paloalto TECHDOCS

# Administration Advanced WildFire

docs.paloaltonetworks.com

## 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

June 29, 2023

# Table of Contents



# Présentation d'Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Advanced WildFire™ assure la détection et la prévention de logiciels malveillants de type « zero-day » en combinant des analyses dynamiques et statiques ainsi qu'une analyse de la mémoire d'exécution intelligente en vue de détecter les menaces très évasives et de créer des protections pour bloquer les logiciels malveillants.

L'environnement d'analyse Advanced WildFire identifie les logiciels malveillants inconnus jusqu'alors et génère des signatures que les NGFW Palo Alto Networks peuvent utiliser pour détecter et bloquer ensuite le logiciel malveillant. Lorsqu'un pare-feu Palo Alto Networks détecte un échantillon inconnu, le pare-feu transmet automatiquement tous les types de fichiers pris en charge de n'importe quelle application au service de cloud WildFire public pour une analyse Advanced WildFire. Basé sur les propriétés, les comportements et les activités que l'échantillon affiche lorsqu'il est analysé et exécuté dans le sandbox, Advanced WildFire détermine que l'échantillon est bénin, indésirable, lié à l'hameçonnage ou malveillant, puis génère des signatures pour reconnaître le logiciel malveillant nouvellement découvert, et rend les dernières signatures mondialement disponibles pour la récupération en temps réel. Tous les pare-feu Palo Alto Networks peuvent alors comparer les échantillons entrants à ces signatures pour bloquer automatiquement le logiciel malveillant détecté en premier par un seul pare-feu.

Pour en savoir plus sur Avanced WildFire ou pour faire vos premiers pas, consultez les sujets suivants :

- Passez en revue les concepts d'Advanced WildFire pour en apprendre davantage sur les types d'échantillons que vous pouvez transférer pour analyse WildFire, sur les verdicts de WildFire et sur les signatures WildFire.
- Apprenez-en davantage sur les déploiements Advanced WildFire que vous pouvez configurer sur le pare-feu. Vous pouvez transférer les échantillons que vous souhaitez analyser à un cloud WildFire hébergé par Palo Alto Networks ou à un cloud WildFire privé hébergé localement, ou vous pouvez utiliser un cloud hybride, où le pare-feu envoie certains échantillons au cloud public et certains échantillons à un cloud privé.
- Premiers pas avec Advanced WildFire pour définir les échantillons que vous souhaitez transférer à des fins d'analyse et pour commencer à envoyer des échantillons à un cloud WildFire.
- Si vous déployez un appareil WildFire, reportez-vous à l'administration de WildFire Appliance.

# Options d’abonnement

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Le service WildFire de base est inclus dans le cadre des pare-feu Palo Alto Networks de nouvelle génération et n’exige aucun abonnement Advanced WildFire. Avec le service WildFire de base, le pare-feu peut transférer les fichiers exécutables portables (PE) pour analyse et peut récupérer les signatures Advanced WildFire uniquement avec les mises à jour antivirus et/ou de prévention des menaces qui sont mises à disposition toutes les 24-48 heures.

Palo Alto Networks propose plusieurs options d’abonnement :

- **WildFire** : l’abonnement WildFire offre une protection contre les logiciels malveillants en transférant des échantillons vers le cloud Advanced WildFire où une série d’environnements d’analyse sont utilisés pour détecter et prévenir les menaces de logiciels malveillants inconnus en générant des protections permettant de bloquer d’autres instances de la menace. Dans le cadre de votre abonnement, vous avez accès aux mises à jour régulières des signatures Advanced WildFire, au transfert avancé des types de fichiers, ainsi qu’à la possibilité de charger des fichiers à l’aide de l’API WildFire. Si vous exploitez un environnement qui nécessite une solution sur site, l’abonnement WildFire peut être utilisé pour transférer des fichiers vers un appareil WildFire local.
- **Advanced WildFire** (PAN-OS 10.0 et versions ultérieures) : l’abonnement Advanced WildFire inclut toutes les fonctionnalités de l’abonnement WildFire standard et l’améliore en fournissant une analyse d’échantillons via un détecteur avancé basé sur le cloud. Le système de détection avancé analyse les échantillons à l’aide d’une analyse intelligente de la mémoire d’exécution en temps réel, de l’émulation de DLL d’exécution, de la décompression automatisée, de la classification des familles, de l’observation furtive et d’autres techniques pour cibler les logiciels malveillants hautement évasifs.
- **API WildFire autonome** : les clients de Palo Alto Networks exploitant des outils SOAR, des applications de sécurité personnalisées et d’autres logiciels d’évaluation des menaces peuvent accéder aux capacités avancées d’analyse de fichiers du cloud WildFire avec un abonnement autonome qui fournit un accès API uniquement. Cela vous permet de tirer parti des analyses basées sur WildFire sans compter sur le pare-feu Palo Alto Networks comme mécanisme de transfert. L’abonnement à l’API WildFire autonome vous permet d’effectuer des requêtes directes à la base de données des menaces cloud WildFire pour obtenir des informations sur le contenu potentiellement malveillant et de soumettre des fichiers pour analyse à l’aide des fonctionnalités avancées d’analyse des menaces de WildFire, en fonction des besoins spécifiques de votre organisation. Les limites d’accès améliorées de l’abonnement permettent aux organisations de différentes tailles de personnaliser leurs limites d’accès en fonction de leur utilisation, notamment des licences évolutives qui permettent un nombre spécifique de requêtes de fichiers/rapports, de soumissions d’échantillons (pour l’analyse Advanced WildFire)

ou une combinaison des deux. Pour plus d'informations, consultez le Guide de référence de l'API WildFire.

L'abonnement WildFire standard débloque les fonctionnalités suivantes :

- **Mises à jour en temps réel de WildFire**(version PAN-OS 10.0 et versions ultérieures) : le pare-feu peut récupérer les signatures WildFire des nouveaux logiciels malveillants dès que le cloud Advanced WildFire public est en mesure de les générer. Les signatures qui sont téléchargées au cours d'une vérification d'échantillon sont enregistrées dans la mémoire cache du pare-feu et sont disponibles pour des recherches rapides (locales). De plus, afin de maximiser la couverture, le pare-feu téléchargera aussi automatiquement un package de signatures de façon régulière lorsque les signatures en temps réel sont activées. Ces signatures complémentaires sont ajoutées à la mémoire cache du pare-feu et restent disponibles jusqu'à ce qu'elles soient dépassées, actualisées ou remplacées par de nouvelles signatures. Il est conseillé d'utiliser les mises à jour Advanced WildFire en temps réel dans le cadre des meilleures pratiques.

  Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** et configurez le pare-feu pour qu'il obtienne les dernières signatures Advanced WildFire en temps réel.

- **Five-Minute Updates (Mises à jour en cinq minutes)** : (pour toutes les versions PAN-OS) le cloud public Advanced WildFire peut générer et distribuer les signatures Advanced WildFire des logiciels malveillants nouvellement découverts toutes les cinq minutes, et vous pouvez configurer le pare-feu pour qu'il récupère et installe ces signatures toutes les minutes (cela permet au pare-feu d'obtenir les dernières signatures dans un délai d'une minute à compter de leur mise à disposition).

  *Si vous exécutez PAN-OS 10.0 ou une version ultérieure, il est recommandé d'utiliser des mises à jour avancées Advanced WildFire en temps réel au lieu de planifier des mises à jour récurrentes.*

  Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** pour activer le pare-feu et obtenir les dernières signatures Advanced WildFire. En fonction de votre déploiement d'Advanced WildFire, vous pouvez configurer une des mises à jour de package de signatures suivantes ou les deux :

  - **WildFire** : obtenez les dernières signatures depuis le cloud WildFire public.
  - **WF-Private (WF-privé)**: obtenez les dernières signatures d'un appareil WildFire configuré pour générer localement des signatures et des catégories d'URL.

- **Advanced WildFire Inline ML** : (PAN-OS 10.0 et versions ultérieures) empêchez les variantes malveillantes de fichiers exécutables portables (PE), au format exécutable et lié (ELF) et les scripts PowerShell de pénétrer votre réseau en temps réel à l'aide de l'apprentissage machine (ML) sur le plan de données du pare-feu. En utilisant la technologie d'analyse du cloud Advanced WildFire sur le pare-feu, Advanced WildFire Inline ML détecte dynamiquement les fichiers malveillants d'un type donné en évaluant plusieurs détails du fichier, y compris les champs et schémas du décodeur, afin de formuler une classification à forte probabilité d'un fichier. Cette protection s'étend aux variantes actuellement inconnues et aux variantes futures des menaces qui correspondent aux caractéristiques que Palo Alto Networks a identifiées comme étant malveillantes. Advanced WildFire inline ML complète la configuration de protection de votre profil Antivirus. Par ailleurs, vous pouvez préciser des exception de hachage de fichier afin d'exclure les faux positifs rencontrés, ce qui vous permet de créer des règles plus fines pour répondre à vos besoins de sécurité spécifiques.
- **Prise en charge des types de fichiers avancés** : en plus des PE, transférez des types de fichiers avancés pour l'analyse WildFire, y compris les fichiers APK, Flash, PDF, Microsoft Office, applets

Java, fichiers Java (.jar et .class), ainsi que les liens d’e-mail HTTP/HTTPS contenus dans les messages électroniques SMTP et POP3. L’analyse du cloud WildFire privé ne prend pas en charge les fichiers APK, Mac OS X, Linux (ELF), d’archive (RAR/7-Zip) et de script (JS, VBS, Shell Script, PS1 et HTA)

- **API Advanced WildFire** : accédez à l’API WildFire, qui permet un accès direct de programmation au cloud Advanced WildFire public ou à un cloud WildFire privé. Utilisez l’API pour envoyer des fichiers pour analyse et pour extraire les rapports d’analyse Advanced WildFire subséquents. Dans le cadre de l’abonnement Advanced WildFire ou Wildfire, vous pouvez soumettre jusqu’à 150 exemples de soumissions et jusqu’à 1 050 exemples de requêtes par jour. Ces limites quotidiennes de soumission d'échantillons peuvent être étendues en fonction des besoins spécifiques de votre organisation. Veuillez contacter votre représentant commercial Palo Alto Networks pour plus d'informations.
- **Prise en charge du cloud privé et hybride WildFire** :Transfert des fichiers pour une analyse par Advanced WildFire. Les déploiements de cloud WildFire privé et cloud WildFire hybride exigent tous deux que le pare-feu soit capable d'envoyer les échantillons à un appareil WildFire. L'activation d'un appareil WildFire n'exige qu'une licence de support.

Si vous avez acheté un abonnement Advanced WildFire, vous devez activer la licence avant de pouvoir bénéficier des fonctionnalités WildFire réservées aux abonnements.

L’abonnement Advanced WildFire déverrouille la fonctionnalité suivante :

- **Analyse intelligente de la mémoire d’exécution** : l’analyse intelligente de la mémoire d’exécution est un moteur d’analyse avancé basé sur le cloud qui complète les moteurs d’analyse statique et dynamique, afin de détecter et de prévenir les menaces évasives de logiciels malveillants. Ces techniques évasives utilisées par les menaces avancées incluent, sans toutefois s’y limiter, les logiciels malveillants utilisant des stratégies de dissimulation, affichant des signes de conception sur mesure / comportements éphémères, créés à l’aide d’outils sophistiqués et présentant des qualités de propagation rapide. En tirant parti d’une infrastructure de détection basée sur le cloud, les détecteurs d’analyse introspective exploitent un large éventail de mécanismes de détection qui sont mis à jour et déployés automatiquement sans que l’utilisateur ait besoin de télécharger des packages de mise à jour de contenu ou d’exécuter des analyseurs gourmands en ressources basés sur des appareils. Les moteurs de détection basés sur le cloud sont surveillés et mis à jour en permanence à l’aide d’ensembles de données basés sur le ML utilisés pour analyser les échantillons Advanced WildFire, avec le soutien supplémentaire des chercheurs sur les menaces de Palo Alto Networks, qui fournissent une intervention humaine pour des améliorations de détection hautement précises.

  L’analyse intelligente de la mémoire d’exécution repose sur les paramètres de profil d’analyse WildFire existants et ne nécessite aucune configuration supplémentaire ; cependant, vous devez disposer d’une licence Advanced WildFire active. Les échantillons qui affichent ou indiquent des qualités de logiciels malveillants évasifs et/ou avancés sont automatiquement transmis aux environnements d’analyse appropriés.

# Concepts Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

- Échantillons
- Transfert du pare-feu
- Partage des informations de session
- Environnement d'analyse
- Analyse du cloud en ligne Advanced WildFire
- Advanced WildFire Inline ML
- Verdicts
- Analyse de fichiers
- Analyse de liens d'e-mail WildFire
- Analyse d’URL
- Analyse de fichier compressé et codé
- Signatures Advanced WildFire
- Exemple Advanced WildFire

## Échantillons

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Les échantillons sont tous des types de fichiers et des liens d'e-mail soumis par le pare-feu et l'API publique pour analyse Advanced WildFire. Reportez-vous à la section Analyse de fichiers et à la section Analyse de liens d'e-mail WildFire pour plus de détails sur les types de fichiers et les liens qu'un pare-feu peut envoyer pour l'analyse Advanced WildFire.

## Transfert du pare-feu

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Le pare-feu transfère les échantillons inconnus, ainsi que les fichiers bloqués qui correspondent aux signatures antivirus, pour l'analyse Advanced WildFire selon les paramètres de profil d'analyse WildFire configurés (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **WildFire Analysis (Analyse WildFire)**). En plus de détecter les liens inclus dans les e-mails, les fichiers joints aux e-mails et les téléchargements de fichiers par navigateur, le pare-feu tire parti de l'ID d'application pour détecter les transferts de fichiers dans les applications. Le pare-feu analyse la structure et le contenu des échantillons qu'il détecte et les compare aux signatures existantes. Si l'échantillon correspond à une signature, le pare-feu applique l'action définie par défaut pour cette signature (autoriser, alerter ou bloquer). Si l'échantillon correspond à une signature antivirus ou si l'échantillon reste inconnu après la comparaison avec les signatures Advanced WildFire, le pare-feu le transfère pour l'analyse Advanced WildFire.

Par défaut, le pare-feu transfère également les renseignements sur la session au cours de laquelle un échantillon inconnu a été détecté. Pour gérer les renseignements sur la session que le pare-feu transfère, sélectionnez **Device (Périphétique)** > **Setup (Configuration)** > **WildFire (WildFire)**, puis modifiez la section Session Information Settings (Paramètres des informations de session).

## Partage des informations de session

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

En plus de transférer des échantillons inconnus et bloqués aux fins d’analyse, le pare-feu transmet également des informations sur la session réseau qui concerne un échantillon. Palo Alto Networks utilise les informations de session pour en apprendre davantage sur le contexte entourant l’événement réseau suspect, sur les indicateurs d'exploitation liés au fichier malveillant, sur les hôtes et les clients affectés ainsi que sur les applications utilisées pour transmettre le fichier malveillant.

Le transfert des informations de session est activé par défaut. Vous pouvez toutefois ajuster les paramètres par défaut et décider du type d’informations de session à transférer vers l’une des options du cloud WildFire.

- Strata Cloud Manager
- PAN-OS et Panorama

## Partage d’informations de session (Cloud Management)

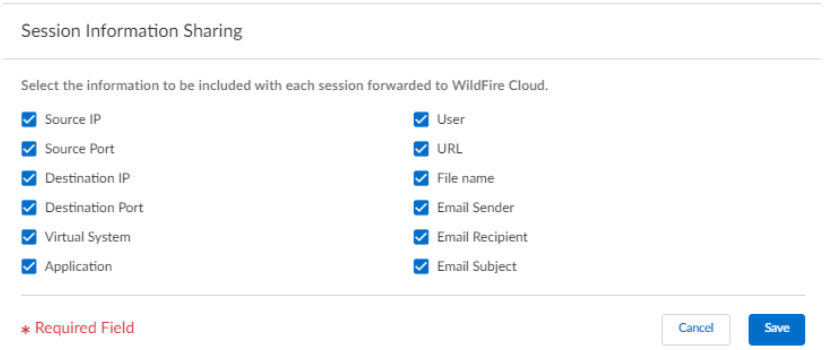
***Si vous utilisez Panorama pour gérer Prisma Access :***

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

***Si vous utilisez Prisma Access Cloud Management, continuez ici.***

**STEP 1 |** Utilisez les informations d’identification associées à votre compte de support Palo Alto Networks et connectez-vous à Strata Cloud Manager l’application sur le hub.

**STEP 2 |** Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and PA (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **WildFire and Antivirus (WildFire et antivirus)** et configurez vos options **Session Information Settings (Paramètres d’informations de session)**.




- **Source IP (Adresse IP source)** : transfère l’adresse IP source ayant envoyé le fichier inconnu.
- **Source Port (Port source)** : transfère le port source ayant envoyé le fichier inconnu.
- **Destination IP (Adresse IP de destination)** : transfère l’adresse IP de destination ayant envoyé le fichier inconnu.
- **Destination Port (Port de destination)** : transfère le port de destination ayant envoyé le fichier inconnu.
- **Virtual System (Système virtuel)** : transfère le système virtuel ayant détecté le fichier inconnu.
- **Application (Application)** : transfère l’application utilisateur ayant transmis le fichier inconnu.
- **User (Utilisateur)** : transfère l’utilisateur ciblé.
- **URL (URL)** : transfère l’URL associée au fichier inconnu.

- **Filename (Nom du fichier)** : transfère le nom du fichier inconnu.
- **Email sender (Expéditeur de l'e-mail)** : transfère l'expéditeur du lien d’e-mail inconnu (le nom de l’expéditeur de l'e-mail apparaît également dans les rapports et journaux WildFire).
- **Email recipient (Destinataire de l'e-mail)** : transfère le destinataire du lien d’e-mail inconnu (le nom du destinataire de l'e-mail apparaît également dans les rapports et journaux WildFire).
- **Email subject (Objet de l'e-mail)** : transfère l'objet du lien d’e-mail inconnu (l’objet de l'e-mail apparaît également dans les rapports et journaux WildFire).

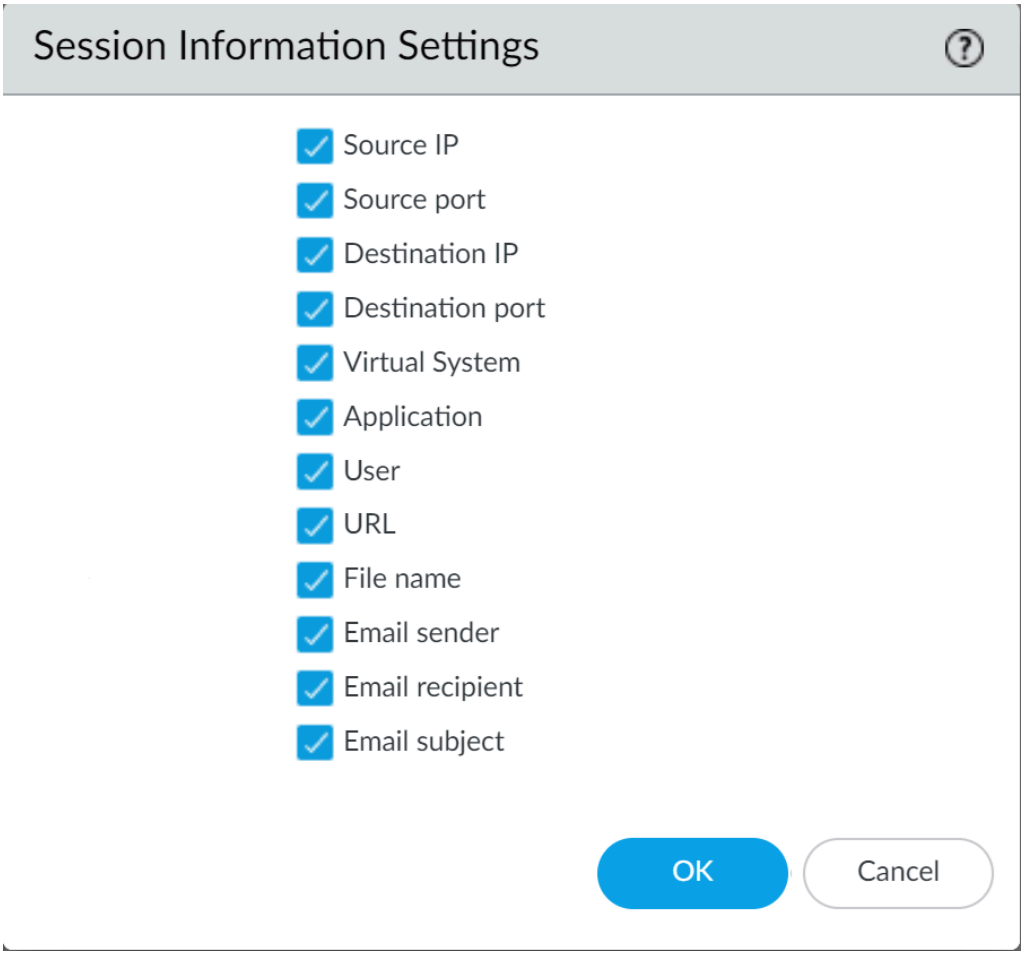
**STEP 3 |** Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

## Partage d’informations de session (PAN-OS et Panorama)

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

**STEP 2 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire**, puis cochez ou décochez les options suivantes des **Session Information Settings (Paramètres des informations de session)**.




- **Source IP (Adresse IP source)** : transfère l’adresse IP source ayant envoyé le fichier inconnu.
- **Source Port (Port source)** : transfère le port source ayant envoyé le fichier inconnu.
- **Destination IP (Adresse IP de destination)** : transfère l’adresse IP de destination ayant envoyé le fichier inconnu.
- **Destination Port (Port de destination)** : transfère le port de destination ayant envoyé le fichier inconnu.
- **Virtual System (Système virtuel)** : transfère le système virtuel ayant détecté le fichier inconnu.
- **Application (Application)** : transfère l’application utilisateur ayant transmis le fichier inconnu.
- **User (Utilisateur)** : transfère l’utilisateur ciblé.
- **URL (URL)** : transfère l’URL associée au fichier inconnu.
- **Filename (Nom du fichier)** : transfère le nom du fichier inconnu.
- **Email sender (Expéditeur de l'e-mail)** : transfère l'expéditeur du lien d’e-mail inconnu (le nom de l’expéditeur de l'e-mail apparaît également dans les rapports et journaux WildFire).
- **Email recipient (Destinataire de l'e-mail)** : transfère le destinataire du lien d’e-mail inconnu (le nom du destinataire de l'e-mail apparaît également dans les rapports et journaux WildFire).

- **Email subject (Objet de l'e-mail)** : transfère l'objet du lien d’e-mail inconnu (l’objet de l'e-mail apparaît également dans les rapports et journaux WildFire).

**STEP 3 |** Cliquez sur **OK** pour enregistrer vos modifications.

## Environnement d'analyse

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Advanced WildFire reproduit une diversité d’environnements d’analyse, dont le système d’exploitation, pour déceler les comportements malveillants dans les échantillons. Selon les caractéristiques et fonctionnalités de l’échantillon, plusieurs environnements d’analyse peuvent être utilisés pour déterminer la nature du fichier. Advanced WildFire se sert d’une analyse statique par apprentissage automatique pour déterminer, dans un premier temps, si les échantillons connus et leurs variantes sont malveillants. Selon le verdict initial de l’envoi, Advanced WildFire transmet les échantillons inconnus aux environnements d’analyse afin d’inspecter le fichier plus en détail en extrayant des indicateurs et des renseignements supplémentaires à partir de l’analyse dynamique. Si le fichier a été décodé au moyen de méthodes personnalisées ou open source, le cloud Advanced WildFire décompresse et déchiffre le fichier dans la mémoire au sein de l’environnement d’analyse dynamique avant de l’analyser au moyen de l’analyse statique. Lors de l’analyse dynamique, Advanced WildFire observe le comportement qu’aurait le fichier lors de son exécution dans les systèmes client et reste à l’affût de divers signes d’activités malveillantes, telles que la modification des paramètres de sécurité du navigateur, l’injection de code dans d’autres processus, la modification de fichiers dans les dossiers du système d’exploitation ou de tentatives de la part de l’échantillon d’accéder à des domaines malveillants. De plus, les PCAP générés pendant l’analyse dynamique dans le cloud Advanced WildFire font l’objet d’une inspection approfondie et sont utilisés pour créer des profils d’activités réseau. Les profils de trafic réseau peuvent détecter les logiciels malveillants connus et les logiciels malveillants inconnus jusqu'alors au moyen d’une correspondance entre un profil et plusieurs profils.

Advanced WildFire peut analyser les fichiers à l’aide des méthodes suivantes, en fonction des caractéristiques de l’échantillon :

- **Static Analysis (Analyse statique)** : détecte les menaces connues en analysant les caractéristiques des échantillons avant leur exécution.
- **Machine Learning (Apprentissage automatique)** : décèle les variantes des menaces connues en comparant les ensembles de fonctionnalités des logiciels malveillants aux systèmes de classification mis à jour dynamiquement.

- **Dynamic Unpacking (WildFire Cloud global cloud only) (Dépaquetage dynamique [Cloud Advanced WildFire global uniquement])** : détermine les fichiers qui ont été chiffrés au moyen des méthodes personnalisées ou open source, les dépaquette et les prépare aux fins d’analyse statique.
- **Dynamic Analysis (Analyse dynamique)** : un environnement virtuel résistant aux fuites dans lequel des échantillons jusqu’alors inconnus sont détonés pour en déterminer le comportement et les effets réels.
- **Intelligent Run-time Memory Analysis (Advanced WildFire License | Advanced WildFire global cloud only — requires PAN-OS 10.0 and later on NGFWs) (Analyse intelligente de la mémoire d’exécution [Licence Advanced WildFire | Cloud Advanced WildFire global uniquement – nécessite PAN-OS 10.0 ou version ultérieure sur les NGFW])** : environnement d’analyse basé sur le cloud exploitant des détecteurs avancés utilisés pour analyser les menaces modernes utilisant une multitude de techniques d’évasion.

Advanced WildFire effectue l’analyse des environnements qui imitent les systèmes d’exploitation suivants :

- **Microsoft Windows XP 32 bits (pris en charge comme option pour le cloud privé WildFire uniquement)**
- **Microsoft Windows 7 64 bits**
- **Microsoft Windows 7 32 bits (pris en charge comme option pour le cloud privé Wildfire uniquement)**
- **Microsoft Windows 10 64 bits (pris en charge en option pour le cloud Advanced WildFire public et le cloud privé WildFire exécutant PAN-OS 10.0 ou une version ultérieure)**
- **Mac OS X (cloud Advanced WildFire public uniquement)**
- **Android (cloud Advanced WildFire public uniquement)**
- **Linux (cloud Advanced WildFire public uniquement)**

Le cloud Advanced WildFire public analyse également les fichiers à partir de plusieurs versions du logiciel dans le but de bien identifier les logiciels malveillants qui ciblent des versions bien précises des applications client. Le cloud WildFire privé ne prend pas en charge l’analyse sur plusieurs versions et n’analyse pas de fichiers propres à certaines applications sur plusieurs versions.

## Analyse du cloud en ligne Advanced WildFire

| Où puis-je l’utiliser ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

Le cloud Advanced WildFire exploite une série de moteurs de détection en ligne basés sur le ML du cloud en ligne pour analyser les échantillons PE (Portable Executable) traversant votre réseau afin de détecter et d’empêcher les logiciels malveillants inconnus de nuire, le tout en temps réel. Cela permet au service cloud Advanced WildFire de détecter des logiciels malveillants inconnus jusqu’à présent (qui n'ont pas de signature WildFire existante ou qui sont détectables via les détecteurs ML cloud en ligne Advanced WildFire locaux) et de les empêcher d’infecter le client. Cela inclut des scénarios où certains types de

logiciels malveillants inconnus jusqu'à présent, et qui ne sont pas interceptés par Advanced WildFire Inline ML, peuvent continuer sans entrave parce que le fichier n'a pas été vu assez récemment pour que sa signature soit présente sur le pare-feu en raison de l'expiration de la signature ou des limites de capacité de la base de données de signatures. Les fichiers malveillants nouvellement définis seront bloqués lors de rencontres ultérieures par le pare-feu, car la signature est devenue une partie de l'ensemble actuel, qui se produit cependant après l'analyse d'un fichier malveillant par le cloud WildFire.

Le cloud en ligne Advanced WildFire peut empêcher des fichiers de se télécharger (et potentiellement de se propager au sein de votre réseau) tout en analysant ces fichiers suspects pour y rechercher des logiciels malveillants dans le cloud, dans un échange en temps réel. Comme pour les autres contenus malveillants analysés par WildFire, toute menace détectée par le cloud en ligne Advanced WildFire génère une signature de menace qui est diffusée par Palo Alto Networks aux clients via un package de mise à jour de signature pour fournir une défense future à tous les clients de Palo Alto Networks.

Le cloud en ligne Advanced WildFire fonctionne à l'aide d'un mécanisme de redirection léger sur le pare-feu pour minimiser tout impact local sur les performances; et pour suivre les derniers changements dans le paysage des menaces, des modèles de détection ML en ligne dans le cloud sont ajoutés et mis à jour en toute transparence dans le cloud, sans nécessiter de mises à jour de contenu ou de prise en charge de la publication de fonctionnalités.

L'analyse du cloud en ligne Advanced WildFire est activée et configurée via le profil l'analyse WildFire et nécessite PAN-OS 11.1 ou une version ultérieure avec une licence Advanced WildFire active.

## Advanced WildFire Inline ML

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

L'option ML en ligne Advanced WildFire dans les profils d'antivirus permet aux plan de données du pare-feu d'appliquer l'apprentissage automatique aux fichiers PE (Portable Executable), ELF (format exécutable et lié) et MS Office, à OOXML, à Mach-O et aux scripts Powershell et shell en temps réel. Cette couche de protection antivirus complète les signatures basées sur Advanced WildFire afin de fournir une couverture étendue pour les fichiers dont les signatures n'existent pas encore. Chaque modèle ML détecte dynamiquement les fichiers malveillants d'un type donné en évaluant les détails du fichier, y compris les champs et schémas du décodeur, afin de formuler une classification à forte probabilité d'un fichier. Cette protection s'étend aux variantes actuellement inconnues et aux variantes futures des menaces qui correspondent aux caractéristiques que Palo Alto Networks a identifiées comme étant malveillantes. Afin d'être au courant des dernières évolutions des menaces, les modèles Inline ML sont ajoutés ou mis à jour via des communiqués de contenu. Avant de pouvoir activer Advanced WildFire inline ML, vous devez posséder un abonnement Advanced WildFire ou WildFire standard actif.

La protection basée sur Inline ML peut également être activée pour détecter les URL malveillantes en temps réel dans le cadre de la configuration de votre URL Filtering.

