paloalto TECHDOCS

Administration avancée de la sécurité DNS

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

November 23, 2022

Table of Contents

À propos des services d’abonnement à la sécurité DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention des menaces avancée ou de prévention des menaces

Palo Alto Networks® offre une protection intégrée spécialisée contre les menaces basées sur DNS avec deux options d’abonnement de sécurité : Sécurité DNS et sécurité DNS avancée. Ces abonnements de sécurité fournis dans le cloud fonctionnent à l’aide de bases partagées avec les solutions de prévention des menaces de Palo Alto Networks pour fournir une solution de sécurité DNS complète et nécessitent, en tant que tels, la présence d’un abonnement de prévention des menaces ou de prévention avancée des menaces.

Le service cloud de la sécurité DNS est conçu pour protéger votre organisation contre une multitude de menaces basées sur DNS avancées. En appliquant un apprentissage automatique avancé et des analyses prédictives à une gamme variée de sources de renseignements sur les menaces, la sécurité DNS génère rapidement des signatures DNS améliorées pour se défendre contre les catégories DNS malveillantes connues, ainsi qu’une analyse en temps réel des requêtes DNS pour défendre votre réseau contre les domaines malveillants nouvellement générés et inconnus. Sécurité DNS peut détecter diverses menaces DNS, notamment la tunnellisation DNS, les attaques de reliaison DNS, les domaines créés à l’aide de la génération automatique, les hôtes de logiciels malveillants et bien d’autres.

Avec une solution de prévention active des menaces fonctionnant sur des plates-formes de sécurité réseau prises en charge, les clients peuvent supprimer les requêtes DNS à l’aide d’une liste de domaines générée par Palo Alto Networks. Ces listes de signatures DNS accessibles localement et personnalisables sont fournies avec les mises à jour antivirus et WildFire et comprennent les menaces les plus pertinentes pour l’application de la politique et la protection au moment de la publication. Pour améliorer la protection contre les menaces au moyen de DNS, l’abonnement à la sécurité DNS permet aux utilisateurs d’accéder à des protections en temps réel au moyen d’analyses prédictives avancées. En utilisant des techniques comme la détection de la tunnelisation DGA/DNS et l’apprentissage machine, les menaces cachées dans le trafic DNS peut être proactivement identifié et partagé à l’intérieur d’un service Cloud évolutif à l’infini. Comme les protections et signatures DNS sont stockées dans une architecture Cloud, vous pouvez accéder à la base de données complète et évolutive des signatures qui ont été générées à l'aide d'une multitude de sources de données. Vous pouvez ainsi vous défendre contre un éventail de menaces à l'aide de DNS en temps réel et contre les nouveaux domaines malveillants générés. Pour vous défendre contre les menaces futures, des mises à jour des capacités d’analyse, de détection et de prévention du service de sécurité DNS sera disponible par l’intermédiaire des versions de contenu.

Pour accéder au service de sécurité DNS de base, vous devez disposer d’une licence prévention avancée des menaces ou prévention des menaces et d’une licence sécurité DNS avancée ou sécurité DNS valides en plus de toutes les licences de base requises pour exploiter votre plateforme de sécurité réseau.

Les abonnements à la sécurité DNS sont disponibles sur les plateformes de sécurité réseau Palo Alto Networks suivantes :

- Pare-feu de nouvelle génération, notamment les VM-Series et CN-Series
- Prisma Access

Le service de sécurité DNS avancée est une offre d’abonnement complémentaire qui fonctionne en conjonction avec l’abonnement à la sécurité DNS qui permet l’accès à de nouveaux détecteurs de domaine dans le cloud de la sécurité DNS avancée qui inspectent les modifications des réponses DNS pour détecter différents types de détournement DNS en temps réel. Avec l’accès à la sécurité DNS avancée fonctionnant sur PAN-OS 11.2 et les versions ultérieures, vous pouvez détecter et bloquer les réponses DNS des domaines détournés et des domaines mal configurés. Les domaines détournés et mal configurés peuvent être introduits dans votre réseau soit en manipulant directement les réponses DNS, soit en exploitant les paramètres de configuration de l’infrastructure DNS d’une organisation afin de rediriger l’utilisateur vers un domaine malveillant à partir duquel il lance des attaques supplémentaires. La principale différence entre ces deux techniques réside dans l’endroit où l’exploit se produit. Dans le cas d’un détournement DNS, les attaquants obtiennent la possibilité de résoudre les requêtes DNS vers des domaines exploités par l’attaquant en compromettant un aspect de l’infrastructure DNS d’une organisation, qu’il s’agisse de l’accès administratif du fournisseur DNS, d’une attaque MiTM pendant le processus de résolution DNS ou du serveur DNS lui-même. Les domaines mal configurés présentent un problème similaire : l’attaquant cherche à incorporer son propre domaine malveillant dans le DNS d’une organisation en profitant des problèmes de configuration du domaine et des enregistrements DNS obsolètes permettant aux attaquants de prendre possession du sous-domaine du client.

La sécurité DNS avancée peut détecter et catégoriser les domaines détournés et mal configurés en temps réel en exploitant des moteurs de détection basés sur le cloud qui fournissent un support de santé DNS en analysant les réponses DNS à l’aide d’analyses basées sur le ML pour détecter les activités malveillantes. Étant donné que ces détecteurs sont situés dans le cloud, vous pouvez accéder à un large éventail de mécanismes de détection qui sont mis à jour et déployés automatiquement sans que l’utilisateur doive télécharger des packages de mise à jour lorsque des modifications sont apportées aux détecteurs. Lors de sa sortie initiale, la sécurité DNS avancée prend en charge deux moteurs d’analyse : Domaines présentant des erreurs de configuration DNS et domaines détournés. De plus, les réponses DNS pour toutes les requêtes DNS sont envoyées au cloud sécurité DNS avancée pour une analyse de réponse améliorée afin de catégoriser plus précisément et de renvoyer un résultat dans un échange en temps réel. Des modèles d’analyse sont fournis via des mises à jour de contenu, cependant, les améliorations des modèles existants sont effectuées sous forme de mise à jour côté cloud, ne nécessitant aucune mise à jour du pare-feu. La sécurité DNS avancée est activée et configurée via le profil antispyware (ou sécurité DNS) et nécessite des licences actives de sécurité DNS avancée et de prévention avancée des menaces (ou prévention des menaces).

Pour accéder au service de sécurité DNS avancée, vous devez disposer d’une licence prévention avancée des menaces ou prévention des menaces et d’une licence sécurité DNS avancée valides en plus de toutes les licences de base requises pour exploiter votre plateforme de sécurité réseau.

Les abonnements à la sécurité DNS avancée sont disponibles sur les plateformes de sécurité réseau Palo Alto Networks suivantes :

- Pare-feu de nouvelle génération, notamment les VM-Series et CN-Series

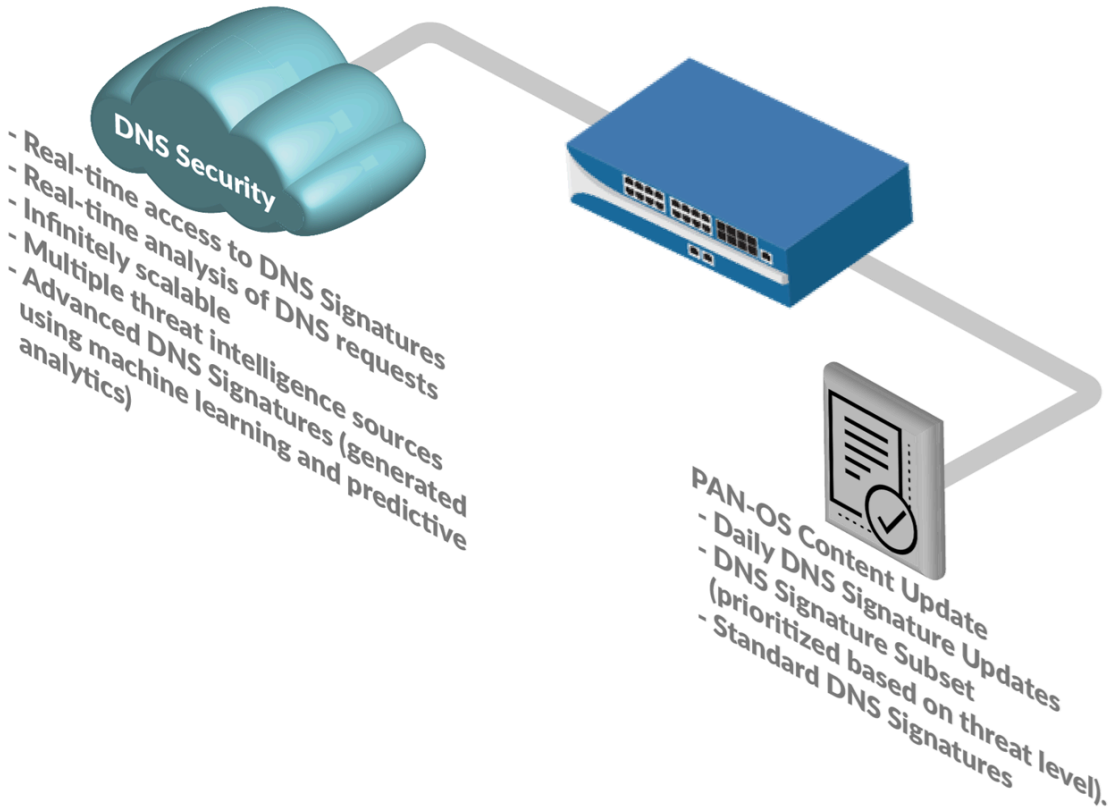
Découvrez comment déployer et surveiller la sécurité DNS et la sécurité DNS avancée sur votre réseau :

- Configuration des services d’abonnement à la sécurité DNS
- Surveillance des services d’abonnement à la sécurité DNS

Protections et signatures DNS fournies par le cloud

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence avancée de prévention des menaces ou de prévention des menaces

En tant que services basés sur le cloud, la sécurité DNS avancée et la sécurité DNS vous permet d’accéder à une source de protections et de signatures DNS infiniment extensible pour défendre votre organisation contre les domaines malveillants. Les protections et signatures de domaine générées par Palo Alto Networks proviennent d’une multitude de sources, y compris l'analyse du trafic WildFire, le DNS passif, l’explorative active du Web et l’analyse du contenu Web malveillant, l’analyse des bacs à sable URL, le réseau HoneyNet, ingénierie DGA inverse, les données télémétriques, whois, l’organisation de recherche Unité 42 et des sources de données tierces, comme la Cyber Threat Alliance. Cette base de données sur le cloud à la demande permet aux utilisateurs d'accéder à l'ensemble des signatures DNS de Palo Alto Networks, y compris des signatures générées à l'aide de techniques d'analyse avancées, ainsi qu’à l’analyse en temps réel des requêtes DNS. Les ensembles de signatures DNS localement disponibles et téléchargeables (compris dans les mises à jour antivirus et de WildFire) s’accompagnent d’une limite de capacité programmée en dur de 100 000 signatures et ne comprennent pas les signatures générées par l'analyse avancée. Pour mieux accueillir l'afflux de nouvelles signatures DNS qui sont produites quotidiennement, la base de données de signatures dans le cloud fournit aux utilisateurs un accès instantané aux signatures DNS nouvellement ajoutée sans qu’ils aient à télécharger des mises à jour. En cas d’échec ou d’indisponibilité de la connectivité réseau, le pare-feu utilise l’ensemble de signatures DNS comprises dans la base de données.



Le service de sécurité DNS effectue une analyse en temps réel des demandes DNS en utilisant l'analyse prédictive et l'apprentissage machine sur de multiples sources de données DNS. Il est utilisé pour générer des protections contre les menaces basées sur le DNS, qui sont accessibles en temps réel grâce à la configuration du profil de sécurité antispyware joint à une règle de politique de sécurité. Chaque catégorie de menace DNS (la source de signature DNS) vous permet de définir des actions stratégiques distinctes ainsi qu'un niveau de gravité de journal pour un type de signature spécifique. Cela vous permet de créer des politiques de sécurité spécifiques basées sur la nature de la menace, en fonction des protocoles de sécurité de votre réseau. Palo Alto Networks génère et maintient également une liste de domaines explicitement autorisés basée sur les mesures de PAN-DB et Alexa. Ces domaines de liste d’autorisation sont fréquemment consultés et sont connus pour être exempts de contenu malveillant. Les catégories de sécurité DNS et la liste d’autorisation sont mises à jour et extensibles par le biais des publications de contenu PAN-OS.

PAN-OS 9.1 et versions antérieures a une gamme limitée de catégories de sources de sécurité DNS.

La sécurité DNS et la sécurité DNS avancée prennent actuellement en charge la détection des catégories de menaces DNS suivantes :

Le numéro d’identification universel de la menace (indiqué en tant qu’ID dans les journaux des menaces) correspond au mécanisme de détection DNS spécifique utilisé par la sécurité DNS pour classer les domaines. Cela montre la catégorisation précise du domaine, à côté de la catégorie de menace largement définie, à laquelle il appartient.

- **Command and Control Domains (Domaines de commande et contrôle)** : les C2 comprennent les URL et les domaines utilisés par des logiciels malveillants et/ou des systèmes compromis pour communiquer subrepticement avec le serveur distant d'un attaquant afin de recevoir des commandes malveillantes ou d'exfiltrer des données (cela inclut la détection de tunnellisation DNS et la détection DGA), ou épuise les ressources sur des serveurs DNS autorisés cibles (comme NXNSattack).
  - **Détection de tunnel DNS** (UTID : 109001001/109001002) : Les pirates peuvent utiliser la tunnellisation DNS pour encoder les données des programmes et protocoles non-DNS dans les requêtes et réponses DNS. Les pirates disposent ainsi d’un canal ouvert par l’intermédiaire duquel ils peuvent transférer des fichiers ou accéder à distance au système. La détection des tunnels DNS utilise l'apprentissage machine pour analyser les qualités comportementales de requêtes DNS, y compris l'analyse de la fréquence n-gramme des domaine, l’entropie, le taux de requêtes et les modèles pour déterminer si la requête est conforme à une attaque basée sur la tunnellisation DNS. Cela inclut certains malwares de tunneling DNS de nouvelle génération qui exfiltrent lentement les données dans plusieurs domaines pour éviter la détection, tels que TriFive et Snugy. Conjugué aux actions automatisées des politiques du pare-feu, cela vous permet de rapidement détecter les C2 ou le vol de données caché dans les tunnels DNS et de les bloquer automatiquement, selon vos règles de politique définies.

    Les domaines qui sont déterminés comme possédant des capacités de tunnellisation DNS sont analysés plus en détail pour fournir des détails sur les outils utilisés pour intégrer des données aux requêtes et réponses DNS et le nom de la campagne de malware associée par la sécurité DNS. Les détails d’attribution sont disponibles dans les journaux de menaces en tant qu’ID/Nom de menace pour le pare-feu et les journaux de sécurité DNS sur Prisma Access en tant que pare-feu de nom de menace en utilisant le format suivant : Tunnellisation :<*optional_list_of_tools/campaigns*; dot-separated string)>:<*domain_name*> ou Tunneling_infil:<*optional_list_of_tools/campaigns*; dot-separated string)>:<*domain_name*> en fonction du type de domaine spécifique du tunnel DNS.
  - **Détection de domaine DGA** (UTID : 109000001) : Les Domain Generation Algorithms (algorithmes de génération de domaines ; DGA) sont utilisés pour autogénérer des domaines, généralement en grand nombre, dans le contexte de l’établissement d’un canal de communications command-and-control (commandement et contrôle ; C2) malveillant. Les logiciels malveillants basés sur DGA (tels que Pushdo, BankPatch et CryptoLocker) limitent le nombre de domaines pouvant être bloqués en cachant l'emplacement de leurs serveurs C2 actifs parmi un grand nombre de suspects possibles, et peuvent être générés de manière algorithmique en fonction de facteurs tels que l'heure de la journée, les clés cryptographiques, les schémas nominatifs dérivés du dictionnaire ou d'autres valeurs uniques. Bien que la plupart des domaines générés par un DGA ne se résolvent pas en un domaine valide, ils doivent tous être identifiés pour offrir une pleine protection contre une menace donnée. L’analyse du DGA détermine la probabilité qu’un domaine ait été généré par une machine, plutôt que par une personne, en utilisant des techniques d’ingénierie inverse et en analysant d’autres techniques fréquemment utilisées que l’on trouve dans les DGA. Palo Alto Networks utilise ensuite ces caractéristiques pour identifier et bloquer, en temps réel, les menaces basées sur les DGA qui étaient préalablement inconnues.
  - **NXNSAttack** (UTID : 109010007) : la vulnérabilité NXNSAttack présente dans le protocole DNS affecte tous les résolveurs DNS récursifs et peut être utilisée par des acteurs malveillants pour lancer des attaques d'amplification de type DDOS afin de perturber le fonctionnement normal des serveurs DNS faisant autorité et vulnérables. NXNSAttack peut introduire des pics de trafic massifs sur un serveur DNS faisant autorité en forçant le résolveur DNS récursif à émettre un grand nombre de requêtes invalides pour potentiellement arrêter le serveur.
  - **Reliaison DNS** (UTID : 109010009) : les attaques de rebinding DNS attirent les utilisateurs vers un domaine contrôlé par un attaquant configuré avec un paramètre TTL court pour manipuler la façon

dont les noms de domaine sont résolus pour exploiter et contourner la politique de même origine dans les navigateurs. Cela permet à des acteurs malveillants d'utiliser la machine cliente comme intermédiaire pour attaquer ou accéder à une ressource contenue dans un réseau privé.

  - **Infiltration DNS** (UTID : 109001003) : l’infiltration DNS inclut les requêtes DNS qui permettent aux acteurs malveillants de masquer et de résoudre des charges utiles infimes via une réponse aux demandes d’enregistrement frauduleuses A (IPv4) et AAAA (IPv6). Lorsque le client résout plusieurs sous-domaines, chacun contenant un enregistrement A/AAAA avec un composant codé, les données qu’ils contiennent peuvent être consolidées pour former une charge utile malveillante, qui peut ensuite être exécutée sur l’ordinateur client. Après avoir exécuté la charge utile, il peut introduire des charges utiles secondaires pour établir un tunnel DNS ou des exploits supplémentaires.
  - **DNS Traffic Profiling** (UTID: 109010010) — (Requiert une sécurité DNS avancée) Le profilage du trafic DNS est un analyseur basé sur le cloud qui détecte les logiciels malveillants tentant d’établir une connexion C2, basé sur une évaluation des modèles de trafic DNS. Comme la sécurité DNS avancée surveille le trafic DNS de votre organisation, les séquences de requêtes DNS sortantes sont vectorisées pour former des profils de trafic DNS, qui sont ensuite analysés à l’aide de techniques ML qui peuvent associer les modèles de requête DNS uniques à des profils de domaine C2 malveillants identifiables.
- **Domaines DNS dynamiques hébergés** (UTID : 109020002) : les services de DNS dynamique (DDNS) fournissent un mappage entre les noms d'hôtes et les adresses IP en temps quasi réel pour continuer à changer les adresses IP liées à un domaine spécifique, lorsque les IP statiques ne sont pas disponibles. Les attaquants disposent ainsi d'une méthode pour infiltrer les réseaux en utilisant les services DDNS pour modifier les adresses IP qui hébergent les serveurs de commande et de contrôle. Les campagnes de logiciels malveillants et les kits d'exploitation peuvent utiliser les services DDNS dans le cadre de leur stratégie de distribution de la charge utile. En utilisant les domaines DDNS dans le cadre de leur infrastructure de noms d'hôtes, les adversaires peuvent changer l'adresse IP associée à des enregistrements DNS donnés et éviter plus facilement la détection. La sécurité DNS détecte les services DDNS exploiteurs en filtrant et en croisant les données DNS provenant de diverses sources pour générer des listes de candidats qui sont ensuite validées pour maximiser la précision.
- **Malware Domains (Domaines malveillants)** : les domaines malveillants hébergent et distribuent des logiciels malveillants et peuvent inclure des sites web qui tentent d'installer diverses menaces (telles que des exécutables, des scripts, des virus, des téléchargements automatiques). Les domaines malveillants se distinguent des domaines C2 en ce sens qu'ils acheminent des charges utiles malveillantes dans votre réseau via une source externe, alors qu'avec les C2, les terminaux infectés tentent généralement de se connecter à un serveur distant pour récupérer des instructions supplémentaires ou d'autres contenus malveillants.
  - **DNS compromis par les logiciels malveillants** (UTID : 109003001) : le DNS compromis par les logiciels malveillants couvre une gamme de techniques, certaines légitimes, qui aboutissent à la génération de noms d’hôte et de sous-domaines apparemment authentiques, qui, en réalité, sont malveillants. Cela inclut les noms d’hôte nouvellement observés qui imitent des noms d’hôte existants et réputés, dans le but d’usurper l’identité ou d’induire en erreur et d’échapper aux solutions de sécurité centrées sur les bases de données. Ceux-ci peuvent être rapidement produits en masse pour préempter leur ajout aux listes de bases de données. L’observation de domaine suit généralement après qu’un attaquant a pris le contrôle d’un compte de domaine par le biais d’une attaque plus conventionnelle. Cela fournit l’accès nécessaire pour créer des sous-domaines

illégitimes utilisés pour coordonner les attaques, même si le domaine racine reste légitime et valide, ce qui augmente la probabilité de contourner la sécurité du réseau.

  - **Domaines ransomware** (UTID : 109003002) — Les rançongiciels sont une sous-catégorie de logiciels malveillants qui verrouillent ou empêchent cryptographiquement les utilisateurs d’accéder aux données en échange du paiement d’une rançon, après quoi le système peut être remis à l’utilisateur par l’attaquant. Les ransomwares peuvent être distribués par le biais de domaines ransomware malveillants, qui hébergent les fichiers apparemment légitimes que les utilisateurs téléchargent.

- **Domaines nouvellement enregistrés** (UTID : 109020001) : les domaines nouvellement enregistrés sont des domaines qui ont été récemment ajoutés par un opérateur de TLD ou dont la propriété a changé au cours des 32 derniers jours. Si de nouveaux domaines peuvent être créés à des fins légitimes, la grande majorité d'entre eux sont souvent utilisés pour faciliter des activités malveillantes, comme le fonctionnement en tant que serveurs C2 ou utilisés pour distribuer des logiciels malveillants, du spam, des PUP/logiciels publicitaires. Palo Alto Networks détecte les domaines récemment enregistrés en surveillant des flux spécifiques (registres de domaines et bureaux d'enregistrement) et en utilisant des fichiers de zone, le DNS passif, les données WHOIS pour détecter les campagnes d'enregistrement.
- **Domaines de hameçonnage** (UTID : 109010001) : les domaines de hameçonnage tentent d'inciter les utilisateurs à soumettre des données sensibles, telles que des informations personnelles ou des identifiants d'utilisateur, en se faisant passer pour des sites web légitimes par le biais du hameçonnage ou du pharming. Ces activités malveillantes peuvent être menées par des campagnes d'ingénierie sociale (par lesquelles une source apparemment fiable manipule les utilisateurs pour qu'ils soumettent des informations personnelles par e-mail ou d'autres formes de communications électroniques) ou par la réorientation du trafic web, qui dirige les utilisateurs vers des sites frauduleux qui semblent légitimes.
- **Domains de logiciels indésirables** (UTID : 109010002) : (disponible avec l'installation du contenu PAN-OS version 8250 et ultérieure). Les domaines indésirables ne constituent généralement pas une menace directe pour la sécurité, mais ils peuvent faciliter les vecteurs d'attaque, produire divers comportements indésirables ou simplement contenir des contenus douteux/offensifs.Cela peut inclure des sites Internet et des domaines qui :
  - Tenter de tromper les utilisateurs pour qu'ils accordent un accès à distance.
  - Exploitez les sous-domaines des services populaires d’hébergement Web et de système dynamique de noms de domaine (DDNS) pour héberger et distribuer du contenu malveillant (**réputation de sous-domaine** - UTIDL 109002004).
  - Contient des logiciels publicitaires et d'autres applications non sollicitées (telles que des cryptomineurs, des pirates de l'air et des PUP [programmes potentiellement indésirables]).
  - Déployez des actions de dissimulation d'identification de domaine à l'aide de techniques de flux rapide (**détection flux rapide** : UTID : 109010005).
  - Démontrer le comportement et l'utilisation malveillants comme en témoignent les analyses prédicatives de sécurité DNS (**NRD malveillant**) : UTID : 109010006).
  - Redirigez le trafic d'une source légitime vers un site Web malveillant en raison d'un enregistrement DNS mal configuré ou périmé sur un serveur DNS faisant autorité qui n'a pas été supprimé ou corrigé (**DNS suspendu**) : UTID : 109010008).
  - Promouvoir des activités illégales ou des escroqueries.
  - Incluez des entrées DNS génériques, qui peuvent être utilisées pour échapper aux listes de blocage ou activer les attaques DNS génériques en acheminant le trafic vers des sites Web malveillants (**abus de caractères génériques** - UTID : 109002001).

    - Indiquez la présence de trafic DNS avec des caractéristiques anormales par rapport aux profils de base établis construits à partir des données DNS collectées (**détection d’anomalies**).
    - Ont été enregistrés des mois ou des années à l’avance et laissés dans un état de dormance pour contourner les contrôles de réputation lorsqu’ils deviennent actifs. Cela inclut également les domaines nouvellement observés qui n’ont jamais été vus ou évalués d’une autre manière (**domaines stratégiquement âgés** - UTID: 109002002).
    - Sont des domaines inutilisés qui ont été enregistrés par un attaquant avec une intention malveillante probable basés sur des journaux de transparence de certificat (**Détection de domaine de stockage** - UTID : 109002005).
    - Trompez les utilisateurs en ressemblant à des domaines de marque populaires ainsi qu’à des adresses de pages Web saisies de manière incorrecte, dans le but de diriger les utilisateurs vers des sites Web contrefaits et frauduleux. (**Domaines de cybersquattage/typosquattage** - UTID : 109002003).
- **Domaines en parqués** (UTID : 109010003) : (disponible avec l’installation du contenu PAN-OS version 109010003 et ultérieure) les domaines en parking sont généralement des sites web inactifs qui hébergent un contenu limité, souvent sous la forme de clics publicitaires qui peuvent générer des revenus pour l'entité hôte, mais qui ne contiennent généralement pas de contenu utile pour l'utilisateur final. Bien qu'ils fonctionnent souvent comme un substitut légitime ou comme une simple nuisance bénigne, ils pourraient également être utilisés comme un vecteur possible de distribution de logiciels malveillants.
- **Contournement de proxy et anonymiseurs** (UTID : 109010004) : (disponible avec l’installation du contenu PAN-OS version 109010004 et ultérieure) le contournement de proxy et les anonymiseurs sont un trafic vers des services qui sont utilisés pour contourner les politiques de filtrage de contenu. Les utilisateurs qui tentent de contourner les politiques de filtrage de contenu d'une organisation via les services proxy de l'anonymiseur sont bloqués au niveau du DNS.
- **Domaines de suivi des publicités** (UTID : 109004000) — (Disponible avec l’installation de la version 8586 et ultérieure du contenu de PAN-OS) Les domaines de suivi des publicités fournissent certains types de contenu d’automatisation marketing pour les pages Web afin de suivre l’engagement des utilisateurs (tels que les clics sur les liens, la navigation sur les pages Web, etc.). Généralement, ces domaines tiers sont dissimulés à l’aide d’une URL de redirection pour sembler faire partie du domaine d’origine.
    - **Dissimulation CNAME** (UTID : 109004001) — La dissimulation CNAME fournit un autre moyen de dissimuler une URL en modifiant une requête Web pour qu’un sous-domaine apparaisse comme s’il provenait du même site Web, bien qu’en réalité, le sous-domaine utilise un CNAME pour résoudre à un domaine tiers. Cette technique contourne certaines protections de confidentialité basées sur le navigateur qui pourraient potentiellement se connecter à une destination CNAME suspecte.
- **Domaines détournés** (UTID : 109004000) — (Requiert une sécurité DNS avancée) Les domaines détournés comprennent les domaines où les attaquants acquièrent la capacité de rendre les domaines légitimes résolus en adresses IP exploitées par les attaquants, généralement en compromettant certains aspects de l’infrastructure DNS d’une organisation. Cela peut inclure l’accès administratif non autorisé au fournisseur DNS, une attaque MiTM pendant le processus de résolution DNS ou l’accès au serveur DNS lui-même.
- **Domaines de mauvaise configuration** (UTID : 109004000)—(Requiert une sécurité DNS avancée) Les domaines mal configurés permettent aux attaquants d’incorporer leurs propres domaines malveillants dans le DNS d’une organisation en tirant parti des problèmes de configuration du domaine. Ces enregistrements DNS obsolètes permettent aux attaquants de s’approprier le sous-domaine du

client et de rediriger les utilisateurs vers des IP contrôlées par l’attaquant ou des sites Web à des fins malveillantes. Ces domaines de mauvaise configuration non résolubles sont basés sur le(s) domaine(s) parent(s) orienté(s) vers le public qui sont spécifiés lors de la configuration de la sécurité DNS avancée.

