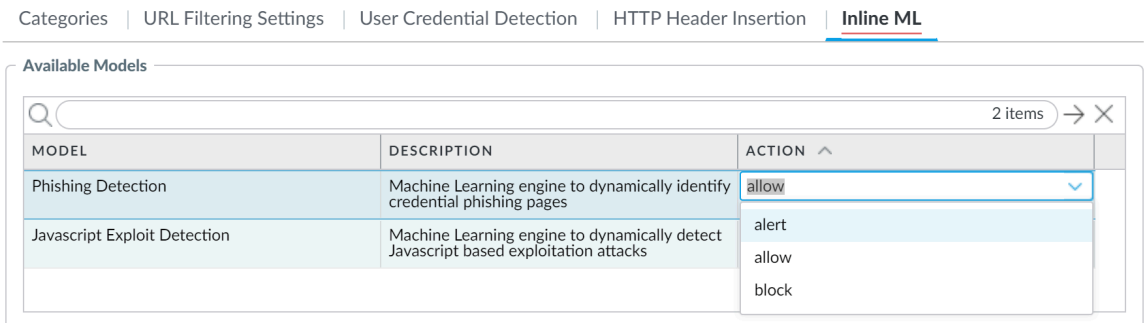


STEP 3 | Configurez les paramètres de filtrage des URL en ligne ML dans un profil de filtrage des URL.

1. Sélectionnez **Objets** > **Profils de sécurité** > **Filtrage des URL**, puis **Ajouter** ou sélectionner un profil de filtrage des URL.
2. Sélectionnez **en ligne ML** et définissez une **Action** pour chaque modèle en ligne ML.

   Il existe deux moteurs de classification disponibles pour chaque type de contenu de page Web malveillant : **Hameçonnage** et **JavaScript Exploit**.

   - **Blocage**—lorsque le pare-feu détecte un site Web avec un contenu de hameçonnage, il génère une entrée de journal de filtrage des URL.
   - **Alerte** : le pare-feu permet l'accès au site Web et génère une entrée de journal de filtrage des URL.
   - **Autoriser**—le pare-feu permet l'accès au site Web, mais ne génère pas d'entrée dans le journal du filtrage des URL.



3. Cliquez sur **OK** pour enregistrer vos modifications.
4. **Commit (Validez)** vos modifications.

STEP 4 | (Facultatif) Ajoutez des exceptions d'URL à votre profil de filtrage des URL si vous rencontrez des faux positifs.

Vous pouvez ajouter des exceptions en spécifiant une liste dynamique externe à partir du profil de filtrage des URL ou en ajoutant une entrée de page Web à partir des journaux de filtrage des URL à une catégorie d'URL personnalisée.

1. Sélectionnez **Objects (Objets) > Security Profiles (Profil de sécurité) > URL Filtering (URL Filtering)**.
2. Sélectionnez un profil de filtrage des URL pour lequel vous souhaitez exclure des URL spécifiques, puis sélectionnez **en ligne ML**.
3. **Ajouter** une liste dynamique externe préexistante de type d'URL. Si aucune n'est disponible, créez une nouvelle liste dynamique externe.
4. Cliquez sur **OK** pour enregistrer vos modifications.
5. **Commit (Validez)** vos modifications.

Ajout d'exceptions de fichier à partir des entrées de journal du URL Filtering.

1. Sélectionnez **Monitor (Moniteur) > Logs (Journaux) > URL Filtering (Filtrage des URL)** et filtrez les journaux pour les entrées d'URL avec un Verdict Inline ML **malicious-javascript (javascript malveillant)** ou **phishing**. Sélectionnez un journal de URL Filtering pour une URL pour laquelle vous souhaitez créer une exception.
2. Accédez à **Vue détaillée du journal** et faites défiler vers le bas jusqu'au volet **Détails** puis sélectionnez **Créer une exception** situé à côté de **Verdict en ligne ML**.

3. Sélectionnez une catégorie personnalisée pour l'exception d'URL et cliquez sur **OK**.

   La nouvelle exception d'URL se trouve dans la liste à laquelle elle a été ajoutée, sous **Objects (Objets) > Custom Objects (Objets personnalisés) > URL Category (Catégorie d'URL)**.

STEP 5 | (Facultatif) Vérifiez l'état de la connectivité de votre pare-feu au service Inline ML dans le cloud.

Utilisez la commande CLI suivante sur le pare-feu pour afficher l'état de la connexion.

```
show mlav cloud-status
```

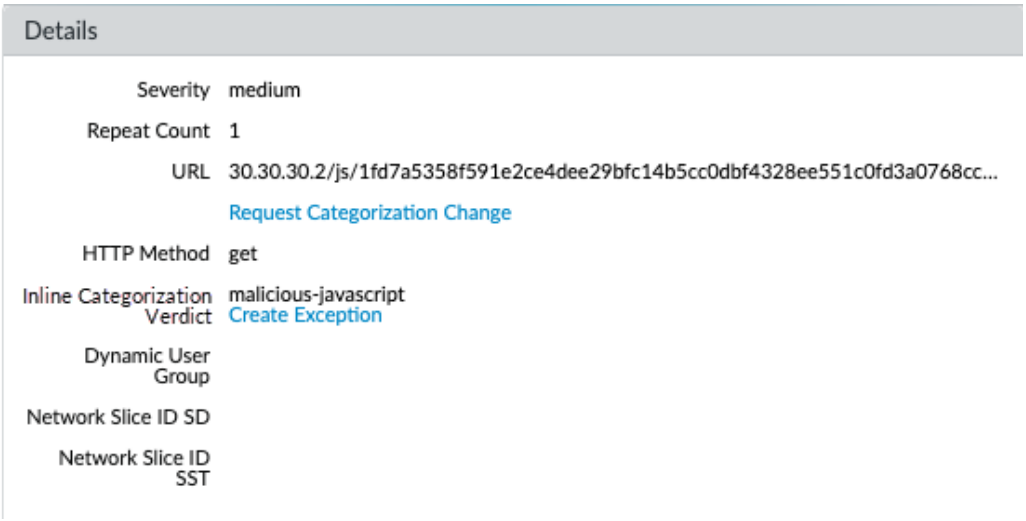
Par exemple :

```
show mlav cloud-status MLAV cloud Current cloud server:
 ml.service.paloaltonetworks.com Cloud connection: connected
```

Si vous ne pouvez pas vous connecter au service cloud en ligne ML, vérifiez que le domaine ML ml.service.paloaltonetworks.com n'est pas bloqué.

STEP 6 | Testez le déploiement de votre filtrage des URL.

Pour afficher des informations sur les pages Web qui ont été traitées à l'aide du filtrage des URL en ligne ML, filtrez les journaux (**Moniteur > Journaux > Filtrage des URL**) sur la base du **Verdict en ligne ML**. Les pages web dont il a été déterminé qu'elles contiennent des menaces sont classées par catégorie, avec des verdicts de **phishing** ou de **malicious-javascript (javascript malveillant)**. Par exemple :



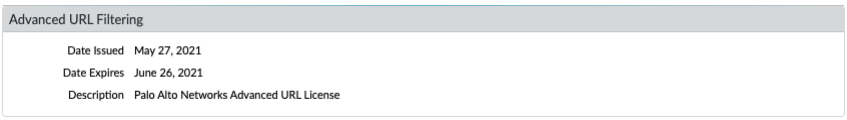
Configurer la catégorisation en ligne (PAN-OS 10.2 et versions ultérieures)

STEP 1 | Connectez-vous à l'interface Web PAN-OS.

STEP 2 | Pour tirer parti de la catégorisation en ligne, vous devez disposer d'un abonnement de filtrage des URL avancé actif.

La catégorisation locale en ligne peut être activée si vous êtes titulaire d'un abonnement de filtrage d'URL hérité.

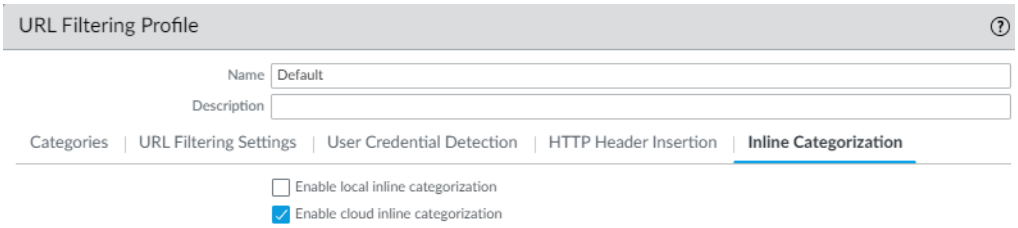
Vérifiez que vous disposez d'un abonnement au filtrage d'URL avancé. Pour vérifier les abonnements pour lesquels vous disposez de licences actuellement actives, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que les licences sont disponibles et ne sont pas expirées.



STEP 3 | Mettez à jour ou créez un nouveau profil de filtrage des URL pour activer la catégorisation en ligne dans le cloud.

*L'action de stratégie utilisée par la catégorisation en ligne locale et cloud dépend des paramètres configurés sous l'onglet **Catégories** .*

1. Sélectionnez un **Profil de filtrage des URL** existant ou **Ajoutez** un nouveau profil (**Objets** > **Profils de sécurité** > **Filtrage des URL**).
2. Sélectionnez votre profil de filtrage d'URL, puis accédez à **Catégorisation en ligne** et activez les méthodes de catégorisation en ligne que vous souhaitez déployer.
   - **Activer la catégorisation en ligne dans le cloud** : un moteur d'apprentissage profond en ligne basé sur le cloud qui analyse le contenu suspect des pages Web en temps réel pour protéger les utilisateurs contre les attaques Web zero-day, y compris les attaques de phishing ciblées et d'autres attaques Web qui utilisent des techniques d'évasion avancées.
   - **Activer la catégorisation locale en ligne** : un moteur de détection basé sur un pare-feu utilisant des techniques d'apprentissage automatique pour empêcher les variantes malveillantes des exploits JavaScript et les attaques de phishing intégrées dans les pages Web.



3. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

STEP 4 | (Facultatif) Ajoutez des exceptions d'URL à votre profil de filtrage des URL si vous rencontrez des faux positifs. Vous pouvez ajouter des exceptions en spécifiant une liste dynamique externe ou une liste de catégories d'URL personnalisée dans le profil filtrage d'URL. Les exceptions spécifiées s'appliquent à la fois à la catégorisation cloud et à la catégorisation en ligne locale.

*Les exceptions d'URL créées via d'autres mécanismes qui ajoutent des entrées à la catégorie d'URL personnalisée (**Objets** > **Custom Objects** > **URL Category**)*

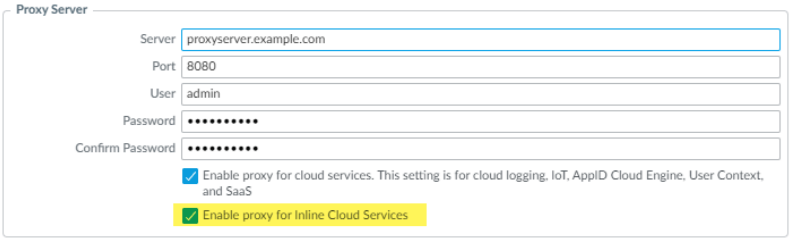
peuvent également fonctionner comme des exceptions pour la catégorisation en ligne.

1. Sélectionnez **Objects (Objets) > Security Profiles (Profil de sécurité) > URL Filtering (URL Filtering)**.
2. Sélectionnez un profil de filtrage des URL pour lequel vous souhaitez exclure des URL spécifiques, puis sélectionnez **Catégorisation en ligne**.
3. Cliquez sur **Ajouter** pour sélectionner une liste dynamique externe basée sur une URL préexistante ou une catégorie d'URL personnalisée. Si aucune n'est disponible, créez une nouvelle liste dynamique externe ou catégorie d'URL personnalisée, respectivement.
4. Cliquez sur **OK** pour enregistrer le profil de URL Filtering et **Commit (Validez)** vos modifications.

STEP 5 | (Obligatoire lorsque le pare-feu est déployé avec un serveur proxy explicite) Configurez le serveur proxy utilisé pour accéder aux serveurs qui facilitent les requêtes générées par toutes les fonctionnalités d'analyse cloud en ligne configurées. Un seul serveur proxy peut être spécifié et s'applique à tous les services de mise à jour de Palo Alto Networks, y compris tous les services de cloud et de journalisation en ligne configurés.

1. (PAN-OS 11.2.3 et versions ultérieures) Configurez le serveur proxy via PAN-OS.
   1. Sélectionnez **Device (Périphérique)** > **Configuration** > **Services** et modifiez les détails des **Services**.
   2. Spécifiez les paramètres du **Proxy Server (Serveur proxy)** et cliquez sur **Enable proxy for Inline Cloud Services (Activer le proxy pour les services cloud en ligne**. Vous pouvez fournir une adresse IP ou un FQDN dans le champ **Server (Serveur)**.

      Le mot de passe du serveur proxy doit contenir au moins six caractères.

   3. Cliquez sur **OK**.
2. (Pour les versions suivantes uniquement : PAN-OS 10.2.11 et versions ultérieures et PAN-OS 11.1.5 et versions ultérieures) Configurez le serveur proxy via la CLI du pare-feu.
   1. Accédez à la CLI du pare-feu.
   2. Configurez les paramètres du serveur proxy de base à l'aide des commandes CLI suivantes :

      ```
      set deviceconfig system secure-proxy-server <FQDN_or_IP>
       set deviceconfig system secure-proxy-port <1-65535>
      ```



```
set deviceconfig system secure-proxy-user <value> set
deviceconfig system secure-proxy-password <value>
```

Le mot de passe du serveur proxy doit contenir au moins six caractères.

3. Autorisez le serveur proxy à envoyer des requêtes aux serveurs de services cloud en ligne à l'aide de la commande CLI suivante :

```
debug dataplane mica set inline-cloud-proxy enable
```

4. Affichez l'état opérationnel actuel de la prise en charge du proxy pour les services cloud en ligne à l'aide de la commande CLI suivante :

```
debug dataplane mica show inline-cloud-proxy
```

Par exemple :

```
debug dataplane mica show inline-cloud-proxy Le proxy pour
 les services avancés est désactivé
```

STEP 6 | (Facultatif) Définissez le nom de domaine complet (FQDN) du contenu cloud utilisé par le pare-feu pour gérer les demandes de service de catégorisation en ligne. Le nom de domaine complet par défaut se connecte à hawkeye.services-edge.paloaltonetworks.com, puis se résout au serveur de services cloud le plus proche. Vous pouvez remplacer la sélection automatique du serveur en spécifiant un serveur de contenu cloud régional qui répond le mieux à vos exigences en matière de résidence et de performances des données.

Le nom de domaine complet de contenu cloud est une ressource utilisée à l'échelle mondiale et affecte la façon dont les autres services qui dépendent de cette connexion envoient des charges utiles de trafic.

Vérifiez que le pare-feu utilise le bon FQDN Content Cloud (**Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (ID de contenu)** > **Content Cloud Setting (Paramètre du Cloud de contenu)**) pour votre région et modifiez le FQDN si nécessaire :

- États-Unis—**us.hawkeye.services-edge.paloaltonetworks.com**
- Europe—**eu.hawkeye.services-edge.paloaltonetworks.com**
- Royaume-Uni —**uk.hawkeye.services-edge.paloaltonetworks.com**

  Le nom de domaine complet du contenu cloud basé au Royaume-Uni fournit une prise en charge du service de catégorisation en ligne du filtrage avancé des URL en se connectant au service principal situé dans l'UE (eu.hawkeye.services-edge.paloaltonetworks.com).
- APAC—**apac.hawkeye.services-edge.paloaltonetworks.com**

STEP 7 | (Facultatif) Vérifiez l'état de la connectivité de votre pare-feu aux serveurs de catégorisation Inline.

1. Le serveur ml.service.paloaltonetworks.com fournit des mises à jour périodiques pour les composants basés sur un pare-feu liés au fonctionnement du cloud et à la catégorisation locale en ligne.

   Utilisez la commande CLI suivante sur le pare-feu pour afficher l'état de la connexion.

   ```
   show mlav cloud-status
   ```

   Par exemple :

   ```
   show mlav cloud-status MLAV cloud Current cloud server:
    ml.service.paloaltonetworks.com Cloud connection: connected
   ```

   Si vous ne pouvez pas vous connecter au service cloud Inline ML, vérifiez que le domaine suivant n'est pas bloqué : ml.service.paloaltonetworks.com.

2. Le serveur hawkeye.services-edge.paloaltonetworks.com est utilisé par la catégorisation en ligne dans le cloud pour gérer les demandes de service.

   Utilisez la commande CLI suivante sur le pare-feu pour afficher l'état de la connexion.

   ```
   show ctd-agent status security-client
   ```

   Par exemple :

   ```
   show ctd-agent status security-client ... Security Client
    AceMlc2(1) Serveur cloud actuel : hawkeye.services-
   edge.paloaltonetworks.com Connexion cloud : connecté ...
   ```

   Sortie CLI raccourcie pour plus de brièveté.

   Si vous ne parvenez pas à vous connecter au service cloud de filtrage avancé d'URL, vérifiez que le domaine suivant n'est pas bloqué : hawkeye.services-edge.paloaltonetworks.com.

STEP 8 | Installez un certificat de périphérique de pare-feu mis à jour utilisé pour s'authentifier auprès du service cloud de filtrage des URL avancé. Répétez l'opération pour tous les pare-feu activés pour la catégorisation en ligne dans le cloud.

STEP 9 | Testez le déploiement de votre filtrage des URL.

Exceptions de catégories d'URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Vous pouvez exclure des sites Web spécifiques de l'application des catégories d'URL, ce qui garantit que ces sites Web sont bloqués ou autorisés, peu importe les catégories d'URL auxquelles ils sont associés. Par exemple, vous pouvez bloquer la catégorie d'URL de réseau social mais autoriser l'accès à LinkedIn. Pour créer des exceptions à la mise en œuvre de la politique de catégorie d'URL :

- Ajoutez les adresses IP ou URL des sites que vous souhaitez bloquer ou autoriser à une catégorie d'URL personnalisée ou à un type de **Liste d'URL**. Définissez ensuite l'accès au site pour la catégorie dans un profil de filtrage d'URL. Enfin, attachez le profil à une règle de stratégie de sécurité.

  Vous pouvez également utiliser une catégorie d'URL personnalisée comme critère de correspondance dans une règle de politique de sécurité. Assurez-vous de placer la règle d'exception au-dessus de toutes les règles qui bloquent ou autorisent les catégories auxquelles appartiennent les exceptions d'URL.

- Ajoutez les URL des sites que vous souhaitez bloquer ou autoriser à une liste dynamique externe de type **Liste d'URL**. Ensuite, Utilisez une liste dynamique externe dans un profil de filtrage d'URL ou comme critères de correspondance dans une règle de politique de sécurité. L'avantage d'utiliser une liste dynamique externe est que vous pouvez mettre à jour la liste sans effectuer de modification de configuration ou de validation sur le pare-feu.

*Les listes dynamiques externes de type **Liste d'URL** ne doivent pas être confondues avec les listes dynamiques externes de type Liste de domaines ou Liste d'adresse IP. Alors que les listes dynamiques externes d'URL autorisent les domaines et les adresses IP, l'inverse n'est pas vrai et entraîne des entrées non valides.*

- Lignes directrices pour les exceptions de catégories d'URL
- Création d'une catégorie d'URL personnalisée
- Utilisation d'une liste dynamique externe dans un profil de URL Filtering

Lignes directrices pour les exceptions de catégories d’URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Les instructions suivantes décrivent comment remplir les listes d’exceptions de catégories d’URL (catégories d’URL personnalisées ou listes dynamiques externes d’URL. Nous fournissons des exemples d’utilisation de caractères génériques et d’entrées spécifiques.

Directives de base pour les listes d'exceptions de catégories d’URL

Tenez compte des correspondances potentielles qu'une entrée peut avoir avant de l'ajouter à une liste d'exceptions de catégorie d'URL. Les directives suivantes spécifient comment créer une entrée qui bloque ou autorise les sites Web et les pages que vous souhaitez.

Par défaut, le pare-feu ajoute automatiquement une barre oblique (/) à la fin des entrées de domaine qui ne se terminent pas par une barre oblique (/) ou un astérisque (*). L'ajout de la barre oblique finale modifie les URL que le pare-feu considère comme une correspondance et pour lesquelles il applique la politique. Dans les entrées de domaine non génériques, les limites de la barre oblique finale correspondent au domaine donné et à ses sous-répertoires. Par exemple, ***example.com*** *(****example.com/*** *après traitement) correspond à lui-même et* ***example.com/search****.*

Dans les entrées de domaine génériques (entrées avec astérisques ou carets), les limites de la barre oblique finale correspondent aux URL conformes au modèle spécifié. Par exemple, pour correspondre à l'entrée ****.example.com****, une URL doit inclure au moins un sous-domaine et se terminer par le domaine racine,* ***example.com****. Le schéma est :****<subdomain>.exemple.com****;* ***news.example.com*** *est une correspondance, mais* ***example.com*** *ne l'est pas car il lui manque un sous-domaine.*

Nous vous recommandons d'ajouter manuellement des barres obliques finales pour clarifier le comportement de correspondance prévu d'une entrée pour toute personne qui l'inspecte. La barre oblique finale est invisible lorsqu'elle est ajoutée par le pare-feu.

Les serveurs de gestion Panorama™ exécutant PAN-OS® 10.2 ne peuvent activer cette fonctionnalité que pour les pare-feu sur la même version du logiciel. Pour activer cette fonctionnalité pour les pare-feu exécutant PAN-OS 10.1 ou une version antérieure, utilisez les commandes CLI suivantes sur chaque pare-feu :

```
admin@PA-850> debug device-server append-end-token on
```

```
admin@PA-850> configure
```

```
admin@PA- 850 # commit
```

*Pour désactiver cette fonctionnalité, sélectionnez****Device (périphérique)*** *>* ***Setup (configuration)*** *>* ***Content-ID (ID de contenu)*** *>* ***URL Filtering (filtrage d'URL)****. Ensuite, désélectionnez* ***Append Ending Token (Ajouter le jeton de fin)****. Vous pouvez toutefois bloquer ou autoriser l'accès à plus d'URL que prévu si vous désactivez cette fonctionnalité. Le pare-feu ajoute un astérisque implicite à la fin des entrées de domaine qui ne se terminent pas par un / ou *. Par exemple, si vous ajoutez* ***example.com*** *à une liste d'URL de sites Web autorisés, le pare-feu interprète cette entrée comme* ***example.com.****. Par conséquent, le pare-feu autorise l'accès à des sites tels que* ***example.com.domain.xyz****. Les exceptions de catégorie d'URL (PAN-OS 10.1 et versions antérieures) décrivent le comportement du pare-feu lorsque vous désactivez cette fonctionnalité.*

- Les entrées de liste ne sont pas sensibles à la casse.
- Omettez `http` et `https` des entrées d'URL.
- Chaque entrée d'URL peut contenir un maximum de 255 caractères.
- Entrez une *correspondance exacte* avec l'adresse IP ou l'URL que vous souhaitez bloquer ou autoriser ou utilisez des caractères génériques pour créer une *correspondance de modèle*.

  *Différentes entrées entraînent différentes correspondances exactes. Si vous entrez l'URL d'une page Web spécifique (**`example.com/contact`**), les limites du pare-feu correspondent à cette page uniquement. La correspondance exacte pour les domaines limite les correspondances au domaine lui-même et à ses sous-répertoires.*
- Envisagez d'ajouter les URL les plus couramment utilisées pour accéder à un site Web ou à une page à votre liste d'exceptions (par exemple, **`blog.paloaltonetworks.com`** et **`paloaltonetworks.com/blog`**) si l'entrée d'origine est accessible depuis plusieurs URL.
- L'entrée **`example.com`** est distincte de **`www.example.com`**. Le nom de domaine est le même, mais la deuxième entrée contient le sous-domaine *www* .

Palo Alto Networks ne prend pas en charge l'utilisation d'expressions régulières dans la catégorie d'URL personnalisée ou les entrées de liste dynamique externe. Vous devez connaître les URL spécifiques ou créer les modèles d'URL que vous souhaitez faire correspondre à l'aide de caractères génériques et des caractères suivants : `. / ? & = ;` +.

Directives sur les caractères génériques pour les listes d'exceptions de catégories d'URL

Vous pouvez utiliser des astérisques (*) et des carets (^) dans les listes d'exceptions de catégorie d'URL pour configurer une seule entrée afin qu'elle corresponde à plusieurs sous-domaines, domaines, domaines de premier niveau (TLD) ou pages sans spécifier d'URL exactes.

Utilisation des astérisques (*) et des carets (^)

Les caractères suivants sont des séparateurs de jetons : `. / ? & = ;` +. Chaque chaîne séparée par un ou deux de ces caractères est un jeton. Utilisez les caractères génériques en tant que marque substitutive d'un jeton, laquelle indique qu'un jeton spécifique peut contenir une valeur. Dans l'entrée **`docs.paloaltonetworks.com`**, les jetons sont « docs », « paloaltonetworks » et « com ».

Le tableau suivant décrit le fonctionnement des astérisques et des carets et fournit des exemples.

*	^
Indique un ou plusieurs sous-domaines, domaines, TLD ou sous-répertoires variables. Peut utiliser un astérisque après une barre oblique finale, par exemple, **`example.com/*`**.	Indique un sous-domaine variable, un domaine racine ou un TLD. Impossible d'utiliser le caret après une barre oblique finale. L'entrée suivante n'est pas valide : **`example.com/^`**.

*	^
Ex : ***.domain.com** correspond **à docs.domain.com** et **abc.xyz.domain.com**.	Ex : **^.domain.com** correspond **à docs.domain.com** et **blog.domain.com**.

Point clé: Les astérisques correspondent à une plus grande plage d'URL que les carets. Un astérisque correspond à n'importe quel nombre de jetons consécutifs, tandis qu'un caret correspond à exactement un jeton.

Une entrée comme **xyz.*.com** correspond à un plus grand nombre de sites que **xyz.^.^.com**; **xyz.*.com** correspond aux sites avec n'importe quel nombre de jetons entre les chaînes, et **xyz.^.^.com** correspond aux sites avec exactement deux jetons.

- Un joker doit être le **seul** caractère dans un jeton. Par exemple, **example*.com** est une entrée non valide car **example** et * sont dans le même jeton. Une entrée peut cependant contenir des caractères génériques dans plusieurs jetons.
- Vous pouvez utiliser des astérisques et des carets dans la même entrée (par exemple, ***.example.^**).

Ne créez pas d'entrée comportant des astérisques (*) consécutifs ou plus de neuf carets (^) consécutifs. De telles entrées peuvent compromettre la performance du pare-feu.

*Par exemple, n'ajoutez pas d'entrée telle que **mail.*.*.com**. Au lieu de cela, selon la gamme de sites Web dont vous souhaitez contrôler l'accès, entrez **mail.*.com** ou **mail.^.^.com**.*

Liste d'exceptions de catégorie d'URL—Exemples

Le tableau suivant affiche des exemples d'entrées de liste d'URL, des sites correspondants et des explications sur le comportement correspondant lorsque le pare-feu ajoute automatiquement des barres obliques à la fin.

Les entrées de ce tableau ne contiennent pas de barre oblique finale pour indiquer que le pare-feu en ajoute une aux entrées applicables en arrière-plan. De plus, les listes d'exceptions peuvent contenir des entrées ajoutées avant la barre oblique finale. Exceptions de catégorie d'URL—Exemples (PAN-OS 10.1) montre un comportement correspondant lorsque le pare-feu n'ajoute pas de barres obliques finales par défaut.

Nous vous recommandons d'ajouter manuellement des barres obliques finales pour clarifier le comportement de correspondance prévu d'une entrée pour toute personne qui l'inspecte. La barre oblique finale est invisible si elle est ajoutée par le pare-feu.

Entrée de la liste d'exceptions d'URL	Sites correspondants	Explication
Ensemble d'exemples 1		

Entrée de la liste d'exceptions d'URL	Sites correspondants	Explication
paloaltonetworks.com	paloaltonetworks.com paloaltonetworks.com/network-security/security-subscriptions	Le pare-feu ajoute une barre oblique finale à l'entrée, limitant les correspondances au domaine exact et à ses sous-répertoires.
paloaltonetworks.com/exemple	paloaltonetworks.com/exemple	Le pare-feu n'ajoute pas de barre oblique à cette entrée car l' **exemple** de sous-répertoire suit le domaine. Lorsque vous entrez l'URL d'une page Web spécifique, le pare-feu applique l'action d'exception à la page Web spécifiée.
Ensemble d'exemples 2—Astérisques		
*.exemple.com	www.exemple.com docs.example.com support.tools.example.com	L'astérisque développe les correspondances avec tous les sous-domaines **example.com** . Le pare-feu ajoute une barre oblique finale à l'entrée, excluant les correspondances à droite de **example.com**, le domaine racine.
mail.exemple.* *Cette entrée donne les mêmes correspondances avec ou sans la fonctionnalité de barre oblique finale activée.*	mail.exemple.com mail.example.co.uk mail.example.com/#inbox	L'astérisque développe les correspondances avec n'importe quelle URL après le schéma **mail.example.<*TLD*>**.
exemple.*.com	exemple.votresite.com exemple.es.domaine.com exemple.abc.xyz.com	L'astérisque développe les correspondances vers les URL où le sous-domaine le plus à gauche est **example** et le domaine de premier niveau est **com**. La barre

Entrée de la liste d'exceptions d'URL	Sites correspondants	Explication
		oblique finale exclut les correspondances à droite du TLD.
exemple.com/*	exemple.com/photos exemple.com/blog/dernier n'importe quel sous-répertoire example.com	Le domaine est suivi d'un / et d'un astérisque, ce qui indique qu'un sous-répertoire doit être présent. L'astérisque sert d'espace réservé de jeton pour tout sous-répertoire **`example.com`** . Le pare-feu n'ajoute pas de barre oblique finale car l'entrée se termine par un astérisque.
Ensemble d'exemples 3—Carets		
google.^	google.com google.info	Le caret étend les correspondances aux URL commençant par **`google`** et

Entrée de la liste d'exceptions d'URL	Sites correspondants	Explication
Des modèles tels que example.co.^ sont généralement utilisés pour faire correspondre des domaines spécifiques à un pays tels que ***example.co.jp****. Cependant, les domaines génériques de premier niveau (gTLD) donnent lieu à des modèles tels que example.co.^ correspondant à example.co.info ou example.co.amzn, qui peuvent ne pas appartenir à la même organisation.*	google.com/search?q=paloaltonetworks	se terminant par un seul TLD. La barre oblique finale exclut les correspondances à droite du dernier jeton.
^.google.com	www.google.com news.google.com	Le caret étend les correspondances aux sous-domaines à un seul niveau de **`google.com`**. Le pare-feu ajoute une barre oblique finale à l'entrée, excluant les correspondances à droite du domaine racine.
^.^.google.com	www.maps.google.com support.tools.google.com	Les deux carets élargissent les correspondances aux URL qui incluent deux sous-domaines consécutifs avant **`google.com`**. Le pare-feu ajoute une barre oblique finale à l'entrée, excluant les

Entrée de la liste d'exceptions d'URL	Sites correspondants	Explication
		correspondances à droite du domaine racine.
google.^.com	google.example.com google.entreprise.com	Le signe d'insertion élargit les correspondances aux URL où **`google`** est le sous-domaine le plus à gauche, suivi d'un jeton et de **`.com`**. Le pare-feu ajoute une barre oblique finale à l'entrée, excluant les correspondances à droite du TLD.

Création d'une catégorie d'URL personnalisée

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering licence (ou une licence de filtrage des URL héritée) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Vous pouvez créer une catégorie d'URL personnalisée pour définir des exceptions à la mise en œuvre de la catégorie URL ou définir une nouvelle catégorie d'URL à partir de plusieurs catégories.

Définissez des exceptions à la mise en œuvre de la catégorie d'URL (liste d'URL)

Spécifiez une liste d'URL (regroupées sous une seule catégorie personnalisée) que vous souhaitez appliquer indépendamment de leurs catégories d'URL prédéfinies. Vous pouvez contrôler l'accès à cette catégorie dans un profil de filtrage des URL que vous appliquez aux règles de politique de sécurité ou utiliser la catégorie comme critères de correspondance dans les règles de politique de sécurité. Par exemple, vous pouvez bloquer la catégorie `réseau social`, mais autoriser l'accès à LinkedIn.

Définissez une catégorie d'URL personnalisée en fonction de plusieurs catégories PAN-DB (Correspondance des catégories)

Créez une nouvelle catégorie pour cibler la mise en œuvre pour les sites Web ou les pages qui correspondent à *toutes* les catégories définies dans le cadre de la catégorie personnalisée. Par exemple, PAN-DB peut classer un blog de développeur que vos ingénieurs utilisent pour la

recherche comme `des sites et des blogs`, personnels,`des informations sur`, les ordinateurs et Internet et `à haut risque`. Pour permettre aux ingénieurs d'accéder au blog et aux sites Web similaires *et* d'obtenir une visibilité sur ces sites Web, vous pouvez créer une catégorie d'URL personnalisée basée sur les trois catégories et définir l'accès au site pour que la catégorie alerte dans un profil de filtrage des URL.

PAN-DB évalue les URL par rapport aux catégories d'URL personnalisées avant les listes dynamiques externes et les catégories d'URL prédéfinies. Par conséquent, le pare-feu met en œuvre les règles de politique de sécurité pour une URL dans une liste d'URL personnalisée sur les règles de politique associées aux catégories d'URL individuelles dans lesquelles elle existe.

Si plusieurs règles de politique de sécurité incluent une catégorie d'URL personnalisée, alors le pare-feu met en œuvre la règle de politique de sécurité avec l'action de profil de filtrage des URL la plus stricte pour le trafic correspondant.

- Strata Cloud Manager
- PAN-OS et Panorama

Création d'une catégorie d'URL personnalisée (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS et Panorama** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès à l'URL** > **Contrôle d'accès**.

STEP 2 | Sous Catégories d'URL personnalisées, sélectionnez **Ajouter une catégorie**.

Saisissez un **nom** descriptif pour la catégorie.

STEP 3 | Définissez le **Type** de catégorie d'URL personnalisée sur **Liste d'URL** ou **Correspondance de catégorie**.

- **Liste d'URL** : utilisez ce type de liste pour ajouter des URL que vous souhaitez mettre en œuvre différemment de la catégorie d'URL à laquelle elles appartiennent ou pour définir une liste d'URL comme appartenant à une catégorie personnalisée. Consultez le Lignes directrices pour les exceptions de catégories d'URL au fur et à mesure que vous créez des entrées de liste d'URL.
- **Category Match (Correspondance à la catégorie)** : fournir une application ciblée pour les sites Web qui correspondent à un ensemble de catégories. Le site Web ou la page doivent faire correspondre *l'ensemble* des catégories définies dans le cadre de la catégorie personnalisée.

STEP 4 | Sous **Éléments**, **ajoutez** des URL ou des catégories existantes.

STEP 5 | **Enregistrez** la catégorie d'URL personnalisée.

STEP 6 | Définissez les paramètres d'accès au site et de soumission des informations d'identification de l'utilisateur pour la catégorie d'URL personnalisée.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion de l'accès à l'URL** > **Profils de gestion de l'accès à l'URL**.
2. Sélectionnez un profil existant à modifier ou cliquez sur **Ajouter un profil**.
3. Sous Contrôle d'accès, sélectionnez la catégorie d'URL personnalisée que vous avez créée précédemment. Elle se trouve sous `Catégories d'URL personnalisées` et au-dessus des `Catégories prédéfinies`.
4. Définissez **l'accès au site** pour la catégorie.
5. Définissez **les soumissions d'informations d'identification d'utilisateur** pour la catégorie.
6. **Enregistrez** le profil.

STEP 7 | Appliquez le profil Gestion des accès à l'URL à une règle de politique de sécurité.

Un profil Gestion des accès à l'URL n'est actif que lorsqu'il est inclus dans un groupe de profils auquel une règle de politique de sécurité fait référence.

Suivez les étapes pour activer un profil Gestion des accès à l'URL (et tout profil de sécurité). Assurez-vous de **Transmettre la configuration**.

*Vous pouvez également utiliser des catégories d'URL personnalisées comme critère de correspondance des règles de politique de sécurité. Dans ce scénario, vous ne définissez pas l'accès au site pour la catégorie d'URL dans un profil de filtrage des URL. Au lieu de cela, après avoir créé une catégorie d'URL personnalisée, sélectionnez la règle de politique de sécurité à laquelle vous souhaitez ajouter la catégorie d'URL personnalisée (**Gérer** > **Configuration** > **Services de sécurité** > **Politique de sécurité**). Sous **Applications, Services et URL** et Entités de catégorie d'URL, cliquez sur **Ajouter des catégories d'URL**. Sélectionnez la catégorie d'URL personnalisée que vous avez créée, puis **enregistrez** la règle de politique de sécurité.*

Création d'une catégorie d'URL personnalisée (PAN-OS & Panorama)

STEP 1 | Sélectionnez **Objets** > **Objets personnalisés** > **Catégorie d'URL**.

