Utilisation des meilleures pratiques de sécurisation des appliances Web

Table des matières

- Introduction
- Informations générales
- EnvironnementRéseau
  - ICMP
  - Pare-Feu
  - Transfert de chemin inverse monodiffusion
  - Usurpation IP avec WCCP
- Configuration du réseau SWA
  - Interfaces
  - Routage du réseau de gestion
  - Télémétrie TALOS
  - DNS
  - Équilibrage de charge
  - Authentification active
  - Authentification passive
- Configuration des services
  - Proxy Web
  - Proxy HTTPS
  - Moniteur de trafic de couche 4 (L4TM)
- Configuration des stratégies
  - Complexité
  - Profils d'identification
  - Stratégies de décodage
  - Politiques d'accès
  - Catégories d'URL personnalisées et externes
- Moniteurs et alertes
  - Moniteurs CLI
  - Journalisation
  - Rapports de sécurité Web avancés (AWSR)
  - Alertes par e-mail
  - Surveillance de disponibilité
  - Surveillance SNMP
- Autres informations utiles

Introduction

Ce document décrit les meilleures pratiques de configuration de l'appliance Web sécurisé Cisco (SWA).

Informations générales

Ce guide constitue une référence pour la configuration des meilleures pratiques et traite de nombreux aspects d'un déploiement SWA. Il inclut l'environnement réseau pris en charge, la configuration des politiques, la surveillance et le dépannage. Bien que les meilleures pratiques documentées soient importantes pour la compréhension de tous les administrateurs, architectes et opérateurs, elles ne sont que des directives et doivent être traitées comme telles. Chaque réseau a ses propres besoins et défis.

En tant que périphérique de sécurité, le SWA interagit avec le réseau de plusieurs manières uniques. Il s'agit à la fois d'une source et d'une destination du trafic Web. Il agit en même temps en tant que serveur Web et client Web. Au minimum, il utilise l'usurpation d'adresse IP côté serveur et les techniques de l'homme du milieu pour inspecter les transactions HTTPS. Il peut usurper les adresses IP des clients, ce qui ajoute une autre couche de complexité au déploiement et impose des exigences supplémentaires en matière de prise en charge des configurations réseau. Ce guide traite des problèmes les plus courants liés à la configuration des périphériques réseau.

La configuration de la stratégie SWA a des conséquences non seulement sur l'efficacité et l'application de la sécurité, mais également sur les performances de l'appliance. Ce guide explique en détail l'impact de la complexité d'une configuration sur les ressources système. Il définit la complexité dans ce contexte et décrit comment la réduire lors de la conception des politiques. En outre, il est fait mention de fonctionnalités spécifiques et de la manière dont elles doivent être configurées pour améliorer la sécurité, l'évolutivité et l'efficacité.

La section Surveillance et alertes de ce document explique les méthodes les plus efficaces pour surveiller l'appliance, les performances et la disponibilité, ainsi que l'utilisation des ressources système. Il fournit également des informations pour le dépannage de base.

Environnement réseau

ICMP

Path MTU Discovery, tel que défini dans la RFC 1191, le mécanisme détermine la taille maximale d'un paquet le long de chemins arbitraires. Avec IPv4, un périphérique peut déterminer l'unité de transmission maximale (MTU) d'un paquet sur un chemin en définissant le bit Ne pas fragmenter

(DF) dans l'en-tête IP du paquet. Si, au niveau d’une liaison sur le chemin, un périphérique ne peut pas transférer le paquet sans fragment, un message ICMP (Internet Control Message Protocol) Fragmentation Needed (Type 3, Code 4) (Fragmentation requise par le protocole ICMP) est renvoyé à la source. Le client renvoie alors un paquet plus petit. Cela continue jusqu'à ce que le MTU du chemin complet soit découvert. IPv6 ne prend pas en charge la fragmentation et utilise un message ICMPv6 de type 2 (Packet Too Big) pour indiquer l'incapacité à faire passer un paquet par une liaison donnée.

Étant donné que le processus de fragmentation des paquets peut avoir de graves répercussions sur les performances d’un flux TCP, le SWA utilise la détection de MTU de chemin. Les messages ICMP mentionnés doivent être activés dans les périphériques réseau appropriés pour permettre au SWA de déterminer le MTU de son chemin à travers le réseau. Ce comportement peut être désactivé dans le SWA en exécutant la commande pathmtudiscovery dans CLI. La désactivation de la détection de MTU de chemin entraîne le passage de la MTU par défaut à 576 octets, comme défini dans la RFC 879, ce qui affecte gravement les performances. L'administrateur doit effectuer une étape supplémentaire de configuration manuelle du MTU dans le SWA à partir de la commande etherconfig CLI.

Dans le cas du protocole WCCP (Web Cache Communication Protocol), le trafic Web est redirigé vers le SWA à partir d'un autre périphérique réseau le long du chemin client vers Internet. Avec d’autres protocoles, tels qu’ICMP, ils ne sont pas redirigés vers le SWA. Il est possible que le SWA déclenche un message ICMP Fragmentation Needed (Fragmentation requise) à partir d'un routeur sur le réseau. Cependant, le message n'est pas remis à l'agent SWA. S'il s'agit d'une possibilité sur le réseau, la détection de MTU de chemin doit être désactivée. Comme mentionné, avec cette configuration, l'étape supplémentaire de réglage manuel de la MTU sur le SWA en exécutant la commande etherconfig dans CLI est requise.

Pare-Feu

Dans une configuration par défaut, le SWA n'usurpe pas l'adresse IP du client lors du proxy d'une connexion. Cela signifie que tout le trafic web sortant provient de l'adresse IP SWA. Vous devez vous assurer que les périphériques de traduction d'adresses de réseau (NAT) disposent d'un pool d'adresses et de ports externes suffisamment important pour prendre en charge cette fonctionnalité. Il est conseillé de réserver une adresse spécifique à cet effet.

Certains pare-feu utilisent des protections DoS (Denial-of-Service) ou d'autres fonctions de sécurité qui se déclenchent lorsque de nombreuses connexions simultanées proviennent d'une adresse IP client unique. Lorsque la mystification IP du client n'est pas activée, l'adresse IP SWA doit être exclue de ces protections.

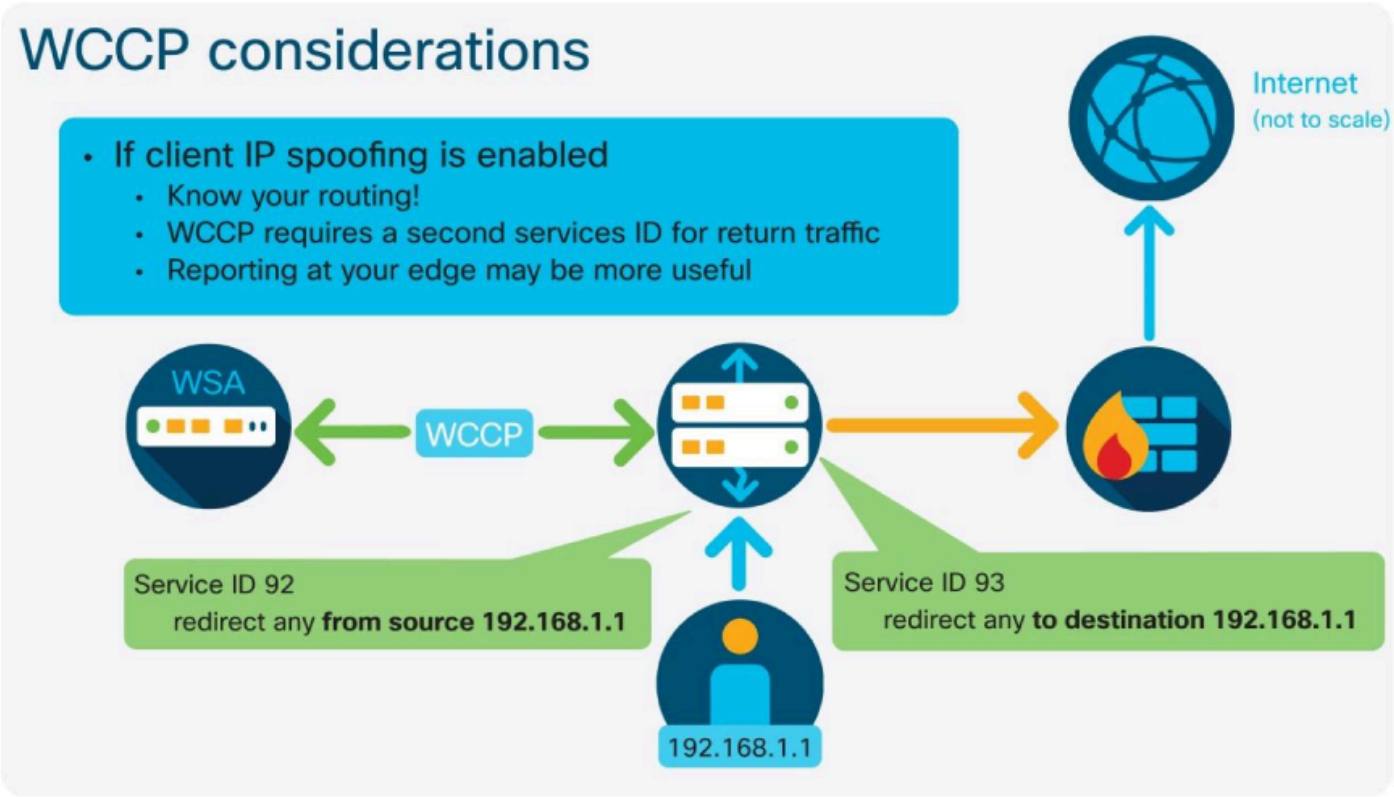
Transfert de chemin inverse monodiffusion

Le SWA usurpe l'adresse IP du serveur lorsqu'il communique avec un client, et peut éventuellement être configuré pour usurper l'adresse IP du client lorsqu'il communique avec un serveur en amont. Des protections telles que le transfert de chemin inverse de monodiffusion (uRPF) peuvent être activées sur les commutateurs pour garantir qu'un paquet entrant correspond au port d'entrée attendu. Ces protections vérifient l'interface source d'un paquet par rapport à la table de routage pour s'assurer qu'il est arrivé sur le port attendu. L'ASF doit être exemptée de ces protections, le cas échéant.

Usurpation IP avec WCCP

Lorsque la fonctionnalité d'usurpation d'adresse IP est activée dans le SWA, les requêtes sortantes quittent l'appliance et utilisent l'adresse source de la requête client d'origine. Cela nécessite une configuration supplémentaire de l'infrastructure réseau associée pour garantir que les paquets de retour sont acheminés vers l'interface de sortie SWA, au lieu du client à l'origine de la demande.

Lorsque le protocole WCCP est mis en oeuvre sur un périphérique réseau (routeur, commutateur ou pare-feu), un ID de service correspondant au trafic est défini en fonction d'une liste de contrôle d'accès (ACL). L'ID de service est ensuite appliqué à une interface et utilisé pour faire correspondre le trafic pour la redirection. Si la mystification IP est activée, un deuxième ID de service doit être créé pour s'assurer que le trafic de retour est également redirigé vers le SWA.



Configuration du réseau SWA

Interfaces

Le SWA dispose de cinq interfaces réseau utilisables : M1, P1, P2, T1 et T2. Chacun de ces éléments doit être exploité pour son objectif spécifique, dans la mesure du possible. Il est avantageux d'utiliser chaque port pour des raisons qui lui sont propres. L'interface M1 doit être connectée à un réseau de gestion dédié et le routage partagé doit être activé pour limiter l'exposition des services administratifs. Le P1 peut être limité au trafic de demande client, mais le P2 n'est pas autorisé à accepter des demandes de proxy explicites. Cela réduit la quantité de trafic sur chaque interface et permet une meilleure segmentation dans la conception du réseau.

Les ports T1 et T2 sont disponibles pour la fonction de surveillance du trafic de couche 4 (L4TM). Cette opération surveille un port de couche 2 en miroir et bloque le trafic en fonction d'une liste bloquée d'adresses IP et de noms de domaine malveillants connus. Pour ce faire, il examine les adresses IP source et de destination du trafic et envoie un paquet de réinitialisation TCP ou un message Port Unreachable (Port inaccessible) si la liste bloquée correspond. Le trafic envoyé avec n'importe quel protocole peut être bloqué avec cette fonctionnalité.

Même si la fonctionnalité L4TM n'est pas activée, le contournement transparent peut être amélioré lorsque les ports T1 et T2 sont reliés à un port en miroir. Dans le cas de WCCP, le SWA ne

connaît que l'adresse IP source et de destination d'un paquet entrant et doit prendre la décision de le transmettre par proxy ou de le contourner en fonction de ces informations. Le SWA résout toutes les entrées de la liste des paramètres de contournement toutes les 30 minutes, indépendamment de la durée de vie (TTL) des enregistrements. Cependant, si la fonctionnalité L4TM est activée, le SWA peut utiliser des requêtes DNS surveillées pour mettre à jour ces enregistrements plus fréquemment. Cela réduit le risque d'un faux négatif dans un scénario où le client a résolu une adresse différente de l'agent SWA.

Routage du réseau de gestion

Si le réseau de gestion dédié ne dispose pas d'un accès Internet, chaque service peut être configuré pour utiliser la table de routage des données. Il peut être adapté à la topologie du réseau, mais en général, il est recommandé d'utiliser le réseau de gestion pour tous les services système et le réseau de données pour le trafic client. Depuis la version 11.0 d'AsyncOS, les services pour lesquels le routage peut être défini sont les suivants :

- DNS
- Active Directory
- Flux URL externes
- Mises à jour
- Analyse et réputation des fichiers AMP (Advanced Malware Protection)

Pour un filtrage de sortie supplémentaire du trafic de gestion, des adresses statiques peuvent être configurées pour être utilisées dans les services suivants :

Flux d'URL externes :
1. Personnalisé ; dépend de l'endroit où ils sont hébergés.
2. Analyse et réputation des fichiers AMP.
3. cloud-sa.amp.cisco.com (Amérique du Nord).
4. cloud-sa.eu.amp.cisco.com (Europe).
5. cloud-sa.apjc.amp.cisco.com (Asie-Pacifique).

Mises à jour et mises à niveau :
1. downloads-static.ironport.com
2. updates-static.ironport.com

Télémétrie TALOS

Le groupe Cisco Talos est bien connu pour identifier les menaces nouvelles et émergentes.

Toutes les données envoyées à Talos sont anonymisées et stockées dans des centres de données américains. La participation à SensorBase améliore la catégorisation et l'identification des menaces Web et permet une meilleure protection contre le SWA et d'autres solutions de sécurité Cisco.