- **Zone d’erreur de configuration** : (UTID : 109004200) — Catégorie générique pour les domaines de mauvaise configuration qui ne correspondent à aucune autre catégorie de mauvaise configuration.
- **Zone de mauvaise configuration suspendue** (UTID : 109004201) — Domaines présentant une erreur de configuration qui redirigent le trafic d’une source légitime vers un site Web malveillant en raison d’un enregistrement DNS mal configuré ou périmé sur un serveur DNS faisant autorité présent dans le domaine public d’une organisation.
- **Erreur de configuration NX réclamable** (UTID : 109004202) — Les domaines présentant une erreur de configuration qui font partie de la configuration DNS d’une organisation, mais qui n’existent plus (NXDOMAINS), peuvent être enregistrés subrepticement par des attaquants et être utilisés pour rediriger les utilisateurs vers des sites Web malveillants et permettent potentiellement à l’attaquant d’accéder au réseau d’un client.

Collecte et journalisation des données

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention avancée des menaces ou de prévention des menaces

Le service de sécurité DNS collecte des informations sur les réponses et les requêtes du serveur en fonction de vos règles de politique de sécurité, de l’action associée et des détails de la requête DNS lors de recherches de domaine pour générer des journaux de sécurité DNS pour des applications d’activité basées Strata Logging Service (AIOps for NGFW Free, Prisma Access, Strata Logging Service, etc.). De plus, la plate-forme de sécurité réseau transmet des données DNS supplémentaires aux serveurs cloud de sécurité DNS et est utilisée par les services de Palo Alto Networks pour fournir des informations de domaine plus précises (telles que l’ASN du fournisseur, les informations d’hébergement et l’identification de géolocalisation). Bien que ces données supplémentaires ne soient pas nécessaires pour faire fonctionner le service de sécurité DNS, elles fournissent les ressources nécessaires pour générer des capacités d'analyse, de détection DNS et de prévention améliorées. Cette action se produit moins de 30 secondes après la collecte des données. Pour minimiser l’impact sur les performances du pare-feu, la télémétrie de la sécurité DNS fonctionne avec une surcharge minimale, ce qui peut limiter la quantité totale de données de télémétrie DNS envoyées à Strata Logging Service ; par conséquent, seul un sous-ensemble de requêtes DNS est transmis à Strata Logging Service en tant qu’entrées de journal de sécurité DNS. Par conséquent, Palo Alto Networks recommande d’afficher les journaux des requêtes DNS malveillantes en tant que journaux des menaces plutôt qu’en tant que journaux de sécurité DNS.

Les requêtes DNS malveillantes sont également enregistrées en tant que journaux des menaces et sont soumises au Strata Logging Service à l’aide du transfert de journaux PAN-OS (lorsque cela est correctement configuré).

La sécurité DNS peut soumettre les champs de données suivants :

Champ	Description
Action	Affiche l'action de stratégie prise sur la requête DNS.
Type	Affiche le type d'enregistrement DNS.
Réponse	L'adresse IP à laquelle le domaine dans la requête DNS a été résolu.
Code de réponse	Le code de réponse DNS qui a été reçu en réponse à votre requête DNS.

Champ	Description
IP source	L'adresse IP du système qui a effectué la requête DNS.
Utilisateur source	Lorsque la fonction d'ID utilisateur du pare-feu est activée, l'identité du demandeur DNS est affichée.
Zone source	La zone source configurée référencée dans votre règle de politique de sécurité.

La collecte de données étendue DNS est contournée pour les domaines ajoutés à la liste verte dans les exceptions DNS.

Les champs de données qui peuvent être utilisés pour identifier potentiellement les utilisateurs (IP source, utilisateur source et zone source) peuvent être exclus de la soumission automatique à l'aide de la commande CLI suivante : **`set deviceconfig setting ctd cloud-dns-privacy-mask yes`**. Vous devez **`commit (valider)`** les modifications pour que la mise à jour prenne effet.

Domaines de services régionaux

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention avancée des menaces ou de prévention des menaces

Palo Alto Networks gère un réseau de domaines mondiaux et régionaux qui fournissent des services pour les opérations de sécurité DNS et de sécurité DNS avancée. Ces domaines de service exploitent des analyseurs de requêtes DNS en temps réel, accèdent à la base de données de signatures DNS et fournissent des fonctionnalités avancées dépendantes du cloud. Par défaut, la sécurité DNS et la sécurité DNS avancée se connectent aux domaines de service globaux (dns.service.paloaltonetworks.com et adv-dns.service.paloaltonetworks.com, respectivement), qui redirigent ensuite automatiquement vers le domaine régional le plus proche de l’emplacement de la plateforme de sécurité réseau.

Domaines de service régionaux de sécurité DNS

Palo Alto Networks recommande d’utiliser la configuration par défaut du domaine de service mondial pour une meilleure gestion du basculement. Toutefois, si vous rencontrez des problèmes de latence en raison de particularités liées à votre emplacement (par exemple, lorsque vous vous trouvez sur plusieurs domaines régionaux qui se chevauchent), vous pouvez spécifier manuellement le domaine de service. Pour spécifier le domaine de service régional utilisé par la sécurité DNS, vous devez ajouter une entrée DNS pour dns.service.paloaltonetworks.com qui inclut un enregistrement CNAME indiquant un domaine régional valide dans le cadre de la configuration de votre serveur DNS. Après vous être connecté à un domaine régional, vous pouvez émettre la commande CLI sur le pare-feu :

```
show dns-proxy dns-signature counters
```

pour examiner la latence moyenne. La section correspondante se trouve sous l’en-tête de l’API de requête de signature.

Le tableau suivant répertorie les domaines du service de sécurité DNS :

Emplacement	URL
Cape Town, Afrique du Sud	dns-za.service.paloaltonetworks.com
Hong Kong	dns-hk.service.paloaltonetworks.com
Tokyo, Japon	dns-jp.service.paloaltonetworks.com

Emplacement	URL
Singapour	dns-sg.service.paloaltonetworks.com
Mumbai, Inde	dns-in.service.paloaltonetworks.com
Sydney, Australie	dns-au.service.paloaltonetworks.com
Londres, Angleterre	dns-uk.service.paloaltonetworks.com
Francfort, Allemagne	dns-de.service.paloaltonetworks.com
Eemshaven, Pays-Bas	dns-nl.service.paloaltonetworks.com
Paris, France	dns-fr.service.paloaltonetworks.com
Bahreïn	dns-bh.service.paloaltonetworks.com
Montréal, Québec, Canada	dns-ca.service.paloaltonetworks.com
Osasco, São Paulo, Brésil	dns-br.service.paloaltonetworks.com
Council Bluffs, Iowa, États-Unis	dns-us-ia.service.paloaltonetworks.com
Ashburn, Virginie du Nord, États-Unis	dns-us-va.service.paloaltonetworks.com
The Dalles, Oregon, États-Unis	dns-us-or.service.paloaltonetworks.com
Los Angeles, Californie, États-Unis	dns-us-ca.service.paloaltonetworks.com

Domaines de service régionaux de sécurité DNS avancée

Vous pouvez spécifier manuellement le serveur utilisé pour faciliter les requêtes de sécurité DNS avancée. Bien que Palo Alto Networks recommande d’utiliser le domaine de service mondial par défaut, vous pouvez remplacer le serveur sélectionné si vous rencontrez une latence plus élevée que prévu ou d’autres problèmes liés au service.

Vous pouvez spécifier le domaine du service de sécurité DNS avancée dans PAN-OS à partir de **Périphérique** > **Configuration** > **Gestion** > **Sécurité DNS avancée** > **Serveur de sécurité DNS**.

Ce paramètre n’a pas d’impact sur la façon dont les requêtes de sécurité DNS standard sont traitées.

Le tableau suivant répertorie les domaines du service de sécurité DNS avancée :

Emplacement	URL
Cape Town, Afrique du Sud	za.adv-dns.service.paloaltonetworks.com
Bahreïn	bh.adv-dns.service.paloaltonetworks.com
Hong Kong	hk.adv-dns.service.paloaltonetworks.com
Tokyo, Japon	jp.adv-dns.service.paloaltonetworks.com
Singapour	sg.adv-dns.service.paloaltonetworks.com
Mumbai, Inde	in.adv.dns.service.paloaltonetworks.com
Sydney, Australie	au.adv-dns.service.paloaltonetworks.com
Londres, Angleterre	uk.adv-dns.service.paloaltonetworks.com
Francfort, Allemagne	de.adv.dns.service.paloaltonetworks.com
Eemshaven, Pays-Bas	nl.adv.dns.service.paloaltonetworks.com
Paris, France	fr.adv-dns.service.paloaltonetworks.com
Bahreïn	bh.adv-dns.service.paloaltonetworks.com
Montréal, Québec, Canada	ca.adv.dns.service.paloaltonetworks.com
Osasco, São Paulo, Brésil	br.adv.dns.service.paloaltonetworks.com
Council Bluffs, Iowa, États-Unis	us-ia.adv.dns.service.paloaltonetworks.com
Ashburn, Virginie du Nord, États-Unis	us-va.adv.dns.service.paloaltonetworks.com
The Dalles, Oregon, États-Unis	us-or.adv.dns.service.paloaltonetworks.com
Los Angeles, Californie, États-Unis	us-ca.adv.dns.service.paloaltonetworks.com

Configuration des services d’abonnement à la sécurité DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence avancée de prévention des menaces ou de prévention des menaces

Avant de pouvoir activer et configurer la sécurité DNS avancée ou la sécurité DNS, vous devez obtenir et installer une licence prévention des menaces (ou prévention avancée des menaces) ainsi qu’une licence sécurité DNS avancée ou sécurité DNS en plus de toutes les licences de plateforme à partir desquelles elle est exploitée. Les licences sont activées à partir du portail d’assistance client de Palo Alto Networks et doivent être actives avant que l’analyse DNS puisse avoir lieu. De plus, les services d’abonnement à la sécurité DNS (similaires aux autres services de sécurité de Palo Alto Networks) sont gérés via des profils de sécurité qui dépendent à leur tour de la configuration des politiques d’application du réseau telles que définies par les règles de politique de sécurité. Avant d’activer un service d’abonnement de sécurité DNS, il est recommandé de vous familiariser avec les principaux composants de la plateforme de sécurité dans laquelle les abonnements de sécurité sont activés. Reportez-vous à votre documentation du produit pour plus d’informations.

Pour activer et configurer un service d’abonnement à la sécurité DNS afin qu’il fonctionne de manière optimale au sein de votre déploiement de sécurité réseau, reportez-vous aux tâches ci-dessous. Bien qu’il ne soit peut-être pas nécessaire de mettre en œuvre tous les processus illustrés ici, Palo Alto Networks recommande de passer en revue toutes les tâches pour vous familiariser avec les options disponibles pour un déploiement réussi. Il est également recommandé de suivre les meilleures pratiques fournies par Palo Alto Networks pour une convivialité et une sécurité optimales.

- Activez la sécurité DNS ou la sécurité DNS avancée sur ma plateforme de sécurité réseau pour empêcher les menaces DNS de pénétrer dans mon réseau (obligatoire)
- Créez des exceptions de signature de domaine et autorisez les listes pour limiter les faux positifs et empêcher les serveurs DNS internes de déclencher la catégorisation DNS
- Testez les actions de politique configurées pour les catégories de domaines disponibles
- Vérifiez la connectivité de mon pare-feu au service de sécurité DNS
- Limitez les connexions interrompues en raison de ma latence en personnalisant mon paramètre de délai d’expiration de recherche DNS sur le pare-feu

Activation de la sécurité DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention avancée des menaces ou de prévention des menaces

Pour activer la sécurité DNS, vous devez créer (ou modifier) un profil de sécurité antispyware pour accéder au service de sécurité DNS, configurer la gravité du journal et les paramètres de stratégie pour la catégorie (ou les catégories) de signature DNS, puis attacher le profil à une règle de politique de sécurité.

- Strata Cloud Manager
- PAN-OS et Panorama

Activation de la sécurité DNS (Strata Cloud Manager)

STEP 1 | Utilisez les informations d’identification associées à votre compte d’assistance Palo Alto Networks et connectez-vous au Strata Cloud Manager sur le hub https://apps.paloaltonetworks.com/.

STEP 2 | Vérifiez qu’une licence de sécurité DNS et une licence de prévention des menaces (ou prévention avancée des menaces) est active. Sélectionnez **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Aperçu** et cliquez sur le lien des conditions d’utilisation de la licence dans le panneau **Licence**. Vous devriez voir des coches vertes à côté des services de sécurité suivants : Antivirus, Antispyware, Protection contre les vulnérabilités et Sécurité DNS.

STEP 3 | Vérifiez que l'ID d'application *paloalto-dns-security* dans votre stratégie de sécurité est configuré pour enable (activer) le trafic provenant du service de sécurité cloud de sécurité DNS.

> *Si le déploiement de votre pare-feu achemine votre trafic de gestion via un pare-feu de périmètre Internet configuré pour appliquer les politiques de sécurité App-ID, vous devez autoriser les App-ID sur le pare-feu de périmètre ; ne pas le faire empêchera la connectivité de sécurité DNS.*

STEP 4 | Configurez les paramètres de la politique de sécurité de signature DNS pour envoyer les demandes de DNS malveillantes à la mise en entonnoir définie.

Si vous utilisez une liste dynamique externe comme liste d'autorisation de domaine, elle n'a pas la priorité sur les actions de politique de domaine de sécurité DNS. Par conséquent, lorsqu'il existe une correspondance de domaine avec une entrée dans l'EDL et une catégorie de domaine de sécurité DNS, l'action spécifiée sous Sécurité DNS est toujours appliquée, même lorsque l'EDL est explicitement configuré avec une action Autoriser. Si vous souhaitez ajouter des exceptions de domaine DNS, configurez un EDL avec une action d’alerte ou ajoutez-les à la DNS Domain/FQDN Allow List (liste d’autorisation de domaine DNS/FQDN) située dans l’onglet DNS Exceptions (Exceptions DNS).

1. Sélectionnez **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Sécurité DNS**.
2. Créez ou modifiez un profil de sécurité DNS existant.
3. Donnez un **Name (Nom)** au profil et vous pouvez également fournir une description.
4. La section **Catégories DNS**, sous la rubrique Sécurité DNS, contient des sources de signature DNS configurables individuellement, qui vous permettent de définir des actions stratégiques distinctes ainsi que le paramètre de capture de paquets.

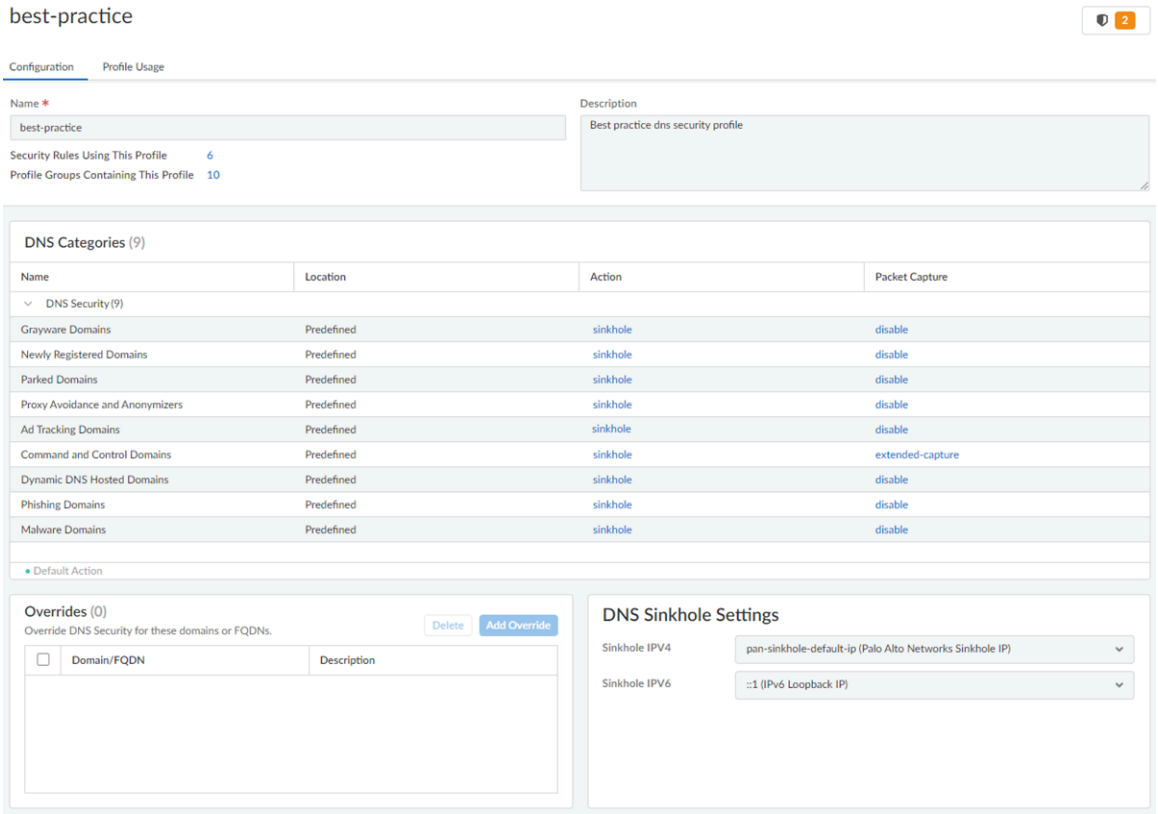
   Palo Alto Networks recommande d’utiliser le paramètre d’action par défaut pour toutes les sources de signature afin d’assurer une couverture optimale et de faciliter la réponse aux incidents et les mesures correctives. Pour plus d’informations sur les meilleures pratiques pour configurer vos paramètres de sécurité DNS, reportez-vous aux Meilleures pratiques pour sécuriser votre réseau contre les fuites au niveau des couches 4 et 7.

   - Sélectionnez une action à prendre lorsque des requêtes DNS correspondant à des sites malveillants connus sont envoyées pour la source de signature de sécurité DNS. Les options sont les suivantes : Alerte, Autoriser, Bloquer ou mise en entonnoir. Palo Alto Networks recommande de régler l’action sur sinkhole.
   - Vous pouvez entièrement contourner l'inspection du trafic DNS en configurant une action de stratégie **Autoriser** avec une gravité de journal correspondante d' **Aucun** pour chaque source de signature DNS.
   - Dans le menu déroulant **Packet Capture (Capture de paquet)**, sélectionnez **single-packet (paquet unique)** pour capturer le premier paquet de la session ou **extended-capture (capture étendue)** pour définir entre 1 et 50 paquets. Vous pouvez ensuite utiliser les captures de paquets pour une analyse plus approfondie.
5. Dans la section **Paramètres DNS Sinkhole**, vérifiez qu’une adresse **Sinkhole** valide est présente. Pour votre commodité, le paramètre par défaut (pan-sinkhole-default-ip) est défini pour

accéder à un serveur sinkhole Palo Alto Networks. Palo Alto Networks peut automatiquement actualiser cette adresse par l’intermédiaire de mises à jour.

***Sinkhole** forge une réponse à une requête DNS pour les domaines qui correspondent à la catégorie DNS configurée pour une action sinkhole sur le serveur sinkhole spécifié, pour aider à identifier les hôtes compromis. Lorsque le nom de domaine complet par défaut du gouffre est utilisé, le pare-feu envoie l’enregistrement CNAME en réponse au client, dans l’espoir qu’un serveur DNS interne résoudra l’enregistrement CNAME, ce qui permettra aux communications malveillantes du client vers le serveur de gouffre configuré d’être enregistrées et facilement identifiables. Toutefois, si les clients se trouvent dans des réseaux sans serveur DNS interne ou utilisent d’autres logiciels ou outils qui ne peuvent pas être correctement résolus un CNAME en une réponse d’enregistrement A, la requête DNS est supprimée, ce qui entraîne des détails incomplets du journal de trafic qui sont cruciaux pour l’analyse des menaces. Dans ces cas, vous devez utiliser l’adresse IP sinkhole suivante : (72.5.65.111).*

Si vous souhaitez modifier l'adresse **Sinkhole IPv4 (IPv4 d'entonnoir)** ou **Sinkhole IPv6 (IPv6 d'entonnoir)** vers un serveur local sur votre réseau ou vers une adresse de boucle, reportez-vous à la section Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.



6. Cliquez sur **OK** pour enregistrer le profil de sécurité DNS.

STEP 5 | Associez le profil de sécurité DNS à une règle de politique de sécurité.

STEP 6 | Vérifiez que l'action de politique est appliquée.

1. Accédez aux domaines de test de sécurité DNS pour vérifier que l’action de la politique pour un type de menace donné est appliquée :
2. Pour suivre l’activité :
    1. Affichez les journaux d’activité et recherchez le domaine URL avec une action sinkhole pour afficher les entrées des journaux pour le domaine de test auquel vous avez accédé.

STEP 7 | Facultatif — Créez une règle de stratégie de dechiffrement pour déchiffrer le trafic DNS-sur-TLS / port 853. La charge utile DNS déchiffrée peut ensuite être traitée à l’aide de la configuration du profil de sécurité DNS contenant vos paramètres de politique DNS. Lorsque le trafic DNS-sur-TLS est déchiffré, les requêtes DNS résultantes dans les journaux de menaces apparaîtront comme une application **dns-base** classique avec un port source de 853.

STEP 8 | Pour les autres options de surveillance, voir Surveillance des services d’abonnement à la sécurité DNS

Activation de la sécurité DNS (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 et versions ultérieures prend en charge les sources de signature DNS configurables individuellement, ce qui vous permet de définir des actions de politique distinctes ainsi qu’un niveau de gravité du journal pour une source de signature donnée. Cela vous permet de créer des actions de sécurité discrètes et précises en fonction de la posture de menace d’un type de domaine en fonction de vos protocoles de sécurité réseau. Les définitions de source de signature DNS sont extensibles via les versions de contenu PAN-OS. Ainsi, lorsque de nouveaux analyseurs de sécurité DNS sont introduits, vous pouvez créer des politiques spécifiques en fonction de la nature de la menace. Lors de la mise à niveau vers PAN-OS 10.0 et ultérieur, la source de sécurité DNS est redéfinie dans de nouvelles catégories pour fournir des contrôles granulaires étendus ; en conséquence, les nouvelles catégories écraseront l'action précédemment définie et acquerront des paramètres par défaut. Assurez-vous d'appliquer à nouveau les paramètres de mise en entonnoir, de gravité du journal et de capture de paquet appropriés pour les catégories de sécurité DNS nouvellement définies.

- PAN-OS 11.0 et versions ultérieures
- PAN-OS 10.x
- PAN-OS 9.1

Activation de la sécurité DNS (PAN-OS 11.0 et versions ultérieures)

STEP 1 | Connectez-vous au NGFW.

STEP 2 | Pour profiter de la sécurité DNS, vous devez avoir un abonnement actif à la sécurité DNS et à la prévention des menaces (ou à la prévention avancée des menaces).

Vérifiez que vous disposez des abonnements nécessaires. 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 3 | Vérifiez que l'ID d'application *paloalto-dns-security* dans votre stratégie de sécurité est configuré pour enable (activer) le trafic provenant du service de sécurité cloud de sécurité DNS.

Si le déploiement de votre pare-feu achemine votre trafic de gestion via un pare-feu de périmètre Internet configuré pour appliquer les politiques de sécurité App-ID, vous devez autoriser les App-ID sur le pare-feu de périmètre ; ne pas le faire empêchera la connectivité de sécurité DNS.

STEP 4 | Configurez les paramètres de la politique de sécurité de signature DNS pour envoyer les demandes de DNS malveillantes à la mise en entonnoir définie.

Si vous utilisez une liste dynamique externe comme liste d'autorisation de domaine, elle n'a pas la priorité sur les actions de politique de domaine de sécurité DNS. Par conséquent, lorsqu'il existe une correspondance de domaine avec une entrée dans l'EDL et une catégorie de domaine de sécurité DNS, l'action spécifiée sous Sécurité DNS est toujours appliquée, même lorsque l'EDL est explicitement configuré avec une action Autoriser. Si vous souhaitez ajouter des exceptions de domaine DNS, configurez un EDL avec une action d’alerte ou ajoutez-les à la DNS Domain/FQDN Allow List (liste d’autorisation de domaine DNS/FQDN) située dans l’onglet DNS Exceptions (Exceptions DNS).

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Créez ou modifiez un profil existant ou sélectionnez un des profils par défaut et clonez-le.
3. Donnez un **Name (Nom)** au profil et vous pouvez également fournir une description.
4. Sélectionnez l’onglet **DNS Policies (Politiques de DNS)**.
5. La colonne **Signature Source (Source de signature)**, sous la rubrique DNS Security (Sécurité DNS), contient des sources de signature DNS configurables individuellement, qui vous permettent de définir des actions stratégiques distinctes ainsi qu'un niveau de gravité du journal.

   Palo Alto Networks recommande de modifier les paramètres par défaut de vos politiques DNS pour les sources de signature afin d'assurer une couverture optimale et de faciliter la réponse aux incidents et les mesures correctives. Suivez les meilleures pratiques pour configurer vos paramètres de sécurité DNS comme indiqué dans les Meilleures pratiques pour sécuriser votre réseau contre les fuites au niveau des couches 4 et 7.

   - Indiquez le niveau de gravité du journal qui est enregistré lorsque le pare-feu détecte un domaine correspondant à une signature DNS. Pour plus d'informations sur les différents niveaux de gravité du journal, consultez Niveaux de gravité des menaces.
   - Sélectionnez une action à prendre lorsque des requêtes DNS correspondant à des sites malveillants connus sont envoyées pour la source de signature de sécurité DNS. Les options

sont défaut, autoriser, bloquer ou sinkhole. Vérifiez que l’action est définie sur la mise en entonnoir.