STEP 2 | **Add (Ajoutez)** ou modifier une catégorie d'URL personnalisée et donnez un **Name (Nom)** descriptif à la catégorie.

STEP 3 | Définissez le **Type** de catégorie sur **Category Match (Correspondance à la catégorie)** ou **URL List (Liste d'URL)** :

- **URL List (Liste d'URL)** : ajoutez les URL que vous souhaitez appliquer différemment de la catégorie d'URL à laquelle ils appartiennent. Utilisez ce type de liste pour définir des exceptions à l'application de la catégorie d'URL ou pour définir qu'une liste d'URL

appartient à une catégorie personnalisée. Consultez Les exceptions de catégorie d'URL pour obtenir des instructions sur la création d'entrées de liste d'URL.

*Par défaut, le pare-feu ajoute automatiquement une barre oblique de fin (/) aux entrées de domaine (**`example.com`**) qui ne se terminent pas par une barre oblique de fin ou un astérisque (*). La barre oblique de fin empêche le pare-feu d'assumer un astérisque implicite à droite du domaine. Dans les entrées de domaine non génériques, les limites de barre oblique de fin correspondent au domaine donné et à ses sous-répertoires. Par exemple, **`example.com`** (**`example.com/`** après traitement) correspond à lui-même et **`example.com/search`**.*

*Dans les entrées de domaine génériques (entrées utilisant des astérisques ou des carets), les limites de barre oblique de fin correspondent aux URL conformes au modèle spécifié. Par exemple, pour correspondre à l'entrée **`*.example.com`**, une URL doit strictement commencer par un ou plusieurs sous-domaines et se terminer par le domaine racine, **`example.com`**; news.example.com est une correspondance, mais **`example.com n'est`** pas parce qu'il manque un sous-domaine.*

Nous vous recommandons d'ajouter manuellement des barres obliques de fin pour clarifier le comportement de correspondance prévu d'une entrée pour toute personne qui inspecte votre liste d'URL. La barre oblique de fin est invisible si elle est ajoutée par le pare-feu. URL Category Exceptions traite plus en détail de la barre oblique de fin et du comportement correspondant.

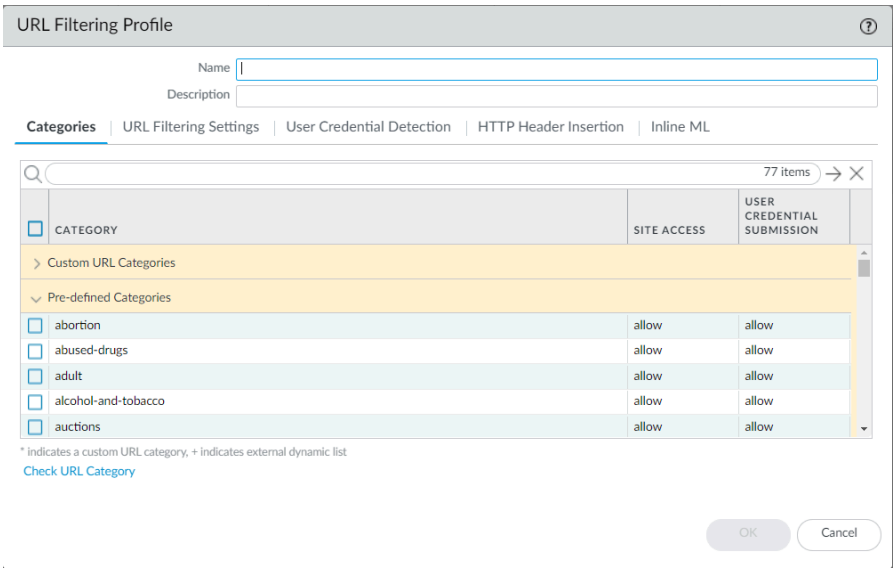
*Pour désactiver cette fonctionnalité, accédez à **Périphérique** > **Configuration** > **Content-ID** > **Filtrage des URL**. Ensuite, désélectionnez **Append Ending Token (Ajouter le jeton de fin)**. Si vous désactivez cette fonctionnalité, vous pouvez bloquer ou autoriser l'accès à plus d'URL que prévu. Url Category Exceptions (PAN-OS 10.1 et versions antérieures) décrit le comportement du pare-feu lorsque cette fonctionnalité est désactivée.*

- **Category Match (Correspondance à la catégorie)** : fournir une application ciblée pour les sites Web qui correspondent à un ensemble de catégories. Le site Web ou la page doivent faire correspondre *l'ensemble* des catégories définies dans le cadre de la catégorie personnalisée.

STEP 4 | Cliquez sur **OK** pour enregistrer la catégorie d'URL personnalisée.

STEP 5 | Sélectionnez **Objets** > **Profils de sécurité** > **Filtrage des URL** et **Ajoutez** ou modifiez un profil de filtrage des URL.

Votre nouvelle catégorie personnalisée s'affiche sous **Catégories d'URL personnalisées**:



STEP 6 | Décidez comment vous voulez appliquer le **Site Access (Accès au site)** et les **User Credential Submissions (Envois des informations d'identification de l'utilisateur** pour la catégorie d'URL personnalisée. (Pour contrôler les sites auxquels les utilisateurs peuvent soumettre leurs informations d'identification d'entreprise, voir Empêcher l'hameçonnage des informations d'identification.)

STEP 7 | Associez le profil de URL Filtering à une Règle de politique de sécurité pour appliquer le trafic qui correspond à cette règle.

Sélectionnez **Politiques** > **Sécurité** > **Actions** et spécifiez que la règle de politique de sécurité applique le trafic en fonction du profil de filtrage des URL que vous venez de mettre à jour. Assurez-vous de **Commit (Valider)** vos modifications.

*Vous pouvez également utiliser des catégories d'URL personnalisée en tant que critères de correspondance de la politique de sécurité. Dans ce cas, vous ne définissez pas l'accès au site pour la catégorie d'URL dans un profil de filtrage d'URL. Après avoir créé une catégorie personnalisée, allez directement à la règle de politique de sécurité à laquelle vous souhaitez ajouter la catégorie d'URL personnalisée (**Politiques** > **Sécurité**). Sélectionnez **Service/URL Category (Catégorie de service/d'URL)** pour utiliser la catégorie d'URL personnalisée en tant que critère de correspondance pour la règle.*

Utilisation d'une liste dynamique externe dans un profil de URL Filtering

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering licence (ou une licence de filtrage des URL héritée) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Une liste dynamique externe est un fichier texte qui est hébergé sur un serveur Web externe. Vous pouvez vous servir de cette liste pour importer des URL et appliquer une politique à ces URL. Le pare-feu importe la liste de manière dynamique à l'intervalle configuré et applique la politique aux URL (les adresses IP ou les domaines sont ignorés) qui figurent dans la liste. Lorsque la liste est mise à jour sur le serveur Web, le pare-feu récupère les modifications apportées et applique la politique à la liste modifiée sans qu'aucune validation n'ait lieu sur le pare-feu.

Pour protéger votre réseau des menaces et des fichiers malveillants nouvellement découverts, vous pouvez utiliser des external dynamic lists (listes dynamiques externes) dans les profils de URL Filtering. Pour obtenir des directives de mise en forme des URL, reportez-vous à la section Lignes directrices pour les exceptions de catégories d'URL.

- Strata Cloud Manager
- PAN-OS et Panorama

Utilisation d'une liste dynamique externe dans un profil de filtrage des URL (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS et Panorama** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Activez Prisma Access pour référencer une liste dynamique externe.

Une liste dynamique externe vous permet de définir une liste importée d'adresses IP, d'URL ou de noms de domaine que vous pouvez utiliser dans les règles de politique pour bloquer ou autoriser le trafic.

Pour configurer une liste dynamique externe, allez à **Gérer** > **Configuration** > **Objets** > **Listes dynamiques externes** :

- Assurez-vous que la liste ne comprenne aucune adresse IP ou aucun nom de domaine ; le pare-feu ignore toutes les entrées qui ne sont pas des URL.

- Utilisez les custom URL list guidelines (directives de liste d'URL personnalisées) pour vérifier la mise en forme de la liste.
- Spécifiez le **Type de liste** comme **Liste URL**.

STEP 2 | Utilisez la liste dynamique externe avec le filtrage des URL.

Allez à**Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès à l'URL**.

- Spécifiez **Accès au site** pour les URL de la liste dynamique externe.
- Excluez les URL de la liste dynamique externe de la catégorisation en ligne avancée.

Vous pouvez également utiliser des listes dynamiques externes pour créer des catégories d'URL personnalisées (retournez au tableau de bord de la gestion des accès à l'URL pour ce faire).

Si une URL qui figure dans une liste dynamique externe figure également dans une catégorie d'URL personnalisée, ou dans une liste de blocage et d'autorisation, l'action précisée dans la catégorie personnalisée est prioritaire par rapport à la liste dynamique externe.

STEP 3 | Vérifiez que l'action de politique est appliquée.

1. Affichez les entrées de la liste dynamique externe (**Gérer** > **Configuration** > **Objets** > **Listes dynamiques externes**) et essayez d'accéder à une URL de la liste.
2. Vérifiez que l'action que vous avez définie est appliquée dans le navigateur.

Utilisation d'une liste dynamique externe dans un profil de filtrage des URL (PAN-OS et Panorama)

STEP 1 | Configure the firewall to access an external dynamic list (Configuration du pare-feu pour qu'il accède à la liste dynamique externe).

- Assurez-vous que la liste ne comprenne aucune adresse IP ou aucun nom de domaine ; le pare-feu ignore toutes les entrées qui ne sont pas des URL.
- Utilisez les custom URL list guidelines (directives de liste d'URL personnalisées) pour vérifier la mise en forme de la liste.
- Sélectionnez **URL List (Liste des URL)** dans la liste déroulante Type.

STEP 2 | Utilisez la liste dynamique externe dans un profil de filtrage des URL.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**.
2. **Add (Ajoutez)** ou modifiez un profil de filtrage des URL existant.
3. Donnez un **Name (Nom)** au profil et, dans l'onglet **Categories (Catégories)**, sélectionnez la liste dynamique externe dans la liste Category (Catégorie).
4. Cliquez sur Action (Action) pour sélectionner une action plus granulaire pour les URL figurant dans la liste dynamique externe.

   Si une URL incluse dans une liste dynamique externe est également incluse dans une catégorie d'URL personnalisée, ou bloquer et autorise la liste, l'action spécifiée dans la catégorie personnalisée est prioritaire sur la liste dynamique externe.
5. Cliquez sur **OK**.
6. Associez le profil de filtrage des URL à une règle de politique de sécurité.
   1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
   2. Sélectionnez l'onglet **Actions (Actions)** puis, dans la section Profile Setting (Paramètre de profil), sélectionnez le nouveau profil dans la liste déroulante **URL Filtering (URL Filtering)**.
   3. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

STEP 3 | Vérifiez que l'action de politique est appliquée.

1. View the external dynamic list entries (Affichez les entrées de la liste dynamique externe) et essayez d'accéder à une URL de la liste.
2. Vérifiez que l'action que vous avez définie est appliquée dans le navigateur.
3. Pour surveiller l'activité sur le pare-feu :
   1. Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité sur le réseau et l'activité bloquée pour l'URL à laquelle vous avez accédé.
   2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **URL Filtering (Filtrage des URL)** pour accéder à la vue détaillée du journal.

STEP 4 | Vérifiez si les entrées de la liste dynamique externe ont été ignorées ou sautées.

Dans une liste d'URL, le pare-feu saute toutes les entrées qui ne sont pas des URL et les considère comme non valables ; il ignore également les entrées qui dépassent le nombre maximum d'entrées permises sur le modèle de pare-feu.

*Pour vérifier si vous avez atteint la limite pour un type de liste dynamique externe, sélectionnez **Objects (Objets)** > **External Dynamic Lists (Listes dynamiques externes)** et cliquez sur **List Capacities (Capacités de liste)**.*

Pour revoir les détails d'une liste, servez-vous de la commande CLI suivante sur un pare-feu :

```
request system external-list show type url name <list_name>
```

Par exemple :

```
request system external-list show type url name My_URL_List vsys5/
My_URL_List: Next update at: Tue Jan 3 14:00:00 2017 Source:
 http://example.com/My_URL_List.txt Referenced: Oui Valide :
 Authentification-Valide : Oui Total des entrées valides : 3
 Nombre total d’entrées non valides : 0 URL valides : www.URL1.com
 www.URL2.com www.URL3.com
```


Bonnes pratiques en matière de filtrage des URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

La solution URL Filtering de Palo Alto Networks vous protège contre les menaces Web et vous procure une façon simple de surveiller l'activité Web et de la contrôler. Pour tirer le meilleur parti de votre déploiement URL Filtering, vous devez commencer par créer des règles d'autorisation pour les applications desquelles vous dépendez pour exercer vos activités. Examinez ensuite les catégories d'URL qui classent le contenu malveillant et à risque. Nous vous recommandons ces types de catégories immédiatement. Ensuite, pour les autres types de contenus, ces bonnes pratiques peuvent vous servir de guide pour la réduction de votre exposition aux menaces Web, sans limiter l'accès de vos utilisateurs au contenu Web dont ils ont besoin.

- Avant de commencer, identifiez les applications que vous souhaitez autoriser et créez des règles d'autorisation des applications dans le cadre de l'élaboration d'une politique de sécurité des passerelles Internet.

  La liste des applications autorisées comprend non seulement les applications que vous obtenez et gérez à des fins d'infrastructure ou d'entreprise, mais également les autres applications que vos utilisateurs pourraient devoir utiliser pour accomplir leur travail ainsi que les applications que vous pourriez décider d'autoriser à des fins personnelles.

  Après que vous ayez identifié ces applications d'entreprise, vous pouvez utiliser le filtrage d'URL pour contrôler et sécuriser toute l'activité web qui n'est pas sur la liste d'autorisation.
- Obtenez une visibilité sur l'activité Web de vos utilisateurs afin de planifier la politique de filtrage des URL la plus efficace pour votre organisation. Cela inclut:
  - À tout moment, vous pouvez utiliser un Test A Site pour voir comment PAN-DB, la base de données de filtrage d'URL de Palo Alto Networks dans le cloud, catégorise une URL spécifique et pour découvrir toutes les catégories d'URL possibles.
  - Commencez par un profil de URL Filtering (pratiquement) passif qui envoie des alertes pour la plupart des catégories. Un tel profil vous donne une visibilité des sites auxquels vos utilisateurs accèdent. Vous pouvez donc décider ce que vous souhaitez autoriser, limiter et bloquer.
  - Surveillez l'activité web pour évaluer les sites que vous utilisateurs accèdent et voir s'ils sont alignés avec vos besoins métier.

- Bloquer les catégories d'URL qui correspondent à du contenu malveillant ou d'exploitation. Bien que nous sachions que ces catégories sont dangereuses, gardez toujours à l'esprit que les catégories d'URLs que vous décidez de bloquer peuvent dépendre de vos besoins métier.
- Vous pouvez également utiliser les catégories d'URL pour introduire graduellement le déchiffrement, et pour exclure les catégories d'URL qui peuvent contenir des renseignements sensibles ou personnels du déchiffrement (comme les sites relatifs à des services financiers et à la santé et aux médicaments).

  Prévoyez de déchiffrer le trafic le plus à risque dans un premier temps (catégories d'URL les plus susceptibles de contenir du trafic malveillant, comme les jeux ou à risque élevé), puis d'en déchiffrer davantage lorsque vous acquérez de l'expérience. Vous pouvez éventuellement déchiffrer les catégories d'URL qui n'affectent pas votre entreprise dans un premier temps (si quelque chose ne se passe pas comme prévu, cela n'affecte pas l'entreprise), par exemple, de nouveaux flux d'informations. Dans les deux cas, déchiffrez quelques catégories d'URL, tenez compte des commentaires des utilisateurs, exécutez les rapports pour vous assurer que le déchiffrement fonctionne comme prévu, puis déchiffrez progressivement quelques catégories d'URL supplémentaires, etc. Prévoyez d'exclure les sites du décryptage si vous ne pouvez pas les décrypter pour des raisons techniques ou parce que vous choisissez de ne pas les décrypter.

  Affiner le décryptage en fonction des catégories d'URL est aussi une bonne pratique du décryptage.
- Prevent credential theft (Évitez le vol des identifiants) en activant la détection des soumissions d'informations d'identification d'entreprise aux sites par le pare-feu, puis contrôlez ces soumissions en fonction de la catégorie d'URL. Empêchez les utilisateurs d'envoyer des informations d'identification à des sites malveillants et non validés, avertissez-les contre la saisie d'informations d'identification professionnelles sur des sites inconnus ou contre la réutilisation d'informations d'identification professionnelles sur des sites hors travail, et autorisez explicitement les utilisateurs à envoyer leurs informations d'identification sur les sites de l'entreprise et les sites validés.
- Bloquez les variantes malveillantes des exploits JavaScript et des attaques de hameçonnage en temps réel. Activer la catégorisation locale en ligne vous permet d'analyser dynamiquement les pages Web à l'aide de l'apprentissage automatique sur le pare-feu.
- Configurer la catégorisation en ligne pour activer l'apprentissage profond en ligne, les moteurs de détection basés sur le ML pour analyser le contenu des pages Web suspectes et protéger les utilisateurs contre les attaques Web de type zero-day. La catégorisation en ligne dans le cloud est capable de détecter et d'empêcher les attaques de phishing avancées et ciblées, ainsi que d'autres attaques basées sur le Web qui utilisent des techniques d'évasion avancées telles que le cloaking, les attaques en plusieurs étapes, les défis CAPTCHA et les URL à usage unique inédites.
- Décrypter, inspecter et limiter de manière stricte la façon dont les utilisateurs interagissent avec le contenu à haut risque et à risque moyen (si vous avez décidé de ne pas bloquer l'une des catégories d'URL malveillantes pur des raisons commerciales, vous devez limiter de manière stricte la façon dont les utilisateurs interagissent avec ces catégories.

  Le contenu web que vous approuvez et les catégories d'URLs malicieuses que vous bloquer sont juste une portion de l'ensemble du trafic web Le reste du contenu auquel accèdent vos utilisateurs est une combinaison de contenu bénin (risque faible) et contenu risqué (haut et moyen risque). Bien que le caractère malveillant des sites à risque élevé et modéré n'ait pas été confirmé, ils sont étroitement liés aux sites malveillants. Par exemple, une URL à haut

risque peut se trouver sur le même domaine qu'un site malveillant ou avoir hébergé du contenu malveillant par le passé.

Cependant, beaucoup des sites qui représentent un risque pour votre entreprise peuvent aussi fournir des services et ressources intéressantes à vos utilisateurs (les services de stockage Cloud sont un bon exemple) Bien que ces ressources et services soient nécessaires pour le métier, ils peuvent aussi vraisemblablement être utilisé lors d'une cyberattaque. Voici comment contrôler comment les utilisateurs interagissent avec ce contenu potentiellement dangereux, tout en fournissant une bonne expérience utilisateur :

- Dans un profil de filtrage des URLs, configurez les catégories haut risque et moyen risque à **continue** pour afficher une page de réponse qui avertit les utilisateurs lorsqu'ils visitent un site potentiellement dangereux. Conseillez-les sur comment prendre leurs précautions s'ils décident de poursuivre sur le site. Si vous ne souhaitez pas afficher une page de réponse pour vos utilisateurs, alertez sur le contenu à haut et moyen risque à la place.
- Décryptez les sites à risque élevé et à risque modéré.
- Suivez les bonnes pratiques antispyware, en matière de protection contre les vulnérabilités et de blocage des fichiers. Une mesure de protection consisterait à bloquer les téléchargements de types de fichiers dangereux et à bloquer le JavaScript obscurs pour les sites pour lesquels vous optez pour les alertes.
- Mettez un terme au vol d'identifiants en empêchant les utilisateurs de soumettre leurs identifiants d'entreprise à des sites y compris ceux qui sont considérés à risque élevé et à risque modéré.

- Les écoles ou les établissements d'enseignement devraient utiliser l'application de la recherche sécurisée pour s'assurer que les moteurs de recherche filtrent les images et les vidéos pour adultes des résultats de recherche.
- Conservez les requêtes Web initiales lors de la recherche de catégorie d'URL.

  Lorsqu'un utilisateur visite un site Web, Advanced URL Filtering vérifie les catégories d'URL mises en cache pour catégoriser le site. Si le pare-feu ne trouve pas la catégorie d'URL dans le cache, il effectue une recherche avec PAN-DB, la base de données d'URL de Palo Alto Networks. Par défaut, la requête Web de l'utilisateur est autorisée lors de cette recherche dans le cloud.

  Mais si vous choisissez de conserver les requêtes Web, vous pouvez à la place bloquer la requête jusqu'à ce que Advanced URL Filtering trouve la catégorie d'URL ou expire. Si l'interrogation expire, le pare-feu choisit la catégorie URL non-résolu Retrouvez cette fonctionnalité dans vos paramètres de filtrage des URL, **Garder en mémoire la demande du client pour la recherche de catégorie**.

Tester la configuration du filtrage d'URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering licence (ou une licence de filtrage des URL héritée) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Pour tester vos configurations de la politique de filtrage des URL, utilisez les pages de test de filtrage des URL de Palo Alto Networks. Ces pages ont été créées pour tester en toute sécurité toutes les catégories d'URL prédéfinies et Advanced URL Filtering catégories de détection en temps réel.

Les pages de test sont accessibles via des connexions HTTP et HTTPS. Cependant, vous devez activer le décryptage SSL pour afficher les pages de test sur HTTPS.

Vous pouvez vérifier la classification d'un site Web spécifique à l'aide de l'outil de recherche de catégorie d'URL de Palo Alto Networks, Test A Site.

Suivez la procédure correspondant à votre abonnement au filtrage des URL :

Vérifier le filtrage d'URL

Si vous disposez d'un abonnement de filtrage des URL hérité, testez et vérifiez que le pare-feu catégorise, applique et enregistre correctement les URL dans les catégories auxquelles accèdent les utilisateurs finaux.

STEP 1 | Accédez à un site Web dans la catégorie d'URL qui vous intéresse.

Envisagez de tester les sites dans les catégories d'URL bloquées. Vous pouvez utiliser une page de test (urlfiltering.paloaltonetworks.com/test-<*url-category*>) pour éviter d'accéder directement à un site. Par exemple, pour tester votre politique de blocage des logiciels malveillants, visitez https://urlfiltering.paloaltonetworks.com/test-malware.

STEP 2 | Consultez les journaux de trafic et de filtrage des URL pour vérifier que votre pare-feu traite le site correctement.

Par exemple, si vous avez configuré une page de blocage à afficher lorsqu'une personne accède à un site qui enfreint la politique de votre organisation, vérifiez qu'elle s'affiche lorsque vous visitez le site de test.

Vérifiez Advanced URL Filtering

Si vous avez un abonnement Advanced URL Filtering, testez et vérifiez que les URL soumises au Advanced URL Filtering sont correctement analysées.

*Palo Alto Networks recommande de définir le paramètre d'action de détection en temps réel (catégorisation en ligne du cloud) sur **alerter** pour les profils de filtrage des URL actifs. Cela offre une visibilité sur les URL analysées en temps réel et bloque (ou autorise, en fonction de vos paramètres de stratégie) en fonction des paramètres de catégorie configurés pour des menaces Web spécifiques.*

Le pare-feu applique l'action la plus sévère des actions configurées pour les catégories d'URL détectées d'une URL donnée. Par exemple, supposons que example.com soit classé en tant que détection en temps réel, commande et contrôle et achats, des catégories avec une action d'alerte, de blocage et d'autorisation configurées, respectivement. Le pare-feu bloque l'URL, car le blocage est l'action la plus sévère parmi les catégories détectées.

STEP 1 | Consultez chacune des URL de test suivantes pour vérifier que le service Advanced URL Filtering catégorise correctement les URL :

- **Logiciel malveillant** — http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-malware
- **Hameçonnage** — http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-phishing
- **C2**—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-command-and-control
- **Logiciel indésirable**—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-grayware

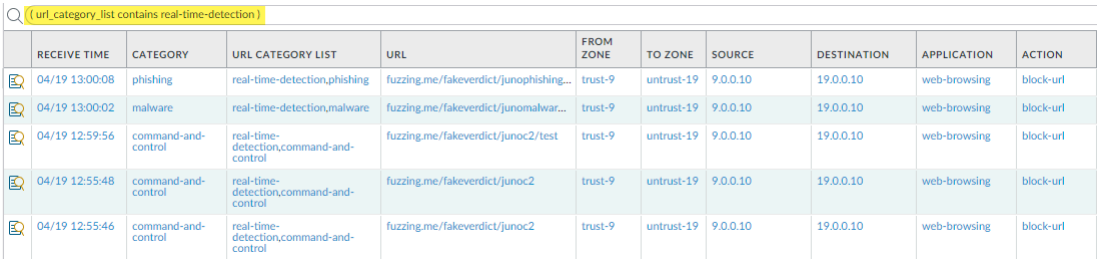
Si la catégorisation en ligne dans le cloud est activée, utilisez les URL suivantes pour tester le bon fonctionnement de la fonctionnalité :

- **Logiciel malveillant**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-malware
- **Hameçonnage**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
- **Logiciel indésirable**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-grayware
- **Parqué**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-parked
- **Adulte**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-adult

STEP 2 | Surveiller l'activité Web pour vérifier que les URL de test ont été correctement classées par Advanced URL Filtering :

1. Filtrez vos journaux de filtrage des URL en utilisant les éléments suivants : `(url_category_list contains real-time-detection)`.

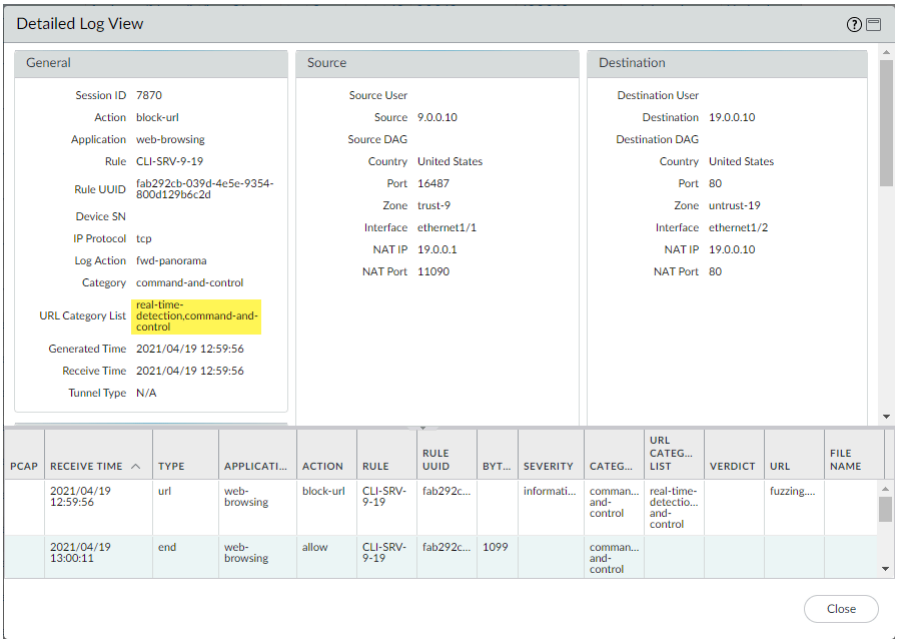
   Des correspondances de catégories de pages Web supplémentaires sont également affichées et correspondent aux catégories définies par PAN-DB.



RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION
04/19 13:00:08	phishing	real-time-detection,phishing	fuzzing.me/fakeverdict/junophishing...	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
04/19 13:00:02	malware	real-time-detection,malware	fuzzing.me/fakeverdict/junomalwar...	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
04/19 12:59:56	command-and-control	real-time-detection,command-and-control	fuzzing.me/fakeverdict/junoc2/test	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
04/19 12:55:48	command-and-control	real-time-detection,command-and-control	fuzzing.me/fakeverdict/junoc2	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
04/19 12:55:46	command-and-control	real-time-detection,command-and-control	fuzzing.me/fakeverdict/junoc2	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url

2. Examinez en détail les journaux pour vérifier que chaque type de menace Web est correctement analysé et catégorisé.

   Dans l'exemple suivant, l'URL est classée comme ayant été analysée en temps réel et comme possédant des qualités qui la définissent comme commande et contrôle (C2). Étant donné que la catégorie C2 est associée à une action plus sévère que la détection en temps réel (blocage par opposition à alerte), l'URL est catégorisée comme commande et contrôle et bloquée.



Fonctionnalités de filtrage des URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering licence (ou une licence de filtrage des URL héritée) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Après avoir configuré les composants de base de votre déploiement de filtrage des URL, envisagez de configurer les fonctionnalités suivantes :

- Catégorisation en ligne
- Inspection de l'établissement de liaison SSL/TLS
- Contrôle prioritaire sur l'URL par l'administrateur
- Prévention contre le hameçonnage des informations d'identification
- Pages de réponse de URL Filtering
- Mise en œuvre de la recherche sécurisée
- (Accès Prisma uniquement) Intégration avec l'isolation du navigateur distant (RBI)

Inspecter les échanges SSL/TLS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

L'examen de l'établissement des liaisons SSL/TLS améliore la sécurité du réseau et optimise les abonnements hérités et de filtrage des URL avancé. Lorsque vous activez l'inspection de l'établissement de liaison SSL/TLS, le filtrage des URL avancé utilise les données de la liaison pour identifier le trafic et appliquer les règles de politique de sécurité applicables le plus tôt possible.

Voici comment cela fonctionne

Tout d'abord, le message Client Hello est analysé pour rechercher le champ *Indication du nom de serveur (SNI)*, une extension du protocole TLS qui contient le nom d'hôte d'un site Web demandé. Ensuite, la catégorie d'URL et la destination du serveur du trafic sont déterminées à partir du nom d'hôte. Ensuite, le trafic est mis en œuvre en fonction de sa catégorie d'URL. Si une menace est détectée, comme un serveur Web malveillant dans le champ SNI, ou si une règle de politique de sécurité bloque le site Web, l'établissement de la liaison se termine et la session Web se termine immédiatement. Si aucune menace n'est détectée et que le trafic est autorisé conformément à la politique, la liaison SSL/TLS est terminée et les données d'application sont échangées via la connexion sécurisée.

Les pages de réponse de filtrage des URL ne s'affichent pas pour les sites bloqués lors des inspections d'établissement de liaison SSL/TLS, car le pare-feu réinitialise la connexion HTTPS. La réinitialisation de la connexion met fin à l'établissement de liaison SSL/TLS et empêche la notification de l'utilisateur par la page de réponse. Au lieu de cela, le navigateur affiche un message d'erreur de connexion standard.

Les détails des liaisons et des sessions SSL/TLS réussies figureront dans les journaux de trafic et de décryptage. Les détails des sessions ayant échoué se trouveront dans les journaux de filtrage des URL ; les journaux de décryptage ne sont pas générés pour les sessions Web bloquées pendant les liaisons SSL/TLS.

- Strata Cloud Manager
- PAN-OS et Panorama

Inspecter les liaisons SSL/TLS (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS et Panorama** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

Une exigence de l'inspection des liaisons SSL est que vous décryptiez le trafic SSL/TLS via SSL Forward Proxy ou SSL Inbound Inspection.

STEP 1 | Confirmez que votre licence Prisma Access inclut un abonnement Filtrage des URL avancé.

1. Sélectionnez **Gérer** > **Configuration du service** > **Vue d'ensemble** et cliquez sur l'hyperlien de la Quantité. Les informations, y compris les services de sécurité, apparaissent.
2. Sous Services de sécurité, confirmez qu'une coche se trouve à côté de Filtrage des URL.

STEP 2 | Vérifiez que vous déchiffrez le trafic SSL/TLS via SSL Forward Proxy (proxy de transfert SSL) ou SSL Inbound Inspection (inspection SSL entrante).

STEP 3 | Activez l'inspection des poignées de main SSL/TLS par CTD. Par défaut, cette option est désactivée.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Décryptage**.
2. Dans Paramètres de décryptage, sélectionnez l'icône paramètres. Sélectionnez ensuite **Inspecter les messages des liaisons TLS**.

   Vous pouvez aussi utiliser la commande CLI **`set deviceconfig setting ssl-decrypt scan-handshake <yes|no>`**.
3. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications. Sous Paramètres de décryptage, le paramètre de message d'inspection des liaisons TLS doit indiquer Activé.

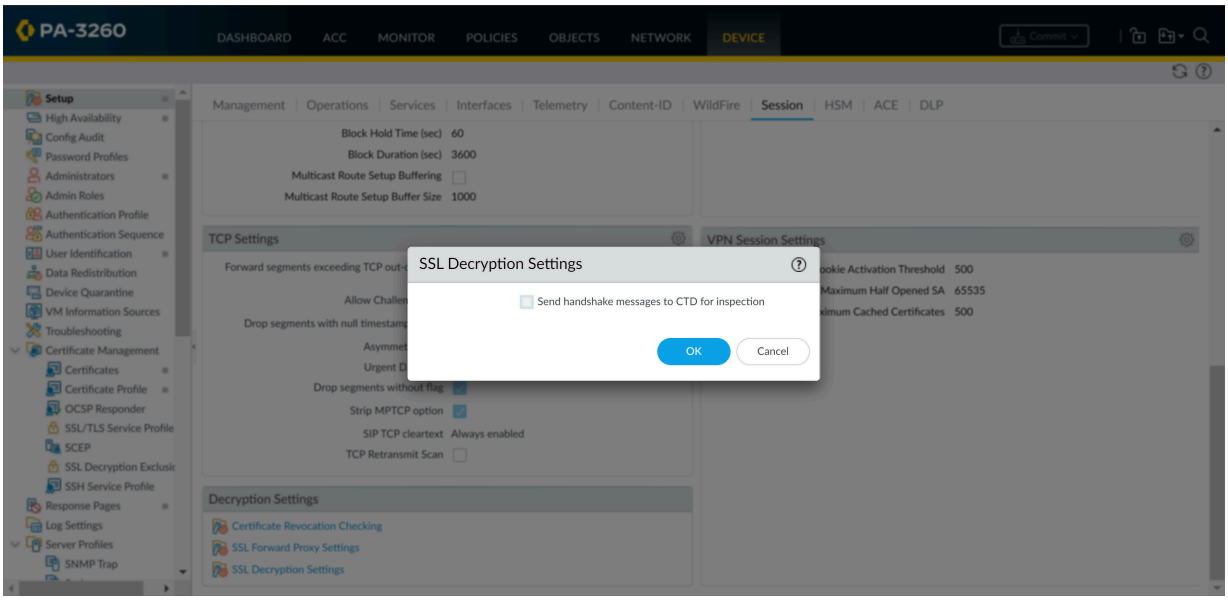
STEP 4 | **Transmettre la configuration** pour enregistrer et valider vos modifications.

Inspecter les liaisons SSL/TLS (PAN-OS et Panorama)

STEP 1 | Sélectionnez **Appareil > Licences** pour confirmer que vous disposez d'une licence active de filtrage d'URL avancé ou de filtrage d'URL héritée.

STEP 2 | Vérifiez que vous déchiffrez le trafic SSL/TLS via SSL Forward Proxy (proxy de transfert SSL) ou SSL Inbound Inspection (inspection SSL entrante).

STEP 3 | Activez l'inspection des poignées de main SSL/TLS par CTD. Par défaut, l'option est désactivée.



1. SélectionnezDevice (périphérique) > Setup (Configuration) > Session > Decryption Settings (Paramètres de décryptage) > SSL Decryption Settings (paramètres de décryptage SSL).
2. Sélectionnez **Send handshake messages to CTD for inspection (Envoyer les messages d'établissement de connexion à CTD pour inspection)**.

   Vous pouvez aussi utiliser la commande CLI **`set deviceconfig setting ssl-decrypt scan-handshake <yes|no>`**.
3. Cliquez sur **OK**.

STEP 4 | **Commit (validez)** vos modifications de configuration.

Autoriser l'accès par mot de passe à certains sites

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering licence (ou une licence de filtrage des URL héritée) ***Remarques :*** • *Les licences de filtrage des URL héritées sont abandonnées, mais les licences héritées actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Dans certains cas, il peut être nécessaire d'exiger un mot de passe pour accéder aux sites Web de certaines catégories. Par exemple, votre entreprise peut bloquer des catégories d'URL qui menacent la sécurité et le bien-être des employés. Cependant, certains employés peuvent devoir accéder à ces catégories à des fins de recherche ou à d'autres fins légitimes. Pour équilibrer la sécurité et les besoins de l'entreprise, la mise en œuvre de remplacements d'administrateur des URL peut être une solution efficace.