DNS

Les meilleures pratiques en matière de sécurité DNS (Domain Name Server) suggèrent que chaque réseau doit héberger deux résolveurs DNS : un pour les enregistrements faisant autorité au sein d'un domaine local et un pour la résolution récursive des domaines Internet. Pour y remédier, le SWA permet de configurer des serveurs DNS pour des domaines spécifiques. Si un seul serveur DNS est disponible pour les requêtes locales et récursives, tenez compte de la charge supplémentaire qu'il ajoute lorsqu'il est utilisé pour toutes les requêtes SWA. La meilleure option consiste à utiliser le résolveur interne pour les domaines locaux et les résolveurs Internet racine pour les domaines externes. Cela dépend du profil de risque et de la tolérance de l'administrateur.

Par défaut, le SWA met en cache un enregistrement DNS pendant au moins 30 minutes, quelle que soit la durée de vie de l'enregistrement. Les sites Web modernes qui font un usage intensif des réseaux de diffusion de contenu (CDN) ont de faibles enregistrements TTL car leurs adresses IP changent fréquemment. Cela peut entraîner la mise en cache par un client d'une adresse IP pour un serveur donné et la mise en cache par SWA d'une adresse différente pour le même serveur. Pour remédier à ce problème, la durée de vie par défaut de SWA peut être réduite à cinq minutes à partir des commandes CLI suivantes :

```
SWA_CLI> dnsconfig
...
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.
[]> SETUP
...
Enter the minimum TTL in seconds for DNS cache.
...
```

Les serveurs DNS secondaires doivent être configurés si le serveur principal n'est pas disponible. Si tous les serveurs sont configurés avec la même priorité, l'adresse IP du serveur est choisie au hasard. Selon le nombre de serveurs configurés, le délai d'attente d'un serveur donné peut varier. Cette table indique le délai d'attente d'une requête pour un maximum de six serveurs DNS :

Nombre de serveurs DNS	Délai de requête (dans l'ordre)
1	60
2	5, 45
3	5, 10, 45
4	1, 3, 11, 45
5	1, 3, 11, 45, 1
6	1, 3, 11, 45, 1, 1

Des options DNS avancées sont disponibles uniquement via l'interface de ligne de commande. Ces options sont disponibles dans CLI en exécutant la commande advanced proxyconfig > DNS.

Sélectionnez une de ces options :

- 0 - Utilisez toujours les réponses DNS dans l'ordre.
- 1 - Utilisez l'adresse fournie par le client, puis DNS.
- 2 - Utilisation DNS limitée
- 3 - Utilisation DNS très limitée

- Pour les options 1 et 2, DNS est utilisé si la réputation Web est activée.
- Pour les options 2 et 3, DNS est utilisé pour les requêtes proxy explicites. S'il n'y a pas de proxy en amont, ou dans le cas où le proxy en amont configuré échoue.
- Pour toutes les options, DNS est utilisé lorsque les adresses IP de destination sont utilisées dans l'appartenance à une stratégie.

Ces options contrôlent la façon dont le SWA décide de l'adresse IP à laquelle se connecter lors de l'évaluation d'une requête client. Lorsqu'une demande est reçue, le SWA voit une adresse IP de destination et un nom d'hôte. Le SWA doit décider s'il doit faire confiance à l'adresse IP de destination d'origine pour la connexion TCP, ou s'il doit terminer sa propre résolution DNS et utiliser l'adresse résolue. La valeur par défaut est 0 = Toujours utiliser les réponses DNS dans l'ordre, ce qui signifie que le SWA ne fait pas confiance au client pour fournir l'adresse IP.

- Option 1 : le SWA tente l'adresse IP fournie par le client pour la connexion, mais revient à l'adresse résolue en cas d'échec. L'adresse résolue est utilisée pour l'évaluation des stratégies (catégorie Web, réputation Web, etc.).
- Option 2 : le SWA utilise uniquement l'adresse fournie par le client pour la connexion et ne se rétablit pas. L'adresse résolue est utilisée pour l'évaluation des stratégies (catégorie Web, réputation Web, etc.).
- Option 3 : le SWA utilise uniquement l'adresse fournie par le client pour la connexion et ne se rétablit pas. L'adresse IP fournie par le client est utilisée pour l'évaluation des stratégies (catégorie Web, réputation Web, etc.).

L'option choisie dépend de la confiance que l'administrateur doit accorder au client lorsqu'il détermine l'adresse résolue d'un nom d'hôte donné. Si le client est un proxy en aval, choisissez l'option 3 pour éviter la latence ajoutée des recherches DNS inutiles.

Équilibrage de charge

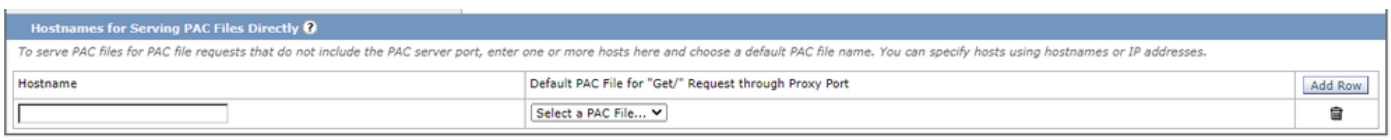
WCCP permet un équilibrage transparent de la charge du trafic lorsque jusqu'à huit appliances sont utilisées. Il permet d'équilibrer les flux de trafic en fonction du hachage ou du masque, il peut être pondéré s'il existe une combinaison de modèles d'appliances sur le réseau et les périphériques peuvent être ajoutés/supprimés du pool de services sans temps d'arrêt. Un équilibreur de charge dédié est recommandé lorsque vous utilisez 8 SWA ou plus.

Les meilleures pratiques de configuration WCCP varient en fonction de la plate-forme utilisée. Pour les commutateurs Cisco Catalyst®, les meilleures pratiques sont documentées dans le Livre blanc sur la solution Cisco Catalyst Instant Access.

Le protocole WCCP présente des limites lorsqu'il est utilisé avec un appareil de sécurité adaptatif Cisco (ASA). L'usurpation d'adresse IP du client n'est pas prise en charge. En outre, les clients et SWA doivent se trouver derrière la même interface. Pour cela, il est plus souple d'utiliser un commutateur ou un routeur de couche 4 pour rediriger le trafic. La configuration WCCP sur la plate-forme ASA est décrite dans WCCP sur ASA : Concepts, limitations et configuration.

Pour les déploiements explicites, un fichier de configuration automatique de proxy (PAC) est la méthode la plus largement déployée, mais elle présente des inconvénients et des implications en matière de sécurité qui sortent du cadre de ce document. Si un fichier PAC est déployé, il est conseillé d'utiliser des objets de stratégie de groupe (GPO) pour configurer l'emplacement plutôt que de compter sur le protocole de découverte automatique de proxy Web (WPAD), qui est une cible courante pour les agresseurs et qui peut être facilement exploité s'il est mal configuré. Le SWA peut héberger plusieurs fichiers PAC et contrôler leur expiration dans le cache du navigateur.

Un fichier PAC peut être demandé directement à partir du SWA à partir d'un numéro de port TCP configurable (9001 par défaut). Si aucun port n'est spécifié, la demande peut être envoyée au processus proxy lui-même comme s'il s'agissait d'une demande Web sortante. Dans ce cas, il est possible de servir un fichier PAC spécifique basé sur l'en-tête d'hôte HTTP présent dans la requête.



Kerberos doit être configuré différemment lorsqu'il est utilisé dans un environnement haute disponibilité (HA). Le SWA prend en charge les fichiers keytab, ce qui permet d'associer plusieurs noms d'hôtes à un nom de principe de service (SPN). Pour plus d'informations, consultez Création d'un compte de service dans Windows Active Directory pour l'authentification Kerberos dans les déploiements haute disponibilité .

Authentification active

Kerberos est un protocole d'authentification plus sécurisé et largement pris en charge que NT LAN Manager Security Support Provider (NTLMSSP). Le système d'exploitation Apple OS X ne prend pas en charge NTLMSSP, mais il peut utiliser Kerberos pour s'authentifier si un domaine est joint. L'authentification de base ne doit pas être utilisée, car elle envoie des informations d'identification non chiffrées dans l'en-tête HTTP et peut facilement être analysée par un pirate sur le réseau. Si l'authentification de base doit être utilisée, le chiffrement des informations d'identification doit être activé pour garantir que les informations d'identification sont envoyées sur un tunnel chiffré.

Plusieurs contrôleurs de domaine doivent être ajoutés à la configuration pour garantir la disponibilité, mais il n'y a pas d'équilibrage de charge inhérent de ce trafic. Le SWA envoie un paquet TCP SYN à tous les contrôleurs de domaine configurés et le premier à répondre est utilisé pour l'authentification.

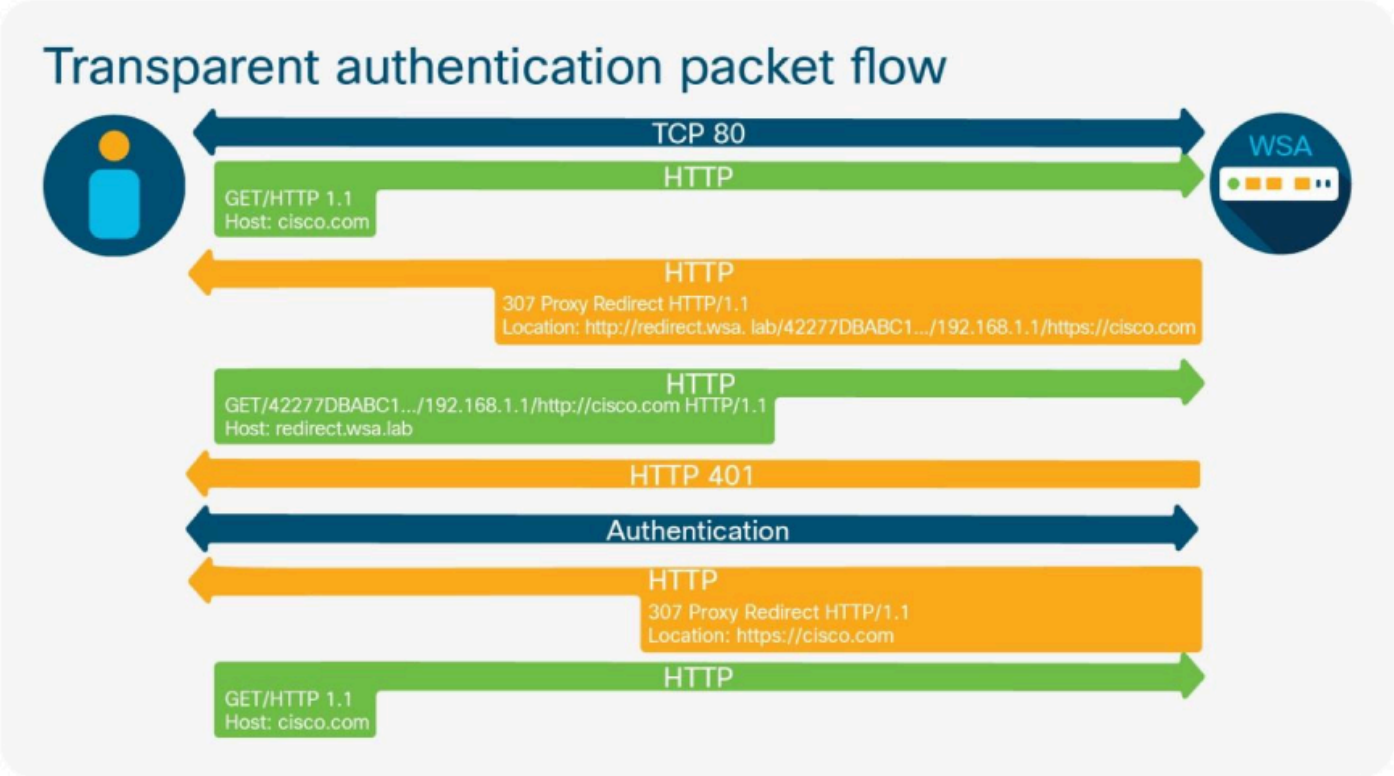
Le nom d'hôte de redirection configuré dans la page des paramètres d'authentification détermine où un client transparent est envoyé pour terminer l'authentification. Pour qu'un client Windows puisse effectuer l'authentification intégrée et obtenir l'authentification unique (SSO), le nom d'hôte de redirection doit se trouver dans la zone Sites de confiance du Panneau de configuration Options Internet. Le protocole Kerberos exige que le nom de domaine complet (FQDN) soit utilisé pour spécifier une ressource, ce qui signifie que le « shortname » (ou le nom « NETBIOS ») ne peut pas être utilisé si Kerberos est le mécanisme d'authentification prévu. Le nom de domaine complet doit être ajouté manuellement aux sites de confiance (par exemple, via la stratégie de groupe). En outre, la connexion automatique avec le nom d'utilisateur et le mot de passe doit être définie dans le panneau de configuration des options Internet.

Des paramètres supplémentaires sont requis dans Firefox pour que le navigateur puisse effectuer l'authentification avec les proxys réseau. Ces paramètres peuvent être configurés dans la page about:config. Pour que Kerberos s'exécute correctement, le nom d'hôte de redirection doit être ajouté à l'option network.negotiation-auth.trusted-uris. Pour NTLMSSP, il doit être ajouté à l'option network.automatic-ntlm-auth.trusted-uris.

Les substituts d'authentification sont utilisés pour mémoriser un utilisateur authentifié pendant une durée définie après la fin de l'authentification. Les substituts IP doivent être utilisés autant que possible pour limiter le nombre d'événements d'authentification actifs qui se produisent.

L'authentification active d'un client est une tâche gourmande en ressources, en particulier lorsque Kerberos est utilisé. Le délai d'attente de substitution est de 3 600 secondes (une heure) par défaut et peut être réduit, mais la valeur la plus basse recommandée est de 900 secondes (15 minutes).

