Guide de conception d'appareils de sécurité Web

Contenu

Introduction

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

Informations générales

Quand vous concevez une solution pour le WSA, il exige la prise en considération soigneuse, non seulement en vue de la configuration de l'appliance elle-même, mais également les périphériques associés de réseau et leurs caractéristiques. Chaque réseau est une Collaboration de plusieurs périphériques, et si l'un d'entre eux ne participe pas correctement au réseau, alors d'expériences utilisateur pourrait refuser.

Il y a deux composants principaux qui doivent être considérés quand vous configurez le WSA : le matériel et le logiciel. Le matériel est livré dans deux types différents. Le premier est le type physique de matériel, tel que les modèles S170, S380, et de gamme S680, aussi bien que toute autre extrémité des modèles de vie (EoL), tels que les modèles S160, S360, S660, S370, et de gamme S670. L'autre type de matériel est virtuel, comme les modèles de gamme S000v, S100v, et S300v. Le système d'exploitation (SYSTÈME D'EXPLOITATION) ces passages sur ce matériel s'appelle *AsyncOS pour le Web*, qui est basé sur le FreeBSD à son noyau.

Le WSA offre le service proxy et aussi balaye, examine, et classe tout le trafic par catégorie (HTTP, HTTPS, et Protocole FTP (File Transfer Protocol)). Tout le passage de ces protocoles sur le TCP et se fonde fortement sur le Système de noms de domaine (DNS) pour le bon fonctionnement. Pour ces raisons, la santé de réseau est essentielle pour le bon fonctionnement de l'appliance et sa transmission avec de diverses parties du réseau, à l'intérieur et à l'extérieur du

contrôle d'entreprise.

Conception

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

Réseau

Un réseau exempt d'erreurs et rapide est essentiel pour le bon fonctionnement du WSA. Si le réseau est instable, l'expérience utilisateur pourrait refuser. Des problèmes de réseau sont habituellement détectés quand les pages Web prennent plus long pour atteindre ou sont inaccessibles. L'inclination initiale est blâme l'appliance, mais c'est habituellement le réseau qui se conduit mal. Ainsi, la prise en considération soigneuse et l'audit devraient être faits afin de s'assurer que le réseau offre le meilleur service pour des protocoles de l'application de haut niveau tels que le HTTP, le HTTPS, le FTP, et les DN.

Généralisations

Voici quelques généralisations que vous pouvez implémenter afin d'assurer le meilleur comportement du réseau :

- Assurez-vous que le réseau de la couche 2 (L2) est stable, que le fonctionnement spanning tree est correct, et qu'il n'y a pas des calculs et topologie fréquents de spanning-tree change.
- Le protocole de routage qui est utilisé devrait également fournir la convergence rapide et la stabilité. Les temporisateurs rapides de Protocole OSPF (Open Shortest Path First) ou le Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) sont de bons choix pour un tel réseau.
- Utilisez toujours au moins deux interfaces de données sur le WSA : un qui fait face aux ordinateurs d'utilisateur, et un autre pour l'exécution sortante (connectée au proxy ou à l'Internet en amont). Ceci est fait afin d'éliminer la ressource possible contraint, comme quand le nombre de ports TCP sont épuisés ou quand les mémoires tampons de réseau deviennent complètement (avec l'utilisation de l'des interfaces uniques pour à l'intérieur et à l'extérieur d'en particulier).
- Dédiez l'interface de gestion pour le trafic réservé à la Gestion afin d'augmenter la Sécurité. Afin de réaliser ceci par l'intermédiaire du GUI, naviguer vers le **réseau > les interfaces** et cocher la case **distincte de routage (port M1 limité aux services de supervision d'appareils seulement)**.
- Serveurs DNS rapides d'utilisation. N'importe quelle transaction par l'intermédiaire du WSA exige au moins une consultation de DN (sinon dans le cache). Un serveur DNS qui est lent ou se conduit mal des affects n'importe quelle transaction et est observé en tant que connexion à internet retardée ou lente.

- Quand des tables de routage distinctes sont utilisées, ces règles s'appliquent :

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

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

  Note: La séparation des tables de routage est non par interface, mais plutôt par service. Par exemple, le trafic entre le WSA et le contrôleur de domaine de Microsoft Active Directory (AD) obéissent toujours les artères qui sont spécifiées dans la table de routage de Gestion, et il est possible de configurer les artères qui précisent de l'interface P1/P2 dans cette table. Il n'est pas possible d'inclure les artères 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 implémenter afin d'assurer le meilleur comportement du réseau :

- Le de d'â de rotation de DN ceci est le terme utilisé quand une adresse Internet simple est utilisée comme proxy, mais elle a des enregistrements du multiple A sur le serveur DNS. Chaque client résout ceci à une adresse IP différente et utilise différents proxys. Une limite est que des modifications des enregistrements DNS sont réfléchies sur des clients sur la réinitialisation (DN locaux cachant), ainsi elle offre un bas niveau de la robustesse si une modification doit être apportée. Cependant, c'est transparent aux utilisateurs.