Pour créer un remplacement d'administrateur des URL, définissez l'action pour une catégorie à **remplacer**. Ensuite, créez un mot de passe que les utilisateurs doivent saisir pour accéder aux sites de cette catégorie. Lorsque les utilisateurs tentent d'accéder à un site Web dans une catégorie que vous avez remplacée, une Page de réponse Continuer et remplacer apparaît. Cette page informe les utilisateurs qu'un site Web est bloqué et les invite à saisir un mot de passe pour continuer sur le site.

- Strata Cloud Manager
- PAN-OS et Panorama

Autoriser l'accès par mot de passe à certains sites (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS et Panorama** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Accédez au tableau de bord Gestion des accès URL.

Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès d'URL**.

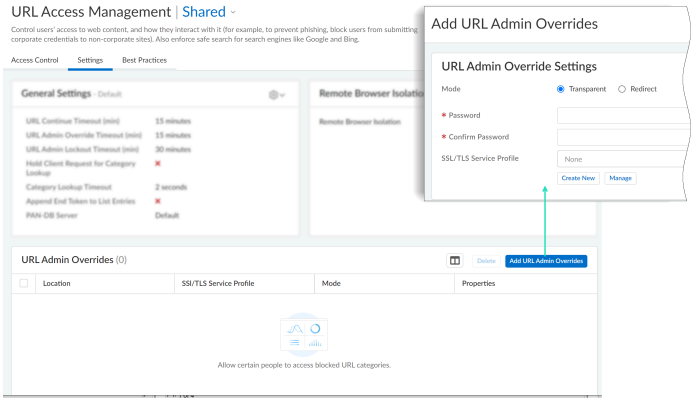
STEP 2 | Sélectionnez **Settings (Paramètres)**.

STEP 3 | Créez un mot de passe de Contrôle prioritaire sur l'URL par l'administrateur.

1. Accédez à Contrôle prioritaire sur l'URL par l'administrateur, puis **Ajouter un Contrôle prioritaire sur l'URL par l'administrateur**.

2. (Facultatif) Sélectionnez un **Mode** pour demander aux utilisateurs le mot de passe :
   - **Transparent** : l'invite de mot de passe semble provenir de l'URL de destination d'origine. Le pare-feu intercepte le trafic du navigateur destiné aux sites d'une catégorie d'URL définie pour être remplacée et émet un HTTP 302 pour demander le mot de passe, qui s'applique au niveau par vsys.
   - **Rediriger** : l'invite de mot de passe s'affiche à partir d'une **Adresse** (adresse IP ou nom d'hôte DNS) que vous spécifiez. Le pare-feu intercepte le trafic HTTP ou HTTPS vers une catégorie d'URL définie pour être remplacée et utilise une redirection HTTP 302 pour envoyer la demande à une interface de couche 3 sur le pare-feu.
3. Entrez un **Mot de passe**, puis entrez-le à nouveau dans **Confirmer le mot de passe**.
4. (Facultatif) Sélectionnez un **profil de service SSL/TLS**.

   Vous pouvez créer et gérer des profils de service SSL/TLS en cliquant respectivement sur **Créer nouveau** et **Gérer**.
5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.



STEP 4 | (Facultatif) Définissez la durée de l'accès de remplacement et des verrouillages par mot de passe.

Par défaut, les utilisateurs peuvent accéder aux sites Web dans les catégories pour lesquelles ils ont réussi à saisir un mot de passe de remplacement pendant 15 minutes. Une fois l'intervalle par défaut ou personnalisé dépassé, les utilisateurs doivent saisir à nouveau le mot de passe.

Par défaut, les utilisateurs sont bloqués pendant 30 minutes après trois tentatives de mot de passe infructueuses. Une fois que l'utilisateur est verrouillé pour la durée par défaut ou personnalisée, il peut essayer d'accéder à nouveau aux sites Web.

1. Personnalisez les paramètres généraux.
2. Pour **Délai de contrôle prioritaire sur l'URL par l'administrateur**, saisissez une valeur (en minutes) entre 1 et 86 400.
3. Pour **Délai d'expiration du verrouillage de l'administrateur d'URL**, entrez une valeur (en minutes) comprise entre 1 et 86 400.
4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 5 | Spécifiez les catégories d'URL qui nécessitent un accès par mot de passe.

1. Dans le tableau de bord Gestion des accès URL, sous l'onglet **Contrôle d'accès**, allez dans Profils de gestion des accès URL et modifiez ou **ajoutez un profil**.
2. Sous Contrôle d'accès, sélectionnez les catégories qui nécessitent un accès par mot de passe.
3. Avec toutes les catégories sélectionnées, cliquez sur **Définir l'accès**, puis sélectionnez **Remplacer**.

   Vous devriez voir que l'accès au site pour les catégories en surbrillance indique maintenant `Remplacer`.
4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 6 | Appliquez le profil Gestion des accès URL à une règle de politique de sécurité.

Un profil Gestion des accès URL n'est actif que lorsqu'il est inclus dans un groupe de profils auquel une règle de politique de sécurité fait référence.

Suivez les étapes pour activer un profil Gestion de l'accès à l'URL (et tout profil de sécurité). Assurez-vous de **Transmettre la configuration** lorsque vous avez terminé.

Autoriser l'accès par mot de passe à certains sites (PAN-OS et Panorama)

STEP 1 | Définissez un mot de passe de remplacement d'administrateur d'URL.

1. Sélectionnez **Device (Périphérique)** > **Setup(Configuration)** > **Content ID**.
2. Dans la section **URL Admin Override (Forçage de l'URL par l'administrateur)**, cliquez sur **Add (Ajouter)**.
3. Dans le champ **Location (Emplacement)**, sélectionnez le système virtuel auquel le mot de passe s'applique.
4. Entrez un **Mot de passe**, puis entrez-le à nouveau dans **Confirmer le mot de passe**.
5. Sélectionnez un **SSL/TLS Service Profile (profil de service SSL/TLS)**.

   Les profils de service SSL/TLS spécifient le certificat que le pare-feu présente à l'utilisateur si le site contenant le remplacement est un site HTTPS.
6. Sélectionnez un **Mode** Pour demander à l'utilisateur le mot de passe :

   - **Transparent** : l'invite de mot de passe semble provenir de l'URL de destination d'origine. Le pare-feu intercepte le trafic du navigateur destiné aux sites d'une catégorie d'URL définie pour être remplacée et émet un HTTP 302 pour demander le mot de passe, qui s'applique au niveau par vsys.

     Le navigateur client affichera des erreurs de certificat s'il ne reconnaît pas le certificat.
   - **Rediriger** : l'invite de mot de passe s'affiche à partir d'une **Adresse** (adresse IP ou nom d'hôte DNS) que vous spécifiez. Le pare-feu intercepte le trafic HTTP ou HTTPS vers une catégorie d'URL définie pour être remplacée et utilise une redirection HTTP 302 pour envoyer la demande à une interface de couche 3 sur le pare-feu.
7. Cliquez sur **OK**.

STEP 2 | (Facultatif) Définissez la durée de l'accès de remplacement et du verrouillage par mot de passe.

Par défaut, les utilisateurs peuvent accéder aux sites Web dans les catégories pour lesquelles ils ont réussi à saisir un mot de passe de remplacement pendant 15 minutes. Une fois l'intervalle par défaut ou personnalisé dépassé, les utilisateurs doivent saisir à nouveau le mot de passe.

Par défaut, les utilisateurs sont bloqués pendant 30 minutes après trois tentatives de mot de passe infructueuses. Une fois que l'utilisateur est verrouillé pour la durée par défaut ou personnalisée, il peut essayer d'accéder à nouveau aux sites Web.

1. Modifiez la section URL Filtering (URL Filtering).
2. Pour **Délai d'expiration du remplacement de l'administrateur d'URL**, entrez une valeur (en minutes) comprise entre 1 et 86 400. ---Par défaut, les utilisateurs peuvent accéder aux sites de la catégorie pendant 15 minutes sans devoir à nouveau saisir le mot de passe.
3. Pour **Délai d'expiration du verrouillage de l'administrateur d'URL**, entrez une valeur (en minutes) comprise entre 1 et 86 400.
4. Cliquez sur **OK**.

STEP 3 | (Mode Rediriger uniquement) Créez une interface de Couche 3 vers laquelle rediriger les requêtes Web vers des sites d'une catégorie configurée pour le contrôle prioritaire.

1. Créez un profil de gestion pour permettre à l'interface d'afficher la page de réponse Continuer et Contrôle prioritaire du filtrage des URL :
   1. Sélectionnez **Network (Réseau)** > **Interface Mgmt (Gestion de l'interface)**, puis cliquez sur **Add (Ajouter)**.
   2. Donnez un **Name (Nom)** au profil, sélectionnez **Response Pages (Pages de réponse)**, puis cliquez sur **OK (OK)**.
2. Créez l'interface de couche 3. Veillez à associer le profil de gestion que vous venez de créer (dans l'onglet **Advanced (Avancé)** > **Other Info (Autres informations)** de la boîte de dialogue Ethernet Interface (Interface Ethernet)).

STEP 4 | (Mode Rediriger uniquement) Pour rediriger en toute transparence les utilisateurs sans afficher d'erreur de certificat, installez un certificat correspondant à l'adresse IP de l'interface vers laquelle vous redirigez les requêtes Web vers un site d'une catégorie d'URL configurée pour le contrôle prioritaire. Vous pouvez générer un certificat auto-signé ou importer un certificat signé par une CA externe.

Pour utiliser un certificat auto-signé, vous devez tout d'abord créer un certificat CA racine puis utiliser cette CA pour signer le certificat que vous utiliserez pour le contrôle prioritaire de l'URL par l'administrateur comme suit :

1. Pour créer un certificat d'autorité de certification racine, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **Certificates (Certificats)** > **Device Certificates (certificats de périphérique)**, puis cliquez sur **Generate (Générer)**. Saisissez un **nom de certificat**, RootCA par exemple. Ne sélectionnez pas de valeur dans le champ **Signed By (Signé par)** (ceci indique qu'il est auto-signé). Veillez à bien cocher la case **Certificate Authority (Autorité de certification)**, puis cliquez sur **Generate (Générer)** le certificat.

2. Pour créer le certificat à utiliser pour le forçage de l'URL par l'administrateur, cliquez sur **Generate (Générer)**. Saisissez le **Certificate Name (Nom du certificat)**, puis le nom DNS de l'hôte ou l'adresse IP de l'interface en tant que **Common Name (Nom commun)**. Dans le champ **Signed By (Signé par)**, sélectionnez l'AC créée à l'étape précédente. Ajoutez un attribut d'adresse IP, puis précisez l'adresse IP de l'interface de Couche 3 vers laquelle les requêtes Web seront redirigées vers des catégories d'URL comprenant l'action de contrôle prioritaire.
3. **Generate (Générez)** le certificat.
4. Pour configurer des clients autorisant le certificat, sélectionnez le certificat AC dans l'onglet **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Export (Exporter)**. Vous devez ensuite importer le certificat en tant que CA racine de confiance dans tous les navigateurs clients, en configurant manuellement le navigateur ou en ajoutant le certificat aux racines de confiance d'un objet GPO (Group Policy Object) d'Active Directory.

STEP 5 | Spécifiez les catégories d'URL qui requièrent un mot de passe de contrôle prioritaire pour en autoriser l'accès.

1. Sélectionnez **Objects (Objets)** > **URL Filtering (Filtrage des URL)**, puis sélectionnez un profil de Filtrage des URL existant ou cliquez sur **Add (Ajouter)** pour en créer un nouveau.
2. Dans l'onglet **Categories (Catégories)**, définissez l'action sur **override (contrôle prioritaire)** pour chaque catégorie demandant un mot de passe.
3. Renseignez les sections restantes du profil de Filtrage des URL, puis cliquez sur **OK (OK)** pour enregistrer le profil.

STEP 6 | Appliquez le profil de filtrage des URL à la ou aux règles de politique de Sécurité qui autorisent l'accès aux sites demandant un mot de passe de contrôle prioritaire pour l'accès.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez la politique de Sécurité adéquate pour la modifier.
2. Cliquez sur l'onglet **Actions** puis, dans la section **Profile Setting (Paramètre de profil)**, cliquez sur la liste déroulante **URL Filtering (URL Filtering)** et sélectionnez le profil.
3. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

STEP 7 | **Commit (Validez)** la configuration.

Prévention contre le hameçonnage des informations d'identification

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Les sites d'hameçonnage sont des sites auxquels les pirates donnent une apparence légitime dans le but de voler les informations des utilisateurs, particulièrement les informations d'identification d'entreprise qui procurent l'accès à votre réseau. Lorsqu'un e-mail d'hameçonnage pénètre dans un réseau, il suffit qu'un seul utilisateur clique sur le lien et saisisse ses informations d'identification pour lancer une violation. Vous pouvez détecter et détecter les attaques par hameçonnage en cours et ainsi empêcher le vol de vos informations d'identification, en contrôlant les sites sur lesquels les utilisateurs peuvent transmettre leurs informations d'identification d'entreprise selon la catégorie d'URL du site. Vous pouvez ainsi empêcher les utilisateurs de transmettre leurs informations d'identifications à des sites non approuvés, tout en leur permettant de continuer de les transmettre aux sites de l'entreprise ou aux sites approuvés.

La prévention du hameçonnage des informations d'identification passe par l'analyse des noms d'utilisateur et des mots de passe transmis aux sites Web et leur comparaison aux informations d'identification d'entreprise valides. Vous pouvez choisir les sites Web auxquels vous souhaitez autoriser ou bloquer l'envoi des informations d'identification d'entreprise selon la catégorie d'URL du site Web. Lorsqu'un utilisateur tente de soumettre des informations d'identification à un site d'une catégorie faisant l'objet d'une restriction, soit une page de réponse de blocage empêche l'utilisateur de transmettre ces informations d'identification ou une page permettant de continuer avertit l'utilisateur de ne pas soumettre ses informations d'identification à des sites appartenant à certaines catégories d'URL, tout en lui permettant tout de même de poursuivre la transmission. Vous pouvez personnaliser ces pages de réponse pour qu'elles informent les utilisateurs de ne pas réutiliser leurs informations d'identification d'entreprise, même sur des sites légitimes qui ne sont pas des sites d'hameçonnage.

Les rubriques suivantes décrivent les différentes méthodes de détection des informations d'identification que vous pouvez utiliser et fournissent des instructions pour la configuration de la protection contre l'hameçonnage des informations d'identification.

- Méthodes de vérification des soumissions d'informations d'identification de l'entreprise
- Configurer la détection des informations d'identification avec l'agent User-ID de Windows
- Configurer la prévention contre l'hameçonnage des informations d'identification

Méthodes de vérification des soumissions d'informations d'identification de l'entreprise

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Avant d'activer la prévention du hameçonnage des identifiants, décidez de la méthode que vous souhaitez utiliser pour vérifier si des informations d'identification d'entreprise valides ont été soumises sur une page Web.

Méthode de vérification des informations d'identification envoyées	Configuration requise pour la configuration de l'User-ID	Comment cette méthode détecte-t-elle les noms d'utilisateur et/ou les mots de passe des entreprises que les utilisateurs soumettent à des sites Web ?
mappage de groupe	Configuration du Mappage de groupe sur le pare-feu	Le pare-feu vérifie si le nom d'utilisateur qu'un utilisateur saisit sur un site restreint correspond à un nom d'utilisateur d'entreprise valide. Pour ce faire, le pare-feu fait correspondre le nom d'utilisateur saisi à la liste des noms d'utilisateur dans sa table de mappage utilisateur / groupe pour détecter quand les utilisateurs saisissent un nom d'utilisateur sur des sites d'une catégorie restreinte. Cette méthode ne vérifie que les envois de noms d'utilisateur d'entreprise en fonction de l'appartenance à un groupe LDAP, ce qui simplifie la configuration, mais l'expose davantage aux faux positifs.
Mappage des adresses IP aux utilisateurs	Mappages des adresses IP aux noms d'utilisateurs identifiés via le Mappage des utilisateurs, GlobalProtect,	Le pare-feu vérifie si le nom d'utilisateur saisi par un utilisateur sur un site restreint correspond à l'adresse IP du nom d'utilisateur utilisé pour la connexion. Pour ce faire, le pare-feu fait correspondre l'adresse IP du nom d'utilisateur utilisé pour la connexion et le nom d'utilisateur soumis à un site Web à sa table de mappage des adresses IP aux utilisateurs pour détecter

Méthode de vérification des informations d'identification envoyées	Configuration requise pour la configuration de l'User-ID	Comment cette méthode détecte-t-elle les noms d'utilisateur et/ou les mots de passe des entreprises que les utilisateurs soumettent à des sites Web ?
	ou la Politique d'authentification et le portail d'authentification.	le moment où les utilisateurs soumettent leurs noms d'utilisateur d'entreprise à des sites d'une catégorie restreinte. Comme cette méthode correspond à l'adresse IP du nom d'utilisateur utilisé pour la connexion à la session par rapport à la table de mappage adresse IP-nom d'utilisateur, elle constitue une méthode efficace pour détecter les soumissions de noms d'utilisateur d'entreprise, mais pas la soumission de mots de passe d'entreprise. Si vous souhaitez détecter la soumission d'un nom d'utilisateur et d'un mot de passe d'entreprise, vous devez utiliser la méthode de filtrage des informations d'identification de domaine.
Filtre d'informations d'identification de domaine	Agent User-ID Windows configuré avec le module complémentaire de service d'informations d'identification User-ID - ET - Mappages des adresses IP aux noms d'utilisateurs identifiés via le Mappage des utilisateurs, GlobalProtect, ou la Politique d'authentification et le portail d'authentification.	Le pare-feu vérifie si le nom d'utilisateur et le mot de passe soumis par un utilisateur correspondent au nom d'utilisateur et au mot de passe d'entreprise de ce même utilisateur. Pour ce faire, le pare-feu doit être capable de faire correspondre les soumissions d'informations d'identification à des noms d'utilisateur et des mots de passe d'entreprise valides et de vérifier que le nom d'utilisateur soumis correspond à l'adresse IP du nom d'utilisateur utilisé pour la connexion comme suit : • **Pour détecter les noms d'utilisateur et les mots de passe d'entreprise** : le pare-feu récupère un masque de bits sécurisé, appelé *filtre bloom*, à partir d'un agent User-ID Windows équipé du module d'extension de service d'identification utilisateur. Ce service complémentaire analyse votre répertoire pour y trouver des hachages de noms d'utilisateur et de mots de passe et les déconstruit en un masque de bits sécurisé (le filtre bloom) et le délivre à l'agent User-ID Windows. Le pare-feu extrait le filtre bloom de l'agent User-ID Windows à intervalles réguliers. Chaque fois qu'il détecte la soumission, par un utilisateur, d'informations d'identification à une catégorie restreinte, il reconstruit le filtre bloom et recherche un hachage de nom d'utilisateur et de mot de passe correspondant. Le pare-feu peut uniquement se connecter à un agent User-ID

Méthode de vérification des informations d'identification envoyées	Configuration requise pour la configuration de l'User-ID	Comment cette méthode détecte-t-elle les noms d'utilisateur et/ou les mots de passe des entreprises que les utilisateurs soumettent à des sites Web ?
		Windows qui exécute le module complémentaire des informations d'identification User-ID. • **Pour vérifier que les informations d'identification appartiennent au nom d'utilisateur utilisé pour la connexion** : Le pare-feu recherche un mappage entre l'adresse IP du nom d'utilisateur utilisé pour la connexion et le nom d'utilisateur détecté dans sa table de mappage des adresses IP aux noms d'utilisateur. Pour en savoir plus sur la méthode des informations d'identification de domaine, consultez Configurer la détection des informations d'identification à l'aide de l'agent d'ID utilisateur Windows.

Configurer la détection des identifiants avec l'agent User-ID de Windows

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

La détection du filtre d'informations d'identification de domaine permet au pare-feu de détecter les mots de passe qui ont été soumis à des pages Web. Cette méthode de détection des identifiants exige que l'agent User-ID Windows et le service d'informations d'identification User-ID, un module d'extension de l'agent User-ID, soient installés sur un *Read-Only Domain Controller (contrôleur de domaine en lecture seule ; RODC).*

La méthode de détection des identifiants de domaine est prise en charge avec l'agent User-ID Windows uniquement. Vous ne pouvez pas utiliser l'agent User-ID intégré à PAN-OS pour configurer cette méthode de détection des informations d'identification.

Un RODC est un serveur Microsoft Windows qui conserve une copie en lecture seule d'une base de données Active Directory qu'un contrôleur de domaine héberge. Lorsque le contrôleur de domaine se trouve au siège social d'une entreprise, les RODC peuvent être déployés à des emplacements réseau distants pour fournir les services d'authentification locale. Il peut être utile d'installer l'agent User-ID sur un RODC pour diverses raisons : l'accès à l'annuaire du contrôleur de domaine n'est pas requis pour activer la détection des informations d'identification et vous pouvez prendre en charge la détection des informations d'identification pour un ensemble d'utilisateurs restreint ou cible. Étant donné que l'annuaire qu'héberge le RODC est en lecture seule, son contenu est protégé sur le contrôleur de domaine.

Comme vous devez installer l'agent User-ID Windows sur le RODC pour utiliser la détection des identifiants, il est recommandé de déployer un agent distinct à cette fin. N'utilisez pas l'agent User-ID qui est installé sur le RODC pour mapper les adresses IP à des utilisateurs.

Après avoir installé l'agent User-ID sur un RODC, le service d'informations d'identification User-ID s'exécute en arrière-plan et analyse l'annuaire afin d'y repérer le hachage des noms d'utilisateur et des mots de passe des membres des groupes qui figurent dans la Password Replication Policy (Stratégie de réplication de mot de passe ; PRP) du RODC. Vous pouvez définir les membres que vous souhaitez voir sur la liste. Le service d'informations d'identification User-ID prend ensuite les hachages de mots de passe et les noms d'utilisateur recueillis et déconstruit les données dans un type de masque de bits que l'on appelle un *filtre de Bloom*. Les filtres de Bloom sont des structures de données compactes qui procurent un moyen sécuritaire de vérifier si un élément (un hachage de mot de passe ou un nom d'utilisateur) fait partie d'un ensemble d'éléments (l'ensemble des informations d'identification que vous avez approuvées aux fins de réplication dans le RODC). Le service d'identifiants User-ID transfère le filtre de Bloom à l'agent User-ID Windows ; le pare-feu récupère le dernier filtre de Bloom auprès de l'agent User-UD à des intervalles réguliers et l'utilise pour détecter tout envoi du hachage d'un mot de passe ou d'un nom d'utilisateur. Selon vos paramètres, le pare-feu bloque, alerte ou autorise l'envoi de mots de passe valides aux pages Web ou présente aux utilisateurs une page de réponse les avertissant des risques d'hameçonnage, tout en les laissant continuer l'envoi.

Tout au long de ce processus, l'agent User-ID ne consigne ni expose aucun hachage de mot de passe et ne transmet aucun hachage de mot de passe au pare-feu. Une fois les hachages de mot de passe déconstruits en un filtre de Bloom, il n'est plus possible de les récupérer.

STEP 1 | Configure user mapping using the Windows User-ID agent (Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows)

> *Pour activer la détection des identifiants, vous devez installer l'agent User-ID Windows sur un RODC. Consultez la grille de compatibilité pour obtenir une liste des serveurs pris en charge. Installez un agent User-ID distinct à cette fin.*

Points importants à ne pas oublier lors de la configuration de User-ID dans le but d'activer la détection du filtre d'informations d'identification de domaine :

- L'efficacité de la détection de l'hameçonnage des informations d'identification dépend de la configuration de votre contrôleur de domaine en lecture seule. Assurez-vous de consulter les meilleures pratiques et les recommandations pour l'administration RODC.
- Téléchargez les mises à jour logicielles de User-ID :
  - Programme d'installation de l'agent User-ID Windows : UaInstall-x.x.x-x.msi.
  - Programme d'installation du service d'informations d'identification de l'agent User-ID Windows : UaCredInstall64-x.x.x-x.msi.
- Installez l'agent User-ID et le service d'informations d'identification de l'agent User-ID sur un RODC en utilisant un compte qui dispose des autorisations nécessaires pour lire Active Directory via LDAP (l'agent User-ID doit également détenir cette autorisation).
  - Le service d'informations d'identification de l'agent User-ID exige la permission d'ouvrir une session au compte de système local. Pour obtenir de plus amples informations, consultez créer un compte de service dédié pour l'agent User-ID.
  - Le compte de service doit être membre du groupe d'administrateurs local sur le RODC.

STEP 2 | Activez l'option de partages des informations sur l'agent User-ID et le service d'informations d'identification de l'agent User-ID (qui s'exécute en arrière-plan pour analyser les informations d'identification autorisées).

1. Sur le serveur RODC, lancez l'agent User-ID.
2. Sélectionnez **Setup (Configuration)** et modifiez la section Setup (Paramétrage).
3. Sélectionnez l'onglet **Credentials (Informations d'identification)**. Cet onglet n'apparaît que si vous avez déjà installé le service d'informations d'identification de l'agent User-ID.
4. Sélectionnez **Import from User-ID Credential Agent (Importer à partir de l'agent d'informations d'identification User-ID)**. Cette sélection permet à l'agent User-ID d'importer le filtre de Bloom que l'agent d'informations d'identification crée pour représenter les utilisateurs et les hachages de mot de passe correspondants.
5. Cliquez sur **OK (OK)**, **Save (Enregistrez)** vos paramètres et **Commit (Validez)**.

STEP 3 | Dans l'annuaire RODC, définissez le groupe d'utilisateurs pour lequel vous souhaitez prendre en charge la détection de l'envoi des informations d'identification.

- Confirmez que les groupes pour lesquels l'envoi des informations d'identification doit faire l'objet d'un contrôle ont été ajoutés au groupe Réplication de mot de passe sur un RODC autorisée.
- Vérifiez qu'aucun des groupes du groupe Réplication de mot de passe sur un RODC autorisée ne se trouve également dans le groupe Réplication de mot de passe sur un RODC

refusée par défaut. Les groupes qui se trouvent dans les deux groupes ne seront pas soumis au contrôle contre l'hameçonnage des informations d'identification.

STEP 4 | Passez à la tâche suivante.

Set up credential phishing prevention Paramétrage de la protection contre l'hameçonnage des informations d'identification) sur le pare-feu.

Configurer la prévention contre le hameçonnage des informations d'identification

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	☐ Advanced URL Filtering licence (ou une licence de filtrage des URL héritée) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Une fois que vous avez décidé quelle méthode de détection d'identification d'utilisateur configurer, procédez comme suit pour empêcher les attaques de phishing d'identification réussies.

Avant d'activer la prévention du phishing des informations d'identification, vérifiez que le Primary Username (nom d'utilisateur principal) que vous configurez sur le pare-feu utilise l'attribut sAMAccountName. La prévention de l'hameçonnage des informations d'identification ne prend pas en charge d'autres attributs.

- Strata Cloud Manager
- PAN-OS et Panorama

Configurer la prévention de l'hameçonnage des informations d'identification (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS et Panorama** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Configurez la méthode de détection des informations d'identification de l'utilisateur que vous souhaitez utiliser.

Examinez les méthodes de vérification des soumissions d'informations d'identification de l'entreprise pour obtenir des détails sur chaque méthode.

- Pour le mappage des utilisateurs IP, configurez des utilisateurs et groupes locaux, la redistribution d'identité ou l'authentification avec Prisma Access.
- Pour utiliser le filtre d'informations d'identification de domaine, définissez la redistribution d'identité et les utilisateurs et groupes locaux ou l'authentification.
- Pour utiliser le mappage de groupe, configurez des utilisateurs et des groupes locaux ou l'authentification.

STEP 2 | Créez une règle politique de décryptage qui décrypte le trafic que vous souhaitez surveiller pour les soumissions d'informations d'identification utilisateur.

STEP 3 | Créer ou modifier un profil de gestion de l'accès à l'URL.

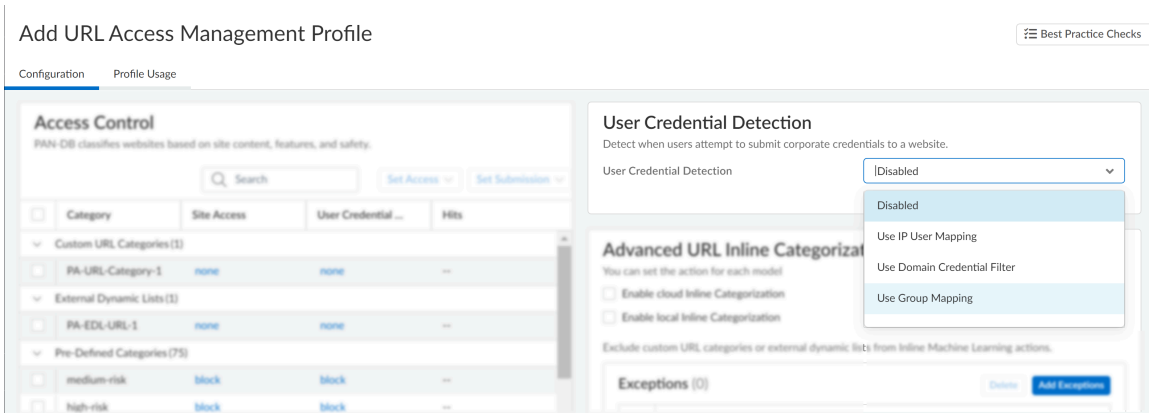
1. Sélectionnez **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Gestion des accès à l'URL**.
2. Sous Profils de gestion des accès à l'URL, cliquez sur **Ajouter un profil** ou sélectionnez un profil existant.

STEP 4 | Configurez les paramètres de détection des informations d'identification de l'utilisateur.

1. Sous Détection des informations d'identification de l'utilisateur, sélectionnez une méthode de **détection des informations d'identification de l'utilisateur**.
   - **Utiliser le mappage d'utilisateur IP** : Vérifie les saisies de noms d'utilisateurs d'entreprise valides et vérifie que le nom d'utilisateur de connexion correspond à l'adresse IP source de la session. Pour ce faire, Prisma Access fait correspondre le nom d'utilisateur saisi et l'adresse IP source de la session à la table de mappage IP-address-to-username.
   - **Utiliser le filtrage des informations de domaine** : vérifie les saisies de noms d'utilisateurs et mots de passe d'entreprise valides et vérifie si le nom d'utilisateur correspond à l'adresse IP de l'utilisateur connecté.
   - **Utiliser le mappage de groupe** : vérifie si les saisies de nom d'utilisateur valide basé sur la table de mappage user-to-group renseignée quand vous mappez des utilisateurs à des groupes. Vous pouvez appliquer la détection d'informations d'identification à

n'importe quelle partie du répertoire ou pour des groupes spécifiques qui ont accès à vos applications les plus sensibles, telles que le service informatique.

Cette méthode est sujette aux faux positifs dans les environnements qui n'ont pas de noms d'utilisateur structurés de manière unique. Pour cette raison, vous devriez utiliser cette méthode uniquement pour protéger les comptes d'utilisateur de haute valeur.



2. Pour **Gravité des journaux détectée par un nom d'utilisateur valide**, sélectionnez le niveau de gravité que le pare-feu enregistre dans le journal lorsqu'il détecte des soumissions d'informations d'identification d'entreprise :
   - **élevée**
   - (par défaut) **moyen**
   - **faible**

STEP 5 | Configurez l'action effectuée lorsque le pare-feu détecte les soumissions d'informations d'identification de l'entreprise.

1. Sous Contrôle d'accès, sélectionnez une action pour la **soumission d'informations d'identification de l'utilisateur** pour chaque catégorie d'URL avec son ensemble **Accès au site** à autoriser ou à signaler.

   Vous pouvez choisir parmi les actions suivantes :

   - (Recommandé) **alerte** — Permet aux utilisateurs de soumettre des informations d'identification aux sites Web de la catégorie d'URL donnée, mais génère un journal de filtrage des URL chaque fois que cela se produit.
   - (Par défaut) **autoriser** – Autorise les utilisateurs à saisir des informations d'identification sur le site Web.
   - (Recommandé) **blocage**—Empêche les utilisateurs de soumettre des informations d'identification à des sites Web appartenant à la catégorie d'URL donnée. Quand un utilisateur essaie de saisir des informations d'identification, le pare-feu affiche la page de blocage anti-hameçonnage.
   - **continuer** - Affiche la page anti-hameçonnage invitant à continuer aux utilisateurs essayant de saisir des informations d'identification. Les utilisateurs doivent sélectionner Continuer sur la page de réponse pour accéder au site Web.
2. **Enregistrez** le profil.

STEP 6 | Appliquez le profil Gestion des accès à l'URL à vos règles de politique de sécurité.

1. Sélectionnez **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Politique de sécurité**.
2. Sous Règles de politique de sécurité, créez ou sélectionnez une règle de politique de sécurité.
3. Sélectionnez **Actions** > **Groupe de profils**, puis sélectionnez un groupe de profils de gestion de l'accès à l'URL.
4. **Save (Enregistrez)** la règle.

STEP 7 | Cliquez sur **Transmettre la configuration**.

Configurer la prévention de l'hameçonnage des informations d'identification (PAN-OS et Panorama)

STEP 1 | Activez User-ID.

Chacune des methods to check for corporate credential submissions (méthodes de vérification des envois d'informations d'identification d'entreprise) nécessite une configuration d'ID utilisateur différente :

- Mappage de groupe — détecte si un utilisateur soumet un nom d'utilisateur d'entreprise valide et vous oblige à mapper les utilisateurs à des groupes.
- Le mappage d'utilisateur IP – détecte si un utilisateur soumet un nom d'utilisateur d'entreprise valide et si le nom d'utilisateur correspond au nom d'utilisateur de connexion – vous oblige à mapper les adresses IP aux utilisateurs.
- Filtre des informations d'identification du domaine – détecte si un utilisateur soumet un nom d'utilisateur et un mot de passe valides et si ces informations d'identification appartiennent à l'utilisateur connecté – vous oblige à configurer la détection des informations d'identification avec l'agent User-ID Windows et à mapper les adresses IP aux utilisateurs.

STEP 2 | Configurez un Profil de URL Filtering suivant les meilleures pratiques pour assurer une protection contre les URL qui ont été signalées comme hébergeant du contenu malveillant ou à risque.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **URL Filtering (URL Filtering)** et **Add (Ajouter)** ou modifiez un profil de URL Filtering.
2. Bloquez l'accès aux catégories d'URL suivantes : logiciels malveillants, phishing, DNS dynamiques, commandes et contrôles, extrémisme,violation des droits d'auteur, contournement des proxy et des anonymiseurs, domaine nouvellement enregistré, logiciel indésirable et URL en parking.

STEP 3 | Créez une règle de politique de décryptage pour décrypter le trafic que vous souhaitez surveiller pour les soumissions d'identifiants d'utilisateurs.

STEP 4 | Détecter les soumissions d'informations d'identification d'entreprise aux sites Web qui sont dans des catégories d'URL autorisées.

Pour offrir les meilleures performances, le pare-feu ne vérifie pas les soumissions d'identifiants pour les sites de confiance, même si vous activez la vérification pour les catégories d'URL pour ces sites. Les sites de confiance représente les sites pour lesquels Palo Alto Networks n'a pas observé d'activités malicieuses ou d'attaques d'hameçonnage Les mises à jour pour cette liste de sites de confiance sont délivrées au travers des mises à jour d'Applications et de Contenu des menaces

1. Sélectionnez un profil de filtrage des URL (**Objets** > **Profils de sécurité** > **Filtrage des URL**) à modifier.
2. Sélectionnez **Détection des identifiants de l'utilisateur** et choisissez l'une des méthodes de détection des identifiants.

   Confirmez que le format du nom d'utilisateur principal est identique au forme du nom d'utilisateur que la source User-ID fournit.

   - **Use IP User Mapping (Utiliser le mappage d'utilisateur IP)** : Contrôle les saisies de noms d'utilisateurs d'entreprise valides et vérifie que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Pour cela, le pare-feu fait correspondre le nom d'utilisateur saisi et l'adresse IP source à la table de mappage adresse IP/nom d'utilisateur. Pour utiliser cette méthode, configurez n'importe laquelle des méthodes de mappage d'utilisateur décrites dans Mappage d'adresses IP à des utilisateurs.
   - **Use Domain Credential Filter (Utiliser le filtrage par informations de domaine)** : Contrôle les saisies de noms d'utilisateurs d'entreprise et mots de passe valides et vérifie que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Pour obtenir des instructions sur la manière de configurer cette méthode, voir la section Configuration de la détection des informations d'identification avec l'agent User-ID Windows.
   - **Use Group Mapping (Utiliser le mappage de groupe)** : contrôle les saisies de nom d'utilisateur valide basé sur la table de mappage d'utilisateurs à des groupes renseignée quand vous configurez le pare-feu pour le map users to groups (Mappage d'utilisateurs à des groupes).