Cette image montre comment « redirect.WSA.lab » est utilisé comme nom d'hôte de redirection :



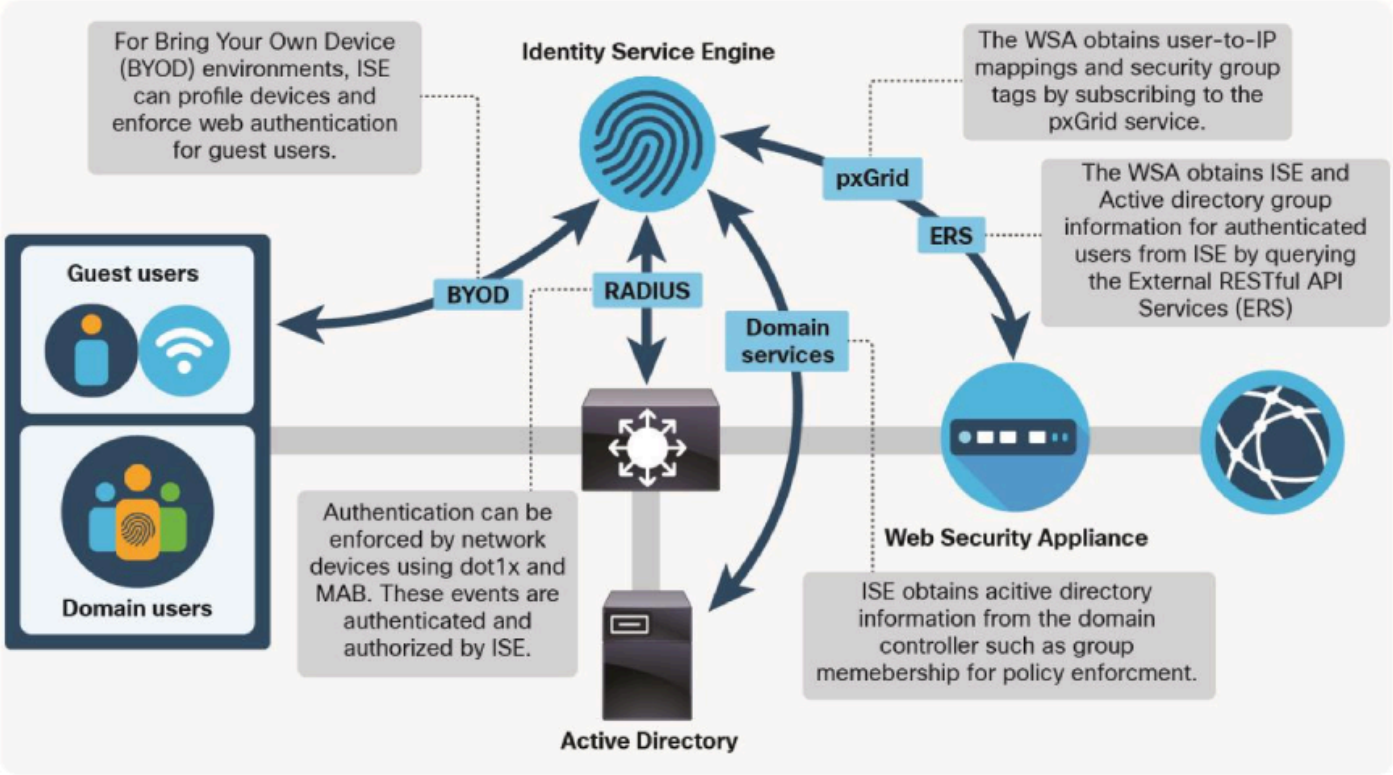
Authentification passive

Le SWA peut exploiter d'autres plates-formes de sécurité Cisco pour identifier passivement les utilisateurs proxy. L'identification passive des utilisateurs élimine les invites d'authentification et les communications Active Directory directes. Cela réduit la latence et l'utilisation des ressources de l'appliance. Les mécanismes actuellement disponibles pour l'authentification passive sont l'agent d'annuaire contextuel (CDA), le moteur ISE (Identity Services Engine) et le connecteur ISE-PIC (Identity Services Connector).

ISE est un produit riche en fonctionnalités qui aide les administrateurs à centraliser leurs services d'authentification et à tirer parti d'un ensemble complet de contrôles d'accès au réseau. Lorsqu'ISE prend connaissance d'un événement d'authentification d'utilisateur (par authentification Dot1x ou redirection d'authentification Web), elle remplit une base de données de session qui contient des informations sur l'utilisateur et le périphérique impliqués dans l'authentification. Le SWA se connecte à ISE sur la plate-forme Exchange Grid (pxGrid) et obtient le nom d'utilisateur, l'adresse IP et la balise de groupe de sécurité (SGT) associés à une connexion proxy. Depuis la

version 11.7 d'AsyncOS, le SWA peut également interroger le service RESTAURAL externe (ERS) sur ISE pour obtenir des informations sur le groupe.

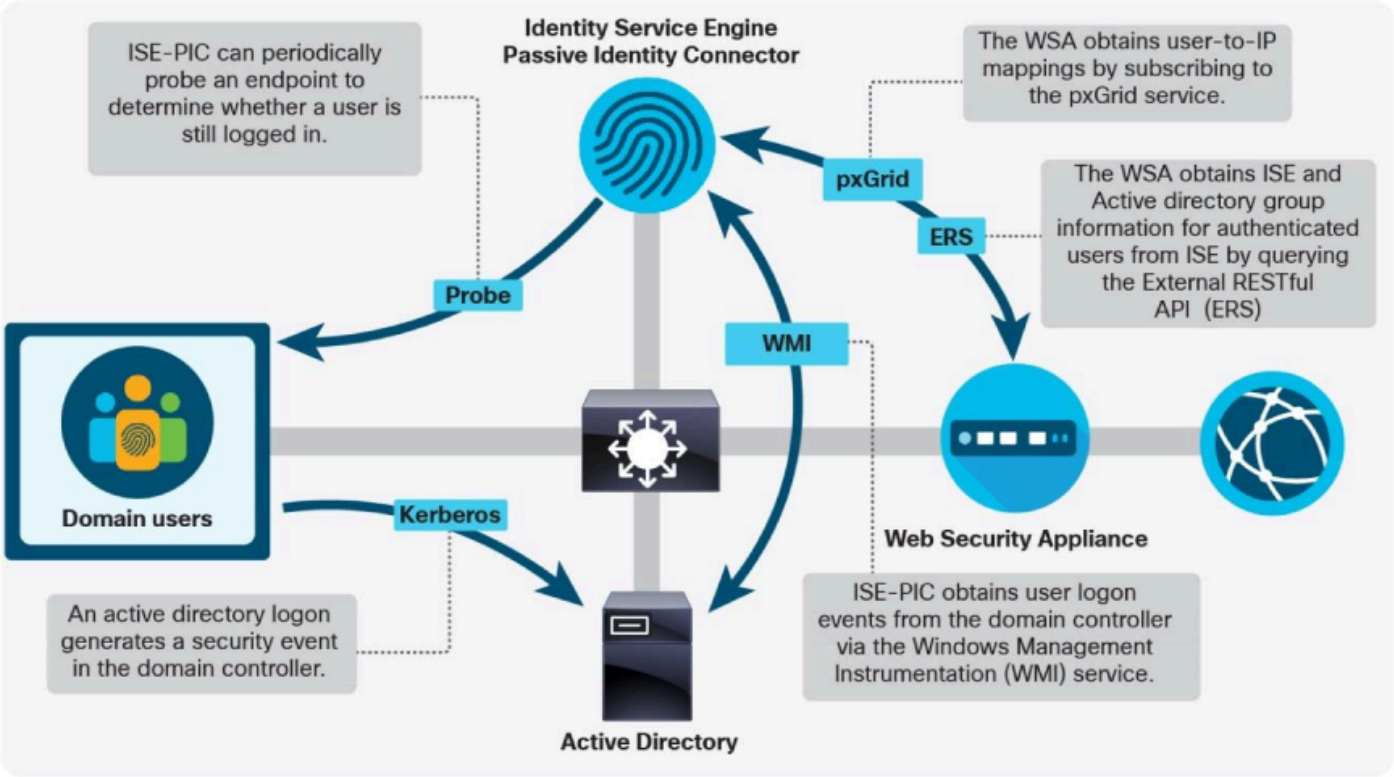
Les versions suggérées sont ISE 3.1 et SWA 14.0.2-X et ultérieures. Pour plus d'informations sur la matrice de compatibilité ISE pour SWA, consultez Matrice de compatibilité ISE pour appareil Web sécurisé. Pour plus d'informations sur les étapes d'intégration complète, consultez le Guide de l'utilisateur final de l'appliance de sécurité Web.



Cisco annonce la fin de vie du logiciel Cisco Context Directory Agent (CDA). Reportez-vous à la section Cisco Context Directory Agent (CDA).

Depuis le patch 6 de CDA, il est compatible avec Microsoft Server 2016. Cependant, les administrateurs sont vivement encouragés à migrer leurs déploiements CDA vers ISE-PIC. Les deux solutions utilisent WMI pour s'abonner au journal des événements de sécurité Windows afin de générer des mappages utilisateur-IP (appelés sessions). Dans le cas de CDA, les requêtes SWA mappent avec RADIUS.

Dans le cas de ISE-PIC, les mêmes connexions pxGrid et ERS sont utilisées dans le déploiement ISE complet. La fonctionnalité ISE-PIC est disponible dans une installation ISE complète et dans un appareil virtuel autonome.

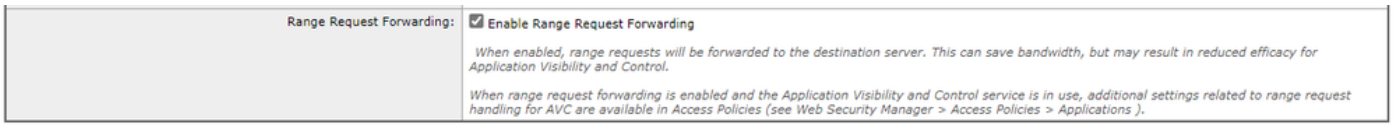


Configuration des services

Proxy Web

La mise en cache doit être activée dans la configuration du proxy Web pour économiser de la bande passante et améliorer les performances. Cela devient moins important à mesure que le pourcentage de trafic HTTPS augmente, car le SWA ne met pas en cache les transactions HTTPS par défaut. Si le proxy est déployé pour servir uniquement des clients explicites, le mode de transfert doit être spécifié pour rejeter tout trafic qui n'est pas spécifiquement destiné au service proxy. De cette manière, la surface d'attaque de l'appliance est réduite et les meilleures pratiques sont en place (désactivez la fonctionnalité si elle n'est pas requise).

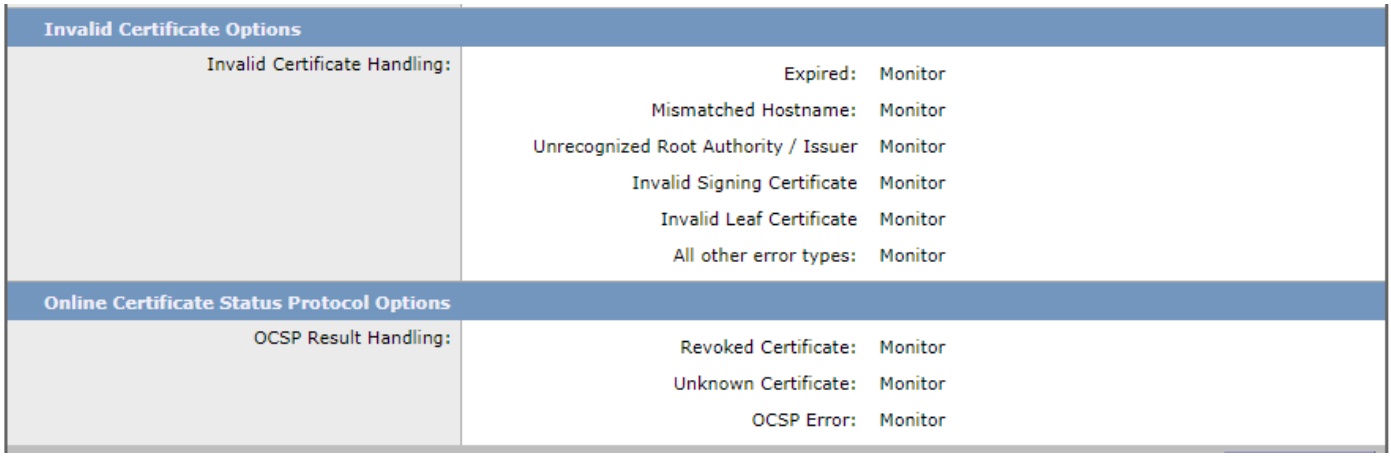
Les en-têtes de requête de plage sont utilisés dans les requêtes HTTP pour spécifier la plage d'octets d'un fichier à télécharger. Il est généralement utilisé par les systèmes d'exploitation et les démons de mise à jour d'applications pour transférer de petites parties d'un fichier à la fois. Par défaut, le SWA supprime ces en-têtes afin d'obtenir le fichier complet à des fins d'analyse antivirus (AV), d'analyse et de réputation des fichiers et de contrôle de la visibilité des applications (AVC). L'activation du transfert global des en-têtes de demande de plage dans les paramètres proxy permet aux administrateurs de créer des stratégies d'accès individuelles qui transfèrent ou suppriment ces en-têtes. Pour plus d'informations sur cette configuration, reportez-vous à la section Stratégies d'accès.



Proxy HTTPS

Les meilleures pratiques en matière de sécurité suggèrent que les clés privées doivent être générées sur l'appliance où elles sont utilisées et ne jamais être transportées ailleurs. L'assistant proxy HTTPS permet de créer la paire de clés et le certificat utilisés pour le déchiffrement des connexions TLS (Transport Layer Security). La demande de signature de certificat (CSR) peut être téléchargée et signée par une autorité de certification (CA) interne. Dans un environnement Active Directory (AD), il s'agit de la meilleure méthode, car une autorité de certification intégrée à AD est approuvée automatiquement par tous les membres du domaine et aucune étape supplémentaire n'est requise pour déployer le certificat.

Une fonction de sécurité du proxy HTTPS est de valider les certificats du serveur. Les meilleures pratiques suggèrent que les certificats non valides nécessitent que la connexion soit abandonnée. L'activation du décryptage pour EUN permet au SWA de présenter une page de blocage expliquant la raison du blocage. Si cette option n'est pas activée, tous les sites HTTPS bloqués génèrent une erreur de navigateur. Cela entraîne une augmentation des tickets d'assistance et une hypothèse de la part des utilisateurs que quelque chose est cassé, plutôt que SWA a bloqué la connexion. Toutes les options de certificat non valides doivent être définies sur au moins Déchiffrer. Si vous laissez l'une de ces options définie sur Surveillance, le système ne pourra pas consigner les messages d'erreur utiles si des problèmes de certificat empêchent le chargement d'un site.



Comme le protocole OCSP (Online Certificate Services Protocol), les vérifications doivent rester activées et le moniteur ne doit être utilisé pour aucune option. Les certificats révoqués doivent être abandonnés et tous les autres doivent au moins être définis sur Déchiffrer pour permettre la consignation des messages d'erreur pertinents. La recherche d'accès aux informations d'autorité

(recherche AIA) est l'endroit où un client peut glaner le signataire du certificat et une URL où des certificats supplémentaires peuvent être récupérés.

Par exemple, si une chaîne de certificats reçue d'un serveur est incomplète (s'il lui manque un certificat intermédiaire ou racine), le SWA peut vérifier le champ AIA et l'utiliser pour récupérer les certificats manquants et vérifier l'authenticité. Ce paramètre est uniquement disponible dans l'interface de ligne de commande à partir des commandes suivantes :

```
SWA_CLI> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters
[]> HTTPS
...
Do you want to enable automatic discovery and download of missing Intermediate Certificates?
[Y]>
...
```



Remarque : Ce paramètre est activé par défaut et ne doit pas être désactivé. De nombreux serveurs modernes s’appuient sur ce mécanisme pour fournir une chaîne de confiance complète aux clients.