- Vous pouvez entièrement contourner l'inspection du trafic DNS en configurant une action de stratégie **Autoriser** avec une gravité de journal correspondante d' **Aucun** pour chaque source de signature DNS.
- Dans le menu déroulant **Packet Capture (Capture de paquet)**, sélectionnez **single-packet (paquet unique)** pour capturer le premier paquet de la session ou **extended-capture (capture étendue)** pour définir entre 1 et 50 paquets. Vous pouvez ensuite utiliser les captures de paquets pour une analyse plus approfondie.

6. À la section **DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS)**, vérifiez que l'option **Sinkhole (Mise entonnoir)** est activée. Pour votre facilité, l'adresse entonnoir par défaut (sinkhole.paloaltonetworks.com) permet d’accéder à un serveur de Palo Alto Networks. Palo

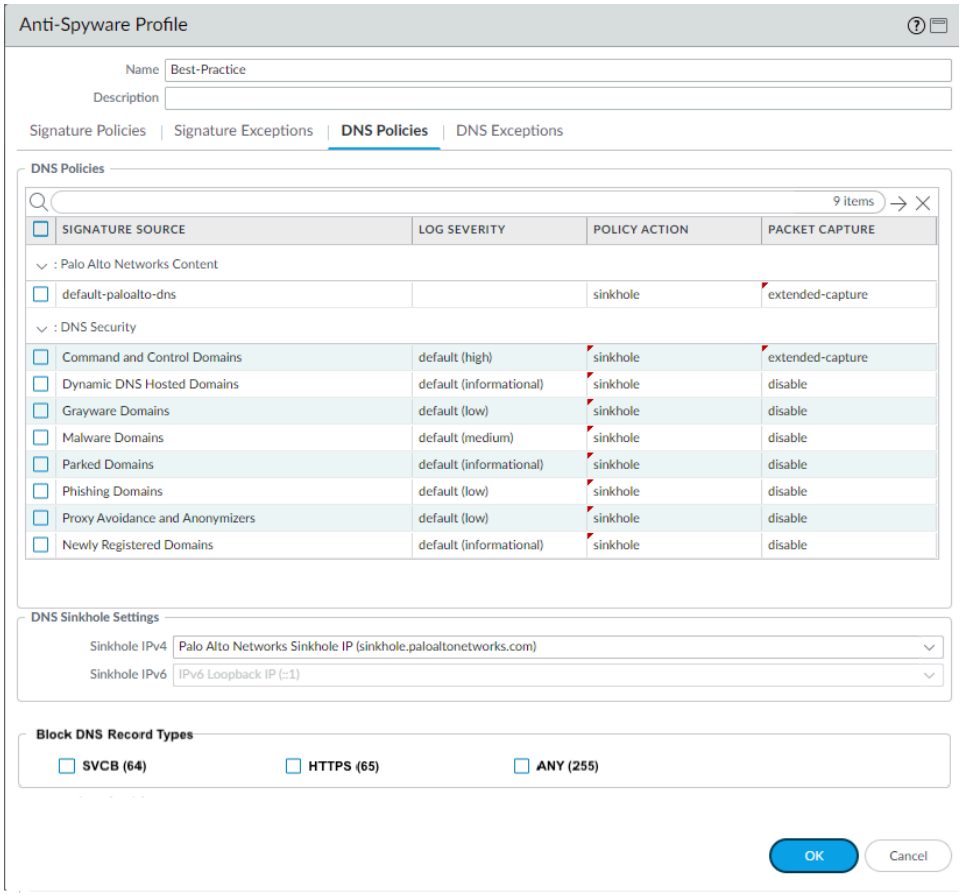
Alto Networks peut automatiquement actualiser cette adresse par l'intermédiaire de mises à jour de contenu.

***Sinkhole** forge une réponse à une requête DNS pour les domaines qui correspondent à la catégorie DNS configurée pour une action sinkhole sur le serveur sinkhole spécifié, pour aider à identifier les hôtes compromis. Lorsque la valeur par défaut sinkhole FQDN (sinkhole.paloaltonetworks.com) est utilisée, le pare-feu envoie l’enregistrement CNAME en réponse au client, dans l’espoir qu’un serveur DNS interne résoudra l’enregistrement CNAME, ce qui permettra aux communications malveillantes du client vers le serveur de gouffre configuré d’être enregistrées et facilement identifiables. Toutefois, si les clients se trouvent dans des réseaux sans serveur DNS interne ou utilisent d’autres logiciels ou outils qui ne peuvent pas être correctement résolus un CNAME en une réponse d’enregistrement A, la requête DNS est supprimée, ce qui entraîne des détails incomplets du journal de trafic qui sont cruciaux pour l’analyse des menaces. Dans ces cas, vous devez utiliser l’adresse IP sinkhole suivante : (72.5.65.111).*

Si vous souhaitez modifier l'adresse **Sinkhole IPv4 (IPv4 d'entonnoir)** ou **Sinkhole IPv6 (IPv6 d'entonnoir)** vers un serveur local sur votre réseau ou vers une adresse de boucle, reportez-vous à la section Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.

7. (Facultatif) Bloquez les types d’enregistrement de ressources DNS spécifiés utilisés pour échanger des informations de clétage lors du chiffrement du hello client dans la connexion TLS suivante. Les types DNS RR suivants sont disponibles : SVCB (64), HTTPS (65) et ANY (255).

   - *Bien qu’il ne soit pas nécessaire de bloquer ECH pour activer la sécurité DNS sur DoH, Palo Alto Networks recommande actuellement de bloquer tous les types d’enregistrement DNS utilisés par ECH pour une sécurité optimale.*
   - *Les normes d’enregistrement des ressources de type 64 et de type 65 sont encore en cours de modification (à l’état d’ébauche) et peuvent être modifiées. Pour plus d’informations sur les RR DNS SVCB et HTTPS, reportez-vous à :* Liaison de service et spécification des paramètres via le DNS (DNS SVCB et HTTPS RRs) *tel que défini par l’*IETF.



8. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.

STEP 5 | Associez le profil antispyware à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Sélectionnez ou créez une **Security Policy Rule (Règle de politique de sécurité)**.
3. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session End (Journalisation en fin de session)** pour activer la journalisation.
4. Dans la section Paramètre de profil, cliquez sur la liste déroulante **Profile Type (Type de profil)** pour voir tous les **Profiles (Profils)**. Sélectionnez le nouveau profil ou le profil modifié dans la liste déroulante **Anti-spyware (Antispyware)**.
5. Cliquez sur **OK (OK)** pour enregistrer la règle de politique.

STEP 6 | Vérifiez que l'action de politique est appliquée.

1. Accédez aux domaines de test de sécurité DNS pour vérifier que l’action de la politique pour un type de menace donné est appliquée :
2. Pour surveiller l'activité sur le pare-feu :
   1. Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité des menaces et l'activité bloquée pour le domaine auquel vous avez accédé.
   2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par `(action eq sinkhole)` pour afficher les journaux des domaines mis en entonnoir.
   3. Pour plus d’options de surveillance, voir Surveillance des services d’abonnement à la sécurité DNS

STEP 7 | Facultatif — Créez une règle de stratégie de déchiffrement pour déchiffrer le trafic DNS-sur-TLS / port 853. La charge utile DNS déchiffrée peut ensuite être traitée à l’aide de la configuration de profil antispyware contenant vos paramètres de stratégie DNS. Lorsque le trafic DNS-sur-TLS est déchiffré, les requêtes DNS résultantes dans les journaux de menaces apparaîtront comme une application **dns-base** classique avec un port source de 853.

STEP 8 | Facultatif—Voir les hôtes infectés qui ont tenté de se connecter à un domaine malveillant

Activationd e la sécurité DNS (PAN-OS 10.x)

STEP 1 | Connectez-vous au NGFW.

STEP 2 | Pour profiter de la sécurité DNS, vous devez avoir un abonnement actif à la sécurité DNS et à la prévention des menaces (ou à la prévention avancée des menaces).

Vérifiez que vous disposez des abonnements nécessaires. 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 3 | Vérifiez que l'ID d'application *paloalto-dns-security* dans votre stratégie de sécurité est configuré pour enable (activer) le trafic provenant du service de sécurité cloud de sécurité DNS.

Si le déploiement de votre pare-feu achemine votre trafic de gestion via un pare-feu de périmètre Internet configuré pour appliquer les politiques de sécurité App-ID, vous devez autoriser les App-ID sur le pare-feu de périmètre ; ne pas le faire empêchera la connectivité de sécurité DNS.

STEP 4 | Configurez les paramètres de la politique de sécurité de signature DNS pour envoyer les demandes de DNS malveillantes à la mise en entonnoir définie.

Si vous utilisez une liste dynamique externe comme liste d'autorisation de domaine, elle n'a pas la priorité sur les actions de politique de domaine de sécurité DNS. Par conséquent, lorsqu'il existe une correspondance de domaine avec une entrée dans l'EDL et une catégorie de domaine de sécurité DNS, l'action spécifiée sous Sécurité DNS est toujours appliquée, même lorsque l'EDL est explicitement configuré avec une action Autoriser. Si vous souhaitez ajouter des exceptions de domaine DNS, configurez un EDL avec une action d’alerte ou ajoutez-les à la DNS Domain/FQDN Allow List (liste d’autorisation de domaine DNS/FQDN) située dans l’onglet DNS Exceptions (Exceptions DNS).

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Créez ou modifiez un profil existant ou sélectionnez un des profils par défaut et clonez-le.
3. Donnez un **Name (Nom)** au profil et vous pouvez également fournir une description.
4. Sélectionnez l’onglet **DNS Policies (Politiques de DNS)**.
5. La colonne **Signature Source (Source de signature)**, sous la rubrique DNS Security (Sécurité DNS), contient des sources de signature DNS configurables individuellement, qui vous permettent de définir des actions stratégiques distinctes ainsi qu'un niveau de gravité du journal.

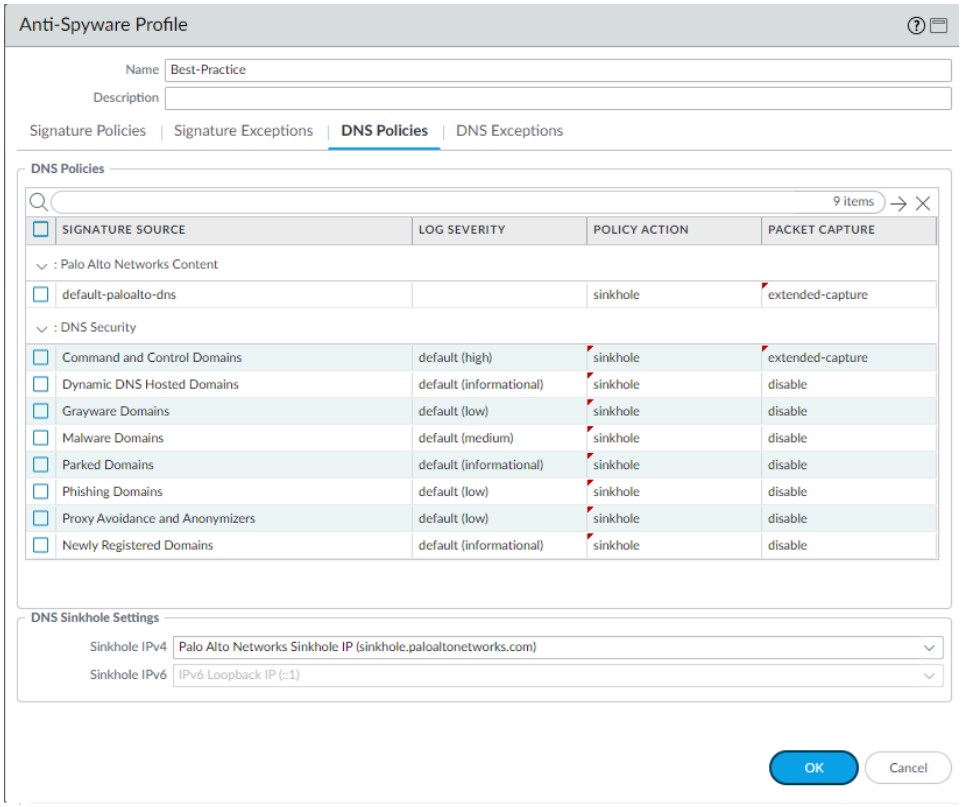
   Palo Alto Networks recommande de modifier les paramètres par défaut de vos politiques DNS pour les sources de signature afin d'assurer une couverture optimale et de faciliter la réponse aux incidents et les mesures correctives. Suivez les meilleures pratiques pour configurer vos paramètres de sécurité DNS comme indiqué dans les Meilleures pratiques pour sécuriser votre réseau contre les fuites au niveau des couches 4 et 7.

   - Indiquez le niveau de gravité du journal qui est enregistré lorsque le pare-feu détecte un domaine correspondant à une signature DNS. Pour plus d'informations sur les différents niveaux de gravité du journal, consultez Niveaux de gravité des menaces.
   - Sélectionnez une action à prendre lorsque des requêtes DNS correspondant à des sites malveillants connus sont envoyées pour la source de signature de sécurité DNS. Les options sont défaut, autoriser, bloquer ou sinkhole. Vérifiez que l’action est définie sur la mise en entonnoir.
   - Vous pouvez entièrement contourner l'inspection du trafic DNS en configurant une action de stratégie **Autoriser** avec une gravité de journal correspondante d' **Aucun** pour chaque source de signature DNS.
   - Dans le menu déroulant **Packet Capture (Capture de paquet)**, sélectionnez **single-packet (paquet unique)** pour capturer le premier paquet de la session ou **extended-capture (capture étendue)** pour définir entre 1 et 50 paquets. Vous pouvez ensuite utiliser les captures de paquets pour une analyse plus approfondie.
6. À la section **DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS)**, vérifiez que l'option **Sinkhole (Mise entonnoir)** est activée. Pour votre facilité, l'adresse entonnoir par défaut (sinkhole.paloaltonetworks.com) permet d’accéder à un serveur de Palo Alto Networks. Palo

Alto Networks peut automatiquement actualiser cette adresse par l'intermédiaire de mises à jour de contenu.

***Sinkhole** forge une réponse à une requête DNS pour les domaines qui correspondent à la catégorie DNS configurée pour une action sinkhole sur le serveur sinkhole spécifié, pour aider à identifier les hôtes compromis. Lorsque la valeur par défaut sinkhole FQDN (sinkhole.paloaltonetworks.com) est utilisée, le pare-feu envoie l’enregistrement CNAME en réponse au client, dans l’espoir qu’un serveur DNS interne résoudra l’enregistrement CNAME, ce qui permettra aux communications malveillantes du client vers le serveur de gouffre configuré d’être enregistrées et facilement identifiables. Toutefois, si les clients se trouvent dans des réseaux sans serveur DNS interne ou utilisent d’autres logiciels ou outils qui ne peuvent pas être correctement résolus un CNAME en une réponse d’enregistrement A, la requête DNS est supprimée, ce qui entraîne des détails incomplets du journal de trafic qui sont cruciaux pour l’analyse des menaces. Dans ces cas, vous devez utiliser l’adresse IP sinkhole suivante : (72.5.65.111).*

Si vous souhaitez modifier l'adresse **Sinkhole IPv4 (IPv4 d'entonnoir)** ou **Sinkhole IPv6 (IPv6 d'entonnoir)** vers un serveur local sur votre réseau ou vers une adresse de boucle, reportez-vous à la section Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.



7. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.

STEP 5 | Associez le profil antispyware à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Sélectionnez ou créez une **Security Policy Rule (Règle de politique de sécurité)**.
3. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session End (Journalisation en fin de session)** pour activer la journalisation.
4. Dans la section Paramètre de profil, cliquez sur la liste déroulante **Profile Type (Type de profil)** pour voir tous les **Profiles (Profils)**. Sélectionnez le nouveau profil ou le profil modifié dans la liste déroulante **Anti-spyware (Antispyware)**.
5. Cliquez sur **OK (OK)** pour enregistrer la règle de politique.

STEP 6 | Vérifiez que l'action de politique est appliquée.

1. Accédez aux domaines de test de sécurité DNS pour vérifier que l’action de la politique pour un type de menace donné est appliquée :
2. Pour surveiller l'activité sur le pare-feu :
   1. Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité des menaces et l'activité bloquée pour le domaine auquel vous avez accédé.
   2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par `(action eq sinkhole)` pour afficher les journaux des domaines mis en entonnoir.
   3. Pour plus d’options de surveillance, voir Surveillance des services d’abonnement à la sécurité DNS

STEP 7 | Facultatif — Créez une règle de stratégie de déchiffrement pour déchiffrer le trafic DNS-sur-TLS / port 853. La charge utile DNS déchiffrée peut ensuite être traitée à l’aide de la configuration de profil antispyware contenant vos paramètres de stratégie DNS. Lorsque le trafic DNS-sur-TLS est déchiffré, les requêtes DNS résultantes dans les journaux de menaces apparaîtront comme une application **dns-base** classique avec un port source de 853.

STEP 8 | Facultatif—Voir les hôtes infectés qui ont tenté de se connecter à un domaine malveillant

Activation de la sécurité DNS (PAN-OS 9.1)

STEP 1 | Connectez-vous au NGFW.

STEP 2 | Pour tirer parti de la sécurité DNS, vous devez disposer d’un abonnement actif à la sécurité DNS et à la prévention des menaces.

Vérifiez que vous disposez des abonnements nécessaires. 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 3 | Vérifiez que l'ID d'application *paloalto-dns-security* dans votre stratégie de sécurité est configuré pour enable (activer) le trafic provenant du service de sécurité cloud de sécurité DNS.

Si le déploiement de votre pare-feu achemine votre trafic de gestion via un pare-feu de périmètre Internet configuré pour appliquer les politiques de sécurité App-ID, vous devez autoriser les App-ID sur le pare-feu de périmètre ; ne pas le faire empêchera la connectivité de sécurité DNS.

STEP 4 | Configurez les paramètres de la politique de sécurité de signature DNS pour envoyer les demandes de DNS malveillants à la mise en entonnoir définie.

Si vous utilisez une liste dynamique externe comme liste d'autorisation de domaine, elle n'a pas la priorité sur les actions de politique de domaine de sécurité DNS. Par conséquent, lorsqu'il existe une correspondance de domaine avec une entrée dans l'EDL et une catégorie de domaine de sécurité DNS, l'action spécifiée sous Sécurité DNS est toujours appliquée, même lorsque l'EDL est explicitement configuré avec une action Autoriser. Si vous souhaitez ajouter des exceptions de domaine DNS, vous pouvez configurer une liste EDL avec une action d’alerte.

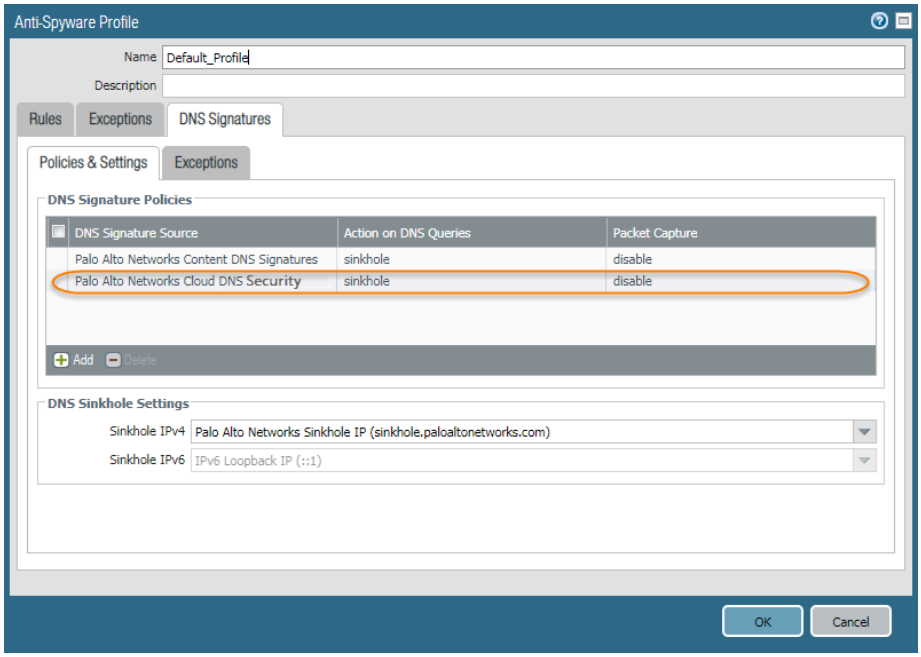
1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Créez ou modifiez un profil existant ou sélectionnez un des profils par défaut et clonez-le.
3. Donnez un **Name (Nom)** au profil et vous pouvez également fournir une description.
4. Sélectionnez l’onglet **DNS Signatures (Signatures DNS) > Policies & Settings (Politiques et paramètres)**.
5. Si la source **Palo Alto Networks DNS Security** (Sécurité DNS Palo Alto Networks) n’est pas présente, cliquez sur **Add (Ajouter)** et sélectionnez-la dans la liste.
6. Sélectionnez une action à prendre lorsque des requêtes DNS correspondant à des sites malveillants connus sont envoyées pour la source de signature de sécurité DNS. Les options sont les suivantes : Alerte, Autoriser, Bloquer ou mise en entonnoir. Vérifiez que l’action est définie sur la mise en entonnoir.
7. (Facultatif) Dans la liste déroulante **Packet Capture (Capture de paquets)**, sélectionnez **single-packet (un seul paquet)** pour capturer le premier paquet de la session ou **extended-capture (capture étendue)** pour définir de 1 à 50 paquets. Vous pouvez ensuite utiliser les captures de paquets pour une analyse plus approfondie.
8. À la section **DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS)**, vérifiez que l'option **Sinkhole (Mise entonnoir)** est activée. Pour votre facilité, l'adresse entonnoir par défaut (sinkhole.paloaltonetworks.com) permet d’accéder à un serveur de Palo Alto Networks. Palo

Alto Networks peut automatiquement actualiser cette adresse par l'intermédiaire de mises à jour de contenu.

***Sinkhole** forge une réponse à une requête DNS pour les domaines qui correspondent à la catégorie DNS configurée pour une action sinkhole sur le serveur sinkhole spécifié, pour aider à identifier les hôtes compromis. Lorsque la valeur par défaut sinkhole FQDN (sinkhole.paloaltonetworks.com) est utilisée, le pare-feu envoie l’enregistrement CNAME en réponse au client, dans l’espoir qu’un serveur DNS interne résoudra l’enregistrement CNAME, ce qui permettra aux communications malveillantes du client vers le serveur de gouffre configuré d’être enregistrées et facilement identifiables. Toutefois, si les clients se trouvent dans des réseaux sans serveur DNS interne ou utilisent d’autres logiciels ou outils qui ne peuvent pas être correctement résolus un CNAME en une réponse d’enregistrement A, la requête DNS est supprimée, ce qui entraîne des détails incomplets du journal de trafic qui sont cruciaux pour l’analyse des menaces. Dans ces cas, vous devez utiliser l’adresse IP sinkhole suivante : (72.5.65.111).*

Si vous souhaitez modifier l'adresse **Sinkhole IPv4 (IPv4 d'entonnoir)** ou **Sinkhole IPv6 (IPv6 d'entonnoir)** vers un serveur local sur votre réseau ou vers une adresse de boucle, reportez-vous à la section Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.

9. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.



STEP 5 | Associez le profil antispyware à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Sélectionnez ou créez une **Security Policy Rule (Règle de politique de sécurité)**.
3. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session End (Journalisation en fin de session)** pour activer la journalisation.
4. Dans la section Paramètre de profil, cliquez sur la liste déroulante **Profile Type (Type de profil)** pour voir tous les **Profiles (Profils)**. Sélectionnez le nouveau profil ou le profil modifié dans la liste déroulante **Anti-spyware (Antispyware)**.
5. Cliquez sur **OK (OK)** pour enregistrer la règle de politique.

STEP 6 | Vérifiez que l'action de politique est appliquée.

1. Accédez aux domaines de test de sécurité DNS pour vérifier que l’action de la politique pour un type de menace donné est appliquée :
2. Pour surveiller l'activité sur le pare-feu :
   1. Affichez l’activité de la menace et recherchez l’URL du domaine de test et l’activité bloquée pour le domaine auquel vous avez accédé.
   2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par `(action eq sinkhole)` pour afficher les journaux des domaines mis en entonnoir.
   3. Pour plus d’options de surveillance, voir Surveillance des services d’abonnement à la sécurité DNS

STEP 7 | Facultatif — Créez une règle de stratégie de déchiffrement pour déchiffrer le trafic DNS-sur-TLS / port 853. La charge utile DNS déchiffrée peut ensuite être traitée à l’aide de la configuration de profil antispyware contenant vos paramètres de stratégie DNS. Lorsque le trafic DNS-sur-TLS est déchiffré, les requêtes DNS résultantes dans les journaux de menaces apparaîtront comme une application **dns-base** classique avec un port source de 853.

STEP 8 | Facultatif—Voir les hôtes infectés qui ont tenté de se connecter à un domaine malveillant

Activation de la sécurité DNS avancée

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour un support amélioré des fonctionnalités) ❑ Licence de prévention avancée des menaces ou de prévention des menaces

La sécurité DNS avancée complète votre configuration de sécurité DNS existante pour fournir une protection supplémentaire contre le détournement DNS en inspectant les modifications apportées aux réponses DNS. Vous devez avoir entièrement configuré les paramètres de sécurité DNS avant de procéder à cette étape.

Pour activer la sécurité DNS avancée, vous devez créer (ou modifier) un profil de sécurité antispyware pour accéder au service de sécurité DNS avancée, configurer la gravité du journal et les paramètres de stratégie pour la catégorie (ou les catégories) de signature DNS, puis attacher le profil à une règle de politique de sécurité.

- PAN-OS 11.2 et versions ultérieures
- Gestion du cloud

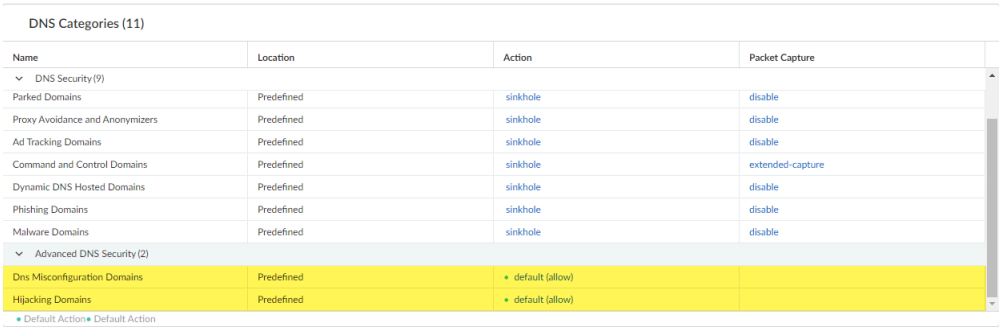
Activation de la sécurité DNS avancée (Strata Cloud Manager)

STEP 1 | Utilisez les informations d’identification associées à votre compte d’assistance Palo Alto Networks et connectez-vous au Strata Cloud Manager sur le hub https://apps.paloaltonetworks.com/.

STEP 2 | Vérifiez qu’une licence de sécurité DNS et une licence de prévention des menaces est active. Sélectionnez **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Aperçu** et cliquez sur le lien des conditions d’utilisation de la licence dans le panneau **Licence**. Vous devriez voir des coches vertes à côté des services de sécurité suivants : Antivirus, Antispyware, Protection contre les vulnérabilités et Sécurité DNS.

STEP 3 | Mettez à jour ou créez un nouveau profil de sécurité DNS pour permettre des requêtes de sécurité DNS avancée en temps réel. Généralement, il s’agit de votre profil de sécurité DNS existant utilisé pour la configuration de la sécurité DNS.