     Avec le mappage de groupe, vous pouvez appliquer la détection des informations d'identification à toute partie du répertoire, ou à des groupes spécifiques, comme le département informatique, qui ont accès à vos applications les plus sensibles.

     Cette méthode est susceptible de générer des faux positifs dans des environnements où les noms d'utilisateurs ne sont pas structurés de manière unique. Pour cette raison, vous devriez utiliser cette méthode dans le seul but de protéger les comptes utilisateurs de haute valeur.
3. Sélectionnez le **Degré de gravité d'enregistrement des détections de nom d'utilisateur valide** que le pare-feu utilise pour consigner la détection des saisies d'informations d'identification d'entreprise. Par défaut, le pare-feu consigne ces événements en tant que gravité moyenne.

STEP 5 | Bloquez (ou signalez) les tentatives de saisies d'informations d'identification sur des sites autorisés.

1. Sélectionnez **Categories (Catégories)**.
2. Pour chaque catégorie pour laquelle l'**Site Access (Accès au site)** est autorisé, choisissez le comportement que vous voulez adopter pour les **User Credential Submissions (saisies d'informations d'identification entreprise)** :
   - **alert (alerter)** - Autorise les utilisateurs à saisir des informations d'identification sur le site Web, mais génère un journal de Filtrage des URL chaque fois qu'un utilisateur saisit des informations d'identification sur les sites de cette catégorie.
   - **allow (autoriser)** (par défaut) – Autorise les utilisateurs à saisir des informations d'identification sur le site Web.
   - **block (bloquer)** - Empêche les utilisateurs de saisir des informations d'identification sur le site Web. Quand un utilisateur essaie de transmettre des informations d'identification, le pare-feu affiche la page de blocage anti-hameçonnage, empêchant la transmission.
   - **continuer** - Affiche la page anti-hameçonnage invitant à continuer aux utilisateurs essayant de transmettre des informations d'identification. Les utilisateurs doivent sélectionner Continuer sur la page de réponse pour poursuivre leur saisie.
3. Sélectionnez **OK** pour enregistrer le profil de filtrage des URL.

STEP 6 | Appliquez le profil de filtrage des URL avec les réglages de détection des informations d'identification à vos règles de politiques de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (ajoutez)** ou modifiez une règle de politique de sécurité.
2. Dans l'onglet **Actions**, définissez le **Profile Type (Type de profil)** sur **Profiles (Profils)**.
3. Sélectionnez le nouveau profil de **URL Filtering (Filtrage des URL)** ou celui mis à jour à associer à votre règle de politique de sécurité.
4. Cliquez sur **OK** pour enregistrer la règle de politique de sécurité.

STEP 7 | **Commit (Validez)** la configuration.

STEP 8 | Surveillez les saisies des informations d'identification que le pare-feu détecte.

*Select **ACC** > **Hosts Visiting Malicious URLs (hôtes visitant des URLS malveillantes)** afin d'afficher la quantité d'utilisateurs ayant visité des sites malveillants ou d'hameçonnage.*

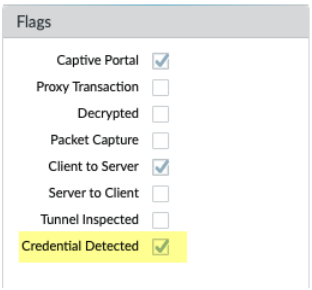
Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **URL Filtering (Filtrage des URL)**.

La nouvelle colonne **Credential Detected (Informations d'identification détectées)** indique les événements où le pare-feu a détecté un requête HTTP Post incluant des informations d'identifications valides.

	CATEGORY	APPLICATION	ACTION	CREDENTIAL DETECTED
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes

Pour afficher cette colonne, placez la souris sur n'importe quelle colonne et cliquez sur la flèche pour sélectionner les colonnes à afficher).

Les détails des entrées du journal indiquent également les saisies d'informations d'identification.



STEP 9 | Confirmation et dépannage des détections de saisies d'informations d'identification.

- Servez-vous de la commande CLI suivante pour voir les statistiques des détections de saisies d'informations d'identification :

```
> show user credential-filter statistics
```

La sortie pour cette commande varie selon la méthode configurée de détection par le pare-feu des saisies d'informations d'identification. Par exemple, si la méthode de Filtrage par Informations de Domaine est configurée pour tout profil de URL Filtering, une liste d'agents User-ID ayant transféré un filtre de Bloom vers le pare-feu est affichée, ainsi que le nombre d'informations d'identification contenue dans ce filtre de Bloom.

- (Uniquement pour la méthode de Mappage de Groupe) - Servez-vous de la commande CLI suivante pour voir les informations de mappage de groupe, dont le nombre de profils de filtrage d'URL avec la détection d'informations d'identification de mappage de groupe activée, ainsi que les noms d'utilisateurs des membres du groupe ayant tenté de saisir des informations d'identification sur des sites restreints.

```
> show user group-mapping statistics
```

- (Méthode de filtrage des informations d'identification de domaine uniquement) Utilisez la commande CLI suivante pour afficher tous les agents d'ID utilisateur Windows qui envoient des mappages au pare-feu :

```
> show user user-id-agent state all
```

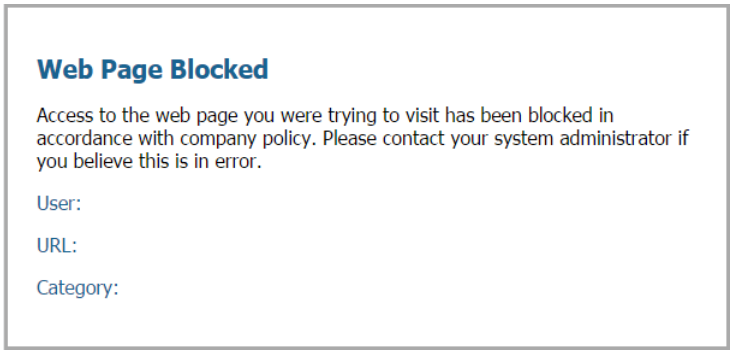
  La sortie de la commande affiche désormais le nombre de filtres de Bloom qui incluent le nombre de mises à jour de filtre de Bloom que le pare-feu a reçues de chaque agent, si des mises à jour de filtre de Bloom n'ont pas pu être traitées, et combien de secondes se sont écoulées depuis la dernière mise à jour du filtre de Bloom.

- (Uniquement pour la méthode de Filtrage par Informations de Domaine) - L'agent User-ID Windows affiche des messages de journal mentionnant des transmissions de filtre de Bloom vers le pare-feu. Dans l'interface agent User-ID, sélectionnez **Surveillance** > **Journaux**.

Pages de réponse de URL Filtering

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Les pages de réponse de filtrage des URL informent les utilisateurs lorsque l'accès à une URL demandée a été restreint. L'accès peut être restreint si un site appartient à une catégorie qui a été configurée avec une action de blocage, de poursuite ou de remplacement, ou si les soumissions d'informations d'identification au site ou à la catégorie ont été bloquées. Si un utilisateur ne dispose pas des paramètres de recherche sécurisée les plus stricts configurés pour un moteur de recherche et qu'une règle de politique de sécurité applique la recherche sécurisée, l'accès est également limité. Cinq pages de réponse prédéfinies existent pour tenir compte de ces raisons. Certaines pages de réponse bloquent simplement l'accès, tandis que d'autres autorisent un accès conditionnel. Par exemple, si la Page de maintien et de contrôle prioritaire du filtrage des URL ou la Page de poursuite anti-hameçonnage s'affiche, les utilisateurs peuvent cliquer sur Continuer pour accéder au site (sauf si l'option Remplacement de l'administrateur d'URL est activée).



En général, les pages de réponse indiquent pourquoi la page n'est pas accessible et répertorient l'utilisateur, l'URL et la catégorie d'URL. Cependant, vous pouvez personnaliser le contenu et l'apparence des pages de réponse. Par exemple, vous pouvez modifier le message de notification, créer un lien vers votre politique d'utilisation acceptable ou ajouter une image de marque de l'entreprise.

Vous pouvez observer des variations dans l'apparence des pages de réponse entre les différentes versions du logiciel PAN-OS. Cependant, la fonctionnalité reste la même.

N'oubliez pas que vous pouvez personnaliser les pages de réponse pour répondre à vos besoins spécifiques.

Les navigateurs n'affichent pas les pages de réponse si les inspections des liaisons SSL/TLS sont activées.

- Pages de réponse de filtrage des URL prédéfinies
- Objets de page de réponse de filtrage des URL
- Personnalisation des pages de réponse de filtrage des URL

Pages de réponse de filtrage des URL prédéfinies

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

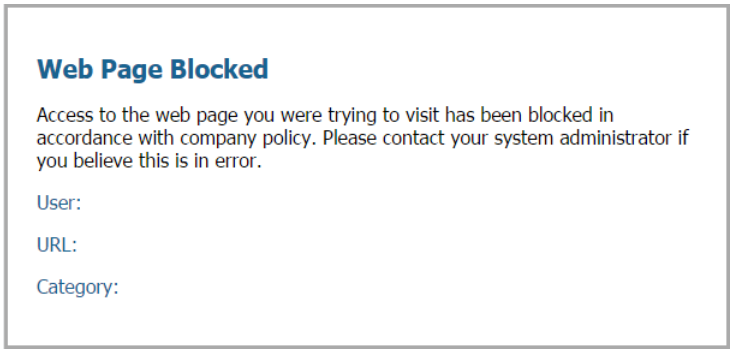
pages de réponse de filtrage des URL s'affichent sur les navigateurs Web lorsque l'accès à une URL demandée a été restreint. Chaque page de réponse explique pourquoi la page n'est pas accessible, et la plupart des pages répertorient des informations sur l'utilisateur, l'URL demandée et la catégorie d'URL qui a déclenché l'action de blocage.

Vous pouvez observer des variations dans l'apparence des pages de réponse entre les différentes versions du logiciel PAN-OS. Cependant, la fonctionnalité reste la même.

N'oubliez pas que vous pouvez personnaliser les pages de réponse pour répondre à vos besoins spécifiques.

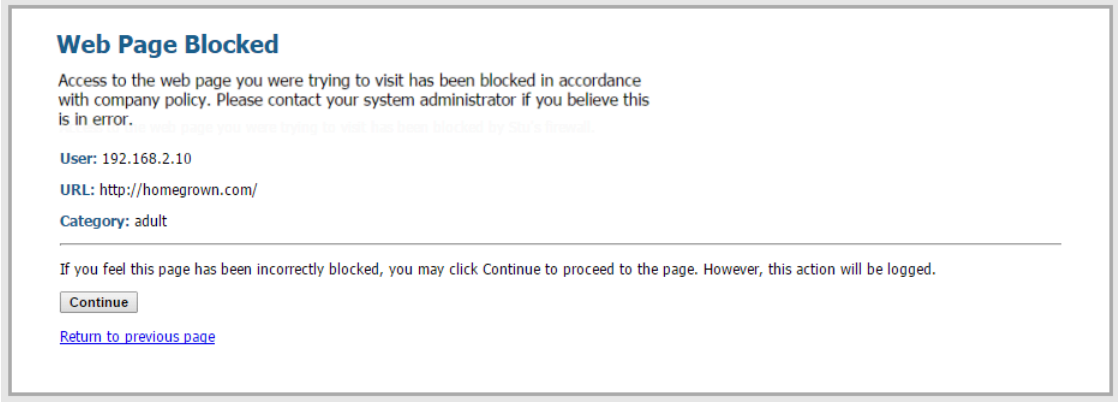
- **Page de blocage du filtrage et des correspondances de catégories des URL**

  Accès bloqué par un profil de URL Filtering ou parce que la catégorie d'URL est bloquée par une règle de politique de Sécurité.



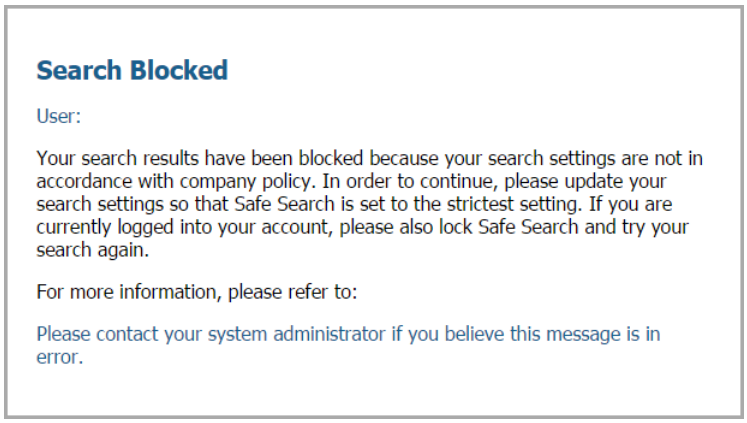
- **Page de maintien et de contrôle prioritaire du URL Filtering**

Page incluant la politique de blocage initiale permettant aux utilisateurs d'ignorer le blocage en cliquant sur **Continue (Continuer)**. Lorsque le contrôle prioritaire de l'URL par l'administrateur est activé (Allow Password Access to Certain Sites (Autoriser l'accès par mot de passe à certains sites), après avoir cliqué sur **Continue (Continuer)**, l'utilisateur doit fournir un mot de passe pour forcer la politique bloquant cette URL.



- **Page de blocage de la recherche sécurisée du filtrage d'URL**

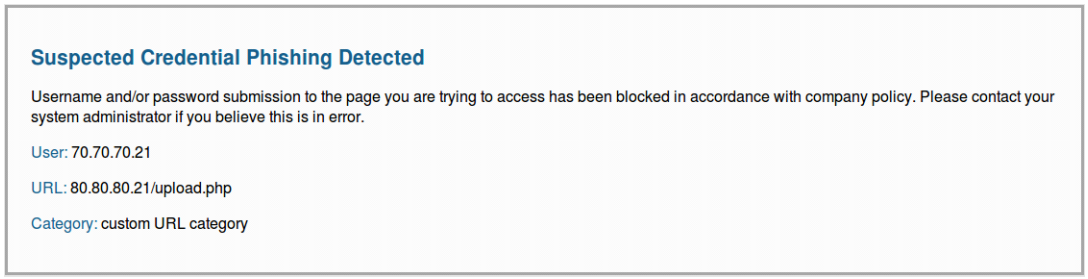
  Accès bloqué par une règle de politique de sécurité dotée d'un profil de filtrage des URL pour lequel l'option Mise en œuvre de la recherche sécurisée est activée (voir Mise en œuvre de la recherche sécurisée). Cette page est présentée à l'utilisateur si une recherche est effectuée à l'aide de Google, Bing, Yahoo ou Yandex et que le paramètre de recherche sécurisée de son compte de moteur de recherche ou de navigateur n'est pas défini sur Strict.



- **Page de blocage anti-hameçonnage**

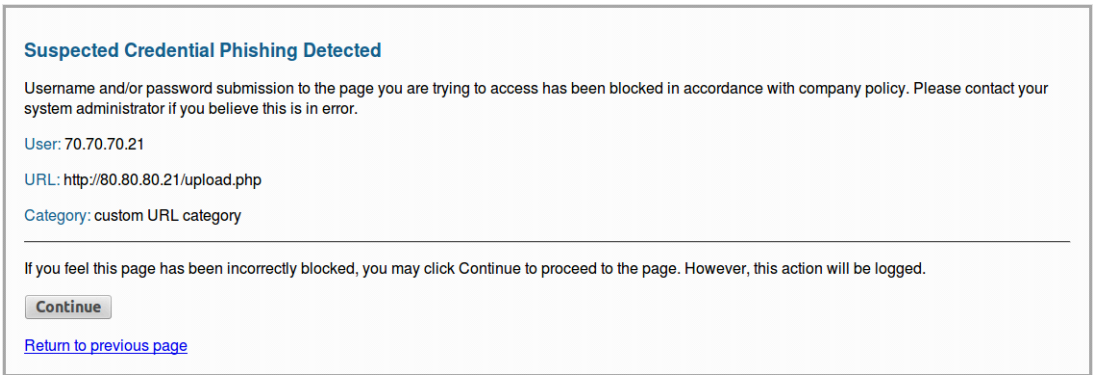
  Cette page s'affiche aux utilisateurs lorsqu'ils tentent de saisir des informations d'identification d'entreprise (noms d'utilisateur ou mots de passe) sur une page Web dans une catégorie sur laquelle l'envoi des informations d'identification est bloqué. L'utilisateur peut accéder au site, mais il ne peut toujours pas saisir des informations d'identification d'entreprise valides pour tous les formulaires Web associés. Pour contrôler les sites auxquels les utilisateurs peuvent

soumettre des informations d'identification d'entreprise, vous devez configurer User-ID et activer Prévention du phishing d'identifiants en fonction de la catégorie d'URL.



- **Page de poursuite anti-hameçonnage**

  Cette page met en garde les utilisateurs contre la transmission des informations d'identification (noms d'utilisateur et mots de passe) vers un site Web. La mise en garde des utilisateurs contre la transmission des informations d'identification peut les décourager de réutiliser les informations d'identification de l'entreprise et les informer sur les éventuelles tentatives d'hameçonnage. Ils doivent sélectionner Continuer pour saisir les informations d'identification sur le site. Pour contrôler les sites auxquels les utilisateurs peuvent soumettre des informations d'identification d'entreprise, vous devez configurer User-ID et activer Prévention du phishing d'identifiants en fonction de la catégorie d'URL.



Objets de page de réponse de filtrage des URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Utilisez les variables et les références décrites dans les sections suivantes pour personnaliser les pages de réponse de filtrage des URL. Les variables de la page de réponse affichent des informations différentes sur les demandes d'URL. Par exemple, le pare-feu remplace la `<category/>` variable dans le code HTML des pages de réponse avec les catégories d'URL d'une URL demandée. Les références de la page de réponse vous permettent d'ajouter des images, des sons, des feuilles de style et des liens externes.

Variables de la page de réponse

Le tableau suivant répertorie les variables de page de réponse et les informations ou objets que le système remplace par chaque variable lors d'un événement de blocage. Par défaut, chaque page de réponse de filtrage des URL utilise les variables suivantes : utilisateur, URL et catégorie. Cependant, les pages de réponse sont personnalisables. Par exemple, vous pouvez modifier l'ordre des variables ou ajouter des messages différents pour des catégories d'URL spécifiques.

Variable	Usage
<user/>	Le pare-feu remplace la variable par le nom d'utilisateur (si disponible via User-ID) ou l'adresse IP de l'utilisateur lors de l'affichage de la page de réponse.
<url/>	Le pare-feu remplace la variable par l'URL demandée lors de l'affichage de la page de réponse.
<category/>	Le pare-feu remplace la variable par la catégorie de URL Filtering de la demande bloquée.
<pan_form/>	Le code HTML pour l'affichage du bouton **Continue (Continuer)** sur la page Continuer et Contrôle prioritaire du URL Filtering.

Vous pouvez également ajouter un code demandant au pare-feu d'afficher différents messages en fonction de la catégorie d'URL à laquelle l'utilisateur tente d'accéder. Par exemple, l'extrait de code suivant d'une page de réponse demande l'affichage du Message 1 si la catégorie d'URL est « jeux », le Message 2 si la catégorie est « voyages » ou le Message 3 si la catégorie est « enfants » :

```
var cat = «<category/>»; switch(cat) { case 'games':
 document.getElementById(« warningText »).innerHTML = « Message 1 »;
 break; case 'travel':
 document.getElementById(« warningText »).innerHTML = « Message 2 »;
 break; case 'kids':
 document.getElementById(« warningText »).innerHTML = « Message 3 »;
 break; }
```


Références de page de réponse

Une seule page HTML peut être chargée sur chaque système virtuel pour chaque type de page de blocage. D'autres ressources comme des images, des sons et des feuilles de styles au format CSS, peuvent toutefois être chargées d'autres serveurs lorsque la page de réponse s'affiche dans le navigateur. Toutes les références doivent contenir une URL complète.

Type de référence	Exemple de code HTML
Image	`<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">`
Son	`<embed src="http://simplythebest.net/sounds/WAV/WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">`
Feuille de styles	`<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />`
Lien hypertexte	`<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">Voir la politique d'entreprise</a>`

Personnalisation des pages de réponse de filtrage des URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Par défaut, les pages de réponse de filtrage des URL expliquent pourquoi une URL demandée ne peut pas être consultée et indiquent l'adresse IP de l'utilisateur, l'URL demandée et la catégorie d'URL. Vous pouvez personnaliser les pages de réponse pour répondre aux besoins de votre

entreprise. Par exemple, vous pouvez modifier le message affiché aux utilisateurs, ajouter une marque d'entreprise ou un lien vers une politique d'utilisation acceptable.

Pour personnaliser une page, exportez-la depuis une plateforme et modifiez-la dans un éditeur de texte. Vous pouvez effectuer des mises à jour en utilisant les variables et références des page de réponse fournies. Les variables de page de réponse correspondent à l'utilisateur, l'URL et la catégorie spécifiques qui ont été bloqués. Les références de page de réponse permettent l'utilisation d'images, de sons, de feuilles de style et de liens.

L'interface web Panorama™ ne prend pas en charge l'exportation des pages de réponse.

Les pages de réponse personnalisées qui dépassent la taille maximale prise en charge ne sont pas déchiffrées ou affichées aux utilisateurs. Dans la version PAN-OS 8.1.2 et les versions PAN-OS 8.1 antérieures, les pages de réponse personnalisées sur un site décrypté ne peuvent dépasser 8 191 octets ; la taille maximale est passée à 17 999 octets dans PAN-OS 8.1.3 et les versions ultérieures.

- Strata Cloud Manager
- PAN-OS et Panorama

Personnalisation des pages de réponse de filtrage des URL (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Exportez les pages de réponse par défaut que vous souhaitez personnaliser.

1. Sélectionnez **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Gestion d'accès à l'URL** > **Paramètres**.
2. Dans le volet Pages de réponse, cliquez sur **Exporter le modèle HTML** pour chaque page de réponse que vous souhaitez modifier.
3. Enregistrez les fichiers sur votre système.

STEP 2 | Modifiez une page de réponse exportée.

1. À l'aide de l'éditeur de texte HTML de votre choix, modifiez la page :
   - Pour afficher des informations personnalisées sur l'utilisateur, l'URL ou la catégorie spécifiques qui a été bloqué, ajoutez une ou plusieurs variables de pages de réponse.
   - Pour inclure des images, des sons, des feuilles de style ou des liens personnalisés, incluez une ou plusieurs références de pages de réponse.
2. Enregistrez la page modifiée avec un nouveau nom de fichier.

   *Veillez à ce que la page conserve son codage UTF-8. Par exemple, dans Notepad, vous sélectionnez **UTF-8** dans la liste déroulante **Codage** de la boîte de dialogue Enregistrer sous.*

STEP 3 | Importez la page de réponse personnalisée.

1. Sélectionnez **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Gestion d'accès à l'URL** > **Paramètres**.
2. Dans le volet Pages de réponse, cliquez sur le type de page de réponse que vous avez personnalisé. Une boîte de dialogue de sélection de fichier apparaît.

   Par exemple, si vous aviez personnalisé la page Blocage de la gestion des accès à l'URL, vous cliqueriez sur la**Page Blocage de la gestion des accès à l'URL**.
3. Cliquez sur **Choisir un fichier**, puis sélectionnez le fichier personnalisé.
4. Cliquez sur **Save (Enregistrer)**.

STEP 4 | Cliquez sur **Transmettre la configuration**.

STEP 5 | Vérifiez que la page de réponse personnalisée s'affiche.

Depuis un navigateur Web, visitez une URL qui déclenchera la page de réponse. Par exemple, pour vérifier une page personnalisée de blocage de gestion des accès à l'URL, visitez une URL bloquée par vos règles de politique de sécurité.

Le pare-feu utilise les ports suivants pour afficher les pages de réponse de la Gestion des accès à l'URL :

- **HTTP** : 6080
- **TLS par défaut avec certificat de pare-feu** : 6081
- **Profil SSL/TLS personnalisé** : 6082

Personnalisation des pages de réponse de filtrage des URL (PAN-OS et Panorama)

STEP 1 | Exportez les pages de réponses prédéfinies que vous souhaitez personnaliser.

L'interface Web Panorama ne prend pas en charge l'exportation des pages de réponse. Vous pouvez exporter des pages de réponse directement à partir de l'interface Web d'un pare-feu spécifique ou utiliser la liste déroulante Contexte de l'interface Web Panorama pour passer rapidement à l'interface Web d'un pare-feu géré.

1. Sélectionnez **Périphérique** > **Pages de réponse**.
2. Sélectionnez le **Type** de page de réponse que vous souhaitez modifier. Une boîte de dialogue pour la page de réponse spécifique apparaît.
3. Sélectionnez **Prédéfini**, puis sélectionnez **Exporter**.
4. **Fermez** la boîte de dialogue.

   (Facultatif) Répétez les étapes deux à quatre pour les pages de réponse supplémentaires.
5. Enregistrez les fichiers sur votre système.

STEP 2 | Personnalisez une page de réponse HTML exportée.

1. Ouvrez le fichier dans un éditeur de texte préféré.
   - Pour afficher des informations personnalisées sur un utilisateur spécifique, une URL demandée ou une catégorie d'URL bloquée, utilisez les variables de page de réponse.
   - Pour intégrer des images, des sons, des feuilles de style ou des liens personnalisés, utilisez des références de page de réponse.
2. Enregistrez le fichier édité avec un nouveau nom.

   *Veillez à ce que la page conserve son codage UTF-8. Par exemple, dans Notepad, vous sélectionnez **UTF-8 (UTF-8)** dans la liste déroulante **Encoding (Codage)** de la boîte de dialogue Save As (Enregistrer sous).*

STEP 3 | Importez la page de réponse personnalisée.

1. Sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**.
2. Sélectionnez le **Type** de page de réponse que vous avez modifié. Une boîte de dialogue pour la page de réponse spécifique apparaît.
3. Sélectionnez **Prédéfini**, puis sélectionnez **Importer**. Une boîte de dialogue Importer un fichier apparaît.

   Pour **Importer un fichier**, **Parcourez** la page de réponse modifiée.
4. (Facultatif) Pour **Destination**, sélectionnez le système virtuel qui utilisera la page de réponse, ou sélectionnez **partagé** pour le rendre disponible à tous les systèmes virtuels.
5. Cliquez sur **OK**, puis **Fermez** la boîte de dialogue.

STEP 4 | **Commit (Validez)** vos modifications.

STEP 5 | Testez la page de réponse personnalisée.

Depuis un navigateur Web, visitez une URL qui déclenche la page de réponse particulière. Par exemple, pour vérifier une page de réponse de filtrage des URL et de correspondance des catégories, visitez une URL bloquée dans une règle de politique de sécurité. Vérifiez que vos modifications apparaissent.

Le pare-feu utilise les ports suivants pour afficher les pages de réponse du URL Filtering :

- **HTTP** : 6080
- **TLS par défaut avec certificat de pare-feu** : 6081
- **Profil SSL/TLS personnalisé** : 6082

Mise en œuvre de la recherche sécurisée

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.* • Une SafeSearch transparente nécessite une licence Prisma Access exécutant une version minimale de 4.1.

De nombreux moteurs de recherche offrent un paramètre de recherche sécurisé qui vous permet de filtrer le contenu adulte des résultats de recherche. Les paramètres de filtre incluent généralement `Modéré`, `Strict` et `Désactivé`. Vous pouvez utiliser le paramètre modéré pour filtrer uniquement les images et vidéos pour adultes ou le paramètre strict, qui filtre en outre le texte explicite. Les établissements d'enseignement, les lieux de travail, les enfants et les adultes bénéficient tous de cette fonctionnalité de recherche sécurisée. Cependant, autoriser les utilisateurs de votre réseau à configurer les paramètres de recherche sécurisée ne fournit pas toujours la protection dont vous avez besoin.

Pour protéger votre réseau contre le contenu destiné aux adultes, vous pouvez imposer le paramètre de recherche sécurisée le plus strict pour tous les utilisateurs finaux, quels que soient leurs paramètres individuels actuels. Le paramètre de recherche sécurisée le plus strict offre l'expérience de navigation la plus sûre. Tout d'abord, sélectionnez l'option **Mise en œuvre de la recherche sécurisée** dans un profil de filtrage des URL. Ensuite, appliquez le profil à toutes les règles de politique de sécurité qui autorisent le trafic des clients de la zone de confiance vers Internet.

Ni les fournisseurs de moteurs de recherche ni Palo Alto Networks ne peuvent garantir une précision de filtrage totale. Les moteurs de recherche classent les sites Web comme sûrs ou dangereux. En conséquence, un site Web classé comme sûr peut contenir un contenu explicite. Palo Alto Networks applique un filtrage basé uniquement sur les mécanismes de filtrage du moteur de recherche.

Le pare-feu peut imposer les options suivantes lorsque les utilisateurs effectuent une recherche avec Bing, Yahoo, Yandex ou YouTube et n'ont pas défini le paramètre de recherche sécurisée pour ces moteurs au niveau le plus strict :

- Bloquer les résultats de recherche lorsque la recherche sécurisée stricte est désactivée (Par défaut) — Le pare-feu empêche les utilisateurs finaux de voir les résultats de recherche jusqu'à ce qu'ils définissent leur paramètre de recherche sécurisée sur l'option disponible la plus

stricte. Dans ce scénario, le navigateur affiche la page de blocage de recherche sécurisée de filtrage des URL. Cette page de réponse permet aux utilisateurs finaux de savoir pourquoi leurs résultats de recherche ont été bloqués et inclut un lien vers les paramètres de recherche du moteur de recherche utilisé pour la recherche.

> *Palo Alto Networks ne peut plus détecter si Google SafeSearch est activé en raison de changements dans l'implémentation de la recherche sécurisée Google. En conséquence, la méthode de blocage ne fonctionne pas pour les recherches Google. Au lieu de cela, vous pouvez configurer Google SafeSearch en utilisant les méthodes décrites dans* Réglages de la recherche sécurisée pour les moteurs de recherche.

- Forcer une recherche sécurisée stricte (pris en charge pour les moteurs de recherche Yahoo et Bing uniquement) — Le pare-feu applique automatiquement et en toute transparence les paramètres de recherche les plus stricts. Plus précisément, le pare-feu redirige les requêtes de recherche vers des URL qui renvoient des résultats de recherche strictement filtrés et modifie la préférence de recherche sécurisée pour le moteur de recherche utilisé. Pour activer cette fonctionnalité, remplacez le texte de la page de blocage de recherche sécurisée de filtrage des URL par le texte spécifié dans la procédure. Le texte de remplacement comprend du code JavaScript qui réécrit les URL des requêtes de recherche avec le paramètre de recherche sécurisée strict pour le moteur de recherche utilisé pour la recherche.

  > *Le navigateur n'affiche pas la page de blocage de la recherche sécurisée de filtrage des URL lorsque vous utilisez cette méthode.*

- SafeSearch transparente (Prisma AccessDéploiements uniquement) — Dans les cas où le trafic ne peut pas être décrypté (par exemple, dans un magasin qui fournit un accès Internet invité) et où vous voulez empêcher les utilisateurs avec des périphériques non gérés, y compris des périphériques d'affichage, de rechercher du matériel restreint, inapproprié ou offensant, vous pouvez utiliser SafeSearch transparente dans Prisma Access, qui résout les requêtes des moteurs de recherche des utilisateurs mobiles vers le portail SafeSearch du moteur en effectuant un mappage FQDN-IP.

Commencez avec l'application de recherche sécurisée en examinant les paramètres de recherche sécurisée de chaque moteur de recherche pris en charge. Ensuite, décidez quelle méthode d'application est la meilleure pour votre contexte.

- Réglages de la recherche sécurisée pour les moteurs de recherche
- Bloquer les résultats de recherche lorsque la recherche sécurisée stricte est désactivée
- Forcer une recherche sécurisée stricte
- Utiliser la fonctionnalité SafeSearch transparente dans Prisma Access

Réglages de la recherche sécurisée pour les moteurs de recherche

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :***

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	• *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Les réglages de la recherche sécurisée varient selon les moteurs de recherche—examinez les réglages suivants pour en savoir plus.

Moteur de recherche	Description du paramètre de recherche sécurisée
Google/YouTube	Permet une recherche sécurisée sur un ordinateur ou un réseau via une adresse IP de recherche sécurisée de Google : **Mise en œuvre de la recherche sécurisée pour des recherches Google sur un ordinateur** Dans les Paramètres de recherche Google, le paramètre **Filter explicit results (Filtrer les résultats explicites)** active la fonctionnalité de recherche sécurisée. Lorsqu'elle est activée, le paramètre est enregistré dans un cookie de navigateur sous la forme FF= et est transmis au serveur chaque fois que l'utilisateur effectue une recherche Google. L'ajout de **`safe=active`** à une URL de recherche Google permet également d'activer les paramètres de recherche sécurisée les plus stricts. **Mise en œuvre de la recherche sécurisée pour des recherches Google et YouTube à l'aide d'une adresse IP virtuelle** Google fournit des serveurs qui verrouillent SafeSearch (forcesafesearch.google.com) paramètres dans chaque recherche Google et YouTube. En ajoutant une entrée DNS pour **`www.google.com`** et **`www.youtube.com`** (et d'autres sous-domaines nationaux Google et YouTube) qui contient un enregistrement CNAME pointant sur **`forcesafesearch.google.com`** à la configuration de votre serveur DNS, vous êtes assuré que tous les utilisateurs de votre réseau utilisent des paramètres de recherche sécurisée stricts chaque fois qu'ils effectuent une recherche Google ou YouTube. N'oubliez toutefois pas que cette solution n'est pas compatible avec la mise en œuvre de la recherche sécurisée sur le pare-feu. Par conséquent, si vous utilisez cette option pour forcer la recherche sécurisée

Moteur de recherche	Description du paramètre de recherche sécurisée
	sur Google, la meilleure pratique consiste à bloquer l'accès aux autres moteurs de recherche sur le pare-feu en créant des catégories d'URL personnalisées et en les ajoutant à la liste d'interdiction du profil de filtrage des URL. • *PAN-OS prend en charge l'application de la recherche sécurisée pour YouTube par l'insertion d'en-têtes HTTP. L'insertion d'en-tête HTTP n'est actuellement pas prise en charge pour HTTP/2. Pour effectuer une recherche sécurisée pour YouTube, App-ID et HTTP/2 Inspection rétrogradent les connexions HTTP/2 à HTTP/1.1 à l'aide de la fonctionnalité **Strip ALPN** dans le profil de décryptage approprié.* • *Si vous envisagez d'utiliser la solution Google Lock SafeSearch, pensez à configurer un proxy DNS (**Réseau > Proxy DNS**) et à définir la source d'héritage sur l'interface de Couche 3 sur laquelle le pare-feu reçoit les paramètres DNS du fournisseur de services via DHCP. Vous devez configurer le proxy DNS avec des **Static Entries (Entrées statiques)** pour www.google.com et www.youtube.com, en utilisant l'adresse IP locale du serveur forcesafesearch.google.com.*
Yahoo	Permet une recherche sécurisée sur un ordinateur uniquement. Les Préférences de recherche Yahoo incluent trois paramètres SafeSearch : **Strict**, **Moderate (Modéré)** ou **Off (Désactivé)**. Lorsqu'elle est activée, le paramètre est enregistré dans un cookie de navigateur

Moteur de recherche	Description du paramètre de recherche sécurisée
	sous la forme `vm=` et est transmis au serveur chaque fois que l'utilisateur effectue une recherche Yahoo. L'ajout de `vm=r` à une URL de recherche Yahoo permet également d'activer les paramètres de recherche sécurisée les plus stricts. *Lorsque vous effectuez une recherche sur Yahoo Japan (**`yahoo.co.jp`**) alors que vous êtes connecté à un compte Yahoo, les utilisateurs finaux doivent également activer l'option **Lock (Verrouiller) SafeSearch**.*
Bing	Permet une recherche sécurisée sur des ordinateurs individuels. Les Paramètres Bing incluent trois paramètres SafeSearch : **Strict**, **Moderate (Modéré)** ou **Off (Désactivé)**. Lorsqu'elle est activée, le paramètre est enregistré dans un cookie de navigateur sous la forme `adlt=` et est transmis au serveur chaque fois que l'utilisateur effectue une recherche Bing. L'ajout de **`adlt=strict`** à une URL de recherche Bing permet également d'activer les paramètres de recherche sécurisée les plus stricts. Le moteur de recherche SSL Bing n'applique pas les paramètres d'URL de recherche sécurisée et vous devez donc prendre en compte le blocage de Bing sur SSL pour une mise en œuvre complète de la recherche sécurisée.