Moniteur de trafic de couche 4 (L4TM)

L4TM est un moyen très efficace d'étendre la portée du SWA pour inclure le trafic malveillant qui ne traverse pas le proxy, et pour inclure le trafic sur tous les ports TCP et UDP. Les ports T1 et T2 sont destinés à être connectés à une prise réseau ou à une session de surveillance de commutateur. Cela permet à SWA de surveiller passivement tout le trafic provenant des clients. Si du trafic destiné à une adresse IP malveillante est détecté, le SWA peut mettre fin aux sessions TCP en envoyant un RST tout en usurpant l'adresse IP du serveur. Pour le trafic UDP, il peut envoyer un message Port Unreachable (Port inaccessible). Lors de la configuration de la session

de surveillance, il est préférable d'exclure tout trafic destiné à l'interface de gestion du SWA afin d'empêcher la fonctionnalité d'interférer potentiellement avec l'accès au périphérique.

En plus de surveiller le trafic malveillant, L4TM surveille également les requêtes DNS pour mettre à jour la liste des paramètres de contournement. Cette liste est utilisée dans les déploiements WCCP pour renvoyer certaines requêtes au routeur WCCP pour un routage direct vers le serveur Web. Les paquets qui correspondent à la liste des paramètres de contournement ne sont pas traités par le proxy. La liste peut contenir des adresses IP ou des noms de serveurs. Le SWA résout toutes les entrées de la liste des paramètres de contournement toutes les 30 minutes, quelle que soit la durée de vie de l'enregistrement. Cependant, si la fonctionnalité L4TM est activée, le SWA peut utiliser des requêtes DNS surveillées pour mettre à jour ces enregistrements plus fréquemment. Cela réduit le risque d'un faux négatif dans un scénario où le client a résolu une adresse différente de l'agent SWA.

Configuration des stratégies

Une configuration correcte des stratégies est essentielle aux performances et à l'évolutivité de l'approche SWA. Des stratégies efficaces protègent les clients et mettent en oeuvre les exigences de l'entreprise. Cependant, la configuration des politiques affecte également l'utilisation des ressources, l'intégrité des appliances et les performances. Des politiques complexes ou mal conçues engendrent instabilité et lenteur de réaction

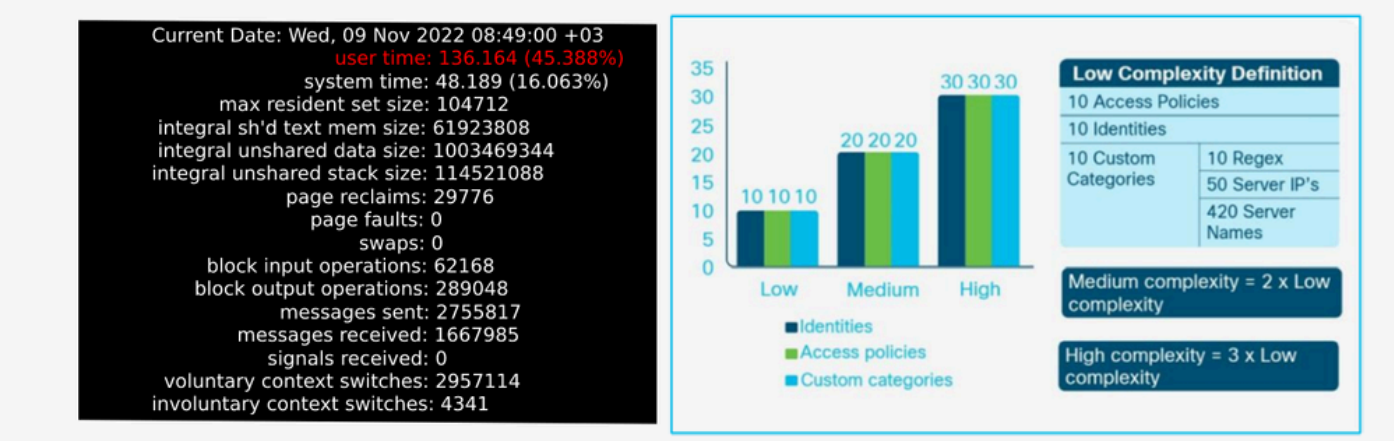
Complexité

Divers éléments de politique sont utilisés dans l'élaboration des politiques relatives aux approches sectorielles. Le fichier XML généré à partir de la configuration est utilisé pour créer un certain nombre de fichiers de configuration principaux et de règles d'accès. Plus la configuration est complexe, plus le processus proxy doit passer de temps à évaluer différents ensembles de règles pour chaque transaction. Lors de l'analyse comparative et du dimensionnement du SWA, un ensemble d'éléments de stratégie de base est créé, représentant trois niveaux de complexité de configuration. Une configuration peu complexe comprend 10 profils d'identité, des politiques de déchiffrement, des politiques d'accès et des catégories personnalisées (contenant 10 entrées regex, 50 adresses IP de serveur et 420 noms d'hôte). En doublant ou en triplant ces valeurs, vous obtenez une configuration de complexité moyenne ou élevée.

Lorsqu’une configuration devient trop complexe, les premiers symptômes incluent généralement une réponse lente dans l’interface Web et l’interface de ligne de commande. Il ne peut pas y avoir d'impact significatif pour les utilisateurs au début. Mais plus la configuration est complexe, plus le processus proxy doit passer de temps en mode utilisateur. De ce fait, la vérification du pourcentage de temps passé dans ce mode peut être utile pour diagnostiquer une configuration

trop complexe comme étant la cause d'un SWA lent.

Le temps processeur, en secondes, est consigné dans le journal track_stats toutes les 5 minutes. Cela signifie que le pourcentage de temps utilisateur peut être calculé comme suit : (temps utilisateur + temps système)/300. Lorsque le temps utilisateur approche 270, le processus passe trop de cycles UC en mode utilisateur, ce qui est généralement dû au fait que la configuration est trop complexe pour être analysée efficacement.



Remarque : Le SWA a une limite maximale de 60 000 connexions client simultanées et de 60 000 connexions serveur simultanées.

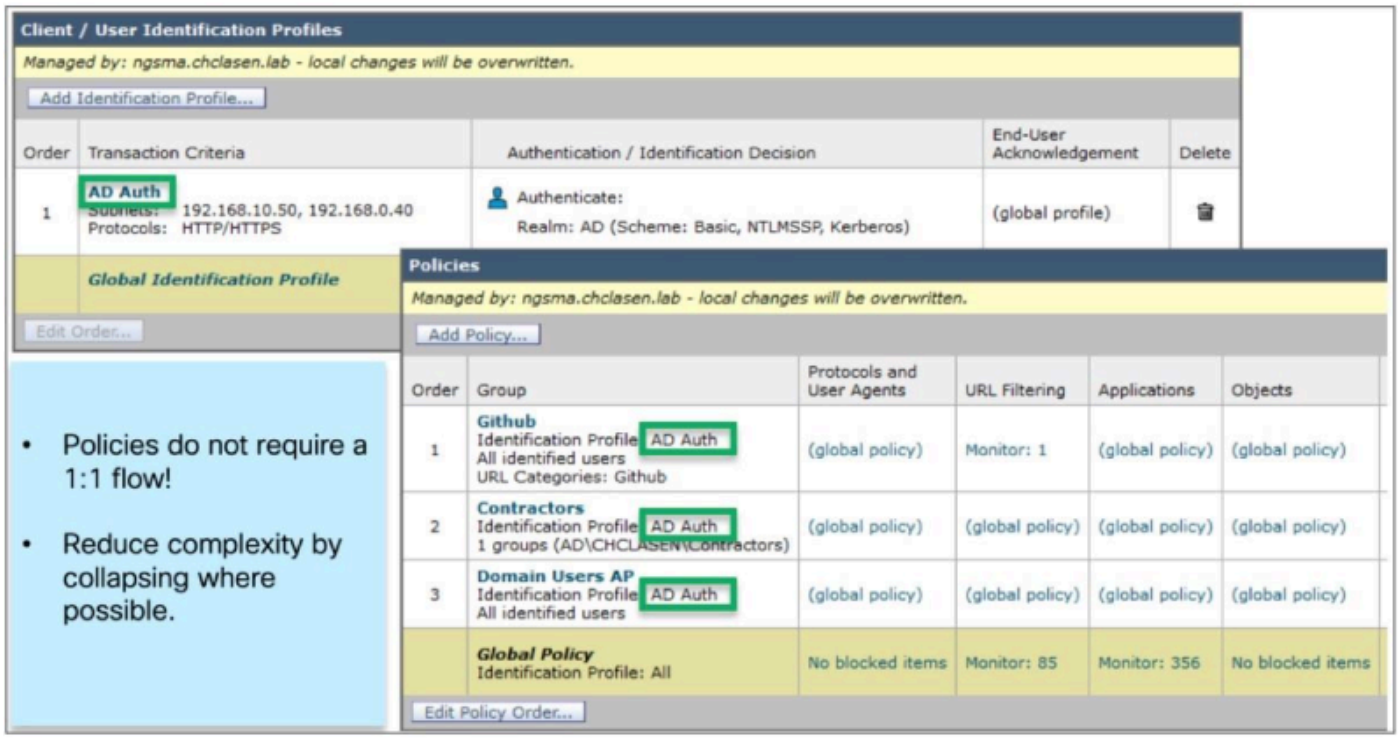
Profils d'identification

Les profils d'identification (ID) sont les premiers éléments de stratégie qui sont évalués lors de la réception d'une nouvelle demande. Toutes les informations configurées dans la première section du profil d'ID sont évaluées à l'aide d'un AND logique. Cela signifie que tous les critères doivent correspondre pour que la demande corresponde au profil. Lors de la création d'une stratégie, celle-ci doit être aussi spécifique que nécessaire. Les profils qui incluent des adresses d'hôte individuelles sont rarement requis et peuvent entraîner des configurations trop volumineuses. L'utilisation de la chaîne d'agent utilisateur trouvée dans les en-têtes HTTP, la liste de catégories personnalisée ou le sous-réseau constitue généralement une meilleure stratégie pour limiter l'étendue d'un profil.

En général, les stratégies qui nécessitent une authentification sont configurées en bas et les exceptions ajoutées en haut. Lors de l'ordonnancement des stratégies qui ne nécessitent pas d'authentification, les stratégies les plus utilisées doivent être les plus proches possible du sommet. Ne comptez pas sur l'échec de l'authentification pour restreindre l'accès. Si un client connu sur le réseau ne peut pas s'authentifier auprès d'un proxy, il doit être exempté de

l'authentification et bloqué dans les stratégies d'accès. Les clients qui ne peuvent pas s'authentifier de façon répétée envoient des requêtes non authentifiées au SWA, qui utilise des ressources et peut entraîner une utilisation excessive du CPU et de la mémoire.

Une idée fausse répandue chez les administrateurs est qu'il doit y avoir un profil d'ID unique et une politique de déchiffrement et d'accès correspondante. Il s'agit d'une stratégie inefficace pour la configuration des stratégies. Si possible, les stratégies doivent être « réduites » afin qu'un profil d'ID unique puisse être associé à plusieurs stratégies de déchiffrement et d'accès. Cela garantit que tous les critères d'une stratégie donnée doivent correspondre (le trafic et la stratégie). D'une manière générale, la stratégie d'authentification et les stratégies résultantes permettent de réduire le nombre de stratégies dans leur ensemble.



Stratégies de décodage

Comme pour le profil d'ID, les critères définis dans la stratégie de déchiffrement sont évalués en tant qu'opération AND logique, avec une exception importante lorsque des informations provenant de l'ISE sont utilisées. Voici comment fonctionne la mise en correspondance des stratégies, selon les éléments configurés (groupe AD, utilisateur ou SGT) :

- Groupes et utilisateurs AD - Aucun changement au comportement précédent ; la stratégie est mise en correspondance si l'utilisateur est membre d'un groupe OU si l'utilisateur est spécifié dans la stratégie.
- Groupes et utilisateurs SGT et AD - La stratégie est mise en correspondance si l'utilisateur est associé au SGT ET est membre du groupe AD, OU si l'utilisateur est spécifié dans la

stratégie.
- SGT et utilisateurs : la stratégie est mise en correspondance si l'utilisateur est associé à la SGT ou si l'utilisateur est spécifié dans la stratégie.

Parmi les services fournis par le SWA, l'évaluation du trafic HTTPS est la plus importante du point de vue des performances. Le pourcentage de trafic décrypté a un impact direct sur la manière dont l'appliance doit être dimensionnée. Un administrateur peut compter sur au moins 75 % du trafic Web pour être HTTPS.

Après l'installation initiale, le pourcentage de trafic décrypté doit être déterminé afin de garantir que les prévisions de croissance future sont définies avec précision. Après le déploiement, ce nombre doit être vérifié une fois par trimestre. Il est facile de trouver le pourcentage de trafic HTTPS déchiffré par le SWA avec une copie de access_logs, même sans logiciel de gestion de journaux supplémentaire. L'exécution de commandes Bash ou PowerShell simples peut être utilisée pour obtenir ce numéro. Voici quelques exemples de commandes pour chaque environnement :

1. Commande Linux :

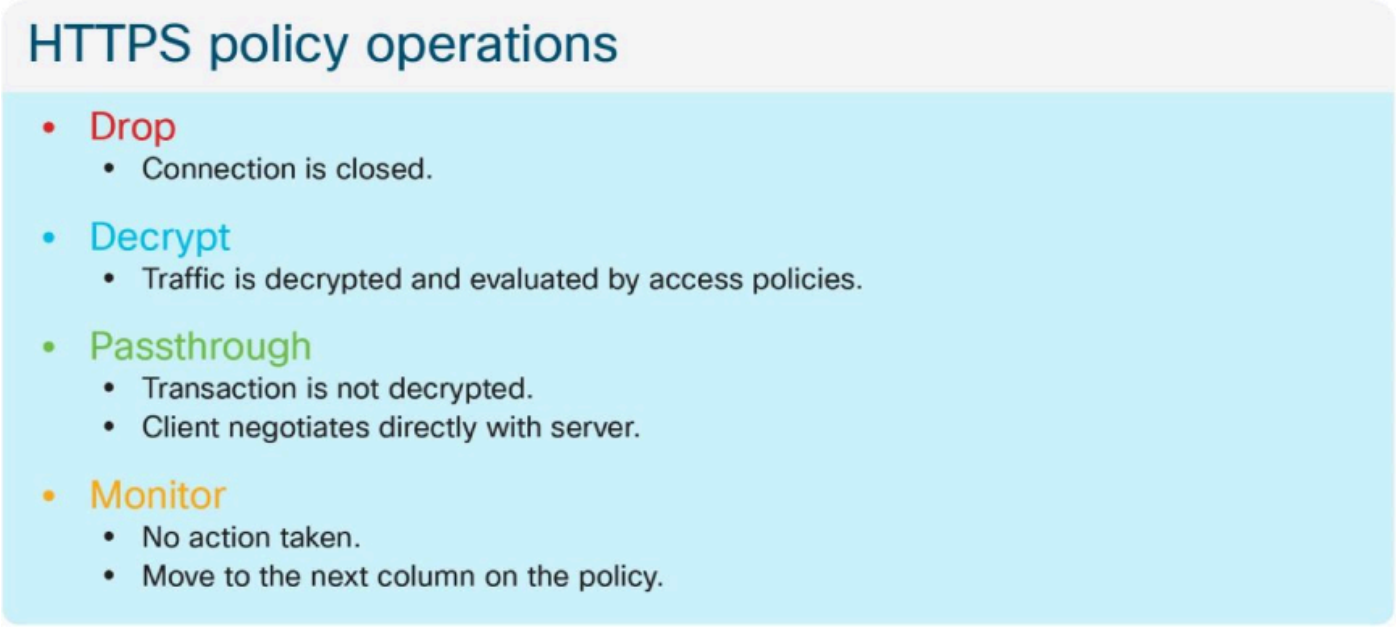
```
cat aclog.current | grep -Ev "\/407|\/401" | awk 'BEGIN { total=0; decrypt=0; ssl=0;} {total++; if($0 ~
```

