

Guide de conception des appareils de sécurité Web

Contenu

[Introduction](#)

[Informations générales](#)

[Conception](#)

[Réseau](#)

[Considérations générales](#)

[Équilibrage de charge](#)

[Pare-feu](#)

[Identités](#)

[Politiques d'accès/de déchiffrement/de routage/de programmes malveillants sortants](#)

[Catégories d'URL personnalisées](#)

[Antiprogrammes malveillants et réputation](#)

Introduction

Ce document décrit comment concevoir l'appareil de sécurité Web Cisco (WSA) et les composants associés pour des performances optimales.

Informations générales

Lorsque vous concevez une solution pour le WSA, elle nécessite une attention particulière, non seulement en ce qui concerne la configuration de l'appareil elle-même, mais aussi les périphériques réseau associés et leurs fonctionnalités. Chaque réseau est une collaboration de plusieurs périphériques. Si l'un d'eux ne participe pas correctement au réseau, l'expérience utilisateur peut alors diminuer.

Deux composants principaux doivent être pris en compte lors de la configuration du WSA : le matériel et le logiciel. Le matériel se décline en deux types différents. Le premier est le type physique de matériel, tels que les modèles des séries S170, S380 et S680, ainsi que d'autres modèles de fin de vie (EoL), tels que les modèles des séries S160, S360, S660, S370 et S670. L'autre type de matériel est virtuel, par exemple les modèles des gammes S000v, S100v et S300v. Le système d'exploitation (OS) qui s'exécute sur ce matériel s'appelle *AsyncOS pour Web*, qui est basé sur FreeBSD à son cœur.

Le WSA offre un service proxy et analyse, inspecte et classe l'ensemble du trafic (HTTP, HTTPS et FTP). Tous ces protocoles s'exécutent au-dessus du protocole TCP et dépendent fortement du système de noms de domaine (DNS) pour fonctionner correctement. Pour ces raisons, l'intégrité du réseau est essentielle au bon fonctionnement de l'appareil et à sa communication avec différentes parties du réseau, à l'intérieur et à l'extérieur du contrôle de l'entreprise.

Conception

Utilisez les informations décrites dans cette section afin de concevoir le WSA et les composants associés pour des performances optimales.

Réseau

Un réseau rapide et sans erreur est essentiel au bon fonctionnement du WSA. Si le réseau est instable, l'expérience utilisateur peut diminuer. Les problèmes réseau sont généralement détectés lorsque les pages Web prennent plus de temps à atteindre ou sont inaccessibles. L'inclinaison initiale est la faute de l'appareil, mais c'est généralement le réseau qui se comporte mal. Par conséquent, il convient d'examiner et d'auditer attentivement le réseau afin de s'assurer qu'il offre le meilleur service pour les protocoles d'application de haut niveau tels que HTTP, HTTPS, FTP et DNS.

Considérations générales

Voici quelques considérations générales que vous pouvez mettre en oeuvre afin de garantir le meilleur comportement du réseau :

- Assurez-vous que le réseau de couche 2 (L2) est stable, que le fonctionnement du Spanning Tree est correct et qu'il n'y a pas de calculs Spanning Tree fréquents ni de modifications de topologie.
- Le protocole de routage utilisé doit également fournir une convergence et une stabilité rapides. Les temporisateurs rapides OSPF (Open Shortest Path First) ou EIGRP (Enhanced Interior Gateway Routing Protocol) sont de bons choix pour un tel réseau.
- Toujours utiliser au moins deux interfaces de données sur le WSA : l'une faisant face aux ordinateurs de l'utilisateur final et l'autre pour l'opération sortante (connectée au proxy en amont ou à Internet). Cela permet d'éliminer les contraintes de ressources possibles, par exemple lorsque le nombre de ports TCP est épuisé ou lorsque les tampons réseau deviennent saturés (avec l'utilisation d'une interface unique pour l'intérieur et l'extérieur en particulier).
- Dédiez l'interface de gestion pour le trafic de gestion uniquement afin d'améliorer la sécurité. Afin d'y parvenir via l'interface utilisateur graphique, accédez à **Réseau > Interfaces** et cochez la case **Routage séparé (port M1 limité aux services de gestion des appliances uniquement)**.
- Utilisez des serveurs DNS rapides. Toute transaction via le WSA nécessite au moins une recherche DNS (si ce n'est dans le cache). Un serveur DNS qui est lent ou se comporte mal affecte toute transaction et est observé comme une connectivité Internet lente ou retardée.
- Lorsque des tables de routage distinctes sont utilisées, ces règles s'appliquent :

Toutes les interfaces sont incluses dans la table de routage *Management* par défaut (M1, P1, P2).

Seules interfaces de données sont incluses dans la table de routage *des données*.

Note: La séparation des tables de routage n'est pas par interface, mais par service. Par

exemple, le trafic entre le WSA et le contrôleur de domaine Microsoft Active Directory (AD) obéit toujours aux routes spécifiées dans la table de routage de gestion, et il est possible de configurer des routes qui pointent vers l'interface P1/P2 dans cette table. Il n'est pas possible d'inclure des routes dans la table de routage de données qui utilisent les interfaces de gestion.