Bloquer les résultats de recherche lorsque la recherche sécurisée stricte est désactivée

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Si vous activez Mise en œuvre de la recherche sécurisée, le comportement par défaut du pare-feu est de bloquer les résultats de recherche des utilisateurs finaux effectuant des recherches sur les moteurs de recherche Bing, Yahoo, Yandex ou Youtube jusqu'à ce qu'ils définissent leur paramètre de recherche sécurisée sur l'option disponible la plus stricte. Par défaut, la page de blocage de recherche sécurisée de filtrage des URL s'affiche dans leur navigateur. La page de blocage prédéfinie fournit un lien vers les paramètres de recherche du moteur de recherche utilisé, afin que les utilisateurs puissent ajuster le paramètre de recherche sécurisée. Vous pouvez personnaliser la page de blocage de recherche sécurisée pour répondre aux besoins spécifiques de votre organisation.

Si vous envisagez d'utiliser cette méthode de mise en œuvre de la recherche sécurisée par défaut, vous devez transmettre la politique aux utilisateurs finaux avant de l'appliquer. Si vous préférez rediriger automatiquement les URL des requêtes de recherche des utilisateurs finaux vers des versions de recherche sécurisée strictes, activez la recherche sécurisée stricte.

Palo Alto Networks ne peut plus détecter si Google SafeSearch est activé en raison de changements dans l'implémentation de Google. Par conséquent, le pare-feu ne peut pas imposer une recherche sécurisée en utilisant cette méthode. Vous pouvez toujours imposer la recherche sécurisée en toute transparence. Cependant, nous ne pouvons garantir que Google filtrera les images et contenus explicites.

- Strata Cloud Manager
- PAN-OS et Panorama

Bloquer les résultats de recherche lorsque la recherche sécurisée stricte est désactivée (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Activez la mise en œuvre de la recherche sécurisée dans un profil de gestion des accès à l'URL.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès à l'URL**.
2. Sous Profils de gestion des accès à l'URL, sélectionnez un profil existant ou **Ajoutez un profil** pour en créer un nouveau. Les options de configuration apparaissent.
3. Sous **Paramètres**, sélectionnez **Mise en œuvre de la recherche sécurisée**.
4. **Enregistrez** le profil.

STEP 2 | (Facultatif) Limiter les moteurs de recherche auxquels les utilisateurs finaux peuvent accéder.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès à l'URL**.
2. Sous **Contrôle d'accès**, **Recherche** ( ) pour la catégorie **moteurs de recherche**.
3. Définissez l'accès au site pour la catégorie **moteurs de recherche** sur **bloquer**.

   Dans une étape suivante 4, vous allez créer une catégorie d'URL personnalisée (type de liste d'URL) avec les moteurs de recherche que vous souhaitez autoriser.
4. **Enregistrez** le profil.

STEP 3 | Appliquer le profil de gestion des accès à l'URL aux règles de politique de sécurité qui autorisent le trafic des clients de la zone de confiance vers Internet.

Pour activer un profil de gestion des accès à l'URL (et tout profil de sécurité), ajoutez-le au `groupe de profils` et référencez-le dans une règle de politique de sécurité.

STEP 4 | Créez une catégorie d'URL personnalisée pour les moteurs de recherche pris en charge.

À l'étape suivante, vous allez configurer le pare-feu pour décrypter le trafic vers cette catégorie personnalisée.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès à l'URL**.
2. Sous **Contrôle d'accès**, pour les catégories d'URL personnalisée, **Ajoutez une catégorie**.
3. Saisissez un **Nom** pour la catégorie, par exemple **`SearchEngineDecryption`**.
4. Pour **Type** de catégorie d'URL personnalisée, sélectionnez **Liste d'URL**.
5. Sous **Éléments**, **Ajoutez** les entrées suivantes à la liste d'URL :
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. **Enregistrez** la catégorie personnalisée.
7. Configurez Accès au site pour la nouvelle catégorie d'URL personnalisée.
   1. Sous Profils de gestion des accès à l'URL, sélectionnez le profil que vous avez configuré précédemment.
   2. Sous Contrôle d'accès, sélectionnez la nouvelle catégorie d'URL personnalisée. Il apparaît dans la section Catégories d'URL personnalisée au-dessus des listes d'URL dynamiques externes et des catégories prédéfinies.
   3. Définissez **Accès au site** sur **autoriser**.
   4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 5 | Configurez le décryptage du proxy de transfert SSL.

Étant donné que la plupart des moteurs de recherche cryptent leurs résultats de recherche, vous devez activer le Décryptage du proxy de transfert SSL afin que le pare-feu puisse inspecter le trafic et détecter les paramètres de recherche sécurisée.

Sous la section **Services et URL** de la règle de politique de décryptage, cliquez sur **Ajouter des catégories d'URL**. Ensuite, sélectionnez la catégorie d'URL personnalisée que vous avez créée précédemment. De nouvelles catégories personnalisées trônent en tête de liste.

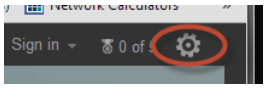
Enregistrez la règle de politique de décryptage.

STEP 6 | Sélectionnez **Transmettre la configuration** pour activer vos modifications.

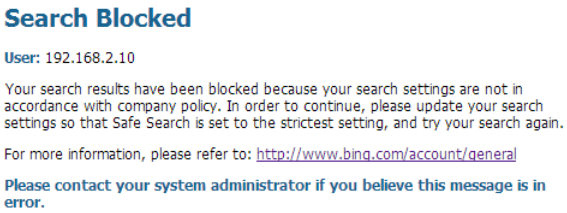
STEP 7 | Vérifiez la configuration de la mise en œuvre de la recherche sécurisée.

Cette étape de vérification ne fonctionne que si vous utilisez des pages bloquées pour appliquer la recherche sécurisée. Il existe une autre étape de vérification si vous activez la recherche sécurisée de manière transparente.

1. À partir d'un ordinateur situé derrière le pare-feu, désactivez les paramètres de recherche stricts d'un moteur de recherche pris en charge. Par exemple, sur bing.com, cliquez sur l'icône **Preferences (Préférences)** dans la barre de menus Bing.



2. Définissez l'option **SafeSearch** sur **Modérée** ou sur **Désactivée**, puis cliquez sur **Enregistrer**.
3. Effectuez une recherche Bing (ou une recherche à l'aide d'un autre fournisseur) pour voir si la page de blocage de recherche sécurisée de gestion des accès à l'URL s'affiche à la place des résultats de recherche :



4. Utilisez le lien sur la page de blocage pour mettre à jour le paramètre de recherche sécurisée sur le paramètre le plus strict (**Strict** dans le cas de Bing), puis cliquez sur **Enregistrer**.
5. Effectuez une nouvelle recherche dans Bing et vérifiez que les résultats de la recherche filtrés s'affichent à la place de la page de blocage.

Bloquer les résultats de recherche lorsque la recherche sécurisée stricte est désactivée (PAN-OS et Panorama)

STEP 1 | Activez mise en œuvre de la recherche sécurisée dans un profil de filtrage des URL.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (URL Filtering)**.
2. Sélectionnez un profil existant pour le modifier ou clonez le profil par défaut pour en créer un nouveau.
3. Sur l'onglet **Paramètres de filtrage des URL**, sélectionnez **Mise en œuvre de la recherche sécurisée**.

STEP 2 | (Facultatif) Limitez les moteurs de recherche auxquels les utilisateurs finaux peuvent accéder dans le même profil de filtrage des URL.

1. Dans l'onglet **Catégories**, **Recherchez** ( ) la catégorie **Moteurs de recherche**.
2. Définissez l'accès au site pour la catégorie **Moteurs de recherche** sur **bloquer**.

   Dans une étape suivante 4, vous allez créer une catégorie d'URL personnalisée (type de liste d'URL) avec les moteurs de recherche que vous souhaitez autoriser.
3. Cliquez sur **OK** pour enregistrer le profil.

STEP 3 | Appliquez le profil de filtrage des URL aux règles de politique de sécurité qui autorisent le trafic des clients de la zone de confiance vers Internet.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**. Cliquez ensuite sur la règle à laquelle vous souhaitez appliquer le profil de filtrage des URL.
2. Sur l'onglet **Actions**, recherchez Paramètres du profil. Pour **Type de profil**, sélectionnez **Profils**. Une liste de profils s'affiche.
3. Pour le profil **Filtrage des URL**, sélectionnez le profil que vous avez créé précédemment.
4. Cliquez sur **OK (OK)** pour enregistrer la Règle de politique de sécurité.

STEP 4 | Créez une catégorie d'URL personnalisée pour les moteurs de recherche pris en charge.

À l'étape suivante, vous allez spécifier que vous souhaitez déchiffrer le trafic vers les sites de la catégorie personnalisée.

1. Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)** et cliquez sur **Add (Ajouter)** pour ajouter une catégorie personnalisée.
2. Saisissez un **Nom** pour la catégorie, par exemple **`SearchEngineDecryption`**.
3. **Ajoutez** les entrées suivantes à la liste**Sites** :
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
4. Cliquez sur **OK** pour enregistrer la catégorie personnalisée.
5. Configurez Accès au site pour la nouvelle catégorie d'URL personnalisée.
   1. Allez à **Objets** > **Profils de sécurité** > **Filtrage des URL** et sélectionnez le profil de filtrage des URL que vous avez configuré précédemment.
   2. Sur l'onglet **Catégorie**, sélectionnez la nouvelle catégorie d'URL personnalisée. Elle apparaît dans la section Catégories d'URL personnalisées, au-dessus des listes des URL dynamiques externes et des catégories prédéfinies.
   3. Définissez **Accès au site** sur **autoriser**.
   4. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 5 | Configurez le décryptage du proxy de transfert SSL.

Étant donné que la plupart des moteurs de recherche cryptent leurs résultats de recherche, vous devez activer le Décryptage du proxy de transfert SSL afin que le pare-feu puisse inspecter le trafic et détecter les paramètres de recherche sécurisée.

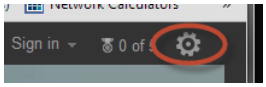
Sur l'onglet **Catégorie de service/d'URL** de la règle de politique de décryptage, **Ajoutez** la catégorie d'URL personnalisée que vous avez créée précédemment. Cliquez ensuite sur **OK**.

STEP 6 | **Commit (Validez)** vos modifications.

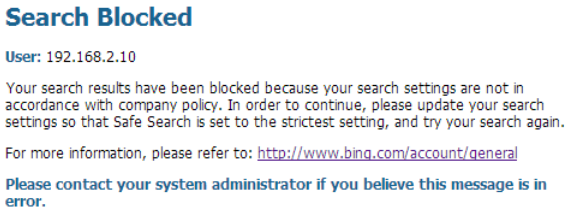
STEP 7 | Vérifiez la configuration de la mise en œuvre de la recherche sécurisée.

Cette étape de vérification ne fonctionne que si vous utilisez des pages bloquées pour appliquer la recherche sécurisée. Il existe une autre étape de vérification si vous activez la recherche sécurisée de manière transparente.

1. À partir d'un ordinateur situé derrière le pare-feu, désactivez les paramètres de recherche stricts d'un moteur de recherche pris en charge. Par exemple, sur bing.com, cliquez sur l'icône **Preferences (Préférences)** dans la barre de menus Bing.



2. Définissez l'option **SafeSearch** sur **Modérée** ou sur **Désactivée**, puis cliquez sur **Enregistrer**.
3. Effectuez une recherche Bing (ou une recherche à l'aide d'un autre fournisseur) pour voir si la page de blocage de recherche sécurisée de filtrage des URL s'affiche à la place des résultats de recherche :



4. Utilisez le lien sur la page de blocage pour mettre à jour le paramètre de recherche sécurisée sur le paramètre le plus strict (**Strict** dans le cas de Bing), puis cliquez sur **Enregistrer**.
5. Effectuez une nouvelle recherche dans Bing et vérifiez que les résultats de la recherche filtrés s'affichent à la place de la page de blocage.

Forcer une recherche sécurisée stricte

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :***

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	• *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Vous pouvez fournir une expérience de recherche sécurisée et transparente pour les utilisateurs finaux Bing et Yahoo en activant de manière transparente la recherche sécurisée stricte. Au lieu de bloquer les résultats de la recherche lorsque les utilisateurs finaux effectuent une recherche sans avoir activé la recherche sécurisée stricte, le pare-feu active automatiquement la recherche sécurisée stricte et ne renvoie que les résultats de recherche strictement filtrés. Les écoles et les bibliothèques, par exemple, peuvent bénéficier d'une mise en œuvre automatique qui assure une expérience d'apprentissage uniforme.

Pour activer la mise en œuvre transparente de la recherche sécurisée, vous devrez activer la mise en œuvre de la recherche sécurisée dans un profil de filtrage des URL et remplacer le texte dans le fichier de page de blocage de la recherche sécurisée de filtrage des URL par du texte fourni dans la procédure suivante. Le texte de remplacement contient JavaScript qui ajoute des URL de requête de recherche avec des paramètres de recherche sécurisée stricte pour le moteur de recherche utilisé pour la recherche.

La page de blocage de recherche sécurisée de filtrage des URL ne s'affiche pas dans le navigateur.

Après avoir terminé ces étapes, le pare-feu exécute JavaScript chaque fois qu'un utilisateur final effectue une recherche. Par exemple, supposons que la préférence Bing SafeSearch d'un étudiant soit définie sur `Désactivée` lorsqu'il effectue des recherches sur un concept susceptible de donner des résultats inappropriés. Détectant la préférence de recherche sécurisée, le pare-feu ajoute `&adlt=strict` à l'URL de la requête de recherche. Le moteur de recherche affiche alors les résultats appropriés et la préférence SafeSearch passe sur `Strict`.

- Strata Cloud Manager
- PAN-OS et Panorama

Forcer une recherche sécurisée stricte (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS et Panorama** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Activez la mise en œuvre de la recherche sécurisée dans un profil de gestion des accès à l'URL.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès à l'URL**.
2. Sous Profils de gestion des accès à l'URL, sélectionnez un profil existant ou **Ajoutez un profil** pour en créer un nouveau. Les options de configuration apparaissent.
3. Sous **Paramètres**, sélectionnez **Mise en œuvre de la recherche sécurisée**.

4. **Enregistrez** le profil.

STEP 2 | (Facultatif) Limiter les moteurs de recherche auxquels les utilisateurs finaux peuvent accéder.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès à l'URL**.
2. Sous **Contrôle d'accès**, **Recherche** ( ) pour la catégorie **moteurs de recherche**.
3. Définissez l'accès au site pour la catégorie **moteurs de recherche** sur **bloquer**.

   Dans une étape suivante 6, vous allez créer une catégorie d'URL personnalisée (type de liste d'URL) avec les moteurs de recherche que vous souhaitez autoriser.
4. **Enregistrez** le profil.

STEP 3 | Appliquer le profil de gestion des accès à l'URL aux règles de politique de sécurité qui autorisent le trafic des clients de la zone de confiance vers Internet.

Pour activer un profil de gestion des accès à l'URL (et tout profil de sécurité), ajoutez-le au `groupe de profils` et référencez-le dans une règle de politique de sécurité.

STEP 4 | Modifiez la page de blocage de recherche sécurisée Gestion d'accès à l'URL, en remplaçant le code existant par JavaScript pour réécrire les URL des requêtes de recherche.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion de l'accès à l'URL** > **Pages de réponse**.
2. **Exporter un modèle HTML** pour la page de blocage de Gestion de l'accès à l'URL.
3. Utilisez un éditeur HTML et remplacez l'ensemble du texte de la page de blocage existant par le texte ci-dessous. Ensuite, enregistrez le fichier.

```
<html> <head> <title>Recherche bloquée</title> <meta http-
equiv="pragma" content="no-cache"> <style> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta name="viewport" content="initial-scale=1.0"> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-
serif; font-size:1em; } h1 { font-size:1.3em; font-
weight:bold; color:#196390; } b { font-weight:normal;
 color:#196390; } </style> </head> <body bgcolor="#e7e8e9">
 <div id="content"> <h1>Rechercher un utilisateur </h1>
 <p> <b>bloqué :</b> <user/> </p> <p>Vos résultats de
 recherche ont été bloqués car vos paramètres de recherche
 ne sont pas conformes à la politique de l'entreprise.
 Pour continuer, veuillez mettre à jour vos paramètres de
 recherche afin que la recherche sécurisée soit définie
 sur le paramètre le plus strict. Si vous êtes actuellement
 connecté à votre compte, veuillez également verrouiller
 safe Search et réessayer votre recherche.</p> <p> Pour plus
 d'informations, veuillez vous référer à: <a href="<ssurl/
>« ></p>  <ssurl/> </a> <p id="java_off"> Veuillez activer
 JavaScript dans votre navigateur.<br></p> <p><b>Veuillez
 contacter votre administrateur système si vous pensez que
 ce message est erroné.</b></p> </div> </body> <script>
 Saisissez l'URL qui se trouve dans le navigateur. var s_u
 = location.href; bing // Correspond aux barres obliques
 au début, n'importe quoi, puis « .bing. » puis tout
```



```
 ce qui est suivi d'une barre oblique non gourmande.
 Espérons que ce soit la première barre oblique. var b_a
 = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u); if (b_a) { s_u
 = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML = 'Vous
 êtes redirigé vers une recherche plus sécurisée!'; } //
yahoo // Correspond aux barres obliques du début, n'importe
 quoi, ensuite ".yahoo."" ensuite n'importe quoi suivi
 d'une barre oblique non gourmande. Par chance la première
 barre oblique. var y_a = /^.*\/\/(.+\.yahoo\.. +?)
 \//.exec(s_u); if (y_a) { s_u = s_u.replace(/&vm=p/ig," »);
 s_u = s_u + « &vm=r »; window.location.replace(s_u);
 document.getElementById(« java_off »).innerHTML =
 'Vous êtes redirigé vers une recherche plus sûre!'; }
 document.getElementById(« java_off »).innerHTML = ' '; </
script> </html>
```

STEP 5 | Importez la page modifiée de blocage de la recherche sécurisée de Gestion de l'accès à l'URL sur le pare-feu.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion de l'accès à l'URL** > **Pages de réponse**.
2. Cliquez sur la page de blocage de recherche sécurisée de Gestion de l'accès à l'URL. Une boîte de dialogue apparaît avec une option **Choisir un fichier**.
3. Sélectionnez le fichier de la page de blocage de recherche sécurisée que vous avez modifié précédemment et cliquez sur **Enregistrer**.

STEP 6 | Créer une catégorie d'URL personnalisée pour les moteurs de recherche pris en charge.

À l'étape suivante, vous allez configurer le pare-feu pour décrypter le trafic vers cette catégorie personnalisée.

1. Sélectionnez **Gérer** > **Configuration** > **Services de sécurité** > **Gestion des accès à l'URL**.
2. Sous **Contrôle d'accès**, pour les catégories d'URL personnalisée, **Ajoutez une catégorie**.
3. Saisissez un **Nom** pour la catégorie, par exemple **`SearchEngineDecryption`**.
4. Pour **Type** de catégorie d'URL personnalisée, sélectionnez **Liste d'URL**.
5. Sous **Éléments**, **Ajoutez** les entrées suivantes à la liste d'URL :
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. **Enregistrez** la catégorie personnalisée.
7. Configurez Accès au site pour la nouvelle catégorie d'URL personnalisée.
   1. Sous Profils de gestion des accès à l'URL, sélectionnez le profil que vous avez configuré précédemment.
   2. Sous Contrôle d'accès, sélectionnez la nouvelle catégorie d'URL personnalisée. Il apparaît dans la section Catégories d'URL personnalisée au-dessus des listes d'URL dynamiques externes et des catégories prédéfinies.
   3. Définissez **Accès au site** sur **autoriser**.
   4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 7 | Configurez le décryptage du proxy de transfert SSL.

Étant donné que la plupart des moteurs de recherche cryptent leurs résultats de recherche, vous devez activer le Décryptage du proxy de transfert SSL afin que le pare-feu puisse inspecter le trafic et détecter les paramètres de recherche sécurisée.

Sous la section **Services et URL** de la règle de politique de décryptage, cliquez sur **Ajouter des catégories d'URL**. Ensuite, sélectionnez la catégorie d'URL personnalisée que vous avez créée précédemment. De nouvelles catégories personnalisées trônent en tête de liste.

Enregistrez la règle de politique de décryptage.

STEP 8 | Sélectionnez **Transmettre la configuration** pour activer vos modifications.

STEP 9 | Vérifiez la configuration de la mise en œuvre de la recherche sécurisée.

À partir d'un ordinateur derrière un pare-feu, ouvrez un navigateur et effectuez une recherche à l'aide de Bing, Yahoo ou Yandex. Ensuite, utilisez l'une des méthodes suivantes pour vérifier votre configuration :

- Examinez la chaîne de requête de l'URL pour les paramètres de recherche sécurisée. Paramètres de recherche sécurisée pour les moteurs de recherche répertorie le paramètre de recherche sécurisée ajouté à chaque URL de requête de recherche.
- Accédez aux paramètres de recherche sécurisés pour un moteur de recherche pris en charge et vérifiez que la préférence SafeSearch sélectionnée est le niveau le plus strict (**Strict** dans la plupart des cas).

Forcer une recherche sécurisée stricte (PAN-OS & Panorama)

STEP 1 | Vérifiez que le pare-feu exécute la version de contenu 475 ou ultérieure.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Consultez la section **Applications and Threats (Applications et menaces)** pour connaître la mise à jour actuelle.
3. Si le pare-feu n'exécute pas la mise à jour requise ou une mise à jour ultérieure, cliquez sur **Check Now (Vérifier maintenant)** pour récupérer la liste des mises à jour disponibles.
4. Localisez la mise à jour requise, puis cliquez sur **Download (Télécharger)**.
5. Une fois le téléchargement terminé, cliquez sur **Install (Installer)**.

STEP 2 | Activez mise en œuvre de la recherche sécurisée dans un profil de filtrage des URL.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (URL Filtering)**.
2. Sélectionnez un profil existant pour le modifier ou clonez le profil par défaut pour en créer un nouveau.
3. Sur l'onglet **Paramètres de filtrage des URL**, sélectionnez **Mise en œuvre de la recherche sécurisée**.

STEP 3 | (Facultatif) Limitez les moteurs de recherche auxquels les utilisateurs finaux peuvent accéder dans le même profil de filtrage des URL.

1. Dans l'onglet **Catégories**, **Recherchez** ( ) la catégorie **moteurs de recherche**.
2. Définissez l'accès au site pour la catégorie **Moteurs de recherche** sur **bloquer**.

   Dans une étape suivante 7, vous allez créer une catégorie d'URL personnalisée (type de liste d'URL) avec les moteurs de recherche que vous souhaitez autoriser.
3. Cliquez sur **OK** pour enregistrer le profil.

STEP 4 | Appliquez le profil de filtrage des URL aux règles de politique de sécurité qui autorisent le trafic des clients de la zone de confiance vers Internet.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**. Cliquez ensuite sur la règle à laquelle vous souhaitez appliquer le profil de filtrage des URL.
2. Sur l'onglet **Actions**, recherchez Paramètres du profil. Pour **Type de profil**, sélectionnez **Profils**. Une liste de profils apparaît.
3. Pour le profil de **Filtrage des URL**, sélectionnez le profil que vous avez créé précédemment.
4. Cliquez sur **OK (OK)** pour enregistrer la Règle de politique de sécurité.

STEP 5 | Modifiez la page de blocage de recherche sécurisée de filtrage des URL, en remplaçant le code existant par JavaScript pour réécrire les URL de requête de recherche.

1. Sélectionnez **Device (Équipement)** > **Response Pages (Pages de réponse)** > **URL Filtering Safe Search Block Page (Page de blocage de la recherche sécurisée du URL Filtering)**.
2. Sélectionnez **Predefined (Prédéfinie)**, puis cliquez sur **Export (Exporter)** pour enregistrer le fichier localement.
3. Utilisez un éditeur HTML et remplacez tout le texte de la page de blocage existante par le texte suivant. Ensuite, enregistrez le fichier.

```
<html> <head> <title>Recherche bloquée</title> <meta http-
equiv="pragma" content="no-cache"> <style> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta name="viewport" content="initial-scale=1.0"> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-
serif; font-size:1em; } h1 { font-size:1.3em; font-
weight:bold; color:#196390; } b { font-weight:normal;
 color:#196390; } </style> </head> <body bgcolor="#e7e8e9">
 <div id="content"> <h1>Rechercher un utilisateur </h1>
 <p> <b>bloqué :</b> <user/> </p> <p>Vos résultats de
 recherche ont été bloqués car vos paramètres de recherche
 ne sont pas conformes à la politique de l'entreprise.
 Pour continuer, veuillez mettre à jour vos paramètres de
 recherche afin que la recherche sécurisée soit définie
 sur le paramètre le plus strict. Si vous êtes actuellement
 connecté à votre compte, veuillez également verrouiller
 safe Search et réessayer votre recherche.</p> <p> Pour plus
 d'informations, veuillez vous référer à: <a href="<ssurl/
>« ></p>  <ssurl/> </a> <p id="java_off"> Veuillez activer
 JavaScript dans votre navigateur.<br></p> <p><b>Veuillez
 contacter votre administrateur système si vous pensez que
 ce message est erroné.</b></p> </div> </body> <script>
 Saisissez l'URL qui se trouve dans le navigateur. var s_u
 = location.href; bing // Correspond aux barres obliques
 au début, n'importe quoi, puis « .bing. » puis tout
 ce qui est suivi d'une barre oblique non gourmande.
 Espérons que ce soit la première barre oblique. var b_a
 = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u); if (b_a) { s_u
 = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML = 'Vous
 êtes redirigé vers une recherche plus sécurisée!'; } //
yahoo // Correspond aux barres obliques du début, n'importe
 quoi, ensuite ".yahoo."" ensuite n'importe quoi suivi
 d'une barre oblique non gourmande. Par chance la première
 barre oblique. var y_a = /^.*\/\/(.+\.yahoo\.. +?)
 \//.exec(s_u); if (y_a) { s_u = s_u.replace(/&vm=p/ig," »);
 s_u = s_u + « &vm=r »; window.location.replace(s_u);
 document.getElementById(« java_off »).innerHTML =
 'Vous êtes redirigé vers une recherche plus sûre!'; }
 document.getElementById(« java_off »).innerHTML = ' '; </
script> </html>
```


STEP 6 | Importez la page modifiée de blocage de la recherche sécurisée du filtrage des URL sur le pare-feu.

1. Sélectionnez **Device (Équipement)** > **Response Pages (Pages de réponse)** > **URL Filtering Safe Search Block Page (Page de blocage de la recherche sécurisée du URL Filtering)**.
2. Cliquez sur **Import (Importer)**. Ensuite, **Parcourir** pour le fichier de la page de blocage ou entrez le chemin d'accès et le nom de fichier dans le champ **Importer un fichier**.
3. (Facultatif) Pour **Destination**, sélectionnez soit le système virtuel sur lequel la page de connexion sera utilisée, soit **partagé** pour le rendre disponible à tous les systèmes virtuels.
4. Cliquez sur **OK** pour importer le fichier.

STEP 7 | Créer une catégorie d'URL personnalisée pour les moteurs de recherche pris en charge.

À l'étape suivante, vous allez configurer le pare-feu pour décrypter le trafic vers cette catégorie personnalisée.

1. Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)** et cliquez sur **Add (Ajouter)** pour ajouter une catégorie personnalisée.
2. Saisissez un **Nom** pour la catégorie, par exemple **`SearchEngineDecryption`**.
3. **Ajoutez** les entrées suivantes à la liste **Sites** :
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
4. Cliquez sur **OK** pour enregistrer la catégorie d'URL personnalisée.

STEP 8 | Configurez le décryptage du proxy de transfert SSL.

Étant donné que la plupart des moteurs de recherche cryptent leurs résultats de recherche, vous devez activer le Décryptage du proxy de transfert SSL afin que le pare-feu puisse inspecter le trafic et détecter les paramètres de recherche sécurisée.

Sur l'onglet **Catégorie de service/d'URL** de la règle de politique de décryptage, **Ajoutez** la catégorie d'URL personnalisée que vous avez créée précédemment. Cliquez ensuite sur **OK**.

STEP 9 | **Commit (Validez)** vos modifications.

STEP 10 | Vérifiez la configuration de la mise en œuvre de la recherche sécurisée.

À partir d'un ordinateur derrière un pare-feu, ouvrez un navigateur et effectuez une recherche à l'aide de Bing ou Yahoo. Ensuite, utilisez l'une des méthodes suivantes pour vérifier que votre configuration fonctionne comme prévu :

- Examinez la chaîne de requête de l'URL pour les paramètres de recherche sécurisée. Paramètres de recherche sécurisée pour les moteurs de recherche répertorie le paramètre de recherche sécurisée ajouté à chaque URL de requête de recherche.
- Accédez aux paramètres de recherche sécurisée du moteur de recherche et vérifiez que la préférence SafeSearch sélectionnée est du niveau le plus strict (**Strict** dans le cas de Bing).

Utiliser la fonctionnalité SafeSearch transparente dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si vous souhaitez utiliser cette fonctionnalité dans votre Prisma Access environnement, contactez votre équipe de compte pour en savoir plus.	❑ Un Prisma Access déploiement exécutant une version minimale de 4.1 ❑ Prisma Access licence

Prisma Access vous permet de résoudre les requêtes des moteurs de recherche des utilisateurs mobiles vers le portail SafeSearch du moteur en effectuant un mappage FQDN vers IP. Utilisez la fonctionnalité SafeSearch transparente comme alternative à la mise en œuvre stricte de SafeSearch lorsque le trafic ne peut pas être décrypté (par exemple, dans un magasin qui fournit un accès Internet aux invités) et que vous souhaitez empêcher les utilisateurs disposant de périphériques non gérés, y compris les périphériques d'affichage, de rechercher du contenu limité, inapproprié ou offensant.

- Strata Cloud Manager
- Panorama

Utilisation de la fonctionnalité SafeSearch transparente dans Prisma Access (Strata Cloud Manager)

Pour configurer la prise en charge de la fonctionnalité SafeSearch transparente pour Prisma Access dans Strata Cloud Manager, procédez comme suit. Vous pouvez configurer la fonctionnalité SafeSearch transparente pour les réseaux distants ou les utilisateurs mobiles GlobalProtect.

STEP 1 | Choisissez le type de déploiement (utilisateurs mobiles ou réseaux distants) pour lequel vous souhaitez configurer SafeSearch.

- Pour les déploiements Utilisateurs mobiles—GlobalProtect, allez à **Gérer** > **Configuration du service** > **Utilisateurs mobiles** ; sélectionnez ensuite**Configuration de GlobalProtect** > **Paramètres d'infrastructure**.

  Si vous utilisez Strata Cloud Manager, allez à **Flux de travail** > **Configuration de Prisma Access** > **Utilisateurs mobiles** ; sélectionnez ensuite **Configuration de GlobalProtect** > **Paramètres d'infrastructure**.
- Pour les déploiements Réseau distant, allez à **Gérer** > **Configuration du service** > **Réseaux distants**.

  Si vous utilisez Strata Cloud Manager, allez à **Flux de travail** > **Configuration de Prisma Access** > **Réseaux distants**.

STEP 2 | Sélectionnez **Paramètres avancés**.

STEP 3 | Utilisez **Entrées statiques** pour résoudre les FQDN en adresses IP spécifiques.

STEP 4 | Entrez un **Nom** unique pour la règle de saisie statique, le **FQDN** pour le moteur de recherche, et l'adresse IP SafeSearch du moteur de recherche **Adresse** où la demande FQDN doit être adressée.

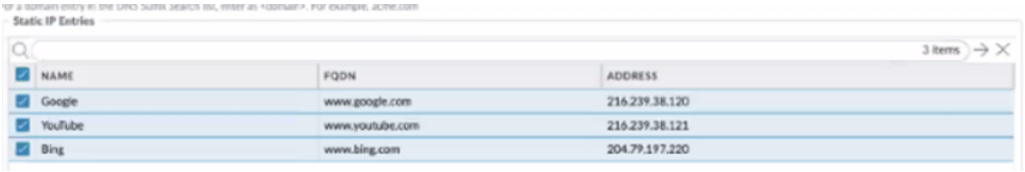
Utilisation de la fonctionnalité SafeSearch transparente dans Prisma Access (Panorama)

Pour configurer la prise en charge de la fonctionnalité SafeSearch transparente pour Prisma Access dans Panorama, procédez comme suit. Vous pouvez configurer la fonctionnalité SafeSearch transparente pour les réseaux distants ou les utilisateurs mobiles GlobalProtect.

STEP 1 | Choisissez le type de déploiement (réseaux distants ou utilisateurs mobiles) pour lequel vous souhaitez configurer SafeSearch.

- Pour les déploiements Utilisateurs mobiles—GlobalProtect, allez à **Panorama** > **Services Cloud** > **Configuration** > **Utilisateurs mobiles—GlobalProtect**, sélectionnez **Configurer** dans la zone **Intégration** et sélectionnez ensuite **Services réseau**.
- Pour les déploiements Réseau distant, allez à **Panorama** > **Services Cloud** > **Configuration** > **Réseaux distants**, cliquez sur l'engrenage pour modifier les **Paramètres** ; puis sélectionnez **Proxy DNS**.

STEP 2 | Saisissez des **Entrées IP statiques** en entrant un**Nom** unique pour la règle de saisie statique, le **FQDN** pour le moteur de recherche et **l'adresse** IP SafeSearch du moteur de recherche où la requête FQDN doit être adressée.



Intégration avec un fournisseur tiers d'isolation de navigateur à distance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence de filtrage des URL avancé ***Note :*** *Prisma Access les licences incluent les capacités Advanced URL Filtering.*

Bien qu'il s'agisse de l'action la plus sécurisée, le blocage de sites inconnus et risqués peut perturber l'expérience et la productivité de vos utilisateurs. L'isolation du navigateur distant (RBI) redirige les utilisateurs de sites inconnus ou à risque vers un environnement isolé hébergé par un fournisseur RBI. Le site Web est rendu pour l'utilisateur et il peut visualiser les ressources dont il a besoin, sans accéder directement au site inconnu ou risqué depuis son terminal.

Prisma Access s'intègre facilement aux fournisseurs RBI pour ce type de redirection du navigateur. En une ou deux étapes, vous pouvez choisir le fournisseur de RBI à intégrer, puis choisir les catégories d'URL que vous souhaitez diriger vers l'environnement hébergé du fournisseur RBI.

En plus des fournisseurs RBI tiers, Isolation de navigateur distant (RBI) de Palo Alto Networks est disponible pour s'intégrer nativement à Prisma Access. Contrairement à d'autres solutions d'isolation, RBI utilise des technologies d'isolation de nouvelle génération pour offrir des expériences quasi natives aux utilisateurs accédant à des sites Web sans compromettre la sécurité.

Voici les fournisseurs RBI auxquels Prisma Access s'intègre – certains fournisseurs peuvent vous demander d'ajouter des détails sur l'environnement RBI (comme une URL de redirection ou un ID de locataire) aux Strata Cloud Manager pour configurer l'intégration :

- **RBI par Palo Alto Networks**

  Pour intégrer au RBI de Palo Alto Networks, vous devrez configurer l'isolation de navigateur distant.

- **Authentic8**

  Pour intégrer à Authentic8, ayez à portée de main l'URL de redirection de l'environnement RBI Authentic8.

- **Proofpoint**

  Pour intégrer à Proofpoint, soyez prêt à choisir d'utiliser l'environnement de production Proofpoint ou PoC pour RBI.

- **Ericom**

  Pour intégrer à Ericom, ayez à portée de main l'ID du locataire de l'environnement Ericom RBI.

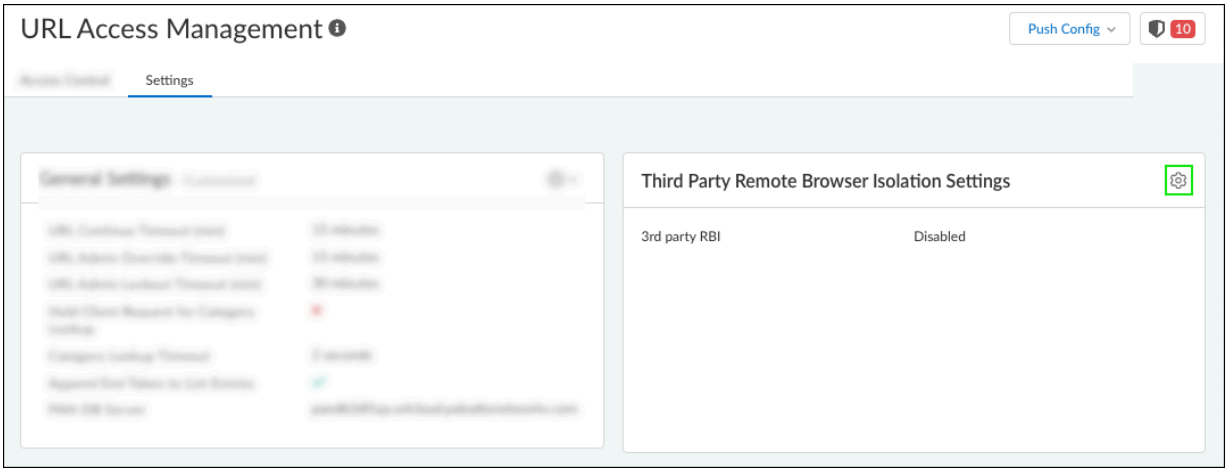
- **Menlo Security**

  Vous n'avez pas besoin de configurer de paramètres pour l'environnement RBI de Menlo Security; il vous suffit d'activer l'intégration.