---

2. Commande PowerShell :

```
$lines = Get-Content -Path "aclog.current" | Where-Object { $_ -notmatch "/407|/401" }; $total = 0; $de
```

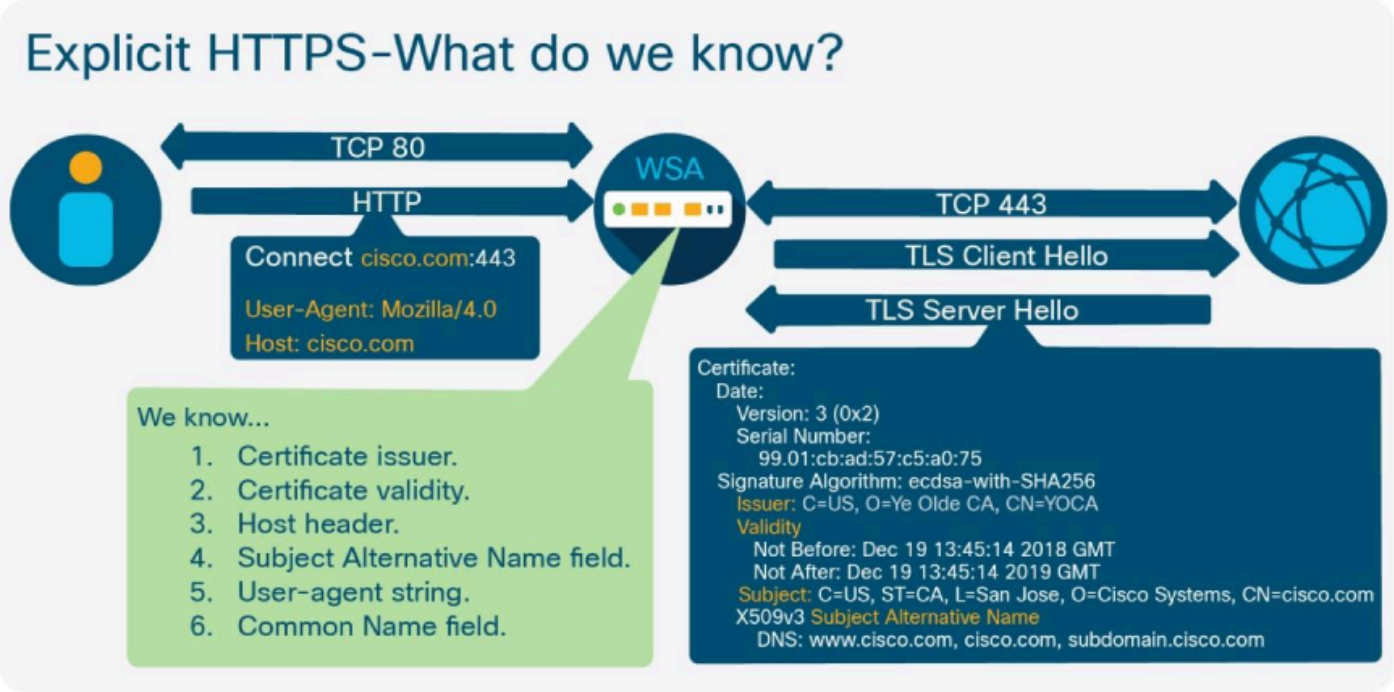
Lors de la conception des stratégies de déchiffrement, il est important de comprendre comment les différentes actions répertoriées dans la stratégie amènent l'appliance à évaluer les connexions HTTPS. L'action Passthrough est utilisée lorsque le client et le serveur doivent être autorisés à terminer chaque extrémité de leur session TLS sans que le SWA ne déchiffre chaque paquet. Même si un site est défini sur Passthrough, le SWA doit toujours être requis pour effectuer une connexion TLS avec le serveur. Le SWA doit choisir de bloquer une connexion en fonction de la validité du certificat, et il doit initier une connexion TLS avec le serveur pour obtenir le certificat. Si le certificat est valide, le SWA ferme la connexion et permet au client de poursuivre la configuration de la session directement avec le serveur.

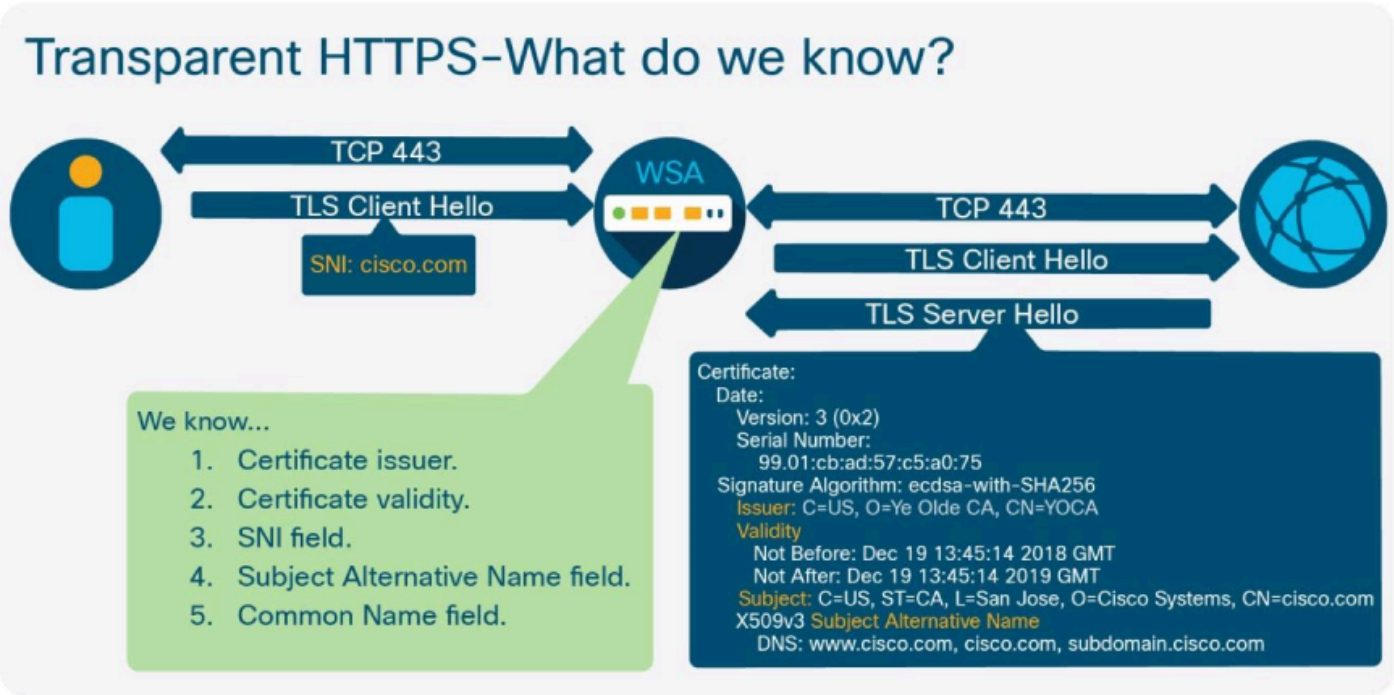


Le seul cas où SWA n'effectue aucune connexion TLS est lorsque le nom du serveur ou l'adresse IP est présent dans une catégorie personnalisée. Ce paramètre est défini sur passthrough et le nom du serveur est disponible dans un HTTP CONNECT ou un TLS Client Hello. Dans un scénario explicite, le client fournit le nom d'hôte du serveur au proxy avant l'ouverture de la session TLS (dans l'en-tête d'hôte), de sorte que ce champ est comparé à la catégorie personnalisée.

Dans un déploiement transparent, SWA vérifie le champ d'indication du nom du serveur (SNI) dans le message Hello du client TLS et l'évalue par rapport à la catégorie personnalisée. Si l'en-tête d'hôte ou le SNI n'est pas présent, SWA doit poursuivre la connexion avec le serveur pour vérifier les champs Subject Alternative Name (SAN) et Common Name (CN) sur le certificat (dans cet ordre).

Pour réduire le nombre d'échanges TLS, configurez les serveurs approuvés pour qu'ils passent à partir des listes de catégories personnalisées. Contrairement aux catégories Web ou aux scores de réputation (qui exigent toujours que SWA effectue une connexion TLS), cette opération contourne la connexion complète, mais empêche les vérifications de validité du certificat.





Étant donné la vitesse à laquelle les nouveaux sites apparaissent sur le Web, il est probable qu'un certain nombre de sites ne soient pas classés dans les catégories des bases de données de réputation et de catégorisation du Web utilisées par SWA. Cela n'indique pas que le site est plus susceptible d'être malveillant, et tous ces sites sont toujours soumis à l'analyse antivirus, à l'analyse de la réputation et des fichiers AMP, et à tout blocage d'objet. Pour ces raisons, il n'est pas recommandé d'abandonner les sites non classés (dans la plupart des cas). Il est préférable de les configurer pour qu'elles soient décryptées et analysées par les moteurs AV et évaluées par AVC, AMP, les politiques d'accès, etc. Vous trouverez plus d'informations sur les sites non classés dans la section Stratégies d'accès.

Politiques d'accès

Tout comme le profil d'ID, les critères définis dans la stratégie de déchiffrement sont également évalués en tant qu'opération AND logique, avec une exception importante lorsque des informations provenant de l'ISE sont utilisées. Le comportement de correspondance de stratégie est expliqué ci-dessous, en fonction des éléments configurés (groupe AD, utilisateur ou SGT) :

- Groupes et utilisateurs AD - Aucun changement au comportement précédent car la stratégie est mise en correspondance si l'utilisateur est membre du groupe OU si l'utilisateur est spécifié dans la stratégie.
- Groupes et utilisateurs SGT et AD - La stratégie est mise en correspondance si l'utilisateur est associé au SGT ET est membre du groupe AD, OU si l'utilisateur est spécifié dans la stratégie.
- SGT et utilisateurs - La stratégie est mise en correspondance si l'utilisateur est associé à la SGT OU si l'utilisateur est spécifié dans la stratégie.

Le trafic HTTP est évalué par rapport aux stratégies d'accès immédiatement après son authentification. Le trafic HTTPS est évalué après son authentification et si l'action de déchiffrement est appliquée conformément à la stratégie de déchiffrement correspondante. Pour les requêtes décryptées, il existe deux entrées access_log. La première entrée de journal indique l'action appliquée à la connexion TLS initiale (déchiffrement) et une seconde entrée de journal indique l'action appliquée par la stratégie d'accès à la requête HTTP déchiffrée.

Comme expliqué dans la section Proxy Web, les en-têtes de demande de plage sont utilisés pour demander une plage d'octets spécifique d'un fichier et sont généralement utilisés par les services de mise à jour du système d'exploitation et des applications. Par défaut, le SWA supprime ces en-têtes des requêtes sortantes, car sans le fichier entier, il est impossible d'effectuer une analyse des programmes malveillants ou d'utiliser les fonctionnalités AVC. Si de nombreux hôtes sur le réseau demandent fréquemment de petites plages d'octets pour récupérer des mises à jour, cela peut déclencher le téléchargement du fichier entier plusieurs fois simultanément. Cela peut rapidement épuiser la bande passante Internet disponible et provoquer des pannes de service. Les causes les plus courantes de ce scénario d'échec sont les mises à jour Microsoft Windows et les démons de mise à jour du logiciel Adobe.

Pour limiter ce risque, la meilleure solution consiste à orienter le trafic sur l'ensemble du SWA. Cela n'est pas toujours possible pour les environnements déployés de manière transparente et, dans ces cas, la meilleure option suivante consiste à créer des politiques d'accès dédiées pour le trafic et à activer le transfert d'en-tête de requête de plage sur ces politiques. Vous devez tenir compte du fait que l'analyse antivirus et l'AVC ne sont pas possibles pour ces requêtes, et que les stratégies doivent être conçues pour cibler uniquement le trafic prévu. La meilleure façon d'y parvenir est de faire correspondre la chaîne agent-utilisateur trouvée dans l'en-tête de la demande. La chaîne user-agent pour les démons de mise à jour courants peut être trouvée en ligne, ou les requêtes peuvent être capturées par un administrateur et examinées. La plupart des

services de mise à jour, y compris les mises à jour logicielles Microsoft Windows et Adobe, n'utilisent pas HTTPS.

Comme décrit dans la section Stratégies de décodage, il n'est pas recommandé de supprimer les sites non classés dans les stratégies de décodage. Pour les mêmes raisons, il n'est pas recommandé de les bloquer dans les stratégies d'accès. Le moteur d'analyse de contenu dynamique (DCA) peut utiliser le contenu d'un site donné, ainsi que d'autres données heuristiques, pour catégoriser des sites qui seraient marqués comme non catégorisés par des recherches dans la base de données d'URL. L'activation de cette fonctionnalité réduit le nombre de verdicts non classés dans le SWA.

Les paramètres d'analyse d'objets d'une stratégie d'accès peuvent inspecter plusieurs types de fichiers d'archive. Si le réseau télécharge régulièrement des fichiers d'archive dans le cadre de mises à jour d'applications, l'activation des inspections de fichiers d'archive peut augmenter considérablement l'utilisation du processeur. Ce trafic doit être exempté et identifié à l'avance si l'intention est d'inspecter tous les fichiers archivés. Le premier endroit pour étudier les méthodes possibles pour identifier le trafic est la chaîne utilisateur-agent, car cela peut aider à éviter les listes IP autorisées qui peuvent devenir fastidieuses à gérer.

Catégories d'URL personnalisées et externes

Les listes de catégories personnalisées permettent d'identifier un serveur par adresse IP ou nom d'hôte. Il est possible d'utiliser des expressions régulières (regex) pour spécifier des modèles où les noms de serveurs correspondent. L'utilisation d'un modèle regex pour faire correspondre un nom de serveur est plus gourmande en ressources que l'utilisation d'une correspondance de sous-chaîne. Ce champ ne doit être utilisé que lorsque cela est nécessaire. Un « ». peut être ajouté au début d'un nom de domaine pour correspondre à un sous-domaine sans utiliser regex.