*Advanced WildFire Inline ML n’est pas pris en charge sur l’appareil virtuel VM-50 ou VM50L.*

## Verdicts

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Lorsque Advanced WildFire analyse des échantillons jusqu’alors inconnus dans le cloud WildFire global hébergé par Palo Alto Networks ou dans un cloud Advanced WildFire privé hébergé localement, un verdict est rendu afin de les identifier comme étant malveillants, indésirables (les échantillons indésirables sont considérés comme dérangeants, mais pas malveillants) ou bénins, ou de l’hameçonnage :

- **Bénin** : l'échantillon est sûr et ne manifeste aucun comportement malveillant.
- **Logiciel indésirable** : l'échantillon n'entraîne pas une menace de sécurité directe, mais peut présenter un comportement indiscret. Les logiciels indésirables incluent généralement les logiciels publicitaires, les logiciels espions et les Browser Helper Objects (objets de l’assistant du navigateur - BHO).
- **Hameçonnage** : le lien dirige les utilisateurs vers un site d’hameçonnage et présente un risque de sécurité. 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 mots de passe d’entreprise qui permettent d’accéder à votre réseau. L’appareil WildFire ne prend pas en charge le verdict d’hameçonnage et continue de classer ces types de liens comme étant malveillants.
- **Malveillant** : l'échantillon est un logiciel malveillant et présente une menace de sécurité. Les logiciels malveillants peuvent inclure les virus, les vers, les chevaux de Troie, Remote Access Tools (outils à accès distant - RAT), les rootkits et les Botnets. Pour les fichiers identifiés comme des logiciels malveillants, des signatures sont générées et distribuées pour empêcher toute exposition future à la menace.

Chaque cloud Advanced WildFire (global, États-Unis et régional) et le cloud privé WildFire analysent des échantillons et génèrent des verdicts WildFire indépendamment des autres options de cloud WildFire. À l’exception des verdicts du cloud WildFire privé, les verdicts sont transmis globalement, ce qui permet aux utilisateurs d’Advanced WildFire d’accéder à une base de données sur les menaces mondiale.

*Si vous pensez que le verdict est un faux positif ou un faux négatif, vous pouvez le transmettre à l’équipe de prévention des menaces de Palo Alto Networks, qui effectuera une analyse plus poussée. Vous pouvez également manuellement modifier les verdicts des échantillons envoyés aux appareils WildFire.*

## Analyse de fichiers

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Un pare-feu Palo Alto Networks sur lequel un profil d’analyse WildFire est configuré transfère les échantillons pour analyse Advanced WildFire selon le type de fichier (y compris les liens d’e-mail). En outre, le pare-feu décode les fichiers qui ont été codés ou compressés jusqu’à quatre fois (comme les fichiers au format ZIP) ; si le fichier décodé correspond à un critère de profil d’analyse Advanced WildFire, le pare-feu transfère le fichier décodé pour analyse.

Les capacités d’analyse d’Advanced WildFire peuvent aussi être activées sur le pare-feu afin de fournir une protection antivirus connectée. L’option inline ML d’Advanced WildFire dans les profils d’antivirus permet aux plan de données du pare-feu d’appliquer une analyse d’apprentissage machine aux fichiers PE et ELF et aux scripts PowerShell en temps réel. Chaque modèle ML détecte dynamiquement les fichiers malveillants d’un type donné en évaluant les détails du fichier, y compris les champs et schémas du décodeur, afin de formuler une classification à forte probabilité d’un fichier. Cette protection s’étend aux variantes actuellement inconnues et aux variantes futures des menaces qui correspondent aux caractéristiques que Palo Alto Networks a identifiées comme étant malveillantes. Afin d’être au courant des dernières évolutions des menaces, les modèles Inline ML sont ajoutés ou mis à jour via des communiqués de contenu. Pour plus d'informations, reportez-vous à la section Advanced WildFire Inline ML.

Le cloud Advanced WildFire est également capable d’analyser certains types de fichiers, qui servent de charges utiles secondaires dans les programmes malveillants PE, APK et ELF multi-étapes. L’analyse des charges utiles secondaires peuvent procurer une protection supplémentaire pour perturber les attaques sophistiquées menées dans le cadre de menaces avancées. Le fonctionnement de ces menaces avancées repose sur l’exécution du code, qui active des charges utiles malveillantes supplémentaires, y compris celles conçues pour contourner les mesures de sécurité ainsi que pour favoriser la prolifération de la charge utile principale. Advanced WildFire analyse les menaces multi-étapes en les traitant dans des environnements d’analyse statiques et dynamiques. Les fichiers référencés par des logiciels malveillants multi-étapes sont traités indépendamment au cours de l’analyse. Par conséquent, les verdicts et les protections sont transmis au fur et à mesure qu’ils sont terminés pour chaque fichier. Le verdict global du fichier multi-étape repose sur une évaluation des menaces que pose le contenu malveillant découvert à toutes les étapes analysées de l’attaque. Le fichier multi-étape est identifié comme étant malveillant dès que du contenu malveillant est découvert au cours de son analyse.

Les entreprises qui ont des procédures de traitement en toute sécurité du contenu malveillant peuvent envoyer manuellement des échantillons protégés par un mot de passe en utilisant le format RAR via l’API ou le portail WildFire. Lorsque le cloud Advanced WildFire reçoit un échantillon qui a été crypté à l’aide d’un mot de passe *infected (infecté)* ou un *virus*, le cloud Advanced WildFire décrypte et analyse le fichier d’archive. Vous pouvez afficher le verdict et les résultats de l’analyse pour le fichier au format dans lequel il a été reçu, dans ce cas, une archive.

Bien que le pare-feu puisse transférer tous les types de fichiers indiqués ci-dessous, les fichiers pris en charge pour analyse Advanced WildFire dépendront du cloud Advanced WildFire auquel vous transmettez les échantillons. Passez en revue la section Prise en charge des types de fichiers Advanced WildFire pour en apprendre davantage à cet égard.

| Types de fichier pris en charge pour le transfert WildFire | Description |
|---|---|
| `apk` | Fichiers Android Application Package (APK).<br><br>*Les fichiers DEX contenus dans les fichiers APK sont analysés dans le cadre de l’analyse de fichiers APK.* |
| `flash` | Applets Adobe Flash et contenu Flash intégré à des pages Web. |
| `jar` | Applets Java (types de fichiers JAR/Class). |
| `ms-office` | Fichiers utilisés par Microsoft Office, y compris les documents (DOC, DOCX, RTF), les classeurs (XLS, XLSX), les présentations PowerPoint (PPT, PPTX) ainsi que les documents XML (OOXML) Open Office 2007+. Les fichiers de requête Internet (IQY) et de lien symbolique (SLK) sont pris en charge avec la version de contenu 8462. |
| `pe` | Fichiers Portable Executable (exécutable portable ; PE). Les fichiers PE englobent les fichiers exécutables, le code objet, les fichiers DLL, les fichiers FON (polices) et les fichiers LNK. Les fichiers MSI sont pris en charge avec la version de contenu 8462. Un abonnement n'est pas requis pour transférer les fichiers PE pour une analyse WildFire, mais est requis pour tous les autres types de fichiers pris en charge. |
| `pdf` | Fichiers Portable Document Format (PDF). |
| `MacOSX` | Divers types de fichiers utilisés par la plateforme macOS. L’analyse statique des fichiers DMG, PKG et ZBundle n’est disponible que dans les régions du cloud Advanced WildFire Global (États-Unis) et du cloud Europe, mais l’analyse statique des autres fichiers Mac OS X (fat et macho) est prise en charge dans tous les clouds régionaux. L’analyse dynamique de tous les fichiers MacOSX n’est prise en charge que dans les régions |

| Types de fichier pris en charge pour le transfert WildFire | Description |
|---|---|
| | du cloud Advanced WildFire Global (États-Unis) et du cloud Europe. Reportez-vous à la section : Prise en charge des types de fichiers pour en savoir plus. |
| `email-link` | Liens HTTP/HTTPS contenus dans des messages électroniques SMTP et POP3. Voir Analyse de lien d'e-mail WildFire. |
| `archive` | Fichiers d'archive Roshal Archive (RAR) et 7-Zip (7z). Les archives multi-volumes fractionnées en plusieurs petits fichiers ne peuvent être transférées pour analyse.<br>Seuls les fichiers RAR protégés par un mot de passe *infected (infecté)* ou un *virus* sont décryptés et analysés par le cloud Advanced WildFire.<br>*Alors que le pare-feu est capable de transférer les fichiers pris en charge contenus dans les archives ZIP après leur décodage, il ne peut pas transférer les fichiers ZIP complets dans son état codé. Si vous souhaitez soumettre des fichiers ZIP complets, vous pouvez télécharger manuellement un fichier ZIP à l'aide du portail WildFire ou via l'API WildFire.* |
| `Linux` | Fichiers Executable and Linkable Format (format exécutable et liable ; ELF). |
| `script` | Divers fichiers script.<br>• Jscript (JS), VBScript (VBS) et les scripts PowerShell (PS1) sont pris en charge avec la version de contenu 8101.<br>• Les fichiers de lot (BAT) sont pris en charge avec la version de contenu 8168.<br>• Les fichiers HTML Application (HTA) sont pris en charge avec la version de contenu 8229. |

## Analyse de liens d'e-mail WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager) | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | |

Un pare-feu Palo Alto Networks peut extraire des liens HTTP/HTTPS contenus dans les messages électroniques SMTP et POP3 et transférer les liens pour l'analyse par WildFire. Le pare-feu extrait uniquement les liens et les informations de session associées (expéditeur, destinataire et objet) des messages électroniques ; il ne reçoit, stocke, transfère ni affiche les messages électroniques.

WildFire suit les liens envoyés afin de déterminer si la page Web correspondante présente une faille de sécurité quelconque ou montre une activité d’hameçonnage. Un lien que WildFire considère comme malveillant ou comme une tentative d’hameçonnage est :

- Enregistré sur le pare-feu en tant qu'entrée de journal des envois WildFire. Le rapport d'analyse WildFire qui détaille le comportement et l'activité observés pour le lien est disponible pour chaque entrée du journal des envois WildFire. L'entrée du journal inclut les informations d'en-tête d'e-mail (expéditeur, destinataire et objet du e-mail) afin que vous puissiez identifier le message et le supprimer du serveur de messagerie ou minimiser la menace si l'e-mail a été distribué ou ouvert.
- Ajouté à PAN-DB et l'URL est classée comme malveillante.

Le pare-feu transfère les liens d'e-mail par lots de 100 ou toutes les deux minutes (selon la première limite atteinte). Chaque chargement par lot sur WildFire compte pour un chargement vers la capacité de chargement par minute pour le pare-feu spécifique Capacité de transfert de fichiers du pare-feu en fonction du modèle. Si un lien contenu dans un e-mail correspond à un fichier de téléchargement plutôt qu'à une URL, le pare-feu transfère le fichier seulement si le type de fichier correspondant est activé pour l'analyse WildFire.

Pour permettre au pare-feu de transférer les liens inclus dans les e-mails pour analyse WildFire, consultez la section Transfert des fichiers pour une analyse par Advanced WildFire. Si vous disposez d’une licence URL Filtering avancé, vous pouvez également bloquer l’accès des utilisateurs à des sites web malveillants ou d’hameçonnage.

## Analyse d’URL

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Le cloud Advanced WildFire global (U.S.) peut analyser des URL et, par extension, des liens d'e-mail afin de fournir des verdicts et des rapports normalisés via l'API WildFire. En accumulant les détails de l'analyse des menaces des services de Palo Alto Networks, y compris les PAN-DB, Advanced WildFire est en mesure de générer un verdict plus exact et de fournir des données d'analyse des URL plus cohérentes.

Les analyseurs d'URL fonctionnant dans le cloud Advanced WildFire global (États-Unis) traitent les flux d'URL, les sources d'URL corrélées (telles que les liens de courrier électronique), les listes NRD (domaine nouvellement enregistré), le contenu PAN-DB et les URL téléchargées manuellement, pour fournir à tous les clouds Advanced WildFire les capacités améliorées, sans affecter la conformité GDPR. Une fois que l'URL a été traitée, vous pouvez récupérer le rapport d'analyse d'URL qui inclut le verdict, les motifs de la détection avec preuve, les copies d'écran et les données d'analyse générées pour la requête web. Vous pouvez aussi récupérer des artefacts de page web (fichiers téléchargés et copies d'écran) vus au cours de l'analyse d'URL afin d'examiner plus en détail l'activité anormale.

Aucune configuration supplémentaire n'est nécessaire pour bénéficier de cette option, mais si vous voulez envoyer automatiquement des liens d'e-mail pour une analyse (qui sont actuellement analysés par ce service), vous devez Transfert des fichiers pour une analyse par Advanced WildFire.

Si vous pensez que le verdict est un faux positif ou un faux négatif, vous pouvez le transmettre à l'équipe de prévention des menaces de Palo Alto Networks, qui effectuera une analyse plus poussée.

## Analyse de fichier compressé et codé

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Par défaut, le pare-feu décode les fichiers qui ont été codés ou compressés jusqu'à quatre fois, y compris les fichiers qui ont été compressés en utilisant le format ZIP. Le pare-feu effectue ensuite l'inspection et applique la politique sur le fichier décodé ; si le fichier est inconnu, le pare-feu transfère le fichier décodé pour l'analyse WildFire. Bien que le pare-feu ne puisse pas transférer les fichiers d'archive ZIP complets pour l'analyse Advanced WildFire, vous pouvez soumettre des fichiers directement au cloud Advanced WildFire public à l'aide du portail WildFire ou de l'API WildFire.

*Les fichiers d'archive RAR et 7-Zip ne sont pas décodés par le pare-feu. Tout le traitement de ces fichiers s'effectue dans le cloud Advanced WildFire public.*

# Signatures Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Advanced WildFire peut détecter les logiciels malveillants de type « zero-day » dans le trafic web (HTTP/HTTPS), les protocoles de messagerie (SMTP, IMAP et POP) et le trafic FTP, et la génération rapide de signatures, permettant d’identifier et de prévenir toute infection future par l’ensemble des logiciels malveillants détectés. Advanced WildFire génère automatiquement une signature en fonction des données utiles malveillantes de l’échantillon et la teste pour en vérifier la précision et la sécurité.

Chaque cloud Advanced WildFire analyse des échantillons et génère des signatures de logiciels malveillants indépendamment des autres clouds Advanced WildFire. À l’exception des signatures du cloud WildFire privé, les signatures Advanced WildFire sont transmises globalement, ce qui permet aux utilisateurs du monde entier de tirer profit d’une protection contre les logiciels malveillants, peu importe l’endroit de la première détection de ces logiciels malveillants. En raison de l’évolution rapide des logiciels malveillants, les signatures générées par Advanced WildFire prennent en compte plusieurs variantes du logiciel malveillant.

Les pare-feu qui disposent d’une licence Advanced WildFire active peuvent récupérer les dernières signatures Advanced WildFire en temps réel, dès qu’elles sont disponibles. Si vous ne disposez pas d’un abonnement Advanced WildFire, les signatures sont disponibles dans un délai de 24 à 48 heures, et sont intégrées à la mise à jour antivirus destinée aux pare-feu avec une licence de prévention des menaces active.

Une fois que le pare-feu télécharge et installe la nouvelle signature, il peut bloquer les fichiers qui contiennent ce logiciel malveillant (ou l'une de ses variantes). Les signatures de logiciels malveillants ne détectent pas les liens malveillants ou d’hameçonnage ; pour surveiller ces liens, vous devez détenir une licence de Filtrage des URL PAN-DB. Vous pouvez alors bloquer l’accès des utilisateurs aux sites malveillants ou d’hameçonnage.

# Déploiements Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Vous pouvez configurer un pare-feu Palo Alto Networks pour qu'il envoie les échantillons inconnus à un cloud public Advanced WildFire hébergé par Palo Alto Networks, au cloud du gouvernement américain ou à un cloud privé WildFire hébergé localement. Vous pouvez également autoriser le pare-feu à transférer certains échantillons à un cloud public Advanced WildFire et certains échantillons à un cloud privé WildFire :

- Cloud Advanced WildFire public
- Cloud WildFire privé
- Cloud WildFire hybride :
- WildFire : Cloud du gouvernement américain

## Cloud Advanced WildFire public

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Un pare-feu Palo Alto Networks qui peut transférer des fichiers et des liens d'e-mail inconnus vers le cloud Advanced WildFire global (U.S.) ou vers les clouds Advanced WildFire régionaux que Palo Alto Networks possède et tient à jour. Choisissez le cloud WildFire public auquel vous souhaitez envoyer les échantillons pour analyse selon votre emplacement et les besoins de votre organisation :

- **Cloud Advanced WildFire global (U.S.)**

  Le cloud Advanced WildFire global (U.S.) est un environnement de cloud public hébergé aux États-Unis.

  Servez-vous de l’URL suivante pour effectuer l’envoi de fichiers pour analyse au cloud Advanced WildFire global (U.S.) et pour accéder au portail Advanced WildFire global (U.S.) : wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Europe**

  Le cloud WildFire Europe est un environnement de cloud public régional hébergé aux Pays-Bas. Il est conçu pour respecter les règlements en matière de protection de la confidentialité des données de l’Union européenne (UE). Les échantillons qui sont soumis à ce cloud ne sortent pas du territoire de l’UE.

  Servez-vous de l’URL suivante pour effectuer l’envoi de fichiers pour analyse au cloud Advanced WildFire Europe et pour accéder au portail du cloud WildFire Europe : eu.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Japon**

  Le cloud Advanced WildFire Japon est un environnement de cloud public régional hébergé au Japon.

  Servez-vous de l’URL suivante pour effectuer l’envoi de fichiers pour analyse au cloud Advanced WildFire Japon et pour accéder au portail du cloud Advanced WildFire Japon : jp.wildfire.paloaltonetworks.com.

- **Advanced WildFire Cloud Singapour**

  Le cloud Advanced WildFire Singapour est un environnement de cloud public régional hébergé à Singapour.

  Servez-vous de l’URL suivante pour effectuer l’envoi de fichiers pour analyse au cloud Advanced WildFire Singapour et pour accéder au portail du cloud Advanced WildFire Singapour : sg.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Royaume-Uni**

  Le cloud Advanced WildFire Royaume-Uni est un environnement de cloud public régional hébergé au Royaume-Uni.

  Servez-vous de l’URL suivante pour effectuer l’envoi de fichiers pour analyse au cloud Advanced WildFire Japon et pour accéder au portail du cloud Advanced WildFire Japon : uk.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Canada**

  Le cloud WildFire Canada est un environnement de cloud public régional hébergé au Canada.

  Servez-vous de l’URL suivante pour effectuer l’envoi de fichiers pour analyse au cloud Advanced WildFire Canada et pour accéder au portail du cloud Advanced WildFire Canada : ca.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Australie**

  Le cloud WildFire Australie est un environnement cloud public régional hébergé en Australie.

  Servez-vous de l’URL suivante pour effectuer l’envoi de fichiers pour analyse au cloud Advanced WildFire Australie et pour accéder au portail du cloud Advanced WildFire Australie : au.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Allemagne**

  Le cloud Advanced WildFire Allemagne est un environnement de cloud public régional hébergé en Allemagne.

  Servez vous de l'URL suivante pour effectuer l'envoi de fichiers au cloud Advanced WildFire Allemagne pour analyse et pour accéder au portail du cloud Advanced WildFire Allemagne : de.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Inde**

  Le cloud Advanced WildFire India est un environnement de cloud public régional hébergé en Inde.

  Servez vous de l'URL suivante pour effectuer l'envoi de fichiers au cloud Advanced WildFire Inde pour analyse et pour accéder au portail du cloud Advanced WildFire Inde : in.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Suisse**

  Le cloud Advanced WildFire Suisse est un environnement de cloud public régional hébergé en Suisse.

  Utilisez l'URL suivante pour effectuer l'envoi de fichiers au cloud Advanced WildFire Suisse pour analyse et pour accéder au portail cloud Advanced WildFire Suisse : ch.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Pologne**

  Le cloud Advanced WildFire Pologne est un environnement de cloud public régional hébergé en Pologne.

  Servez vous de l'URL suivante pour effectuer l'envoi de fichiers au cloud Advanced WildFire Pologne pour analyse et pour accéder au portail du cloud Advanced WildFire Pologne : pl.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Indonésie**

  Le cloud Advanced WildFire Indonésie est un environnement de cloud public régional hébergé en Indonésie.

  Servez vous de l'URL suivante pour effectuer l'envoi de fichiers au cloud Advanced WildFire Indonésie pour analyse et pour accéder au portail du cloud Advanced WildFire Indonésie : id.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Taiwan**

  Le cloud Advanced WildFire Taïwan est un environnement de cloud public régional hébergé à Taïwan.

  Servez-vous de l'URL suivante pour effectuer l'envoi de fichiers pour analyse au cloud Advanced WildFire Taïwan et pour accéder au portail du cloud Advanced WildFire Taïwan : tw.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire France**

  Le cloud Advanced WildFire France est un environnement de cloud public régional hébergé en France.

  Servez-vous de l'URL suivante pour effectuer l'envoi de fichiers pour analyse au cloud Advanced WildFire France et pour accéder au portail du cloud Advanced WildFire France : fr.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Qatar**

  Le cloud Advanced WildFire Qatar est un environnement de cloud public régional hébergé au Qatar.

  Servez-vous de l'URL suivante pour effectuer l'envoi de fichiers pour analyse au cloud Advanced WildFire Qatar et pour accéder au portail du cloud Advanced WildFire Qatar : qatar.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Corée du Sud**

  Le cloud Advanced WildFire Corée du Sud est un environnement de cloud public régional hébergé en Corée du Sud.

  Servez-vous de l'URL suivante pour envoyer des fichiers au cloud Advanced WildFire Corée du Sud pour analyse et pour accéder au portail du cloud Advanced WildFire Corée du Sud : kr.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Israël**

  Le cloud Advanced WildFire Israël est un environnement de cloud public régional hébergé en Israël.

  Servez vous de l'URL suivante pour effectuer l'envoi de fichiers au cloud Advanced WildFire Israël pour analyse et pour accéder au portail du cloud Advanced WildFire Israël : il.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Arabie saoudite**

  Le cloud Advanced WildFire Arabie saoudite est un environnement de cloud public régional hébergé en Arabie saoudite.

  Servez-vous de l'URL suivante pour effectuer l'envoi de fichiers au cloud Advanced WildFire Arabie saoudite pour analyse et pour accéder au portail du cloud Advanced WildFire Arabie saoudite : sa.wildfire.paloaltonetworks.com.

- **Cloud Advanced WildFire Espagne**

  Le cloud Advanced WildFire Espagne est un environnement de cloud public régional hébergé en Espagne.

  Servez-vous de l'URL suivante pour effectuer l'envoi de fichiers pour analyse au cloud Advanced WildFire Espagne et pour accéder au portail du cloud Advanced WildFire Espagne : es.wildfire.paloaltonetworks.com.

Chaque cloud Advanced WildFire (global [U.S.] et régional) analyse les échantillons et génère des signatures de logiciels malveillants et des verdicts indépendamment des autres clouds WildFire. Les signatures et verdicts Advanced WildFire sont ensuite transmis globalement, ce qui permet à tous les utilisateurs de WildFire du monde entier de tirer profit d'une protection contre les logiciels malveillants, peu importe l'endroit de la première détection de ces logiciels malveillants. Passez en revue la section Prise en charge des types de fichiers Advanced WildFire pour en apprendre davantage à propos des types de fichiers analysés par chaque cloud.

Si vous avez un appareil WildFire, vous pouvez activer un déploiement de cloud WildFire hybride, où le pare-feu peut transférer certains fichiers à un cloud WildFire public et d'autres fichiers à un cloud WildFire privé pour une analyse locale. L'appareil WildFire peut également être configuré pour recueillir rapidement des verdicts pour les échantillons connus en interrogeant le cloud public avant d'effectuer une analyse. L'appareil WildFire peut alors consacrer ses ressources d'analyse aux échantillons qui sont inconnus dans le réseau privé et dans la communauté WildFire mondiale.

## Cloud WildFire privé

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire ou WildFire |

Dans un déploiement de cloud privé Palo Alto Networks, les pare-feu Palo Alto Networks transfèrent des fichiers vers un appareil WildFire installé sur le réseau de votre entreprise qui sert à l'hébergement d'un emplacement d'analyse sur un cloud privé.

Pour plus d’informations sur le transfert vers le cloud hybride, reportez-vous au Guide de l’administrateur de l’appareil WildFire.

## Cloud WildFire hybride :

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire ou WildFire |

Dans un déploiement de cloud WildFire hybride, un pare-feu peut transférer certains échantillons au cloud WildFire public hébergé par Palo Alto Networks et d'autres échantillons à un cloud WildFire privé hébergé par un appareil WildFire.

Pour plus d’informations sur le transfert vers le cloud hybride, reportez-vous au Guide de l’administrateur de l’appareil WildFire.

## Plateformes cloud autorisées par FedRAMP WildFire

| Où puis-je l’utiliser ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.*<br>❑ Module complémentaire FedRAMP Advanced WildFire |

En plus des options de déploiement du cloud WildFire Global, du cloud privé et du cloud hybride, Palo Alto Networks donne également accès à plusieurs environnements de cloud de haute sécurité autorisés

par FedRAMP pour les entreprises qui doivent se conformer aux normes opérationnelles sécurisées du cloud. Les clouds autorisés par FedRAMP sont disponibles en deux niveaux d'impact : Élevé et modéré, modéré étant disponible dans deux configurations de nuage. Le cloud Advanced WildFire gouvernemental est conforme à la norme de certification élevée FedRAMP, tandis que le cloud WildFire du gouvernement américain est conforme à la norme de certification modérée FedRAMP.

*Le cloud WildFire du gouvernement américain (qui est conforme aux normes de certification modérées FedRAMP) doit être mis hors service. Pour tous les nouveaux clients, Palo Alto Networks recommande d'utiliser le cloud Advanced WildFire du secteur public. Ce cloud dispose d'un ensemble de fonctionnalités amélioré et prend en charge le cloud Advanced WildFire.*

Les clouds modérés FedRAMP (cloud Advanced WildFire gouvernemental et cloud WildFire du gouvernement américain) sont généralement disponibles pour les clients de Palo Alto Networks. Cependant, le cloud Advanced WildFire gouvernemental, conforme aux normes de certification élevées FedRAMP, n'est disponible que pour le ministère fédéral de la Défense ou clients fédéraux de la base industrielle de défense approuvée (DIB).

En raison de la nature sensible de ces services, les clouds FedRAMP ont un processus d'intégration spécifique qui diffère de celui des autres services. Pour plus d'informations, reportez-vous au type de cloud FedRAMP spécifique :

- Cloud Advanced WildFire gouvernemental
- Cloud Advanced WildFire du secteur public
- WildFire : Cloud du gouvernement américain

Les nuages FedRAMP listés ci-dessus ne peuvent pas être mélangés et appariés sur le même périphérique, ni être utilisés simultanément avec les clouds mondiaux ou régionaux Advanced WildFire. Cependant, tout cloud FedRAMP peut être utilisé en coopération avec d'autres services de sécurité basés sur le cloud (par exemple Advanced Threat Prevention, DLP, etc.). Si vous devez incorporer plusieurs niveaux de sécurité FedRAMP sur un seul périphérique, vous devez utiliser des ID de compte distincts. Une fois l'intégration terminée, vous pouvez référencer l'URL du cloud FedRAMP dans votre profil de sécurité antivirus et vos API de la même manière que tout autre cloud Advanced WildFire.

## Cloud Advanced WildFire gouvernemental

| Où puis-je l'utiliser ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.*<br>❑ Module complémentaire Advanced WildFire GovCloud |

Palo Alto Networks propose aux clients de l'administration fédérale, du ministère de la Défense ou de la base industrielle de défense approuvée (DIB), le cloud Advanced WildFire gouvernemental, plateforme

d’analyse de logiciels malveillants de haute sécurité conforme aux normes de certification élevées du programme FedRAMP (Federal Risk and Authorization Management Program).

Le cloud du secteur public Advanced WildFire fonctionne comme une entité distincte et séparée des régions du cloud commercial ou gouvernemental. Toutes les informations de confidentialité qui pourraient être présentes dans les échantillons envoyés pour analyse, telles que les adresses e-mail, les adresses IP et le DNS passif, ne seront partagées avec aucune autre instance de cloud WildFire. Il arrive toutefois à exploiter les données sur les menaces générées par les clouds publics Advanced WildFire afin de maximiser la couverture ainsi que les protections et les signatures antivirus produites dans le cadre de l’analyse des fichiers.

*Pour obtenir de plus amples renseignements sur les autorisations FedRAMP Advanced WildFire de Palo Alto Networks, visitez :* FedRAMP.gov

Pour obtenir de plus amples renseignements sur l’autorisation FedRAMP WildFire de Palo Alto Networks, visitez : Services du cloud du gouvernement de Palo Alto Networks - WildFire

Le cloud gouvernemental Advanced WildFire présente plusieurs différences fonctionnelles par rapport aux clouds publics Advanced WildFire commerciaux standard. La fonctionnalité suivante n’est pas disponible pour les clients se connectant aux clouds gouvernementaux Advanced WildFire :

- L’analyse Bare Metal n’est pas prise en charge par les régions du cloud Advanced WildFire du gouvernement américain.
- Le cloud gouvernemental Advanced WildFire n’est pas accessible via le portail WildFire.
- Le droit de supprimer la fonctionnalité n'est pas disponible sans requête de service.

**Commencer à utiliser le cloud gouvernemental Advanced WildFire**

Suivez toutes les mesures procédurales internes pour déterminer la pertinence de l’utilisation du cloud Advanced WildFire du gouvernement américain au sein de votre réseau, notamment, sans toutefois s’y limiter, pour mener une analyse des risques et une évaluation du package de soumission CSP et pour accorder des approbations d’autorisation. Veuillez contacter votre représentant des ventes Palo Alto Networks/votre point de contact Advanced WildFire Cloud cloud WildFire du gouvernement américain pour discuter des détails opérationnels supplémentaires.

L’accès aux régions du cloud Advanced WildFire du gouvernement américain commence lorsque vous avez satisfait aux exigences organisationnelles en ce qui a trait à l’exploitation d’un service FedRAMP autorisé.

Communiquez avec l’équipe de compte Palo Alto Networks pour lancer le processus d’intégration. Une fois l’activation d’Advanced WildFire terminée, reconfigurez les pare-feu pour transférer les fichiers et les liens d’e-mail inconnus à des fins d’analyse à l’aide de l’URL suivante : gov-cloud.wildfire.paloaltonetworks.com. Pour plus d’informations, reportez-vous à la section Transfert de fichiers pour analyse WildFire. Si vous avez besoin d’aide, communiquez avec le Support client de Palo Alto Networks.

## Cloud Advanced WildFire du secteur public

| Où puis-je l’utiliser ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.*<br>❑ Module complémentaire Advanced WildFire PubSec |

Palo Alto Networks propose à ses clients le cloud Advanced WildFire du secteur public, plateforme d’analyse de logiciels malveillants de haute sécurité conforme aux normes de certification modérées FedRAMP (Federal Risk and Authorization Management Program). Le cloud Advanced WildFire du secteur public remplace le cloud WildFire du gouvernement américain.

Le cloud du secteur public Advanced WildFire fonctionne comme une entité distincte et séparée des régions du cloud commercial ou gouvernemental. Toutes les informations de confidentialité qui pourraient être présentes dans les échantillons envoyés pour analyse, telles que les adresses e-mail, les adresses IP et le DNS passif, ne seront partagées avec aucune autre instance de cloud WildFire. Il arrive toutefois à exploiter les données sur les menaces générées par les clouds publics Advanced WildFire afin de maximiser la couverture ainsi que les protections et les signatures antivirus produites dans le cadre de l’analyse des fichiers.