Équilibrage de charge

Voici quelques considérations d'équilibrage de charge que vous pouvez mettre en oeuvre afin d'assurer le meilleur comportement du réseau :

- Rotation DNS : terme utilisé lorsqu'un nom d'hôte unique est utilisé comme proxy, mais qu'il comporte plusieurs enregistrements A sur le serveur DNS. Chaque client résout ce problème à une adresse IP différente et utilise des proxies différents. Une limitation est que les modifications des enregistrements DNS sont répercutées sur les clients lors du redémarrage (mise en cache DNS locale), de sorte qu'il offre un faible niveau de robustesse si une modification doit être effectuée. Cependant, ceci est transparent pour les utilisateurs finaux.
- Fichiers PAC (Proxy Address Control) : il s'agit de fichiers de script automatique par proxy qui déterminent la manière dont chaque URL doit être gérée sur un navigateur en fonction des fonctions écrites qu'il contient. Il a la fonction de transférer la même URL toujours directement ou au même proxy.
- Détection automatique : décrit l'utilisation des méthodes DNS/DHCP afin d'obtenir des fichiers PAC (décrits dans la précédente analyse). Généralement, ces trois premières considérations sont combinées en une seule solution. Cependant, cela peut être compliqué et de nombreux agents utilisateurs, tels que Microsoft Office, Adobe Downloader, Javascripts et Flash, ne peuvent pas du tout lire les fichiers PAC.
- Web Cache Control Protocol (WCCP) : ce protocole (en particulier WCCP version 2) fournit un moyen robuste et très puissant de créer un équilibrage de charge entre plusieurs WSA et d'incorporer également une haute disponibilité.
- Distincts dispositifs d'équilibrage de charge : Cisco vous recommande d'utiliser des équilibreurs de charge comme machines dédiées.

Pare-feu

Voici quelques considérations de pare-feu que vous pouvez mettre en oeuvre afin d'assurer le meilleur comportement du réseau :

- Assurez-vous que le protocole ICMP (Internet Control Message Protocol) est autorisé sur l'ensemble du réseau à partir de chaque source. Ceci est essentiel, car le WSA dépend du mécanisme de détection MTU (Maximum Transition Unit) du chemin, comme décrit dans [RFC 1191](#), qui dépend des requêtes Echo ICMP (type $\diamond\diamond$ et réponses Echo (type 0), et ICMP unreachable-fragmentation est requis (type 3, code 4). Si vous désactivez la découverte MTU de chemin sur le WSA avec la commande CLI `pathmtudiscovery`, le WSA utilise la MTU par défaut de 576 octets, conformément à la [RFC 879](#). Cela affecte les performances en raison

d'une surcharge accrue et d'un réassemblage de paquets.

- Assurez-vous qu'il n'y a pas de routage asymétrique à l'intérieur du réseau. Bien qu'il ne s'agisse pas d'un problème sur le WSA, tout pare-feu rencontré le long du chemin abandonne les paquets car il n'a pas reçu les deux côtés de la communication.
- Avec les pare-feu, il est très important d'exclure les adresses IP WSA des menaces en tant que stations d'ordinateurs finaux ordinaires. Le pare-feu peut bloquer
- les adresses IP WSA en raison d'un trop grand nombre de connexions (selon les connaissances générales du pare-feu).
- Si la traduction d'adresses réseau (NAT) est utilisée pour toute adresse IP WSA sur le périphérique du client, assurez-vous que chaque WSA utilise une adresse globale externe distincte dans la NAT. Si vous utilisez NAT pour plusieurs WSA qui ont une adresse globale externe unique, vous pourriez rencontrer ces problèmes :

Toutes les connexions de tous les WSA au monde extérieur utilisent une adresse globale externe unique et le pare-feu manque rapidement de ressources.

En cas de pic de trafic vers cette destination unique, le serveur de destination peut la bloquer et empêcher toute l'entreprise d'accéder à cette ressource. Il peut s'agir d'une ressource précieuse comme le stockage cloud de l'entreprise, les connexions au cloud d'Office ou les mises à jour logicielles antivirus par ordinateur.

Identités

N'oubliez pas que le principe *logique AND* s'applique à toutes les composantes de l'identité. Par exemple, si vous configurez à la fois l'agent utilisateur et l'adresse IP, cela signifie l'agent utilisateur *à partir de* cette adresse IP. Cela ne signifie pas l'agent utilisateur *ni* cette adresse IP.

Utilisez une identité pour l'authentification du même type de substitution (ou pas de substitution) et/ou de l'agent utilisateur.

Il est important de s'assurer que chaque identité nécessitant une authentification inclut les chaînes d'agent utilisateur pour les navigateurs/agents utilisateur connus qui prennent en charge l'authentification par proxy, tels qu'Internet Explorer, Mozilla Firefox et Google Chrome. Certaines applications nécessitent un accès Internet mais ne prennent pas en charge l'authentification par proxy/WWW.

Les identités sont associées de haut en bas avec la recherche de correspondances qui se termine sur la première entrée correspondante. Pour cette raison, si vous avez configuré *Identité 1* et *Identité 2* et qu'une transaction correspond à Identité 1, elle n'est pas cochée sur Identité 2.