Par exemple, cisco.com correspond également à www.cisco.com. Comme expliqué dans la section Complexité, la complexité faible correspond à 10 listes de catégories personnalisées, la complexité moyenne à 20 et la complexité élevée à 30. Il est recommandé de conserver ce nombre sous 20, en particulier si les listes utilisent des modèles d'expressions rationnelles ou contiennent un grand nombre d'entrées. Reportez-vous à la section Stratégies d'accès pour plus de détails sur le nombre d'entrées pour chaque type.

Les flux d'URL externes sont plus flexibles que les listes de catégories personnalisées statiques, et leur utilisation peut avoir un impact direct sur la sécurité, car elle évite à un administrateur de les gérer manuellement. Cette fonctionnalité peut être utilisée pour récupérer des listes qui ne sont pas mises à jour ou contrôlées par un administrateur SWA. La possibilité d'ajouter des exceptions individuelles aux adresses téléchargées a été introduite dans AsyncOS Version 11.8.

L'API Office365 est utile pour aider à la prise de décisions stratégiques sur ce service couramment déployé et peut être utilisée pour des applications individuelles (PowerPoint, Skype, Word, etc.). Microsoft recommande de contourner les proxys pour tout le trafic Office365 afin d'optimiser les performances. La documentation Microsoft indique :

⚠ Mise en garde : Alors que SSL Break and Inspect crée la latence la plus importante, d'autres services tels que l'authentification proxy et la recherche de réputation peuvent entraîner des performances médiocres et une mauvaise expérience utilisateur. En outre, ces périphériques réseau de périphérie ont besoin d'une capacité suffisante pour traiter toutes les demandes de connexion réseau. Il est recommandé de contourner votre proxy ou vos périphériques d'inspection pour les requêtes réseau Office 365 directes. Pour plus d'informations, consultez : Gestion des terminaux Microsoft 365.

À partir de la version 11.8 d'AsyncOS, vous pouvez utiliser la liste de catégories dynamique récupérée à partir de l'API Office365 pour remplir la liste des paramètres de contournement. La liste est utilisée pour renvoyer le trafic redirigé vers le périphérique WCCP pour un routage direct. Cependant, il peut être difficile d'utiliser ces conseils dans un environnement de proxy transparent.

Le contournement de tout le trafic Office365 crée un angle mort pour les administrateurs qui ont besoin de contrôles de sécurité de base et de rapports pour le trafic. Si le trafic Office365 n'est pas contourné par SWA, il est important de comprendre les défis techniques spécifiques qui peuvent survenir. L'un d'eux est le nombre de connexions requises par les applications. Le dimensionnement doit être ajusté de manière appropriée pour prendre en charge les connexions TCP supplémentaires requises par les applications Office365. Cela peut augmenter le nombre total de connexions entre 10 % et 15 % de sessions TCP persistantes par utilisateur.

Les actions de déchiffrement et de rechiffrement effectuées par le proxy HTTPS introduisent une faible latence dans les connexions. Les applications Office365 peuvent être sensibles à la latence, et si d'autres facteurs tels que la lenteur des connexions WAN et la disparité des emplacements géographiques viennent compliquer cette situation, l'expérience utilisateur peut en pâtir.

Certaines applications Office365 utilisent des paramètres TLS propriétaires qui empêchent le proxy HTTPS d'établir une connexion avec le serveur d'applications. Cette opération est nécessaire pour valider le certificat ou récupérer le nom d'hôte. Lorsqu'il est combiné à une application telle que Skype Entreprise, cela n'envoie pas de champ d'indication de nom de serveur (SNI) dans le message Hello du client TLS, vous devez contourner entièrement ce trafic. AsyncOS v11.8 a introduit la possibilité de contourner le trafic en fonction de l'adresse IP de destination uniquement, sans vérification de certificat pour répondre à ce scénario.

Moniteurs et alertes

Moniteurs CLI

L'interface de ligne de commande SWA fournit des commandes pour la surveillance en temps réel des processus importants. Certaines commandes utiles affichent des statistiques liées au processus proxy. L'exécution de la commande status detail est une bonne source pour un résumé de l'utilisation des ressources et des mesures de performances, y compris le temps de disponibilité, la bande passante utilisée, la latence de réponse, le nombre de connexions, etc.

Voici un exemple de résultat :

```
SWA_CLI>  status detail

Status as of:                  Fri Nov 11 14:06:52 2022 +03
Up since:                      Fri Apr 08 10:15:00 2022 +03 (217d 3h 51m 52s)
System Resource Utilization:
  CPU                                3.3%
  RAM                                6.2%
  Reporting/Logging Disk            45.6%
Transactions per Second:
  Average in last minute               55
  Maximum in last hour                201
  Average in last hour                 65
  Maximum since proxy restart        1031
  Average since proxy restart          51
Bandwidth (Mbps):
  Average in last minute            4.676
  Maximum in last hour            327.258
  Average in last hour             10.845
  Maximum since proxy restart     1581.297
  Average since proxy restart       11.167
Response Time (ms):
  Average in last minute               635
  Maximum in last hour              376209
  Average in last hour                 605
  Maximum since proxy restart      2602943
  Average since proxy restart          701
Cache Hit Rate:
  Average in last minute                 0
  Maximum in last hour                   2
  Average in last hour                   0
  Maximum since proxy restart           15
  Average since proxy restart            0
Connections:
  Idle client connections              186
  Idle server connections              184
  Total client connections            3499
  Total server connections            3632
SSLJobs:
  In queue Avg in last minute            4
  Average in last minute             45214
  SSLInfo Average in last min           94
```

```
Network Events:
  Average in last minute                   0.0
  Maximum in last minute                    35
  Network events in last min            124502
```

L'exécution de la commande rate affiche des informations en temps réel sur le pourcentage de CPU utilisé par le processus proxy, le nombre de requêtes par seconde (RPS) et les statistiques de cache. Cette commande continue d'interroger et d'afficher de nouvelles sorties jusqu'à interruption. Voici un exemple de résultat :

```
SWA_CLI>  rate

Press Ctrl-C to stop.
  %proxy  reqs                          client    server    %bw  disk  disk
     CPU  /sec   hits blocks misses     kb/sec    kb/sec  saved   wrs   rds
  5.00    51      1    147    370      2283      2268    0.6    48    37
  4.00    36      0    128    237     21695     21687    0.0    47    38
  4.00    48      2    179    307      8168      8154    0.2    65    33
  5.00    53      0    161    372      2894      2880    0.5    48    32
  6.00    52      0    198    328     15110     15100    0.1    63    33
  6.00    77      0    415    363      4695      4684    0.2    48    34
  7.00    85      1    417    433      5270      5251    0.4    49    35
  7.00    67      1    443    228      2242      2232    0.5    85    44
```

L'exécution de la commande tcpservices affiche des informations sur les ports d'écoute de processus sélectionnés. Une explication de chaque processus, de l'adresse et de la combinaison de ports est également affichée :

```
SWA_CLI> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon

Feature Processes
  coeuslogd    - Main WSA controller
  gui          - GUI process
  hermes       - Mail server for sending alerts, etc.
  java         - Processes for storing and querying Web Tracking data
  musd         - AnyConnect Secure Mobility server
  pacd         - PAC file hosting daemon
  prox         - WSA proxy
```

```
  trafmon      - L4 Traffic Monitor
  uds          - User Discovery System (Transparent Auth)
  wccpd        - WCCP daemon

COMMAND      USER         TYPE NODE   NAME
connector    root         IPv4 TCP    127.0.0.1:8823
java         root         IPv6 TCP    [::127.0.0.1]:18081
hybridd      root         IPv4 TCP    127.0.0.1:8833
gui          root         IPv4 TCP    172.16.40.80:8443
ginetd       root         IPv4 TCP    172.16.40.80:ssh
nginx        root         IPv6 TCP    *:4431
nginx        root         IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
api_serve    root         IPv4 TCP    172.16.40.80:6080
api_serve    root         IPv4 TCP    127.0.0.1:60001
api_serve    root         IPv4 TCP    172.16.40.80:6443
chimera      root         IPv4 TCP    127.0.0.1:6380
nectar       root         IPv4 TCP    127.0.0.1:6382
redis-ser    root         IPv4 TCP    127.0.0.1:6383
redis-ser    root         IPv4 TCP    127.0.0.1:6379
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25255
prox         root         IPv4 TCP    127.0.0.1:socks
prox         root         IPv6 TCP    [::1]:socks
prox         root         IPv4 TCP    172.16.11.69:socks
prox         root         IPv4 TCP    172.16.11.68:socks
prox         root         IPv4 TCP    172.16.11.252:socks
prox         root         IPv4 TCP    127.0.0.1:ftp-proxy
prox         root         IPv6 TCP    [::1]:ftp-proxy
prox         root         IPv4 TCP    172.16.11.69:ftp-proxy
```

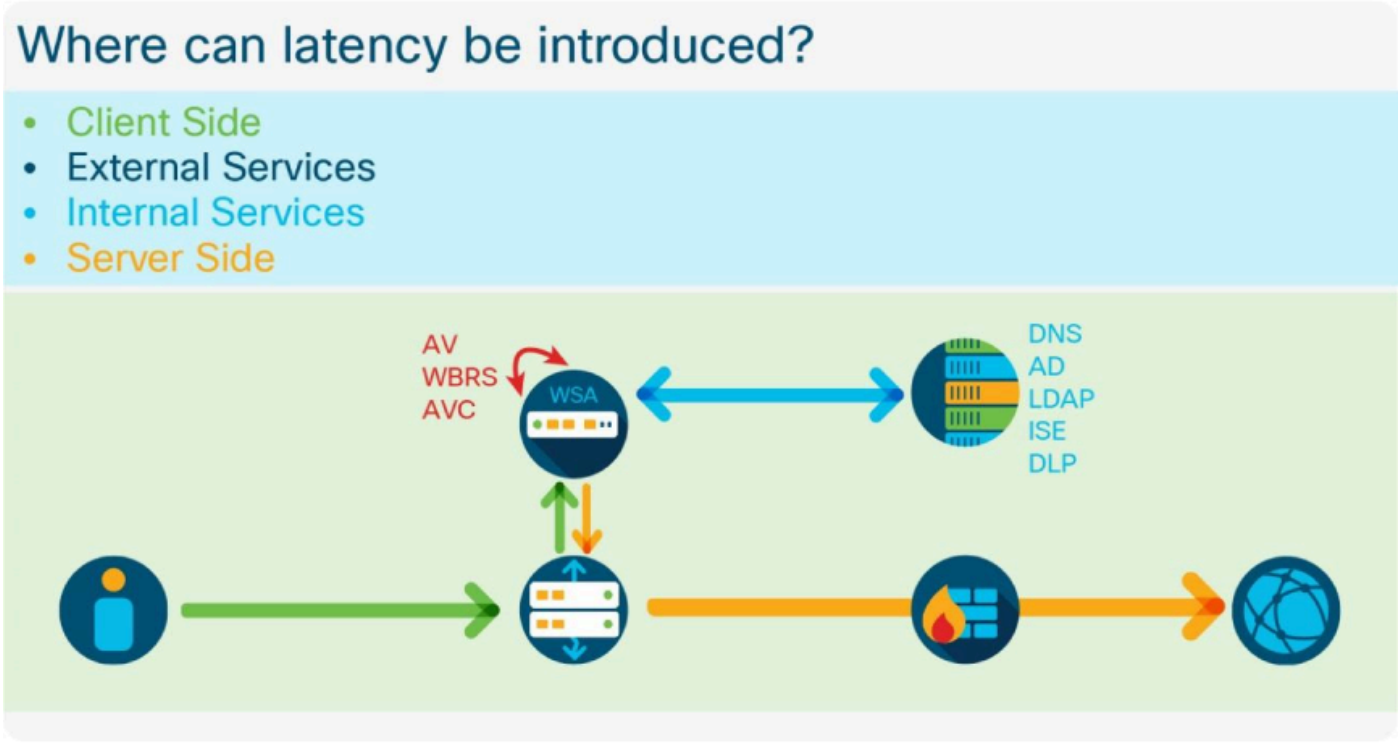
```
prox         root         IPv4 TCP    172.16.11.68:ftp-proxy
prox         root         IPv4 TCP    172.16.11.252:ftp-proxy
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25256
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.21.11.69:https
prox         root         IPv4 TCP    172.21.11.68:https
prox         root         IPv4 TCP    172.21.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25257
smart_age    root         IPv6 TCP    [::127.0.0.1]:65501
smart_age    root         IPv6 TCP    [::127.0.0.1]:28073
interface    root         IPv4 TCP    127.0.0.1:domain
stunnel      root         IPv4 TCP    127.0.0.1:32137
```

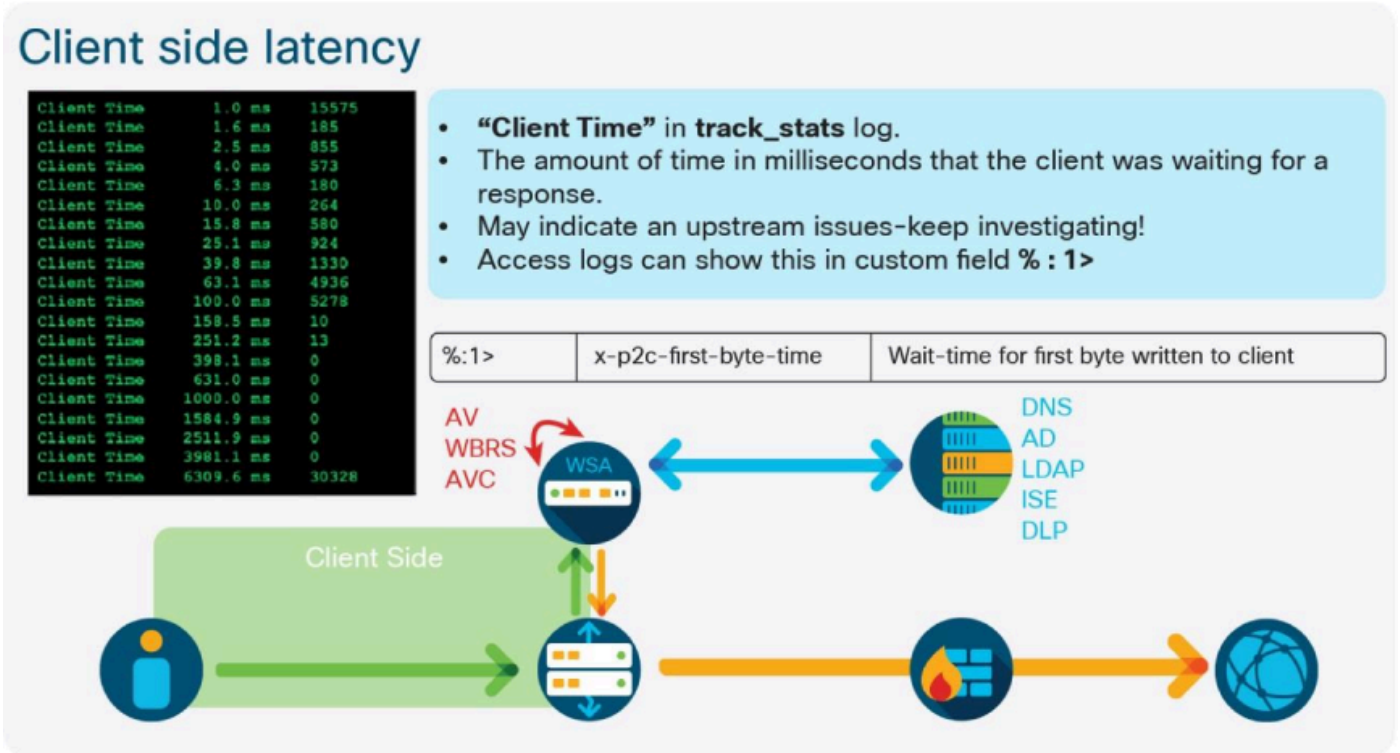
Journalisation

Le trafic Web est très dynamique et varié. Une fois le déploiement d'un proxy terminé, il est important de réévaluer régulièrement la quantité et la composition du trafic transitant par l'appliance. Vous devez vérifier régulièrement (une fois par trimestre) le pourcentage de trafic décrypté pour vous assurer que la taille est conforme aux attentes et aux spécifications de l'installation initiale. Pour ce faire, vous pouvez utiliser un produit de gestion des journaux tel que Advanced Web Security Reporting (AWSR) ou des commandes Bash ou PowerShell avec des journaux d'accès. Le nombre de RPS doit être réévalué régulièrement afin de s'assurer que l'appliance dispose d'une surcharge suffisante pour prendre en compte les pics de trafic et le basculement éventuel dans une configuration à haute disponibilité et à charge équilibrée.