*Pour obtenir de plus amples renseignements sur les autorisations FedRAMP Advanced WildFire de Palo Alto Networks, visitez :* FedRAMP.gov

Le cloud Advanced WildFire du secteur public présente quelques différences fonctionnelles par rapport aux clouds publics commerciaux Advanced WildFire standard. La fonctionnalité suivante n’est pas disponible pour les clients se connectant aux clouds Advanced WildFire du secteur public :

- L’analyse Bare Metal n’est pas prise en charge par les régions du cloud Advanced WildFire du gouvernement américain.
- La région du cloud Advanced WildFire du secteur public américain n’est pas accessible via le portail WildFire.
- Le droit de supprimer la fonctionnalité n'est pas disponible sans requête de service.

**Commencer à utiliser le cloud Advanced WildFire du secteur public**

Suivez toutes les mesures procédurales internes pour déterminer la pertinence de l’utilisation du cloud Advanced WildFire du secteur public au sein de votre réseau, telles que, mais sans s'y limiter, la réalisation d’une analyse des risques, l’évaluation du package de soumission CSP et les approbations d’autorisation. Veuillez contacter votre représentant des ventes Palo Alto Networks/votre point de contact Advanced WildFire Cloud du secteur public américain pour discuter des détails opérationnels supplémentaires.

L'accès aux régions du cloud Advanced WildFire du secteur public commence lorsque vous avez satisfait aux exigences organisationnelles appropriées pour exploiter un service autorisé FedRAMP.

Communiquez avec l'équipe de compte Palo Alto Networks pour lancer le processus d'intégration. Une fois l'activation d'Advanced WildFire terminée, reconfigurez les pare-feu pour transférer les fichiers et les liens d'e-mail inconnus à des fins d'analyse à l'aide de l'URL suivante : pubsec-cloud.wildfire.paloaltonetworks.com.

Pour plus d'informations, reportez-vous à la section Transfert de fichiers pour analyse WildFire. Si vous avez besoin d'aide, communiquez avec le Support client de Palo Alto Networks.

## WildFire : Cloud du gouvernement américain

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.*<br>❑ Cloud du gouvernement américain WildFire : intégration |

*À compter du 15 juillet 2024, le cloud Palo Alto Networks WildFire du gouvernement américain a été remplacé par le Cloud Advanced WildFire gouvernemental et le Cloud Advanced WildFire du secteur public, qui permettent d'accéder à des environnements de cloud Advanced WildFire hautement sécurisés exploitant une base de code plus récente avec un ensemble de fonctionnalités améliorées. En conséquence, Palo Alto Networks n'intègre plus de nouveaux clients au cloud WildFire du gouvernement américain. Les clients existants peuvent continuer à accéder au cloud WildFire du gouvernement jusqu'à la date de mise hors service du 30 novembre 2024, date à laquelle l'URI existante sera redirigée vers le cloud Advanced WildFire du secteur public.*

*Pour plus de détails sur les nouvelles offres de cloud, contactez votre représentant commercial Palo Alto Networks pour discuter de tout détail opérationnel supplémentaire.*

Le cloud WildFire du gouvernement américain Palo Alto Networks est une plateforme d'analyse des programmes malveillants à sécurité élevée qui est autorisée par le programme FedRAMP (Federal Risk and Authorization Management Program). Cet environnement cloud WildFire est destiné à être utilisé uniquement par les Agences fédérales des États-Unis exigeant une approche standardisée de l'évaluation de la sécurité, de l'autorisation et de la surveillance continue des produits et services cloud. Le cloud Cloud du gouvernement américain est une entité distincte : tous les renseignements privés qui peuvent se trouver dans les échantillons soumis aux fins d'analyse, comme les adresses électroniques, les adresses IP et les DNS passifs, ne seront soumis à aucune autre instance du cloud WildFire. Il arrive toutefois à exploiter les données sur les menaces générées par le cloud public WildFire afin de maximiser la couverture ainsi que les protections et les signatures antivirus produites dans le cadre de l'analyse des fichiers.

Pour obtenir de plus amples renseignements sur l'autorisation FedRAMP WildFire de Palo Alto Networks, visitez : Services du cloud du gouvernement de Palo Alto Networks - WildFire

Le cloud public WildFire (les clouds globaux et régionaux) et le cloud du gouvernement américain possèdent plusieurs différences fonctionnelles. La fonctionnalité suivante n'est pas offerte aux clients qui se connectent au cloud Cloud du gouvernement américain :

- L’analyse sans système d’exploitation n’est pas prise en charge par le Palo Alto Networks.
- L’analyse des fichiers Script (Bat, JS, BVS, PS1, Shell script et HTA) n’est pas prise en charge à l’heure actuelle.
- Le cloud Cloud du gouvernement américain n’est pas accessible par l’intermédiaire du portail WildFire.
- Le cloud du gouvernement américain ne peut être intégré aux autres services dans le cloud.
- La suppression de la fonctionnalité n’est pas autorisée.
- Le cloud Le cloud du gouvernement américain ne prend actuellement pas en charge l’analyse Advanced WildFire.

**Premiers pas avec le Cloud du gouvernement américain**

Pour se connecter au cloud WildFire Cloud américain, vous devez en demander l’accès. Suivez les mesures procédurales internes pour déterminer la pertinence d’utiliser le cloud WildFire du gouvernement américain au sein de votre réseau, notamment, sans toutefois s’y limiter, pour mener une analyse des risques et une évaluation du package de soumission CSP et pour accorder des approbations d’autorisation. Veuillez communiquer avec votre représentant des ventes Palo Alto Networks/votre Cloud cloud WildFire du gouvernement américain pour discuter des détails opérationnels supplémentaires.

Les demandes d’accès au cloud WildFire du gouvernement américain commencent lorsque vous avez satisfait aux exigences organisationnelles en ce qui a trait à l’exploitation d’un service FedRAMP autorisé. Il y a deux catégories d’entités qui peuvent accéder au cloud WildFire du gouvernement américain : Cloud Entrepreneurs du gouvernement américain et agences fédérales américaines (et autres ministères approuvés). Les deux entités doivent satisfaire à des exigences spécifiques pour accéder au cloud WildFire du gouvernement américain :

1. **Les agences fédérales américaines**

   Les agences, départements et bureaux fédéraux américains doivent recevoir une autorisation d’exploitation (ATO) de l’autorité approbatrice désignée (DAA), qui autorise l’exploitation du cloud WildFire du gouvernement américain au sein des opérations d’une agence, avant que l’accès ne soit accordé.

   1. Informez le point de contact Palo Alto Networks (fedramp@paloaltonetworks.com) de votre intention d’utiliser le cloud WildFire du gouvernement américain.
   2. Envoyez une requête à info@fedramp.gov.
   3. Remplissez le formulaire de requête d’accès au package FedRAMP et soumettez-le à info@fedramp.gov.

      *Le Program Management Office (Bureau de gestion du programme ; PMO) FedRAMP examine le formulaire et autorise généralement un accès temporaire de 30 jours au package FedRAMP de WildFire.*
   4. Examinez le package de sécurité FedRAMP du cloud Wildfire du gouvernement américain. Palo Alto Networks. Effectuez les processus internes exigés pour déployer le cloud WildFire du gouvernement américain au sein de votre organisation.
   5. Délivrez l’autorisation ATO.
   6. Envoyez une requête au PMO FedRAMP pour obtenir un accès permanent au cloud WildFire du gouvernement américain.

2. **Les entrepreneurs du gouvernement américain**

   Les entrepreneurs du gouvernement américain qui utilisent ou consultent le cloud WildFire du gouvernement américain doit répondre aux exigences suivantes.

   1. Ils doivent être citoyens des États-Unis.
   2. Détenir un contrat actif (ou un contrat de sous-traitance) avec une agence du gouvernement fédéral américain ayant une exigence professionnelle d’échange d’informations à l’aide d’Internet, comme la correspondance par e-mail, le partage de documents et d’autres formes de communication sur Internet.
   3. Lorsque l’emploi d’un entrepreneur prend fin, l’utilisateur doit cesser d’utiliser ou de consulter le cloud WildFire du gouvernement américain.
   4. Il convient de respecter les dispositions en matière de confidentialité contenues dans le Contrat de licence d’utilisateur final (CLUF) de Palo Alto Networks.

Une fois que votre organisation a délivré une autorisation d’exploitation (ATO) ou, le cas échéant, lorsque les entrepreneurs du gouvernement américain satisfont à toutes les exigences d’utilisation, ce n’est qu’à ce moment-là qu’il est possible de formuler une requête d’accès au cloud WildFire du gouvernement américain. Pour ce faire, vous devez appeler votre équipe Palo Alto Networks.

1. Communiquez avec votre bureau de gestion du programme FedRAMP pour déterminer la viabilité du cloud WildFire du gouvernement américain pour la satisfaction de vos besoins en matière de sécurité.
2. Communiquez avec votre personne-ressource Palo Alto Networks, précisée dans le FedRAMP Marketplace. La personne-ressource vous donne des renseignements supplémentaires sur le service ainsi que d’autres renseignements opérationnels qui sont pertinents pour votre déploiement WildFire.
3. Communiquez avec l’équipe de compte Palo Alto Networks pour lancer le processus d’intégration. L’équipe de compte demandera les renseignements suivants concernant le client et les spécificités du déploiement.

   - Les coordonnées.
   - Une brève description justifiant la migration vers le Palo Alto Networks.
   - Un énoncé de conformité organisationnelle contenant les dispositions relatives à la confidentialité qui sont énoncées dans le CLUF de Palo Alto Networks.
   - Les adresses IP de sortie de toutes les passerelles du pare-feu (y compris les plans de gestion) ainsi que toutes les instances de Panorama.
4. Lorsque la gestion de programme WildFire donne son approbation à l’utilisation du cloud WildFire du gouvernement américain (généralement dans un délai de un à trois jours ouvrables), les Opérations de développement de Palo Alto Networks appliquent les contrôles appropriés.
5. Une fois l’accès au cloud WildFire du gouvernement américain accordé, reconfigurez le pare-feu pour qu’il transfère les fichiers et les liens d’e-mail inconnus à des fins d’analyse à l’aide de l’URL suivante : wildfire.gov.paloaltonetworks.com. Pour plus d’informations, reportez-vous à la section Transfert de fichiers pour analyse WildFire. Si vous avez besoin d’aide, communiquez avec le Support client de Palo Alto Networks.

# Prise en charge des types de fichiers

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Le tableau suivant présente les types de fichiers qui sont pris en charge pour analyse dans les environnements de cloud WildFire.

*Pour obtenir une liste complète des types de fichiers spécifiques pris en charge par WildFire, reportez-vous à la section* Types de fichiers pris en charge (Liste complète).

| Types de fichiers pris en charge pour l'analyse | Cloud Advanced WildFire public (toutes les régions) | Cloud du du gouvernement américain | Portail Advanced WildFire \| API (téléchargement direct ; toutes les régions) |
|---|---|---|---|
| Liens contenus dans les e-mails | ✓ | ✓ | ✓ |
| Fichiers Android Application Package (APK). | ✓ | ✓ | ✓ |
| Fichiers Adobe Flash | ✓ | ✓ | ✓ |
| Fichiers Java Archive (JAR) | ✓ | ✓ | ✓ |
| Fichiers Microsoft Office (comprend les fichiers SLK et IQY) | ✓ | ✓ | ✓ |
| Fichiers exécutables portables | ✓ | ✓ | ✓ |

| Types de fichiers pris en charge pour l’analyse | Cloud Advanced WildFire public (toutes les régions) | Cloud du du gouvernement américain | Portail Advanced WildFire \| API (téléchargement direct ; toutes les régions) |
|---|---|---|---|
| (comprend les fichiers MSI) | | | |
| Fichiers Portable Document Format (PDF) | ✓ | ✓ | ✓ |
| Fichiers Mac OS X* | ✓ | ✓ | ✓ |
| Fichiers Linux (fichiers ELF et scripts Shell) | ✓ | ✓ | ✓ |
| Fichiers d’archive (RAR, 7-Zip, ZIP**) | ✓ | ✓ | ✓ |
| Fichiers de script (BAT, JS, VBS, PS1 et HTA) | ✓ | ✗ | ✓ |
| Scripts Python | ✓ | ✓ | ✓ |
| Scripts Perl | ✗ | ✗ | ✓ |
| Fichiers d'archives (ZIP [téléchargement direct] et ISO) | ✗ | ✗ | ✓ |
| Fichiers image (JPG et PNG) | ✗ | ✗ | ✓ |

* L’analyse statique des fichiers DMG, PKG et ZBundle n’est disponible que dans les régions du cloud Advanced WildFire Global (États-Unis) et du cloud Europe, mais l’analyse statique des autres fichiers Mac OS X (fat et macho) est prise en charge dans tous les clouds régionaux. L’analyse dynamique de tous les fichiers Mac OS X n’est prise en charge que dans les régions du cloud Advanced WildFire Global (États-Unis) et cloud Europe.

** Les fichiers ZIP ne sont pas directement transférés vers le cloud Advanced Wildfire pour analyse. Au lieu de cela, ils sont d'abord décodés par le pare-feu, et les fichiers qui correspondent aux critères du profil d'analyse WildFire sont transférés séparément pour analyse.

*Vous souhaitez en savoir plus ?*

- *Pour plus d'informations sur chaque déploiement cloud Advanced WildFire, reportez-vous à la section* Déploiements Advanced WildFire.
- *Pour obtenir des précisions sur chaque type de fichier pris en charge pour l'analyse WildFire, reportez-vous à la section* Analyse de fichiers.

## Types de fichiers pris en charge (Liste complète)

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Le tableau suivant répertorie les types de fichiers pris en charge par l'analyse WildFire. Pour les fichiers marqués Oui dans la colonne Forwarding Support (Prise en charge du transfert), cela inclut les fichiers codés MIME dans le trafic Web (HTTP/HTTPS) et les protocoles de messagerie (SMTP, IMAP, POP).

| Type de contenu pris en charge | Exemple d'extension | Prise en charge du transfert |
|---|---|---|
| Archives 7zip | 7z | Oui |
| Fichier Adobe Flash | swf | Oui |
| Android APK | apk | Oui |
| Android DEX | dex | Oui |
| batch | bat | Oui |
| Archives bzip2 | bz | Oui |
| Valeurs séparées par des virgules | csv | Non |
| DLL, DLL64 | dll | Oui |
| ELF | elf | Oui |
| Archive Gzip | gz | Non |

| Type de contenu pris en charge | Exemple d’extension | Prise en charge du transfert |
|---|---|---|
| Application HTML | hta | Oui |
| ISO | iso | Non |
| Classe JAVA | class | Oui |
| JAVA JAR | jar | Oui |
| Javascript/JScript | js, jse, wsf | Oui (JS uniquement) |
| Groupe mixte d’experts en photographie | jpg | Non |
| Lien | elink | Oui |
| Mach-O | macho | Oui |
| Programme d’installation de l’application macOS | pkg | Oui |
| Ensemble d’applis macOS dans l’archive ZIP | zbundle | Non |
| Fichier binaire universel macOS | fat | Non |
| Image disque macOS | dmg | Oui |
| Document Microsoft Excel 97-2003 | xls | Oui |
| Document Microsoft Excel | xlsx | Oui |
| Document Microsoft One Note | one | Oui |
| Document Microsoft PowerPoint 97-2003 | ppt | Oui |
| Document Microsoft PowerPoint | pptx | Oui |
| Fichier SYLK Microsoft | slk | Oui |
| Fichier de requête web Microsoft | iqy | Oui |

| Type de contenu pris en charge | Exemple d'extension | Prise en charge du transfert |
|---|---|---|
| Document Microsoft Word 97-2003 | doc | Oui |
| Document Microsoft Word | docx | Oui |
| Feuille de calcul OpenDocument | ods | Non |
| Document texte OpenDocument | odt | Non |
| PDF | pdf | Oui |
| PE, PE64 | exe | Oui |
| Perl Script | pl | Non |
| Fichier Portable Network Graphics | png | Non |
| PowerShell | ps1 | Oui |
| Script Python | py | Oui |
| Archives RAR | rar | Oui |
| RTF | rtf | Oui |
| Script Shell | sh | Oui |
| Archive Tar | tar | Non |
| VBScript | vbs, vbe | Oui (VBS uniquement) |
| Package d'installation Windows | msi | Oui |
| Fichier de lien Windows | lnk | Oui |
| Script Windows | wsf | Non |
| Archive zippée | zip | Non |
| Pages du serveur actives | asp | Non |
| Active Server Pages Extended | aspx | Non |

| Type de contenu pris en charge | Exemple d’extension | Prise en charge du transfert |
|---|---|---|
| Extensible Markup Language | xml | Non |
| Langage de balisage hypertexte | html | Non |

# Exemple Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Le scénario de l'exemple suivant récapitule le cycle de vie Advanced WildFire™ complet. Dans cet exemple, un représentant commercial de Palo Alto Networks télécharge un nouvel outil de vente informatique qu'un partenaire commercial a chargé sur le site Dropbox. Ce dernier a chargé, sans le savoir, une version infectée du fichier d'installation de cet outil de vente que le représentant commercial va ensuite télécharger.

Cet exemple montre comment un pare-feu Palo Alto Networks, associé à Advanced WildFire, va détecter un logiciel malveillant de type « zero-day » téléchargé par un utilisateur final, même s'il s'agit de trafic crypté SSL. Lorsque Advanced WildFire identifie le logiciel malveillant, un journal est envoyé au pare-feu. Celui-ci informe l'administrateur qui contacte alors l'utilisateur afin de supprimer le logiciel malveillant. Advanced WildFire génère ensuite une nouvelle signature pour le logiciel malveillant, après quoi les pare-feu téléchargent automatiquement la signature pour se protéger contre une exposition future. Bien que certains sites Web de partage de fichiers disposent d'une fonction antivirus contrôlant les fichiers une fois chargés, ils fournissent uniquement une protection contre les logiciels malveillants connus.

*Cet exemple utilise un site Web crypté SSL. Dans le cas présent, le décryptage est activé sur le pare-feu, y compris l'option de transfert de contenu crypté pour analyse.*

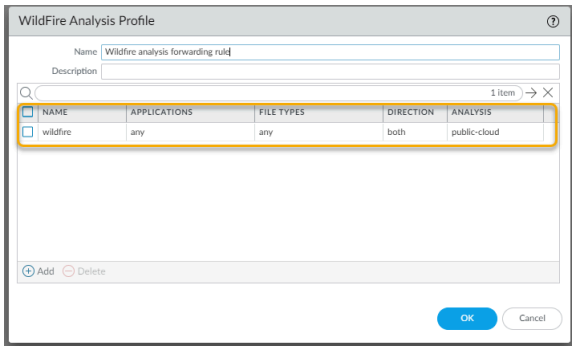
**STEP 1 |** Le représentant commercial d'une société partenaire charge un fichier contenant un outil de vente nommé sales-tool.exe sur son compte Dropbox, puis envoie un e-mail contenant un lien vers ce fichier au représentant commercial de Palo Alto Networks.

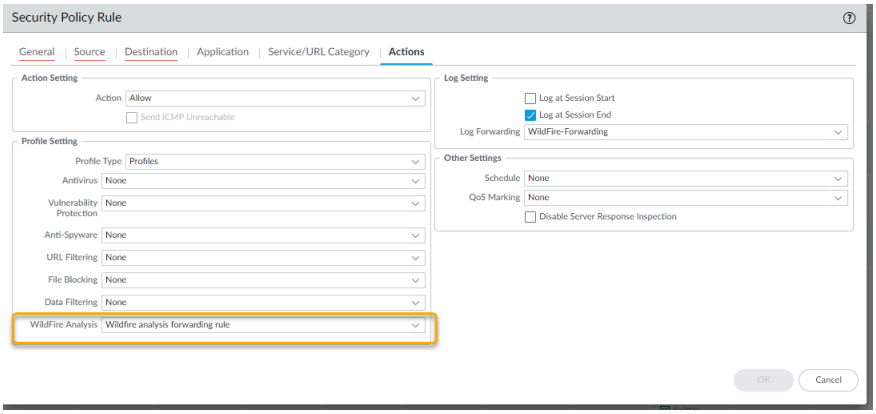
**STEP 2 |** Ce dernier reçoit l'e-mail et clique sur ce lien de téléchargement qui ouvre le site Dropbox. Puis, il clique sur **Download (Télécharger)** pour enregistrer le fichier sur son bureau.

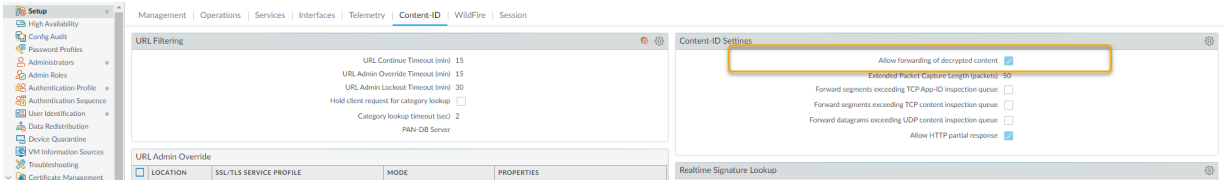
**STEP 3 |** Le pare-feu qui protège le représentant commercial de Palo Alto dispose d'une règle au profil d'analyse WildFire associée à une règle de politique de sécurité qui recherche des fichiers quelle que soit l'application utilisée pour télécharger ou charger un type de fichier pris en charge. Le pare-feu peut également être configuré pour transférer le type de fichier « email-link », qui permet au pare-feu d'extraire des liens HTTP/HTTPS contenus dans des courriers électroniques SMTP et POP3. Dès que le représentant commercial clique pour télécharger ce fichier, le pare-feu transfère le fichier sales-tool.exe vers Advanced WildFire, où le fichier est analysé afin de détecter tout logiciel malveillant de type « zero-day ». Bien que le représentant commercial utilise Dropbox, site doté d'un cryptage SSL, le pare-feu est configuré pour décrypter le trafic ; ainsi tout le trafic peut être inspecté. Les captures

d'écran suivantes montrent la règle associée au profil d'analyse WildFire, la politique de sécurité configurée avec la règle associée au profil d'analyse WildFire jointe, ainsi que l'option permettant d'autoriser le transfert de contenu crypté.

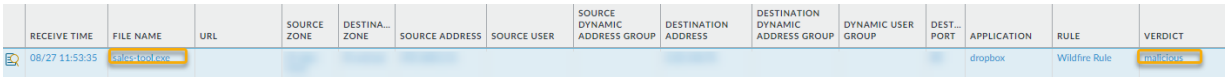



**STEP 4 |** À ce stade, Advanced WildFire a reçu le fichier et l’analyse pour plus de 200 comportements malveillants différents.

**STEP 5 |** Une fois qu’Advanced WildFire a terminé l’analyse des fichiers, il renvoie un journal Advanced WildFire au pare-feu avec les résultats de l’analyse. Dans cet exemple, le journal montre que le fichier est malveillant.



**STEP 6 |** Le pare-feu est configuré avec un profil de transfert de journaux qui enverra des alertes à l’administrateur de sécurité lorsqu’un logiciel malveillant est découvert.

| NAME | LOCATION | DESCRIPTION | LOG TYPE | FILTER | PANORAMA | SNMP | EMAIL | SYSLOG | HTTP | QUARANTINE | BUILT-IN ACTIONS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| WildFire-Forwarding | | | threat | (severity eq critical) | | | WildFire-Forwarding | | | | |
| | | | wildfire | (category eq benign) | ☐ | | | | | | |
| | | | wildfire | (category neq benign) and (category neq malicious) | | | WildFire-Forwarding | | | | |
| | | | wildfire | (category eq malicious) | ☐ | | WildFire-Forwarding | | | | |

**STEP 7 |** L'administrateur de sécurité identifie l'utilisateur par son nom (si l'option User-ID est configurée) ou par son adresse IP si l'option User-ID n'est pas activée. À ce stade, l'administrateur peut fermer le réseau ou la connexion VPN que le représentant commercial utilise et contacte ensuite le groupe d'assistance informatique afin de contrôler et de nettoyer le système avec l'utilisateur.

Grâce au rapport d’analyse détaillé Advanced WildFire, l’employé de l’assistance informatique peut déterminer si le système de l’utilisateur est infecté par le logiciel malveillant en observant les fichiers, les processus et les informations détaillées du registre figurant dans le rapport d’analyse Advanced WildFire. Si l'utilisateur exécute le logiciel malveillant, l'employé de l'assistance informatique peut essayer de nettoyer le système manuellement ou de créer une nouvelle image.

## FILE INFORMATION

| | |
|---|---|
| **File Type** | PE |
| **File Signer** | |
| **SHA-256** | 721b79505757ec7831844795afc4e88c23ce57cd4590118895cbfb86bcd34a77 |
| **SHA-1** | 2e8a6dd285f8fa829918aae60cb1b6172d918437 |
| **MD5** | c67fdb7887368e41469a1a2556ac30df |
| **File Size** | 55296 bytes |
| **First Seen Timestamp** | 2016-12-13 18:39:45 UTC |
| **Sample File** | Download File |
| **Verdict** | Malware |

## SESSION INFORMATION

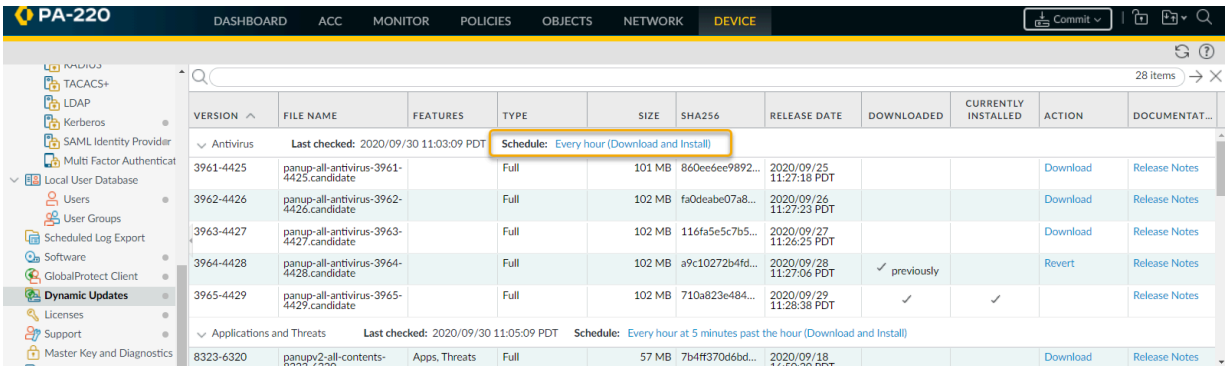
| | |
|---|---|
| **File Source** | |
| **File Destination** | |
| **User-ID** | |
| **Timestamp** | 2016-12-13 18:39:45 UTC |
| **Serial Number** | Manual |
| **Firewall Hostname/IP** | |
| **Virtual System** | |
| **Application** | |
| **URL** | |
| **File Name** | wildfire-test-pe-file (3).exe |
| **Status** | |

## COVERAGE STATUS

For endpoint antivirus coverage information for this sample, visit VirusTotal

**STEP 8 |** Maintenant que l'administrateur a identifié le logiciel malveillant et que le système de l'utilisateur est en cours de vérification, que faites-vous pour prévenir toute exposition future ? Réponse'A0;: Dans cet exemple, l’administrateur a défini un calendrier sur le pare-feu pour télécharger et installer des signatures Advanced WildFire toutes les 15 minutes et pour télécharger et installer quotidiennement des mises à jour antivirus. Moins d’une heure et demie après que le représentant commercial a téléchargé le fichier infecté, Advanced WildFire a identifié un logiciel malveillant de type « zero-day », généré une signature, l’a ajoutée à la base de données des signatures mises à jour Advanced WildFire fournie par Palo Alto Networks et le pare-feu a téléchargé et installé la nouvelle signature. Ce pare-feu et tous les autres pare-feu Palo Alto Networks configurés pour télécharger des signatures Advanced WildFire et antivirus sont désormais protégés contre ce nouveau logiciel malveillant. La capture d’écran suivante montre le calendrier de mise à jour Advanced WildFire :




Tout ceci se produit bien avant que la majorité des fournisseurs d'antivirus ne soient informés de ce logiciel malveillant au jour 0. Dans cet exemple, en très peu de temps, le logiciel malveillant n'est plus considéré au jour 0 car Palo Alto Networks l'a déjà détecté et a déjà fourni une protection à ses clients pour prévenir toute exposition future.

# Premiers pas avec Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Les étapes suivantes fournissent un flux de travail rapide pour démarrer avec Advanced WildFire™ sur le pare-feu. Si vous souhaitez en apprendre plus sur WildFire avant de commencer, consultez la section Présentation d'Advanced WildFire et lisez la section Meilleures pratiques Advanced WildFire.

Pour plus d'informations sur l'utilisation du cloud privé ou du cloud hybride WildFire, reportez-vous à l'administration de l'appareil WildFire.

Si vous utilisez Advanced WildFire sur Prisma Access, familiarisez-vous avec le produit avant de configurer votre profil de sécurité d'analyse WildFire pour Transfert des fichiers pour une analyse par Advanced WildFire.

**STEP 1 |** Obtenez votre abonnement Advanced WildFire ou WildFire. Si vous ne disposez pas d'un abonnement, vous pouvez tout de même transférer des PE pour l'analyse WildFire.

**STEP 2 |** Choisissez entre Déploiements Advanced WildFire celui qui fonctionne pour vous :

- Cloud Advanced WildFire public : transférez des échantillons à un cloud Advanced WildFire public hébergé par Palo Alto Networks.
- Cloud du gouvernement américain WildFire : transférez des échantillons à un cloud WildFire gouvernemental hébergé par Palo Alto Networks.

*Si vous déployez un cloud privé ou hybride WildFire, reportez-vous à l'administration de l'appareil WildFire.*

**STEP 3 |** Confirmez que votre licence est active sur le pare-feu.

1. Connectez-vous au pare-feu.
2. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que la licence WildFire est active.

   Si la licence WildFire n'est pas affichée, sélectionnez l'une des options de gestion de licence pour activer la licence.

**STEP 4 |** Connectez le pare-feu à WildFire et configurez les paramètres de WildFire.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire** et modifiez les General Settings (Paramètres généraux).
2. Utilisez le champ **WildFire Public Cloud (Cloud WildFire public)** pour transférer des échantillons vers le cloud Advanced WildFire public.
3. Définissez les limites de taille des fichiers que le pare-feu transfère à WildFire et configurez les paramètres de journalisation et de génération de rapports.

   *Il s'agit d'une* Meilleures pratiques Advanced WildFire *de définir la* ***File Size (Taille de fichier)*** *des fichiers PE sur la taille maximale, soit 10 Mo, et de laisser la valeur de* ***File Size (Taille de fichier)*** *définie par défaut pour les autres types de fichiers.*
4. Cliquez sur **OK** pour enregistrer les paramètres généraux WildFire.

**STEP 5 |** Activez, sur le pare-feu, le transfert du trafic SSL décrypté pour analyse par Advanced WildFire.

*Il s'agit d'une* meilleure pratique recommandée Advanced WildFire.

**STEP 6 |** Commencez à envoyer des échantillons pour analyse.

1. Définissez le trafic à transférer vers WildFire pour analyse. (Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **WildFire Analysis (Analyse WildFire)** et modifiez ou **Add (Ajoutez)** un profil d'analyse WildFire.)