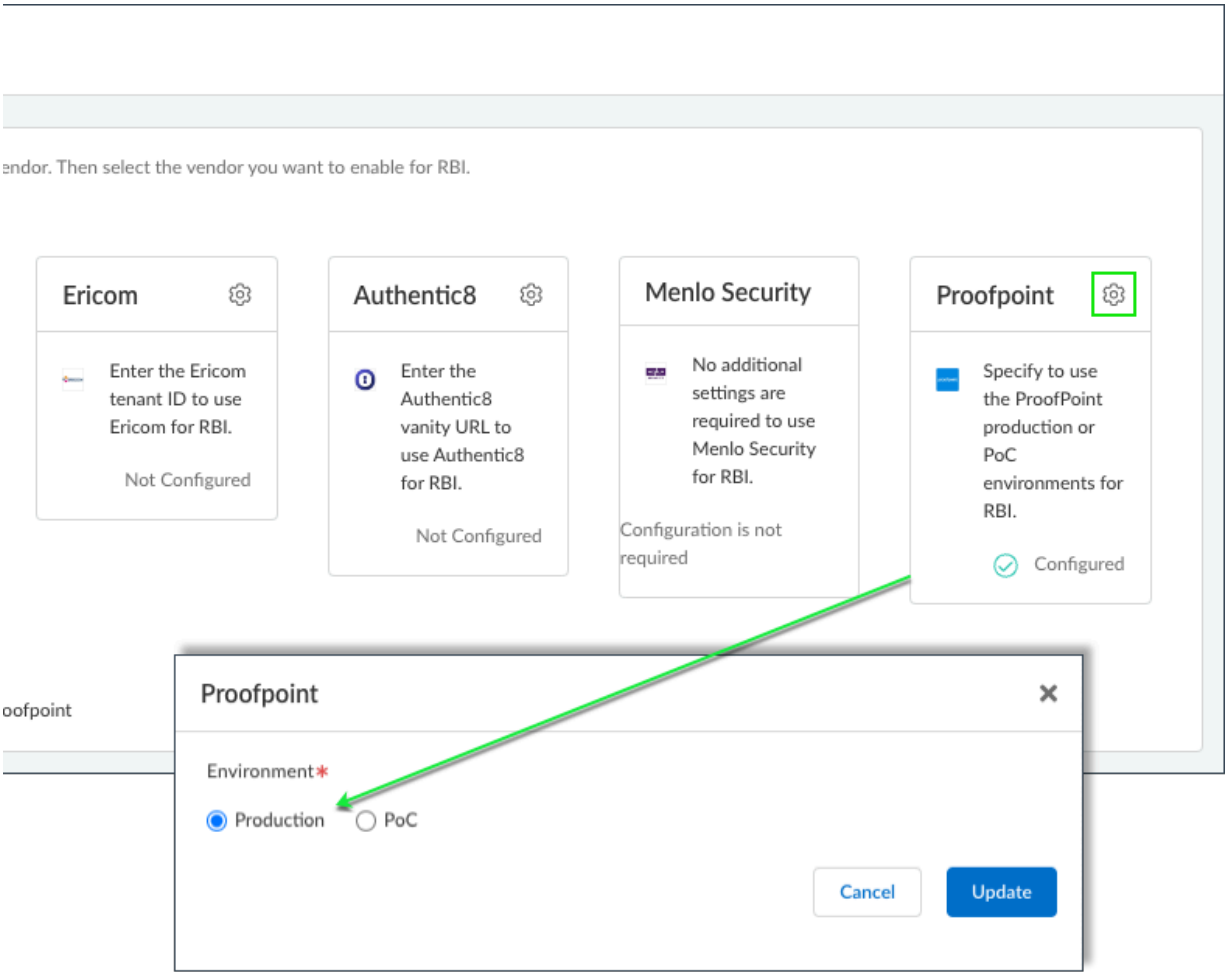
Voici comment ajouter votre fournisseur RBI tiers à Strata Cloud Manager et spécifier les catégories d'URL qui redirigeront les utilisateurs vers l'environnement RBI.

STEP 1 | Configurez l'isolation du navigateur distant (RBI).

- Allez à **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Gestion de l'accès à l'URL** > **Paramètres** et ouvrez les **Paramètres d'isolation du navigateur distant tiers**.
- **SI VOUS ÊTES UN ADMINISTRATEUR DE SÉCURITÉ WEB** : Allez à **Gérer** > **Configuration** > **Sécurité Web** > **Gestiond des menaces** et ouvrez les **Paramètres d'isolation du navigateur distant tiers**.

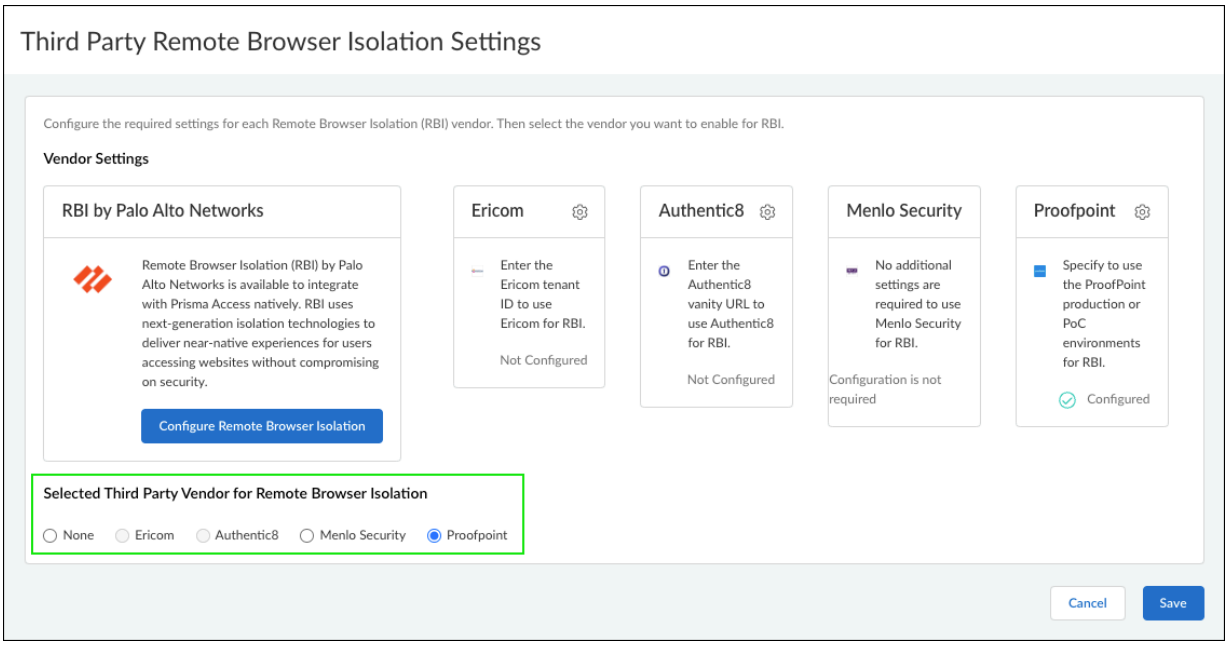


STEP 2 | Vérifiez si votre RBI exige que vous spécifiiez l'environnement RBI que vous souhaitez utiliser; si oui, entrez les paramètres requis.



STEP 3 | Ensuite, choisissez le fournisseur RBI tiers que vous souhaitez activer et **Enregistrez**. Voilà ! Lors de votre prochaine **Transmettre la configuration**, votre fournisseur RBI s'intégrera à Prisma Access.

*Vous pouvez également **configurer l'isolation du navigateur distant** si vous avez déjà acheté et activé la licence pour RBI de Palo Alto Networks. Cependant, vous ne pouvez pas utiliser à la fois RBI de Palo Alto Networks et un fournisseur RBI tiers pour l'isolation. Si vous choisissez d'utiliser RBI de Palo Alto Networks, sélectionnez **Aucun**, sinon, sélectionnez un fournisseur RBI tiers dans **Fournisseur tiers sélectionné pour l'isolation du navigateur distant**.*

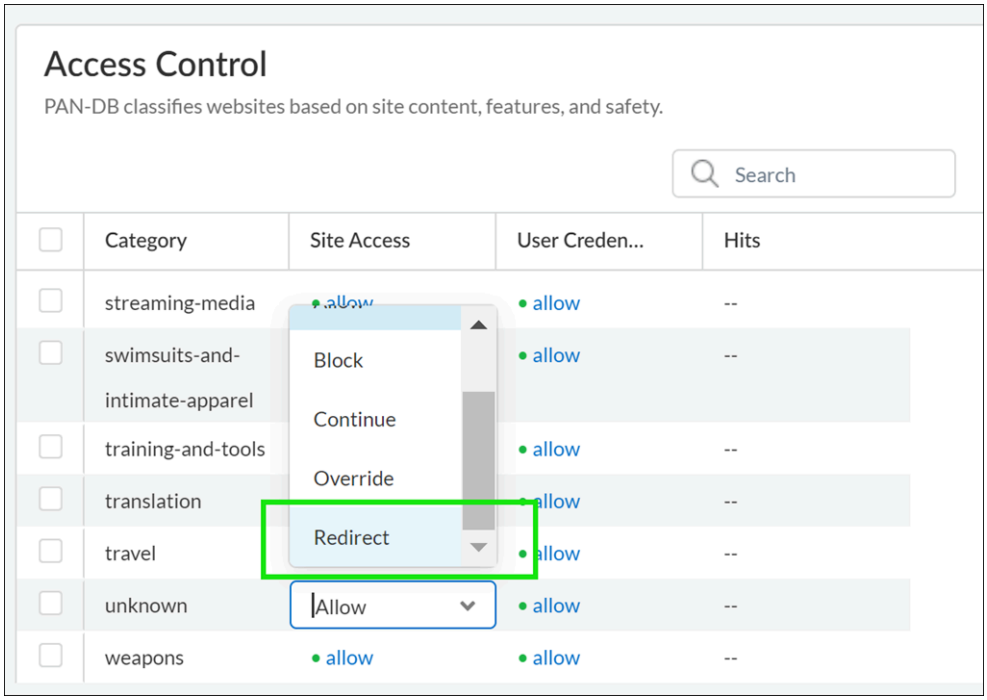


STEP 4 | Maintenant, spécifiez les catégories d'URL qui redirigeront les utilisateurs vers l'environnement RBI.

Allez à **Gestion des accès à l'URL > Contrôle d'accès** et ajoutez ou modifiez un **profil de gestion des accès à l'URL**.

Dans les paramètres **Contrôle d'accès**, mettez à jour **Accès au site** sur **Rediriger**.

La nouvelle action de **Redirection** redirige les utilisateurs vers l'environnement RBI au lieu de leur présenter une page blocage.



Surveillance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

La surveillance de l'activité Web sur votre réseau est essentielle pour protéger votre organisation et garantir l'efficacité de votre politique de filtrage des URL. Les plates-formes Palo Alto Networks génèrent des journaux détaillés, qui servent de source pour les tableaux de bord et les rapports. Vous pouvez personnaliser les journaux, les tableaux de bord et les rapports pour répondre à vos besoins spécifiques en matière de surveillance et de rapports. Si nécessaire, vous pouvez demander des modifications de la catégorie d'URL à partir des journaux de filtrage des URL. Utilisez les informations fournies par nos outils de surveillance pour affiner les règles de politique d'accès Web, analyser et prendre des mesures en cas d'activité suspecte.

Les fonctions de journalisation de l'en-tête HTTP et de page de conteneur de journaux uniquement permettent de contrôler les détails et le volume des journaux. La journalisation de l'en-tête HTTP augmente la granularité des journaux. La journalisation de l'accès des utilisateurs à la page principale uniquement réduit le nombre de journaux générés.

Explorez les rubriques suivantes pour en savoir plus sur les outils et fonctionnalités de surveillance de l'activité Web.

- Surveillance de l'activité sur le Web
- Journalisez uniquement la page visitée par un utilisateur
- Journalisation de l'en-tête HTTP
- Demande de changement de la catégorie d'une URL

Surveillance de l'activité sur le Web

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Vous pouvez consulter divers tableaux de bord, rapports et journaux pour examiner et analyser l'activité Web sur votre réseau. Par exemple, sur les pare-feu PAN-OS de nouvelle génération, le Centre de commande des applications (ACC), les journaux de filtrage des URL et les rapports montrent toute l'activité Web de l'utilisateur pour les catégories d'URL qui sont définies sur **alerte**, **blocage**, **continuer** ou **remplacer**. En surveillant l'activité des utilisateurs avec les outils suivants, vous pouvez mieux comprendre l'activité Web de votre base d'utilisateurs et déterminer les règles de politique d'accès Web appropriées.

Platform (Plateforme)	Façons de voir l'activité Web de l'utilisateur
PAN-OS et Panorama	• Centre de commande de l'application (ACC) • Widgets d'activité réseau • Journaux de filtrage des URL • Rapports de filtrage des URL
Prisma Access	• Journaux • Informations • DEM autonome • Activité

- Strata Cloud Manager
- PAN-OS et Panorama

Surveillance de l'activité sur le Web (Strata Cloud Manager)

Quelle que soit l'interface que vous utilisez pour gérer Prisma Access (Panorama ou Strata Cloud Manager), le volet Activité dans Strata Cloud Manager fournit une vue complète de ce qui se passe sur votre réseau. Différents tableaux de bord composent le volet Activité, qui est disponible

dans le Strata Cloud Manager et l'application Device Insights. Vous pouvez également partager les données d'activité avec d'autres utilisateurs de votre organisation.

Les tableaux de bord interactifs suivants vous aident à surveiller et à analyser l'activité Web sur votre réseau :

- **Informations sur les menaces**- Une vue globale de toutes les menaces que le filtrage des URL avancé et d'autres services de sécurité de Palo Alto Networks ont détectées et bloquées sur votre réseau. Vous pouvez afficher les tendances des menaces, les applications affectées, les utilisateurs et les règles de politique de sécurité qui autorisent ou bloquent les menaces.
- **Visionneuse de journaux** : vos journaux fournissent une piste d'audit pour les événements de système, de configuration et de réseau. Passez d'un tableau de bord d'activité à vos journaux pour obtenir des détails et examiner les résultats.
- **Utilisation de l'application** : affichez une vue d'ensemble des applications de votre réseau, y compris leur risque, l'état des sanctions, la bande passante consommée et les principaux utilisateurs de ces applications.
- **Résumé** (**Filtrage des URL**) : identifiez les catégories d'URL qui génèrent le plus d'activité Web sur votre réseau, les 10 principales URL malveillantes et les 10 URL présentant les risques les plus élevés.
- **Activité de l'utilisateur** : consultez les habitudes de navigation de chaque utilisateur : les sites les plus fréquemment visités, les sites avec lesquels ils transfèrent des données et les tentatives d'accès aux sites à haut risque. Les données de vos journaux de filtrage des URL et du moteur d'identité sur le cloud permettent cette visibilité.
  - *Pour accéder aux données d'activité des utilisateurs et partager des rapports facilement et en toute sécurité, nous vous recommandons* d'activer *et* de configurer le moteur d'identité sur le cloud.

Visibilité supplémentaire et méthodes de surveillance :

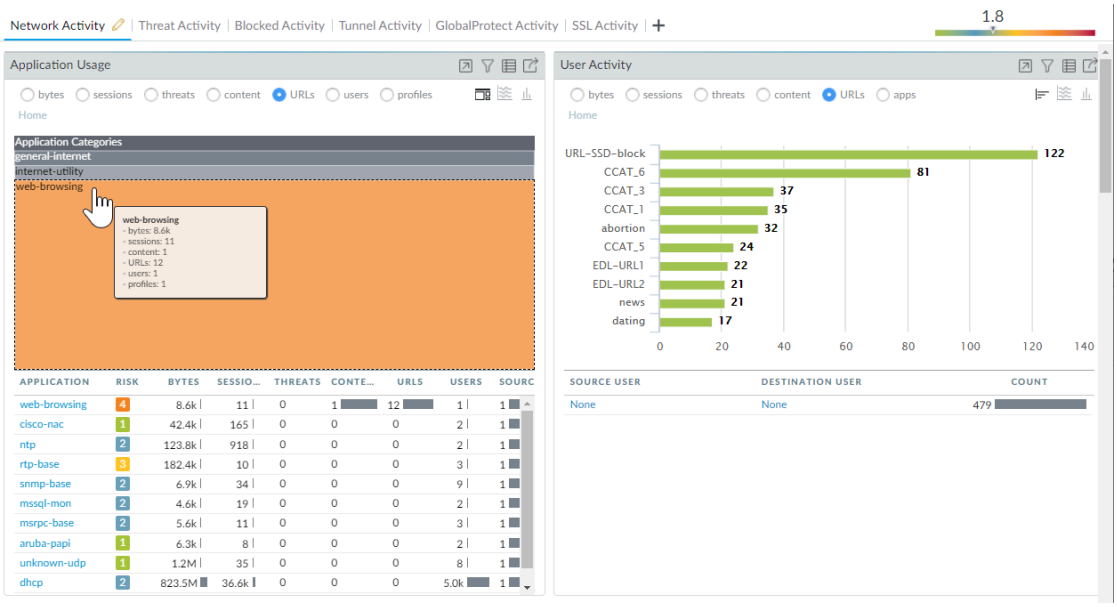
- Le volet Rapports comprend des options permettant de planifier la remise d'un rapport ou de télécharger et de partager un rapport à tout moment pour une consultation hors ligne.
- Vous pouvez également Rechercher un artefact de sécurité (une adresse IP, un domaine, une URL ou un hachage de fichier) qui interagit avec des données uniquement pour cet artefact, tirées à la fois de votre réseau et des résultats des informations sur les menaces mondiales.

1. Ouvrez un tableau de bord d'activité.
   - Sélectionnez **Activité** > **Informations sur les menaces | Utilisation des applications | Activité de l'utilisateur | Résumé**.

     Pour afficher le résumé du filtrage des URL, vous devez cliquer sur l'onglet de filtrage des URL lorsque vous arrivez sur le tableau de bord.
   - Pour accéder à la Visionneuse de journaux, sélectionnez **Activité** > **Journaux** > **Visionneuse de journaux**.
2. Téléchargez, partagez et planifiez des rapports d'activité.

Surveillance de l’activité sur le Web (PAN-OS et Panorama)

- Pour afficher rapidement les catégories les plus couramment consultées par les utilisateurs dans votre environnement, vérifiez les widgets **ACC**. La plupart des widgets de l'onglet **Network Activity (Activité réseau)** vous permettent de trier sur les URL. Par exemple, dans le widget Application Usage (Utilisation de l'application), vous pouvez voir que la catégorie de mise en réseau est la plus consultée, suivie du tunnel crypté et de SSL. Vous pouvez également consulter les listes **Threat Activity** (Activités des menaces) et **Blocked Activity** (Activités bloquées) triées sur les URL.



Afficher les journaux et configurer les options de journal :

- À partir de l'ACC, vous pouvez directement accéder aux journaux ( ) ou sélectionnez **Surveillance** > **Journaux** > **Filtrage des URL**.

  L'action du journal pour chaque entrée dépend du paramètre Site Access (Accès au site) que vous avez défini pour la catégorie correspondante :

  - **Journal d'alerte** : Dans cet exemple, la catégorie computer-and-internet-info (infos sur l'ordinateur et internet) est définie sur alert (alerter).

RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
2020/04/16 14:10:53	computer-and-internet-info	outlook.office36...	pm wifi	UNTRUST	[redacted]	[redacted]	[redacted]	outlook-web-online	alert

  - **Journal bloc** : dans cet exemple, la catégorie contenu-insuffisant est définie pour continuer. Si la catégorie avait été mise à block (bloc), le journal d'action serait à block-url.

RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
2020/04/08 18:47:49	insufficient-content	munchkin.mark...	pm wifi	UNTRUST	[redacted]	[redacted]	[redacted]	ssl	block-continue

  - **Journal d'alerte sur un site Web crypté** : Dans cet exemple, la catégorie est private-ip-addresses (addresses ip privées) et l'application est web-browsing (navigation sur le Web). Ce journal indique également que le pare-feu a décrypté ce trafic.

RECEIVE TIME	CATEGORY	URL	DECRYPTED	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
2020/04/09 14:11:29	private-ip-addresses	[redacted]/Updates/Updat...	yes	TRUST	UNTRUST	192.168.58.3	[redacted]	[redacted]	web-browsing	alert

- Le verdict de ML en ligne [local] (PAN-OS 10.0/10.1) et le verdict de catégorisation en ligne [local et cloud] (PAN-OS 10.2 et versions ultérieures) indiquent le verdict déterminé par les analyseurs basés sur le ML en ligne.

  - Le verdict du ML en ligne s'applique aux URL qui ont été classées à l'aide du ML en ligne du filtrage des URL géré localement sur PAN-OS 10.0/10.1.

RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE ML VERDICT	ACTION	URL
10/11 17:32:10	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
10/11 14:15:14	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
04/30 15:19:30	medium-risk	medium-risk,unknown	malicious-javascript	block	130.127.24.16/0x39814f84/448d21c8e396e8f4e0eb75de69d6473e033422b...

    Les verdicts suivants sont disponibles :

    - **Hameçonnage** : contenu d'une attaque d'hameçonnage détecté par le ML local en ligne.
    - **Malicious-javascript** : contenu JavaScript malveillant détecté par le ML en ligne local.
    - **Inconnu** : l'URL a été classée et le contenu a été jugé inoffensif.

  - Le verdict de la catégorisation en ligne s'applique aux URL qui ont été catégorisées à l'aide du ML en ligne de filtrage des URL exploité localement (qui a été renommé Catégorisation en ligne locale dans PAN-OS 10.2) et de la catégorisation en ligne dans le

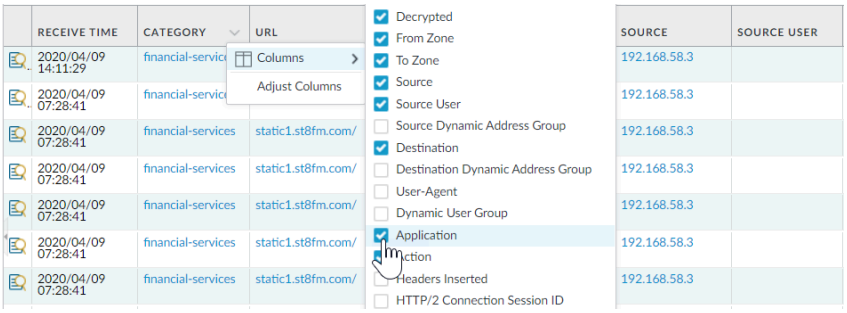
cloud, fonctionnant dans le cloud de filtrage des URL avancé. Le type spécifique d'attaque est spécifié dans la colonne catégorie du journal.

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE CATEGORIZATI... VERDICT	ACTION	URL
	08/16 15:16:58	computer-and-internet-info	computer-and-internet-info,high-risk	N/A	alert	mlav.testpanw.com/js.html
	08/16 15:16:58	phishing	computer-and-internet-info,high-risk	local	block	mlav.testpanw.com/phishing.html
	08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
	08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com:80/test-inline-content-analysis-phishing

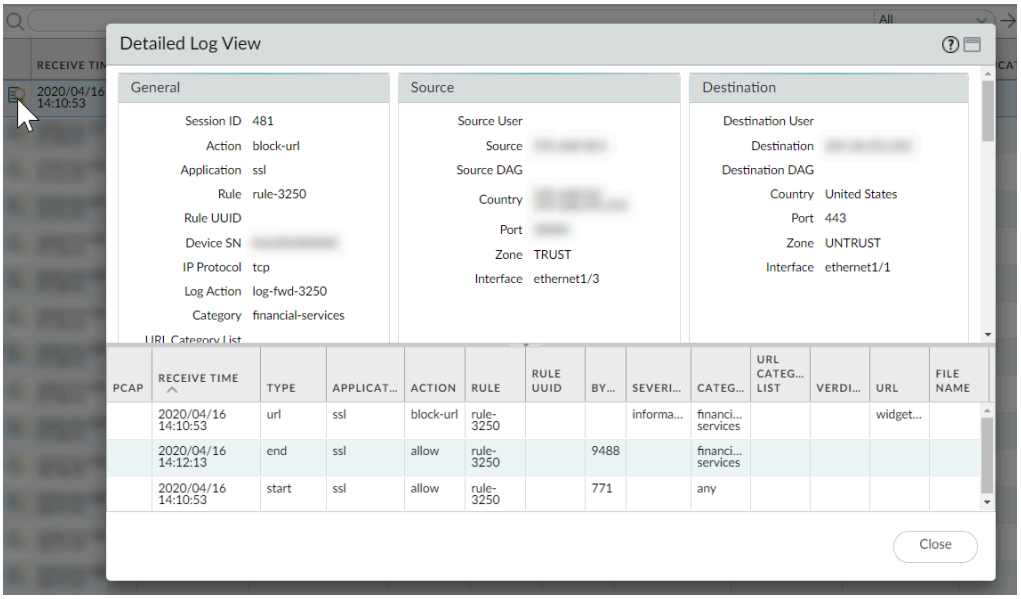
Les verdicts suivants sont disponibles :

- **Local** : contenu malveillant détecté à l'aide de la catégorisation en ligne locale.
- **Cloud** : contenu malveillant détecté à l'aide du moteur de catégorisation en ligne du cloud situé dans le cloud de filtrage des URL avancé.
- **N/A** : l'URL n'a pas été analysée par les moteurs de catégorisation en ligne locaux ou dans le cloud.

- Vous pouvez également ajouter plusieurs autres colonnes à votre vue de journal de URL Filtering, comme : zone À et De, type de contenu et indiquer si des paquets ont été capturés ou non. Pour modifier les colonnes à afficher, cliquez sur la flèche vers le bas d'une colonne et sélectionnez l'attribut à afficher.

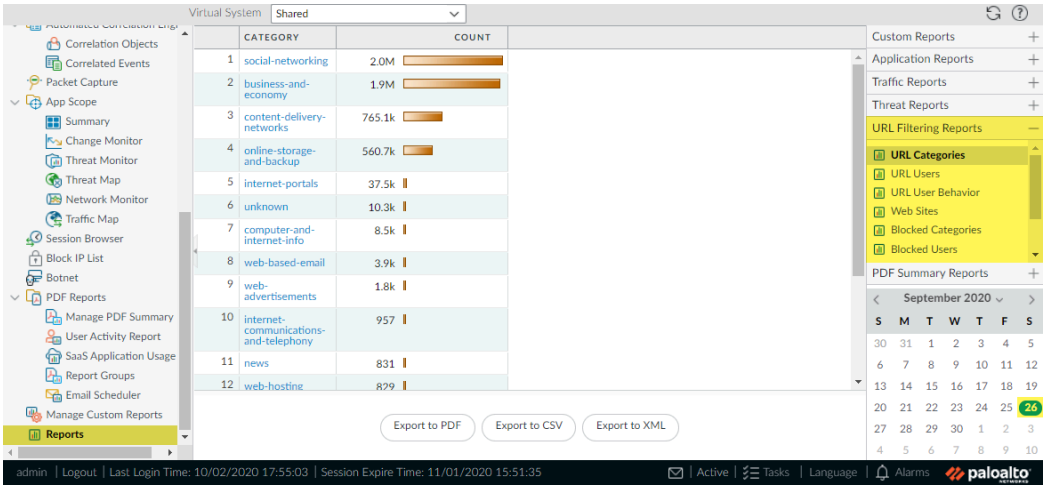


- Pour afficher l'ensemble des détails d'un journal et/ou demander la modification d'une catégorie pour une URL donnée ayant été consultée, cliquez sur l'icône Détails du journal qui se trouve dans la première colonne du journal.



- Générez des rapports de filtrage des URL prédéfinis sur les catégories d'URL, les utilisateurs des URL, les sites Web consultés, les catégories bloquées, etc.

  Sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**et dans la section **URL Filtering Reports (Rapports de filtrage d'URL)**, sélectionnez l'un des rapports. Les rapports couvrent la période de 24 heures de la date que vous sélectionnez dans le calendrier. Vous pouvez également exporter le rapport au format PDF, CSV ou XML.



Affichage du rapport d'activités des utilisateurs

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité)

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Ce rapport permet de consulter rapidement l'activité des utilisateurs ou des groupes, mais aussi d'afficher la durée de navigation.

- Strata Cloud Manager
- PAN-OS et Panorama

Affichage du rapport d'activités des utilisateurs (Strata Cloud Manager)

Que vous utilisiez Panorama ou Strata Cloud Manager pour gérer Prisma Access, vous pouvez accéder à l'application Strata Cloud Manager pour générer un rapport d'activité des utilisateurs. Dans l'application, allez à **Activité** pour trouver le tableau de bord du **Rapport d'activité des utilisateurs**. L'accès aux données d'activité des utilisateurs nécessite un locataire actif de moteur d'identité sur le cloud.

STEP 1 | Activez l'application moteur d'identité sur le cloud.

STEP 2 | Configuration du moteur d'identité sur le cloud.

STEP 3 | Configurez un rapport d'activités des utilisateurs

1. Sélectionnez **Activité** > **Activité de l'utilisateur**.
2. **Entrez le Nom d'utilisateur** pour générer un rapport pour une personne.
3. Sélectionnez le **Type** de rapport :
   - Sélectionnez **User (Utilisateur)** pour générer un rapport pour une personne.
   - Sélectionnez **Group (Groupe)** pour un groupe d'utilisateurs.

   Vous devez enable User-ID (Activer l'User-ID) *pour pouvoir sélectionner des noms d'utilisateurs ou de groupes. Si User-ID n'est pas configuré, vous pouvez sélectionner le type* ***User (Utilisateur)*** *et saisir l'adresse IP de l'ordinateur de l'utilisateur.*
4. Saisissez les valeurs pour **Username/IP Address (Nom d'utilisateur/adresse IP)** pour un rapport d'utilisateur ou le nom de groupe pour un rapport de groupe d'utilisateurs.
5. Sélectionnez la période. Vous pouvez sélectionner une période existante ou **Custom (Personnalisé)**.
6. Cochez la case **Include Detailed Browsing (Inclure la navigation détaillée)** afin d'inclure les informations de navigation dans le rapport.

STEP 4 | Exécutez le rapport.

1. Cliquez sur **Run Now (Exécuter maintenant)**.
2. Lorsque le pare-feu finit de générer le rapport, cliquez sur un des liens pour le télécharger :
   - Cliquez sur **Download User Activity Report (Télécharger le rapport sur l'activité des utilisateurs)** pour télécharger une version PDF du rapport.
   - Cliquez sur **Download URL Logs (Télécharger les journaux d'URL)** pour télécharger un fichier CSV des entrées de journal correspondantes.
3. Après avoir téléchargé le rapport, cliquez sur **Cancel (Annuler)**.
4. Si vous souhaitez enregistrer les paramètres du rapport d'activité des utilisateurs pour pouvoir l'exécuter à nouveau plus tard, cliquez sur **OK (OK)** ; sinon, cliquez sur **Cancel (Annuler)**.

STEP 5 | Consultez le rapport d'activités de l'utilisateur en ouvrant le fichier que vous avez téléchargé. La version PDF du rapport montre l'utilisateur ou groupe sur lequel vous avez basé le rapport, la période du rapport et une table des matières :

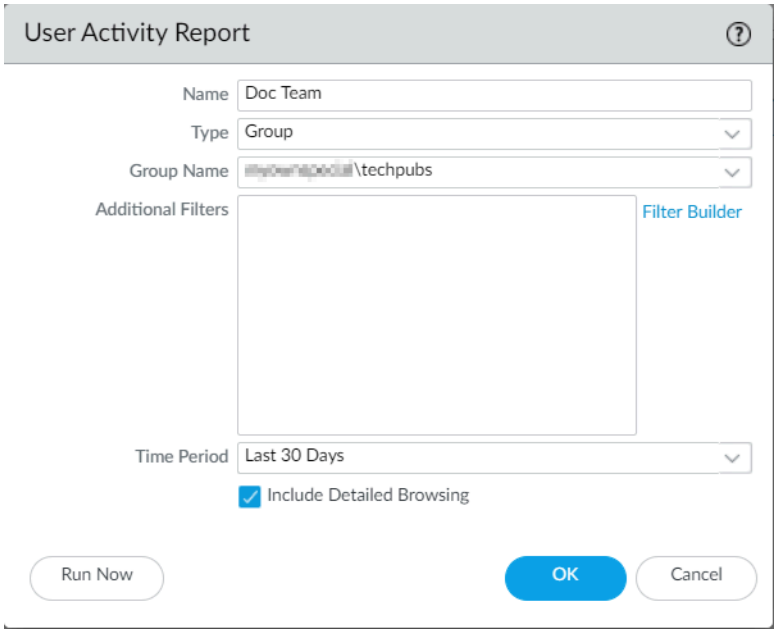
STEP 6 | Cliquez sur un élément de la table des matières pour en afficher les détails du rapport. Par exemple, cliquez sur **Traffic Summary by URL Category (Récapitulatif du trafic par catégorie d'URL)** pour afficher les statistiques de l'utilisateur ou du groupe sélectionné.

Affichage du rapport d'activités des utilisateurs (PAN-OS & Panorama)

STEP 1 | Configurez un rapport d'activités des utilisateurs

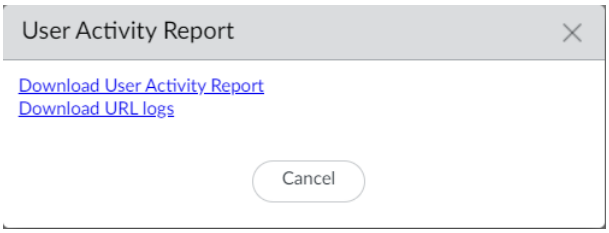
1. Sélectionnez **Monitor (Surveillance)** > **PDF Reports (Rapports PDF)** > **User Activity Report (Rapport d'activité de l'utilisateur)**.
2. **Add (Ajoutez)** un rapport et donnez-lui un **Name (Nom)**.
3. Sélectionnez le **Type** de rapport :
   - Sélectionnez **User (Utilisateur)** pour générer un rapport pour une personne.
   - Sélectionnez **Group (Groupe)** pour un groupe d'utilisateurs.

   *Vous devez activer l'User-ID pour pouvoir sélectionner des noms d'utilisateur ou de groupe. Si User-ID n'est pas configuré, vous pouvez sélectionner le type **User (Utilisateur)** et saisir l'adresse IP de l'ordinateur de l'utilisateur.*
4. Saisissez les valeurs pour **Username/IP Address (Nom d'utilisateur/adresse IP)** pour un rapport d'utilisateur ou le nom de groupe pour un rapport de groupe d'utilisateurs.
5. Sélectionnez la période. Vous pouvez sélectionner une période existante ou **Custom (Personnalisé)**.
6. Cochez la case **Include Detailed Browsing (Inclure la navigation détaillée)** afin d'inclure les informations de navigation dans le rapport.



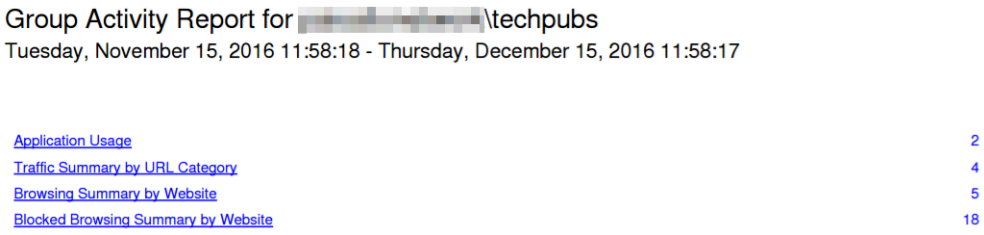
STEP 2 | Exécutez le rapport.

1. Cliquez sur **Run Now (Exécuter maintenant)**.
2. Lorsque le pare-feu finit de générer le rapport, cliquez sur un des liens pour le télécharger :
   - Cliquez sur **Download User Activity Report (Télécharger le rapport sur l'activité des utilisateurs)** pour télécharger une version PDF du rapport.
   - Cliquez sur **Download URL Logs (Télécharger les journaux d'URL)** pour télécharger un fichier CSV des entrées de journal correspondantes.