Le journal track_stats est ajouté toutes les cinq minutes et inclut plusieurs sections de sortie

directement liées au processus proxy et à ses objets en mémoire. Dans la surveillance des performances, les processus de demande de latence moyenne, notamment le temps de recherche DNS, le temps d'analyse du moteur antivirus et bien d'autres, sont des champs utiles. Ce journal n'est pas configurable à partir de l'interface utilisateur graphique ou de l'interface de ligne de commande et n'est accessible que via le protocole SCP (Secure Copy Protocol) ou FTP (File Transfer Protocol). Il s'agit d'un journal important à conserver lors du dépannage des performances, car il doit être interrogé fréquemment.



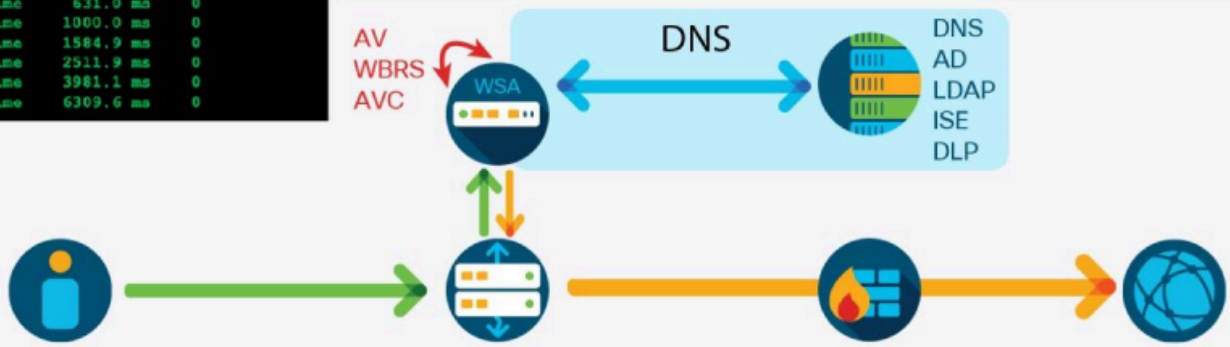


DNS latency

```
DNS Time       1.0 ms    51
DNS Time       1.6 ms    347
DNS Time       2.5 ms    152
DNS Time       4.0 ms    71
DNS Time       6.3 ms    98
DNS Time      10.0 ms    7
DNS Time      15.8 ms    11
DNS Time      25.1 ms    13
DNS Time      39.8 ms    2
DNS Time      63.1 ms    3
DNS Time     100.0 ms    7
DNS Time     158.5 ms    16
DNS Time     251.2 ms    4
DNS Time     398.1 ms    1
DNS Time     631.0 ms    0
DNS Time    1000.0 ms    0
DNS Time    1584.9 ms    0
DNS Time    2511.9 ms    0
DNS Time    3981.1 ms    0
DNS Time    6309.6 ms    0
```

- The amount of time in milliseconds that the WSA waited for a DNS response.
- Calls for investigation for your DNS resolvers (or path to them).
- **access logs** can show this in custom field **% : >d**

%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS Process to send a DNS result to ehe Web proxy.

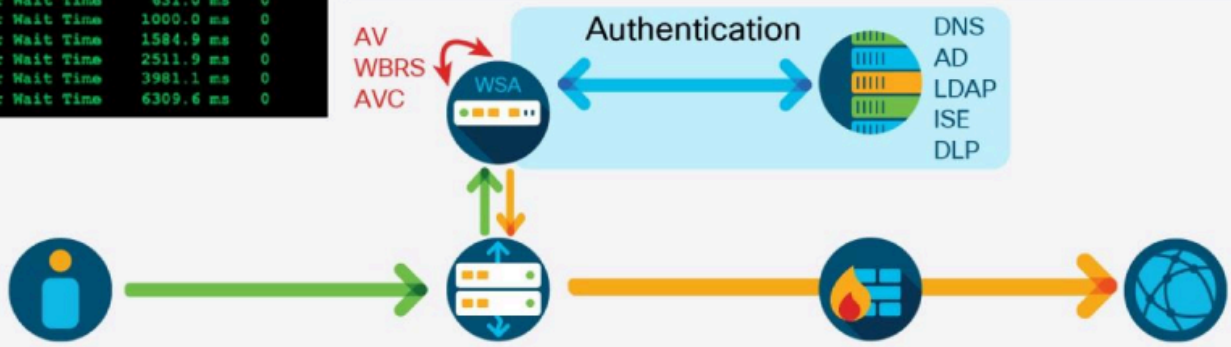


Authentication latency

```
Server Wait Time       1.0 ms    0
Server Wait Time       1.6 ms    0
Server Wait Time       2.5 ms    0
Server Wait Time       4.0 ms    0
Server Wait Time       6.3 ms    0
Server Wait Time      10.0 ms    0
Server Wait Time      15.8 ms    0
Server Wait Time      25.1 ms    0
Server Wait Time      39.8 ms    0
Server Wait Time      63.1 ms    0
Server Wait Time     100.0 ms    0
Server Wait Time     158.5 ms    1
Server Wait Time     251.2 ms    1
Server Wait Time     398.1 ms    0
Server Wait Time     631.0 ms    0
Server Wait Time    1000.0 ms    0
Server Wait Time    1584.9 ms    0
Server Wait Time    2511.9 ms    0
Server Wait Time    3981.1 ms    0
Server Wait Time    6309.6 ms    0
```

- There are two metrics: **“Auth Helper Wait Time”** and **“Auth Helper Service Wait Time.”**
- Use the first to get pure auth time without the request time added.
- **access logs** can show this in custom field **% : >a**

%:<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.

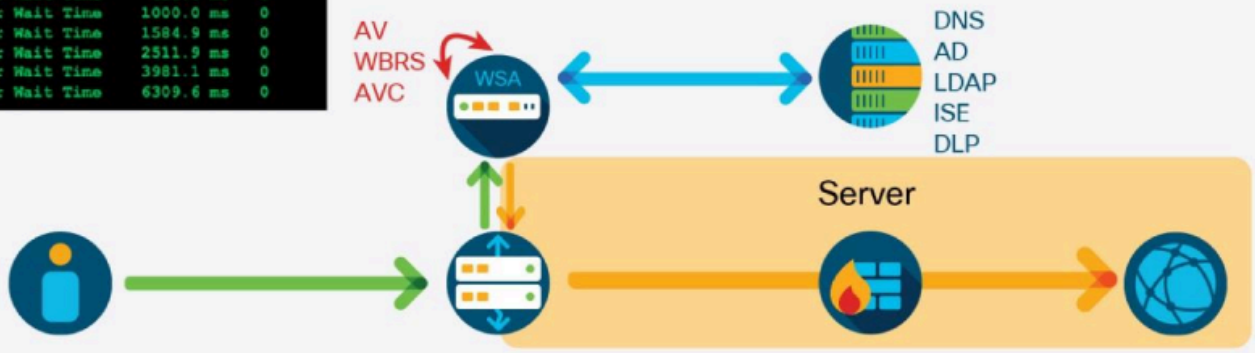


Server latency-wait time

```
Server Wait Time        1.0 ms    0
Server Wait Time        1.6 ms    0
Server Wait Time        2.5 ms    0
Server Wait Time        4.0 ms    0
Server Wait Time        6.3 ms    0
Server Wait Time       10.0 ms    0
Server Wait Time       15.8 ms    0
Server Wait Time       25.1 ms    0
Server Wait Time       39.8 ms    0
Server Wait Time       63.1 ms    0
Server Wait Time      100.0 ms    0
Server Wait Time      158.5 ms    1
Server Wait Time      251.2 ms    1
Server Wait Time      398.1 ms    0
Server Wait Time      631.0 ms    0
Server Wait Time     1000.0 ms    0
Server Wait Time     1584.9 ms    0
Server Wait Time     2511.9 ms    0
Server Wait Time     3981.1 ms    0
Server Wait Time     6309.6 ms    0
```

- The amount of time in milliseconds that the WSA waited for the first byte of the server response.
- Calls for investigation of your upstream devices and WAN connection.
- **access logs** can show this in custom field **% : >1**

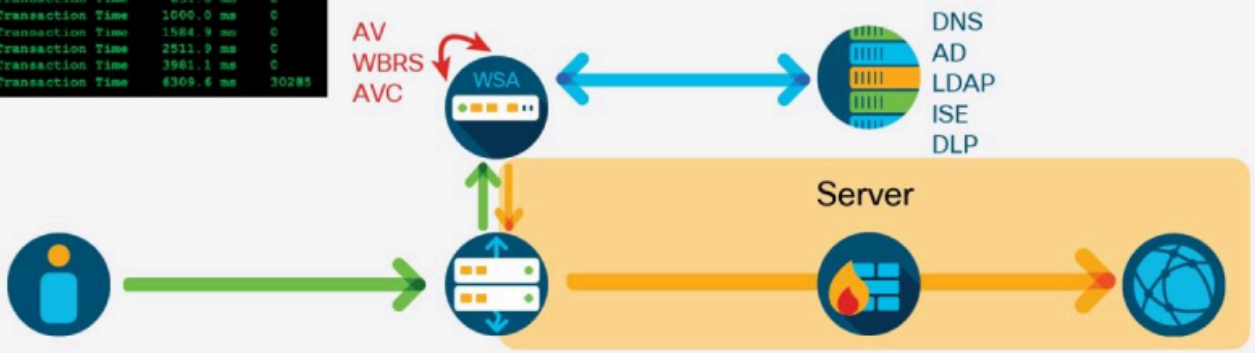
%:>1	x-s2p-first-byte-time	Wait-time for first response byte from server

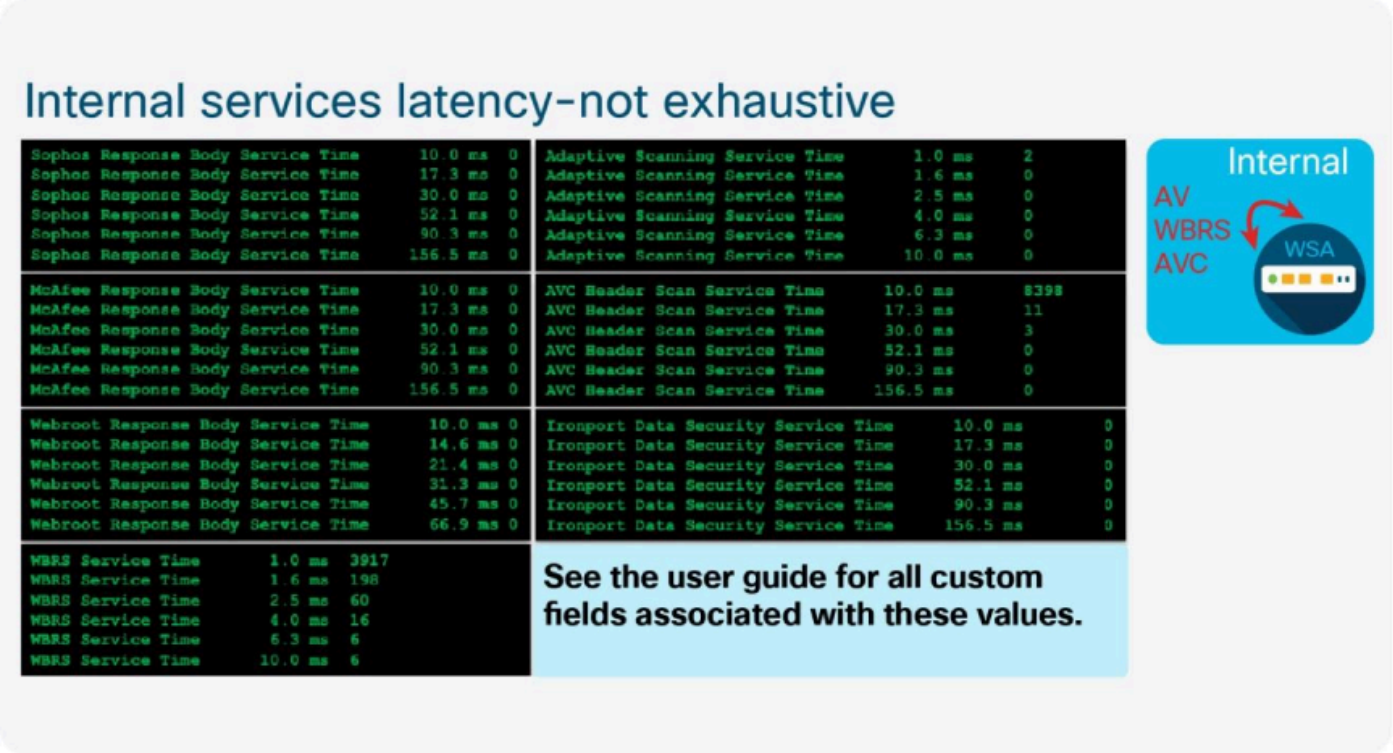


Server latency-transaction time

```
Server Transaction Time        1.0 ms    1422
Server Transaction Time        1.6 ms    858
Server Transaction Time        2.5 ms    1035
Server Transaction Time        4.0 ms    1106
Server Transaction Time        6.3 ms    758
Server Transaction Time       10.0 ms    810
Server Transaction Time       15.8 ms    288
Server Transaction Time       25.1 ms    45
Server Transaction Time       39.8 ms    73
Server Transaction Time       63.1 ms    4221
Server Transaction Time      100.0 ms    8897
Server Transaction Time      158.5 ms    5
Server Transaction Time      251.2 ms    0
Server Transaction Time      398.1 ms    2
Server Transaction Time      631.0 ms    0
Server Transaction Time     1000.0 ms    0
Server Transaction Time     1584.9 ms    0
Server Transaction Time     2511.9 ms    0
Server Transaction Time     3981.1 ms    0
Server Transaction Time     6309.6 ms    30285
```

- The amount of time in milliseconds for the entire server-side transaction to complete.
- Calls for investigation of your upstream devices and WAN connection.
- No **access logs** custom field, but can be determined by a combinationof them.