   *Il est recommandé d'utiliser le profil d'analyse WildFire par défaut pour garantir une protection complète du trafic autorisé par le pare-feu. Si vous décidez tout de même de créer un profil d'analyse WildFire personnalisé, définissez le transfert de* ***Any (Tout)*** *type de fichier sur le pare-feu. Le pare-feu peut ainsi automatiquement commencer à transférer, aux fins d'analyse, les types de fichiers qui sont nouvellement pris en charge.*
2. Pour chaque règle de profil, définissez le **public-cloud (cloud public)** comme **destination** pour transférer les échantillons vers le cloud Advanced WildFire pour analyse.
3. Associez le profil d'analyse WildFire à une règle de politique de sécurité. Le trafic correspondant à la règle de politique est transféré aux fins d'analyse WildFire (**Policies (Politiques)** > **Security (Sécurité)**, puis **Add (Ajoutez)** ou modifiez une règle de politique de sécurité).

**STEP 7 |** Configurez le pare-feu pour qu’il reçoive les dernières signatures Advanced WildFire.

Les nouvelles signatures Advanced WildFire sont récupérées en temps réel afin de détecter et d’identifier les logiciels malveillants. Si vous utilisez PAN-OS 9.1 ou une version antérieure, vous pouvez recevoir des nouvelles signatures toutes les cinq minutes.

- PAN-OS 9.1 et versions antérieures
  1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** :
     - Vérifiez que les mises à jour **WildFire** sont affichées.
     - Sélectionnez **Check Now (Vérifier maintenant)** pour récupérer les derniers packages de mise à jour de signature.
  2. Définissez le **Schedule (Calendrier)** pour télécharger et installer les dernières signatures Advanced WildFire.
  3. Utilisez le champ **Récurrence** pour définir la fréquence à laquelle le pare-feu recherche de nouvelles mises à jour pour **Chaque minute**.

     *Comme de nouvelles signatures WildFire sont disponibles toutes les cinq minutes, ce paramètre garantit que le pare-feu récupère ces signatures dans la minute suivant la disponibilité.*
  4. Permettez au pare-feu de **Download and Install (Télécharger et installer)** ces mises à jour lorsqu'il les récupère.
  5. Cliquez sur **OK**.
- PAN-OS 10.0.x et versions ultérieures
  1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** :
  2. Vérifiez que les mises à jour de **WildFire** sont affichées.
  3. Sélectionnez Schedule (Programmer) pour configurer la fréquence de mise à jour puis utilisez le champs **Recurrence (Récurrence)** pour configurer le pare-feu et récupérer les signatures WildFire en **Real-time (temps réel)**.
  4. Cliquez sur **OK**.

**STEP 8 |** Commencez l’analyse du trafic afin de détecter les menaces potentielles, y compris les fichiers malveillants qu’Advanced WildFire identifie.

Associez le profil antivirus **default (par défaut)** à une règle de politique de sécurité pour analyser le trafic autorisé par les règles selon les signatures antivirus WildFire (sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis ajoutez ou modifiez les **Actions (Actions)** définies pour une règle).

**STEP 9 |** Contrôlez l’accès aux sites web dont les liens qui y sont associés ont été déterminés comme étant malveillants ou de l’hameçonnage par Advanced WildFire.

*Cette option exige une licence de URL Filtering PAN-DB. Apprenez-en davantage sur URL Filtering et sur la manière dont il vous permet de contrôler l’accès aux sites web et l’envoi des informations d’identification d’entreprise (pour empêcher les tentatives d’hameçonnage) selon la catégorie d’URL.*

Pour configurer URL Filtering :

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **URL Filtering (URL Filtering)** et **Add (Ajouter)** ou modifiez un profil de URL Filtering.
2. Sélectionnez **Categories (Catégories)** et définissez le **Site Access (Accès aux sites)** pour les catégories d’URL malveillantes et d’hameçonnage.
3. **Block (Bloquer)** l’accès des sites de ces catégories aux utilisateurs. Vous pouvez également décider d’autoriser l'accès tout en générant une **Alert (Alerte)** lorsque les utilisateurs accèdent aux sites de ces catégories ce qui vous permet d'avoir une visibilité de ces événements.
4. Activez la prévention contre l’hameçonnage des informations d’identification pour empêcher les utilisateurs d’envoyer leurs informations d’identification à des sites non sécurisés, sans bloquer leur accès à ces sites.
5. Appliquez le profil de URL Filtering nouvellement créé ou mis à jour et associez-le à une règle de politique de sécurité en vue d’appliquer les paramètres du profil au trafic autorisé :
   1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (ajoutez)** ou modifiez une règle de politique de sécurité.
   2. Sélectionnez **Actions (Actions)** et, dans la section Profile Setting (Paramètre de profil), définissez le **Profile Type (Type de profil)** sur Profiles (Profils).
   3. Associez le profil de **URL Filtering (Filtrage des URL)** nouvellement créé ou mis à jour à votre règle de politique de sécurité.
   4. Cliquez sur **OK (OK)** pour enregistrer la règle de politique de sécurité.

**STEP 10 |** Confirmez que le pare-feu transfère correctement les échantillons.

- Si vous avez activé la journalisation des fichiers bénins, sélectionnez **Monitor (Surveillance)** > **WildFire Submissions (Envois WildFire)** et vérifiez que les entrées sont journalisées pour les fichiers bénins envoyés pour analyse. (Si vous souhaitez désactiver la journalisation de fichiers bénins après avoir vérifié que le pare-feu est connecté à WildFire, sélectionnez **Device [Périphérique]** > **Setup [Configuration]** > **WildFire** et décochez la case **Report Benign Files [Signaler les fichiers bénins]**).
- Autres options pour vous permettre de confirmer que le pare-feu a transmis un échantillon spécifique, afficher des exemples du pare-feu en fonction du type de fichier et afficher le nombre total d'échantillons transférés par le pare-feu.
- Test d'un échantillon de fichier malveillant pour tester votre configuration WildFire complète.

**STEP 11 |** Étudiez les résultats de l’analyse.

- Rechercher les résultats de l’analyse :
  - utilisez le pare-feu pour surveiller les logiciels malveillants et affichez les rapports d’analyse WildFire concernant un échantillon.
  - Procédez à l’affichage des rapports sur le portail Advanced WildFire pour tous les échantillons envoyés au cloud Advanced WildFire public, y compris les échantillons que vous avez envoyés manuellement au cloud WildFire public.
  - Utilisez l’API Advanced WildFire pour récupérer les verdicts d’échantillon à partir d’un appareil WildFire.

**STEP 12 |** Etapes suivantes :

Passez en revue et mettez en œuvre les Meilleures pratiques Advanced WildFire.

# Meilleures pratiques pour le déploiement d'Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

Les rubriques suivantes décrivent déploiements et configurations recommandés par Palo Alto Networks lorsque vous utilisez du matériel ou des services WildFire® dans le cadre de votre solution de détection et de prévention des menaces réseau.

- Meilleures pratiques Advanced WildFire

# Meilleures pratiques Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c'est généralement inclus avec votre licence Prisma Access.* |

*Utilisateurs de Prisma Access : reportez-vous à la documentation Prisma Access contenant des informations spécifiques au produit sur l'interface utilisateur.*

- ❑ Suivez les meilleures pratiques pour sécuriser votre réseau contre des évasions de couches 4 et 7 et ainsi garantir la fiabilité de l'identification du contenu et de l'analyse. Assurez-vous particulièrement d'appliquer les meilleures pratiques aux paramètres TCP (**Device [Périphérique]** > **Setup [Configuration]** > **Session** > **TCP Settings [Paramètres TCP]**) et aux paramètres Content-ID™ (**Device [Périphérique]** > **Setup [Configuration]** > **Content-ID** > **Content-ID Settings [Paramètres Content-ID]**).
- ❑ Assurez-vous de disposer également d'un abonnement Prévention des menaces actif. Ensemble, Advanced WildFire® et l'abonnement Prévention des menaces vous offrent une prévention et une détection des menaces complètes.
- ❑ Téléchargez et installez les mises à jour de contenu quotidiennement pour recevoir les dernières mises à jour de produits et les protections contre les menaces générées par Palo Alto Networks. Consultez les instructions d'installation du contenu et des mises à jour logicielles.
- ❑ Si vous utilisez PAN-OS 10.0 ou une version ultérieure, configurez votre pare-feu pour récupérer les signatures Advanced WildFire en temps réel. Cela donne accès aux signatures de logiciels malveillants nouvellement découvertes dès que le cloud public Advanced WildFire peut les générer, empêchant ainsi les attaques de réussir en réduisant la durée d'exposition à l'activité malveillante.
- ❑ Si votre pare-feu est configuré pour décrypter le trafic SSL, activez le transfert du trafic SSL décrypté pour analyse WildFire. Seul un super utilisateur peut activer cette option.
- ❑ Utilisez le profil d'analyse WildFire par défaut pour définir le trafic que le pare-feu doit transférer pour analyse (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **WildFire Analysis (Analyse WildFire)**). Le profil d'analyse WildFire par défaut garantit une protection complète du trafic autorisé par votre politique de sécurité. Il précise que tous les types de fichiers pris en charge par l'ensemble des applications sont transférés aux fins d'analyse par Advanced WildFire, et ce, que les fichiers soient chargés ou téléchargés.

  Si vous décidez de créer un profil d'analyse WildFire personnalisé, il est recommandé de tout de même définir le profil pour qu'il transfère **any (tous)** les types de fichiers. Ainsi, le pare-feu pourra

commencer à transférer automatiquement les types de fichiers dès qu'ils sont pris en charge pour l'analyse.

Pour plus d'informations sur l'application d'un profil d'analyse WildFire au trafic du pare-feu, passez en revue les étapes à suivre pour Transfert des fichiers pour une analyse par Advanced WildFire.

*Les paramètres d'action WildFire dans le Profil antivirus peuvent avoir un impact sur le trafic si celui-ci génère une signature Advanced WildFire entraînant une action de réinitialisation ou d'abandon. Vous pouvez exclure le trafic interne comme les applications de distribution de logiciels par l'entreprise desquelles vous déployez les programmes développés sur mesure afin d'*effectuer la transition en toute sécurité *vers les meilleures pratiques, car il se peut que Advanced WildFire détermine que les programmes sur mesure sont malveillants et qu'il génère une signature pour ceux-ci. Consultez* ***Monitor (Surveillance)*** *>* ***Logs (Journaux)*** *>* ***WildFire Submissions (Envois WildFire)*** *pour voir si des programmes sur mesure déclenchent des signatures Advanced WildFire.*

- Lors de la configuration du pare-feu pour transférer les fichiers pour Transfert des fichiers pour une analyse par Advanced WildFire, vérifiez la **Size Limit (taille limite)** du fichier pour tous les types de fichiers pris en charge. Définissez la valeur de **Size Limit (taille limite)** de tous les autres types de fichiers sur les limites définies par défaut. (Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire (WildFire)** et modifiez les General Settings (Paramètres généraux) pour régler les limites de taille des fichiers selon le type de fichier. Vous pouvez afficher les informations d'aideLes « Informations pour trouver la limite de taille par défaut pour chaque type de fichier).

  **À propos des limites de taille de fichier définies par défaut pour le transfert WildFire**

  Les limites de taille de fichier définies par défaut sur le pare-feu sont conçues pour inclure la majorité des fichiers malveillants qui courent (dont la taille est inférieure aux limites définies par défaut) et pour exclure les gros fichiers qui ne risquent pas d'être malveillants et qui peuvent nuire à la capacité de transfert de WildFire. Étant donné que le pare-feu possède une capacité de transfert de fichiers pour analyse par Advanced WildFire très précise, le transfert d'un haut volume de fichiers volumineux peut amener le pare-feu à ignorer le transfert de certains fichiers. Cette condition se produit lorsque les limites de taille de fichier sont configurées pour un type de fichier qui traverse le pare-feu à un fort débit. Dans une telle situation, un fichier potentiellement malveillant pourrait ne pas être transféré aux fins d'analyse par Advanced WildFire. Songez à cette condition éventuelle si vous aimeriez fixer une limite supérieure à la limite définie par défaut pour des fichiers autres que les fichiers PE.

  Le graphique suivant est une illustration représentative de la distribution de la taille des fichiers malveillants, qui se fonde sur les observations de l'équipe de recherche des menaces Palo Alto Networks. Vous pouvez faire passer les paramètres relatifs aux tailles de fichier qui sont définis par

défaut sur le pare-feu aux tailles de fichier maximales pour profiter d'une légère augmentation du taux de détection des fichiers malveillants de chaque type.

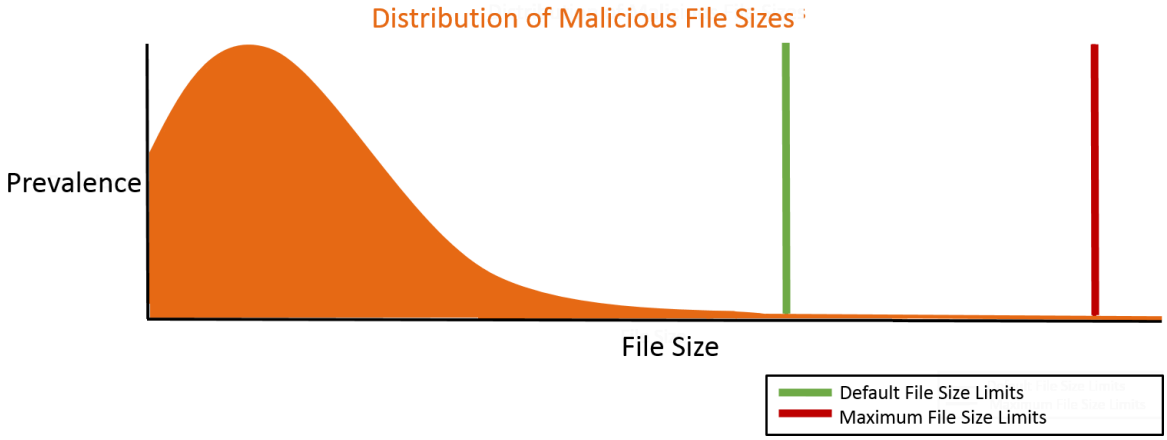



**Figure 1: Limites de taille de fichier recommandées pour détecter les fichiers malveillants anormalement volumineux**

Si vous vous préoccupez particulièrement des fichiers malveillants anormalement volumineux, vous pourriez souhaiter augmenter les limites de taille de fichier à une valeur qui est supérieure aux paramètres par défaut. Dans de telles situations, les paramètres suivants sont recommandés pour détecter les rares fichiers malveillants qui sont très volumineux.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire** et modifiez les General Settings (Paramètres généraux) pour régler la **Size Limit (Limite de taille)** de chaque type de fichier :

| Type de fichier | Recommandations relatives au transfert de fichiers dans PAN-OS 9.0 et versions ultérieures. | Recommandations relatives au transfert de fichiers dans PAN-OS 8.1 |
|---|---|---|
| pe | 16 Mo | 10 Mo |
| apk | 10 Mo | 10 Mo |
| pdf | 3 072 Ko | 1 000 Ko |
| ms-office | 16 384 Ko | 2 000 Ko |
| jar | 5 Mo | 5 Mo |
| flash | 5 Mo | 5 Mo |
| MacOSX | 10 Mo | 1 Mo |
| archive | 50 Mo | 10 Mo |
| Linux | 50 Mo | 10 Mo |
| script | 20 Ko | 20 Ko |

# Configuration de l’analyse Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Les rubriques suivantes décrivent comment activer l’analyse Advanced WildFire™ dans votre déploiement réseau. Vous pouvez configurer les pare-feu Palo Alto Networks pour qu’ils transfèrent automatiquement les fichiers inconnus vers le cloud Advanced WildFire public ou vers un cloud WildFire privé ; vous pouvez également envoyer manuellement des fichiers pour analyse au moyen du portail Advanced WildFire. Les échantillons envoyés pour analyse reçoivent un verdict bénin, indésirable, malveillant ou d’hameçonnage ; un rapport d’analyse détaillé de chacun des échantillons est également généré.

- Transfert des fichiers pour une analyse par Advanced WildFire
- Transfert du trafic SSL décrypté pour analyse par Advanced WildFire
- Activation d’Advanced WildFire Inline ML
- Activer l’analyse du cloud en ligne Advanced WildFire
- Activation du mode d’attente pour la recherche de signatures en temps réel
- Vérification des envois WildFire
- Chargement manuel de fichiers dans le portail WildFire
- Capacité de transfert de fichier de pare-feu par modèle

# Transfert des fichiers pour une analyse par Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Configurez les pare-feu Palo Alto Networks pour qu'ils transfèrent les fichiers ou les liens d'e-mail inconnus et les fichiers bloqués qui correspondent à des signatures antivirus existantes aux fins d’analyse. Utilisez le profil **WildFire Analysis (Analyse WildFire)** pour définir les fichiers qui doivent être transférés à une des options de cloud public Advanced WildFire, puis associez le profil à une règle de sécurité qui déclenchera l’inspection des logiciels malveillants de type « zero-day ».

Précisez le trafic à transférer pour analyse selon l'application utilisée, le type de fichier détecté, les liens contenus dans les courriels ou le sens de transmission de l'échantillon (chargement, téléchargement ou les deux). Par exemple, vous pouvez configurer le pare-feu pour qu'il transfère les fichiers PE (Portable Executables/Exécutable portable) que les utilisateurs essaient de télécharger au cours d'une session de navigation Web. En plus des échantillons inconnus, le pare-feu transfère les fichiers bloqués qui correspondent aux signatures antivirus existantes. Palo Alto Networks dispose ainsi d’une source précieuse de renseignements sur les menaces qui se fondent sur les variantes des fichiers malveillants que les signatures ont réussi à bloquer, mais qui n’avaient jamais été observées.

Si vous utilisez un appareil WildFire pour héberger un cloud WildFire privé, vous pouvez étendre les ressources d'analyses WildFire à un cloud WildFire hybride en configurant le pare-feu pour qu'il poursuive le transfert des fichiers de nature délicate vers votre cloud WildFire privé pour analyse locale et qu'il transfère les types de fichiers de nature moins délicate ou non pris en charge vers le cloud WildFire public. Pour plus d’informations sur l’utilisation et la configuration de l’appareil WildFire, reportez-vous à l’administration de l’appareil WildFire.

Avant de commencer :

- La prise en charge de l’analyse de fichiers peut présenter des différences mineures entre les régions du cloud Advanced WildFire. Reportez-vous à la section : Prise en charge des types de fichiers pour en savoir plus.

- S’il existe un pare-feu entre le pare-feu que vous configurez pour effectuer le transfert des fichiers et le cloud Advanced WildFire, vérifiez que ce pare-feu autorise les ports suivants :

| Port | Usage |
|---|---|
| 443 | Inscription, Téléchargements PPCE, Téléchargements d’échantillons, Récupération de rapports, Envoi de fichiers, Téléchargements de rapports PDF |
| 10443 | Mises à jour dynamiques |

- Strata Cloud Manager
- PAN-OS et Panorama

# Transférer des fichiers pour une analyse par Advanced WildFire (Cloud Management)

***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 Prisma Access Cloud Management, continuez ici.***

**STEP 1 |** Spécifiez le cloud Advanced WildFire vers lequel vous souhaitez transférer des échantillons.

Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW et Prisma Access** > **Security Services (Services de sécurité)** > **WildFire and Antivirus (WildFire et antivirus)** > **General Settings (Paramètres généraux)** et modifiez les paramètres généraux en fonction de votre déploiement cloud WildFire (public, gouvernemental, privé ou hybride).

*Le cloud WildFire américain n’est offert qu’aux agences fédérales américaines, en tant qu’environnement d’analyse facultatif.*

Ajoutez l’URL **WildFire Cloud** pour l’environnement cloud à laquelle transférer des échantillons pour analyse.

**Optionsdu cloud Advanced WildFire public :**

1. Saisissez l'URL du **WildFire Public Cloud (cloud WildFire public)** :
   - États-Unis : **`wildfire.paloaltonetworks.com`**
   - Europe : **`eu.wildfire.paloaltonetworks.com`**
   - Japon : **`jp.wildfire.paloaltonetworks.com`**
   - Singapour : **`sg.wildfire.paloaltonetworks.com`**
   - United Kingdom: **`uk.wildfire.paloaltonetworks.com`**
   - Canada: **`ca.wildfire.paloaltonetworks.com`**
   - Australie : **`au.wildfire.paloaltonetworks.com`**
   - Allemagne : **`de.wildfire.paloaltonetworks.com`**

- Inde : **in.wildfire.paloaltonetworks.com**
- Suisse : **ch.wildfire.paloaltonetworks.com**
- Pologne : **pl.wildfire.paloaltonetworks.com**
- Indonésie : **id.wildfire.paloaltonetworks.com**
- Taïwan : **tw.wildfire.paloaltonetworks.com**
- France : **fr.wildfire.paloaltonetworks.com**
- Qatar : **qatar.wildfire.paloaltonetworks.com**
- Corée du Sud : **kr.wildfire.paloaltonetworks.com**
- Israël : **il.wildfire.paloaltonetworks.com**
- Arabie Saoudite : **sa.wildfire.paloaltonetworks.com**
- Espagne : **es.wildfire.paloaltonetworks.com**

2. Assurez-vous que le champ **WildFire Private Cloud (cloud WildFire privé)** est vierge.

**Options du cloud FedRAMP WildFire :**

1. Saisissez l’URL **du cloud FedRAMP WildFire** :
   - Cloud du gouvernement américain**wildfire.gov.paloaltonetworks.com**
   - Cloud gouvernemental Advanced WildFire : gov-cloud.wildfire.paloaltonetworks.com
   - Cloud Advanced WildFire du secteur public : pubsec-cloud.wildfire.paloaltonetworks.com
2. Assurez-vous que le champ **WildFire Private Cloud (cloud WildFire privé)** est vierge.

**STEP 2 |** Activez Prisma Access pour transférer le trafic SSL décrypté pour l’analyse avancée WildFire en sélectionnant **Allow Forwarding of Decrypted Content (Autoriser le transfert de contenu décrypté)**. Le trafic décrypté est évalué en fonction des règles de la politique de sécurité ; s’il correspond au profil d’analyse WildFire joint à la règle de sécurité, le trafic décrypté est transféré pour analyse avant que le pare-feu ne le crypte de nouveau.

*Le transfert du trafic SSL décrypté pour analyse est une meilleure pratique Advanced WildFire.*

**STEP 3 |** Définissez les limites de taille des échantillons que Prisma Access transmet pour analyse.

*Définir les valeurs de transfert de fichiers sur le paramètre par défaut est une* meilleure pratique Advanced WildFire.

**STEP 4 |** Configurez les paramètres du journal des soumissions.

1. Sélectionnez **Report Benign Files (Rapporter les fichiers bénins)** pour permettre la journalisation des fichiers qui reçoivent un verdict bénin.
2. Sélectionnez **Report Grayware Files (Signaler des fichiers indésirables)** pour permettre la journalisation des fichiers qui reçoivent un verdict indésirable.

**STEP 5 |** Une fois terminé, cliquez sur **Save (Enregistrer)** pour enregistrer les modifications.

**STEP 6 |** Définissez le trafic à transférer pour analyse.

1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et PA)** > **Security Services (Services de sécurité)** > **WildFire and Antivirus (WildFire et antivirus)**, puis **Add Profile (Ajouter un profil)**. Fournissez un **Name (Nom)** et une **Description** pour le profil.
2. Sélectionnez **Add Rule (Ajouter une règle)** pour définir le trafic à transférer pour analyse et donnez à la règle un **Name (Nom)** descriptif, tel que « analyse-PDF-locale ».
3. Définissez une règle de profil à faire correspondre au trafic inconnu pour le transfert des échantillons en vue de leur analyse selon les éléments suivants :
   - **Direction of Traffic (Sens du trafic)** : cette option permet le transfert des fichiers pour analyse selon le sens de transmission du fichier (**Upload [Chargement]**, **Download [Téléchargement]** ou **Upload and Download [Chargement et téléchargement]**). Par exemple, sélectionnez **Upload and Download (Chargement et téléchargement)** pour transférer tous les PDF inconnus pour qu’ils soient analysés, peu importe le sens de transmission.
   - **Applications** : cette option permet le transfert des fichiers pour analyse selon l'application utilisée.
   - **File Types (Types de fichiers)** : cette option permet le transfert des fichiers pour analyse selon les types de fichiers, y compris les liens contenus dans les messages électroniques. Par exemple, sélectionnez **PDF (PDF)** pour envoyer, pour analyse, des PDF inconnus qui ont été détectés par le pare-feu.
   - Sélectionnez la destination du trafic à transférer pour analyse.
     - Sélectionnez **Public Cloud (Cloud public)** afin que l’ensemble du trafic correspondant à la règle soit transféré vers le cloud Advanced WildFire public pour analyse.
     - Sélectionnez **Pivate Cloud (Cloud privé)** afin que l’ensemble du trafic correspondant à la règle soit transféré vers l’appareil WildFire pour analyse.
     - **Save (Enregistrez)** la règle de transfert d’analyse WildFire une fois terminée.
4. **Save (Enregistrez)** le profil de sécurité WildFire et Antivirus.

**STEP 7 |** Activez le profil de sécurité WildFire et antivirus.

Le trafic autorisé par la règle de politique de sécurité est évalué par rapport au profil d’analyse WildFire joint ; Prisma Access transfère le trafic correspondant au profil pour l’analyse WildFire.

**STEP 8 |** Transférez les modifications de configuration.

**STEP 9 |** (Facultatif) Activation d’Advanced WildFire Inline ML

**STEP 10 |** Décidez ce que vous devez faire ensuite...

- Procédez à la vérification des envois WildFire pour confirmer que le pare-feu transfère correctement les fichiers pour analyse.
- Effectuez la surveillance de l'activité WildFire pour évaluer les alertes et les informations données sur les échantillons malveillants.

# Transférer des fichiers pour une analyse avancée des incendies de forêt (PAN-OS et Panorama)

**STEP 1 |** (Pare-feu de la série PA-7000 uniquement) Pour permettre à un pare-feu de la série PA-7000 de transférer des fichiers et des liens d’e-mail pour analyse, vous devez d’abord configurer un port de données sur un NPC comme interface de type carte de journal. Si vous disposez d'un appareil de la série PA-7000 équipé d'une LFC (log forwarding card (carte de transfert des journaux)), vous devez configure a port used by the LFC (configurer un port utilisé par la LFC). Lorsqu’il est configuré, le port de carte de journal ou l’interface LFC a priorité sur le port de gestion lors du transfert d’échantillons.

**STEP 2 |** Spécifiez les Déploiements Advanced WildFire auxquels vous souhaitez transférer les échantillons.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire (WildFire)**, puis modifiez les General Settings (Paramètres généraux) selon votre déploiement de cloud WildFire (public, gouvernement, privé ou hybride).

*Le cloud WildFire américain n’est offert qu’aux agences fédérales américaines, en tant qu’environnement d’analyse facultatif.*

**Cloud Advanced WildFire public :**

1. Saisissez l'URL du **WildFire Public Cloud (cloud WildFire public)** :
   - États-Unis : **wildfire.paloaltonetworks.com**
   - Europe : **eu.wildfire.paloaltonetworks.com**
   - Japon : **jp.wildfire.paloaltonetworks.com**
   - Singapour : **sg.wildfire.paloaltonetworks.com**
   - United Kingdom: **uk.wildfire.paloaltonetworks.com**
   - Canada: **ca.wildfire.paloaltonetworks.com**
   - Australie : **au.wildfire.paloaltonetworks.com**
   - Allemagne : **de.wildfire.paloaltonetworks.com**
   - Inde : **in.wildfire.paloaltonetworks.com**
   - Suisse : **ch.wildfire.paloaltonetworks.com**
   - Pologne : **pl.wildfire.paloaltonetworks.com**
   - Indonésie : **id.wildfire.paloaltonetworks.com**
   - Taïwan : **tw.wildfire.paloaltonetworks.com**
   - France : **fr.wildfire.paloaltonetworks.com**
   - Qatar : **qatar.wildfire.paloaltonetworks.com**
   - Corée du Sud : **kr.wildfire.paloaltonetworks.com**
   - Israël : **il.wildfire.paloaltonetworks.com**
   - Arabie Saoudite : **sa.wildfire.paloaltonetworks.com**
   - Espagne : **es.wildfire.paloaltonetworks.com**
2. Assurez-vous que le champ **WildFire Private Cloud (cloud WildFire privé)** est vierge.

**Options du cloud FedRAMP WildFire :**

1. Saisissez l’URL **du cloud FedRAMP WildFire** :
   - Cloud du gouvernement américain**wildfire.gov.paloaltonetworks.com**
   - Cloud gouvernemental Advanced WildFire : gov-cloud.wildfire.paloaltonetworks.com
   - Cloud Advanced WildFire du secteur public : pubsec-cloud.wildfire.paloaltonetworks.com
2. Assurez-vous que le champ **WildFire Private Cloud (cloud WildFire privé)** est vierge.

**STEP 3 |** Définissez les limites de taille des fichiers que le pare-feu transfère et configurez les paramètres de journalisation et de génération de rapports.

Continuez à modifier les paramètres généraux (**Device (Périphérique)** > **Setup (Configuration)** > **WildFire**).

- Passez en revue les **File Size Limits (Limites de taille de fichier)** pour les fichiers transférés à partir du pare-feu.

  *Une des Meilleures pratiques Advanced WildFire consiste à définir la **File Size (Taille de fichier)** pour les PE sur la limite de taille maximale de 10 Mo et de laisser la **File Size (Taille de fichier)** pour tous les autres types de fichiers sur la valeur par défaut.*

- Sélectionnez **Report Benign Files (Rapporter les fichiers bénins)** pour permettre la journalisation des fichiers qui reçoivent un verdict bénin.
- Sélectionnez **Report Grayware Files (Signaler des fichiers indésirables)** pour permettre la journalisation des fichiers qui reçoivent un verdict indésirable.
- Définissez les informations de session qui sont consignées dans les rapports d’analyse WildFire en modifiant la section Session Information Settings (Paramètres d'informations de session). Par défaut, toutes les informations de session sont affichées dans les rapports d'analyse de WildFire. Décochez les cases correspondant à des champs pour les supprimer des rapports d'analyse WildFire, puis cliquez sur **OK (OK )** pour enregistrer les paramètres.

**STEP 4 |** Définissez le trafic à transférer pour analyse.

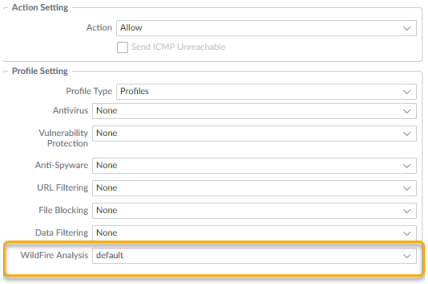
1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **WildFire Analysis (Analyse WildFire)**, puis **Add (Ajouter)** un nouveau profil d'analyse WildFire et donnez un **Name (Nom)** descriptif au profil.
2. **Add (Ajoutez)** une règle au profil pour définir le trafic à transférer vers WildFire pour analyse et donnez à la règle un **Name (Nom)** descriptif, tel quel analyse-PDF-locale.
3. Définissez une règle de profil à faire correspondre au trafic inconnu pour le transfert des échantillons en vue de leur analyse selon les éléments suivants :
   - **Applications** : cette option permet le transfert des fichiers pour analyse selon l'application utilisée.
   - **File Types (Types de fichiers)** : cette option permet le transfert des fichiers pour analyse selon les types de fichiers, y compris les liens contenus dans les messages électroniques. Par exemple, sélectionnez **PDF (PDF)** pour envoyer, pour analyse, des PDF inconnus qui ont été détectés par le pare-feu.
   - **Direction (Sens)** : cette option permet le transfert des fichiers pour analyse selon le sens de transmission du fichier (chargement, téléchargement ou les deux). Par exemple, sélectionnez **both (les deux)** pour transférer tous les PDF inconnus pour qu'ils soient analysés, peu importe le sens de transmission.
4. Cliquez sur **OK** pour enregistrer le profil d'analyse WildFire.