Politiques d'accès/de déchiffrement/de routage/de programmes malveillants sortants

Ces stratégies sont appliquées à différents types de trafic :

- Les politiques d'accès sont appliquées aux connexions HTTP ou FTP ordinaires. Ils

déterminent si la transaction doit être acceptée ou abandonnée.

- Les politiques de déchiffrement déterminent si les transactions HTTPS doivent être décryptées, abandonnées ou transmises. Si la transaction est déchiffrée, la partie consécutive de celle-ci peut être vue comme une requête HTTP simple et est comparée aux stratégies Access. Si vous devez supprimer une demande HTTPS, supprimez-la dans les stratégies de déchiffrement, et non dans les stratégies d'accès. Sinon, il consomme plus de CPU et de mémoire pour qu'une transaction abandonnée soit d'abord déchiffrée puis abandonnée.
- Les politiques de routage déterminent la direction en amont d'une transaction une fois qu'elle est autorisée par le WSA. Cela s'applique s'il existe des proxy en amont ou si le WSA est en mode *Connecteur* et envoie le trafic vers la tour de sécurité Web du cloud.
- Les politiques de programmes malveillants sortants sont appliquées aux téléchargements HTTP ou FTP des utilisateurs finaux vers les serveurs Web. Ceci est généralement vu comme une requête HTTP Post.

Pour chaque type de politique, il est important de se rappeler que le principe *OR logique* s'applique. Si plusieurs identités sont référencées, la transaction doit correspondre à l'une des identités configurées.

Pour un contrôle plus précis, utilisez ces stratégies. Les identités mal configurées par stratégie peuvent créer des problèmes, où il est plus avantageux d'utiliser plusieurs identités référencées dans une stratégie. N'oubliez pas que les identités n'affectent pas le trafic, elles identifient simplement les types de trafic pour les correspondances ultérieures dans une stratégie.

Souvent, les stratégies de déchiffrement utilisent des identités avec authentification. Bien que cela ne soit pas faux et soit parfois nécessaire, l'utilisation d'une identité avec authentification référencée dans la stratégie de déchiffrement signifie que toutes les transactions qui correspondent à la stratégie de déchiffrement sont déchiffrées afin que l'authentification ait lieu. L'action de déchiffrement peut être abandonnée ou transmise, mais comme il y a une identité avec authentification, le déchiffrement a lieu afin d'abandonner ou de passer par le trafic ultérieurement. C'est coûteux et il faut éviter cela.

Certaines configurations contiennent 30 identités ou plus et 30 stratégies Access ou plus, où toutes les stratégies Access incluent toutes les identités. Dans ce cas, il n'est pas nécessaire d'utiliser ces nombreuses identités si elles sont associées dans toutes les politiques d'accès. Bien que cela ne nuise pas au fonctionnement de l'appareil, cela crée de la confusion avec les tentatives de dépannage et coûte cher en termes de performances.

Catégories d'URL personnalisées

L'utilisation de catégories d'URL personnalisées est un outil puissant sur le WSA qui est généralement mal compris et mal utilisé. Par exemple, il existe des configurations qui contiennent tous les sites vidéo pour les correspondances dans l'identité. Le WSA dispose d'un outil intégré qui se met automatiquement à jour lorsque les sites vidéo changent d'URL, ce qui se produit fréquemment. Ainsi, il est logique de permettre au WSA de gérer automatiquement les catégories d'URL et d'utiliser les catégories d'URL personnalisées pour les sites spéciaux non encore classés.

Faites très attention avec les expressions régulières. Si des caractères spéciaux tels que dot (.) et

star (*) sont utilisés, ils peuvent s'avérer très importants en termes de CPU et de mémoire. Le WSA étend toute expression régulière pour la faire correspondre à chaque transaction. Par exemple, voici une expression régulière :

`example.*`

Cette expression correspond à toute URL qui contient le mot *exemple*, pas seulement le domaine *exemple.com*. Évitez l'utilisation de *point* et *étoile* dans les expressions régulières et utilisez-les uniquement en dernier recours.

Voici un autre exemple d'expression régulière qui pourrait créer des problèmes :

`www.example.com`

Si vous utilisez cet exemple dans le champ Expressions régulières, il ne correspond pas seulement à www.example.com, mais aussi à www.www3example2com.com, car le point ici signifie *n'importe quel caractère*. Si vous souhaitez faire correspondre uniquement www.example.com, évitez le point :

`www\.example\.com`

Dans ce cas, il n'y a aucune raison d'utiliser la fonction Expressions régulières lorsque vous pouvez inclure ceci dans le domaine de catégorie d'URL personnalisé avec ce format :

`www.example.com`

Antiprogrammes malveillants et réputation

Si plusieurs moteurs d'analyse sont activés, envisagez également d'activer l'analyse adaptative. L'analyse adaptative est un moteur puissant mais de petite taille sur le WSA qui analyse chaque requête au préalable et détermine le moteur complet qui doit être utilisé pour analyser les requêtes. Cela augmente légèrement les performances sur le WSA.