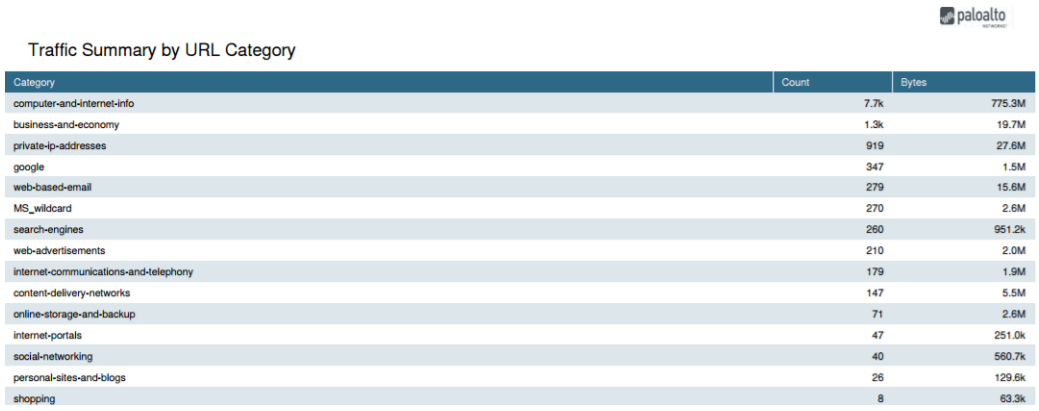


3. Après avoir téléchargé le rapport, cliquez sur **Cancel (Annuler)**.
4. Si vous souhaitez enregistrer les paramètres du rapport d'activité des utilisateurs pour exécuter à nouveau le même rapport ultérieurement, cliquez sur **OK** ; sinon, cliquez sur **Annuler**.

STEP 3 | Consultez le rapport d'activités de l'utilisateur en ouvrant le fichier que vous avez téléchargé. La version PDF du rapport montre l'utilisateur ou groupe sur lequel vous avez basé le rapport, la période du rapport et une table des matières :



STEP 4 | Cliquez sur un élément de la table des matières pour en afficher les détails du rapport. Par exemple, cliquez sur **Traffic Summary by URL Category (Récapitulatif du trafic par catégorie d'URL)** pour afficher les statistiques de l'utilisateur ou du groupe sélectionné.



Category	Count	Bytes
computer-and-internet-info	7.7k	775.3M
business-and-economy	1.3k	19.7M
private-ip-addresses	919	27.6M
google	347	1.5M
web-based-email	279	15.6M
MS_wildcard	270	2.6M
search-engines	260	951.2k
web-advertisements	210	2.0M
internet-communications-and-telephony	179	1.9M
content-delivery-networks	147	5.5M
online-storage-and-backup	71	2.6M
internet-portals	47	251.0k
social-networking	40	560.7k
personal-sites-and-blogs	26	129.6k
shopping	8	63.3k

Planifier et partager des rapports de filtrage des URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

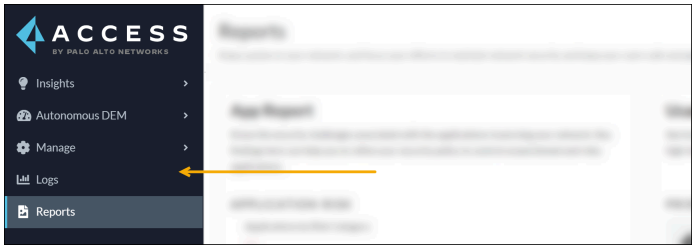
Vous pouvez planifier, générer et partager divers rapports liés au filtrage des URL et à l'activité Web.

- Strata Cloud Manager
- PAN-OS et Panorama

Planifier et partager des rapports de filtrage des URL (Strata Cloud Manager)

Que vous utilisiez Panorama ou Strata Cloud Manager pour gérer Prisma Access, vous pouvez utiliser Strata Cloud Manager pour les rapports de filtrage des URL. Dans Strata Cloud Manager, allez à Activité pour le filtrage interactif des URL des données et des rapports. Vous pouvez partager des rapports d'activité au sein de votre organisation et également les programmer pour des mises à jour régulières. Voici les Prisma Access tableaux de bord et outils qui exploitent et sont les plus pertinents pour le filtrage des URL :

- **Résumé** : identifiez les catégories d'URL qui génèrent le plus d'activité Web sur votre réseau, les 10 principales URL malveillantes et les 10 URL présentant le plus haut risque.
- **Activité de l'utilisateur** - Consultez les habitudes de navigation de chaque utilisateur : les sites les plus fréquemment visités, les sites avec lesquels ils transfèrent des données et les tentatives d'accès aux sites à haut risque. Les données de vos journaux de filtrage des URL et du moteur d'identité sur le cloud permettent cette visibilité.
- Rechercher un artefact de sécurité (une adresse IP, un domaine, une URL ou un hachage de fichier) qui interagit avec des données uniquement pour cet artefact, tirées à la fois de votre réseau et des résultats des informations sur les menaces mondiales.



Pour accéder aux données d'activité des utilisateurs et partager des rapports facilement et en toute sécurité, nous vous recommandons d'activer *et* de configurer le moteur d'identité sur le cloud.

STEP 1 | Téléchargez, partagez et planifiez des rapports d'activité.

STEP 2 | Accédez au résumé du filtrage des URL.

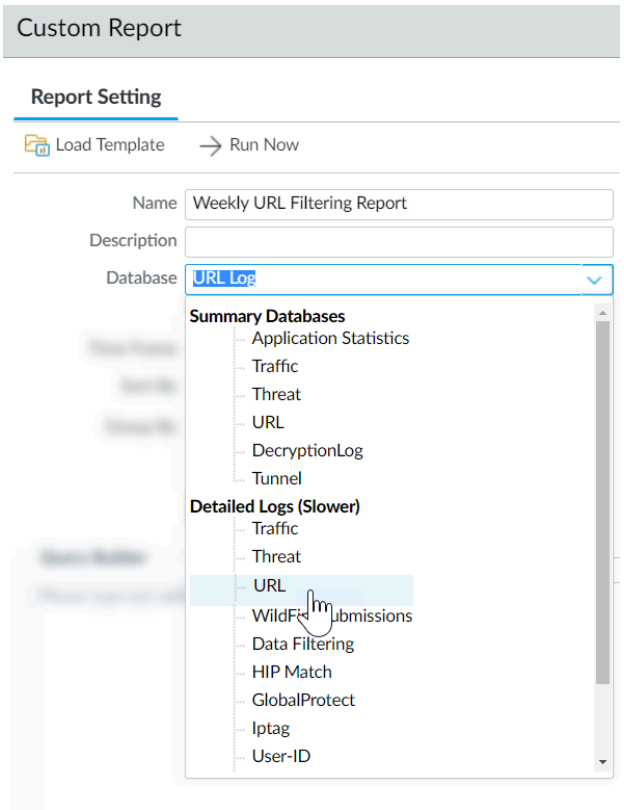
Sélectionnez **Activité** > **Résumé** et cliquez sur l'onglet Filtrage des URL.

STEP 3 | Recherche d'artefacts de sécurité.

Planifier et partager des rapports de filtrage des URL (PAN-OS et Panorama)

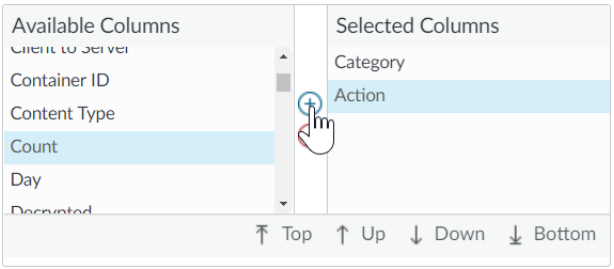
STEP 1 | Ajoutez un nouveau rapport personnalisé.

1. Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)** et **Add (Ajoutez)** un rapport.
2. Donnez un **Name (Nom)** unique au rapport et, éventuellement, une **Description (Description)**.
3. Sélectionnez la **Database (Base de données)** à utiliser pour générer le rapport. Pour générer un rapport de filtrage des URL détaillé, sélectionnez **URL (URL)** à la section Detailed Logs (Journaux détaillés) :

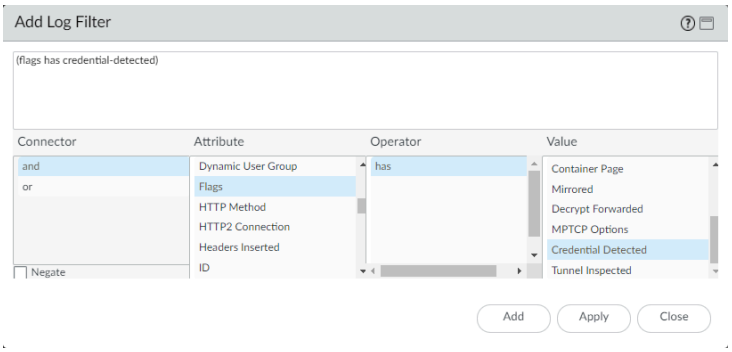


STEP 2 | Configurez les options du rapport.

1. Sélectionnez un **Time Frame (Calendrier)** prédéfini ou sélectionnez **Custom (Personnalisé)**.
2. Sélectionnez les colonnes des journaux à inclure dans le rapport dans la liste Available Columns (Colonnes disponibles), puis ajoutez-les ( ) aux Selected Columns (Colonnes sélectionnées). Par exemple, dans le cas d'un rapport de filtrage des URL, vous pourriez sélectionner les options suivantes :
   - Action (Action)
   - Catégorie d'applications
   - Catégorie
   - Pays de destination
   - Source User (Utilisateur source)
   - URL

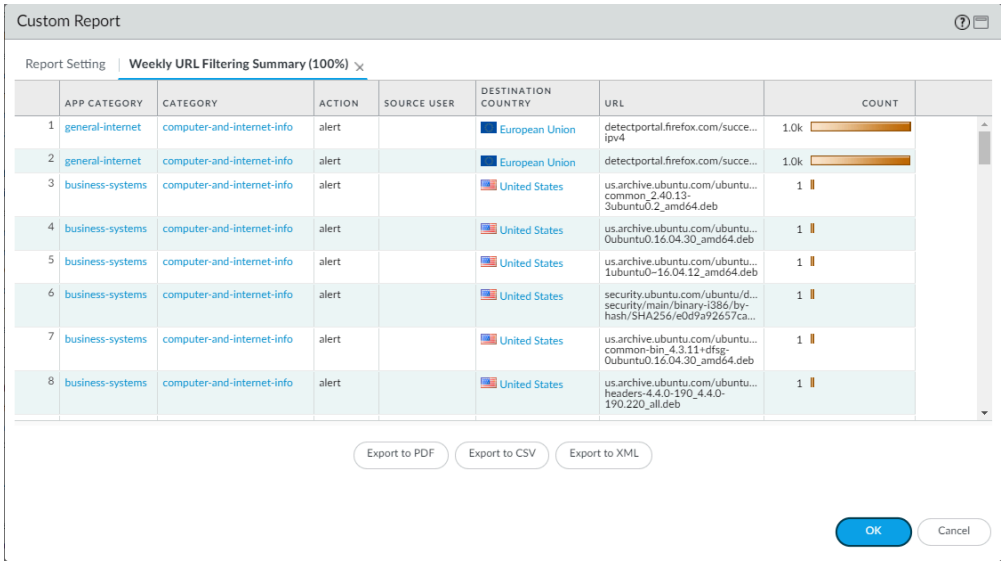


3. Si l'option prevent credential phishing (Empêcher l'hameçonnage des informations d'identification) est activée sur le pare-feu, sélectionnez les **Flags (Indicateurs)**, l'opérateur **has (a)** et la valeur **Credential Detected (Informations d'identification détectées)** pour également inclure les événements dans le rapport afin de consigner les situations où un utilisateur soumet des informations d'identification d'entreprise valide à un site.



4. (Facultatif) Sélectionnez une option **Trier par** pour définir l'attribut à utiliser pour agréger les détails du rapport. Si vous ne sélectionnez pas d'attribut pour le tri, le rapport renvoie les N premiers résultats sans agrégation. Sélectionnez un attribut **Group By (Regrouper par)** à utiliser comme ancrage pour regrouper des données. Voici un exemple d'un rapport dans lequel l'attribut **Group By (Regrouper par)** est défini sur **App Category**

(Catégorie d'application) et l'option **Sort By (Trier par)** est définie sur un **Count** (nombre) de **Top 5** (5 premières).



STEP 3 | Exécutez le rapport.

1. Cliquez sur l'icône **Run Now (Exécuter maintenant)** pour générer immédiatement le rapport, qui s'ouvre dans un nouvel onglet.
2. Lorsque vous avez terminé votre examen du rapport, retournez à l'onglet **Report Setting (Paramètres de rapport)**, puis précisez les paramètres et générez le rapport de nouveau ou passez à l'étape suivante pour planifier la génération du rapport.
3. Cochez la case **Schedule (Calendrier)** pour exécuter le rapport une fois par jour. Il sera généré quotidiennement et détaillera l'activité Web des 24 dernières heures.

STEP 4 | **Commit (Validez)** la configuration.

STEP 5 | Affichez le rapport personnalisé.

1. Sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**.
2. Développez le panneau **Custom Reports (Rapports personnalisés)** dans la colonne de droite et sélectionnez le rapport à afficher. Le rapport le plus récent s'affiche automatiquement.
3. Pour consulter le rapport d'une date antérieure, sélectionnez la date souhaitée dans le calendrier. Vous pouvez également exporter le rapport au format PDF, CSV ou XML.

Journalisez uniquement la page visitée par un utilisateur

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Une page conteneur est la page principale à laquelle accède un utilisateur lorsqu'il visite un site Web, mais d'autres pages peuvent être chargées en même temps que cette page principale. Si l'option **Page Conteneur de journaux uniquement** est activée dans un profil de filtrage des URL (profil de gestion d'accès à l'URL pour Prisma Access), seule la page principale du conteneur sera enregistrée, et non les pages suivantes qui peuvent être chargées dans la page du conteneur. Étant donné que le URL Filtering peut potentiellement générer un grand nombre d'entrées de journal, vous pouvez activer cette option afin que les entrées de journal ne contiennent que les URL dont le nom de fichier de la page demandée correspond à des types MIME spécifiques. Les types MIME suivants sont fournis par défaut :

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml

*Si vous activez l'option **Log container page only (Page conteneur de journaux uniquement)**, il est possible qu'une entrée corrélée du journal des URL n'existe pas pour identifier les menaces détectées par l'antivirus ou la protection contre les vulnérabilités.*

- Strata Cloud Manager
- PAN-OS et Panorama

Journalisez uniquement la page visitée par un utilisateur (Strata Cloud Manager)

Si vous utilisez Panorama pour gérer Prisma Access :

*Basculez sur l'onglet **PAN-OS et Panorama** et suivez les indications qui s'y trouvent.*

Si vous utilisez Strata Cloud Manager, continuez ici.

STEP 1 | Dans un profil Gestion des accès à l'URL, sélectionnez **Journaliser la page de conteneur uniquement**.

STEP 2 | Appliquez le profil Gestion des accès à l'URL à une règle de politique de sécurité.

Un profil Gestion des accès à l'URL n'est actif que lorsqu'il est inclus dans un groupe de profils auquel une règle de politique de sécurité fait référence.

Suivez les étapes pour activer un profil Gestion des accès à l'URL (et tout profil de sécurité). Assurez-vous de **Transmettre la configuration**.

Journalisez uniquement la page visitée par un utilisateur (PAN-OS et Panorama)

STEP 1 | Créez ou sélectionnez un profil de filtrage des URL à modifier.

Sélectionnez **Objets** > **Profils de sécurité** > **Filtrage des URL**.

STEP 2 | Activez **Journalise la page de conteneur uniquement**.

STEP 3 | Cliquez sur **OK** pour enregistrer le profil.

STEP 4 | **Commit (Validez)** vos modifications.

Journalisation de l'en-tête HTTP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Le URL Filtering permet la visibilité et le contrôle du trafic Web sur votre réseau. Pour une meilleure visibilité sur le contenu Web, vous pouvez configurer le profil de filtrage des URL pour consigner les attributs d'en-tête HTTP inclus dans une requête Web. Lorsqu'un client demande une page Web, l'en-tête HTTP inclut les champs Utilisateur-Agent, Référant et X-Forwarded-For sous forme de paire attribut/valeur et les transmet au serveur Web. Lorsque cette option est activée pour consigner les en-têtes HTTP, le pare-feu consigne les paires attributs/valeurs suivantes dans les journaux de filtrage des URL.

Vous pouvez utiliser les en-têtes HTTP pour gérer l'accès aux applications SaaS. Pour ce faire, vous n'avez pas besoin d'un abonnement de filtrage des URL, mais vous devez utiliser un profil de filtrage des URL pour activer cette fonction.

Attribut	Description
User-Agent (Utilisateur-Agent)	Le navigateur Web utilisé par l'utilisateur pour accéder à l'URL, Internet Explorer par exemple. Ces informations sont incluses dans la demande HTTP envoyée au serveur. L'en-tête HTTP ne contient pas la chaîne complète de l'agent utilisateur. Le nombre maximal d'octets enregistrés du paquet précédant le paquet contenant la fin d'en-tête est de 36 octets.
Référant	L'URL de la page Web associée qui relie l'utilisateur à une autre page Web ; il s'agit de la source qui a redirigé (référé) l'utilisateur vers (à) la page Web demandée.
X-Forwarded-For (XFF)	L'option du champ d'en-tête de requête HTTP qui conserve l'adresse IP de l'utilisateur qui a demandé la page Web. Si votre réseau comporte un serveur proxy, XFF vous permet d'identifier l'adresse IP de l'utilisateur qui a demandé le contenu au lieu d'enregistrer uniquement l'adresse IP du

Attribut	Description
	serveur proxy en tant qu'adresse IP de l'utilisateur qui a demandé la page Web.
Insertion d’en-têtes	Le type d’en-tête et le texte de l’en-tête que le pare-feu insère.

Demande de changement de catégorie d'une URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Remarques :*** • *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.* • Prisma Access *les licences incluent les capacités Advanced URL Filtering.*

Si vous pensez qu'un domaine ou une URL a été mal catégorisé, vous pouvez soumettre une demande de recatégorisation via votre pare-feu ou Test A Site, notre outil de recherche de catégorie d'URL. Vous pouvez également soumettre des demandes de recatégorisation en masse via Test A Site. Les deux méthodes nécessitent que vous suggériez au moins une nouvelle catégorie pour l'URL que vous souhaitez examiner.

Vous ne pouvez pas demander de modification de la catégorie de risque qu'une URL reçoit, ou pour les URL classées comme `contenu insuffisant` *ou* `domaines nouvellement enregistrés`.

Sur le pare-feu, vous pouvez demander une modification de catégorie d'URL à partir de la vue détaillée du journal d'une entrée de journal de filtrage des URL. Sur Test A Site, vous devez saisir le site Web que vous souhaitez recatégoriser pour afficher sa catégorisation PAN-DB. Le lien du formulaire de demande suit les résultats de la recherche. De même, dans Strata Cloud Manager, un lien vers le formulaire Test A Site s'affiche avec les résultats des requêtes vers l'outil interne Test A Site disponible lors de la modification des profils de gestion des accès à l'URL. Pour accéder au formulaire de demande de modification en masse, vous devez vous connecter à Test A Site. Une fois connecté, la page Web affiche un lien vers le formulaire de demande en masse.

Immédiatement après qu'une personne soumet une demande de modification, un robot d'exploration automatisé analyse l'URL. Si le robot valide votre suggestion de catégorie, Palo Alto Networks approuve votre demande et met immédiatement à jour PAN-DB avec la nouvelle catégorie. Dans le cas contraire, les rédacteurs humains des équipes de recherche sur les menaces et de science des données de Palo Alto Networks examinent votre demande. Ils peuvent décider de conserver la catégorie d'origine, d'être d'accord avec la catégorie que vous proposez ou de modifier la catégorie (s'ils ne sont pas d'accord avec la catégorie d'origine et la catégorie suggérée).

Après avoir soumis une demande de modification, vous recevrez un e-mail de confirmation. Une fois l'enquête terminée, vous recevrez un deuxième e-mail avec les résultats.

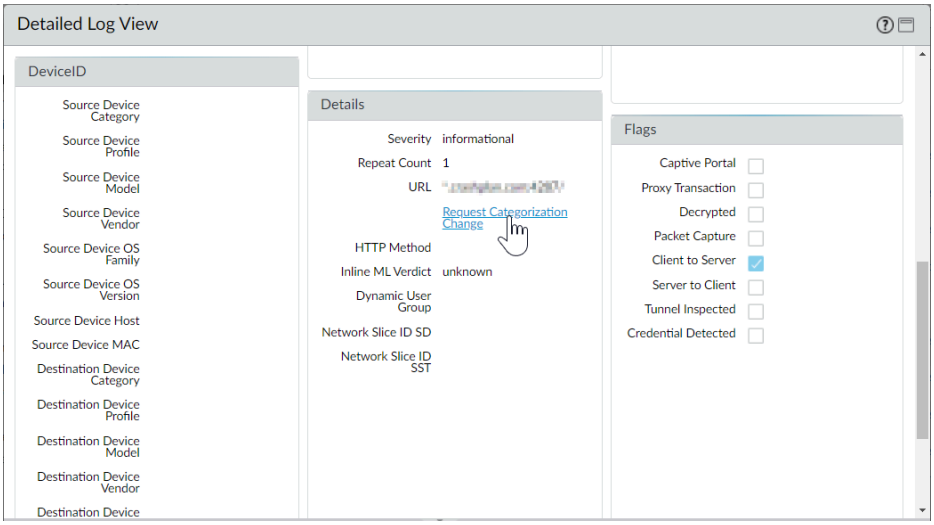
- PAN-OS et Panorama
- Test A Site

Demande de modification de la catégorie d'une URL (PAN-OS et Panorama)

STEP 1 | Accédez aux journaux de filtrage des URL (**Moniteur** > **Journaux** > **Filtrage des URL**).

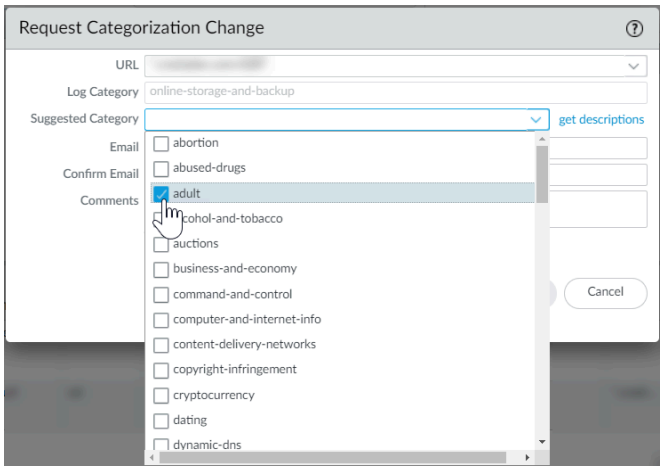
STEP 2 | Ouvrez la vue détaillée du journal pour une entrée de journal de filtrage des URL avec la catégorisation d'URL que vous souhaitez modifier.

1. Cliquez sur la longue-vue ( ) correspondant à l'entrée du journal. La vue détaillée du journal s'affiche.



STEP 3 | Sous Détails, cliquez sur **Demander un changement de catégorisation**.

STEP 4 | Remplissez le formulaire de demande et soumettez-le.



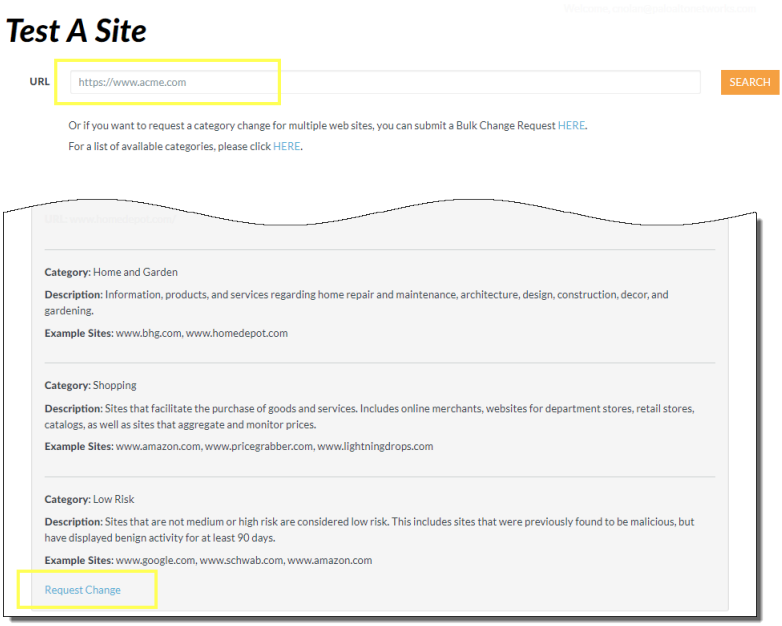
Demande de modification de la catégorie d'une URL (Test A Site)

STEP 1 | Allez à Test A Site.

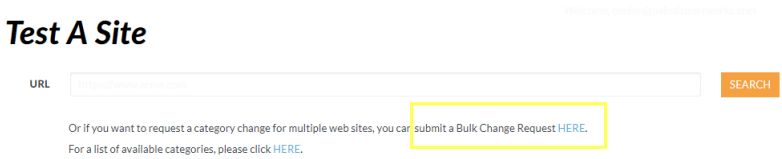
> ***Connectez-vous*** *pour éviter de réaliser un test CAPTCHA et de saisir votre email sur le formulaire de demande de modification. Notez que la connexion est le seul moyen d'accéder au formulaire de demande de modification en masse.*

STEP 2 | Sélectionnez un formulaire de demande de modification à remplir.

- **Demande de modification pour une URL unique** : saisissez **l'URL** que vous souhaitez recatégoriser et cliquez sur **Rechercher**. Sous les résultats de la catégorie d'URL, cliquez sur **Demander une modification**.



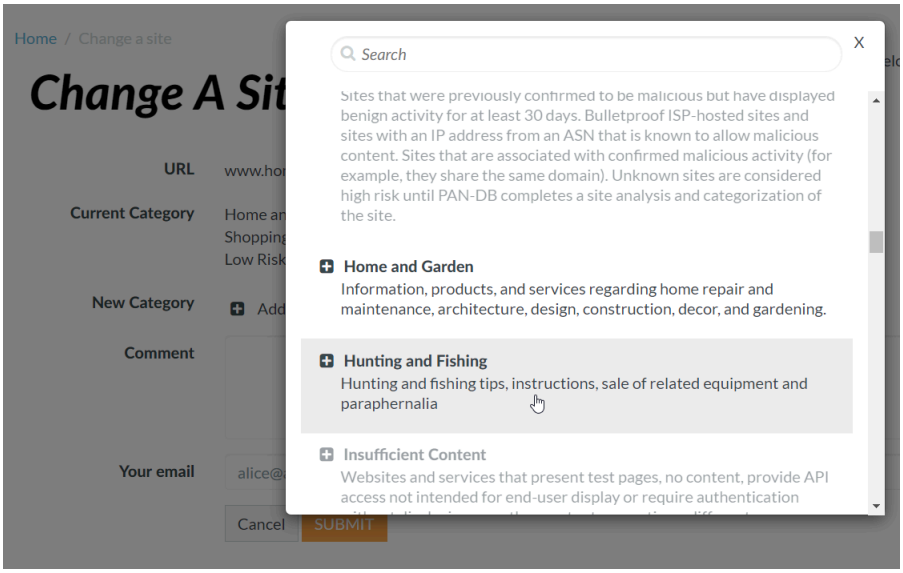
- **Demande de modification en masse—Connectez-vous à** Test A Site. Ensuite, cliquez sur Soumettre une demande de modification en masse **ICI**.



STEP 3 | Remplissez le formulaire de demande de modification.

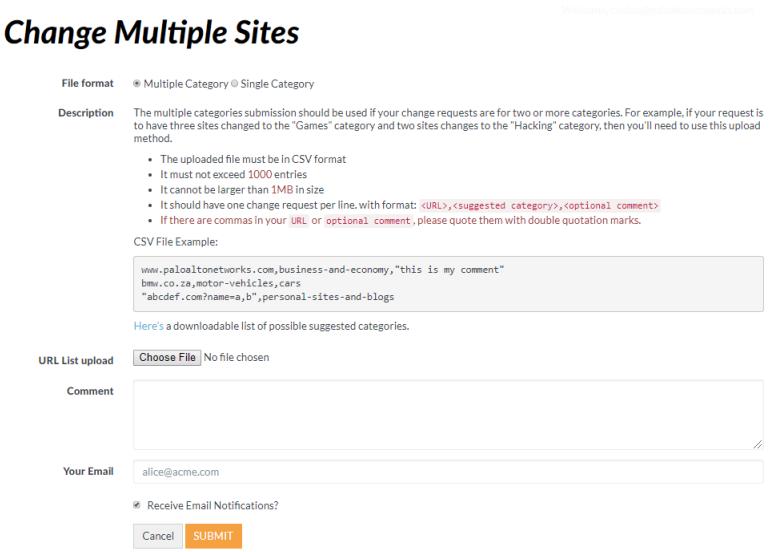
- **Demande de modification pour une URL unique** : suggérez jusqu'à deux nouvelles catégories pour l'URL. Cliquez sur **Sélectionner une catégorie (dans une liste)**et

sélectionnez une catégorie à la fois. En option, laissez un **commentaire** sur votre demande. Vous pouvez expliquer pourquoi votre suggestion est appropriée, par exemple.



- **Demande de modification en masse**— Choisissez un **Format de fichier**. Sélectionnez plusieurs catégories si votre demande de modification comprend deux catégories ou plus. Par exemple, si vous souhaitez reclasser la moitié des URL de votre liste dans `business-and-economy` et l'autre moitié en `personal-sites-and-blogs`.

  Cliquez ensuite sur **Choisir un fichier**et sélectionnez un fichier CSV à télécharger. Le fichier doit contenir une demande de modification par ligne dans ce format : `<URL>,<first suggested category>,<second suggested category>,<(optional) comment>`. Le fichier ne peut pas dépasser 1 000 entrées ni dépasser 1 Mo. En option, laissez un **commentaire** sur votre demande.



STEP 4 | **Submit (Envoyez)** le formulaire.

Dépannage

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Ce chapitre partage les tâches de diagnostic et de résolution des problèmes courants de filtrage des URL pour les pare-feu de nouvelle génération de Palo Alto Networks. Avant de contacter l'assistance de Palo Alto Networks pour ces questions, suivez les étapes des tâches pertinentes. Si vous devez alors encore contacter l'assistance, assurez-vous d'inclure toutes les informations que vous avez apprises lors de l'exécution des tâches de dépannage.

Le dépannage et la surveillance de l'activité Web vont souvent de pair. Tirez souvent parti des outils de surveillance et de journalisation pour identifier et résoudre les problèmes que ce chapitre n'aborde pas explicitement. Familiarisez-vous avec les outils et les tâches de surveillance dans le chapitre Surveillance.

- Problèmes d'activation du filtrage d'URL avancé
- Problèmes de connectivité au cloud PAN-DB
- URL classées comme étant non résolues
- Catégorisation incorrecte
- Résoudre les problèmes d'accès au site Web
- Résoudre les problèmes d'affichage de la page de réponse du filtrage des URL

Problèmes d’activation du filtrage d’URL avancé

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Utilisez le flux de travail suivant pour résoudre les problèmes d’activation du filtrage d’URL avancé.

STEP 1 | Accès à la CLI PAN-OS.

STEP 2 | Vérifiez si le filtrage avancé des URL a été activé en exécutant la commande suivante :

```
show system setting url-database
```

Si la réponse est `paloaltonetworks`, PAN-DB, la base de données de filtrage d’URL palo alto networks, est le fournisseur actif.

STEP 3 | Vérifiez que le pare-feu dispose d’une licence de filtrage des URL avancé valide.

Exécutez la commande CLI **`demande d’informations sur la licence`**.

L'entrée de licence `Feature: URL Filtering avancé`. Si la licence n'est pas installée, vous devrez vous procurer et installer une licence. Reportez-vous à la section Configuration du URL Filtering.

STEP 4 | Vérifiez l’état de la connexion au cloud PAN-DB.

Problèmes de connectivité au cloud PAN-DB

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Pour garantir la connectivité au cloud PAN-DB, créez une règle de politique de sécurité dédiée pour autoriser tout le trafic du service de gestion de Palo Alto. Cela évitera que le trafic de gestion soit classé comme `non résolu` *et empêchera le trafic d'être bloqué lorsqu'il est acheminé via le plan de données.*

Pour vérifier la connectivité entre le pare-feu et le cloud PAN-DB :

```
show url-cloud status
```

Si le Cloud est accessible, la réponse attendue doit être semblable à la suivante :

```
show url-cloud status Licence de filtrage d'URL PAN-DB : valide
 Serveur cloud actuel : serverlist.urlcloud.paloaltonetworks.com
 Connexion cloud : connecté Mode cloud : version de la base de
 données d'URL publique - appareil : 20200624.20296 Version de la
 base de données d'URL - cloud : 20200624.20296 (dernière mise à jour
 2020/06/24 12:39:19) État de la base de données d'URL : bon Version
 du protocole d'URL - appareil : pan/2.0.0 Version du protocole d'URL
 - cloud : pan/2.0.0 État de compatibilité du protocole : compatible
```

Si le cloud est inaccessible, la réponse attendue doit être semblable à la suivante :

```
show url-cloud status Licence de filtrage d'URL PAN-DB : valide
 Connexion au cloud : non connecté Version de la base de données
 d'URL - appareil : 0000.00.00.000 Version du protocole URL -
 appareil : pan/0.0.2
```

Utilisez la liste de vérification suivante pour identifier et résoudre les problèmes de connectivité :

- ❑ Le champ de la licence de filtrage des données PAN-DB affiche-t-il invalid (non valide) ? Obtenez et installez une licence PAN-DB valide.
- ❑ La version du protocole d'URL affiche-t-elle not compatible (non compatible) ? Passez à la dernière version de PAN-OS.

- Pouvez-vous envoyer une requête ping au serveur cloud PAN-DB à partir du pare-feu ? Exécutez la commande suivante pour vérifier :

  ```
  ping source <ip-address> host
   serverlist.urlcloud.paloaltonetworks.com <
  ```

  Par exemple, si l'adresse IP de votre interface de gestion est 10.1.1.5, exécutez la commande suivante :

  ```
  ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
  ```

- Le pare-feu est-il dans une configuration HA ? Vérifiez que l'état HA des pare-feu est à l'état actif, actif-principal ou actif-secondaire. L'accès au cloud PAN-DB sera bloqué si l'état du pare-feu est autre. Exécutez la commande suivante sur chaque pare-feu de la paire pour voir l'état :

  ```
  show high-availability state
  ```

Si vous avez toujours des problèmes de connectivité entre le pare-feu et le cloud PAN-DB, contactez le support Palo Alto Networks.

URL classées comme étant non résolues

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Les URL sont classées comme `non résolues` si votre pare-feu ne peut pas se connecter au service cloud de filtrage des URL PAN-DB pour effectuer des recherches, ou si PAN-DB met trop de temps à répondre aux requêtes d'URL. L'état de la connexion au cloud et la classification des URL ne s'appliquent pas aux licences d'abonnement expirées ou aux utilisateurs sans licence. Pour une explication détaillée du processus de catégorisation des URL, voir Fonctionnement du filtrage des URL.

Utilisez le flux de travail suivant lorsque certaines ou toutes les URL identifiées par PAN-DB sont classées comme étant Not-resolved (non résolues) :

STEP 1 | Vérifiez la connexion cloud PAN-DB en exécutant la commande CLI **`show url-cloud status`**.

Le champ `Connexion cloud :` doit indiquer `connecté`. Si une valeur autre que `connecté` s'affiche, toutes les URL qui ne figurent pas dans le cache du plan de gestion seront classées comme `non résolues`. Pour résoudre ce problème, consultez Problèmes de connectivité Cloud PAN-DB.

STEP 2 | Si le statut de connexion au cloud indique `connected`, vérifiez l'utilisation actuelle du pare-feu.

Si l'utilisation du pare-feu monte en flèche, les requêtes d'URL peuvent être abandonnées (et éventuellement ne pas atteindre le plan de gestion) et seront classées comme étant `non résolues`.

Pour afficher les ressources système, exécutez la commande CLI **`afficher les ressources système`**. Affichez ensuite les colonnes %CPU et %MEM.

Vous pouvez également visualiser les ressources du système sur le widget System Resources (Ressources système) dans le **Dashboard (Tableau de bord)** de l'interface Web.

STEP 3 | Envisagez d'augmenter la valeur du **délai d'attente de recherche de la catégorie (sec)**.