**STEP 5 |** Associez le profil d'analyse WildFire à une règle de politique de sécurité.

Le trafic qui est autorisé par la règle de politique de sécurité est évalué selon le profil d'analyse WildFire joint ; les pare-feu transfèrent le trafic correspondant au profil pour analyse par WildFire.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajoutez)** ou modifiez une règle de politique.
2. Cliquez sur l'onglet **Actions (Actions)** de la règle de politique.
3. Dans la section Paramètres des profils, sélectionnez **Profiles (Profils)** en tant que **Profile Type (Type de profil)** et sélectionnez un profil d'**WildFire Analysis (Analyse WildFire)** à joindre à la règle de politique




**STEP 6 |** Configurez également le pare-feu pour qu’il effectue le transfert du trafic SSL décrypté pour analyse par Advanced WildFire.

*Il s’agit d’une* meilleure pratique recommandée.

**STEP 7 |** (Facultatif) Activation d’Advanced WildFire Inline ML

**STEP 8 |** (Facultatif) Activation du mode d’attente pour la recherche de signatures en temps réel

**STEP 9 |** Passez en revue et mettez en œuvre les Meilleures pratiques Advanced WildFire.

**STEP 10 |** Cliquez sur **Commit (Valider)** pour appliquer les paramètres mis à jour.

**STEP 11 |** (Facultatif) Installez un certificat du périphérique pour mettre à jour vers la dernière version du certificat utilisé par le pare-feu pour communiquer avec les services cloud Palo Alto Networks.

**STEP 12 |** (Facultatif) Configurer les paramètres FQDN du cloud de contenu.

**STEP 13 |** Décidez ce que vous devez faire ensuite...

- Procédez à la vérification des envois WildFire pour confirmer que le pare-feu transfère correctement les fichiers pour analyse.
- Effectuez la surveillance de l'activité WildFire pour évaluer les alertes et les informations données sur les échantillons malveillants.

# Chargement manuel de fichiers dans le portail WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

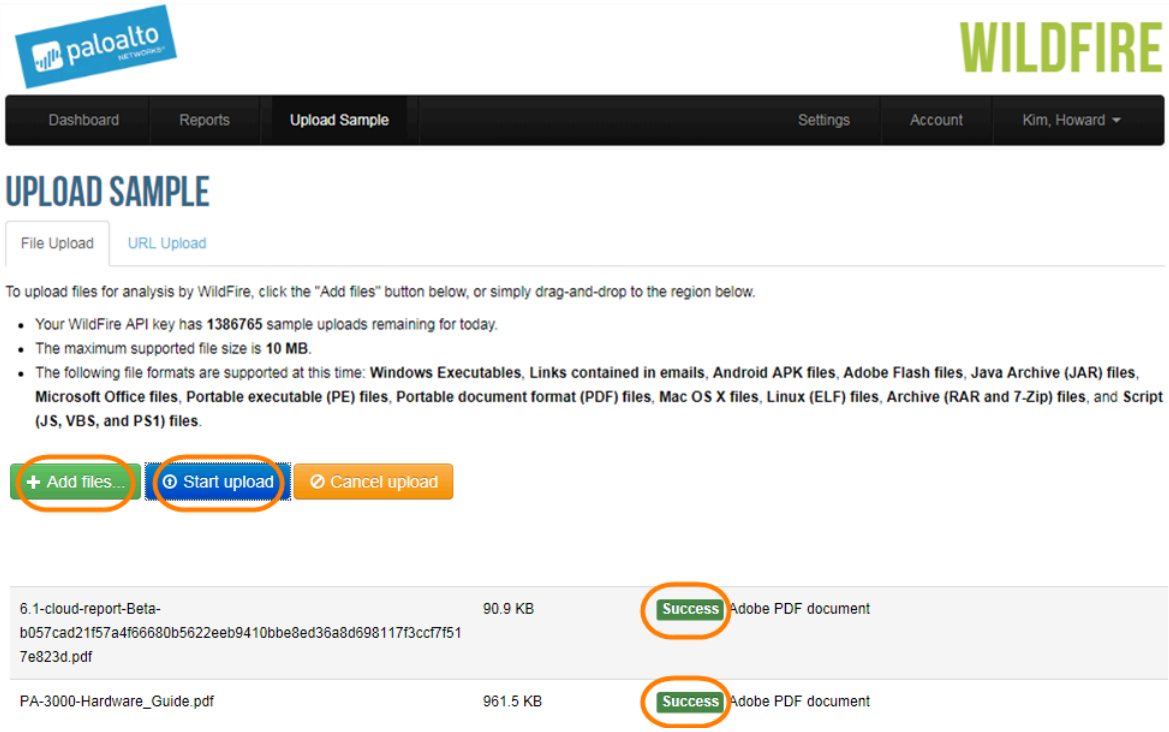
Tous les clients Palo Alto Networks qui possèdent un compte de support peuvent utiliser le portail WildFire de Palo Alto Networks pour envoyer manuellement jusqu’à cinq échantillons par jour pour analyse. Si vous disposez d’un abonnement Advanced WidlFire ou WildFire, vous pouvez envoyer manuellement les échantillons au portail dans le cadre de votre limite quotidienne de 1000 chargements d’échantillon ; toutefois, souvenez-vous que la limite quotidienne de 1000 échantillons inclut aussi les envois de l’API WildFire.

**STEP 1 |** Chargez manuellement des fichiers ou des URL vers le portail WildFire pour analyse.

1. Connectez-vous au portail WildFire.
2. Cliquez sur **Upload Sample (Charger un échantillon)** dans la barre de menus.
   - Pour transférer des fichiers aux fins d’analyse, sélectionnez **File Upload (Charger le fichier)** et **Open (Ouvrez)** les fichiers que vous souhaitez envoyer aux fins d’analyse. Cliquez sur **Start (Démarrer)** pour commencer l’analyse d’un seul fichier ou cliquez sur **Start Upload (Commencer le chargement)** pour envoyer tous les fichiers que vous avez ajoutés pour l’analyse.

- Pour soumettre une URL pour l’analyse, cliquez sur **URL Upload (Chargement d’une URL)**, saisissez une URL et **Submit (Envoyez)** pour analyse.




3. Fermez la fenêtre contextuelle **Uploaded File Information (Informations sur le fichier chargé)**.

**STEP 2 |** Affichez le verdict et les résultats d’analyse du fichier.

Veuillez patienter au moins cinq minutes pour qu’Advanced WildFire analyse l’échantillon.

*Étant donné qu'un chargement manuel n'est associé à aucun pare-feu spécifique, les chargements manuels n'affichent pas d'informations de sessions dans les rapports.*

1. Revenez au tableau de bord du portail WildFire.
2. Dans la section Heure précédente, sélectionnez **Manual (Manuel)** dans la colonne source pour afficher les informations d'analyse des derniers échantillons envoyés manuellement.
3. Recherchez les fichiers ou URL que vous avez chargés et cliquez sur l'icône Détails située à gauche du champ de l'heure de réception.

# Transfert du trafic SSL décrypté pour analyse par Advanced WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Activez, sur le pare-feu, le transfert du trafic SSL décrypté pour analyse par Advanced WildFire. Le trafic que le pare-feu décrypte est évalué en fonction des règles de la politique de sécurité ; s’il correspond au profil d’analyse WildFire joint à la règle de sécurité, le trafic décrypté est transféré pour analyse avant que le pare-feu ne le crypte de nouveau. Seul un super utilisateur peut activer cette option.

*Transférer le trafic SSL décrypté pour analyse est une des* Meilleures pratiques Advanced WildFire.

- Sur un pare-feu sur lequel il n’y a pas plusieurs systèmes virtuels activés :
  1. Si ce n’est pas déjà fait, configurez le pare-feu pour qu’il effectue le décryptage et le Transfert des fichiers pour une analyse par Advanced WildFire.
  2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content ID**.
  3. Modifiez les paramètres Content-ID (Content-ID) et **Allow Forwarding of Decrypted Content (Autoriser le transfert de contenu décrypté)**.
  4. Cliquez sur **OK (OK)** pour enregistrer les modifications.

- Sur un pare-feu prenant en charge la fonction de systèmes virtuels activés :
  1. Si ce n’est pas déjà fait, activez le decryption (décryptage) et la Transfert des fichiers pour une analyse par Advanced WildFire.
  2. Sélectionnez **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)**, cliquez sur le système virtuel à modifier et sur **Allow Forwarding of Decrypted Content (Autoriser le transfert de contenu décrypté)**.

- Pour Prisma Access, cela fait partie des paramètres de votre profil de sécurité **WildFire and Antivirus (WildFire et antivirus)**. Pour en savoir plus, reportez-vous à la section : Transfert des fichiers pour une analyse par Advanced WildFire sur Prisma Access.

# Activer l’analyse du cloud en ligne Advanced WildFire

| Où puis-je l’utiliser ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

Palo Alto Networks Advanced WildFire exploite une série de moteurs de détection ML basés sur le cloud qui fournissent une analyse en ligne des fichiers PE (Portable Executable) traversant votre réseau afin de détecter et de prévenir les logiciels malveillants avancés en temps réel. Comme pour les autres contenus malveillants détectés par WildFire, les menaces détectées par l’analyse du cloud en ligne Advanced WildFire génèrent une signature qui est ensuite diffusée aux clients par le biais d’un package de mise à jour, fournissant ainsi une défense future pour tous les clients de Palo Alto Networks.

Les moteurs basés sur le cloud permettent de détecter des logiciels malveillants jamais vus auparavant (par exemple, un logiciel malveillant de type « zero-day » de Palo Alto Networks, c’est-à-dire des logiciels malveillants inédits dans la nature ou par Palo Alto Networks) et de les empêcher de pénétrer dans votre environnement. L’analyse du cloud en ligne Advanced WildFire utilise un mécanisme de transfert léger sur le pare-feu pour minimiser l’impact sur les performances. Les modèles de ML basés sur le cloud sont mis à jour de manière transparente, pour s’adapter au paysage des menaces en constante évolution, sans nécessiter de mises à jour du contenu ou de prise en charge des versions de fonctionnalités.

L’analyse du cloud en ligne Advanced WildFire est activée et configurée via le profil d’analyse WildFire et nécessite PAN-OS 11.1 ou une version ultérieure avec une licence Advanced WildFire active.

**STEP 1 |** Installez un certificat de périphérique de pare-feu mis à jour utilisé pour vous authentifier auprès du service d’analyse du cloud Advanced WildFire. Répétez l'opération pour tous les pare-feu activés pour l'analyse cloud en ligne.

*Cette étape n’est pas nécessaire si vous avez déjà installé la version actuelle du certificat du périphérique sur votre pare-feu.*

**STEP 2 |** Connectez-vous à l'interface Web PAN-OS.

**STEP 3 |** Pour activer l’analyse du cloud en ligne Advanced WildFire, vous devez disposer d’un abonnement Advanced WildFire actif. Pour en savoir plus, reportez-vous à la section : Licence, enregistrement et activation.

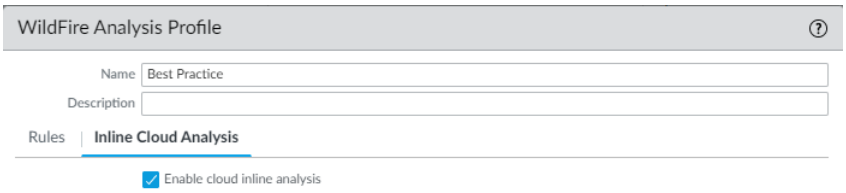
Pour vérifier les abonnements pour lesquels vous disposez de licences actuellement actives, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que les licences adéquates sont disponibles et ne sont pas expirées.


*Si votre licence WildFire actuelle a expiré et que vous installez une licence Advanced WildFire, vous devez d’abord supprimer la licence WildFire du système NGFW avant d’installer la licence Advanced WildFire.*

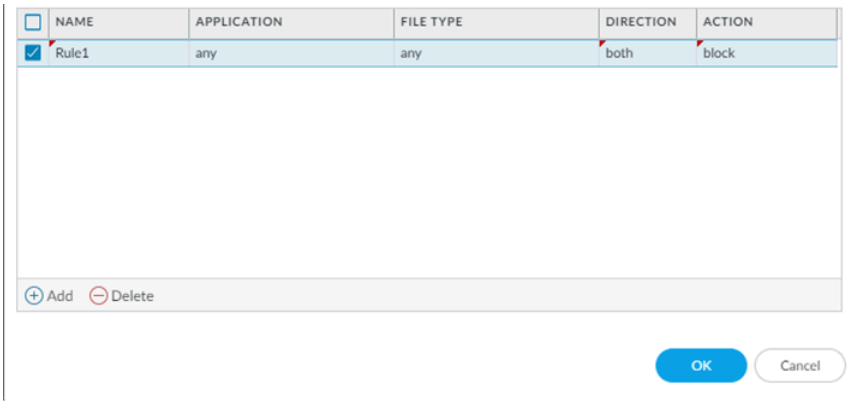
 

**STEP 4 |** Mettez à jour ou créez un profil de sécurité d’analyse WildFire pour activer l’analyse du cloud en ligne Advanced WildFire.

1. Sélectionnez un **profil d’analyse Wildfire** ou **ajoutez**-en un (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **WildFire Analysis (Analyse Wildfire)**).
2. Sélectionnez votre profil d’analyse WildFire, puis accédez à **Inline Cloud Analysis (Analyse du cloud en ligne)** et **Enable cloud inline analysis (Activer l’analyse en ligne dans le cloud)**.




3. Spécifiez une règle définissant une action à effectuer lorsque l’analyse du cloud en ligne Advanced WildFire détecte un logiciel malveillant avancé.




   - Nom : entrez un nom descriptif pour toutes les règles que vous ajoutez au profil (jusqu’à 31 caractères).
   - Application : ajoutez le trafic d’application à mettre en correspondance pour lequel les règles définissant les actions ML du cloud en ligne sont régies.
   - Type de fichier : sélectionnez un type de fichier à analyser à la destination d’analyse définie pour la règle.

     *Seuls les PE (Portable Executable) sont pris en charge pour le moment.*

   - Direction : appliquez la règle au trafic en fonction de la direction de la transmission. Vous pouvez appliquer la règle pour **télécharger** le trafic.
   - Action : configurez l’action à effectuer lorsqu’une menace est détectée à l’aide de l’analyse du cloud en ligne Advanced WildFire. Vous pouvez **permettre** au trafic de l’application de continuer vers la destination ou **bloquer** le trafic provenant d’une source ou d’une source-destination.

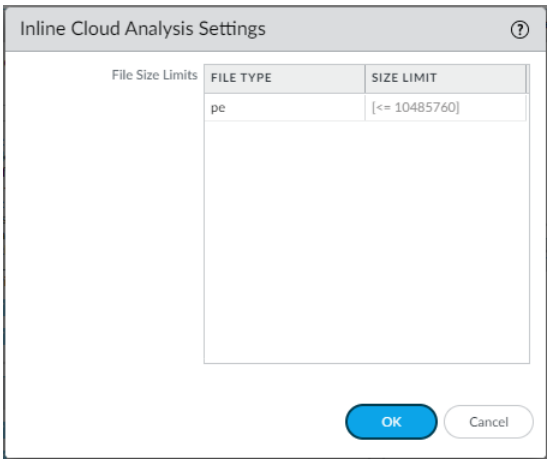
     *Palo Alto Networks recommande de définir l’action sur block (bloquer) pour une sécurité optimale.*

4. Cliquez sur **OK** pour quitter la boîte de dialogue de configuration du profil d’analyse WildFire.

**STEP 5 |** Vérifiez la taille maximale du fichier qui peut être transféré pour l’analyse à l’aide de l’analyse avancée du cloud en ligne WildFire.

*L’analyse du cloud en ligne Advanced WildFire fournit un verdict WildFire rapide. Cependant, un rapport complet sur un échantillon malveillant n’est disponible qu’une fois que l’échantillon a fait l’objet d’une analyse dynamique complète, ce qui peut prendre jusqu’à 30 minutes.*

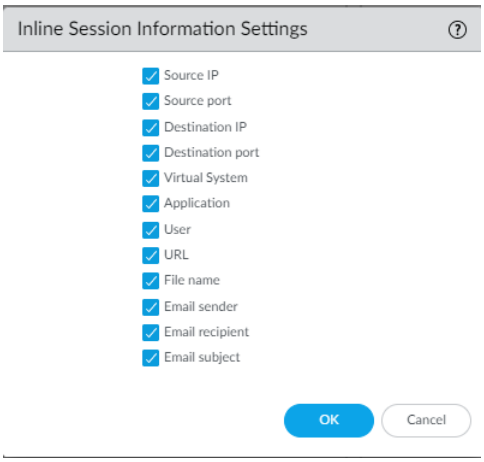



1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Wildfire** > **Inline Cloud Analysis Settings (Paramètres d’analyse du cloud en ligne)** et passez en revue les limites de taille de fichier.
2. Cliquez sur **OK** pour confirmer vos modifications.

**STEP 6 |** Spécifiez les informations de session réseau que le pare-feu transfère à propos d’un échantillon donné. Palo Alto Networks utilise les informations de session pour en apprendre davantage sur le contexte entourant l’événement réseau suspect, sur les indicateurs d'exploitation liés au fichier

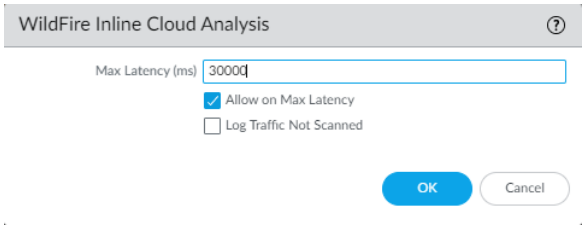
malveillant, sur les hôtes et les clients affectés ainsi que sur les applications utilisées pour transmettre le fichier malveillant. Ces options sont activées par défaut.




1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire** > **Inline Session Information Settings (Paramètres d’informations de session en ligne)** et sélectionnez ou décochez les options si nécessaire.
   - **Source IP (Adresse IP source)** : transfère l’adresse IP source ayant envoyé le fichier inconnu.
   - **Source Port (Port source)** : transfère le port source ayant envoyé le fichier inconnu.
   - **Destination IP (Adresse IP de destination)** : transfère l’adresse IP de destination ayant envoyé le fichier inconnu.
   - **Destination Port (Port de destination)** : transfère le port de destination ayant envoyé le fichier inconnu.
   - **Virtual System (Système virtuel)** : transfère le système virtuel ayant détecté le fichier inconnu.
   - **Application (Application)** : transfère l’application utilisateur ayant transmis le fichier inconnu.
   - **User (Utilisateur)** : transfère l’utilisateur ciblé.
   - **URL (URL)** : transfère l’URL associée au fichier inconnu.
   - **Filename (Nom du fichier)** : transfère le nom du fichier inconnu.
   - **Email sender (Expéditeur de l'e-mail)** : transfère l'expéditeur du lien d’e-mail inconnu (le nom de l’expéditeur de l'e-mail apparaît également dans les rapports et journaux WildFire).
   - **Email recipient (Destinataire de l'e-mail)** : transfère le destinataire du lien d’e-mail inconnu (le nom du destinataire de l'e-mail apparaît également dans les rapports et journaux WildFire).
   - **Email subject (Objet de l'e-mail)** : transfère l'objet du lien d’e-mail inconnu (l’objet de l'e-mail apparaît également dans les rapports et journaux WildFire).
2. Cliquez sur **OK** pour confirmer vos modifications.

**STEP 7 |** Configurez la latence du délai d’expiration et l’action à effectuer lorsque la requête dépasse la latence maximale.




1. Spécifiez l’action à effectuer lorsque les limites de latence sont atteintes pour les requêtes d’analyse du cloud en ligne Advanced WildFire :
   - Latence maximale (ms) : spécifiez le temps de traitement maximal acceptable, en millisecondes, pour que l’analyse du cloud en ligne Advanced WildFire renvoie un résultat.
   - Autoriser sur la latence maximale : permet au pare-feu d’effectuer l’action Allow (Autoriser) lorsque la latence maximale est atteinte. La désélection de cette option définit l’action du pare-feu sur bloquer.
   - Enregistrer le trafic non analysé : permet au pare-feu d’enregistrer les requêtes d’analyse du cloud en ligne Advanced WildFire qui exposent la présence d’un logiciel malveillant avancé, mais qui n’ont pas été traitées par le cloud Advanced WildFire.
2. Cliquez sur **OK** pour confirmer vos modifications.

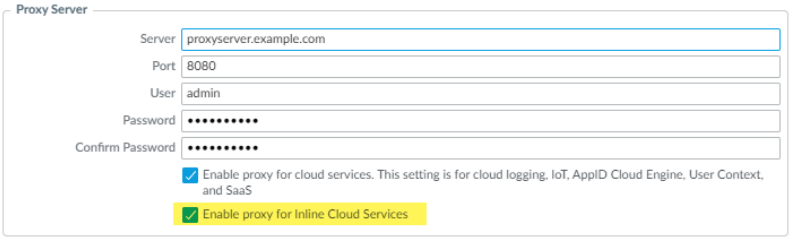
**STEP 8 |** (Obligatoire lorsque le pare-feu est déployé avec un serveur proxy explicite) Configurez le serveur proxy utilisé pour accéder aux serveurs qui facilitent les requêtes générées par toutes les fonctionnalités d’analyse cloud en ligne configurées. Un seul serveur proxy peut être spécifié et

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)** > **Setup (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. (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 9 |** (Recommandé) Configurez le pare-feu pour empêcher le client d’extraire une partie d’un fichier, puis de démarrer une nouvelle session pour extrait le reste d’un fichier une fois que le pare-feu a mis fin à la session d’origine en raison d’une activité malveillante détectée. Cela se produit lorsqu’un navigateur Web implémente l’option HTTP Range. L’activation du paramètre **Allow HTTP partial response (Autoriser la réponse partielle HTTP)** offre une disponibilité maximale mais peut également augmenter le risque de réussite d’une cyberattaque. Palo Alto Networks recommande de désactiver **Allow HTTP partial response (Autoriser la réponse partielle HTTP)** pour une sécurité maximale.

> *Le paramètre **Allow HTTP partial response (Autoriser la réponse partielle HTTP)** est un paramètre global et affecte les transferts de données HTTP qui utilisent l’en-tête RANGE, ce qui peut entraîner des anomalies de service pour certaines applications. Après avoir désactivé **Allow HTTP partial response (Autoriser la réponse partielle HTTP)**, validez le fonctionnement de vos applications stratégiques.*

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (ID-contenu)** > **Content-ID Settings (Paramètres ID-contenu)**.
2. Désélectionner **Allow HTTP partial response (Autoriser la réponse partielle HTTP)** et cliquez sur **OK**.

**STEP 10 |** **Commit (Validez)** vos modifications.

**STEP 11 |** (Facultatif) Configurer les paramètres FQDN du cloud de contenu.

# Activation d’Advanced WildFire Inline ML

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Vous pouvez empêcher les variantes malveillantes de fichiers Portable Executable (PE) et scripts PowerShell de pénétrer votre réseau en temps réel à l’aide d’analyses basées sur l’apprentissage machine (ML) sur le plan de données du pare-feu. En utilisant la technologie d’analyse WildFire® Cloud sur votre plateforme de sécurité, Advanced WildFire Inline ML détecte dynamiquement les fichiers malveillants d’un type donné en évaluant plusieurs détails du fichier, y compris les champs et schémas du décodeur, afin de formuler une classification à forte probabilité d’un fichier. Cette protection s’étend aux variantes actuellement inconnues et aux variantes futures des menaces qui correspondent aux caractéristiques que Palo Alto Networks a identifiées comme étant malveillantes. Advanced WildFire inline ML complète la configuration de protection de votre profil Antivirus. Par ailleurs, vous pouvez préciser des exception de hachage de fichier afin d’exclure les faux positifs rencontrés, ce qui vous permet de créer des règles plus fines pour répondre à vos besoins de sécurité spécifiques.

Pour activer Advanced WildFire Inline ML, vous devez disposer d’un abonnement Advanced WildFire ou WildFire actif, créer (ou modifier) un profil de sécurité antivirus (ou WildFire et Antivirus pour Prisma Access) pour configurer et activer le service, puis attacher le profil antivirus à une règle de politique de sécurité.

*Advanced WildFire Inline ML n’est actuellement pas pris en charge sur l’appareil virtuel VM-50 ou VM50L.*

- Strata Cloud Manager
- PAN-OS et Panorama

## Activer Advanced WildFire Inline ML (PAN-OS et Panorama)

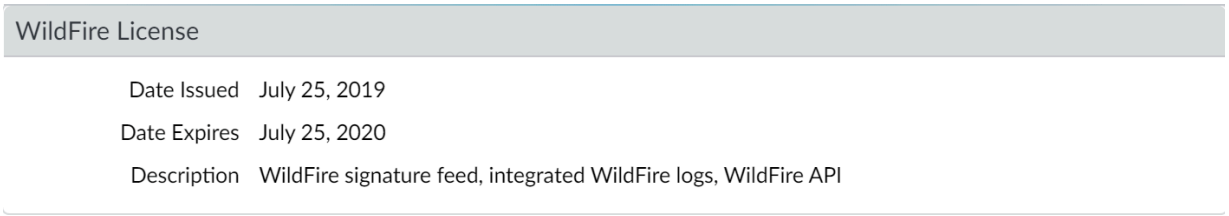
Pour activer votre configuration ML en ligne WildFire, attachez le profil antivirus configuré avec les paramètres d’Inline ML à une règle de politique de sécurité.

Pour contourner Advanced WildFire Inline ML, vous devez définir **Action Setting (paramètre d’action)** sur **disable (for all protocols) (désactiver (pour tous les protocoles))** par modèle ou créer une exception de fichier WildFire Inline ML à l’aide du hachage partiel. Ne configurez pas votre profil antivirus avec des exceptions de signature basées sur les ID de menace WildFire Inline ML. Cela amènera le pare-feu à bloquer tout le trafic de votre réseau vers l’adresse IP.

*WildFire Inline ML n'est actuellement pas pris en charge sur l'appareil virtuel VM-50 ou VM50L.*

**STEP 1 |** Pour profiter de WildFire Inline ML, vous devez avoir un abonnement WildFire actif pour analyser les exécutables Windows.

Vérifiez que vous disposez d’un abonnement WildFire. Pour vérifier quels sont les abonnements pour lesquels vous avez actuellement des licences, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifier que les licences appropriées s'affichent et n'ont pas expiré.

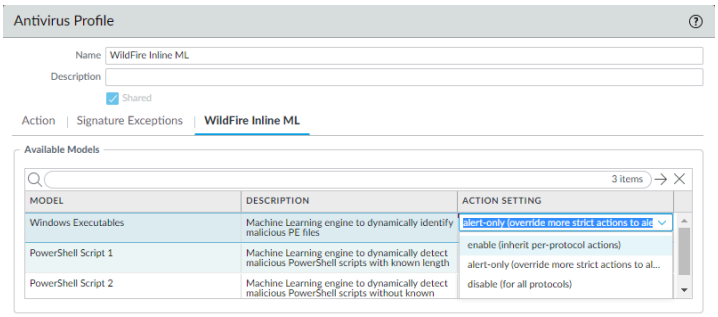



**STEP 2 |** Créez un nouveau profil de sécurité antivirus ou mettez à jour votre ou vos profils de sécurité antivirus existants pour utiliser les modèles de WildFire Inline ML en temps réel.

1. Sélectionnez un **Antivirus Profile (Profil antivirus)** existant ou créez un nouveau profil (sélectionnez **Objects (Objets) > Security Profiles (Profils de sécurité) > Antivirus** et **Add (Ajoutez)** un nouveau profil.
2. Configurez votre profil antivirus.
3. Sélectionnez l’onglet **WildFire Inline ML** et appliquez un **Action Setting (Paramètre d’action)** pour chaque modèle WildFire Inline ML. Cela permet d'appliquer les paramètres des actions WildFire Inline ML configurés pour chaque protocole sur la base d'un modèle. Les moteurs de classification suivants sont disponibles :
   - Exécutables Windows
   - Scripts PowerShell 1
   - Scripts PowerShell 2
   - Format lié exécutable (disponible avec l'installation du contenu PAN-OS version 8367 et ultérieure).
   - MSOffice (disponible avec l'installation du contenu PAN-OS version 8434 et ultérieure).
   - Scripts Shell (disponible avec l'installation du contenu PAN-OS version 8543 et ultérieure).
   - OOXML (disponible avec l’installation de PAN-OS 11.1.3 et versions ultérieures et la version de contenu PAN-OS 8825 et versions ultérieures)

- Mach-O (disponible avec l'installation de PAN-OS 11.1.3 et versions ultérieures et de la version de contenu PAN-OS 8885-8930 et versions ultérieures)




Les paramètres d’action suivants sont disponibles :

- **enable (activer) (hériter des actions par protocole)** : WildFire inspecte le trafic en fonction de vos sélections dans la colonne Action WildFire Inline ML dans la section décodeurs de l'onglet **Action**.
- **alert-only (alerte uniquement) (passer outre des actions plus strictes pour alerter)** : WildFire inspecte le trafic en fonction de vos sélections dans la colonne Action WildFire Inline ML dans la section décodeurs de l'onglet **Action** et annule toute action dont le niveau de gravité est supérieur à `alert (alerte)` (`drop (abandon)`, `reset-client (réinitialisation du client)`, `reset-server (réinitialisation du serveur)`, `reset-both (réinitialisation des deux))alert (alerte)`, qui permet le passage du trafic tout en générant et en enregistrant une alerte dans les journaux des menaces.
- **disable (désactiver) (pour tous les protocoles)** : WildFire permet au trafic de passer sans aucune action de politique.

4. Cliquez sur **OK** pour quitter la fenêtre de configuration du profil antivirus et **Commit (Validez)** vos nouveaux paramètres.

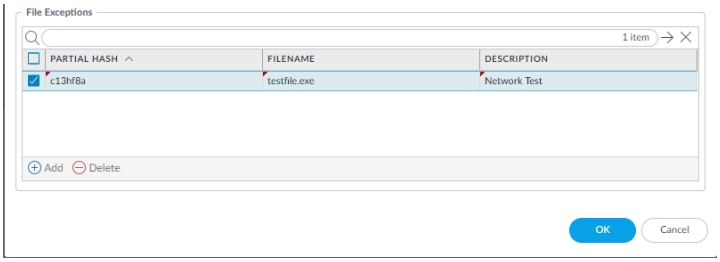
**STEP 3 |** (Facultatif) Ajoutez des exceptions de fichier à votre profil de sécurité antivirus si vous rencontrez des faux positifs. Cela est généralement fait pour les utilisateurs qui ne transfèrent pas de fichiers à

WildFire pour analyse. Vous pouvez ajouter les détails des exceptions de fichiers directement à la liste des exceptions ou en spécifiant un fichier à partir des journaux des menaces.