1. Sélectionnez un profil de sécurité DNS existant ou **Ajoutez**-en un nouveau (**Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Sécurité DNS**).
2. Sélectionnez votre profil de sécurité DNS, puis accédez à **Catégories DNS**.



3. Pour chaque catégorie de domaine de sécurité DNS avancée, spécifiez une **Action** de stratégie à prendre lorsqu’un type de domaine correspondant est détecté. Deux moteurs d’analyse sont actuellement disponibles : **Domaines de mauvaise configuration DNS** et **Détournement de domaines**.

   Options d’action stratégique :

   - **autoriser** : la requête DNS est autorisée.

     Vous pouvez configurer Strata Cloud Manager pour générer une alerte lorsque le type de domaine applicable est détecté en définissant l’action sur autoriser et la gravité des journaux sur informationnel.

   - **bloquer** : la requête DNS est bloquée.
   - **sinkhole** : forge une réponse DNS pour une requête DNS ciblant un domaine malveillant détecté. Cela dirige la résolution du nom de domaine malveillant vers une adresse IP spécifique (appelée IP Sinkhole), qui est intégrée en tant que réponse. L’adresse IP Sinkhole par défaut est définie pour accéder à un serveur Palo Alto Networks. Palo Alto Networks peut automatiquement actualiser cette adresse IP par l'intermédiaire de mises à jour de contenu.

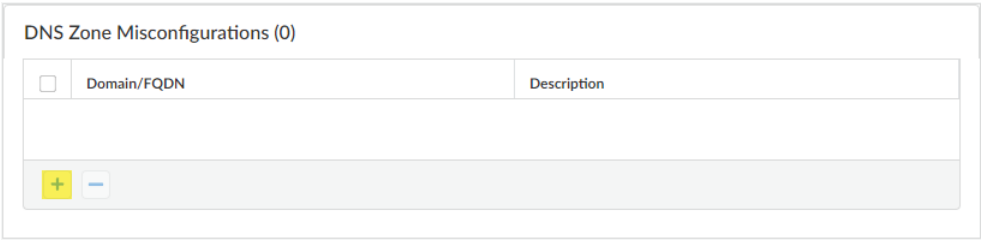
STEP 4 | (Facultatif) Spécifiez les domaines parents publics au sein de votre organisation pour lesquels vous souhaitez que la sécurité DNS avancée analyse et surveille la présence de domaines mal configurés. Les domaines mal configurés sont créés par inadvertance par des propriétaires de domaines qui pointent des enregistrements d’alias vers des domaines tiers à l’aide de types d’enregistrements CNAME, MX, NS, à l’aide d’entrées qui ne sont plus valides, ce qui permet à un attaquant de prendre le contrôle du domaine en enregistrant les domaines expirés ou inutilisés.

Les TLD (domaines de premier niveau) et les domaines de niveau racine ne peuvent pas être ajoutés à la liste des erreurs de configuration de la zone DNS.

1. Sélectionnez un profil de sécurité DNS (**Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Sécurité DNS**) qui contient une configuration de sécurité DNS avancée.

2. Dans la section **Erreurs de configuration de la zone DNS**, ajoutez des domaines parents publics avec une description facultative pour vous aider à identifier l’utilisation ou la propriété du domaine au sein de votre organisation.

   Les entrées doivent contenir un « . » dans le domaine au format suivant (ex. paloaltonetworks.com), sinon il est analysé comme un nom d’hôte, qui est considéré comme un domaine privé.



3. Cliquez sur **OK** pour quitter et enregistrer le profil de sécurité DNS.

STEP 5 | (Facultatif) Surveillez l’activité sur Strata Cloud Manager pour les requêtes DNS détectées à l’aide de la sécurité DNS avancée. Les catégories de sécurité DNS analysées à l’aide de l’analyse en temps réel de la sécurité DNS avancée du paquet de réponse DNS ont le préfixe « adns » suivi de la catégorie. Par exemple, adns-dnsmisconfig, où ’dnsmisconfig’ indique le type de catégorie DNS pris en charge. Si la catégorie de domaine DNS a été déterminée en analysant le paquet de requête DNS, la catégorie spécifiée s’affiche avec le préfixe « dns » suivi de la catégorie. Par exemple, ’dns-grayware.’

1. Accédez aux domaines de test de la sécurité DNS avancée pour vérifier que l’action de stratégie pour un type de menace donné est appliquée.
2. Sélectionnez **Incidents et alertes** > **Visionneuse de journaux**. Vous pouvez filtrer les journaux de menaces en fonction du type spécifique de catégorie de domaine de sécurité DNS avancée, par exemple `threat_category.value = ’adns-hijacking’`, où la variable `adns-hijacking` indique les requêtes DNS qui ont été catégorisées comme une tentative de détournement DNS malveillante par la sécurité DNS avancée. Les catégories de menaces de la sécurité DNS avancée suivantes sont disponibles dans les journaux :

   Catégories de sécurité DNS avancées

   - **Détournement de DNS**—`adns-hijacking`

     Les domaines de détournement de DNS ont un ID de menace de (UTID : 109,004,100).

   - **Mauvaise configuration DNS**—`adns-dnsmisconfig`

     Les domaines de mauvaise configuration DNS ont trois ID de menace, qui correspondent à trois variantes de types de domaines de mauvaise configuration DNS : dnsmisconfig_zone (UTID : 109,004,200), dnsmisconfig_zone_dangling (UTID : 109 004 201) et dnsmisconfig_claimable_nx (UTID : 109,004,202). Vous pouvez limiter la recherche en croisant une valeur d’ID de menace qui correspond à un type de domaine spécifique de mauvaise configuration DNS. Par exemple, `threat_category.value = ’adns-dnsmisconfig’` et `Threat ID = 109004200`, où 109004200 indique l’ID de menace

d’un domaine de mauvaise configuration DNS qui n’achemine pas le trafic vers un domaine actif en raison d’un problème de configuration du serveur DNS.

Catégories DNS analysées à l’aide de l’analyse des réponses améliorée de la sécurité DNS avancée.

- **DNS** —`adns-benign`
- **Domaines de logiciels malveillants** —`adns-malware`
- **Domaines de commande et de contrôle**—`adns-c2`
- **Domaines de phishing**—`adns-phishing`
- **Domaines hébergés DNS dynamiques**—`adns-ddns`
- **Domaines nouvellement enregistrés**—`adns-new-domain`
- **Domaines de logiciel indésirable**—`adns-grayware`
- **Domaines parqués**—`adns-parked`
- **Évitement de proxy et anonymiseurs**—`adns-proxy`
- **Domaines de suivi des publicités**—`adns-adtracking`

Si la requête DNS ne se termine pas dans le délai d’expiration spécifié pour la sécurité DNS avancée, la catégorisation de la sécurité DNS sera utilisée, dans la mesure du possible. Dans ces cas, la notation héritée de la catégorie est utilisée, par exemple, au lieu de `adns-malware`, ce sera classé comme suit : `dns-malware`, indiquant que la valeur de catégorisation de la sécurité DNS a été utilisée.

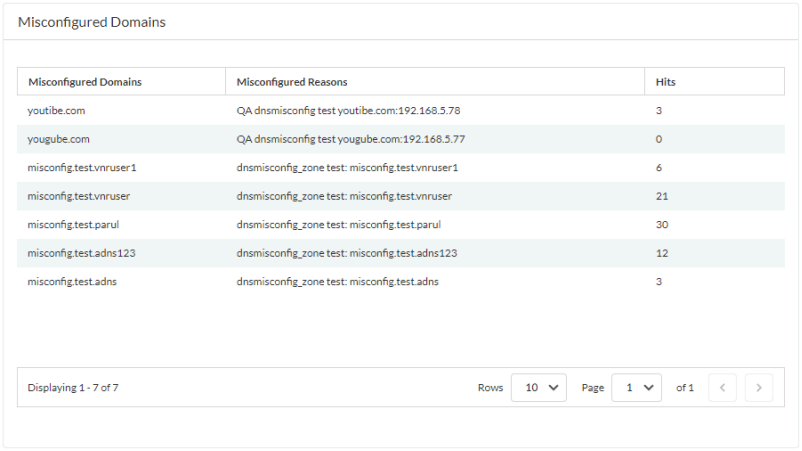
3. Sélectionnez une entrée de journal pour afficher les détails de la requête DNS.
4. La **catégorie** DNS s’affiche sous le volet **Général** de la vue détaillée du journal. En outre, vous pouvez voir d’autres aspects si la menace, y compris l’URL d’origine, le type de menace spécifique et les caractéristiques associées.

STEP 6 | (Facultatif) Récupérez la liste des domaines mal configurés et des domaines détournés détectés par le service de sécurité DNS avancée. Les domaines mal configurés sont basés sur les entrées de domaine parent publiques ajoutées aux **Erreurs de configuration de la zone DNS**.

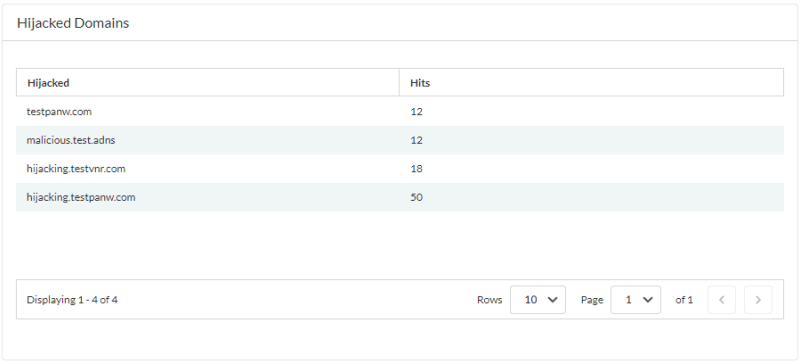
Les entrées de domaine mal configurées qui sont supprimées de votre réseau ne sont pas immédiatement répercutées dans les statistiques du tableau de bord de la sécurité DNS avancée.

1. Utilisez les informations d’identification associées à votre compte d’assistance Palo Alto Networks et connectez-vous à Strata Cloud Manager sur le hub.
2. Sélectionnez **Tableaux de bord** > **Plus de tableaux de bord** > **Sécurité DNS** pour ouvrir le tableau de bord de la sécurité DNS.
3. Depuis le tableau de bord de la sécurité DNS, reportez-vous aux widgets suivants :
   - **Domaines mal configurés**: affiche une liste des domaines non résolubles associés au(x) domaine(s) parent(s) public(s) spécifié(s) par l’utilisateur. Pour chaque entrée, il y a une

raison pour l’erreur de configuration et un nombre de correspondances de trafic basé sur l’IP source.



- **Domaines détournés** : affiche une liste des domaines détournés, tel que déterminé par la sécurité DNS avancée. Pour chaque entrée, il y a une raison de catégorisation et un nombre de correspondances de trafic basé sur l’IP source.



Activation de la sécurité DNS avancée (PAN-OS 11.2 et versions ultérieures)

Palo Alto Networks recommande d’activer votre fonctionnalité de sécurité DNS avant de configurer la sécurité DNS avancée.

STEP 1 | Connectez-vous au NGFW.

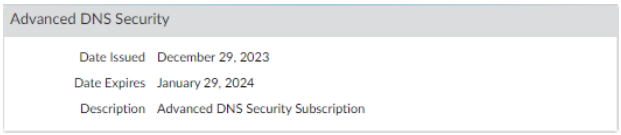
STEP 2 | Mettre à jour la version du contenu version 8832 ou ultérieure.

STEP 3 | Pour empêcher l’accès à des domaines malveillants connus et inconnus à l’aide de la sécurité DNS avancée, vous devez disposer d’une licence de sécurité DNS avancée active. Elle ne doit être installée qu’après la mise à niveau vers PAN-OS 11.2.

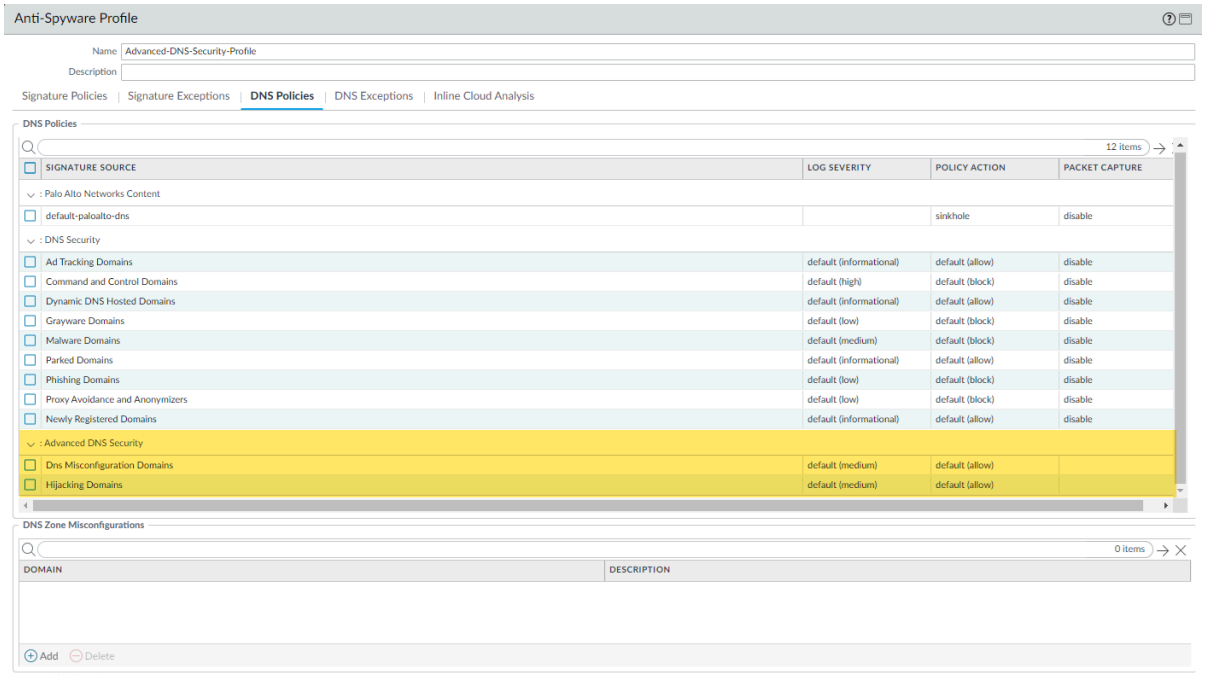
La sécurité DNS avancée prend en charge un modèle de licence qui englobe la fonctionnalité de sécurité DNS dans la licence de sécurité DNS avancée lorsqu’elle est installée sur un pare-feu jusque là sans licence. Si vous effectuez une mise à niveau à partir d’un pare-feu avec une licence de sécurité DNS existante, des entrées indiquant la présence de licences de sécurité DNS et de sécurité DNS avancée distinctes sont affichées. Dans ce cas, la licence de sécurité DNS est une entrée passive et toutes les fonctionnalités de sécurité DNS et de sécurité DNS avancée sont conférées par la licence DNS avancée, y compris la date d’expiration pertinente. Les pare-feu jusque là sans licence de sécurité DNS affichent une licence de sécurité DNS avancée, cependant, elle fournit à la fois des fonctionnalités de sécurité DNS et de sécurité DNS avancée.

Par conséquent, si vous passez d’une version PAN-OS exploitant une licence de sécurité DNS avancée à une version qui ne prend pas en charge la sécurité DNS avancée, le pare-feu continue d’afficher et de conférer des fonctionnalités de sécurité DNS par le biais de la licence de sécurité DNS avancée, mais cela est limité aux fonctionnalités de base de la sécurité DNS.

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



STEP 4 | Mettez à jour ou créez un nouveau profil de sécurité antispyware pour activer les requêtes de sécurité DNS avancée en temps réel. En règle générale, il s’agit de votre profil de sécurité antispyware existant utilisé pour la configuration de la sécurité DNS.



1. Sélectionnez un profil de sécurité Antispyware existant ou **Ajoutez** un nouveau (**Objets** > **Profils de sécurité** > **Antispyware**).
2. Sélectionnez votre profil de sécurité Antispyware, puis accédez à **Politiques DNS**.
3. Pour chaque catégorie de domaine de sécurité DNS avancée, spécifiez une **Gravité des journaux** et une **Action politique** à prendre lorsqu’un type de domaine est détecté à l’aide d’un moteur d’analyse correspondant. Deux moteurs d’analyse sont actuellement disponibles : **Domaines de mauvaise configuration DNS** et **Détournement de domaines**.

   Options d’action stratégique :

   - **autoriser** : la requête DNS est autorisée.

     Vous pouvez configurer le pare-feu pour qu’il génère une alerte lorsque le type de domaine applicable est détecté en définissant l’action sur autoriser et la gravité des journaux sur informative.

   - **bloquer** : la requête DNS est bloquée.
   - **sinkhole** : forge une réponse DNS pour une requête DNS ciblant un domaine malveillant détecté. Cela dirige la résolution du nom de domaine malveillant vers une adresse IP spécifique (appelée IP Sinkhole), qui est intégrée en tant que réponse. L’adresse IP Sinkhole par défaut est définie

pour accéder à un serveur Palo Alto Networks. Palo Alto Networks peut automatiquement actualiser cette adresse IP par l'intermédiaire de mises à jour de contenu.

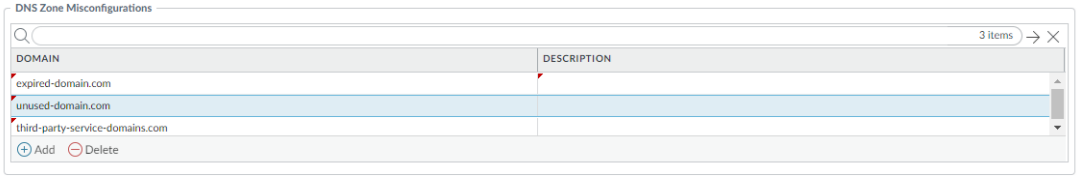
Options de gravité des journaux :

- **aucun**: l’événement n’a pas de niveau de gravité des journaux associé.
- **faible**—Menaces de niveau d’alerte ayant très peu d’incidence sur l’infrastructure de l’entreprise. Celles-ci requièrent généralement un accès au système physique ou local et peuvent entraîner des problèmes DoS ou de confidentialité de la victime, ainsi qu'une fuite des informations.
- **informationnel**—Événements suspects qui ne constituent pas une menace immédiate, mais qui sont signalés pour attirer l’attention sur des problèmes plus profonds qui pourraient éventuellement exister.
- **moyen**—Menaces mineures dans lesquelles l’incidence est minimisée, telles que les attaques DoS qui ne compromettent pas la cible ou les exploits nécessitant qu’un pirate réside sur le même réseau local que la victime, affectent uniquement les configurations non standard ou les applications obscures, ou fournissent un accès très limité.
- **élevé**—Menaces pouvant devenir critiques mais ayant des facteurs atténuants ; par exemple, elles peuvent être difficiles à exploiter, ne mènent pas à des privilèges élevés ou ne ciblent pas un grand nombre de victimes.
- **critique**—Menaces graves, telles que celles affectant les installations par défaut des logiciels déployés à grande échelle et menant à la compromission des serveurs, et où le code d’exploitation est largement accessible aux pirates. Le pirate n'a généralement pas besoin d'informations d'authentification spéciales ni de connaissances relatives à chaque victime, et la cible n'a pas besoin d'être manipulée au point d'effectuer des fonctions spéciales.

4. Cliquez sur **OK** pour quitter la boîte de dialogue de configuration du profil de sécurité antispyware et **Commettre** vos modifications.

STEP 5 | (Facultatif) Spécifiez les domaines parents publics au sein de votre organisation pour lesquels vous souhaitez que la sécurité DNS avancée analyse et surveille la présence de domaines mal configurés. Les domaines mal configurés sont créés par inadvertance par des propriétaires de domaines qui pointent des enregistrements d’alias vers des domaines tiers à l’aide de types d’enregistrements CNAME, MX, NS, à l’aide d’entrées qui ne sont plus valides, ce qui permet à un attaquant de prendre le contrôle du domaine en enregistrant les domaines expirés ou inutilisés.

Les TLD (domaines de premier niveau) et les domaines de niveau racine ne peuvent pas être ajoutés à la liste des erreurs de configuration de la zone DNS.



1. Sélectionnez un profil de sécurité Antispyware (**Objets** > **Profils de sécurité** > **Antispyware**) et allez à **Politiques DNS**.

2. Dans la section **Erreurs de configuration de la zone DNS**, ajoutez des domaines parents publics avec une description facultative pour vous aider à identifier l’utilisation ou la propriété du domaine au sein de votre organisation.

   Les entrées doivent contenir un « . » dans le domaine au format suivant (ex. paloaltonetworks.com), sinon il est analysé comme un nom d’hôte, qui est considéré comme un domaine privé.

3. Cliquez sur **OK** pour quitter la boîte de dialogue de configuration du profil de sécurité antispyware et **Commettre** vos modifications.

STEP 6 | (Facultatif) Configurez le paramètre maximal de délai d’expiration de la recherche de signature DNS avancée. Lorsque cette valeur est dépassée, la réponse DNS passe sans effectuer d’analyse à l’aide de la sécurité DNS avancée.

STEP 7 | (Facultatif [Si vous ne disposez pas du dernier certificat de périphérique]) Installez un certificat de pare-feu mis à jour utilisé pour vous authentifier auprès du service d’analyse cloud en ligne de prévention avancée des menaces. Répétez l'opération pour tous les pare-feu activés pour l'analyse cloud en ligne.

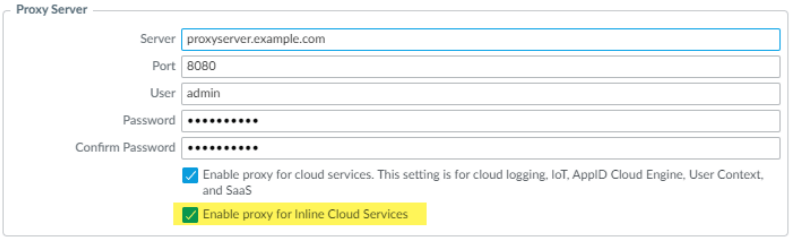
Si vous avez déjà installé un certificat de pare-feu mis à jour dans le cadre de votre processus d’intégration de la sécurité IoT, de la télémétrie du périphérique, de la prévention avancée des menaces ou du filtrage avancé d’URL, cette étape n’est pas nécessaire.

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 **Périphérique** > **Configuration** > **Services** et éditez les détails des **Services**.
   2. Spécifiez les paramètres **Serveur proxy** et **Activer le proxy pour les services cloud en ligne**. Vous pouvez fournir une adresse IP ou un FQDN dans le champ **Serveur**.

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



   3. Cliquez sur **OK**.

STEP 9 | (Facultatif) Vérifiez l’état de la connectivité de votre pare-feu au service cloud de sécurité DNS avancée.

STEP 10 | (Facultatif) Surveillez l’activité sur le pare-feu pour détecter les requêtes DNS qui ont été détectées à l’aide de la sécurité DNS avancée. Les catégories de sécurité DNS analysées à l’aide de l’analyse en temps réel de la sécurité DNS avancée du paquet de réponse DNS ont le préfixe « adns » suivi de la catégorie. Par exemple, adns-dnsmisconfig, où ’dnsmisconfig’ indique le type de catégorie DNS pris en charge. Si la catégorie de domaine DNS a été déterminée en analysant le paquet de requête DNS, la catégorie spécifiée s’affiche avec le préfixe « dns » suivi de la catégorie. Par exemple, ’dns-grayware.’

1. Accédez aux domaines de test de la sécurité DNS avancée pour vérifier que l’action de stratégie pour un type de menace donné est appliquée.
2. Sélectionnez **Moniteur** > **Journaux** > **Menace**. Vous pouvez filtrer les journaux en fonction du type spécifique de catégorie de domaine de sécurité DNS avancée, par exemple `(category-of-threatid eq adns-hijacking)`, où la variable `adns-hijacking` indique les requêtes DNS qui ont été classées comme une tentative de détournement de DNS malveillante par la sécurité DNS avancée. Les catégories de menaces de la sécurité DNS avancée suivantes sont disponibles dans les journaux :

   Catégories de sécurité DNS avancées

   - **Détournement de DNS**—`adns-hijacking`

     Les domaines de détournement de DNS ont un ID de menace de (UTID : 109,004,100).

   - **Mauvaise configuration DNS**—`adns-dnsmisconfig`

     Les domaines de mauvaise configuration DNS ont trois ID de menace, qui correspondent à trois variantes de types de domaines de mauvaise configuration DNS : dnsmisconfig_zone (UTID : 109,004,200), dnsmisconfig_zone_dangling (UTID : 109 004 201) et dnsmisconfig_claimable_nx (UTID : 109,004,202). Vous pouvez limiter la recherche en croisant une valeur d’ID de menace qui correspond à un type de domaine spécifique de mauvaise configuration DNS. Par exemple, (category-of-threatid eq adns-dnsmisconfig) et (threatid eq 109004200), où 109004200 indique l’ID de menace d’un domaine de mauvaise configuration DNS qui n’achemine pas le trafic vers un domaine actif en raison d’un problème de configuration de serveur DNS.

   Catégories DNS analysées à l’aide de l’analyse des réponses améliorée de la sécurité DNS avancée.

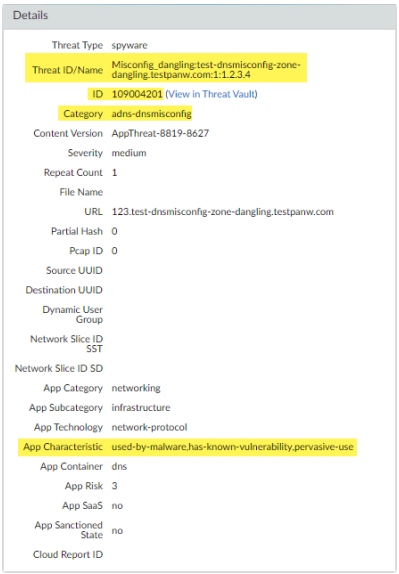
   Vous devez utiliser un pare-feu exécutant PAN-OS 11.2 et versions ultérieures pour tirer parti de l’analyse en temps réel améliorée de la sécurité DNS avancée.

   - **DNS** —`adns-benign`
   - **Domaines de logiciels malveillants** —`adns-malware`
   - **Domaines de commande et de contrôle**—`adns-c2`
   - **Domaines de phishing**—`adns-phishing`
   - **Domaines hébergés DNS dynamiques**—`adns-ddns`
   - **Domaines nouvellement enregistrés**—`adns-new-domain`
   - **Domaines de logiciel indésirable**—`adns-grayware`
   - **Domaines parqués**—`adns-parked`

- **Évitement de proxy et anonymiseurs**—`adns-proxy`
- **Domaines de suivi des publicités**—`adns-adtracking`

Si la requête DNS ne se termine pas dans le délai d’expiration spécifié pour la sécurité DNS avancée, la catégorisation de la sécurité DNS sera utilisée, dans la mesure du possible. Dans ces cas, la notation héritée de la catégorie est utilisée, par exemple, au lieu de `adns-malware`, ce sera classé comme suit : `dns-malware`, indiquant que la valeur de catégorisation de la sécurité DNS a été utilisée.

