Exemple de configuration de la fonction de contournement de l'état TCP ASA 8.2.X

Contenu

Introduction

Ce document décrit comment configurer la caractéristique de contournement d'état de TCP. Cette caractéristique permet en partance et d'arrivée traverse le Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 distinct.

Conditions préalables

Exigences de licence

Le Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 devrait avoir au moins le permis de base.

Composants utilisés

Les informations dans ce document sont basées sur l'appliance de sécurité adaptable Cisco (ASA) avec la version 8.2(1) et ultérieures.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions de document.

Contournement d'état de TCP

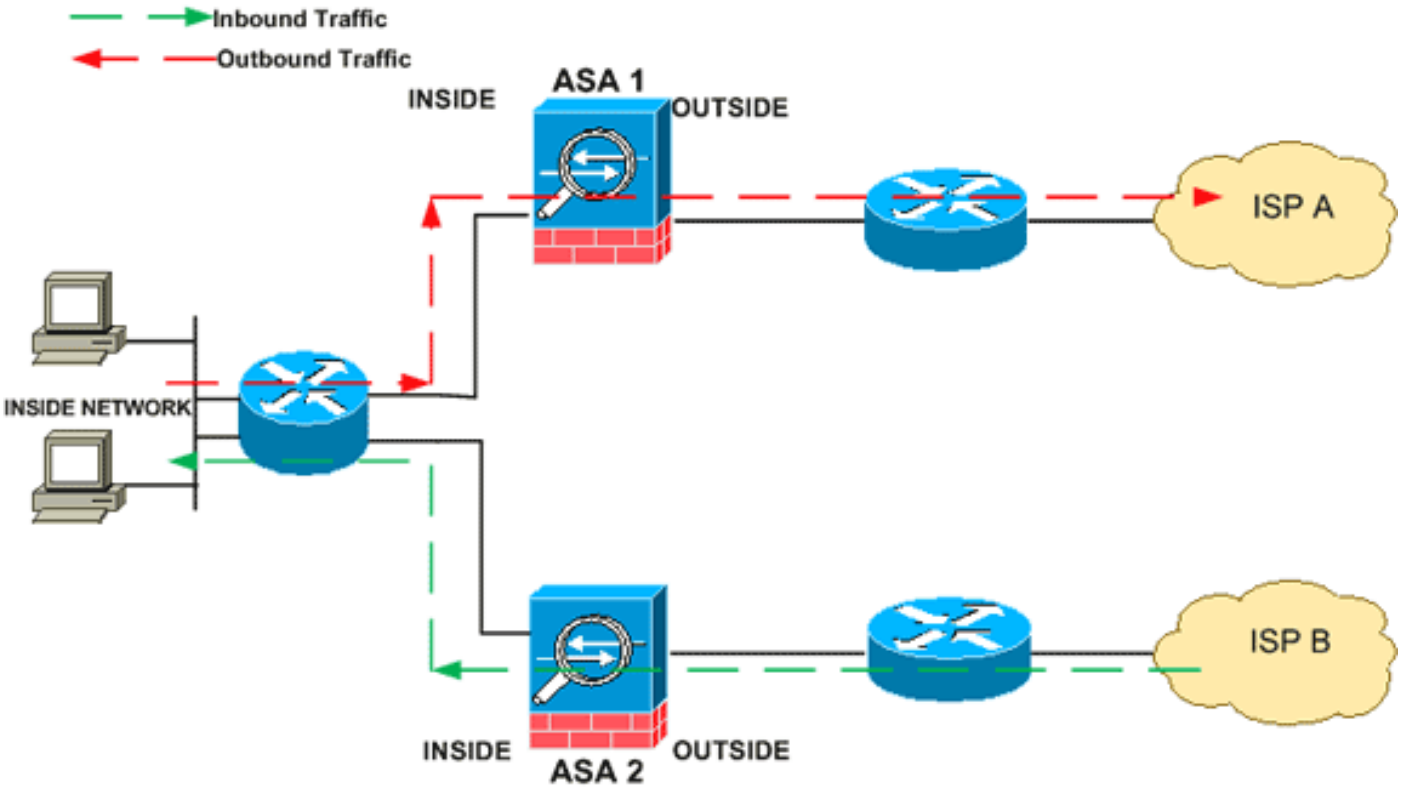
Par défaut, tout le trafic qui traverse l'appliance de sécurité adaptable Cisco (ASA) est examiné utilisant Adaptive Security Algorithm et est laissé ou abandonné basé sur la stratégie de sécurité. Afin de maximiser la représentation de Pare-feu, l'ASA vérifie l'état de chaque paquet (par exemple, est c'une nouvelle connexion ou une connexion établie ?) et l'assigne au chemin de Gestion de session (un nouveau paquet de synchronisation de connexion), au chemin rapide (une connexion établie), ou au chemin d'avion de contrôle (inspection avancée).