Augmentez la valeur de délai d'attente de recherche de catégorie améliore la probabilité que la catégorie URL soit résolue et réduit la fréquence des URL `non résolues` dans les journaux.

1. Sélectionnez **Périphérique** > **Configuration** > **Content-ID** et modifiez les paramètres de filtrage des URL.
2. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

   Vous pouvez également mettre à jour la valeur en utilisant la commande CLI **`set deviceconfig setting ctd url-wait-timeout`**.

STEP 4 | Si le problème persiste, contactez le support de Palo Alto Networks.

Catégorisation incorrecte

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Il se peut parfois que vous tombiez sur une URL qui, selon vous, est mal catégorisée. Servez-vous du flux de travail suivant pour déterminer la catégorisation de l'URL d'un site et pour demander que la catégorie soit modifiée, si nécessaire.

STEP 1 | Vérifiez la catégorie dans le plan de données en exécutant la commande suivante :

```
show running url <URL>
```

Par exemple, pour afficher la catégorie du site Web de Palo Alto Networks, exécutez la commande suivante :

```
show running url paloaltonetworks.com
```

Si l'URL stockée dans le cache du plan de données affiche la catégorie correcte (computer-and-internet-info dans cet exemple), alors la catégorisation est correcte et aucune autre action n'est requise. Si la catégorie est incorrecte, passez à l'étape suivante.

STEP 2 | Vérifiez si la catégorie figure dans le plan de gestion en exécutant la commande suivante :

```
test url-info-host <URL>
```

Par exemple :

```
test url-info-host paloaltonetworks.com
```

Si l'URL stockée dans le cache du plan de gestion affiche la catégorie correcte, supprimez l'URL du cache du plan de gestion en exécutant la commande suivante :

```
clear url-cache url <URL>
```

La prochaine fois que le pare-feu demandera la catégorie de cette URL, la requête sera transférée au plan de gestion. Ceci va résoudre le problème et aucune autre action ne sera requise. Si le problème n'est toujours pas résolu, passez à l'étape suivante pour vérifier la catégorie d'URL sur les systèmes Cloud.

STEP 3 | Vérifiez la catégorie dans le Cloud en exécutant la commande suivante :

```
test url-info-cloud <URL>
```

STEP 4 | Si l'URL stockée dans le cloud affiche la catégorie correcte, supprimez l'URL des caches des plans de données et de gestion.

Exécutez la commande suivante pour supprimer une URL du cache du plan de données :

```
clear url-cache url <URL>
```

Exécutez la commande suivante pour supprimer une URL du cache du plan de gestion :

```
delete url-database url <URL>
```

La prochaine fois que le pare-feu demandera la catégorie de l'URL donné, la requête sera transférée au plan de gestion, puis au cloud. Ceci devrait résoudre le problème de recherche de catégorie. Si le problème persiste, passez à l'étape suivante pour soumettre une requête de modification de catégorisation.

STEP 5 | Pour soumettre une requête de modification depuis l'interface Web, accédez au journal des URL et sélectionnez l'entrée de journal de l'URL que vous souhaitez modifier.

STEP 6 | Cliquez sur lien **Request Categorization (Demander un changement de catégorisation)** et suivez les instructions. Vous pouvez également demander un changement de catégorie à partir du site Web Test A Site de Palo Alto Networks en recherchant l'URL et en cliquant sur l'icône **Demander un changement**. Pour afficher les descriptions de chaque catégorie, reportez-vous à Catégories d'URL prédéfinies.

Vous recevez une notification par courrier électronique si votre requête de modification est approuvée. Deux options pour vérifier que la catégorie d'URL est mise à jour sur le pare-feu sont possibles :

- Patientez jusqu'à ce que l'URL dans le cache arrive à expiration et la prochaine fois qu'un utilisateur accède à l'URL, la nouvelle mise à jour de catégorisation sera mise dans le cache.
- Exécutez la commande suivante pour forcer une mise à jour dans le cache :

```
request url-filtering update url <URL>
```


Résoudre les problèmes d'accès au site Web

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Les utilisateurs finaux peuvent rencontrer des problèmes d'accès à un site Web pour diverses raisons, y compris une licence de filtrage d'URL manquante, une mauvaise configuration des règles de politique, des problèmes de connectivité PAN-DB ou une mauvaise catégorisation d'un site Web. Suivez les étapes suivantes pour diagnostiquer et résoudre les problèmes d'accès à un site Web.

Il est possible que le problème ne soit pas lié au filtrage des URL. La section « Que faire ensuite » qui suit les étapes de cette tâche répertorie d'autres domaines dans lesquels concentrer votre résolution de problème.

STEP 1 | Vérifiez que vous disposez d'une licence active de filtrage des URL avancé ou de filtrage des URL hérité.

Une licence active de filtrage des URL est nécessaire pour les pare-feu de nouvelle génération afin de catégoriser avec précision les sites Web et les applications. Si vous n'avez pas de licence de filtrage des URL, le problème d'accès au site Web n'est pas lié au filtrage des URL.

Sélectionnez **Périphérique** > **Licences** et cherchez la licence de filtrage des URL avancé (ou filtrage des URL PAN-DB). Une licence active affiche une date d'expiration postérieure à la date actuelle.

Sinon, utilisez la **`commande CLI de demande d'informations sur la`** licence. Si la licence est active, l'interface affiche les informations de licence, y compris le statut d'expiration : `Expiré ? : non`.

STEP 2 | Vérifiez le statut de la connexion cloud PAN-DB sur votre CLI.

Le champ `Connexion cloud :` doit indiquer `connecté`. Sinon, toute URL qui n'existe pas dans le cache du plan de gestion (MP) sera classée comme `non résolue` et peut être bloquée par les paramètres de profil de filtrage des URL dans vos règles de politique de sécurité.

STEP 3 | Videz le cache MP et plan de données (DP) pour l'URL spécifique.

Vider le cache peut être coûteux en ressources. Pensez à vider le cache pendant une fenêtre de maintenance.

1. Pour vider le cache MP, utilisez la commande **`delete url-database url <affected url>`** commande CLI.
2. Pour vider le cache DP, utilisez la commande **`clear url-cache url <affected url>`** commande CLI.

STEP 4 | Examinez les journaux de filtrage des URL pour vérifier si la catégorie d'URL à laquelle appartient le site Web a été bloquée.

1. Sélectionnez **Surveiller** > **Filtrage des URL**.
2. Recherchez l'URL concernée, puis sélectionnez l'entrée de journal la plus récente.
3. Examinez les colonnes Catégorie et Action.

   L'URL a-t-elle été catégorisée correctement ? Vérifiez ses catégories en utilisant Test A Site, l'outil de recherche de catégorie d'URL de Palo Alto Networks. Si vous pensez toujours que la catégorisation est incorrecte, soumettez une demande de modification.

   Si la colonne Action affiche `block-url`, notez le nom de la règle de la politique de sécurité associée à l'entrée de journal.

STEP 5 | Examinez la règle de politique de sécurité et mettez-la à jour, si nécessaire.

1. Sélectionnez **Politiques** > **Sécurité**, puis sélectionnez la règle de politique avec le nom que vous avez noté à l'étape précédente.
2. Vérifiez que la règle de politique de sécurité autorise l'accès à l'URL demandée ou à sa catégorie d'URL.

   Recherchez l'une des deux configurations suivantes :

   - **Catégorie d'URL comme critère de correspondance :** Sous **Catégorie de service/d'URL**, l'une des catégories spécifiées contient l'URL demandée. Sous **Actions**, le paramètre Action est défini sur **Autoriser**.
   - **Profil de filtrage des URL :** Sous **Actions**, le paramètre Profil est défini sur un profil de filtrage des URL qui permet d'accéder à l'URL demandée.

STEP 6 | Testez vos règles de politique de sécurité.

Si les étapes ci-dessus ne mettent pas en évidence ou ne résolvent pas le problème, un dépannage supplémentaire pourrait être nécessaire pour isoler davantage le problème. Les domaines d'intervention devraient inclure :

- Connectivité de l'adresse IP de base
- Configuration du routage
- Résolution DNS
- Configuration des proxys
- Pare-feu en amont ou périphériques d'inspection dans le chemin des paquets

Pour les problèmes intermittents ou complexes, contactez le support de Palo Alto Networks pour obtenir une assistance supplémentaire.

Résoudre les problèmes d'affichage de la page de réponse du filtrage des URL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Les pages de réponse de filtrage des URL peuvent ne pas s'afficher pour diverses raisons, notamment :

- Les inspections de l'établissement de liaison SSL/TLS sont activées.
- Le site Web a été bloqué lors de l'inspection d'une liaison SSL/TLS. Les pages de réponse de filtrage des URL ne s'affichent pas dans ce cas, car le pare-feu réinitialise la connexion HTTPS.
- Le site Web utilise le protocole HTTPS ou contient du contenu diffusé sur HTTPS (comme des annonces), mais le site Web ou la catégorie d'URL n'a pas été décrypté.
- La page de réponse personnalisée est plus grande que la taille maximale prise en charge.

Utilisez les étapes suivantes comme point de départ pour dépanner une page de réponse de filtrage des URL qui ne s'affiche pas. Si le problème persiste, contactez le support de Palo Alto Networks.

STEP 1 | Déterminez la portée du problème.

Le problème est-il spécifique à un site Web particulier ou à un sous-ensemble de pages Web ? Vérifiez si une page de réponse s'affiche lorsque vous visitez une page différente sur le site Web.

STEP 2 | Identifiez le protocole du site Web (HTTP ou HTTPS).

Cette distinction aide à mieux isoler et diagnostiquer le problème.

STEP 3 | (Sites HTTPS ou sites HTTP avec contenu HTTPS) Vérifiez qu'une règle de politique de décryptage SSL/TLS décrypte le trafic vers le site Web ou la catégorie d'URL.

En général, le pare-feu ne peut pas servir de pages de réponse sur les sites Web HTTPS à moins qu'il ne puisse décrypter les sites Web.

Certains sites Web peuvent servir sa page principale sur HTTP, mais diffusent des annonces ou d'autres contenus sur HTTPS. Ces sites Web devraient également être décryptés pour assurer l'affichage des pages de réponse.

1. Connectez-vous à l'interface Web.
2. Sélectionnez **Politiques** > **Décryptage**, et assurez-vous que la règle pertinente décrypte le trafic vers le site Web ou la catégorie d'URL spécifique.

   Si ce n'est pas le cas, mettez à jour la règle de politique de décryptage pour décrypter le site Web ou la catégorie d'URL.

- Si le décryptage SSL/TLS est activé et que la page de réponse ne s'affiche toujours pas, alorsactivez l'inspection des liaisons SSL/TLS.
- Pour servir une page de réponse de filtrage des URL sur une session HTTPS sans activer le décryptage SSL/TLS, procédez comme suit.

STEP 4 | Vérifiez que la catégorie d'URL à laquelle appartient le site Web a été bloquée.

Si la catégorie a été bloquée dans un profil de filtrage des URL appliqué à une règle de politique de sécurité ou par une règle de politique de sécurité avec la catégorie d'URL spécifique comme critères de correspondance, la valeur de la colonne Action pour une entrée donnée affiche `block-url`.

1. Sélectionnez **Surveiller** > **Filtrage des URL**.
2. Recherchez le site Web affecté et sélectionnez l'entrée de journal la plus récente.
3. Examinez les colonnes Catégorie et Action.

   Les catégories attribuées au site Web sont-elles exactes ? Vérifiez ses catégories en utilisant Test A Site, l'outil de recherche de catégorie d'URL de Palo Alto Networks. Si vous pensez toujours que le site Web est mal classé, soumettez une demande de modification.

   La valeur Action est-elle `block-url` ? Sinon, mettez à jour le profil de filtrage des URL ou la règle de politique de sécurité.
4. Pour référence future, notez la règle associée à cette entrée de journal.

STEP 5 | Déterminez si une page de réponse personnalisée est la cause de ce problème.

1. Sélectionnez **Périphérique** > **Pages de réponse**.
2. Confirmez que seul **Prédéfini** est sélectionné.

   Une page de réponse personnalisée est active si **le partage** est répertorié (en plus de **Prédéfini**) dans l'un ou l'autre de ces endroits :

   - **Périphérique** > **Pages de réponse** : Sous la colonne Emplacement correspondant à une page de réponse donnée.
   - **Périphérique** > **Pages de réponse** > ***Type*** : Sous Emplacement.
3. (Si **Partagé** est répertorié) Ramenez la page personnalisée à son état par défaut pour confirmer que la page de réponse personnalisée est le problème.

   1. **Supprimez** la page personnalisée.
   2. **Commit (Validez)** vos modifications.
   3. Visitez le site Web concerné pour voir si la page de réponse par défaut s'affiche.

   Si le problème persiste, appelez le support pour une analyse plus approfondie.

Si les étapes ci-dessus ne corrigent pas le problème, contactez le support de Palo Alto Networks. Un dépannage supplémentaire peut être nécessaire pour identifier le problème. Par exemple, l'analyse du trafic via un outil de capture de paquets (pcap) parallèlement au support peut être utile si une page de réponse ne fonctionne pas pour certaines pages Web, mais fonctionne pour d'autres.

Cloud privé PAN-DB

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Le cloud privé PAN-DB est une solution sur site adaptée aux organisations limitant l'utilisation des services de cloud public. Notamment, les pare-feu interrogent les serveurs de cloud privé PAN-DB lors des recherches d'URL au lieu des serveurs de cloud public PAN-DB. Pour mettre en œuvre cette solution, vous devez déployer un ou plusieurs appareils M-600 ou M-700 en tant que serveurs PAN-DB au sein de votre réseau ou de votre centre de données. Seuls les pare-feu exécutant PAN-OS 9.1 ou versions ultérieures peuvent communiquer avec le cloud privé PAN-DB.

Les déploiements de cloud privé PAN-DB ne prennent pas en charge les fonctionnalités d'analyse d'URL basées sur le cloud de Advanced URL Filtering l'abonnement.

Le tableau suivant décrit les différences entre le cloud public PAN-DB et le cloud privé PAN-DB.

Table 1: Différences entre le cloud public PAN-DB et le cloud privé PAN-DB

Différences	Cloud public PAN-DB	Cloud privé PAN-DB
Mises à jour du contenu et de la base de données	Les mises à jour du contenu (régulières et critiques) et les mises à jour complètes de la base de données d'URL sont publiées plusieurs fois par jour. Le cloud public PAN-DB met à jour les catégories d'URL de logiciels malveillants et d'hameçonnage toutes les cinq minutes. Le pare-feu recherche également des mises à jour critiques lorsqu'il recherche des URL sur les serveurs de cloud.	Des mises à jour du contenu et de la base de données d'URL complète sont disponibles une fois par jour pendant la semaine de travail.
Requêtes de catégorisation des URL	Vous pouvez demander une modification de la catégorisation de l'URL via : • Site Web Test A Site de Palo Alto Networks.	Vous pouvez demander une modification de la catégorisation des URL via le site Web Test A Site de Palo Alto Networks.

Différences	Cloud public PAN-DB	Cloud privé PAN-DB
	• Un profil de filtrage des URL. • Un journal de filtrage des URL.	
Requêtes d'URL non résolues	Si le pare-feu ne parvient pas à résoudre une requête d'URL, celle-ci est envoyée aux serveurs du cloud public.	Si le pare-feu ne parvient pas à résoudre une requête, celle-ci est envoyée aux appareils du cloud privé PAN-DB. S'il n'y a pas de correspondance pour l'URL, le cloud privé PAN-DB envoie une réponse de catégorie *inconnu* au pare-feu ; la requête n'est pas envoyée au cloud public tant que vous n'avez pas configuré vos appareils pour accéder au cloud public PAN-DB. Si les appareils de votre cloud privé PAN-DB fonctionnent complètement hors ligne, le pare-feu n'envoie pas de données ou d'analyses au cloud public.

- Comment fonctionne le cloud privé PAN-DB
- Équipements de cloud privé PAN-DB
- Configurer le cloud privé PAN-DB

Comment fonctionne le cloud privé PAN-DB

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Lorsque vous configurez le cloud privé PAN-DB, vous pouvez configurer vos appareils M-600 ou M-700 pour avoir un accès Internet direct ou rester hors ligne. Les appareils nécessitent des mises à jour de base de données et de contenu pour effectuer des recherches d'URL. Si les appareils ne disposent pas d'une connexion Internet active, vous devez télécharger manuellement les mises à jour sur un serveur de votre réseau et importer les mises à jour dans chaque appareil M-600 ou M-700 dans le cloud privé PAN-DB à l'aide de SCP. De plus, les appareils doivent être en mesure d'accéder à la base de données initiale et à toute autre mise à jour du contenu périodique ou critique pour les pare-feu qu'ils desservent.

Le processus de recherche d'URL est le même pour les pare-feu dans les déploiements de cloud privé et public. Cependant, dans les déploiements de cloud privé, les pare-feu interrogent les serveurs du cloud privé PAN-DB. Vous devrez spécifier l'adresse IP ou le FQDN de chaque appareil M-600 ou M-700 qu'ils peuvent interroger pour accorder à vos pare-feu l'accès aux serveurs de cloud privé.

Les appareils M-600 et M-700 utilisent des certificats de serveur pré-packagés pour authentifier les pare-feu se connectant au cloud privé PAN-DB. Vous ne pouvez pas importer ou utiliser un autre certificat de serveur pour l'authentification. Si vous modifiez le nom d'hôte sur un appareil, l'appareil génère automatique un nouveau jeu de certificats pour authentifier les pare-feu.

Équipements de cloud privé PAN-DB

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Pour déployer un cloud privé PAN-DB, vous avez besoin d'un ou plusieurs appareils M-600 ou M-700. Les deux appareils sont livrés en mode Panorama, mais pour être déployés en tant que cloud privé PAN-DB, vous devez les configurer pour fonctionner en mode PAN-URL-DB. En mode PAN-URL-DB, l'appareil propose des services de catégorisation d'URL pour les entreprises ne souhaitant pas utiliser le cloud public PAN-DB.

Les appareils M-600 et M-700, lorsqu'ils sont déployés en tant que cloud privé PAN-DB, utilisent deux ports : MGT (Eth0) et Eth1 ; le port Eth2 ne peut pas être utilisé. Le port de gestion est utilisé pour l'accès administrateur à l'appareil et pour obtenir les dernières mises à jour du contenu du cloud public PAN-DB ou d'un serveur sur votre réseau. Pour établir une communication entre le cloud privé PAN-DB et les pare-feu de votre réseau, vous pouvez utiliser le port MGT ou Eth1.

L'appareil M-200 ne peut pas être déployé en tant que cloud privé PAN-DB.

Les appareils M-600 et M-700 en mode PAN-URL-DB :

- N'est pas équipé d'une interface Web et prend donc seulement en charge une interface de ligne de commande (CLI).
- Ne peut pas être géré par Panorama.
- Ne peut pas être déployé dans une paire haute disponibilité.
- Ne nécessite pas une licence Filtrage des URL. Les pare-feu doivent disposer d'une licence Filtrage des URL PAN-DB valide pour pouvoir se connecter au cloud privé PAN-DB.
- Est fourni avec un jeu de certificats du serveur par défaut utilisés pour authentifier les pare-feu qui se connectent au cloud privé PAN-DB. Vous ne pouvez pas importer ou utiliser un autre certificat du serveur pour authentifier les pare-feu. Si vous modifiez le nom d'hôte sur un des appareils, cet appareil génère automatiquement un nouveau jeu de certificats pour authentifier les pare-feu qu'il dessert.
- Peut être réinitialisé en mode Panorama uniquement. Si vous souhaitez déployer le périphérique en tant que collecteur de journaux dédié, passez en mode Panorama et définissez-le en mode Collecteur de journaux.

Configurer le cloud privé PAN-DB

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Pour déployer un ou plusieurs appareils M-600 ou M-700 en tant que cloud privé PAN-DB dans votre réseau ou centre de données, vous devez réaliser les tâches suivantes :

- Configurer le cloud privé PAN-DB
- Configuration des pare-feu pour accéder au cloud privé PAN-DB
- Configuration de l'authentification au moyen de certificats personnalisés sur le cloud privé PAN-DB

Configuration du cloud privé PAN-DB

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

STEP 1 | Montez l'appareil M-600 ou M-700 dans une baie.

Reportez-vous aux instructions d'installation du rack dans le guide de référence matériel correspondant.

STEP 2 | Enregistrez l'appareil.

STEP 3 | Effectuez la configuration initiale de l'appareil.

Les appareils M-600 et M-700, en mode PAN-DB, utilisent deux ports : MGT (Eth0) et Eth1. Le port Eth2 n'est pas utilisé en mode PAN-DB. Le port de gestion est utilisé pour l'accès administrateur au périphérique et pour obtenir les dernières mises à jour du contenu du cloud public PAN-DB. Pour établir une communication le périphérique (serveur PAN-DB) et les pare-feu de votre réseau, vous pouvez utiliser le port MGT ou Eth1.

1. Connectez-vous à l'appareil d'une des façons suivantes :
   - Connectez un câble série à l'ordinateur et au port de console de l'appareil, puis connectez-vous en utilisant un logiciel d'émulation (9600-8-N-1).
   - Connectez un câble Ethernet RJ-45 d'un ordinateur au port MGT de l'appareil. Depuis un navigateur, accédez à https://192.168.1.1. Permettre l'accès à cette URL pourrait nécessiter de modifier l'adresse IP de l'ordinateur à une adresse dans le réseau 192.168.1.0 (par exemple, 192.168.1.2).
2. Lorsque vous y êtes invité, connectez-vous au périphérique. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe par défaut (admin/admin). Le périphérique commence son initialisation.
3. Configurez des paramètres d'accès réseau, notamment l'adresse IP de l'interface MGT :

   Utilisez la commande CLI suivante : **set deviceconfig system ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***

   Description des variables :
   - *<server-IP>* est l'adresse IP que vous souhaitez attribuer à l'interface de gestion du serveur
   - *<netmask>* est le masque de sous-réseau
   - *<gateway-IP>* est l'adresse IP de la passerelle réseau, et *<DNS-IP>* est l'adresse IP du serveur DNS principal
   - *<DNS-IP>* est l'adresse IP du serveur DNS
4. Configurez des paramètres d'accès réseau, notamment l'adresse IP de l'interface Eth1 :

   Utilisez la commande suivante : **set deviceconfig system eth1 ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***.
5. Enregistrez vos modifications sur le serveur PAN-DB.

   Utilisez la commande **valider**.

STEP 4 | Passez en mode cloud privé PAN-DB.

Vous pouvez basculer du mode Panorama au mode PAN-DB et vice-versa, et du Mode Panorama au mode Collecteur de journaux et vice-versa. Le passage direct du mode PAN-DB au mode Collecteur de journaux, ou vice versa, n'est pas possible. Le changement de mode opérationnel déclenche une réinitialisation des données. À l'exception des paramètres de Gestion de l'accès, toutes les configurations et tous les journaux existants sont supprimés au redémarrage.

1. Pour passer en mode PAN-DB, utilisez la commande **`request system-mode pan-url-db`**.
2. Pour vérifier le commutateur de mode, utilisez la commande **`show system info`**.

   Si vous avez réussi à passer en mode cloud privé PAN-DB, le champ `system-mode` affiche `PAN-URL-DB`.

```
admin@M-600> show system info  nom d'hôte : Adresse IP M-600 :
 1.2.3.4 public-ip-address: netmask: Passerelle par défaut
 255.255.255.0 : 1.2.3.1 Adresse ipv6 : adresse-locale_lien
 ipv6 inconnue : fe80:00/64 passerelle par défaut ipv6 :
 adresse mac : 00:56:90:e7:f6:8e heure: Lun Apr 27 13:43:59
 2015 disponibilité: 10 jours, 1:51:28 famille: m modèle:
 Série M-600 : 0073010000xxx sw-version: 7.0.0 app-version:
 492-2638 app-release-date: 2015/03/19 20:05:33 av-version:
 0 av-release-date: inconnu wf-private-version: 0 wf-private-
release-date: unknown wildfire-version: 0 wildfire-release-
date: logdb-version: 7.0.9 platform-family: m pan-url-db:
 20150417-220 system-mode: Pan-URL-DB operational-mode: normal
 licensed-device-capacity: 0 device-certificate-status: aucune
```

3. Pour vérifier la version de la base de données cloud sur l'appareil, utilisez la commande **`show pan-url-cloud-statut`**.

   Le champ `pan-url-db` dans l'affichage des informations système contient les mêmes informations.

STEP 5 | Installez les mises à jour du contenu et de la base de données.

L'appareil stocke uniquement la version en cours d'exécution du contenu et une version antérieure.

Choisissez l'une des méthodes d'installation suivantes :

- Si le serveur PAN-DB dispose d'un accès direct à Internet, utilisez les commandes suivantes :
  - Pour vérifier si une nouvelle version est publiée : **demander une vérification de mise à niveau pan-url-db**
  - Pour vérifier la version qui est actuellement installée sur votre serveur : **demandez des informations de mise à niveau pan-url-db**.
  - Pour télécharger la dernière version : **demander le dernier téléchargement de mise à jour pan-url**.

    Pour installer la dernière version : **demander l'installation de la mise à niveau pan-url-db <*version latest | file*>**.
  - Pour programmer l'appareil afin qu'il recherche automatiquement les mises à jour : **set deviceconfig system update-schedule pan-url-db recurring weekly action download-and-install day-of-week <*day of week*> at <*hr:min*>**.
- Si le serveur PAN-DB est hors ligne, accédez au site Web de support aux clients de Palo Alto Networks pour télécharger et enregistrer les mises à jour du contenu sur un serveur SCP sur votre réseau. Vous pouvez ensuite importer et installer les mises à jour à l'aide des commandes suivantes :
  - **scp import pan-url-db remote-port <*port-number*> depuis username@host:path**
  - **demander fichier d'installation de mise à niveau pan-url-db <*filename*>**

STEP 6 | Paramétrez l'accès administrateur au cloud privé PAN-DB.

Le périphérique dispose d'un compte `admin` par défaut. Tous les utilisateurs administrateurs supplémentaires que vous créez peuvent être des super utilisateurs (accès intégral) ou des super utilisateurs avec un accès en lecture seule.

Le cloud privé PAN-DB ne prend pas en charge l'utilisation de VSA RADIUS. Un échec d'authentification se produit si les VSA utilisés sur le pare-feu ou Panorama sont utilisés pour accéder au cloud privé PAN-DB.

- Pour configurer un utilisateur administratif local sur le serveur PAN-DB, utilisez les commandes suivantes :
  1. **configure**
  2. **set mgt-config users <*username*> permissions role-based <superreader | superuser> oui**
  3. **set mgt-config users <*username*> mot de passe**
  4. Saisir le mot de passe :**xxxxx**
  5. Confirmez le mot de passe :**xxxxx**
  6. **commit**
- Pour configurer un utilisateur administratif avec authentification RADIUS, utilisez les commandes suivantes :
  1. Pour créer un profil de serveur RADIUS : **définissez un rayon de profil de serveur partagé <*server_profile_name*> serveur <*server_name*> adresse ip <*ip_address*> port <*port_no*> secret <*shared_password*>**.
  2. Pour créer un profil d'authentification : **définissez un profil d'authentification partagé <*auth_profile_name*> domaine d'utilisateur <*domain_name_for_authentication*> liste d'autorisation <all> profil de serveur radius méthode <*server_profile_name*>**
  3. Pour joindre le profil d'authentification à un utilisateur : **définissez les utilisateurs mgt-config <*username*> profil d'authentification <*auth_profile_name*>**.
  4. Pour valider vos modifications : **valider**.
- Pour afficher la liste des utilisateurs, utilisez la commande **afficher les utilisateurs mgt-config**.

STEP 7 | Configure the firewalls to access the PAN-DB private cloud (Configurez les pare-feu pour accéder au cloud privé PAN-DB)

Configuration des pare-feu pour accéder au cloud privé PAN-DB

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Lors de l'utilisation du cloud public PAN-DB, chaque pare-feu accède aux serveurs PAN-DB du cloud AWS pour télécharger la liste des serveurs éligibles auxquels il peut se connecter pour rechercher des URL. Avec le cloud privé PAN-DB, vous devez configurer les pare-feu avec une liste (statique) de vos serveurs de cloud privé PAN-DB qui seront utilisés pour la recherche d'URL. La liste importée peut contenir jusqu'à 20 entrées ; les adresses IPv4, les adresses IPv6 et les FQDN sont pris en charge. Chaque entrée de la liste (adresse IP ou FQDN) doit être affectée au port de gestion ou eth1 du serveur PAN-DB.

STEP 1 | From the PAN-OS CLI (À partir de la CLI PAN-OS), ajoutez une liste de serveurs cloud privés PAN-DB statiques utilisés pour les recherches d'URL.

- Utilisez la commande CLI suivante pour ajouter les adresses IP des serveurs PAN-DB privés :

```
> configurer
```

```
# set deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

Ou, dans l'interface Web de chaque pare-feu, sélectionnez **Périphérique** > **Configuration** > **Content-ID**, modifiez la section de filtrage des URL et saisissez les adresses IP ou les FQDN des serveurs PAN-DB. La liste doit être séparée par des virgules.

- Pour supprimer les entrées des serveurs PAN-DB privés, utilisez la commande CLI suivante :

```
# delete deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

La suppression de la liste des serveurs PAN-DB privés déclenche un processus de réélection sur le pare-feu. Le pare-feu recherche d'abord dans la liste de serveurs cloud privés PAN-DB et, s'il n'en trouve aucun, il accède aux serveurs PAN-DB du cloud AWS pour télécharger la liste des serveurs éligibles auxquels il peut se connecter.

STEP 2 | Entrez**`# commit (valider)`** pour enregistrer vos modifications.

STEP 3 | Pour vérifier que la modification est appliquée, utilisez la commande CLI suivante sur le pare-feu :

```
> show url-cloud status Cloud status: Version de la base de données
 URL supérieure : 20150417-220
```

Configuration de l'authentification au moyen de certificats personnalisés sur le cloud privé PAN-DB

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama)	☐ Licence de filtrage des URL avancé (ou licence de filtrage des URL hérité) ***Note :*** *Les licences de filtrage des URL hérité sont abandonnées, mais les licences de filtrage hérité actives sont toujours prises en charge.*

Par défaut, un serveur PAN-DB utilise des certificats prédéfinis pour l'authentification mutuelle afin d'établir les connexions SSL utilisées pour l'accès de gestion et la communication entre appareils. Cependant, vous pouvez configurer l'authentification à l'aide de certificats personnalisés. Les certificats personnalisés vous permettent d'établir une chaîne de confiance unique pour assurer une authentification mutuelle entre votre serveur PAN-DB et vos pare-feu. Dans le cas d'un cloud privé PAN-DB, le pare-feu fait office de client et le serveur PAN-DB, de serveur.

STEP 1 | Obtenez des paires de clés et des certificats d'autorité de certification (CA) pour le serveur PAN-DB et le pare-feu.

STEP 2 | Importez le certificat d'autorité de certification pour valider le certificat sur le pare-feu.

1. Connectez-vous à la CLI du serveur PAN-DB, puis saisissez le mode de configuration.

   ```
   admin@M-600> configurer
   ```

2. Utilisez TFTP ou SCP pour importer le certificat de l'autorité de certification.

   ```
   admin@M-600# {tftp | scp} import certificate from <value>
    file <value> remote-port <1-65535> source-ip <ip/netmask>
    certificate-name <value> passphrase <value> format {pkcs12 |
    pem}
   ```

STEP 3 | Utilisez TFTP ou SCP pour importer la paire de clés contenant le certificat du serveur et la clé privée de l'appareil cloud privé.

```
admin@M-600# {tftp | scp} import keypair from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```


STEP 4 | Configurez un profil de certificat incluant l'autorité de certification racine et l'autorité de certification intermédiaire. Ce profil de certificat définit l'authentification des périphériques entre le serveur PAN-DB et le pare-feu.

1. Dans la CLI du serveur PAN-DB, saisissez le mode de configuration.

```
admin@M-600> configurer
```

2. Nommez le profil de certificat.

```
admin@M-600# set shared certificate-profile <name>
```

3. (Facultatif) Définissez le domaine d'utilisateur.

```
admin@M-600# set shared certificate-
profile <name>domain<value>
```

4. Configurez le CA.

   *Les paramètres **Default-ocsp-url** et **ocsp-verify-cert** sont facultatifs.*

admin@M-600# **set shared certificate-profile <name> CA <name>**

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [default-ocsp-url <value>]
```

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [ocsp-verify-cert <value>]
```


STEP 5 | Configurez un profil de service SSL/TLS pour l'appareil. Ce profil définit le certificat et la plage de protocoles utilisés par PAN-DB et les périphériques client pour les services SSL / TLS.

1. Identifiez le profil de service SSL/TLS.

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. Sélectionnez le certificat.

```
admin@M-600# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. Définissez la plage SSL/TLS.

   *PAN-OS 8.0 et les versions ultérieures prennent uniquement en charge les versions TLSv1.2 et les versions TLS ultérieures. Vous devez définir la version maximale sur **TLS 1.2** ou sur **max**.*

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 | max
```

STEP 6 | Configurez la communication sécurisée avec le serveur sur PAN-DB.

1. Définissez le profil de service SSL/TLS. Ce profil s'applique à toutes les connexions SSL entre PAN-DB et les pare-feu.

```
admin@M-600# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. Définissez le profil de certificat.

```
admin@M-600# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

3. Définissez le délai d'attente de déconnexion. Il s'agit du nombre de minutes que PAN-DB attend avant d'interrompre et de rétablir la connexion avec son pare-feu (la plage est comprise entre 0 et 44 640).

```
admin@M-600# set deviceconfig setting management secure-conn-
server disconnect-wait-time <0-44640
```

STEP 7 | Importez le certificat CA pour valider le certificat de l'appareil.

1. Connectez-vous à l'interface Web du pare-feu.
2. Importez le certificat de l'autorité de certification.

STEP 8 | Configurez un certificat local ou SCEP pour le pare-feu.

1. Si vous configurez un certificat local, importez la paire clé pour le pare-feu.
2. Si vous configurez un certificat SCEP, configurez un profil SCEP.

STEP 9 | Configurez le profil de certificat sur le pare-feu. Vous pouvez le configurer sur chaque pare-feu individuellement ou vous pouvez envoyer cette configuration de Panorama aux périphériques dans le cadre d'un modèle.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil du certificat)** pour les pare-feu ou **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil du certificat)** pour Panorama.
2. Configuration d'un profil de certificat.

STEP 10 | Déployez des certificats personnalisés sur chaque pare-feu. Vous pouvez déployer des certificats de manière centralisée à partir de Panorama ou le configurer manuellement sur chaque pare-feu.

1. Connectez-vous à l'interface Web du pare-feu.
2. Sélectionnez **Périphérique** > **Configuration** > **Gestion** pour un pare-feu ou **Panorama** > **Configuration** > **Gestion** pour Panorama et **Editez** la communication sécurisée paramètres.
3. Sélectionnez le **Certificate Type (type de certificat)**, le **Certificate (Certificat)**, et le **Certificate Profile (profil du certificat)** dans leurs menus déroulants respectifs.
4. Sous Customize Communication (Personnaliser la communication), sélectionnez **PAN-DB Communication (Communication PAN-DB)**.
5. Cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

   Une fois vos changements validés, les pare-feu ne mettent pas fin aux sessions actives avec le serveur PAN-DB tant que le **Délai d'attente de déconnexion** n'a pas été atteint. Le délai d'attente de déconnexion commence le compte à rebours après que vous appliquez l'utilisation des certificats personnalisés à l'étape suivante.

STEP 11 | Appliquer l'authentification par certificat personnalisé.

1. Connectez-vous à la CLI du serveur PAN-DB, puis saisissez le mode de configuration.

   ```
   admin@M-600> configurer
   ```

2. Appliquez l'utilisation des certificats personnalisés.

   ```
   admin@M-600# set deviceconfig setting management secure-conn-
   server disable-pre-defined-cert yes
   ```

Une fois ce changement validé, le délai d'attente de déconnexion commence son compte à rebours (si vous avez configuré ce paramètre sur PAN-DB). Lorsque le délai d'attente de déconnexion prend fin, PAN-DB et son pare-feu se connectent au moyen des certificats configurés uniquement.

STEP 12 | Deux choix s'offrent à vous lorsque vient le temps d'ajouter de nouveaux pare-feu ou Panorama à votre déploiement de cloud privé PAN-DB.

- Si vous n'avez pas activé **Certificats personnalisés uniquement**, vous pouvez ajouter un nouveau pare-feu au cloud privé PAN-DB, puis déployer le certificat personnalisé.
- Si vous avez activé l'option **Certificats personnalisés uniquement** sur le cloud privé PAN-DB, vous devez déployer les certificats personnalisés sur les pare-feu avant de les connecter au cloud privé PAN-DB.