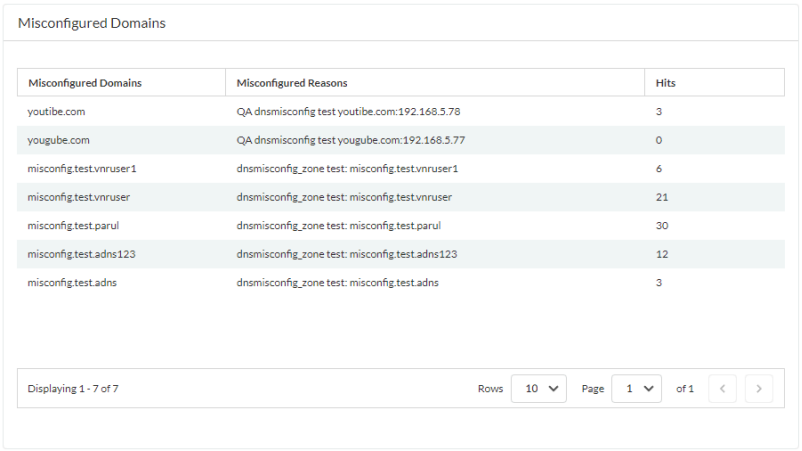
3. Sélectionnez une entrée de journal pour afficher les détails de la requête DNS.
4. La **Catégorie** DNS s’affiche sous le volet**Détails** de la vue détaillée du journal. En outre, vous pouvez voir d’autres aspects de la menace, y compris l’ID de menace, qui inclut le domaine d’origine, la catégorie de menace spécifique et d’autres caractéristiques associées, ainsi que le type Q associé et les données R à l’aide du format suivant : détournement :<FQDN>:<QTYPE>:<RDATA>où <QTYPE> représente le type d’enregistrement de ressource DNS et <RDATA> représente l’adresse IP détournée.



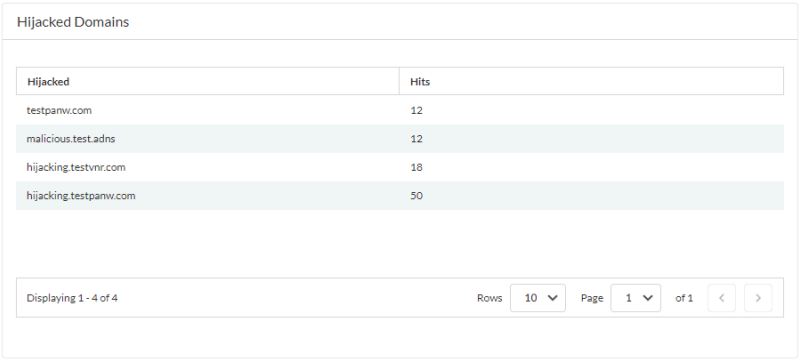
STEP 11 | (Facultatif) Récupérez la liste des domaines mal configurés et des domaines détournés détectés par le service de sécurité DNS avancée. Les domaines mal configurés sont basés sur les entrées de domaine parent publiques ajoutées aux **Erreurs de configuration de la zone DNS**.

Les entrées de domaine mal configurées qui sont supprimées de votre réseau ne sont pas immédiatement répercutées dans les statistiques du tableau de bord de la sécurité DNS avancée.

1. Utilisez les informations d’identification associées à votre compte d’assistance Palo Alto Networks et connectez-vous à Strata Cloud Manager sur le hub.
2. Sélectionnez **Tableaux de bord** > **Plus de tableaux de bord** > **Sécurité DNS** pour ouvrir le tableau de bord de la sécurité DNS.
3. Depuis le tableau de bord de la sécurité DNS, reportez-vous aux widgets suivants :
   - **Domaines mal configurés**: affiche une liste des domaines non résolubles associés au(x) domaine(s) parent(s) public(s) spécifié(s) par l’utilisateur. Pour chaque entrée, il y a une raison pour l’erreur de configuration et un nombre de correspondances de trafic basé sur l’IP source.



   - **Domaines détournés** : affiche une liste des domaines détournés, tel que déterminé par la sécurité DNS avancée. Pour chaque entrée, il y a une raison de catégorisation et un nombre de correspondances de trafic basé sur l’IP source.



Configuration de la sécurité DNS sur TLS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence avancée de prévention des menaces ou de prévention des menaces

Vous pouvez obtenir une visibilité et un contrôle sur la sécurité DNS sur les requêtes TLS en déchiffrant la charge utile DNS contenue dans la requête DNS chiffrée. La charge utile DNS déchiffrée peut ensuite être traitée à l’aide de la configuration du profil de sécurité contenant vos paramètres de politique DNS. Les requêtes DNS dont il a été déterminé qu’elles provenaient de sources TLS ont un port source de 853 dans les journaux des menaces.

- Strata Cloud Manager
- PAN-OS et Panorama

Configuration de la sécurité DNS sur TLS (Strata Cloud Manager)

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 | Activation de la sécurité DNS est configuré pour inspecter les requêtes DNS. Vous pouvez utiliser votre profil de sécurité existant si vous souhaitez utiliser les mêmes paramètres des **politiques DNS** pour la sécurité DNS sur le trafic TLS.

STEP 3 | Créez une règle de politique de déchiffrement avec une action de déchiffrement du trafic HTTPS sur le port 853, qui inclut la sécurité DNS sur le trafic TLS (reportez-vous aux meilleures pratiques de déchiffrement pour plus d’informations). Lorsque la sécurité DNS sur le trafic TLS est déchiffrée, les requêtes DNS résultantes dans les journaux apparaissent comme des applications conventionnelles **base DNS**.

STEP 4 | (Facultatif) Recherchez une activité sur le pare-feu pour les requêtes DNS chiffrées-TLS déchiffrées qui ont été traitées à l’aide de la sécurité DNS.

1. Sélectionnez **Activité** > **Visionneuse de journaux** et sélectionnez les journaux des **Menaces**. Utilisez le générateur de requêtes pour filtrer en fonction de l’application à l’aide de **base DNS** et le port 853 (qui est exclusivement utilisé pour la sécurité DNS sur les transactions TLS), par exemple, `app = 'dns-base' ET source_port = 853`.
2. Sélectionnez une entrée de journal pour afficher les détails de la menace DNS détectée.

3. L’**application** devrait afficher la**base DNS** dans le volet **Généralités** et le **Port** dans le volet**Source** de la vue détaillée du journal. D’autres détails pertinents sur la menace sont affichés dans les onglets correspondants.

Configuration de la sécurité DNS sur TLS (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | Connectez-vous au NGFW.

STEP 2 | Activation de la sécurité DNS est configuré pour inspecter les requêtes DNS. Vous pouvez utiliser votre profil de sécurité existant si vous souhaitez utiliser les mêmes paramètres des **politiques DNS** pour la sécurité DNS sur le trafic TLS.

STEP 3 | Créez une règle de politique de déchiffrement (similaire à l’exemple ci-dessous) avec une action de déchiffrement du trafic HTTPS sur le port 853, qui inclut la sécurité DNS sur le trafic TLS (reportez-vous à la section Meilleures pratiques de déchiffrement pour plus d’informations). Lorsque la sécurité DNS sur le trafic TLS est déchiffrée, les requêtes DNS résultantes dans les journaux apparaissent comme des applications conventionnelles **base DNS**.

		Source				Destination					Decrypt Options				
	NAME	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE
1	Decrypt Port 853	any	any	any	any	any	any	any	any	Port 853	decrypt	ssl-forward-proxy	default	none	false

STEP 4 | (Facultatif) Recherchez une activité sur le pare-feu pour les requêtes DNS chiffrées-TLS déchiffrées qui ont été traitées à l’aide de la sécurité DNS.

1. Sélectionnez **Moniteur** > **Journaux** > **Trafic** et filtrez en fonction de l’application à l’aide de **base DNS** et le port 853 (qui est exclusivement utilisé pour la sécurité DNS sur les transactions TLS), par exemple, `( app eq dns-base ) et ( port.src eq 853 )`.
2. Sélectionnez une entrée de journal pour afficher les détails d’une menace DNS détectée.
3. L’**application** devrait afficher la**base DNS** dans le volet **Généralités** et le **Port** dans le volet**Source** de la vue détaillée du journal. D’autres détails pertinents sur la menace sont affichés dans les fenêtres correspondantes.

Configuration de la sécurité DNS sur DoH

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence avancée de prévention des menaces ou de prévention des menaces

Vous pouvez analyser et catégoriser la charge utile DNS contenue dans les demandes de trafic DNS chiffrées vers des hôtes DNS à l’aide de HTTPS (DoH—[DNS sur HTTPS]). Si votre organisation bloque actuellement toutes les requêtes DoH comme le recommande Palo Alto Networks, vous pouvez abandonner cette politique, car la sécurité DNS vous permet désormais d’extraire le nom d’hôte DNS de la demande chiffrée et d’appliquer les stratégies de sécurité DNS existantes de votre organisation. Cela vous permet d’accéder en toute sécurité à davantage de sites Web à mesure que la prise en charge du DoH s’étend. La prise en charge de la sécurité DNS pour DoH est activée par la configuration du pare-feu pour déchiffrer la charge utile des requêtes DNS provenant d’une liste de résolveurs DNS spécifiée par l’utilisateur, ce qui permet de prendre en charge une gamme d’options de serveur. La charge utile DNS déchiffrée peut ensuite être traitée à l’aide de la configuration de profil antispyware contenant la configuration de votre stratégie DNS. Les requêtes DNS qui ont été déterminées comme étant DoH sont étiquetées comme **dns-sur-https** dans les journaux de trafic.

- Strata Cloud Manager
- PAN-OS 11.0 et versions ultérieures

Configuration de la sécurité DNS sur DoH (Strata Cloud Manager)

STEP 1 | Utilisez les informations d’identification associées à votre compte d’assistance Palo Alto Networks et connectez-vous au Strata Cloud Manager sur le hub https://apps.paloaltonetworks.com/.

STEP 2 | Créer une catégorie d’URL personnalisée liste qui inclut tous les résolveurs DoH à destination et en provenance desquels vous souhaitez activer le trafic (vous aurez besoin de la ou des URL du serveur DNS).

STEP 3 | Créer une règle de politique de déchiffrement qui fait référence à la liste de catégories d’URL personnalisée que vous avez créée à l’étape précédente.

STEP 4 | Mettez à jour ou créez un profil de sécurité antispyware utilisé pour inspecter les demandes DoH.

STEP 5 | Créez ou mettez à jour une règle de politique de sécurité et référencez un profil de sécurité DNS et une liste de catégories d’URL personnalisée (**Gérer** > **Configuration** > **PAN-OS et Prisma Access** > **Services de sécurité** > **Gestion de l’accès URL**) contenant la liste approuvée des serveurs DoH.

STEP 6 | Créer une politique de blocage pour déchiffrer le trafic HTTPS et bloquer tout le trafic DoH non approuvé restant qui n’est pas explicitement autorisé par la liste de catégories d’URL personnalisée (référencée à l’étape 5) à l’aide de l’identifiant de l’application : **dns-sur-https** et la catégorie d’URL suivante : **dns chiffré**.

Si vous disposez déjà d’une stratégie de blocage pour bloquer le trafic DoH, vérifiez que la règle est placée sous la règle de politique de sécurité précédente utilisée pour correspondre à des résolveurs DoH spécifiques répertoriés dans un objet de liste de catégories d’URL personnalisée.

STEP 7 | (Facultatif) Recherche d’activité sur le pare-feu pour les requêtes DNS chiffrées HTTPS qui ont été traitées à l’aide de la sécurité DNS.

1. Sélectionnez **Activité** > **Journaux** > **Visionneuse de journaux** et sélectionnez **Menace**.
2. Soumettez une requête de journal basée sur l’application, en utilisant **dns-sur-https**, par exemple, `app = 'dns-sur-https'`.
3. Sélectionnez une entrée de journal pour afficher les détails d’une menace DNS détectée qui utilise DoH.
4. La menace **Application** est affichée dans le volet **Général** de la vue journal détaillée. D’autres détails pertinents sur la menace sont affichés dans les fenêtres correspondantes.

Configurer la sécurité DNS sur DoH (PAN-OS 11.0 et versions ultérieures)

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

STEP 2 | Créer une catégorie d’URL personnalisée liste qui inclut tous les résolveurs DoH à destination et en provenance desquels vous souhaitez activer le trafic (vous aurez besoin de la ou des URL du serveur DNS).

STEP 3 | Créer une règle de politique de déchiffrement qui fait référence à la liste de catégories d’URL personnalisée que vous avez créée à l’étape précédente.

STEP 4 | Mettez à jour ou créez un profil de sécurité antispyware utilisé pour inspecter les demandes DoH.

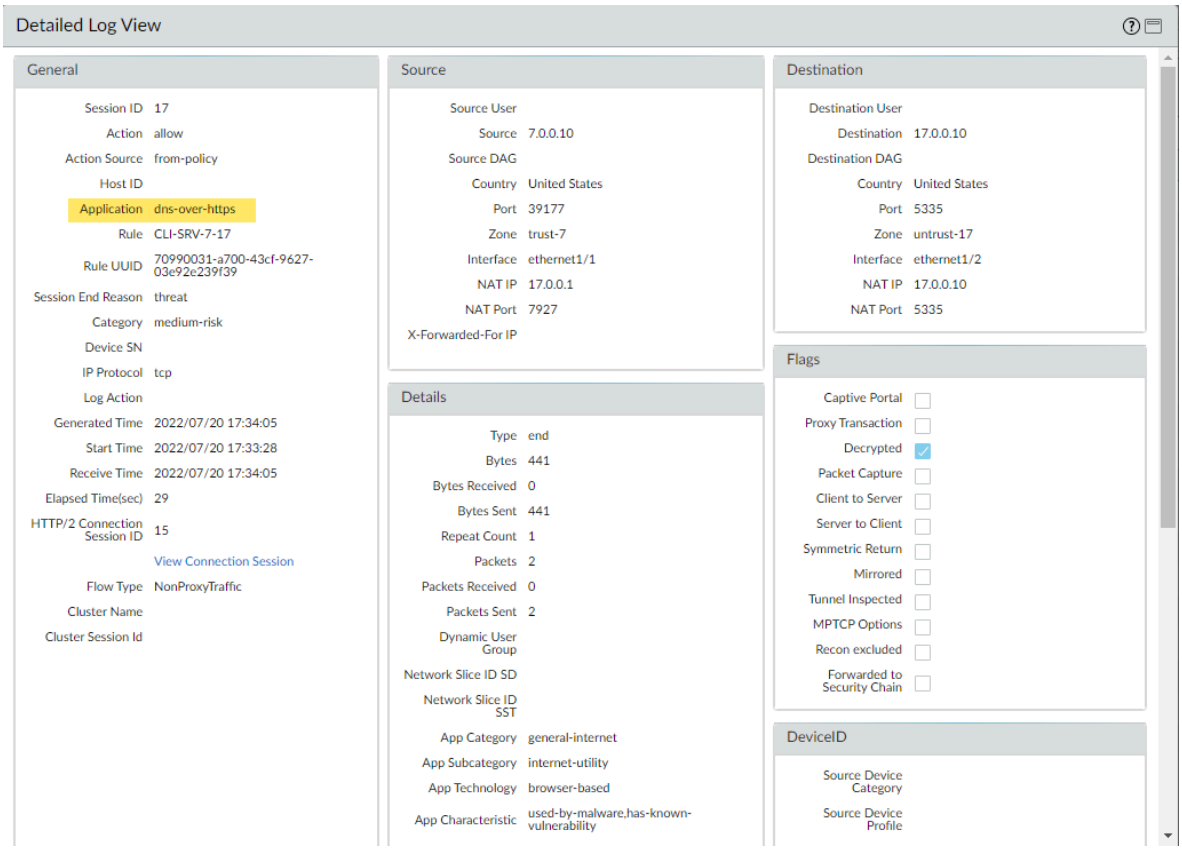
STEP 5 | Créer ou mettre à jour une règle de politique de sécurité et référencer un profil antispyware et une liste de catégories d’URL personnalisée (**Objets** > **Objets personnalisés** > **Catégorie d’URL**) contenant la liste approuvée des serveurs DoH.

STEP 6 | Créer une politique de blocage pour déchiffrer le trafic HTTPS et bloquer tout le trafic DoH non approuvé restant qui n’est pas explicitement autorisé par la liste de catégories d’URL personnalisée (référencée à l’étape 5) à l’aide de l’identifiant de l’application : **dns-sur-https** et la catégorie d’URL suivante : **dns chiffré**.

Si vous disposez déjà d’une stratégie de blocage pour bloquer le trafic DoH, vérifiez que la règle est placée sous la règle de politique de sécurité précédente utilisée pour correspondre à des résolveurs DoH spécifiques répertoriés dans un objet de liste de catégories d’URL personnalisée.

STEP 7 | (Facultatif) Recherchez une activité sur le pare-feu pour les requêtes DNS chiffrées en HTTPS qui ont été traitées à l’aide de la sécurité DNS.

1. Choisir **Moniteur** > **Journaux** > **Trafic** et filtrer en fonction de l’application à l’aide de **dns-sur-https**par exemple `(app eq dns-sur-https )`.
2. Sélectionnez une entrée de journal pour afficher les détails d’une menace DNS détectée.
3. L’**Application** devrait afficher dns-sur-https dans le volet**Généralités** de la vue détaillée du journal, indiquant qu’il s’agit du trafic DoH qui a été traité à l’aide de la sécurité DNS. D’autres détails pertinents sur la menace sont affichés dans les fenêtres correspondantes.



Création d’exceptions de domaine et des listes d’autorisation | de blocage

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence avancée de prévention des menaces ou de prévention des menaces

Sécurité DNS crée des signatures de menaces pour les domaines qui ont été analysés par le service de sécurité DNS. Pour ces domaines connus, les signatures sont référencées lorsqu’une requête DNS est reçue. Dans certains cas, il est possible que la signature ait classé à tort un domaine comme une menace, en raison de certaines caractéristiques ou qualités présentes dans le domaine. Dans de telles circonstances, vous pouvez ajouter des exceptions de signature pour contourner ces faux positifs. S’il existe des domaines sûrs connus classés comme malveillants, tels que des domaines internes, vous pouvez ajouter une liste de domaines qui contourneront toute analyse DNS. Si votre organisation utilise des flux de menaces tiers dans le cadre d’une solution complète de renseignement sur les menaces, vous pouvez également les référencer sous la forme de listes dynamiques externes (EDL) dans votre profil de sécurité DNS.

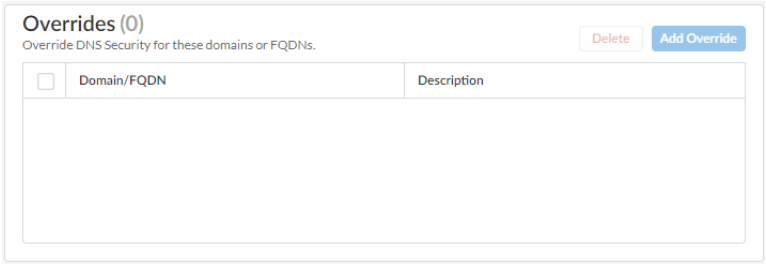
- Strata Cloud Manager
- PAN-OS et Panorama

Création d’exceptions de domaine et des listes d’autorisation | de blocage (Strata Cloud Manager)

STEP 1 | Utilisez les informations d’identification associées à votre compte d’assistance Palo Alto Networks et connectez-vous au Strata Cloud Manager sur le hub https://apps.paloaltonetworks.com/.

STEP 2 | Ajouter des remplacements de domaine dans les cas où des faux positifs se produisent.

1. Sélectionnez **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Sécurité DNS** et sélectionnez un profil de sécurité DNS à modifier.
2. **Ajoutez Remplacer** ou **Supprimer** pour modifier les entrées de la liste de domaines si nécessaire. Chaque entrée supplémentaire nécessite le domaine et une description.



3. Cliquez sur **OK** pour enregistrer votre profil de sécurité DNS modifié.

STEP 3 | Référencez une liste dynamique externe (EDL) dans le cadre de votre profil de sécurité DNS pour importer des flux de menaces tiers.

1. Créez une liste dynamique externe basée sur le domaine (**Gérer** > **Configuration** > **NGFW et Prisma Access** > **Objets** > **Listes dynamiques externes**). Pour plus d’informations sur les EDL, consultez Liste dynamique externe.
2. Sélectionnez **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Sécurité DNS**.
3. Dans le panneau **Listes dynamiques externes**, sélectionnez une liste de domaines EDL et fournissez les paramètres **Action de stratégie** et **Capture de paquets**. Dans **Appliquer aux profils**, sélectionnez le profil de sécurité DNS pour lequel vous souhaitez que la liste de domaines EDL s’applique.
4. **Enregistrez** vos modifications lorsque vous avez terminé de faire vos mises à jour.

Création d’exceptions de domaine et des listes d’autorisation | de blocage (NGFW (Managed by PAN-OS or Panorama))

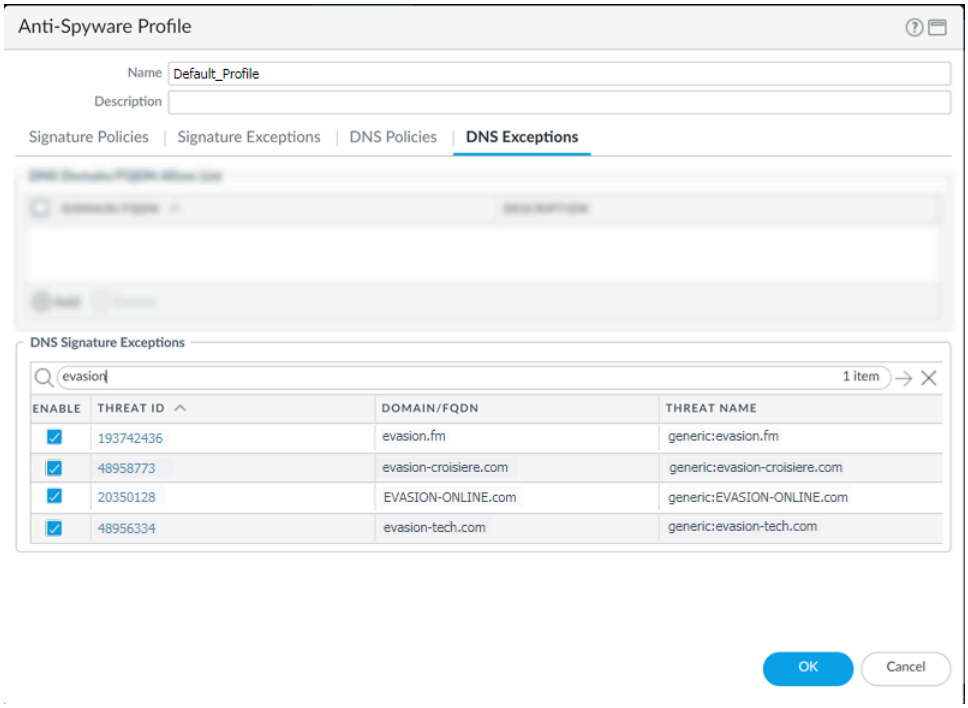
PAN-OS 10.0 et versions ultérieures fournissent une option supplémentaire pour ajouter explicitement des domaines autorisés via le profil de sécurité antispyware. Vous pouvez ajouter des entrées de domaine/FQDN pour les sources de domaine approuvées si elles déclenchent une réponse faux positif de la sécurité DNS.

- PAN-OS 10.0.x et versions ultérieures
- PAN-OS 9.1

Création d’exceptions de domaine et de listes d’autorisation | de blocage (PAN-OS 10.0 et versions ultérieures)

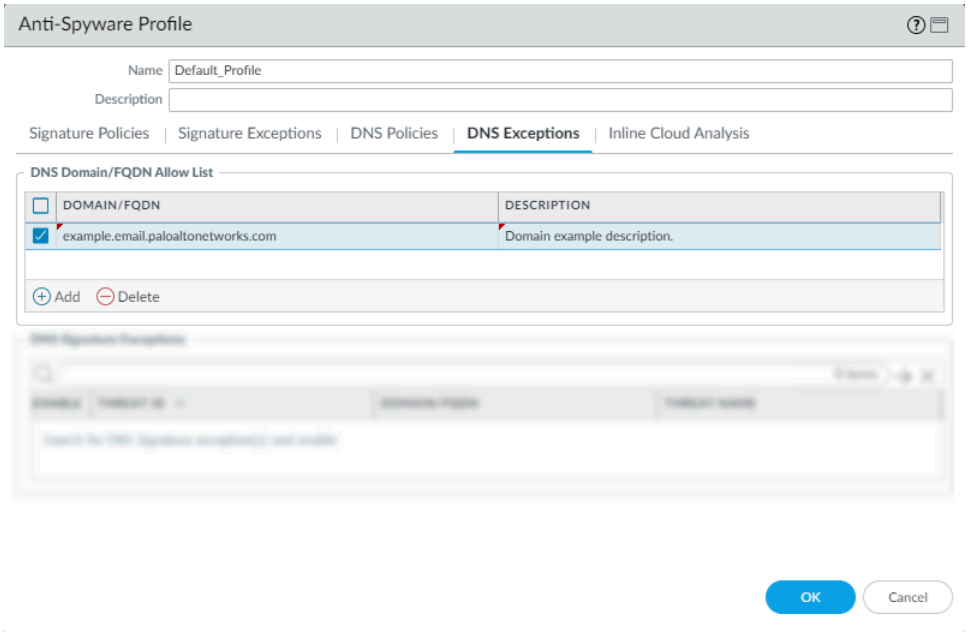
- Connectez-vous au NGFW.

- Ajoutez des exceptions de signature de domaine dans les cas où des faux positifs se produisent.
  1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
  2. Sélectionnez un profil à modifier.
  3. **Add (Ajoutez)** ou modifiez le profil antispyware duquel vous souhaitez exclure la signature de menaces, puis sélectionnez **DNS Exceptions (Exceptions de DNS)**.
  4. Cherchez une signature DNS à exclure en entrant le nom ou le FQDN.
  5. Sélectionnez la case à cocher pour chaque **ID de menace** de la signature DNS que vous souhaitez exclure de l’application.



  6. Cliquez sur **OK (OK)** pour enregistrer votre profil antispyware, qu'il soit nouveau ou modifié.

- Ajoutez une liste d’autorisation pour spécifier une liste de domaines DNS/FQDN qui doivent être explicitement autorisés.
  1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
  2. Sélectionnez un profil à modifier.
  3. **Add (Ajoutez)** ou modifiez le profil antispyware duquel vous souhaitez exclure la signature de menaces, puis sélectionnez **DNS Exceptions (Exceptions de DNS)**.
  4. Pour **Add (Ajouter)** une nouvelle entrée de liste d’autorisation FQDN, fournissez le domaine DNS ou l’emplacement FQDN et une description.



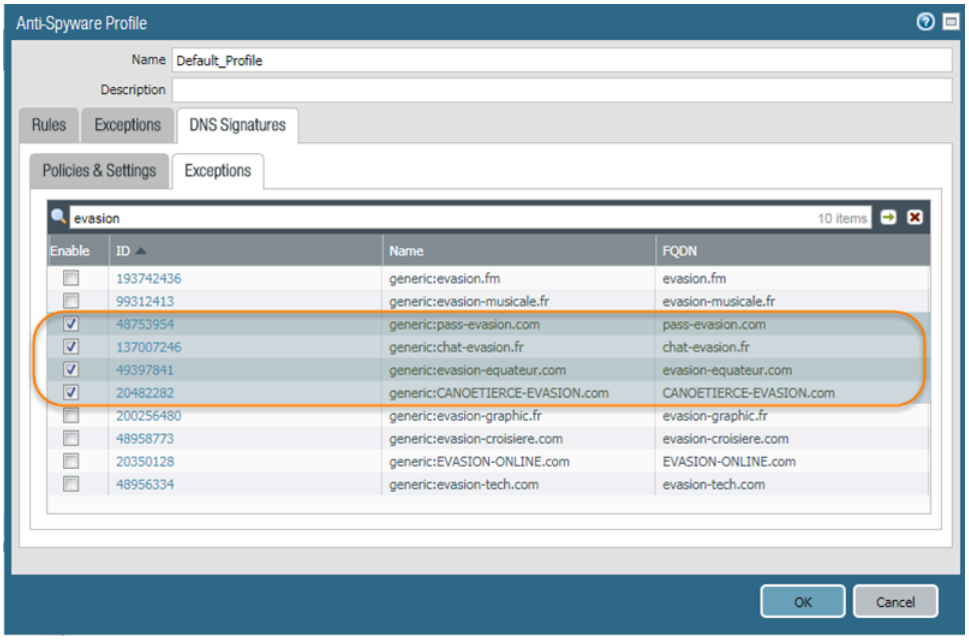
  5. Cliquez sur **OK (OK)** pour enregistrer votre profil antispyware, qu'il soit nouveau ou modifié.