*Si votre profil de sécurité WildFire Analysis est configuré pour transmettre les types de fichiers analysés à l'aide de WildFire inline ML, les faux positifs sont automatiquement corrigés dès leur réception. Si vous continuez à voir des alertes ml-virus pour des fichiers classés comme bénins par WildFire Analysis, veuillez contacter l'assistance de Palo Alto Networks.*

- Ajout d’exceptions de fichiers directement à la liste des exceptions.
  1. Sélectionnez **Objects (Objets) > Security Profiles (Profils de sécurité) > Antivirus**.
  2. Sélectionnez un profil antivirus pour lequel vous souhaitez exclure des fichiers spécifiques, puis sélectionnez **WildFire Inline ML**.
  3. Ajoutez le hachage, le nom de fichier et la description du fichier que vous voulez exclure de l'application.




  4. Cliquez sur **OK** pour enregistrer le profil antivirus puis **Commit (Validez)** vos mises à jour.
- Ajout d’exceptions de fichiers à partir des entrées des journaux des menaces.
  1. Sélectionnez **Monitor (Moniteur) > Logs (Journaux) > Threat (Menace)** et filtrer les journaux pour le type de menace **ml-virus**. Sélectionnez un journal des menaces pour un fichier pour lequel vous souhaitez créer une exception de fichier.
  2. Accédez à **Detailed Log View (Vue détaillée du journal)** et faites défiler vers le bas jusqu’au volet **Details (Détails)** puis sélectionnez **Create Exception (Créer une exception)**.


  3. Ajoutez une **Description** et cliquez sur **OK** pour ajouter l’exception de fichier.
  4. La nouvelle exception de fichier se trouve dans la liste **File Exceptions (Exceptions de fichier)** sous **Objects (Objets) > Security Profiles (Profils de sécurité) > Antivirus > WildFire Inline ML**.

**STEP 4 |** (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
```

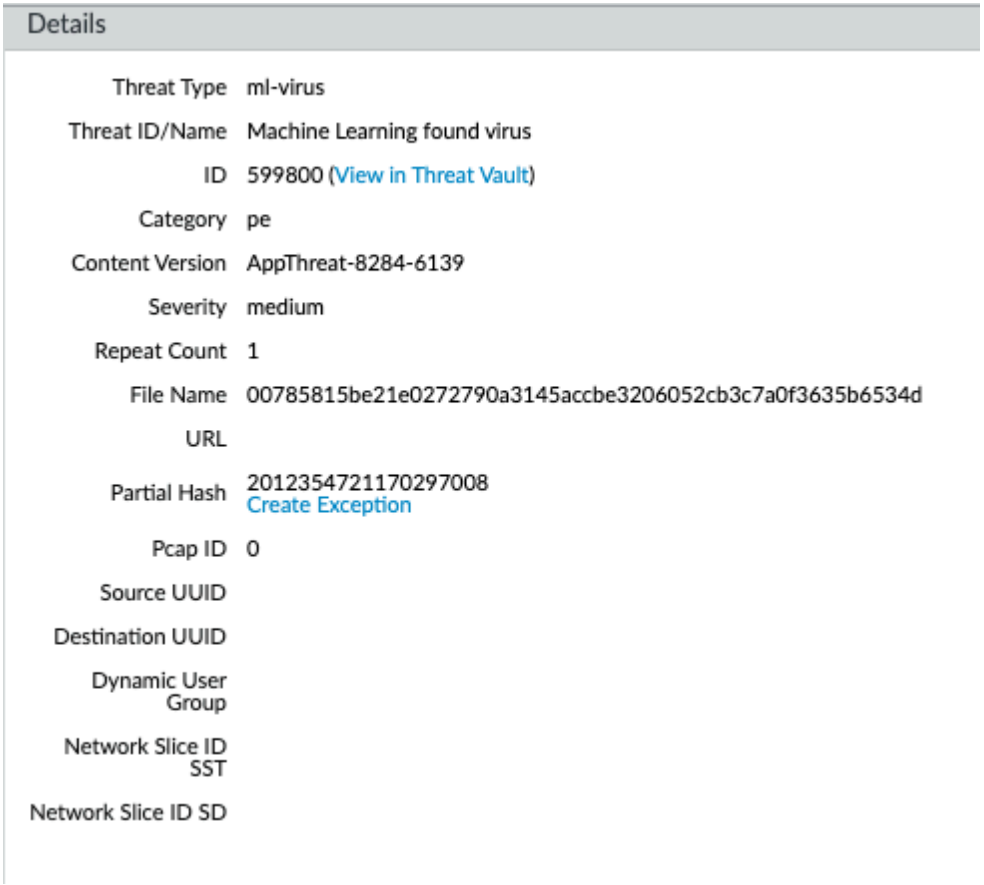
Par exemple :

```
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 Inline ML, vérifiez que le domaine suivant n'est pas bloqué : ml.service.paloaltonetworks.com.

**STEP 5 |** (Facultatif) Configurer les paramètres FQDN du cloud de contenu.

Pour consulter les informations sur les fichiers qui ont été détectés à l'aide de WildFire Inline ML, examinez les journaux de menaces (**Monitor (Moniteur) > Logs (Journaux) > Threat (Menace)**, puis sélectionnez le type de journal dans la liste). Les fichiers qui ont été analysés à l'aide de WildFire Inline ML sont étiquetés avec le type de menace **ml-virus** :



# Activation d’Advanced WildFire Inline ML (Cloud Management)

***Si vous utilisez Panorama pour gérer Prisma Access :***

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

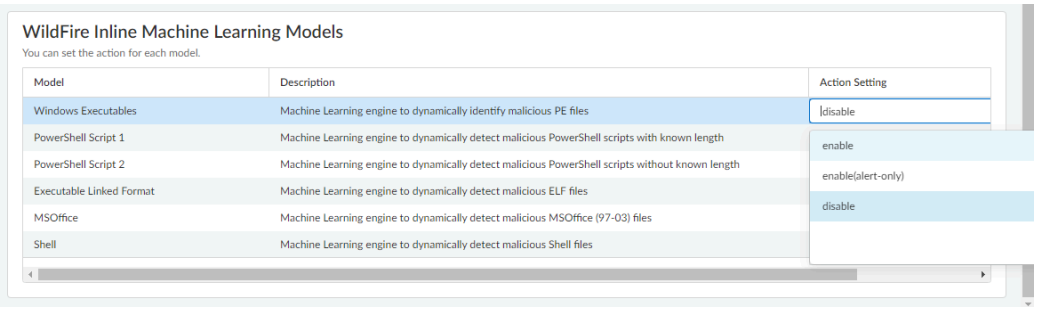
***Si vous utilisez Prisma Access Cloud Management, continuez ici.***

**STEP 1 |** Pour profiter de WildFire Inline ML, vous devez avoir un abonnement WildFire actif dans le cadre de votre abonnement Prisma Access.

Vérifiez que vous avez un abonnement WildFire valide et non expiré.

**STEP 2 |** Mettez à jour votre profil de sécurité **WildFire and Antivirus (WildFire et Antivirus)** existant ou créez-en un nouveau pour utiliser les modèles de WildFire Inline ML en temps réel.

1. Sélectionnez un profil de sécurité **WildFire and Antivirus (WildFire et antivirus)** existant ou créez-en un nouveau (sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access** > **Security Services (Services de sécurité** > **WildFire and Antivirus(WildFire et antivirus)** et **Add Profile (Ajouter un profil)**).
2. Configurez votre WildFire and Antivirus profile (profil WildFire et antivirus) pour transférer des échantillons pour analyse.
3. Sélectionnez **WildFire Inline Machine Learning Models (Modèles WildFire Inline Machine Learning)** et appliquez un **Action Setting (Paramètre d’action)** pour chaque modèle WildFire Inline ML. Cela permet d'appliquer les paramètres des actions WildFire Inline ML configurés pour chaque protocole sur la base d'un modèle.




Les moteurs de classification suivants sont disponibles :

- Exécutables Windows
- Scripts PowerShell 1
- Scripts PowerShell 2
- Format exécutable lié
- MSOffice
- Scripts Shell
- **enable (activer)** : WildFire inspecte le trafic en fonction de vos sélections dans la colonne Action WildFire Inline ML dans la section décodeurs de l’onglet **Action**.
- **enable(alert-only) (activer [alerte uniquement])** : WildFire inspecte le trafic en fonction de vos sélections dans la colonne Action WildFire Inline ML dans la section décodeurs de l’onglet **Action** et annule toute action dont le niveau de gravité est supérieur à `alert (alerte)`

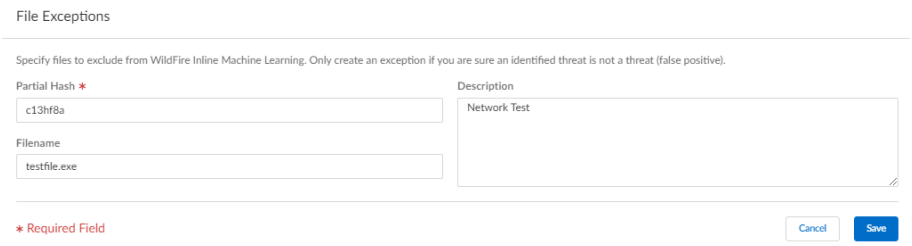
(`drop [abandon]`, `reset-client [réinitialisation du client]`, `reset-server [réinitialisation du serveur]`, `reset-both [réinitialisation des deux]`) `alert (alerte)`, qui permet le passage du trafic tout en générant et en enregistrant une alerte dans les journaux des menaces.

- **disable (désactiver)** : WildFire permet au trafic de passer sans aucune action de stratégie.

**STEP 3 |** (Facultatif) Ajoutez des exceptions de fichier à votre profil de sécurité WildFire et antivirus si vous rencontrez des faux positifs. Cela est généralement fait pour les utilisateurs qui ne transfèrent pas de fichiers à WildFire pour analyse. Vous pouvez ajouter les détails des exceptions de fichiers directement à la liste des exceptions ou en spécifiant un fichier à partir des journaux des menaces.

*Si votre profil de sécurité WildFire Analysis est configuré pour transmettre les types de fichiers analysés à l'aide de WildFire inline ML, les faux positifs sont automatiquement corrigés dès leur réception. Si vous continuez à voir des alertes ml-virus pour des fichiers classés comme bénins par WildFire Analysis, veuillez contacter l'assistance de Palo Alto Networks.*

- Ajout d’exceptions de fichiers directement à la liste des exceptions.
  1. Sélectionnez **Advanced Settings (Paramètres avancés)** et **Add Exception (Ajouter une exception)** dans le volet **File Exceptions (Exceptions de fichiers)**.
  2. Ajoutez le hachage, le nom de fichier et la description du fichier que vous voulez exclure de l'application.




  3. Une fois terminé, cliquez sur **Save (Enregistrer)** pour enregistrer vos exceptions de fichier.

**STEP 4 |** Cliquez sur **Save (Enregistrer)** pour enregistrer votre configuration de profil WildFire et Antivirus et sur push configuration changes (transmettre les modifications de configuration).

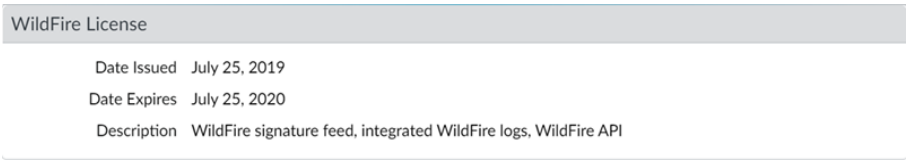
# Activation du mode d’attente pour la recherche de signatures en temps réel

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

Vous pouvez configurer le NGFW pour qu’il conserve le transfert d’un échantillon pendant que le cloud de signatures en temps réel effectue une recherche de signatures. Une fois la recherche terminée, le fichier est remis au client demandeur (ou bloqué), en fonction de la stratégie de sécurité de votre organisation pour des verdicts WildFire spécifiques, empêchant ainsi le transfert initial de logiciels malveillants connus. Vous pouvez configurer le mode d’attente par profil antivirus et appliquer un paramètre global pour le délai d’expiration de la recherche de signatures et l’action associée.

Cette fonctionnalité est disponible pour tous les utilisateurs disposant d’une licence WildFire ou Advanced WildFire active exécutant PAN-OS 11.0.2 ou une version ultérieure.

**STEP 1 |** Pour activer le mode d’attente pour les recherches de signatures en temps réel WildFire, vous devez disposer d’une licence de service d’abonnement WildFire ou Advanced WildFire. Assurez-vous de cliquer sur activate the license (activer la licence) sur le pare-feu si vous ne l’avez pas déjà fait. Pour vérifier les abonnements pour lesquels vous disposez de licences actuellement actives, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que les licences appropriées s’affichent et ne sont pas expirées. L’exemple ci-dessous montre la description de la licence WildFire standard.




**STEP 2 |** Définissez le calendrier pour que le pare-feu récupère les signatures WildFire en temps réel.

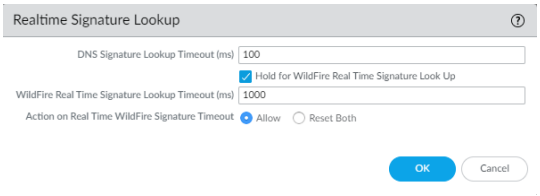
Même lorsque le pare-feu est configuré pour utiliser des signatures en temps réel, des packages de signatures supplémentaires sont toujours installés régulièrement. Cela fournit une source de signature à jour lorsque vous rencontrez des problèmes de connectivité, ainsi qu'un avantage en matière de vitesse, lorsque les signatures sont disponibles localement.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Sélectionnez le **calendrier** des mises à jour de WildFire.
3. Définissez la **récurrence** (la fréquence à laquelle le pare-feu vérifie le serveur de mise à jour de Palo Alto Networks pour rechercher de nouvelles signatures) des mises à jour **en temps réel** .
4. Cliquez sur **OK** pour enregistrer le calendrier des mises à jour de WildFire, puis **validez** vos modifications.

**STEP 3 |** Configurez le paramètre de délai d’expiration et l’action lorsque la demande dépasse le délai d’expiration.

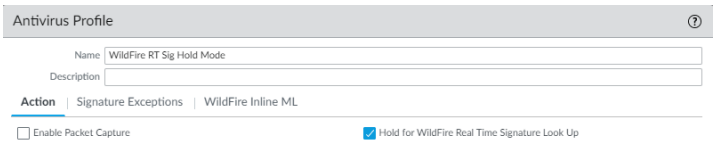
*Vous devez activer le mode d’attente globalement avant d’activer le mode d’attente pour les recherches de signatures en temps réel WildFire par profil antivirus.*




1. Sélectionnez **Device Setup (Configuration du périphérique)** > **ContentID** > **Realtime Signature Lookup (Recherche de signatures en temps réel)**
2. Activez **Hold for WildFire Real Time Signature Look Up (Mise en attente pour la recherche de signatures WildFire en temps réel)**
3. Spécifiez le **WildFire Real Time Signature Lookup Timeout (ms) (Délai d’expiration de la recherche de signatures en temps réel WildFire [ms])** en millisecondes (la valeur par défaut est 1000).

   *Palo Alto Networks recommande d’utiliser la valeur par défaut de 1000 ms, sauf si vous rencontrez des délais d’expiration répétés pendant les tests.*
4. Spécifiez l’**Action On Real Time WildFire Signature Timeout (Action sur le délai d’expiration de la signature WildFire en temps réel)** La valeur par défaut est **Allow (Autoriser)**. Cependant, Palo Alto Networks recommande de définir cette valeur sur **Reset Both (Réinitialiser les deux)** lorsque le mode d’attente est activé. Les options sont les suivantes :
   - Allow (Autoriser) : le NGFW autorise le passage des paquets lorsque le seuil de délai d’expiration est atteint.
   - Reset Both (Réinitialiser les deux) : le NGFW réinitialise la connexion côté client et côté serveur lorsque le seuil de délai d’expiration est atteint.
5. Sélectionnez **OK** lorsque vous avez terminé.

**STEP 4 |** Mettez à jour le profil de sécurité antivirus ou créez-en un nouveau pour activer le mode d’attente pour les recherches de signature en temps réel WildFire.

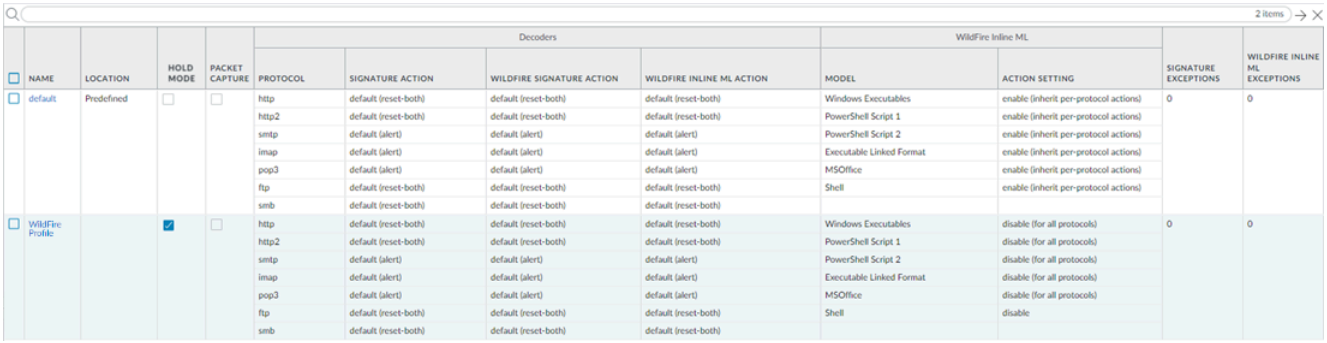



1. Sélectionnez un profil de sécurité antivirus existant ou cliquez sur **Add (Ajouter)** pour en ajouter un nouveau (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Antivirus**).
2. Sélectionnez votre profil de sécurité antivirus, puis accédez à **Action**.
3. Sélectionnez **Hold for WildFire Real Time Signature Look Up (Mise en attente pour la recherche de signature WildFire en temps réel)**.
4. Répétez les étapes 4.1-4.3 pour tous les profils antivirus actifs pour lesquels vous souhaitez activer le mode d’attente pour les recherches de signatures en temps réel WildFire.

**STEP 5 |** **Commit (Validez)** vos modifications.

**STEP 6 |** (Facultatif) Vous pouvez afficher un résumé des paramètres de votre profil de sécurité antivirus, y compris l’activation du mode d’attente, sur la page d’affichage récapitulatif de l’antivirus.



2 items

| NAME | LOCATION | HOLD MODE | PACKET CAPTURE | Decoders | | | | WildFire Inline ML | | SIGNATURE EXCEPTIONS | WILDFIRE INLINE ML EXCEPTIONS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | PROTOCOL | SIGNATURE ACTION | WILDFIRE SIGNATURE ACTION | WILDFIRE INLINE ML ACTION | MODEL | ACTION SETTING | | |
| default | Predefined | | | http | default (reset-both) | default (reset-both) | default (reset-both) | Windows Executables | enable (inherit per-protocol actions) | 0 | 0 |
| | | | | http2 | default (reset-both) | default (reset-both) | default (reset-both) | PowerShell Script 1 | enable (inherit per-protocol actions) | | |
| | | | | smtp | default (alert) | default (alert) | default (alert) | PowerShell Script 2 | enable (inherit per-protocol actions) | | |
| | | | | imap | default (alert) | default (alert) | default (alert) | Executable Linked Format | enable (inherit per-protocol actions) | | |
| | | | | pop3 | default (alert) | default (alert) | default (alert) | MSOffice | enable (inherit per-protocol actions) | | |
| | | | | ftp | default (reset-both) | default (reset-both) | default (reset-both) | Shell | enable (inherit per-protocol actions) | | |
| | | | | smb | default (reset-both) | default (reset-both) | default (reset-both) | | | | |
| WildFire Profile | | ✓ | | http | default (reset-both) | default (reset-both) | default (reset-both) | Windows Executables | disable (for all protocols) | 0 | 0 |
| | | | | http2 | default (reset-both) | default (reset-both) | default (reset-both) | PowerShell Script 1 | disable (for all protocols) | | |
| | | | | smtp | default (alert) | default (alert) | default (alert) | PowerShell Script 2 | disable (for all protocols) | | |
| | | | | imap | default (alert) | default (alert) | default (alert) | Executable Linked Format | disable (for all protocols) | | |
| | | | | pop3 | default (alert) | default (alert) | default (alert) | MSOffice | disable (for all protocols) | | |
| | | | | ftp | default (reset-both) | default (reset-both) | default (reset-both) | Shell | disable | | |
| | | | | smb | default (reset-both) | default (reset-both) | default (reset-both) | | | | |

# Configurer les paramètres FQDN du cloud de contenu

| Où puis-je l’utiliser ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

Vous pouvez spécifier le Fully Qualified Domain Name (nom de domaine complet - FQDN) de contenu cloud utilisé par le NGFW pour gérer les demandes de service Advanced WildFire. 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 FQDN 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.

*Dans certains cas, le FQDN de contenu cloud peut ne pas prendre en charge entièrement les fonctionnalités d’un produit Palo Alto Networks particulier dans certaines régions. Vérifiez que le produit est entièrement pris en charge avant de modifier le FQDN de contenu cloud.*

Selon les services que vous utilisez, le FQDN de contenu cloud facilite les requêtes de service d’analyse, y compris les charges utiles de trafic, qui envoient des données aux serveurs de la région sélectionnée. Si vous spécifiez un FQDN de cloud de contenu qui se trouve en dehors de votre région (par exemple, si vous êtes dans la région UE, mais que vous spécifiez le FQDN de la région APAC), vous risquez d’enfreindre les réglementations légales et de confidentialité de votre organisation. Reportez-vous à la documentation spécifique du produit pour plus d’informations sur l’utilisation du FQDN de contenu cloud par vos produits Palo Alto Networks.

*Si vous rencontrez des problèmes de connectivité de service, vérifiez que le FQDN de contenu cloud configuré n’est pas bloqué.*

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

**STEP 2 |** Sélectionnez (**Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (ID de contenu)** > **Content Cloud Settings (Paramètres de cloud de contenu)**) et modifiez le nom de domaine complet comme vous le souhaitez :

- Par défaut : **hawkeye.services-edge.paloaltonetworks.com**
- Centre des États-Unis (Iowa, États-Unis) : **us.hawkeye.services-edge.paloaltonetworks.com**
- Europe (Francfort, Allemagne) : **eu.hawkeye.services-edge.paloaltonetworks.com**
- Asie-Pacifique (Singapour) : **apac.hawkeye.services-edge.paloaltonetworks.com**
- Inde (Bombay) : **in.hawkeye.services-edge.paloaltonetworks.com**
- Royaume-Uni (Londres, Angleterre) : **uk.hawkeye.services-edge.paloaltonetworks.com**
- France (Paris, France) : **fr.hawkeye.services-edge.paloaltonetworks.com**
- Japon (Tokyo, Japon) : **jp.hawkeye.services-edge.paloaltonetworks.com**
- Australie (Sydney, Australie) : **au.hawkeye.services-edge.paloaltonetworks.com**
- Canada (Montréal, Canada) : **ca.hawkeye.services-edge.paloaltonetworks.com**
- Suisse : **ch.hawkeye.services-edge.paloaltonetworks.com**
- Pays-Bas : **nl.hawkeye.services-edge.paloaltonetworks.com**
- Indonésie : **id.hawkeye.services-edge.paloaltonetworks.com**
- Qatar : **qa.hawkeye.services-edge.paloaltonetworks.com**
- Taïwan : **tw.hawkeye.services-edge.paloaltonetworks.com**
- Pologne : **pl.hawkeye.services-edge.paloaltonetworks.com**
- Corée du Sud (Séoul, Corée du Sud) : **kr.hawkeye.services-edge.paloaltonetworks.com**
- Arabie saoudite : **sa.hawkeye.services-edge.paloaltonetworks.com**
- Italie : **it.hawkeye.services-edge.paloaltonetworks.com**

**STEP 3 |** Cliquez sur **OK**.

# Vérification des envois d’échantillons

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

Testez votre déploiement à l’aide des échantillons de fichier malveillant ; vérifiez également que le pare-feu transfère correctement les fichiers pour analyse WildFire.

- Test d'un échantillon de fichier malveillant
- Vérification du transfert des fichiers

## Test d'un échantillon de fichier malveillant

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire ou WildFire |

Palo Alto Networks fournit des échantillons de fichier malveillant que vous pouvez utiliser pour tester une configuration Advanced WildFire. Suivez les étapes décrites ci-dessous pour télécharger l’échantillon de fichier malveillant, vérifier que le fichier est transféré pour analyse Advanced WildFire et afficher les résultats de l’analyse.

**STEP 1 |** Téléchargez l’une des fichiers malveillants pour le test. Vous pouvez sélectionner PE, APK, MacOSX et ELF.

> *Avant de télécharger un échantillon de fichier malveillant WildFire chiffré, vous devez temporairement désactiver l’entrée *.wildfire.paloaltonetworks.com dans la liste d’exclusion du déchiffrement à la page* ***Device (Périphérique) > Certificate Management (Gestion des périphériques) > SSL Decryption Exclusion (Exclusion du déchiffrement SSL)****. Autrement, l’échantillon ne sera pas correctement téléchargé. Après avoir effectué un test de vérification, assurez-vous de réactiver l’entrée *.wildfire.paloaltonetworks.com à la page d’exclusion du déchiffrement SSL.*

- Si le déchiffrement SSL est activé sur le pare-feu, utilisez l’une des URL suivantes :
  - PE : https://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK : https://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX : https://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF : wildfire.paloaltonetworks.com/publicapi/test/elf
- Si le déchiffrement SSL n’est *pas* activé sur le pare-feu, utilisez l’une des URL suivantes :
  - PE : http://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK : http://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX : http://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF : wildfire.paloaltonetworks.com/publicapi/test/elf

Le fichier d'essai est nommé wildfire-test-*file_type*-file.exe, et chaque fichier d'essai comporte une valeur de hachage SHA-256 unique.

> *Vous pouvez aussi utiliser l'API WildFire pour récupérer le fichier test malveillant. Reportez-vous au* Référentiel de l'API WildFire *pour plus de détails.*

**STEP 2 |** Sur l'interface Web du pare-feu, sélectionnez **Monitor (Surveillance)** > **WildFire Submissions (Envois WildFire)** pour confirmer que le fichier a été transféré pour analyse.

Veuillez patienter au moins cinq minutes pour que les résultats de l'analyse du fichier s'affichent sur la page **WildFire Submissions (Envois WildFire)**. Le fichier d'essai recevra toujours un verdict de fichier malveillant.

## Vérification du transfert des fichiers

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire ou WildFire |

Une fois le pare-feu configuré pour le Transfert des fichiers pour une analyse par Advanced WildFire, servez-vous des options suivantes pour vérifier la connexion entre le pare-feu et le cloud Advanced WildFire public ou WildFire privé et pour surveiller le transfert des fichiers.

*Plusieurs des options pour vérifier qu’un pare-feu transfère les échantillons pour l’analyse sont des commandes CLI ; pour plus de détails sur la prise en main et l’utilisation de la CLI, reportez-vous au* Guide de démarrage rapide de la CLI PAN-OS.

- Vérifiez l’état de la connexion entre le pare-feu et le cloud Advanced WildFire public ou le cloud WildFire privé, ou les deux, y compris le nombre total de fichiers que le pare-feu transfère pour analyse.

  Utilisez la commande **`show wildfire status`** pour :

  - Vérifier l’état du cloud WildFire public ou le cloud WildFire privé auquel le pare-feu est connecté. L’état `Idle` indique que le cloud Advanced WildFire (public ou privé) est prêt à recevoir des fichiers pour analyse.
  - Confirmer les limites de taille configurées pour les fichiers transférés par le pare-feu (**Device (Périphérique)** > **Setup (Configuration)** > **WildFire (WildFire)**).
  - Surveillez le transfert des fichiers, y compris le nombre total de fichiers que le pare-feu transfère pour analyse. Si le pare-feu est déployé sous forme de cloud hybride, le nombre de fichiers qui sont transférés vers le cloud WildFire public et le cloud WildFire privé s'affiche également.

  Les exemples suivants illustrent le résultat de la commande `show wildfire status` pour un pare-feu dans un déploiement de cloud privé :

```
admin@VM-FW> show wildfire status

Connection info:
  Signature verification:            enable
  Server selection:                  enable
  File cache:                        enable
WildFire Public Cloud:
  Server address:                    wildfire.paloaltonetworks.com
  Status:                            Disabled due to configuration
  Best server:
  Device registered:                 no
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
WildFire Private Cloud:
  Server address:                    X.X.X.X
  Status:                            Idle
  Best server:                       X.X.X.X:XXXXX
  Device registered:                 yes
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
File size limit info:
  pe                                 9 MB
  apk                                49 MB
  pdf                                1000 KB
  ms-office                          9500 KB
  jar                                9 MB
  flash                              10 MB
  MacOSX                             1 MB
Forwarding info:
  file idle time out (second):       90
  total concurrent files:            0
  Public Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
  Private Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
```

  Pour afficher les informations de transfert uniquement pour le cloud public Advanced WildFire ou le cloud privé WildFire, utilisez les commandes suivantes :

  - **`show wildfire status channel public`**
  - **`show wildfire status channel private`**

- Affichez les échantillons transférés par le pare-feu selon le type de fichier (y compris les liens d'e-mail).

  *Utilisez cette option pour confirmer que les liens d’e-mail sont transférés pour analyse, étant donné que seuls les liens d’e-mail qui reçoivent un verdict d’échantillon malveillant ou d’hameçonnage sont consignés sous forme d’entrée du journal des **WildFire Submissions (Envois WildFire)** sur le pare-feu, même si la journalisation des échantillons bénins et indésirables est activée. Cela s'explique par le nombre impressionnant d'entrées qui seraient consignées au journal des Envois WildFire si les liens d'e-mail bénins étaient consignés.*

  Utilisez la commande **`show wildfire statistics (afficher les statistiques WildFire)`** pour confirmer les types de fichiers qui sont transférés vers le cloud WildFire public ou privé :

  - La commande affiche le résultat d’un pare-feu en fonctionnement et indique les compteurs de chaque type de fichier que le pare-feu transfère pour analyse. Si un champ de compteurs indique 0, cela signifie que le pare-feu ne transfère pas ce type de fichier.
  - Confirmez que les liens d'e-mail sont transférés pour l'analyse en vérifiant que les compteurs suivants n'indiquent pas zéro :
  - `FWD_CNT_APPENDED_BATCH` : indique le nombre de liens d’e-mails ajoutés à un lot en attente de chargement sur un cloud public Advanced WildFire ou un cloud privé WildFire.
  - `FWD_CNT_LOCAL_FILE` : indique le nombre total de liens d’e-mail chargés sur un cloud Advanced WildFire public ou un cloud WildFire privé.

- Vérifiez que le pare-feu a transféré un échantillon donné et vérifiez l'état de cet échantillon.

  *Cette option peut être utile lors du dépannage, pour :*

  - Confirmez que les échantillons qui n’ont pas encore reçu de verdict ont été correctement transmis par le pare-feu. Puisque les **WildFire Submissions (envois WildFire)** sont journalisés sur le pare-

feu uniquement lorsque l’analyse est terminée et que l’échantillon a reçu un verdict, utilisez cette option pour vérifier que le pare-feu a transféré un échantillon qui est en cours d’analyse.