- Le de d'â de fichiers de la modification d'adresse de proxy (PAC) ceux-ci sont des fichiers proxy-automatiques de script qui déterminent comment chaque URL devrait être manipulé sur un navigateur basé sur les fonctions écrites dans lui. Il a la caractéristique pour expédier le même URL toujours directement ou au même proxy.

- Le automatique de d'â de détection ceci décrit l'utilisation des méthodes DNS/DHCP afin d'obtenir des fichiers PAC (décrits dans la considération précédente). Habituellement, ces trois premières considérations sont combinées dans une solution. Cependant, ceci peut être compliqué et beaucoup d'utilisateur-agents, tels que la Microsoft Office, téléchargeur d'Adobe, les Javascript, et l'éclair, ne peuvent pas indiquer des fichiers PAC du tout.

- de d'â de Protocol de contrôle du cache de Web (WCCP) ce protocole (particulièrement la version WCCP 2) fournit une manière robuste et très puissante de créer l'Équilibrage de charge entre les plusieurs WSAs et d'incorporer également la Haute disponibilité.

- Le distinct Cisco de d'â d'appareils d'Équilibrage de charge recommande que vous utilisiez des équilibreurs de charge en tant qu'ordinateurs dédiés.

Pare-feu

Voici quelques considérations de Pare-feu que vous pouvez implémenter afin d'assurer le meilleur comportement du réseau :

- Assurez-vous qu'on permet le Protocole ICMP (Internet Control Message Protocol) dans tout le réseau de chaque source. C'est essentiel, pendant que le WSA dépend du mécanisme maximum de détection d'unité de transition de chemin (MTU), comme décrit dans RFC 1191, qui dépend des requêtes d'écho d'ICMP (type 8) et réponses d'écho (type 0), et l'inaccessible-fragmentation d'ICMP est exigée (type 3, code 4). Si vous désactivez la découverte de MTU de chemin sur le WSA avec la commande CLI de **pathmtudiscovery**, alors le WSA utilise le MTU par défaut de 576 octets, selon RFC 879. Ceci affecte la représentation due au temps système accru et un réassemblage des paquets.

- Assurez-vous qu'il n'y a aucun routage asymétrique à l'intérieur de du réseau. Tandis que ce n'est pas un problème sur le WSA, n'importe quel Pare-feu qui est produit le long du chemin relâche les paquets parce qu'il n'a pas reçu les deux côtés de la transmission.

- Avec des Pare-feu, il est très important d'exclure les adresses IP WSA des menaces en tant que stations régulières d'ordinateur d'extrémité. Le Pare-feu pourrait mettre les adresses IP sur la liste noire WSA dues à trop de connexions (selon la connaissance générale de Pare-feu).

- Si le Traduction d'adresses de réseau (NAT) est utilisé pour n'importe quelle adresse IP WSA sur le périphérique de sites du client, assurez-vous que chaque WSA utilise une adresse globale externe distincte dans le NAT. Si vous utilisez NAT pour plusieurs WSAs qui ont une adresse globale externe simple, vous pourriez rencontrer ces questions :

  Toutes les connexions de tout les WSAs au monde extérieur utilisent une adresse globale externe simple, et le Pare-feu manque rapidement de ressources.

  S'il y a un pic du trafic vers cette destination simple, le serveur cible pourrait la mettre et découper sur la liste noire l'entreprise entière de l'accès à cette ressource. Ceci pourrait être une importante ressource comme mémoire de nuage de société, connexions de nuage de bureau, ou mises à jour de logiciel anti-virus de par-ordinateur.

Identités

Souvenez-vous que le *logique ET le* principe s'applique dans des tous les composants de l'identité. Par exemple, si vous configurez l'utilisateur-agent et l'adresse IP, il signifie l'utilisateur-agent de cette adresse IP. Il ne signifie pas l'utilisateur-agent *ou* cette adresse IP.

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

Il est important de s'assurer que chaque identité qui exige l'authentification inclut les chaînes d'utilisateur-agent pour les navigateurs/utilisateur-agents qui prennent en charge l'authentification de proxy, telle que l'Internet Explorer, Mozilla Firefox, et le Google Chrome connus. Il y a quelques applications qui exigent l'accès Internet mais ne prend en charge pas l'authentification proxy/WWW.

Les identités sont de haut en bas apparié avec les matchs de rechercher qui finit sur la première entrée appariée. Pour cette raison, si vous faites configurer l'*identité 1* et l'*identité 2*, et une identité 1 de correspondances de transaction, il n'est pas vérifié contre l'identité 2.