Création d’exceptions de domaine et listes d’autorisation | de blocage (PAN-OS 9.1)

Les listes d’autorisation et de blocage ne sont pas disponibles dans PAN-OS 9.1.

- Connectez-vous au NGFW.

- Ajoutez des exceptions de signature de domaine dans les cas où des faux positifs se produisent.
  1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
  2. Sélectionnez un profil à modifier.
  3. **Add (Ajoutez)** ou modifiez le profil antivirus duquel vous souhaitez exclure la signature de menaces, puis sélectionnez **DNS Signatures (Signatures DNS) > Exceptions**.
  4. Cherchez une signature DNS à exclure en entrant le nom ou le FQDN.
  5. Sélectionnez le **ID menace DNS** pour la signature DNS que vous souhaitez exclure de l’application.



  6. Cliquez sur **OK (OK)** pour enregistrer votre profil antispyware, qu'il soit nouveau ou modifié.

Domaines de test

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention avancée des menaces ou de prévention des menaces

Palo Alto Networks fournit les domaines de test de sécurité DNS suivants pour valider la configuration de votre politique en fonction de la catégorie DNS.

STEP 1 | Accédez aux domaines d’essai suivants pour vérifier que l’action de la politique pour un type de menace donné est appliquée :

Sécurité DNS

- C2 : test-c2.testpanw.com
- DNS Tunneling : test-dnstun.testpanw.com
- DGA : test-dga.testpanw.com
- Dynamic DNS : test-ddns.testpanw.com
- Malware : test-malware.testpanw.com
- Domaines récemment enregistrés* : test-nrd.testpanw.com
- Hameçonnage* : test-phishing.testpanw.com
- Logiciel indésirable* : test-grayware.testpanw.com
- Domaine en parking* : test-parked.testpanw.com
- Contournement de proxy et anonymiseurs* : test-proxy.testpanw.com
- Flux rapide*—test-fastflux.testpanw.com
- NRD malveillant*—test-malicious-nrd.testpanw.com
- Attaque NXNS*—test-nxns.testpanw.com
- Suspendu*—test-dangling-domain.testpanw.com
- Reliaison DNS*—test-dns-rebinding.testpanw.com
- Infiltration DNS*—test-dns-infiltration.testpanw.com
- Abus de joker*—test-wildcard-abuse.testpanw.com
- Stratégiquement âgé*—test-strategically-aged.testpanw.com
- DNS compromis*—test-compromised-dns.testpanw.com
- Suivi publicitaire*—test-adtracking.testpanw.com
- Camouflage CNAME*—test-cname-cloaking.testpanw.com
- Rançongiciel*—test-ransomware.testpanw.com
- Stock*—test-stockpile-domain.testpanw.com
- Cybersquattage*—test-squatting.testpanw.com
- Réputation du sous-domaine*—test-subdomain-reputation.testpanw.com

*Les domaines de test marqués d’un * ne sont pas pris en charge dans PAN-OS 9.1.*

Sécurité DNS avancée

Accédez au domaine de test suivant pour vérifier que l’action de la politique pour un type de menace donné est appliquée :

- **Domaine de mauvaise configuration DNS** (Réclamable)—http://test-dnsmisconfig-claimable-nx.testpanw.com

Les cas de test de domaine de test suivants doivent être ajoutés à votre fichier de zone de serveur DNS de testpanw.com avant d’accéder au domaine. Ces cas de test correspondent aux signatures de sécurité DNS avancée et génèrent les journaux appropriés. Vérifiez que l’action de stratégie pour un type de menace donné est appliquée.

Table 1: Cas de test de domaine de mauvaise configuration DNS (zone suspendue)

Hôte	Type d’enregistre	Enregistrer les données
*.test-dnsmisconfig-zone-dangling.testpanw.com	A	1.2.3.4

Table 2: Détournement des cas de test de domaine

Hôte	Type d’enregistre	Enregistrer les données
test-ipv4.hijacking.testpanw.com	A	1.2.3.5
*.test-ipv4-wildcard.hijacking.testpanw.com	A	1.2.3.6
test-ipv6.hijacking.testpanw.com	AAAA	2607:f8b0:4005:80d::2005
test-cname-rrname.hijacking.testpanw.com	CNAME	1.test-cname-wc.hijacking.testpanw.com
test-cname-rrname-wc.hijacking.testpanw.com	CNAME	1.test-cname-wildcard-1.hijacking.testpanw.com
*.test-cname-rrname-sub-wc.hijacking.testpanw.com	CNAME	2.test-cname-wc.hijacking.testpanw.com
test-ns-rrname.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-ns-rrname-rdata-wc.hijacking.testpanw.com	NS	1.test-ns-wc.hijacking.testpanw.com
1.test-ns-rrname-sub-wc.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-rrname-wc.hijacking.testpanw.com	NS	test-ns-2.hijacking.testpanw.com

*Pour les enregistrements NS, vous devez utiliser l’option suivante :**dig +trace NS**"*

STEP 2 | Vérifiez que la demande de requête DNS a été traitée par la sécurité DNS en surveillant l’activité.

Test de la connectivité aux services cloud de la sécurité DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence avancée de prévention des menaces ou de prévention des menaces

Sécurité DNS

Vérifiez la connectivité de votre pare-feu avec le service de sécurité DNS. Si vous ne pouvez pas accéder au service, vérifiez que le domaine suivant n'est pas bloqué : dns.service.paloaltonetworks.com.

STEP 1 | Accédez à la CLI du pare-feu.

STEP 2 | Utilisez la commande CLI suivante pour vérifier la disponibilité de la connexion de votre pare-feu au service de sécurité DNS.

```
show dns-proxy dns-signature info
```

Par exemple :

```
afficher les informations de signature DNS du proxy DNS URL du
 cloud : dns.service.paloaltonetworks.com:443 URL de télémétrie :
 io.dns.service.paloaltonetworks.com:443 Dernier résultat : Aucune
 Adresse du dernier serveur : Échange de paramètres : Intervalle
 300 s Autoriser l'actualisation de la liste : Intervalle 43200
 s Requête en attente de transmission : 0 Demande en attente de
 réponse : 0 Taille du cache : 0
```

Si votre pare-feu a une connexion active au service de sécurité DNS, les détails du serveur s’affichent dans la sortie de réponse.

STEP 3 | Récupérez les détails des transactions d’un domaine spécifique, tels que la latence, le TTL et la catégorie de signature.

Pour revoir les détails d’un domaine, servez-vous de la commande CLI suivante sur le pare-feu :

```
test dns-proxy dns-signature fqdn
```

Par exemple :

```
test dns-proxy dns-signature fqdn www.yahoo.com Requête de
 signature DNS [ www.yahoo.com ] Terminée en 178 ms Entrées
 de réponse de signature DNS : 2 Domain Category GTID TTL
```

```
 ------------------------------------------------------------------------------
 *.yahoo.com Benign 0 86400 www.yahoo.com Benign 0 3600
```

Sécurité DNS avancée

Vérifiez la connectivité de votre pare-feu avec le service de sécurité DNS avancée. Si vous ne pouvez pas accéder au service, vérifiez que le domaine suivant n’est pas bloqué : dns.service.paloaltonetworks.com. Si vous avez configuré manuellement un serveur régional de sécurité DNS avancée, vous devrez peut-être vérifier que le domaine régional spécifique est également débloqué.

Vérifiez l’état de la connectivité de votre pare-feu au service cloud de sécurité DNS avancée.

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

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

Par exemple :

```
show ctd-agent status security-client ... Client
 de sécurité ADNS(1) Serveur cloud actuel : qa.adv-
dns.service.paloaltonetworks.com :443 Connexion cloud : config.
 connecté : Nombre de connexions gRPC : 2, Nombre de travailleurs :
 8 Niveau de débogage : 2, Connexion non sécurisée : false, Cert
 valide : true, Clé valide: true, Nombre CA : 306 Nombre maximum
 de travailleurs : 12 Nombre maximum de sessions qu’un travailleur
 doit traiter avant de se reconnecter : 10240 Nombre maximum
 de messages par travailleur : 0 Skip cert verify: false Grpc
 Statut de la connexion : État prêt (3), last err rpc : code =
 Unavailable desc = code d’état HTTP inattendu reçu du serveur :
 502 (Bad Gateway) ; transport : reçu type de contenu inattendu
 "text/html" État du pool : Prêt (2) dernière mise à jour :
 2024-01-24 11:15:00.549591469 -0800 PST m=+1197474.129493596
 dernier nouvel essai de connexion : 2024-01-23 00:03:09.093756623
 -0800 PST m=+1070762.673658768 dernier pool fermé : 2024-01-22
 14:15:50.36062031 -0800 PST m=+1035523.940522446 Security
 Client AdnsTelemetry(2) Serveur cloud actuel : io-qa.adv-
dns.service.paloaltonetworks.com:443 Connexion cloud : config.
 connecté : Nombre de connexions gRPC : 2, Nombre de travailleurs :
 8 Niveau de débogage : 2, Connexion non sécurisée : false, Cert
 valide : true, Clé valide: true, Nombre CA : 306 Nombre maximum
 de travailleurs : 12 Nombre maximum de sessions qu’un travailleur
 doit traiter avant de se reconnecter : 10240 Nombre maximum de
 messages par travailleur : 0 Skip cert verify: false Grpc Statut
 de la connexion : État prêt (3), last err rpc error : code =
 Internal desc = flux terminé par RST_STREAM avec code erreur :
 PROTOCOL_ERROR État du pool : Prêt (2) dernière mise à jour :
 2024-01-24 11:25:58.340198656 -0800 PST m=+1198131.920100772
 dernier nouvel essai de connexion : 2024-01-23 00:03:36.78141425
 -0800 PST m=+1070790.361316421 dernier pool fermé : 2024-01-22
 14:24:26.954340157 -0800 PST m=+1036040.534242289 ...
```

Vérifiez que l’état de la connexion cloud pour `Security Client AdnsTelemetry(2)` et `Security Client ADNS(1)` affiche des connexions actives.

Sortie CLI raccourcie pour plus de brièveté.

Si vous ne parvenez pas à vous connecter au service cloud de sécurité DNS avancée, vérifiez que le serveur DNS avancé n’est pas bloqué : dns.service.paloaltonetworks.com.

Configuration du délai d’expiration de la recherche

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence avancée de prévention des menaces ou de prévention des menaces

Sécurité DNS

Si le pare-feu n’arrive pas à extraire un verdict de signature dans le temps alloué dû à des problèmes de connectivité, la requête et toutes les réponses DNS suivantes sont autorisées. Vous pouvez vérifier la latence moyenne pour vérifier que les requêtes se situent dans la période configurée Si la latence moyenne excède la période configurée, considérez à mettre à jour la valeur avec une valeur plus haute que la latence moyenne afin de prévenir les expirations de requêtes

STEP 1 | Avec la CLI, tapez la commande suivante pour voir la latence moyenne

```
show dns-proxy dns-signature counters
```

Le délai d’expiration par défaut est 100 secondes.

STEP 2 | Faites défiler vers le bas vers la section de la latence sous l’en-tête API de la requête et vérifiez que la latence moyenne se situe dans l’intervalle d’expiration défini Cette latence indique le temps qu’il faut, en moyenne, pour récupérer un verdict de signatures du service de sécurité DNS Des statistiques de latence additionnelles pour différentes périodes de latence peuvent être trouvées sous les moyennes

```
demande signature API: . . . [latence ] : max 1870 (ms) min 16(ms)
 moy 27(ms) 50 ou moins 47246 100 ou moins : 113 200 ou moins : 25
 400 ou moins : 15 autres : 21
```

STEP 3 | Si la latence moyenne est constamment au dessus de la valeur par défaut d’expiration, vous pouvez augmenter cette valeur afin que les requêtes se situent dans un intervalle donné Sélectionnez **Device (Périphérique) > Content-ID (ID de contenu)** et mettez à jour le paramètres **Realtime Signature Lookup (Recherche de signature en temps réel)**.

STEP 4 | Commit (Validez) les modifications.

Sécurité DNS avancée

STEP 1 | Affichez l’enregistrement des temps aller-retour (en millisecondes) pour les requêtes de sécurité DNS avancée à l’aide de la commande CLI de débogage suivante. Ceux-ci sont répartis en tranches

de latence allant de 0 ms à 450 ms. Vous pouvez l’utiliser pour déterminer le paramètre de latence maximale idéal pour votre NGFW.

```
admin@PA-VM débogage du plan de données afficher les statistiques
 de fonctionnalités avancées ctd
```

Dans la sortie de réponse, naviguez jusqu’à la section `PAN_CTDF_DETECT_SERVICE_ADNS`.

```
PAN_CTDF_DETECT_SERVICE_ADNS cli_timeout : 1 req_total: 2
 req_timed_out: 0 Hold: adns rtt>=0ms: 0 adns rtt>=50ms: 2
 adns rtt>=100ms: 0 adns rtt>=150ms: 0 adns rtt>=200ms: 0
 adns rtt>=250ms: 0 adns rtt>=300ms: 0 adns rtt>=350ms: 0 adns
 rtt>=400ms: 0 adns rtt>=450ms: 0
```

STEP 2 | Configurez le paramètre de délai d’expiration maximal de la recherche de signature DNS avancée. Lorsque cette valeur est dépassée, la réponse DNS passe sans effectuer d’analyse à l’aide de la sécurité DNS avancée. Les signatures DNS (et leurs politiques associées) qui sont fournies via des mises à jour de contenu régulières ou qui font partie de listes dynamiques externes (EDL) configurées ou d’exceptions DNS sont toujours appliquées.

1. Sélectionnez **Périphérique** > **Configuration** > **ID contenu** > **Sécurité DNS avancée**.
2. Spécifiez un paramètre mis à jour de délai d’expiration maximal de recherche de signature DNS avancée en millisecondes. La valeur par défaut est de 100 ms et constitue le paramètre recommandé.
3. Cliquez sur **OK** pour confirmer vos modifications.

Vous pouvez également utiliser la commande CLI suivante pour configurer la valeur du délai d’expiration de la sécurité DNS avancée. Vous pouvez définir une valeur de 100 à 15 000 ms par incréments de 100 ms. La valeur par défaut est de 100 ms et constitue le paramètre recommandé.

```
admin@PA-VM#définir le paramètre deviceconfig paramètre adns
 latence maximale <timeout_value_in_milliseconds>
```

Par exemple :

```
admin@PA-VM# définir le paramètre deviceconfig paramètre adns
 latence maximale 500
```

Vous pouvez vérifier la configuration actuelle du délai d’expiration à l’aide de la commande CLI suivante (reportez-vous à l’entrée de **`latence maximale`** de la sortie).

```
admin@PA-VM afficher le modèle poussé de configuration
 ... } deviceconfig { setting { dns { dns-cloud-server dns-
qa.service.paloaltonetworks.com; } adns-setting { max-latency
 100; } } } ...
```


Contourner les services d’abonnement à la sécurité DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention avancée des menaces ou de prévention des menaces

Les requêtes de sécurité DNS peuvent être contournées dans les cas où des problèmes de latence ou d’autres problèmes de réseau sont présents.

Dans les cas où des faux positifs se produisent, Palo Alto Networks recommande de créer des exceptions spécifiques au lieu de contourner les requêtes de sécurité DNS.

- Gestion du cloud
- PAN-OS et Panorama

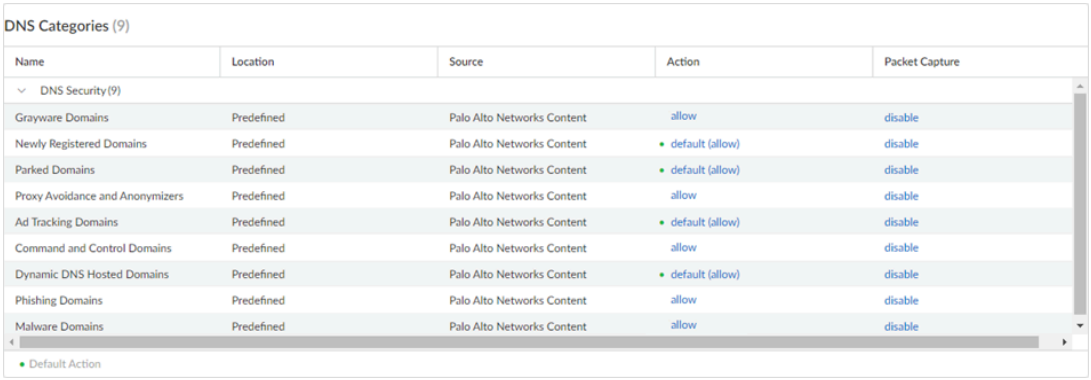
Contourner les services d’abonnement à la sécurité DNS (Strata Cloud Manager)

STEP 1 | Utilisez les informations d’identification associées à votre compte d’assistance Palo Alto Networks et connectez-vous au Strata Cloud Manager sur le hub https://apps.paloaltonetworks.com/.

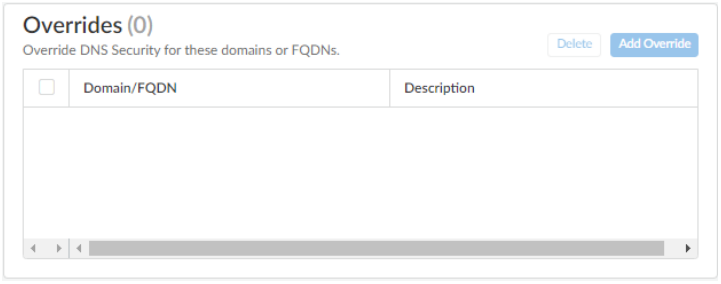
STEP 2 | Accédez à **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Sécurité DNS** et sélectionnez le profil de sécurité DNS approprié.

STEP 3 | Configurez les paramètres de la stratégie de signature de sécurité DNS pour contourner les requêtes de sécurité DNS. Pour chaque catégorie DNS, définissez l’**action** sur **autoriser** et **la capture de**

paquets sur **désactivé**. Dans ce qui suit, les catégories de sécurité DNS ont été configurées pour contourner les requêtes de sécurité DNS.



STEP 4 | Dans la section **Remplacements**, vérifiez qu’aucune entrée n’est présente ; si nécessaire, supprimez tous les remplacements **de domaine/FQDN**.



STEP 5 | Cliquez sur **OK** pour enregistrer le profil de sécurité DNS.

Contourner les services d’abonnement à la sécurité DNS (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 et versions ultérieures prend en charge les sources de signature DNS configurables individuellement, ce qui vous permet de définir des actions de politique distinctes ainsi qu’un niveau de gravité du journal pour une source de signature donnée. Vous devez pour ce faire configurer à la fois l’action de stratégie et la gravité des journaux pour chaque source de signature DNS disponible afin de contourner la sécurité DNS. En outre, vous devez également supprimer les entrées d’exceptions DNS pour que la sécurité DNS soit entièrement contournée. Sur PAN-OS 9.1, vous pouvez simplement définir l’action de stratégie pour la sécurité DNS de Palo Alto Networks sur une action autoriser.

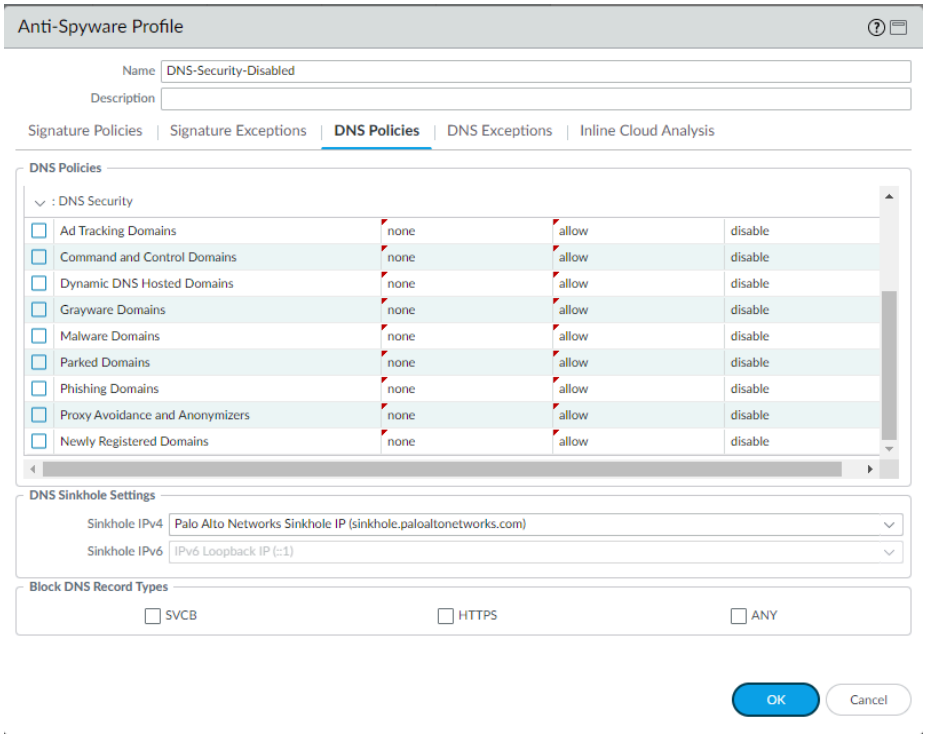
- PAN-OS 10.0.x et versions ultérieures
- PAN-OS 9.1

Contourner les services d’abonnement de sécurité DNS (PAN-OS 10.0 et versions ultérieures)

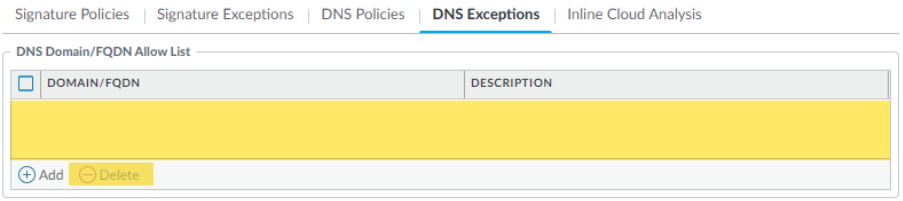
STEP 1 | Connectez-vous au NGFW.

STEP 2 | Configurez les paramètres de la stratégie de signature de sécurité DNS pour contourner les requêtes de sécurité DNS.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Sélectionnez le profil contenant vos paramètres de politique de sécurité DNS actifs.
3. Sélectionnez l’onglet **DNS Policies (Politiques de DNS)**.
4. Pour chaque catégorie DNS, définissez la gravité des journaux sur **aucune**, l’action de stratégie sur **autoriser**et la capture de paquets sur **désactiver**. Dans ce qui suit, les catégories de sécurité DNS ont été configurées pour contourner les requêtes de sécurité DNS.



STEP 3 | Sélectionnez **Exceptions DNS** et supprimez toutes les entrées **de Domaine DNS/Liste d’autorisations FQDN**.



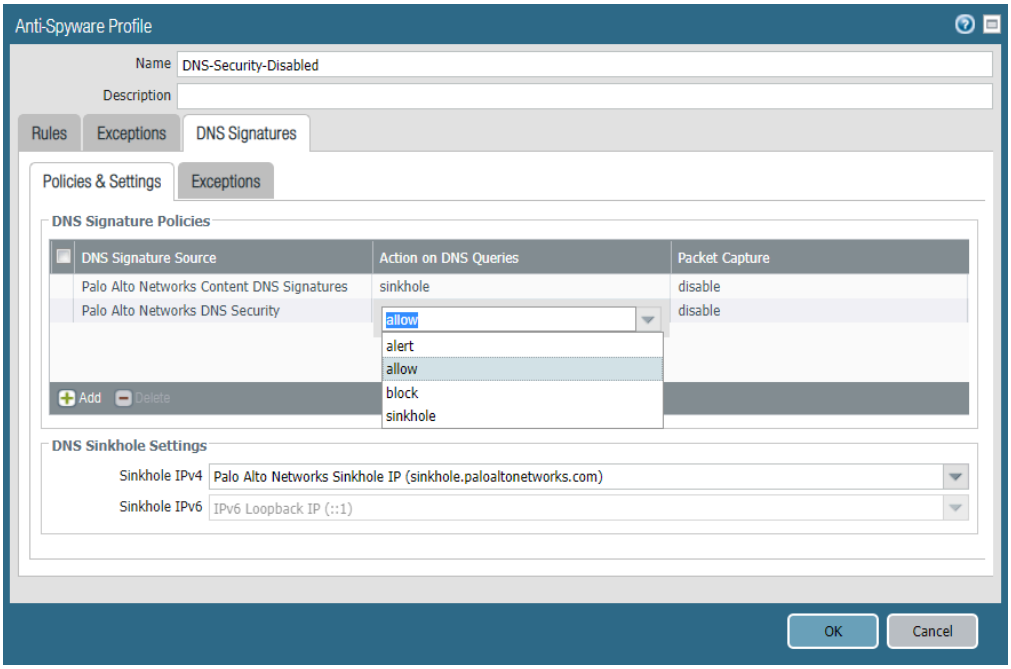
STEP 4 | Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.

Contourner les services d’abonnement à la sécurité DNS (PAN-OS 9.1)

STEP 1 | Connectez-vous au NGFW.

STEP 2 | Configurez les paramètres de la stratégie de signature de sécurité DNS pour contourner les recherches de sécurité DNS.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Sélectionnez le profil contenant vos paramètres de politique de sécurité DNS actifs.
3. Sélectionnez l’onglet **Signatures DNS**.
4. Sous **Politiques et paramètres**, définissez l’action de politique pour **la sécurité DNS de Palo Alto Networks** sur une action **autorisation**.



STEP 3 | Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.

Surveillance des services d’abonnement à la sécurité DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention avancée des menaces ou de prévention des menaces

Palo Alto Networks fournit plusieurs options pour surveiller les activités de sécurité DNS et de sécurité DNS avancée afin de permettre la recherche de renseignements pour une gamme de produits qui reposent sur les services d’abonnement de sécurité DNS et les données de trafic associées. Selon la plate-forme du produit, vous pouvez accéder à des tableaux de bord de haut niveau qui fournissent des statistiques sur les requêtes DNS et les tendances d’utilisation, y compris le contexte dans l’activité du réseau, à des détails spécifiques sur les requêtes DNS d’utilisateurs spécifiques sous forme de données de journalisation.

Vous pouvez également visualiser la façon dont les services d’abonnement de sécurité DNS s’intègrent aux autres applications et services de sécurité de Palo Alto Networks pour protéger votre organisation 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.