- Suivez l’état d’un lien d’e-mail ou d’un fichier unique qui était autorisé en vertu de votre politique de sécurité, a été mis en correspondance avec un profil d’analyse WildFire, puis a été transféré pour analyse.
- Vérifiez qu’un pare-feu déployé sous forme de cloud hybride transfère les bons types de fichiers et de liens d’e-mail vers le cloud Advanced WildFire public ou vers un cloud WildFire privé.

Exécutez les commandes de la CLI suivantes sur le pare-feu pour afficher les échantillons que le pare-feu a transférés pour analyse :

- Affichez tous les échantillons transmis par le pare-feu en utilisant la commande de la CLI suivante : **`debug wildfire upload-log`**.
- N’affichez que les échantillons qui ont été transmis au cloud Advanced WildFire public au moyen de la commande de la CLI suivante : **`debug wildfire upload-log channel public`**.
- N'affichez que les échantillons qui ont été transmis au cloud WildFire privé au moyen de la commande de la CLI suivante : **`debug wildfire upload-log channel private`**.

Cet exemple montre le résultat que l’on obtient lorsque les trois commandes présentées ci-dessus sont émises sur un pare-feu déployé sous forme de cloud Advanced WildFire public :

```
user@firewall> debug wildfire upload-log
+ channel   WildFire channel (Public/Private)
  |         Pipe through a command
  <Enter>   Finish input

user@firewall> debug wildfire upload-log channel private

Private Cloud upload logs:


user@firewall> debug wildfire upload-log channel public

Public Cloud upload logs:

    log: 0, filename: support-login.swf
    processed 353590 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 169651, transaction_id: 261
    file_len:  91536, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 1238, app_id: 872
    from XX.XX.XX.XX/XXXX to XX.XXX.XXX.XXX/XXX
    SHA256: 6b2f1a23407ab2db9a17ccdf686bacc6dad7d2489c65ba90dbdf02508b3d4efd

    log: 1, filename: G2M_D_because_12.03.2014_300x250.swf
    processed 611505 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 259049, transaction_id: 260
    file_len:  39206, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 20583, app_id: 872
    from XX.XX.XX.XX/XXXXX to XXX.XX.XXX.XXX/XX
    SHA256: cd52d1b7a7521a14237c1531edb109627fee084806a300d907b57322b1efd6e7
```

- Surveillez les échantillons qui ont été correctement envoyés pour analyse.

  À l'aide de l'interface Web du pare-feu, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **WildFire Submissions (Envois WildFire)**. Tous les fichiers transférés par un pare-feu vers un cloud Advanced WildFire public ou WildFire privé pour analyse sont journalisés à la page des Envois WildFire.

  - Vérifiez le verdict pour un échantillon :

    Par défaut, seuls les échantillons qui reçoivent des verdicts malveillants ou d’hameçonnage sont affichés en tant qu’entrées **WildFire Submissions (Envois WildFire)**. Pour activer la journalisation

des échantillons bénins et/ou de graywares, sélectionnez **Configuration** > **périphérique** > **WildFire** > **Signaler les fichiers bénins/ Signaler les fichiers de graywares**.

*Activez la journalisation des fichiers bénins comme étape de dépannage rapide pour vérifier que le pare-feu transfère les fichiers. Examinez les journaux **WildFire Submissions (Envois WildFire)** pour vérifier que les fichiers sont envoyés pour analyse et qu’ils reçoivent un verdict WildFire (dans le cas présent, il s’agit d’un verdict de fichier bénin).*

- Confirmez l’emplacement de l’analyse d’un échantillon :

  La colonne **WildFire Cloud (Cloud WildFire)** affiche l’emplacement vers lequel le fichier a été transféré et où il a été analysé. C'est une étape qui s’avère utile lors du déploiement d'un cloud hybride.

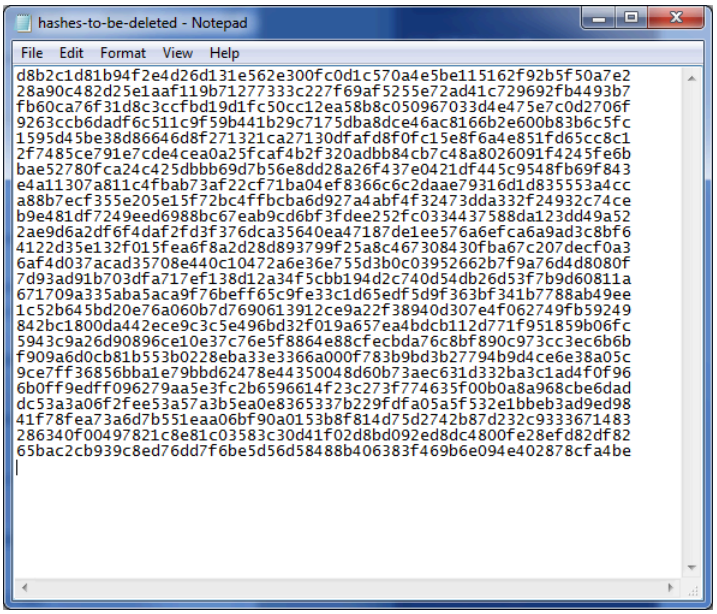
# Demande de suppression d’échantillons

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Les échantillons uniques envoyés au cloud Advanced WildFire à des fins d’analyse peuvent être supprimés si l’utilisateur le souhaite. Les utilisateurs qui sont soumis aux politiques de protection des données, y compris ceux qui doivent respecter le RGPD, peuvent ainsi supprimer de manière permanente les données d’échantillon en se conformant aux politiques de conservation des données de leur organisation. Les données d’échantillon comprennent les données sur les sessions et les chargements et le fichier d’échantillon en tant que tel.

**STEP 1 |** Créer un fichier texte comportant une liste de hachages SHA256 ou MD5 des échantillons à être supprimés. Chaque hachage doit figurer sur une ligne individuelle du fichier et peut comprendre un maximum de 100 échantillons.

*Seuls les fichiers qui sont propres à votre environnement peuvent être supprimés. Si l’on découvre que les fichiers sont disponibles dans d’autres flux privés ou publics, seules les données de session et de chargement d’un compte donné sont supprimées.*

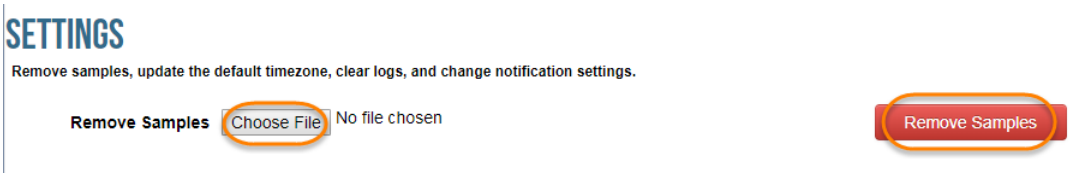


**STEP 2 |** Connectez-vous au portail WildFire à l’aide de vos informations d’identification du support Palo Alto Networks ou de votre compte WildFire.

**STEP 3 |** Sélectionnez **Settings (Paramètres)** dans la barre de menus.

**STEP 4 |** Cliquez sur **Choose File (Choisir le fichier)**, puis sélectionnez le fichier texte d’une liste de hachage que vous avez créé à l’étape 1, puis **Remove Samples (Supprimer les échantillons)**. Vous recevrez une confirmation lorsque le fichier aura été chargé avec succès.




**STEP 5 |** Une fois les échantillons supprimés du cloud WildFire, vous recevrez un courriel de confirmation contenant les détails de la demande. Cela comprend une liste des échantillons dont la suppression a été demandée ainsi que l’état de suppression de chaque échantillon. Ce processus peut prendre jusqu'à sept jours.

```
Dear WildFire customer,
your request for removal of samples from WildFire cloud has been completed. In total 1 samples were removed from WildFire,
the following table shows removal status for each individual sample hash

+------------------------------------------------------------------+---------+--------------------+
| Hash                                                             |  Status |      Information   |
+------------------------------------------------------------------+---------+--------------------+
|6d2ef9f79b5b81429cb1ffeebd6b2919a9a84ec0cc0e5023cbf45a68967c6e1c  | Deleted ||                   |
+------------------------------------------------------------------+---------+--------------------+
```

*Les échantillons qui n'existent pas ou qui ne sont pas propres à votre environnement s’accompagneront des états **Not found (Introuvé)** et **Rejected (Rejeté)**, respectivement.*

# Capacité de transfert de fichiers du pare-feu en fonction du modèle

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series | ❑ Licence Advanced WildFire |

La capacité de transfert de fichiers correspond au débit maximum par minute auquel chaque modèle de pare-feu Palo Alto Networks peut envoyer des fichiers vers le cloud Advanced WildFire® pour analyse. Si le pare-feu atteint la limite par minute, il met les échantillons restants en file d'attente.

La colonne Espace lecteur réservé du tableau ci-dessous représente la taille du lecteur du pare-feu qui est réservée à la mise en file d'attente des fichiers. Si le pare-feu atteint la limite d'espace lecteur, il annule le transfert de nouveaux fichiers vers WildFire jusqu'à ce que plus d'espace soit disponible dans la file d'attente.

*La vitesse à laquelle le pare-feu peut transférer des fichiers vers le cloud Advanced WildFire dépend également de la bande passante de la liaison de chargement depuis le pare-feu.*

| Platform (Plateforme) | Nombre maximum de fichiers par minute | Espace lecteur réservé |
|---|---|---|
| VM-50 | 5 | 100 Go |
| VM-100 | 10 | 100 Go |
| VM-200 | 15 | 200 Go |
| VM-300 | 25 | 200 Go |
| VM-500 | 30 | 250 Mo |
| VM-700 | 40 | 250 Mo |
| PA-220 | 20 | 100 Go |
| PA-400 | 20 | 100 Go |
| PA-820 | 75 | 300 Go |
| PA-850 | 75 | 300 Go |
| Série PA-1400 | 20 | 100 Go |

| Platform (Plateforme) | Nombre maximum de fichiers par minute | Espace lecteur réservé |
|---|---|---|
| PA-3220 | 100 | 200 Go |
| PA-3250/3260 | 100 | 500 Mo |
| Série PA-3400 | 100 | 500 Mo |
| PA-5200 Series | 250 | 1 500 Mo |
| Série PA-5400 | 250 | 1 500 Mo |
| PA-7000 Series | 300 | 1 Go |

# Surveillance de l’activité

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Selon le type de déploiement WildFire™ que vous avez sélectionné (public, privé ou hybride), vous pouvez afficher les échantillons envoyés à WildFire et les résultats d'analyse de chaque échantillon à l'aide du portail WildFire en accédant au pare-feu qui a envoyé l'échantillon (ou Panorama, si vous gérez centralement de multiples pare-feu) ou à l'aide de l'API WildFire.

Une fois que WildFire a analysé un échantillon et rendu un verdict de fichier malveillant, indésirable ou bénin ou d’hameçonnage, un rapport d'analyse détaillé est généré pour l'échantillon. Les rapports d'analyse WildFire qui sont visualisés sur le pare-feu qui a envoyé l'échantillon comprennent également des informations sur la session au cours de laquelle l'échantillon a été détecté. Pour les échantillons qui sont identifiés comme étant malveillants, le rapport d'analyse WildFire donne des détails sur les signatures WildFire existantes qui pourraient être liées à ce logiciel malveillant qui vient d'être identifié et des renseignements sur les attributs, le comportement et l'activité du fichier qui ont indiqué que l'échantillon était malveillant.

Vous pouvez également consulter la façon dont Advanced WildFire s’intègre aux autres applications et services de sécurité de Palo Alto Networks pour protéger votre entreprise contre les menaces, ainsi qu’obtenir une vue de haut niveau de la santé opérationnelle globale de votre déploiement, via le centre de commande Strata Cloud Manager. Le centre de commande fonctionne comme votre page d’accueil NetSec et fournit un résumé complet de la santé, de la sécurité et de l’efficacité de votre réseau, dans un tableau de bord visuel interactif avec de multiples facettes de données pour une évaluation facile et rapide.

Selon la plateforme de produits, vous pouvez accéder à des tableaux de bord de haut niveau qui fournissent des statistiques de détection des logiciels malveillants par Advanced WildFire et des tendances d’utilisation, y compris le contexte de l’activité réseau sous forme d’informations sur l’analyse et plus encore.

Palo Alto Networks fournit plusieurs méthodes pour surveiller l’activité d’Advanced WildFire :

- Centre de commande Strata Cloud Manager
- Tableau de bord Advanced WildFire
- À propos des journaux et de la génération de rapports WildFire
- Configuration des paramètres du journal des envois WildFire.
- Utilisation du portail WildFire pour surveiller les logiciels malveillants

- Rapports d'analyse WildFire : aperçu de près
- Paramétrage des alertes pour les logiciels malveillants

# À propos des journaux et de la génération de rapports WildFire

| Où puis-je l’utiliser ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Vous pouvez Surveillance de l’activitésur le pare-feu, avec le portail WildFire, Strata Cloud Manager ou avec l’API WildFire.

Pour chaque échantillon analysé par WildFire, WildFire classe l'échantillon sous la catégorie appropriée (logiciel malveillant, hameçonnage, fichier indésirable ou fichier bénin) et expose de façon détaillée de l'information sur l'échantillon ainsi que sur son comportement dans le rapport d'analyse WildFire. Les rapports d'analyse de WildFire sont accessibles sur le pare-feu qui a envoyé l'échantillon et sur le cloud WildFire (public ou privé) qui a analysé l'échantillon ou peuvent être récupérés en utilisant l'API WildFire :

- Sur le pare-feu : tous les échantillons envoyés par un pare-feu pour analyse WildFire sont journalisés sous forme d’entrées d’envois WildFire. La colonne Action (Action) du journal d’envois WildFire indique si un fichier a été autorisé ou bloqué par le pare-feu. Pour chaque envoi WildFire, vous pouvez ouvrir une vue détaillée du journal afin de visualiser le rapport d'analyse WildFire qui correspond à l'échantillon ou télécharger le rapport au format PDF.
- Sur le portail WildFire : surveillance de l'activité WildFire, y compris le rapport d'analyse WildFire de chaque échantillon, qui peut également être téléchargé au format PDF. Si le cloud WildFire est déployé sous forme de cloud privé, le portail WildFire offre des précisions sur les échantillons qui sont manuellement chargés vers le portail et sur les échantillons qui sont envoyés par un appareil WildFire lorsque l'intelligence du cloud est activée.

  *L'option pour consulter les rapports d'analyse WildFire sur le portail est uniquement prise en charge pour les appareils WildFire avec la fonction* intelligence du cloud *activée.*
- Sur Strata Cloud Manager : tous les échantillons soumis par Prisma Access pour analyse WildFire sont enregistrés en tant que journaux WildFire et peuvent être lus via la visionneuse de journaux Strata Cloud Manager. Vous pouvez afficher les détails du trafic, le contexte et d’autres détails pertinents, y compris des informations sur la façon dont l’échantillon a progressé dans votre réseau.
- Avec l'API WildFire : récupérez les rapports d'analyse WildFire à partir d'un appareil WildFire ou à partir du cloud WildFire public.

# Rapports d’analyse Advanced WildFire : aperçu de près

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

Accès aux rapports d’analyse Advanced WildFire sur le pare-feu, sur le portail WildFire et sur l’API WildFire.

Les rapports d’analyse Advanced WildFire affichent des informations détaillées sur l’échantillon ainsi que des informations sur les utilisateurs ciblés, des informations d’en-tête d’e-mail (si activé), l’application contenant le fichier et toutes les URL impliquées dans la transmission ou dans l’activité de commande et contrôle du fichier. Les rapports Advanced WildFire contiennent quelques ou toutes les informations décrites dans le tableau suivant selon les informations de session configurées sur le pare-feu ayant transféré le fichier et selon le comportement observé du fichier.

*Lors de l’affichage du rapport Advanced WildFire d’un fichier chargé manuellement dans le portail WildFire ou à l’aide de l’API WildFire, ce rapport ne fournit aucune information de session, car le trafic n’a pas traversé le pare-feu. Par exemple, le rapport ne va pas afficher le pirate/source et la victime/destination.*

| En-tête du rapport | Description |
|---|---|
| **Informations sur le fichier** | • **File Type (Type de fichier)** : Flash, PE, PDF, APK, JAR/Class, archive, linux, script ou MS Office. Ce champ correspond à l'URL nommée pour les rapports de lien d'e-mail HTTP/HTTPS et affiche l'URL qui a été analysée.<br>• **File Signer (Signataire du fichier)** - Entité qui a signé le fichier à des fins d'authenticité.<br>• **Hash Value (Valeur de hachage)** - Le hachage de fichier s'apparente à une empreinte qui identifie de manière unique un fichier pour s'assurer qu'il n'a subi aucune modification. Voici une liste des versions de hachage générées par WildFire pour chaque fichier analysé :<br>  • **SHA-1** - Affiche la valeur SHA-1 du fichier.<br>  • **SHA-256** - Affiche la valeur SHA-256 du fichier.<br>  • **MD5** - Affiche les informations MD5 du fichier.<br>• **File Size (Taille du fichier)** - Taille (en octets) du fichier analysé par WildFire.<br>• **First Seen Timestamp (Horodatage de la première analyse)** - Si le système WildFire a analysé le fichier précédemment, il s'agit de la date et de l'heure auxquelles il a été observé en premier. |

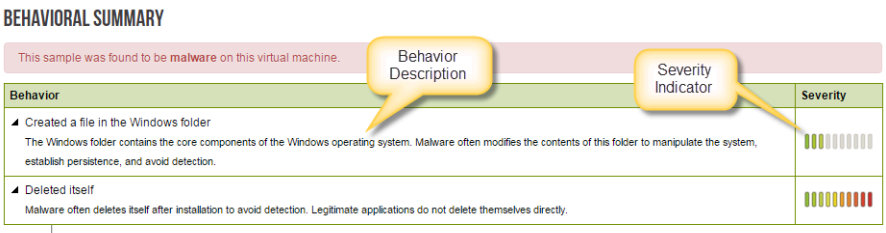
 

| En-tête du rapport | Description |
|---|---|
| | • **Verdict (Verdict)** : affiche les Verdicts de l'analyse :<br>• **Sample File (Échantillon de fichier)** - Cliquez sur le lien **Download File (Télécharger le fichier)** pour télécharger l'échantillon de fichier sur votre système local. Notez que vous pouvez uniquement télécharger des fichiers avec le verdict Malveillant, et non Bénin. |
| **État de la couverture** | Cliquez sur le lien **Virus Total (Total de virus)** pour afficher les informations de couverture antivirus du point d'extrémité des échantillons qui ont déjà été identifiés par d'autres fournisseurs. Si le fichier est inconnu des fournisseurs répertoriés, le message Fichier introuvable s'affiche.<br>De plus, lorsque le rapport est affiché sur le pare-feu, des informations actualisées sur cette signature et la couverture de filtrage des URL fournie par Palo Alto Networks pour protéger contre la menace s'affichent également dans cette section. Ces informations étant récupérées de manière dynamique, elles n'apparaissent pas dans le rapport PDF.<br>Les informations de couverture suivantes sont fournies pour les signatures actives :<br>• **Coverage Type (Type de couverture)** - Le type de protection proposée par Palo Alto Networks (virus, DNS, WildFire ou URL malveillante).<br>• **Signature ID (ID de signature)** - Un numéro d'ID unique attribué à chaque signature fournie par Palo Alto Networks.<br>• **Detail (Détail)** - Le nom connu du virus.<br>• **Date Released (Date de publication)** - La date à laquelle Palo Alto Networks a publié la couverture de protection contre le logiciel malveillant.<br>• **Latest Content Version (Dernière version du contenu)** - Le numéro de version du contenu offrant une protection contre le logiciel malveillant. |
| **Informations sur la session** | Contient des informations de session selon que le trafic traverse ou non le pare-feu ayant transféré l'échantillon. Pour définir les informations de session que WildFire inclura dans les rapports, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire (WildFire)** > **Session Information Settings (Paramètres d'informations de session)**.<br>Les options suivantes sont disponibles'A0;:<br>• IP source<br>• Port source<br>• IP de destination |

| En-tête du rapport | Description |
| --- | --- |
| | • Port de destination<br>• Système virtuel (si l'option Systèmes virtuels multiples est configurée sur le pare-feu)<br>• Application<br>• Utilisateur (si l'option User-ID est configurée sur le pare-feu)<br>• URL<br>• Filename<br>• Expéditeur de l'e-mail<br>• Destinataire de l'e-mail<br>• Objet de l'e-mail<br>Les informations de session comprennent par défaut le champ Status (État), qui indique si le pare-feu a autorisé ou bloqué l’échantillon. |
| **Analyse dynamique** | Si un fichier présente un risque faible et si WildFire peut facilement déterminer qu’il est sûr, seule une analyse statique du fichier est effectuée, au lieu d’une analyse dynamique.<br>Lorsqu’une analyse dynamique est effectuée, cette section contient des onglets présentant les résultats d’analyse pour chaque type d’environnement pour lequel un échantillon a été analysé. Par exemple, l’onglet Machine virtuelle 4 peut afficher un environnement d’analyse fonctionnant sous Windows 7, Adobe Reader 11, Flash 11 et Office 2010.<br>*Sur l'appareil WildFire, une seule machine virtuelle est utilisée pour l'analyse. Vous la sélectionnez en fonction des attributs de l'environnement d’analyse qui correspondent le mieux à votre environnement local. Par exemple, si la plupart des utilisateurs ont Windows 7 32 bits, cette machine virtuelle doit être sélectionnée.* |
| **Récapitulatif comportemental** | Chaque onglet de machine virtuelle récapitule le comportement de l'échantillon de fichier dans l'environnement spécifique. Des exemples montrent si l'échantillon a créé ou modifié des fichiers, démarré un processus, créé de nouveaux processus, modifié le registre ou installé des objets'A0;BHO (Browser Helper Objects).<br>La colonne Gravité indique la gravité de chaque comportement. Un niveau de gravité faible est indiqué par une barre et plus la gravité est élevée, plus le nombre de barres augmente. Ces |

| En-tête du rapport | Description |
| --- | --- |
| | informations sont également ajoutées aux sections d'analyse dynamique et statique.<br>  <br>Voici une description des divers comportements analysés :<br>• **Network Activity (Activité réseau)** - Indique l'activité réseau de l'échantillon, notamment l'accès à d'autres hôtes sur le réseau, les requêtes DNS et l'activité phone-home. Un lien est fourni pour télécharger la capture de paquets.<br>• **Host Activity (by process) (Activité d'hôte (par processus))** - Répertorie les activités exécutées sur l'hôte comme les clés de registre qui ont été définies, modifiées ou supprimées.<br>• **Process Activity (Activité de processus)** - Répertorie les fichiers qui ont démarré un processus parent, le nom du processus et l'action exécutée par ce processus.<br>• **File (Fichier)** - Répertorie les fichiers qui ont démarré des processus enfants, le nom du processus et l'action exécutée par ce processus.<br>• **Mutex** - Si l'échantillon de fichier génère d'autres threads du programme, le nom mutex et le processus parent sont journalisés dans ce champ.<br>• **Activity Timeline (Chronologie des activités)** - Répertorie une liste détaillée de toutes les activités de l'échantillon qui ont été enregistrées. Celle-ci permet de mieux comprendre la séquence d'événements qui s'est produite lors de l'analyse.<br>*Les informations de chronologie des activités sont uniquement disponibles dans l'export'A0;PDF des rapports'A0;WildFire.* |
| **Envoyer malveillant** | Utilisez cette option pour envoyer manuellement l'échantillon à Palo Alto Networks. Le cloud WildFire va analyser de nouveau l'échantillon et générer une signature s'il détermine qu'il est malveillant. Ceci est utile sur un appareil WildFire sur lequel la génération de signatures ou l'intelligence du cloud n'est pas activée, et qui est utilisé pour transférer un logiciel malveillant depuis l'appareil sur le cloud WildFire. |

| En-tête du rapport | Description |
| --- | --- |
| **Signaler un verdict incorrect** | Cliquez sur ce lien pour envoyer l'échantillon à l'équipe de prévention des menaces de Palo Alto Networks, si vous pensez que le verdict est un faux positif ou un faux négatif. L'équipe de prévention des menaces effectuera une autre analyse de l'échantillon pour déterminer s'il doit être reclassé. Si un échantillon malveillant est déterminé comme étant sûr, la signature du fichier est désactivée dans la prochaine mise à jour de signature antivirus ; si un fichier bénin est déterminé comme étant malveillant, une nouvelle signature est générée. Une fois la recherche terminée, vous recevez un e-mail décrivant l'action exécutée. |

# Configuration des paramètres du journal des envois WildFire.

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

Un journal des envois WildFire est un fichier horodaté généré automatiquement qui fournit une piste d’audit pour suivre les événements lorsqu’une plateforme de sécurité réseau Palo Alto Networks transmet des échantillons (liens de fichiers et d’e-mails) au cloud WildFire pour analyse basée sur les paramètres du profil d’analyse WildFire (Objects [Objets] >Security Profiles [Profils de sécurité] > WildFire Analysis [Analyse WildFire]). Des entrées du journal des envois WildFire sont générées pour chaque échantillon transféré au cloud WildFire qui a terminé l’analyse statique et/ou dynamique de l’échantillon. Les entrées du journal des envois WildFire incluent l’action entreprise sur l’échantillon (autoriser ou bloquer), le verdict WildFire pour l’échantillon soumis tel que déterminé par l’analyse WildFire, le niveau de gravité de l’échantillon et d’autres détails.

Par défaut, les journaux d’envois WildFire sont créés pour les échantillons bénins et malveillants ; tandis que les échantillons Indésirables et Bénins ne génèrent aucun journal. Vous pouvez modifier les paramètres du journal de soumission WildFire pour inclure des échantillons Indésirables et Bénins ainsi que des informations de session supplémentaires contenues dans les liens d’e-mails.

Activez les options suivantes pour les journaux **WildFire Submissions (Envois WildFire)**

- Activation de la journalisation des échantillons de fichiers bénins ou indésirables
- Insertion des informations d'en-tête d'e-mail dans les journaux et rapports WildFire

## Activation de la journalisation des échantillons de fichiers bénins ou indésirables

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

La journalisation des échantillons bénins et indésirables est désactivée par défaut. Les liens d'e-mail qui reçoivent des verdicts bénins ou indésirables ne sont pas journalisés.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire (WildFire)**, puis modifiez les **General Settings (Paramètres généraux)**.

**STEP 2 |** Sélectionnez **Report Benign Files (Signaler des fichiers bénins)** ou **Report Grayware Files (Signaler des fichiers indésirables)**, puis cliquez sur **OK** pour enregistrer les paramètres.

# Insertion des informations d'en-tête d'e-mail dans les journaux et rapports WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

Utilisez les étapes suivantes pour inclure les informations d'en-tête d'e-mail (expéditeur, destinataire(s) et objet de l'e-mail) dans les journaux et rapports WildFire.

Les informations de session sont transférées au cloud WildFire conjointement à l'échantillon et servent à la production du rapport d'analyse WildFire. Ni le pare-feu, ni le cloud WildFire ne reçoit, ne stocke ou n'affiche le contenu de l'e-mail.

*Les informations de session peuvent vous permettre d'identifier et de corriger rapidement les menaces détectées dans les e-mails, les pièces jointes ou les liens, y compris d'identifier les destinataires ayant téléchargé du contenu malveillant ou accéder à un tel contenu.*

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire**.

**STEP 2 |** Modifiez la section Paramètres d'informations de session et activez une ou plusieurs des options (**Email sender (Expéditeur de l'e-mail)**, **Email recipient (Destinataire de l'e-mail)** et **Email subject (Objet de l'e-mail)**).

**STEP 3 |** Cliquez sur **OK (OK)** pour enregistrer les paramètres.

# Paramétrage des alertes pour les logiciels malveillants

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire |

Vous pouvez configurer un pare-feu Palo Alto Networks afin d'envoyer une alerte lorsque WildFire identifie un échantillon malveillant ou d’hameçonnage. Vous pouvez également configurer des alertes pour les fichiers bénins ou indésirables, mais pas pour les liens d'e-mail bénins ou indésirables. Cet exemple décrit comment configurer une alerte d'e-mail. Vous pouvez toutefois configurer également le transfert de logs pour établir des alertes qui seront envoyées sous forme de messages Syslog, de pièges SNMP ou d'alertes Panorama.

**STEP 1 |** Configurer un profil de serveur de messagerie.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **Email (Messagerie)**.
2. Cliquez sur **Add (Ajouter)**, puis saisissez un **Name (Nom)** pour le profil. Par exemple, Profil de messagerie WildFire.
3. (Facultatif) Sélectionnez le système virtuel auquel ce profil s'applique dans la liste déroulante **Location (Emplacement)**.
4. Cliquez sur **Add (Ajouter)** pour ajouter une nouvelle entrée de serveur de messagerie, puis saisissez les informations requises pour vous connecter au serveur SMTP (Simple Mail Transport Protocol) et envoyer un e-mail (un maximum de quatre serveurs de messagerie peuvent être ajoutés au profil) :
   - **Server (Serveur)** : nom identifiant le serveur de messagerie (1 à 31 caractères). Ce champ est un simple intitulé et ne doit pas comporter le nom d'hôte d'un serveur'A0;SMTP existant.
   - **Display Name (Nom complet)** : nom à afficher dans le champ De du courrier électronique.
   - **From (De)** : adresse de messagerie à partir de laquelle les e-mails de notification sont envoyés.
   - **To (À)** : adresse de messagerie vers laquelle les e-mails de notification sont envoyés.
   - **Additional Recipient(s) (Autre(s) destinataire(s))** - Saisissez une adresse e-mail à laquelle les notifications seront envoyées à un second destinataire.
   - **Gateway (Passerelle)** : adresse IP ou nom d'hôte de la passerelle SMTP à utiliser pour envoyer les messages électroniques.
5. Cliquez sur **OK** pour enregistrer le profil de serveur.
6. Cliquez sur **Commit (Valider)** pour enregistrer les modifications de la configuration active.

**STEP 2 |** Testez le profil du serveur de messagerie.

1. Sélectionnez **Monitor (Surveillance)** > **PDF Reports (rapports PDF)** > **Email Scheduler (Planificateur de messagerie électronique)**.
2. Cliquez sur **Add (Ajouter)** et sélectionnez le nouveau profil de messagerie dans la liste déroulante **Email Profile (Profil de messagerie)**.
3. Cliquez sur le bouton **Send test (Envoyer un e-mail de test)** et un e-mail de test doit être envoyé aux destinataires définis dans le profil de messagerie.