Access/déchiffrement/routage/stratégies sortantes de malware

Ces stratégies sont appliquées contre différents types de trafic :

- Les stratégies d'Access sont appliquées contre le HTTP ou les connexions FTP ordinaire. Ils déterminent si la transaction devrait être reçue ou abandonnée.

- Les stratégies de déchiffrement déterminent si des transactions HTTPS devraient être déchiffrées, abandonnées, ou traversées. Si la transaction est déchiffrée, alors la partie consécutive de elle peut être vue comme demande de HTTP ordinaire et est appariée contre des stratégies d'Access. Si vous devez relâcher une demande HTTPS, relâchez-la dans les stratégies de déchiffrement, pas dans les stratégies d'Access. Autrement, il consomme plus de CPU et mémoire pour une transaction relâchée d'abord à déchiffrer et puis à relâcher.

- En conduisant des stratégies déterminez la direction en amont d'une transaction une fois qu'il que le sien a permis par le WSA. Ceci applique s'il y a des proxys en amont ou si le WSA est en mode de *connecteur* et envoie le trafic au tower de sécurité Web de nuage.

- Les stratégies sortantes de malware sont appliquées contre des téléchargements de HTTP ou de FTP des utilisateurs vers des web server. Ceci est habituellement vu est une demande de courrier de HTTP.

Pour chaque type de stratégie, il est important de se souvenir que le *logique OU le* principe s'applique. Si vous faites se référer de plusieurs identités, alors la transaction devrait apparier les identités l'unes des qui sont configurées.

Pour un contrôle plus granulaire, utilisez ces stratégies. Les identités incorrectement configurées par stratégie peuvent créer des questions, où il est plus salutaire d'utiliser plusieurs identités référencées dans une stratégie. Souvenez-vous que des identités n'affectent pas le trafic, ils identifient juste les types de trafic pour les correspondances postérieures dans une stratégie.

Souvent des périodes, les stratégies de déchiffrement utilisent des identités avec l'authentification. Tandis que ce n'est pas erroné et est parfois nécessaire, l'utilisation d'une identité avec l'authentification référencée dans la stratégie de déchiffrement signifie que toutes les transactions qui apparient la stratégie de déchiffrement sont déchiffrées pour que l'authentification ait lieu. L'action de déchiffrement pourrait être abandonnée ou traversée, mais puisqu'il y a une identité avec l'authentification, le déchiffrement a lieu afin de plus tard relâcher ou traverser le trafic. C'est cher et devrait être évité.

On a observé quelques configurations qui contiennent 30 identités ou plus et 30 ou plus des stratégies d'Access, où toutes les stratégies d'Access incluent toutes les identités. Dans ce cas, il n'y a aucun besoin d'utiliser ce beaucoup d'identités si elles sont appariées dans toutes les stratégies d'Access. Tandis que ceci ne nuit pas à l'exécution d'appareils, il crée la confusion avec des tentatives de dépanner et est cher en vue de la représentation.

Catégories faites sur commande URL

L'utilisation des catégories faites sur commande URL est un outil puissant sur le WSA qui est habituellement mal compris et abusé. Par exemple, il y a des configurations qui contiennent tous les sites visuels pour des correspondances dans l'identité. Le WSA a un outil intégré qui automatiquement des mises à jour quand les sites visuels changent l'URLs, qui se produit fréquemment. Ainsi, il semble raisonnable de permettre au WSA pour gérer les catégories URL automatiquement, et utilise les catégories URL de coutume pour l'offre spéciale, les sites pas encore classés par catégorie.

Faites attention très avec des expressions régulières. Si des correspondances de caractère particulier telles que le point (.) et l'étoile (*) sont utilisées, elles pourraient s'avérer être très CPU et mémoire étendue. Le WSA développe n'importe quelle expression régulière pour l'apparier contre chaque transaction. Par exemple, voici une expression régulière :

```
example.*
```

Cette expression l'URL de match any qui contient l'*exemple de* mot, non seulement le domaine d'*example.com*. Évitez l'utilisation du *point* et *tenez le premier rôle* dans les expressions régulières et utilisez-les seulement en dernier recours.

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

```
www.example.com
```

Si vous utilisez cet exemple dans les expressions régulières classé, il appariera non seulement *www.example.com*, mais également *www.www3example2com.com*, comme point ici signifie n'importe quel *caractère*. Si vous désirez apparier seulement *www.example.com*, échappez au point :

```
www\.example\.com
```

Dans ce cas, il n'y a aucune raison d'utiliser la caractéristique d'expressions régulières quand vous pouvez inclure ceci à l'intérieur du domaine de catégorie URL de coutume avec ce format :

```
www.example.com
```

Anti-malware et réputation

Si plus d'une engine de balayage est activée, considérez l'option d'activer le balayage adaptatif également. La lecture adaptative est une engine puissante mais petite sur le WSA que les pré-balayages chaque demande et détermine l'engine complète qui devrait être des demandes SCAN utilisées. Ceci augmente légèrement des performances sur le WSA.