Pour plus de détails sur les opérations de service d’abonnement de sécurité DNS, le tableau de bord fournit une vue sur vos réseaux de données de requête DNS ainsi que la possibilité d’approfondir les diverses tendances DNS. Chaque carte de tableau de bord offre une vue unique sur la façon dont les requêtes et les réponses DNS sont traitées et classées dans un format de rapport graphique. Cela vous permet d’obtenir, en un coup d’œil, une vue de haut niveau des statistiques d’utilisation DNS de votre organisation. Cela fournit également une liste des domaines mal configurés et des domaines détournés détectés par le service de sécurité DNS avancée, ce qui vous permet de corriger toute erreur de configuration DNS. Les domaines mal configurés sont basés sur les entrées de domaine parent publiques ajoutées à la liste **Erreurs de configuration de la zone DNS**.

Vous pouvez également afficher les journaux générés automatiquement lorsque les requêtes DNS sont traitées. Ces fichiers d’événements sont horodatés et fournissent une piste d’audit lorsqu’ils sont configurés pour le faire, en fonction de la configuration du journal de catégorie DNS. Les entrées du journal DNS peuvent contenir divers détails sur la requête DNS, y compris la nature de la menace DNS posée par le domaine associé, ainsi que les mesures prises lorsque la menace a été détectée.

Palo Alto Networks fournit plusieurs méthodes pour surveiller l’activité de la sécurité DNS en fonction de votre plateforme.

- Centre de commande Strata Cloud Manager
- Affichage du tableau de bord de la sécurité DNS
- Afficher les journaux de sécurité DNS pour les requêtes DNS qui ont transité par mon réseau

Affichage du tableau de bord de la sécurité DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention avancée des menaces ou de prévention des menaces

Le tableau de bord de sécurité DNS affiche les données statistiques générées par les services d’abonnement de sécurité DNS avancée et de sécurité DNS dans un rapport d’évaluation visuel rapide de l’utilisation DNS de votre organisation. Affichez et explorez en détail les différentes tendances DNS découvertes sur votre réseau. Chaque carte du tableau de bord fournit une vue unique sur la manière dont les requêtes DNS sont traitées et catégorisées. Sélectionnez des cartes de tableau de bord pour modifier le contexte du tableau de bord ou afficher plus d’informations sur une tendance, un domaine ou une statistique spécifique.

Le tableau de bord de sécurité DNS est disponible sur Prisma Access et AIOps pour NGFW. Vous pouvez interagir avec le Cartes de tableau de bord de la sécurité DNS pour modifier le contexte du tableau de bord ou afficher plus d’informations sur une tendance, un domaine ou une statistique spécifique. Vous pouvez également personnaliser la mise en forme pour afficher les tendances actuelles ou les données historiques, sur des points de données pertinents.

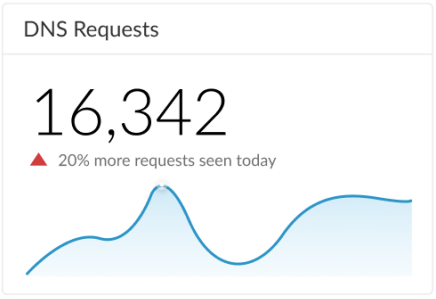
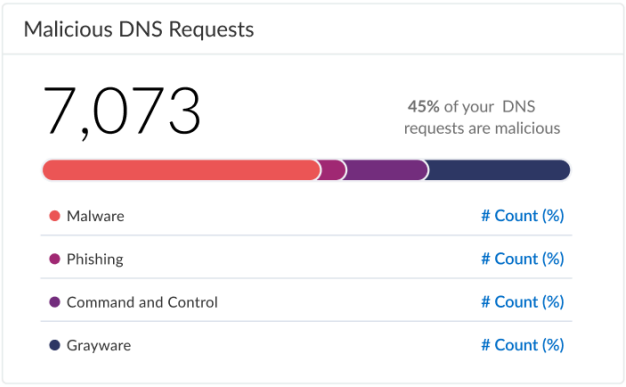
- Strata Cloud Manager
- AIOps pour NGFW gratuit

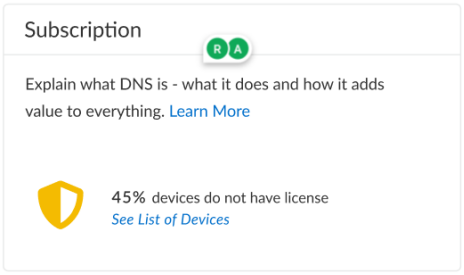
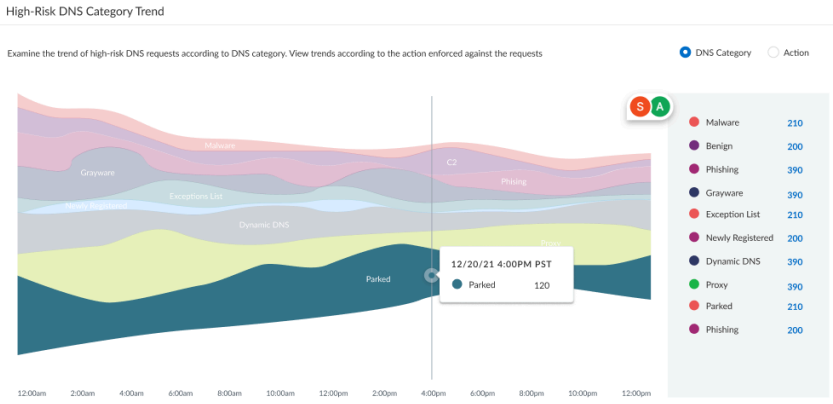
Cartes de tableau de bord de la sécurité DNS

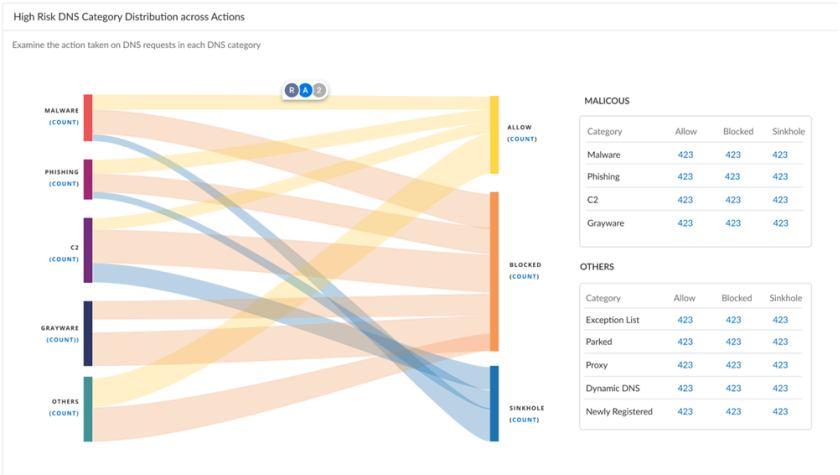
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention avancée des menaces ou de prévention des menaces

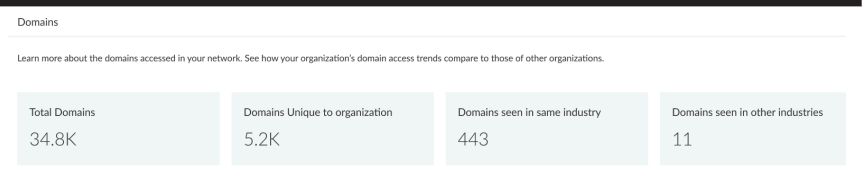
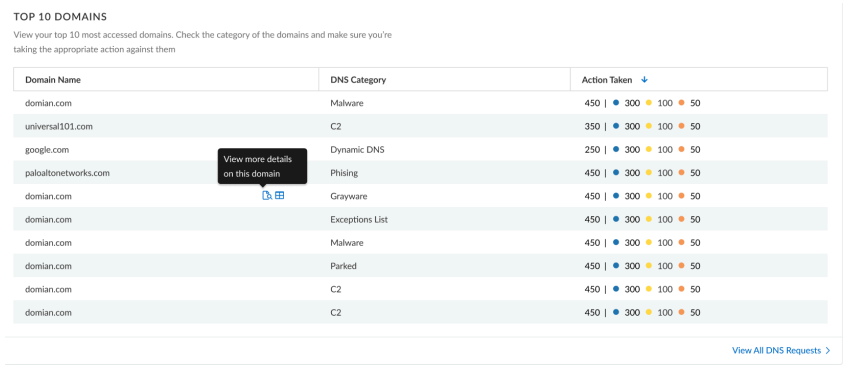
Les cartes qui peuplent le tableau de bord de sécurité DNS sont interactives et vous permettent d’afficher des détails supplémentaires ou de pivoter vers une liste de requêtes, d’événements et de domaines spécifiques, en ce qui concerne la façon dont le contenu est affiché.

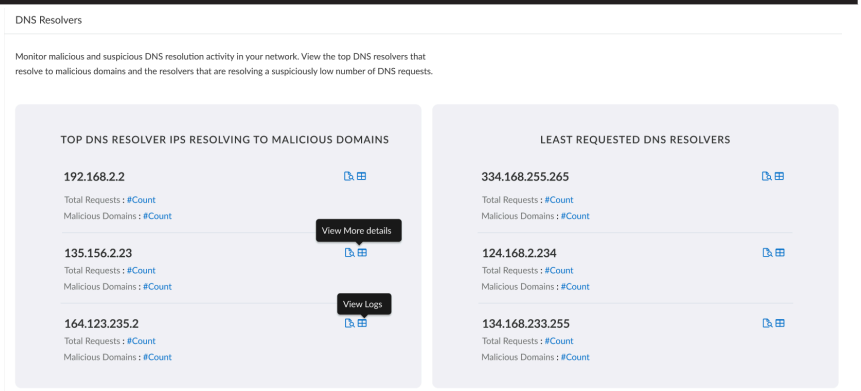
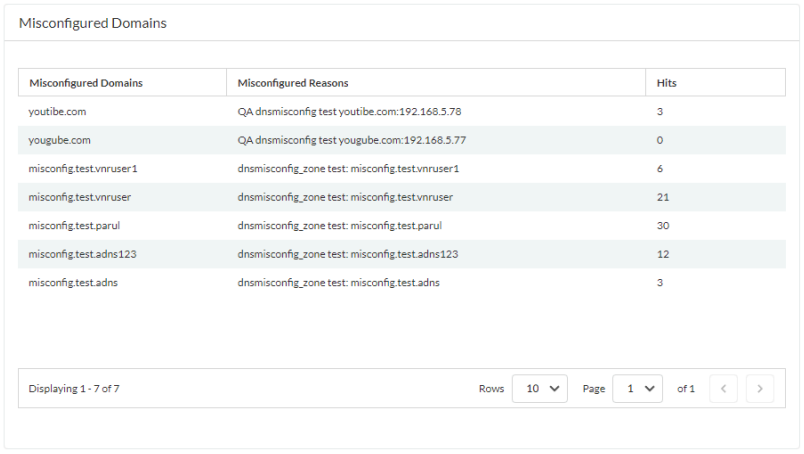
La liste suivante fournit une vue d’ensemble des cartes de tableau de bord de la sécurité DNS :

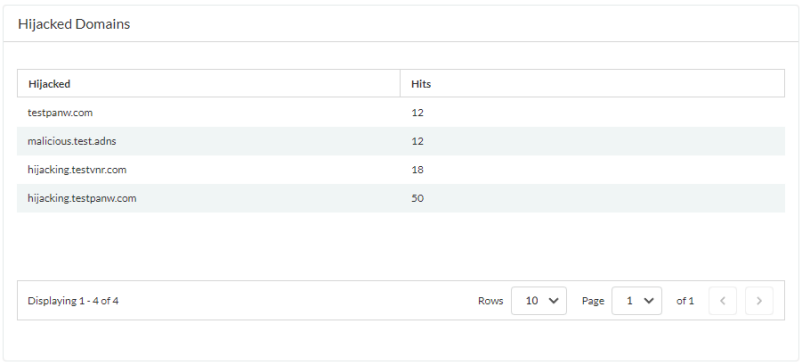
Nom de carte	Description
Requêtes DNS	Affiche le nombre total de requêtes DNS qui ont été traitées par la sécurité DNS.  • Le graphique linéaire schématise le nombre de requêtes DNS en fonction de la plage de temps définie par l’utilisateur. Spécifier une plage de temps personnalisée met à jour le graphique linéaire en conséquence. • La catégorie DNS et les filtres d’action ne modifient pas le contenu de la carte.
Requêtes DNS malveillantes	Affiche un graphique à barres empilées montrant les requêtes DNS qui ont été classées en fonction des types actuellement disponibles qui sont considérés comme malveillants. Le nombre total est indiqué en haut à gauche tandis qu’une ventilation des variables catégorielles est indiquée ci-dessous.  • Le graphique linéaire schématise le nombre de requêtes DNS en fonction de la plage de temps définie par l’utilisateur. Spécifier une plage de temps personnalisée met à jour le graphique linéaire en conséquence. • La catégorie DNS et les filtres d’action ne modifient pas le contenu de la carte.

Nom de carte	Description
Abonnement	Affiche le nombre de périphériques de votre réseau avec un abonnement de sécurité DNS actif. Un pourcentage des périphériques qui ne sont pas équipés de la sécurité DNS ou d’un abonnement écoulé est également affiché avec un lien vers une liste complète.  • Vous pouvez sélectionner **Voir une liste de périphériques** pour afficher une liste complète. • Cette carte montre un instantané de l’état actuel de l’abonnement - les options de filtre n’ont aucun impact.
Tendance des catégories DNS à risque élevé	Affiche un graphique de tendance montrant une ventilation des requêtes DNS basées sur la catégorie DNS ou de l’action appliquée à la requête DNS sur la plage de temps observable.  • Sélectionnez entre une catégorie DNS ou un graphique de tendances d’action à l’aide du bouton radio. • Survolez un segment du graphique vapeur représentant un type de données pour isoler et ouvrir une fenêtre contextuelle indiquant le nombre de requêtes DNS ou le type d’action effectué. • Spécifier une plage de temps personnalisée met à jour le graphique de tendance en conséquence. • La catégorie DNS et les filtres d’action soulignent la variable sélectionnée dans la carte, mais ne la suppriment pas du graphique.

Nom de carte	Description
Distribution des catégories DNS dans les actions	Affiche un organigramme qui fournit une visualisation des distributions des actions effectuées pour les catégories DNS à haut risque. Un tableau secondaire indique les mesures prises pour les catégories DNS moins prioritaires. • Survolez un flux spécifique pour ouvrir une fenêtre contextuelle indiquant le nombre d’actions effectuées du type spécifié. Spécifier une plage horaire personnalisée met à jour l’organigramme en conséquence. • La catégorie DNS et les filtres d’action ne modifient pas le contenu de la carte.  • La liste des domaines supérieurs est générée en fonction des paramètres de filtre appliqués en haut du tableau de bord. Les widgets qui affectent les paramètres généraux de la page déterminent également les domaines affichés. • Survolez une barre pour afficher les statistiques d’utilisation. • Cliquez sur un domaine pour afficher les détails de l’analyse DNS.
Domaines	Affiche le nombre de domaines vus dans votre réseau, au sein de votre secteur d’activité, d’autres secteurs d’activité, ainsi que le nombre total, sur la base de la catégorie DNS sélectionnée. Vous permet de comparer l’utilisation DNS de votre organisation à d’autres organisations du secteur ainsi qu’à des données collectées à l’échelle mondiale, y compris une liste de demandes de domaine trouvées exclusivement dans votre réseau.

Nom de carte	Description
	 • Les domaines répertoriés dans cette carte incluent toutes les catégories DNS indépendamment de la catégorie DNS et des filtres d’action. Seule la plage horaire met à jour le contenu de la carte.
Top 10 des domaines	Fournit une liste des 10 domaines les plus demandés de votre réseau avec la catégorie DNS et les mesures prises. Vous pouvez afficher plus de détails et les journaux pertinents pour un domaine en cliquant sur l’icône appropriée. Sélectionnez **Afficher toutes les demandes DNS** pour obtenir une liste complète des domaines auxquels vous avez accédé.  • Les domaines répertoriés dans cette carte incluent toutes les catégories DNS indépendamment de la catégorie DNS et des filtres d’action. Seule la plage horaire met à jour le contenu de la carte. • Cliquez sur un domaine pour afficher les détails de l’analyse DNS.
Résolveurs DNS	Fournit deux listes montrant les domaines malveillants les plus résolus et les domaines les moins résolus de votre réseau.

Nom de carte	Description
	 • Cliquez sur un résolveur DNS pour afficher les détails de l’analyse DNS.
Domaines présentant une erreur de configuration (sécurité DNS avancée)	Fournit une liste des domaines non résolvables associés au(x) domaine(s) parent(s) public(s) spécifié(s) par l’utilisateur. Pour chaque entrée, il y a une raison pour l’erreur de configuration et un nombre de correspondances de trafic basé sur l’IP source. 
Domaines détournés (sécurité DNS avancée)	Fournit une liste des domaines détournés tels que déterminés par la sécurité DNS avancée. Pour chaque entrée, il y a une raison de catégorisation et un nombre de correspondances de trafic basé sur l’IP source.

Nom de carte	Description
	

Affichage du tableau de bord de la sécurité DNS (Strata Cloud Manager)

STEP 1 | Utilisez les informations d’identification associées à votre compte d’assistance Palo Alto Networks et connectez-vous Strata Cloud Manager au hub.

STEP 2 | Sélectionnez **Tableaux de bord** > **Plus de tableaux de bord** > **Sécurité DNS** pour ouvrir le tableau de bord de la sécurité DNS.

STEP 3 | À partir du tableau de bord, configurez vos options de filtre à l’aide des menus déroulants disponibles.

1. Filtrer par plage horaire — Sélectionnez parmi **Dernière heure**, **Dernières 24 heures**, **7 derniers jours** ou **30 derniers jours** pour afficher les données pour une période spécifique.
2. Filtrer par catégorie DNS—Sélectionnez parmi **Sélectionner tout**, **Logiciel malveillantCommande et contrôle**, **Phishing**, **Logiciel indésirable**, **Liste d’exceptions**, **Enregistré dernièrement**, **DNS dynamique**, **Proxy**, **Parqué**, **Bénin**, **Suivi des publicités** pour filtrer l’ensemble de données sur la base d’un type de DNS.

   La catégorie Liste d’exceptions est une liste gérée par Palo Alto Networks de domaines explicitement autorisés en fonction des métriques de PAN-DB et Alexa. Ces domaines de liste d’autorisation sont fréquemment consultés et sont connus pour être exempts de contenu malveillant.
3. Filtrer par action DNS—Sélectionnez parmi **Autoriser**, **Bloquer** et **Sinkhole** pour filtrer en fonction de l’action effectuée sur une requête DNS en fonction des paramètres d’action de votre profil de sécurité DNS.

STEP 4 | En option, vous pouvez également télécharger, partager et planifier des rapports d’activité.

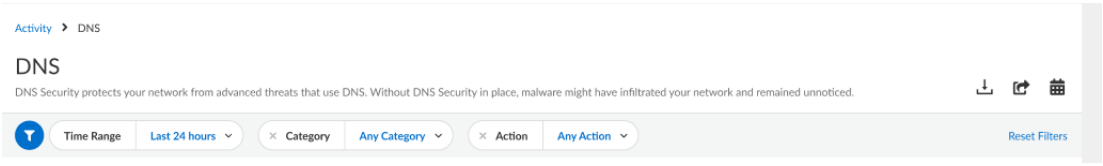
STEP 5 | Vous pouvez re-contextualiser, interagir et pivoter à partir des données fournies par les cartes du tableau de bord. Pour une vue d’ensemble de chacune des cartes de tableau de bord de la sécurité DNS, voir les cartes du Tableau de bord de la sécurité DNS.

Affichage du tableau de bord de la sécurité DNS (AIOps for NGFW Free)

STEP 1 | Utilisez les informations d’identification associées à votre compte de support Palo Alto Networks et connectez-vous à AIOps for NGFW Free l’application sur le hub.

STEP 2 | Sélectionnez **Tableaux de bord** > **Plus de tableaux de bord** > **Sécurité DNS** pour ouvrir le tableau de bord de la sécurité DNS.

STEP 3 | À partir du tableau de bord, configurez vos options de filtre à l’aide des menus déroulants disponibles.



1. Filtrer par plage horaire — Sélectionnez parmi **Dernière heure**, **Dernières 24 heures**, **7 derniers jours** ou **30 derniers jours** pour afficher les données pour une période spécifique.
2. Filtrer par catégorie DNS — Sélectionnez parmi **C2 (DGA, tunnellisation, autre C2)**, **Logiciel malveillant**, **Nouveau domaine enregistré**, **Phishing**, **DNS dynamique**, **Liste d’autorisation**, **Bénin**, **Logiciel indésirable**, **Parqué**, **Proxy** et **Toute catégorie**, pour filtrer l’ensemble de données en fonction d’un type DNS.

   La catégorie Liste d’autorisation est une liste tenue par Palo Alto Networks des domaines explicitement autorisés basée sur les mesures de PAN-DB et Alexa. Ces domaines de liste d’autorisation sont fréquemment consultés et sont connus pour être exempts de contenu malveillant.
3. Filtrer par action DNS—Sélectionnez parmi **Autoriser**, **Bloquer** et **Sinkhole** pour filtrer en fonction de l’action effectuée sur une requête DNS en fonction des paramètres d’action de votre profil de sécurité DNS.

STEP 4 | En option, vous pouvez également télécharger, partager et planifier des rapports d’activité.

STEP 5 | Vous pouvez re-contextualiser, interagir et pivoter à partir des données fournies par les cartes du tableau de bord. Pour une vue d’ensemble de chacune des cartes de tableau de bord de la sécurité DNS, voir les cartes du Tableau de bord de la sécurité DNS.

Affichage des journaux de la sécurité DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence de sécurité DNS avancée (pour une prise en charge des fonctionnalités améliorées) ou licence de sécurité DNS ❑ Licence de prévention avancée des menaces ou de prévention des menaces

Vous pouvez parcourir, rechercher et afficher les journaux de sécurité DNS qui sont automatiquement générés lorsque la sécurité DNS rencontre un événement qualifiant. Généralement, cela inclut toute catégorie de domaine que la sécurité DNS analyse, à moins qu’elle ne soit spécifiquement configurée avec un niveau de gravité des journaux aucun. Les entrées des journaux fournissent de nombreux détails sur l’événement, y compris le niveau de menace et, le cas échéant, la nature de la menace.

Les journaux de la sécurité DNS sont accessibles directement sur le pare-feu ou via des visionneuses de journaux basées sur Strata Logging Service (AIOps for NGFW Free, Cloud Management, Strata Logging Service, etc.). Alors que le pare-feu vous permet d’accéder aux entrées des journaux des menaces malveillantes générées lorsque les utilisateurs effectuent des requêtes DNS, les requêtes DNS bénignes ne sont pas enregistrées. Les données de sécurité DNS sont également transmises aux Strata Logging Service via la redirection des journaux (sous forme de journaux de menaces) et la télémétrie de la sécurité DNS (sous forme de journaux de la sécurité DNS) qui sont ensuite référencées par diverses applications de visionneuses de journaux d’activité. La télémétrie de la sécurité DNS fonctionne avec un minimum de surcharge, ce qui limite la quantité de données envoyées aux Strata Logging Service ; par conséquent, seul un sous-ensemble de requêtes DNS est transmis aux Strata Logging Service en tant qu’entrées de journal de la sécurité DNS, quel que soit le niveau de gravité, le type de menace ou la catégorie. Les journaux de menaces pour les requêtes DNS malveillantes qui sont transférées aux Strata Logging Service à l’aide d’un transfert de journaux sont disponibles dans leur intégralité. Par conséquent, Palo Alto Networks recommande d’afficher les journaux des requêtes DNS malveillantes en tant que journaux des menaces plutôt qu’en tant que journaux de sécurité DNS.

- Strata Cloud Manager
- PAN-OS et Panorama
- AIOps pour NGFW gratuit
- Service de journalisation Strata

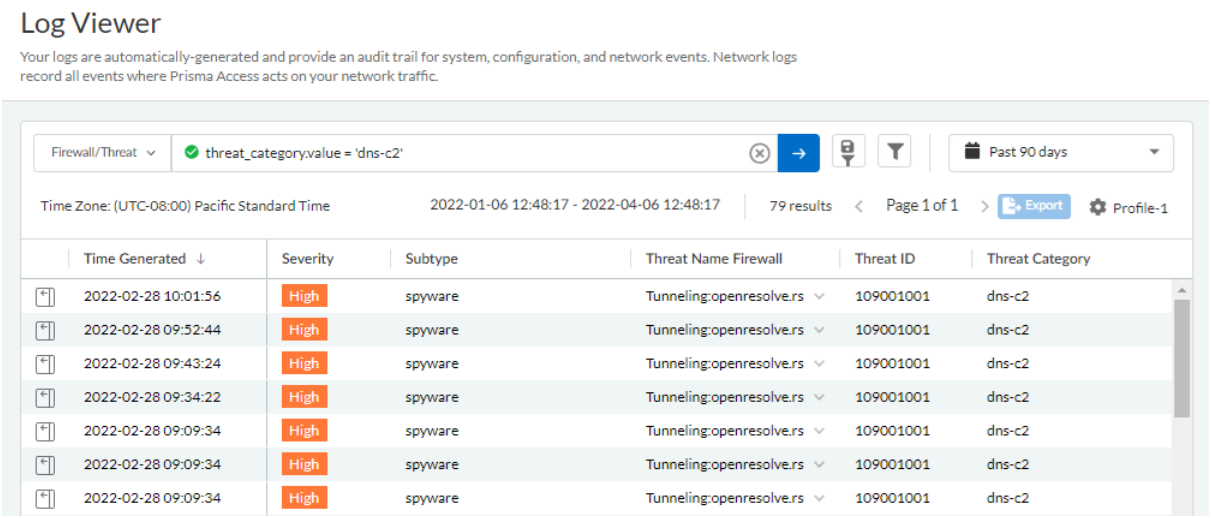
Affichage des journaux de la sécurité DNS (Strata Cloud Manager)

Les requêtes DNS bénignes qui ont été analysées par la sécurité DNS ne sont pas affichées dans la visionneuse de journaux. Connectez-vous à votre application Strata Logging Service pour accéder aux entrées des journaux DNS bénignes.

STEP 1 | Utilisez les informations d’identification associées à votre compte d’assistance Palo Alto Networks et connectez-vous au Strata Cloud Manager sur le hub https://apps.paloaltonetworks.com/.