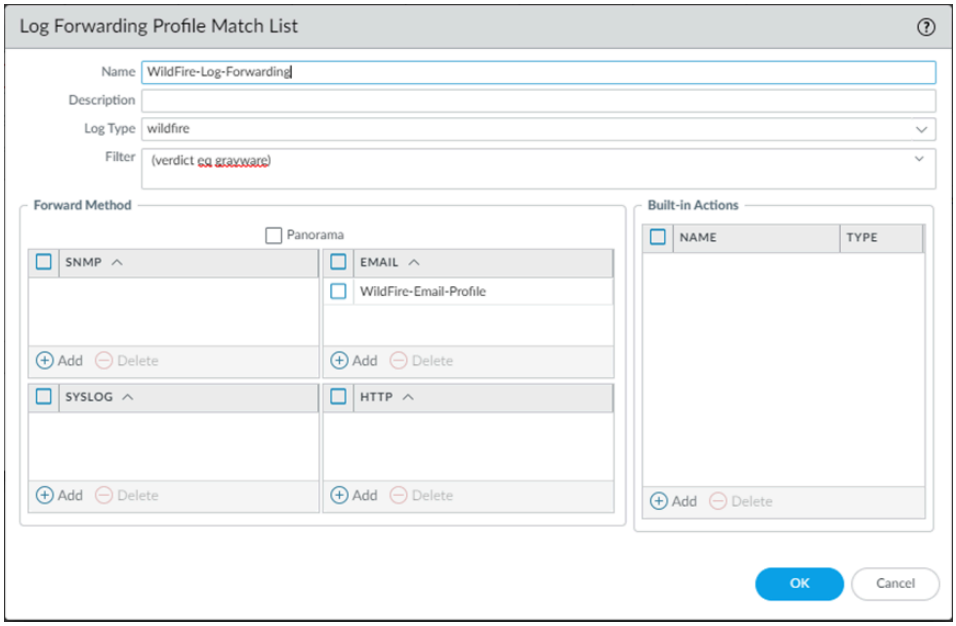
 

**STEP 3 |** Configurez un profil de transfert de logs pour activer l'envoi des logs WildFire vers Panorama, un compte de messagerie, SNMP, un serveur syslog et des requêtes HTTP.

Dans cet exemple, vous établirez l'envoi par e-mail des journaux lorsqu'un échantillon est déterminé comme étant malveillant. Vous pouvez également activer l'envoi des journaux de fichiers bénins et indésirables, ce qui produira plus d'activité lors du test.

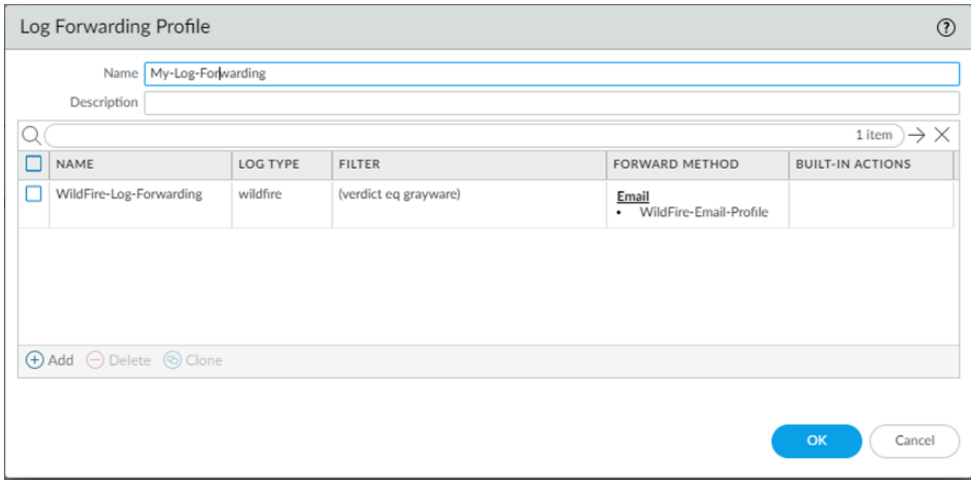
*Le pare-feu ne transmet pas les journaux WildFire des fichiers bloqués à un compte de messagerie électronique.*

1. Sélectionnez **Objects (Objets)** > **Log Forwarding (Transfert des journaux)**.
2. **Add (Ajoutez)** le profil et donnez-lui un nom, par exemple, Transfert-Journaux-WildFire. En option, vous pouvez ajouter une**Description** du profil de transfert des journaux.
3. **Add (Ajoutez)** pour configurer les méthodes de transfert.




   1. Donnez un nom à la**Log Fowarding Profile Match List (Liste de correspondance du profil de transfert de journaux)**.
   2. Sélectionnez le type de journal **WildFire**.
   3. **Filter (Filtrez)** les journaux en utilisant la requête **(verdict eq malicious)**.
   4. Dans les options de**Forward Method (Méthode de transfert)**, choisissez le profil d’e-mail qui a été créé dans l’étape 1 (dans ce cas, le profile d’email), et cliquez sur**OK** pour enregistrer les mises à jour des listes de correspondance.
4. Cliquez sur **OK** à nouveau pour enregistrer les mises à jour du profil de transfert des journaux.




**STEP 4 |** Ajoutez le profil de transfert des journaux à une politique de sécurité utilisée pour le transfert WildFire (avec un profil d'analyse WildFire associé).

Le profil d’analyse WildFire définit le trafic que le pare-feu envoie pour analyse Advance WildFire. Pour configurer un profil d’analyse WildFire et l’associer à une règle de stratégie de sécurité, reportez-vous à la section Transfert des fichiers pour une analyse par Advanced WildFire.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur la politique utilisée pour le transfert WildFire.
2. Dans l'onglet **Actions** de la section **Log Setting (Paramètre des journaux)**, sélectionnez le profil de **Log Forwarding (Transfert des journaux)** que vous avez configuré.
3. Cliquez sur **OK** pour enregistrer les modifications, puis sur **Commit (Valider)** pour valider la configuration.

# Affichage des journaux et des rapports d’analyse WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Les journaux WildFire contiennent des informations sur les échantillons (fichiers et liens d’e-mail) chargés dans le cloud WildFire pour analyse. Il comprend des artefacts, qui sont des propriétés, des activités ou des comportements associés à l’événement enregistré, tels que le type d’application ou l’adresse IP d’un attaquant ainsi que des qualités spécifiques à WildFire, telles que des résultats d’analyse de haut niveau, y compris la catégorisation de l’échantillon comme malveillant, hameçonnage, indésirable ou bénin et détaille des informations sur l’échantillon. L’examen des journaux des envois WildFire peut également indiquer si un utilisateur de vos réseaux a téléchargé un fichier suspect. Le rapport d’analyse WildFire affiche des informations détaillées sur l’échantillon ainsi que des informations sur les utilisateurs ciblés, des informations d’en-tête d’e-mail (si activé), l’application contenant le fichier et toutes les URL impliquées dans la transmission ou dans l’activité de commande et contrôle du fichier. Il vous dit si le fichier est malveillant, s'il a modifié des clés de registre, lu/écrit dans des fichiers, créé de nouveaux fichiers, ouvert des canaux de communication, provoqué des pannes d'applications, s'est intégré à des processus, a téléchargé des fichiers ou présenté d'autres comportements malveillants.

Les journaux WildFire sont affichés sous forme de journaux des envois WildFire sur les pare-feu NGFW, tandis que sur les plateformes de gestion du cloud, vous devez d’abord configurer le transfert des journaux pour télécharger les journaux pertinents sur Strata Logging Service. Cette action affichera ensuite les journaux WildFire sous forme de journaux des menaces (type WildFire).

- Strata Cloud Manager
- PAN-OS et Panorama

## Affichage des journaux et des rapports d’analyse WildFire (PAN-OS et Panorama)

Les échantillons que les pare-feu envoient pour analyse WildFire s'affichent en tant qu'entrées du journal des **WildFire Submissions (Envois WildFire)** sur l'interface Web du pare-feu. Pour chaque entrée WildFire, vous pouvez ouvrir une vue élargie du journal, dans laquelle apparaissent les détails du journal et le rapport d'analyse WildFire de l'échantillon.

*Utilisateurs de Mozilla Firefox : Le rapport d’analyse WildFire s’affiche correctement uniquement dans Firefox v54 et les versions antérieures. Si vous rencontrez des problèmes lors de l’affichage du rapport, envisagez d’utiliser un autre navigateur Web tel que Google Chrome. Vous pouvez également télécharger et ouvrir la version PDF ou afficher le rapport via le portail WildFire.*

**STEP 1 |** Transfert des fichiers pour une analyse par Advanced WildFire.

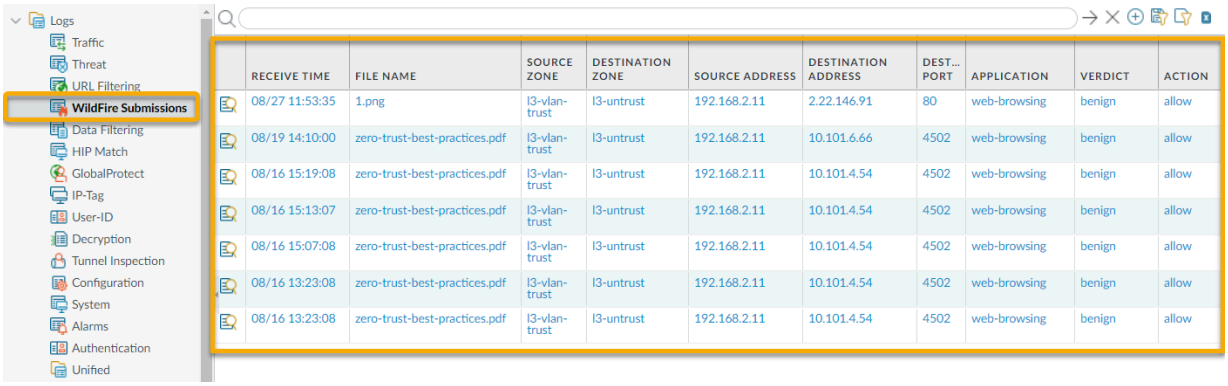
**STEP 2 |** Configuration des paramètres du journal des envois WildFire.

**STEP 3 |** Pour afficher les échantillons envoyés par un pare-feu à un cloud hybride, privé ou public, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **WildFire Submissions (Envois WildFire)**. Une fois l'analyse WildFire d'un échantillon terminée, les résultats sont renvoyés au pare-feu qui a envoyé l'échantillon et sont accessibles dans les journaux des envois WildFire. Les journaux des envois comprennent des renseignements sur un échantillon donné, y compris les renseignements suivants :

- La colonne Verdict indique si l'échantillon est bénin, malveillant ou indésirable ou hameçonnage.
- La colonne Action (Action) indique si le pare-feu a autorisé ou bloqué l’échantillon.
- La colonne Severity (Gravité) indique le degré de menace que pose un échantillon pour une organisation en se basant sur les valeurs suivantes : critique, élevé, moyen, faible et informatif.

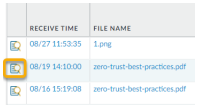
  *Les valeurs des degrés de gravité suivants sont déterminées par une combinaison de valeurs de verdict et d’action.*

  - *Faible : échantillons indésirables dont l’action est définie sur autoriser.*
  - *Élevé : échantillons malveillants dont l’action est définie sur autoriser.*
  - *Informations :*
    - *échantillons bénins dont l’action est définie sur autoriser.*
    - *Les échantillons, peu importe le verdict, dont l'action est définie sur bloquer.*

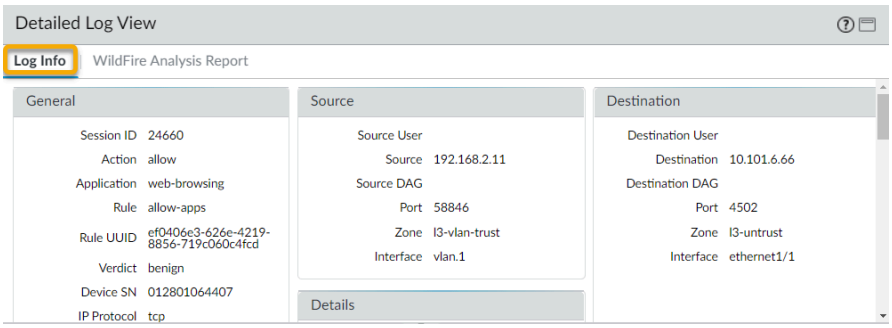


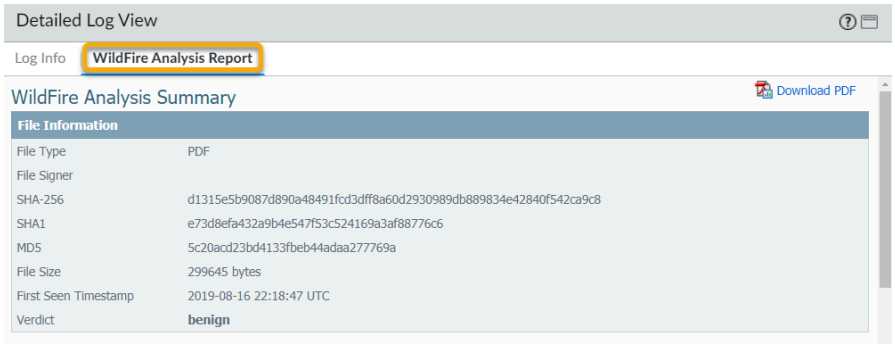
**STEP 4 |** Pour toute entrée, sélectionnez l'icône Détails du log pour ouvrir une vue détaillée pour chaque entrée du journal :




la vue détaillée du journal présente des informations sur le journal et le rapport d'analyse WildFire relatifs à l'entrée. Si la capture de paquet (PCAP) est activée pour le pare-feu, les échantillons de PCAP s'affichent également.




Pour tous les échantillons, le rapport d'analyse WildFire affiche le fichier et les détails de la session. Pour les échantillons de logiciels malveillants, le rapport d'analyse WildFire est élargi pour y inclure des détails sur le comportement et les attributs du fichier qui indiquaient son caractère malveillant.




**STEP 5 |** (Facultatif) **Download PDF (Téléchargez le PDF)** du rapport d'analyse WildFire.

# Affichage des journaux et des rapports d’analyse WildFire (Cloud Management)

***Si vous utilisez Panorama pour gérer Prisma Access,**, vous pouvez suivre le processus ci-dessous pour accéder au contenu dans Prisma Access ou passer à l’onglet **PAN-OS** et suivre les instructions.*

**STEP 1 |** Utilisez les informations d’identification associées à votre compte de support Palo Alto Networks et connectez-vous à Strata Cloud Manager l’application sur le hub.

*Pour plus d’informations sur l’utilisation de l’Activity (Activité), reportez-vous à Log Viewer (Visionneuse de journaux).*

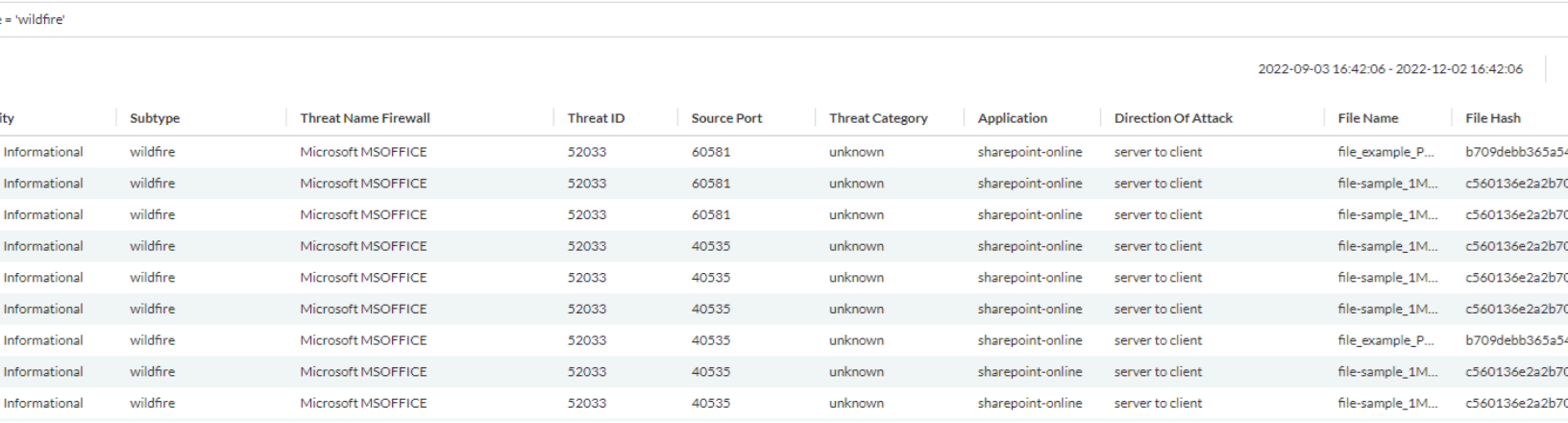
**STEP 2 |** Filtrez les journaux des menaces pour afficher vos envois d’échantillons WildFire dans Prisma Access.

1. Sélectionnez **Incidents and Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**.
2. Remplacez le type de journal à rechercher par **Threat (Menace)**.
3. Créez un filtre de recherche à l’aide du sous-type WildFire utilisé pour indiquer un exemple de soumission WildFire à l’aide du générateur de requêtes. Par exemple, vous pouvez utiliser `sub_type.value = 'wildfire'` pour afficher vos journaux WildFire. Ajustez les

critères de recherche si nécessaire pour votre recherche, y compris des paramètres de requête supplémentaires (tels que le niveau de gravité et l’action) ainsi qu’une plage de dates.

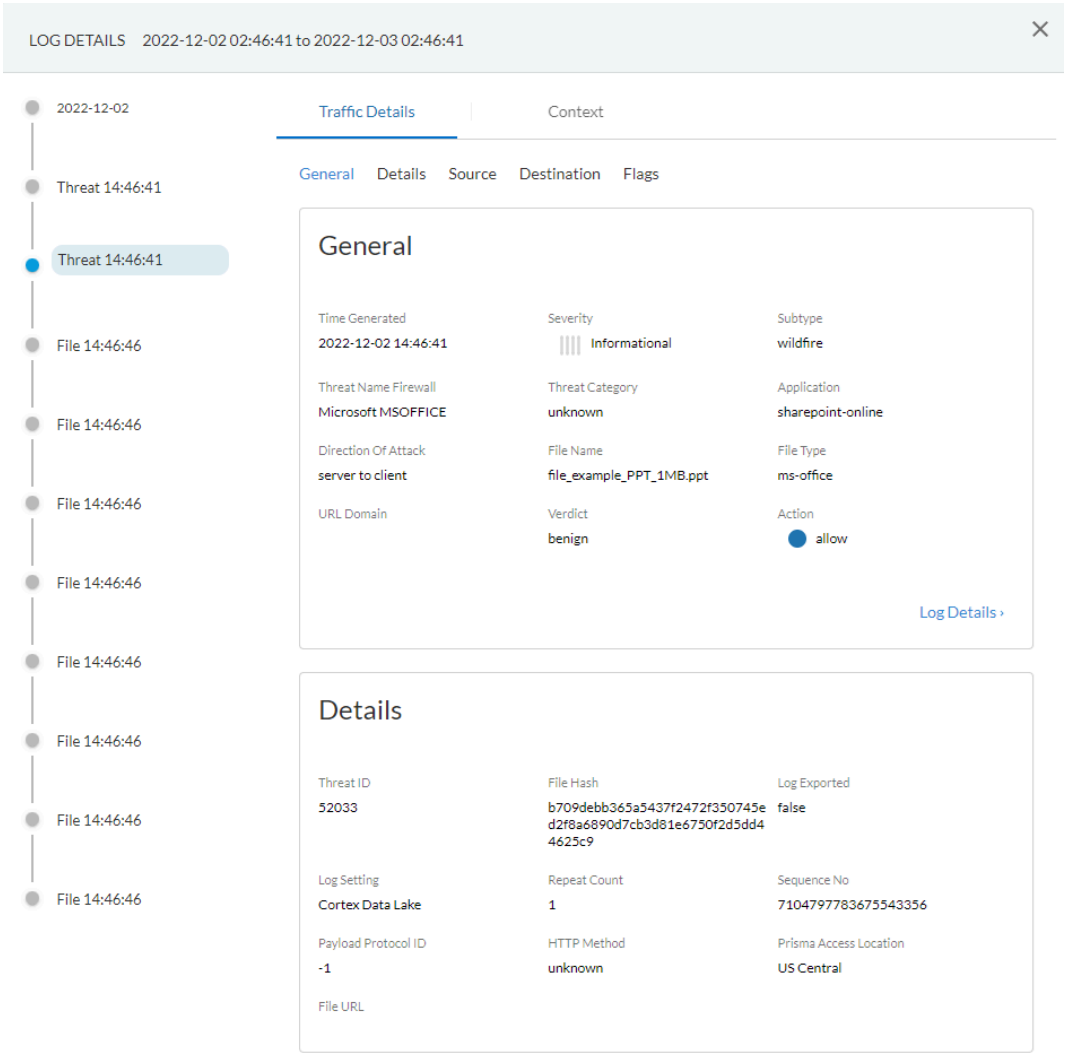
*Pour afficher le rapport d’analyse WildFire, vous devez vous connecter au portail WildFire et utiliser la valeur de hachage ou le nom du fichier pour récupérer le fichier du rapport. Pour en savoir plus, reportez-vous à la section* Affichage des rapports sur le portail WildFire.


= 'wildfire'

2022-09-03 16:42:06 - 2022-12-02 16:42:06

| ity | Subtype | Threat Name Firewall | Threat ID | Source Port | Threat Category | Application | Direction Of Attack | File Name | File Hash |
|---|---|---|---|---|---|---|---|---|---|
| Informational | wildfire | Microsoft MSOFFICE | 52033 | 60581 | unknown | sharepoint-online | server to client | file_example_P... | b709debb365a5 |
| Informational | wildfire | Microsoft MSOFFICE | 52033 | 60581 | unknown | sharepoint-online | server to client | file-sample_1M... | c560136e2a2b70 |
| Informational | wildfire | Microsoft MSOFFICE | 52033 | 60581 | unknown | sharepoint-online | server to client | file-sample_1M... | c560136e2a2b70 |
| Informational | wildfire | Microsoft MSOFFICE | 52033 | 40535 | unknown | sharepoint-online | server to client | file-sample_1M... | c560136e2a2b70 |
| Informational | wildfire | Microsoft MSOFFICE | 52033 | 40535 | unknown | sharepoint-online | server to client | file-sample_1M... | c560136e2a2b70 |
| Informational | wildfire | Microsoft MSOFFICE | 52033 | 40535 | unknown | sharepoint-online | server to client | file-sample_1M... | c560136e2a2b70 |
| Informational | wildfire | Microsoft MSOFFICE | 52033 | 40535 | unknown | sharepoint-online | server to client | file_example_P... | b709debb365a5 |
| Informational | wildfire | Microsoft MSOFFICE | 52033 | 40535 | unknown | sharepoint-online | server to client | file-sample_1M... | c560136e2a2b70 |
| Informational | wildfire | Microsoft MSOFFICE | 52033 | 40535 | unknown | sharepoint-online | server to client | file-sample_1M... | c560136e2a2b70 |

4. Exécutez la requête une fois que vous avez fini d’assembler votre filtre.
5. Sélectionnez une entrée de journal dans les résultats pour afficher les détails du journal.
6. Le **Subtype (Sous-type)** du journal des menaces s’affiche dans le volet **General (Général)** avec d’autres informations sur l’échantillon. D’autres détails pertinents sur la menace sont affichés dans les fenêtres correspondantes.



# Utilisation du portail WildFire pour surveiller les logiciels malveillants

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Connectez-vous au portail WildFire de Palo Alto Networks à l'aide de vos informations d'identification du support Palo Alto Networks ou de votre compte WildFire. Le portail affiche le tableau de bord, qui répertorie les informations des rapports de synthèse de l'ensemble des pare-feux associés à un abonnement WildFire spécifique ou à un compte de support. Pour chaque périphérique répertorié, le portail propose des statistiques sur le nombre d'échantillons infectés par des logiciels malveillants, les échantillons bénins ayant été analysés et le nombre de fichiers attendant d'être analysés. Votre compte du portail WildFire affiche des données sur chacun des échantillons envoyés par les pare-feu de votre réseau qui sont connectés au cloud WildFire public ainsi que des données sur les échantillons envoyés manuellement au portail. De plus, si vous avez enabled a WildFire appliance to forward malware to the WildFire public cloud (autorisé un appareil WildFire à transférer les fichiers et logiciels malveillants vers le cloud WildFire public) pour qu'une signature soit générée et distribuée, les rapports de ces échantillons malveillants sont également accessibles sur le portail.

Reportez-vous aux sections suivantes pour obtenir de plus amples précisions sur l'utilisation du portail WildFire pour surveiller l'activité WildFire :

- Configuration des paramètres du portail WildFire
- Ajout des utilisateurs du portail WildFire
- Affichage des rapports sur le portail WildFire

## Configuration des paramètres du portail WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • CN-Series | |

Cette section décrit les différents paramètres d'un compte du cloud WildFire pouvant être personnalisés, comme le fuseau horaire et les notifications par e-mail dans chaque pare-feu connecté au compte. Vous pouvez également supprimer les journaux du pare-feu stockés dans le cloud.

**STEP 1 |** Accédez aux paramètres du portail.

1. Connectez-vous au portail WildFire.
2. Sélectionnez **Settings (Paramètres)** dans la barre de menus.

**STEP 2 |** Configurez le fuseau horaire du compte du cloud WildFire.

Sélectionnez un fuseau horaire dans la liste déroulante **Set Time Zone (Définir le fuseau horaire)**, puis **Update Time Zone (Mettre à jour le fuseau horaire)** pour enregistrer la modification.

*L'horodatage qui s'affiche sur les rapports d'analyse WildFire est basé sur le fuseau horaire configuré pour le compte du cloud WildFire.*

**STEP 3 |** (Facultatif) Supprimez les journaux WildFire de certains pare-feu qui sont hébergés sur le cloud.

1. Dans la liste déroulante **Delete WildFire Reports (Supprimer les rapports WildFire)**, sélectionnez un pare-feu (par numéro de série), puis sélectionnez **Delete Reports (Supprimer les rapports)** pour retirer les journaux propres à ce pare-feu du portail WildFire. Cette action ne supprime pas les journaux stockés sur le pare-feu.
2. Cliquez sur **OK** pour confirmer la suppression.

**STEP 4 |** (Facultatif) Configurez les notifications par e-mail selon les verdicts d'analyse WildFire.

*Le portail WildFire n’envoie pas d’alertes pour les fichiers bloqués que le pare-feu a transmis aux fins d’analyse par WildFire.*

1. Dans la section Configure Alerts (Configuration des alertes, cochez la case **Malware (Malveillant), Phishing (Hameçonnage)**, **Grayware (Indésirable)** ou **Benign (Bénin)** pour recevoir des notifications par e-mail en fonction des verdicts suivants :
   - Pour recevoir des notifications selon les verdicts pour l'ensemble des échantillons chargés sur le cloud WildFire, cochez les cases de verdict qui se trouvent à la ligne intitulée **All (Tout)**.
   - Pour recevoir des notifications selon les verdicts pour l'ensemble des échantillons qui sont chargés manuellement sur le cloud WildFire public au moyen du portail WildFire, cochez les cases de verdict qui se trouvent à la ligne intitulée **Manual (Manuel)**.
   - Sélectionnez les cases de verdict pour un ou plusieurs numéros de série de pare-feu pour recevoir des avis selon les verdicts pour les échantillons envoyés par ces pare-feu.
2. Sélectionnez **Update Notification (Mettre à jour la notification)** pour activer l'envoi des notifications selon les verdicts à l'adresse e-mail associée à votre compte de support.

# Ajout des utilisateurs du portail WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Les comptes du portail WildFire sont créés par un super utilisateur (le propriétaire enregistré d'un périphérique Palo Alto Networks) afin que d'autres utilisateurs puissent se connecter au cloud WildFire et consulter les données des périphériques auxquels le super utilisateur leur a autorisé l'accès. Un utilisateur WildFire peut être un utilisateur associé à un compte Palo Alto Networks existant ou un utilisateur qui n'est pas associé à un compte de support Palo Alto Networks, à qui vous pouvez accorder l'accès uniquement aux clouds WildFire publics et à un ensemble défini de données provenant des pare-feu.

**STEP 1 |** Sélectionnez le compte pour lequel vous souhaitez ajouter des utilisateurs qui peuvent accéder au portail WildFire.

Les utilisateurs du portail WildFire peuvent visualiser les données de tous les pare-feu associés au compte de support.

1. Connectez-vous au portail de support de Palo Alto Networks.
2. Sous **Manage Account (Gérer un compte)**, cliquez sur **Users and Accounts (Utilisateurs et comptes)**.
3. Sélectionnez un compte ou un sous-compte existant.

**STEP 2 |** Ajoutez un utilisateur WildFire.

1. Cliquez sur le bouton **Add WildFire User (Ajouter un utilisateur WildFire)**.
2. Saisissez l'adresse e-mail de l'utilisateur que vous souhaitez ajouter.

   *Lors de l'ajout d'un utilisateur, la seule restriction est que l'adresse e-mail ne doit pas provenir d'un compte e-mail gratuit basé sur le Web (Gmail, Hotmail ou Yahoo). Si une adresse e-mail est saisie pour un domaine qui n'est pas pris en charge, une fenêtre d'avertissement contextuelle s'affiche.*

**STEP 3 |** Assignez des pare-feu au nouveau compte utilisateur et accédez au cloud WildFire.

Sélectionnez le ou les pare-feu par numéro de série au(x)quel(s) vous voulez autoriser l'accès et renseignez les détails facultatifs du compte.

Les utilisateurs titulaires d'un compte de support existant vont recevoir un e-mail avec une liste des pare-feu permettant désormais de consulter les rapports WildFire. Si un utilisateur ne dispose pas d'un

compte de support, le portail envoie un e-mail avec des instructions indiquant comment accéder au portail et comment configurer un nouveau mot de passe.

Le nouvel utilisateur peut désormais se connecter au cloud WildFire et consulter les rapports WildFire des pare-feu dont l'accès lui a été autorisé. Les utilisateurs peuvent également configurer l'envoi d'alertes automatiques par e-mail pour ces périphériques concernant les fichiers analysés. Il peut choisir de recevoir des rapports de fichiers malveillants et/ou bénins.

## Affichage des rapports sur le portail WildFire

| Où puis-je utiliser ceci ? | De quoi ai-je besoin ? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series<br>• CN-Series | ❑ Licence Advanced WildFire<br>*Pour Prisma Access, c’est généralement inclus avec votre licence Prisma Access.* |

Le portail WildFire affiche les rapports des échantillons qui sont envoyés du pare-feu, chargés manuellement ou chargés à l'aide de l'API du pare-feu. Sélectionnez **Reports (Rapports)** pour afficher les plus récents rapports des échantillons analysés par le cloud WildFire. Pour chaque échantillon répertorié, l'entrée du rapport indique la date et l'heure de réception de l'échantillon par le cloud, le numéro de série du pare-feu qui a envoyé le fichier, le nom de fichier ou l'URL ainsi que le verdict rendu par WildFire (bénin, indésirable, malveillant ou hameçonnage).

Utilisez l'option de recherche pour chercher des rapports selon le nom de fichier ou la valeur de hachage de l'échantillon. Vous pouvez également restreindre les résultats affichés en n'affichant que les rapports des échantillons envoyés par une **Source (Source)** donnée (afficher uniquement les résultats des échantillons envoyés manuellement ou par un pare-feu donné) ou des échantillons qui ont reçu un **Verdict (Verdict)** WildFire particulier (tous les verdicts, verdict bénin, verdict malveillant, verdict indésirable, hameçonnage ou en attente).

Pour afficher un rapport dans le portail, cliquez sur l'icône **Reports (Rapports)** située à gauche du nom du rapport. Pour enregistrer le rapport détaillé, cliquez sur le bouton **Download as PDF (Télécharger au format PDF)** qui figure dans le coin supérieur droit de la page du rapport. Pour plus de précisions sur les rapports d'analyse WildFire, reportez-vous à la section Rapports d'analyse WildFire : aperçu de près.

Voici une liste des échantillons de fichiers envoyés par un pare-feu donné :