Une ligne de journal SHD individuelle est écrite toutes les 60 secondes et contient des champs importants pour la surveillance des performances, notamment la latence, le RPS, le nombre total de connexions côté client et côté serveur. Voici un exemple de ligne de journal SHD :

```
Fri Nov 11 14:16:42 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 62 Band 11383 Latency 61
Fri Nov 11 14:17:42 2022 Info: Status: CPULd 2.6 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 10532 Latency 77
Fri Nov 11 14:18:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.6 Reqs 48 Band 7285 Latency 579
Fri Nov 11 14:19:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.6 Reqs 52 Band 34294 Latency 79
Fri Nov 11 14:20:43 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 8696 Latency 691
Fri Nov 11 14:21:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 49 Band 7064 Latency 140
Fri Nov 11 14:22:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.8 Reqs 41 Band 5444 Latency 788
Fri Nov 11 14:23:43 2022 Info: Status: CPULd 2.2 DskUtil 45.7 RAMUtil 6.8 Reqs 48 Band 6793 Latency 820
Fri Nov 11 14:24:44 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 44 Band 8735 Latency 673
Fri Nov 11 14:25:44 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 53 Band 8338 Latency 731
```

Des champs personnalisés supplémentaires peuvent être ajoutés aux access_logs pour indiquer les informations de latence des demandes individuelles. Ces champs incluent la réponse du serveur, la résolution DNS et la latence de l'analyseur antivirus. Les champs doivent être ajoutés au journal pour obtenir des informations utiles pour le dépannage. Il s'agit de la chaîne de champ personnalisée recommandée à utiliser :

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms)
```

Les informations de performances dérivées de ces valeurs sont répertoriées dans le tableau :

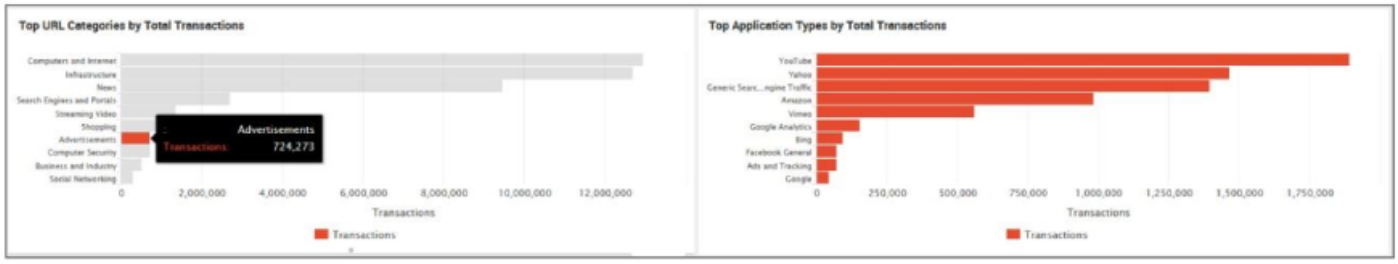
Champ personnalisé	Description
% : <a	Temps d'attente pour recevoir la réponse du processus d'authentification du proxy Web après que le proxy Web ait envoyé la demande.
% : <b	Temps d'attente pour écrire un corps de requête sur le serveur après l'en-tête.
% : <d	Temps d'attente pour recevoir la réponse du processus DNS du proxy Web après que le proxy Web a envoyé la demande.
% : <h	Temps d'attente pour écrire un en-tête de requête sur le serveur après le premier octet.
% : <r	Temps d'attente pour recevoir la réponse des filtres de réputation de sites Web après que le proxy Web ait envoyé la demande.
% : <s	Temps d'attente pour recevoir le verdict du processus anti-spyware du proxy Web après que le proxy Web ait envoyé la requête.
% : >	Temps d'attente du premier octet de réponse du serveur.
%:>a	Temps d'attente pour recevoir la réponse du processus d'authentification du proxy Web. Inclut le temps nécessaire au proxy Web pour envoyer la demande.
%:>b	Temps d'attente du corps de réponse complet après réception de l'en-tête.
%:>c	Temps nécessaire au proxy Web pour lire une réponse à partir du cache disque.
%:>d	Temps d'attente pour recevoir la réponse du processus DNS du proxy Web. Inclut le temps nécessaire au proxy Web pour envoyer la demande.
%:>h	Temps d'attente de l'en-tête du serveur après le premier octet de réponse.
%:>r	Délai d'attente pour recevoir le verdict des filtres de réputation Web. Inclut le temps nécessaire au proxy Web pour envoyer la demande.
%:>s	Délai d'attente pour recevoir le verdict du processus antispyware du proxy Web. Inclut le temps nécessaire au proxy Web pour envoyer la demande.
%:1<	Temps d'attente du premier octet de requête d'une nouvelle connexion client.
%:1>	Temps d’attente du premier octet écrit sur un client.
% : b<	Temps d'attente pour un corps de client complet.
%:b>	Temps d'attente pour le corps complet écrit sur un client.
%:e>	Temps d'attente pour recevoir la réponse du moteur d'analyse AMP après l'envoi de la requête par le proxy Web.
% : e<	Temps d'attente pour recevoir le verdict du moteur d'analyse AMP. Inclut le temps nécessaire au proxy Web pour envoyer la demande.
% : h<	Temps d'attente de l'en-tête client complet après le premier octet.
%:h>	Temps d'attente pour l'en-tête complet écrit sur un client.
%:m<	Délai d'attente pour recevoir le verdict du moteur d'analyse McAfee. Inclut le

	temps nécessaire au proxy Web pour envoyer la demande.
%:m>	Délai d'attente pour recevoir la réponse du moteur d'analyse McAfee. Une fois que le proxy Web a envoyé la demande.
%F	Port source du client.
%p	Port du serveur Web.
%k	Adresse IP de la source de données (adresse IP du serveur Web).
% : w<	Temps d'attente pour recevoir le verdict du moteur d'analyse webroot. Inclut le temps nécessaire au proxy Web pour envoyer la demande.
%:w>	Temps d'attente pour recevoir la réponse du moteur d'analyse webroot. Une fois que le proxy Web a envoyé la demande.

Le modèle de licence SWA permet de réutiliser les licences d'appareils physiques pour les appareils virtuels. Vous pouvez en tirer parti et déployer des appliances SWAv de test à utiliser dans un environnement de travaux pratiques. De nouvelles fonctionnalités et configurations peuvent être testées pour garantir la stabilité et la fiabilité sans enfreindre les conditions de licence.

Rapports de sécurité Web avancés (AWSR)

La fonction AWSR doit être exploitée pour garantir la génération de rapports à partir de SWA, en particulier dans les environnements où de nombreux SWA sont déployés. Cette solution est plus évolutive que l'utilisation de rapports centralisés sur un appareil de gestion de la sécurité (SMA) et fournit des attributs de rapports personnalisés qui ajoutent profondeur et personnalisation à vos données. Les rapports peuvent être regroupés et personnalisés pour répondre aux besoins de n'importe quelle entreprise. Cisco Advanced Services Group doit être optimisé en termes de dimensionnement pour AWSR.



Alertes par e-mail

Le système d'alerte par e-mail intégré sur SWA est mieux exploité comme système d'alerte de base. Il doit être adapté de manière appropriée pour répondre aux besoins de l'administrateur, car il peut être bruyant si tous les événements d'information sont activés. Il est important de limiter les alertes et de les surveiller activement, plutôt que de tout signaler et de les ignorer comme spam.

Paramètres d'alerte	Configuration
Adresse d'expéditeur à utiliser lors de l'envoi d'alertes.	Généré automatiquement
Nombre initial de secondes à attendre avant d'envoyer une alerte en double.	300 secondes
Nombre maximal de secondes à attendre avant d'envoyer une alerte en double.	3 600 secondes

Surveillance de disponibilité

Deux méthodes peuvent être utilisées pour surveiller la disponibilité d'un proxy Web.

1. La première est la surveillance de couche 3 (L3), qui teste si l'adresse IP de l'appliance est accessible sur le réseau. La façon la plus simple de tester cela est d'envoyer une requête d'écho ICMP (ping) à l'adresse à intervalles réguliers et de vérifier la présence d'un paquet de réponse. Les attributs de la réponse, tels que la durée de vie et la latence, peuvent être analysés pour déterminer l'état de santé de la couche réseau.
2. Il est possible qu'un périphérique réponde aux requêtes ping, mais les processus proxy ne répondent pas ou sont intermittents. Dans ce cas, il est conseillé d'ajouter un moniteur de couche 7 (L7) qui envoie une requête proxy explicite à l'appliance et attend un code de réponse HTTP 200 OK. Ceci teste l'accessibilité de l'interface réseau, la réactivité des services proxy et la viabilité des services en amont si une ressource externe est demandée. Ce type de surveillance prend généralement la forme d'une requête HTTP HEAD explicite qui demande au proxy de se connecter à une ressource. La méthode HEAD demande le renvoi des en-têtes et le client doit envoyer une requête GET. Cela inclut uniquement les en-têtes de réponse sans données.
    - Si vous utilisez un script ou un outil de surveillance de couche 7, assurez-vous que le trafic est exempt d'authentification. Dans le cas contraire, cela entraîne des échecs d'authentification et une consommation des ressources. Lorsque vous utilisez une chaîne utilisateur-agent personnalisée dans l'outil de surveillance, elle doit être utilisée pour identifier le trafic. Bien que le trafic soit exempté de l'authentification, il peut toujours être restreint de l'accès inutile à Internet par le biais des stratégies d'accès.

Lorsque vous utilisez une ou plusieurs de ces méthodes, un administrateur doit établir une ligne de base de mesures acceptables autour de la réponse proxy et l'utiliser pour créer des seuils d'alerte.

Surveillance SNMP

Le protocole SNMP (Simple Network Management Protocol) est la principale méthode de surveillance de l'état de l'appliance. Il peut être utilisé pour recevoir des alertes de l'appliance

(déroutements) ou pour interroger divers identificateurs d'objet (OID) afin de collecter des informations. Il existe de nombreux OID disponibles sur le SWA qui détaillent l'utilisation du matériel aux ressources, aux processus individuels et aux informations statistiques.

Un certain nombre de bases MIB (Machine Information Base) spécifiques doivent être surveillées pour des raisons liées au matériel et aux performances. Reportez-vous à la liste complète des MIB.

Voici une liste des MIB recommandées à surveiller :

OID matériel	Nom
1.3.6.1.4.1.15497.1.1.1.18.1.3	IDraid
1.3.6.1.4.1.15497.1.1.1.18.1.2	ÉtatRaid
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError
1.3.6.1.4.1.15497.1.1.1.10	fanTable
1.3.6.1.4.1.15497.1.1.1.9.1.2	degrés Celsius

Ces OID correspondent directement à la sortie de la commande CLI status detail :

OID	Nom	Champ Détails du statut
Ressources système		
1.3.6.1.4.1.15497.1.1.1.2.0	PourcentageUtilisationUC	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	PourcentageUtilisationMémoire	BÉLIER
Transactions par seconde		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheDébitMaintenant	Nombre moyen de transactions par seconde au cours de la dernière minute.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheDébit1hPic	Nombre maximal de transactions par seconde au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheDébit1hMoyenne	Nombre moyen de transactions par seconde au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheDuréeDébitMaximale	Nombre maximal de transactions par seconde depuis le redémarrage du proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheMoyenneDuréeDébit	Nombre moyen de transactions par seconde depuis le redémarrage du

		proxy.
Bande passante		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalMaintenant	Bande passante moyenne de la dernière minute.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hPic	Bande passante maximale au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hMoyenne	Bande passante moyenne au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBasseDuréeTotalePic	Bande passante maximale depuis le redémarrage du proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBasseMoyenneDuréeTotale	Bande passante moyenne depuis le redémarrage du proxy.
Temps de réponse		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	Taux moyen d'accès au cache au cours de la dernière minute.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	Taux d'accès maximal au cache au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	Taux moyen d'accès au cache au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheNombreAtteintesMaximumVie	Taux de succès maximal du cache depuis le redémarrage du proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheMoyenneDuréeRésultats	Taux moyen d'accès au cache depuis le redémarrage du proxy.
Taux d'accès au cache		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	Taux moyen d'accès au cache au cours de la dernière minute.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	Taux d'accès maximal au cache au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	Taux moyen d'accès au cache au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheNombreAtteintesMaximumVie	Taux de succès maximal du cache depuis le redémarrage du proxy.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheMoyenneDuréeRésultats	Taux moyen d'accès au

		cache depuis le redémarrage du proxy.
Connexions		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientInactivitéConnexions	Connexions client inactives.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServeurConnexionsInactives	Connexions serveur inactives.
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConnexions	Nombre total de connexions client.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheTotalConnexionsServeur	Nombre total de connexions serveur.

Autres informations utiles

Configurer le pare-feu pour l'appliance Web sécurisée

Comprendre les journaux d'accès sécurisés des appliances Web

Installer l'appliance Web sécurisée sur Vmware Esxi

Installer l'appliance Web sécurisée sur Microsoft Hyper-V

Migration de la configuration entre deux SWA

Rétablir la version précédente de l'appliance Web sécurisée

Configurer la sauvegarde dans l'appliance Web sécurisée

Configurer l'authentification Active Directory dans SWA

Configurer l'authentification unique Kerberos dans SWA

Contourner l'authentification dans l'appliance Web sécurisée

Bloquer le téléchargement de fichiers exécutables dans SWA

Configurer la restriction du service partagé Microsoft O365 dans SWA

Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée

Activer une chaîne/vidéo YouTube spécifique et bloquer le reste de YouTube dans SWA

Configurer des catégories d'URL personnalisées dans Secure Web Appliance

Configurer le proxy en amont dans l'appliance Web sécurisée

Configuration et dépannage du protocole SNMP dans SWA

Dépannage du service DNS de l'appliance Web sécurisée

Configurer la capture de paquets sur l'appliance de sécurité du contenu

Accéder aux journaux de l'appliance Web sécurisée

Configurer le paramètre de performance dans les journaux d'accès

Dépannage des performances de l'appliance Web sécurisée avec les journaux SHD

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.