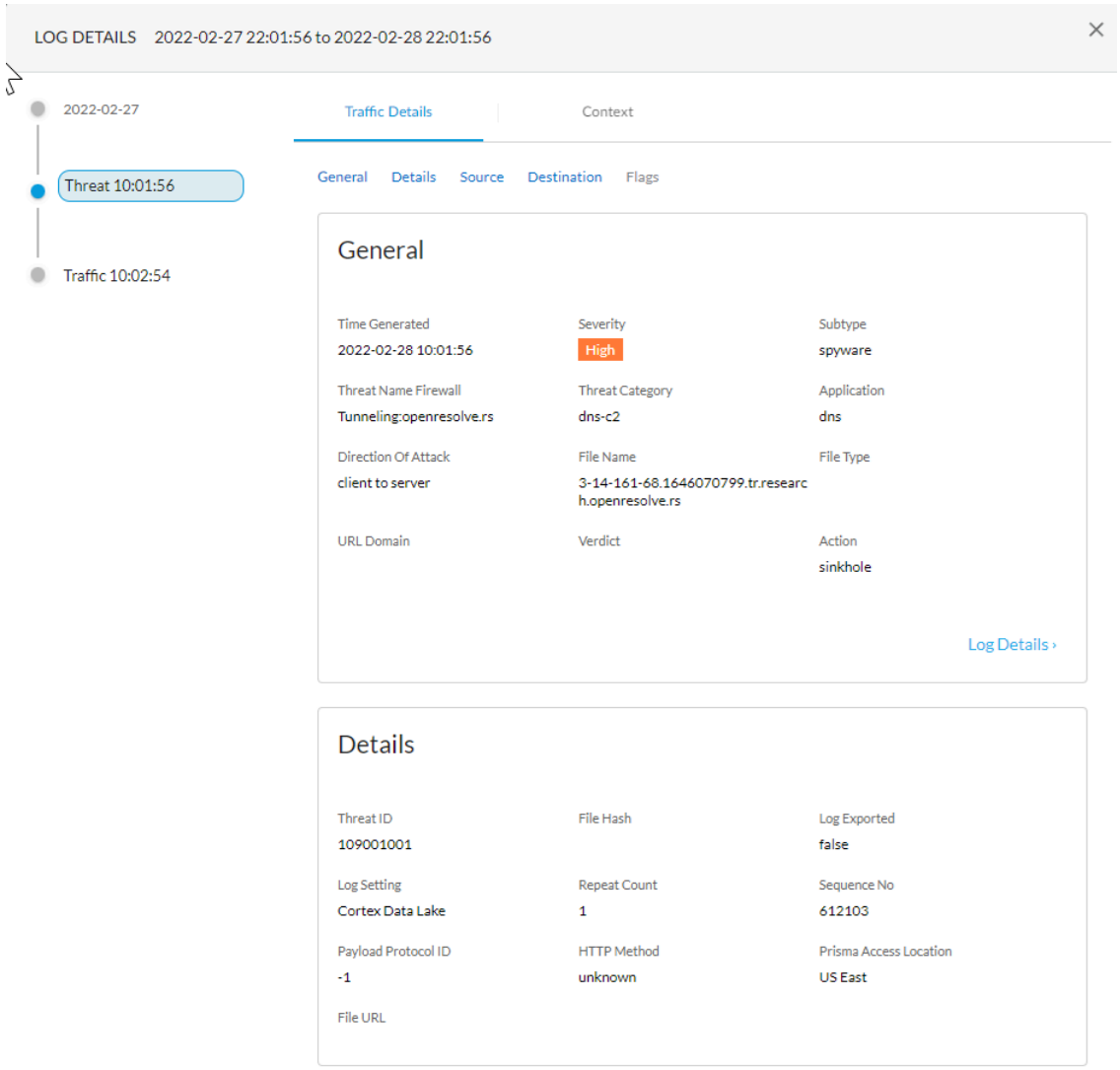
STEP 2 | Recherchez les requêtes DNS qui ont été traitées à l’aide de la sécurité DNS.

1. Sélectionnez **Incidents et alertes** > **Visionneuse de journaux**.
2. Limitez votre recherche à l’aide du filtre de menaces et soumettez une requête de journal basée sur la catégorie DNS, par exemple, `threat_category.value = 'dns-c2'` pour afficher les journaux qui ont été déterminés comme étant un domaine C2. Pour rechercher d’autres types de DNS, remplacez c2 par une autre catégorie DNS prise en charge (ddns, parqué, logiciel malveillant, etc.). Ajustez les critères de recherche si nécessaire pour votre recherche, y compris des paramètres de requête supplémentaires (tels que le niveau de gravité et le sous-type) ainsi qu’une plage de dates.



3. Sélectionnez une entrée de journal pour afficher les détails d’une menace DNS détectée.

4. La **catégorie** de menaces est affichée dans le volet **Général** de la vue détaillée du journal. D’autres détails pertinents sur la menace sont affichés dans les fenêtres correspondantes.



5. Pour les domaines stockés et les domaines de tunnellisation de DNS, y compris les APT (menaces persistantes avancées) basées sur la tunnellisation, vous pouvez afficher les différents outils utilisés dans l’attaque, ainsi que les campagnes d’attaque associées au domaine. Cela se reflète dans le champ ID/Nom de la menace pour l’entrée de journal d’un domaine donné. L’ID/le nom de la menace pour les domaines DNS avec attributions utilisent le format suivant : dans cet exemple, pour les domaines de tunnel DNS : `Tunnellisation :<tool_name>,<tool_name>,<tool_name>,...:<domain_name>`, où `tool_name` fait référence aux outils de tunnellisation de DNS utilisés pour intégrer des données dans les requêtes et les réponses DNS, mais aussi au nom de la campagne de cybermenace, dans une liste séparée par des virgules. Ces campagnes peuvent être des incidents acceptés par l’industrie et qui utilisent les mêmes conventions d’appellation ou peuvent être identifiées et nommées par Palo Alto Networks et décrites dans l’unité 42 des blogs des recherches sur les menaces. Un blog d’une telle campagne, dans ce cas, qui exploite les

techniques de tunnellisation de DNS, peut être trouvé ici : Exploitation de la tunnellisation de DNS pour le suivi et l’analyse.

Les attributions de campagne et d’outils associées peuvent prendre un certain temps après la fin de la détection initiale pour être visibles dans les journaux, ainsi que dans ThreatVault et Test-A-Site de Palo Alto Networks. Une fois le composant d’attribution terminé et vérifié, les outils de tunnellisation de DNS et les détails de la campagne s’affichent comme prévu dans les champs ID/Nom de la menace et Campagne.

Affichage des journaux de la sécurité DNS (NGFW (Managed by PAN-OS or Panorama))

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

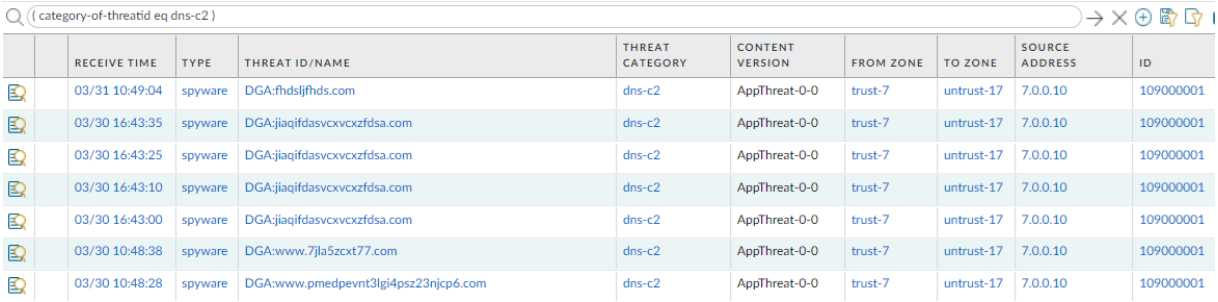
STEP 2 | Recherchez une activité sur le pare-feu pour les requêtes qui ont été traitées à l’aide de la sécurité DNS.

1. Sélectionnez **Moniteur** > **Journaux** > **Menace** et filtrer en fonction de la catégorie DNS.

   Prenons les exemples suivants :

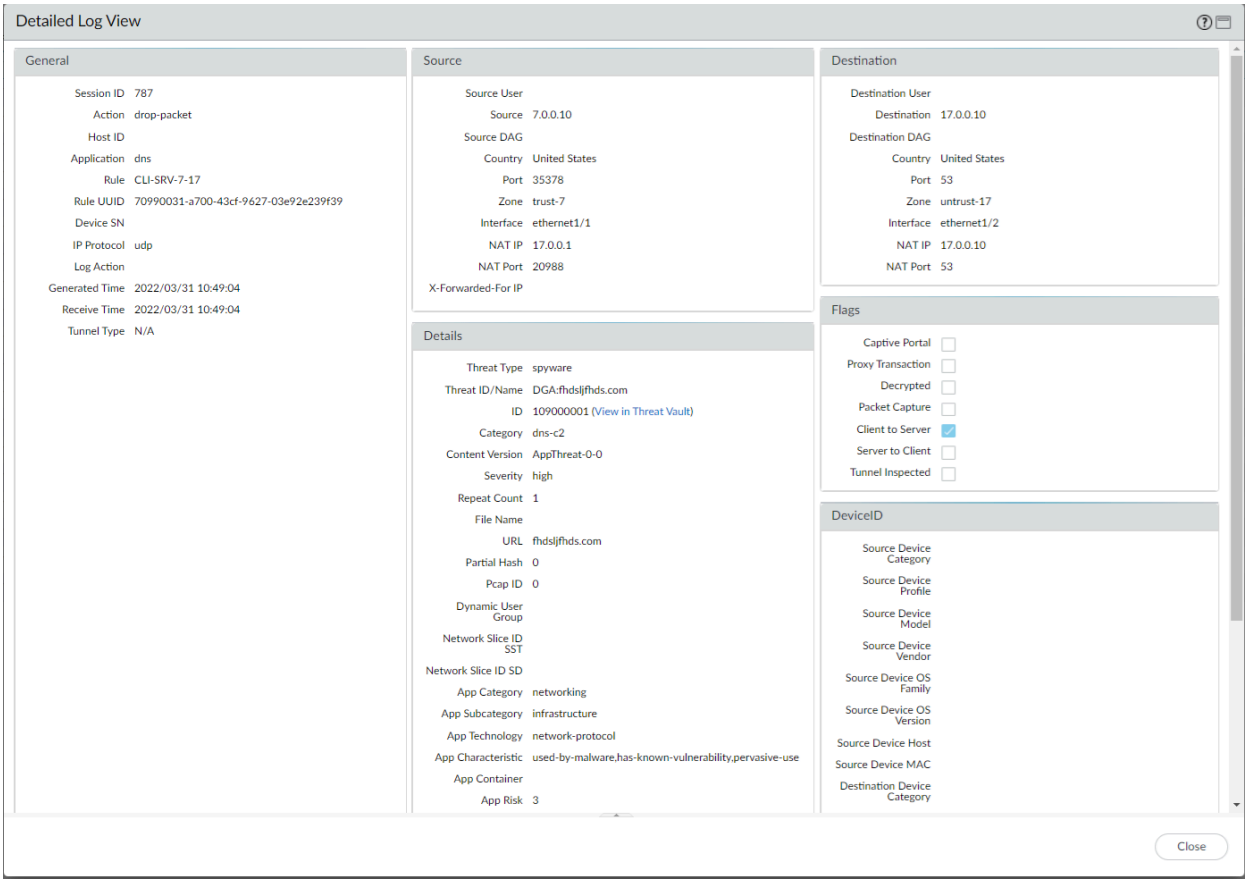
   - `( category-of-threatid eq dns-c2 )` pour afficher les journaux qui ont été déterminés comme étant un domaine C2 par la sécurité DNS
   - `(category-of-threatid eq adns-hijacking )`, où la variable `adns-hijacking` indique les requêtes DNS qui ont été classées comme une tentative de détournement de DNS malveillante par la sécurité DNS avancée.

   Pour rechercher d’autres types de DNS, remplacez c2 par une autre catégorie DNS prise en charge (ddns, parqué, logiciel malveillant, etc.).



	RECEIVE TIME	TYPE	THREAT ID/NAME	THREAT CATEGORY	CONTENT VERSION	FROM ZONE	TO ZONE	SOURCE ADDRESS	ID
	03/31 10:49:04	spyware	DGA:fhdsljfhds.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:35	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:25	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:10	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:00	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:38	spyware	DGA:www.7jla5zcxt77.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:28	spyware	DGA:www.pmedpevnt3lgi4psz23njcp6.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001

2. Sélectionnez une entrée de journal pour afficher les détails d’une menace DNS détectée.
3. La **catégorie** de menaces s’affiche dans le volet **Détails** de la vue détaillée du journal. D’autres détails pertinents sur la menace sont affichés dans les fenêtres correspondantes.



4. Pour les domaines stockés et les domaines de tunnellisation de DNS, y compris les APT (menaces persistantes avancées) basées sur la tunnellisation, vous pouvez afficher les différents outils utilisés dans l’attaque, ainsi que les campagnes d’attaque associées au domaine. Cela se reflète dans le champ ID/Nom de la menace pour l’entrée de journal d’un domaine donné. L’ID/le nom de la menace pour les domaines DNS avec attributions utilisent le format suivant : dans cet exemple, pour les domaines de tunnel DNS : `Tunnellisation :<tool_name>,<tool_name>,<tool_name>,...:<domain_name>`, où `tool_name` fait référence aux outils de tunnellisation de DNS utilisés pour intégrer des données dans les requêtes et les réponses DNS, mais aussi au nom de la campagne de cybermenace, dans une liste séparée par des virgules. Ces campagnes peuvent être des incidents acceptés par l’industrie et qui utilisent les mêmes conventions d’appellation ou peuvent être identifiées et nommées par Palo Alto Networks et décrites dans l’unité 42 des blogs des recherches sur les menaces. Un blog d’une telle campagne, dans ce cas, qui exploite les techniques de tunnellisation de DNS, peut être trouvé ici : Exploitation de la tunnellisation de

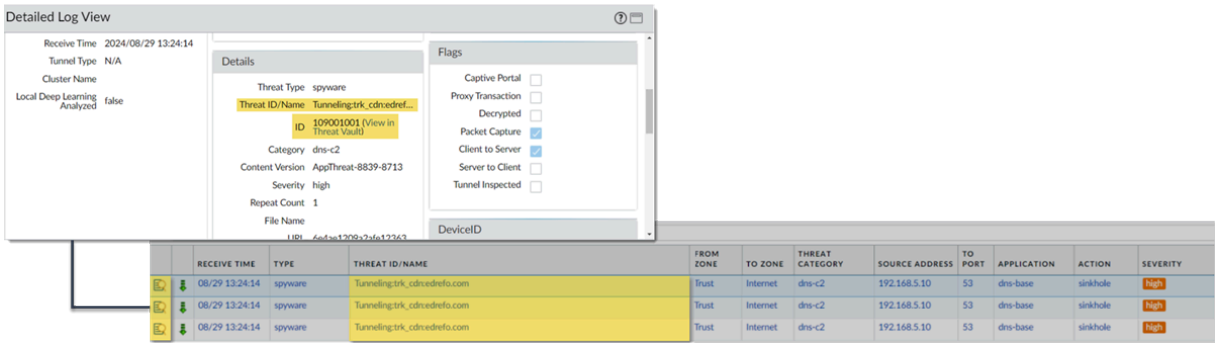
DNS pour le suivi et l’analyse. Vous pouvez également afficher les informations d’attribution à partir de ThreatVault et Test-A-Site de filtrage d’URL de Palo Alto Networks.

Les attributions de campagne et d’outils associées peuvent prendre un certain temps après la fin de la détection initiale pour être visibles dans les journaux, ainsi que dans ThreatVault et Test-A-Site de Palo Alto Networks. Une fois le composant d’attribution terminé et vérifié, les outils de tunnellisation de DNS et les détails de la campagne s’affichent comme prévu dans les champs ID/Nom de la menace et Campagne.

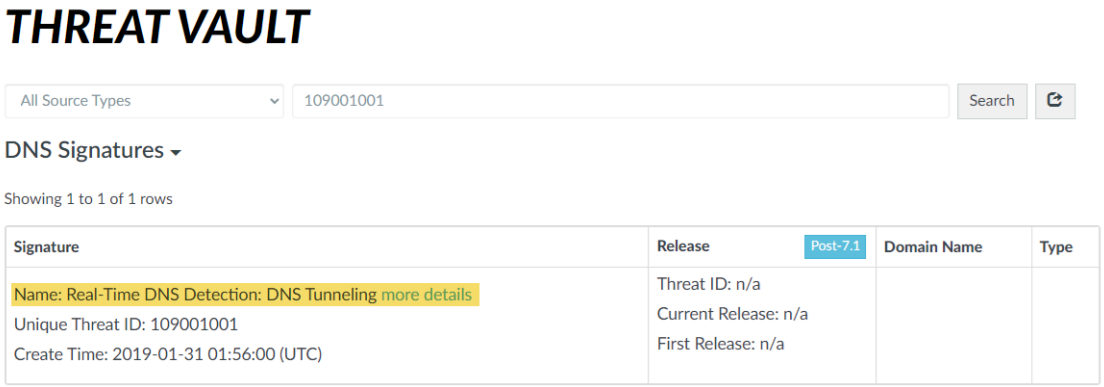
Prenons les exemples suivants :

- **Attribution APT du domaine de tunnellisation de DNS**

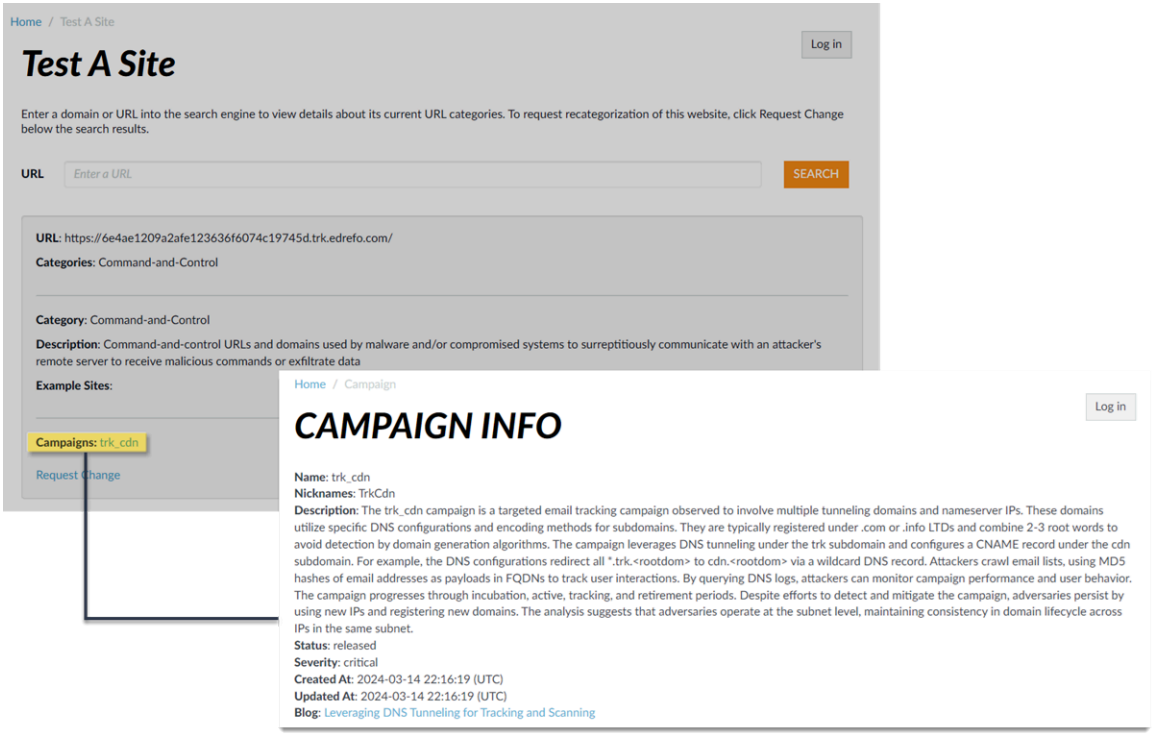
  1. PAN-OS



  2. ThreatVault

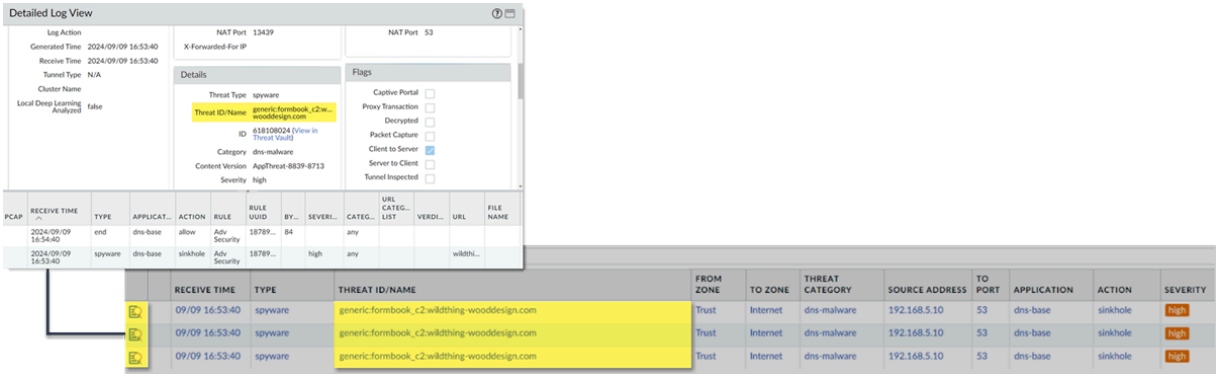


  3. Filtrage d’URL Test-A-Site

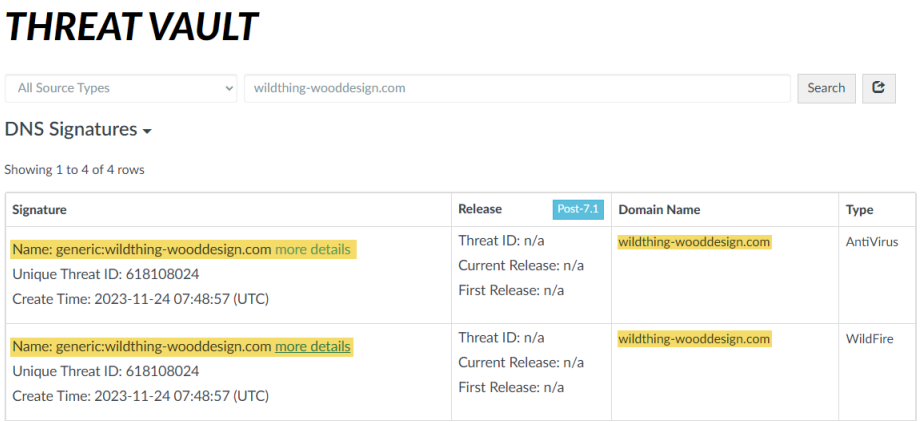


- **Attribution APT du domaine stocké**

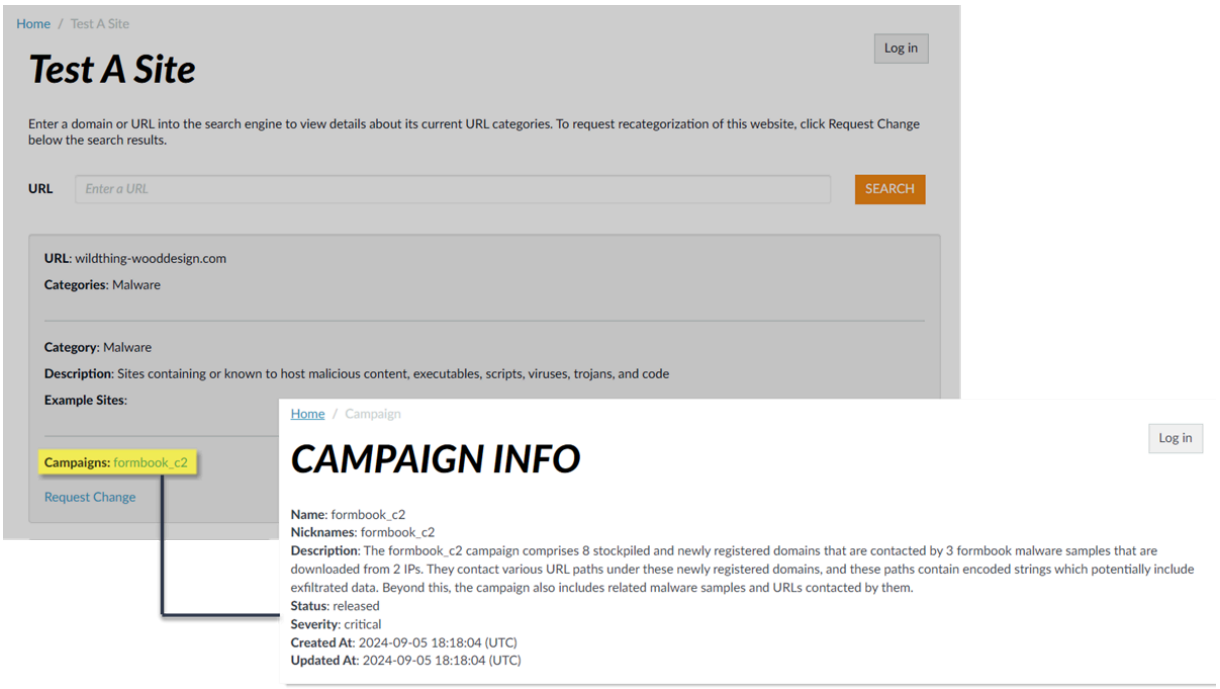
  1. PAN-OS



  2. ThreatVault



3. Filtrage d’URL Test-A-Site



Affichage des journaux de la sécurité DNS (AIOps for NGFW Free)

Les requêtes DNS bénignes qui ont été analysées par la sécurité DNS ne sont pas affichées dans la visionneuse de journaux de AIOps for NGFW Free. Connectez-vous à votre application Strata Logging Service pour accéder aux entrées des journaux DNS bénignes.

STEP 1 | Utilisez les informations d’identification associées à votre compte de support Palo Alto Networks et connectez-vous à AIOps for NGFW Free l’application sur le hub.

STEP 2 | Recherchez les requêtes DNS qui ont été traitées à l’aide de la sécurité DNS dans AIOps for NGFW Free.

1. Sélectionnez **Incidents et alertes** > **Visionneuse de journaux**.
2. Limitez votre recherche à l’aide du filtre de menaces et soumettez une requête de journal basée sur la catégorie DNS, par exemple, `threat_category.value = 'dns-c2'` pour afficher les journaux qui ont été déterminés comme étant un domaine C2. Pour rechercher d’autres types de DNS, remplacez c2 par une autre catégorie DNS prise en charge (ddns, parqué, logiciel malveillant, etc.). Ajustez les critères de recherche si nécessaire pour votre recherche, y compris des paramètres de requête supplémentaires (tels que le niveau de gravité et le sous-type) ainsi qu’une plage de dates.
3. Sélectionnez une entrée de journal pour afficher les détails d’une menace DNS détectée.
4. La **catégorie** de menaces s’affiche dans le volet **Détails** de la vue détaillée du journal. D’autres détails pertinents sur la menace sont affichés dans les fenêtres correspondantes.

Affichage des journaux de la sécurité DNS (Strata Logging Service)

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

STEP 2 | Allocation du stockage en fonction du type de journal. Si l’espace de stockage n’a pas été alloué pour les journaux de la sécurité DNS sur Strata Logging Service, les entrées de journalisation ne seront pas visibles via Strata Logging Service.

STEP 3 | Recherchez les requêtes DNS qui ont été traitées à l’aide de la sécurité DNS dans Strata Logging Service.

1. Sélectionnez **Explorer** pour ouvrir la visionneuse du journal Strata Logging Service.
2. Limitez votre recherche à l’aide du filtre de menaces et soumettez une requête de journal basée sur la catégorie DNS, par exemple, `threat_category.value = 'dns-c2'` pour afficher les journaux qui ont été déterminés comme étant un domaine C2. Pour rechercher d’autres types de DNS, remplacez c2 par une autre catégorie DNS prise en charge (ddns, parqué, logiciel malveillant, etc.). Ajustez les critères de recherche si nécessaire pour votre recherche, y compris des paramètres de requête supplémentaires (tels que le niveau de gravité et le sous-type) ainsi qu’une plage de dates.
3. Sélectionnez une entrée de journal pour afficher les détails d’une menace DNS détectée.
4. La **catégorie** de menaces s’affiche dans le volet **Détails** de la vue détaillée du journal. D’autres détails pertinents sur la menace sont affichés dans les fenêtres correspondantes.