Les paquets TCP qui apparient des connexions existantes dans le chemin rapide peuvent traverser l'appliance de sécurité adaptable sans revérifier chaque aspect de la stratégie de sécurité. Cette caractéristique maximise la représentation. Cependant, la méthode utilisée pour établir la session dans le chemin rapide (qui utilise le paquet de synchronisation) et les contrôles qui se produisent dans le chemin rapide (tel que le numéro de séquence de TCP) peut incommoder les solutions asymétriques de routage : l'écoulement sortant et d'arrivée d'une connexion doit traverser la même ASA.

Par exemple, une nouvelle connexion va à *ASA 1.* Le paquet de synchronisation traverse le chemin de Gestion de session, et une entrée pour la connexion est ajoutée à la table de chemin rapide. Si les paquets suivants de cette connexion passent par *ASA 1*, les paquets apparieront l'entrée dans le chemin rapide et sont traversés. Si les paquets suivants vont à *ASA 2*, où il n'y avait pas un paquet de synchronisation qui est passé par le chemin de Gestion de session, alors il n'y a aucune entrée dans le chemin rapide pour la connexion, et les paquets sont lâchés.

Si vous avez le routage asymétrique configuré sur les Routeurs en amont, et trafiquez des remplaçants entre deux ASA, alors vous pouvez configurer le contournement d'état de TCP pour le trafic spécifique. Le contournement d'état de TCP modifie la manière que des sessions sont établies dans le chemin rapide et désactive les contrôles de chemin rapide. Cette caractéristique traite le trafic TCP beaucoup pendant qu'elle traite une connexion d'UDP : quand un paquet de non-synchronisation appariant les réseaux spécifiés écrit l'ASA, et il n'y a pas une entrée de chemin rapide, alors le paquet passe par le chemin de Gestion de session pour établir la connexion dans le chemin rapide. Une fois dans le chemin rapide, le trafic saute les contrôles de chemin rapide.

Cette image fournit un exemple du routage asymétrique, où le trafic sortant passe par une ASA différente que le trafic d'arrivée :



Remarque: La caractéristique de contournement d'état de TCP est désactivée par défaut sur le Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500.

Les informations de support

Cette section fournit les informations de support pour la caractéristique de contournement d'état de TCP.

- Mode de contexte — Pris en charge dans simple et le mode de contexte multiple.
- Mode de Pare-feu — Pris en charge en mode conduit et transparent.
- Basculement — Prend en charge le Basculement.

Ces caractéristiques ne sont pas prises en charge quand vous utilisez le contournement d'état de TCP :

- Inspection d'application — L'inspection d'application exige les deux le trafic en entrée et en sortie pour traverser la même ASA, ainsi l'inspection d'application n'est pas prise en charge avec le contournement d'état de TCP.
- L'AAA a authentifié des sessions — Quand un utilisateur authentifie avec une ASA, le trafic retournant par l'intermédiaire de l'autre ASA sera refusé parce que l'utilisateur n'a pas authentifié avec cette ASA.
- Interception TCP, limite embryonnaire maximum de connexion, randomisation de numéro de séquence de TCP — L'ASA ne maintient pas l'état de la connexion, ainsi ces caractéristiques ne sont pas appliquées.
- Normalisation de TCP — Le normalisateur de TCP est désactivé.
- Fonctionnalité de SSM et de SSC — Vous ne pouvez utiliser le contournement d'état de TCP et aucune application en cours d'exécution sur un SSM ou SSC, tel que l'IPS ou le CSC.

Instructions NAT : Puisque la session de traduction est établie séparément pour chaque ASA, soyez sûr de configurer NAT statique sur les deux ASA pour le trafic de contournement d'état de TCP ; si vous utilisez NAT dynamique, l'adresse choisie pour la session sur *ASA 1* différera de

l'adresse choisie pour la session sur *ASA 2.*

Configurez

Cette section décrit comment configurer la caractéristique de contournement d'état de TCP sur l'appliance de sécurité adaptatif de la gamme Cisco ASA 5500 (ASA).

Configuration de caractéristique de contournement d'état de TCP

Terminez-vous ces étapes afin de configurer la caractéristique de contournement d'état de TCP sur l'appliance de sécurité adaptatif de la gamme Cisco ASA 5500 :

1. Employez la commande de class_map_name de class-map afin de créer un *class map*. Le class map est utilisé pour identifier le trafic pour lequel vous voulez désactiver l'inspection de pare-feu dynamique. Le class map utilisé dans cet exemple est des *tcp_bypass*.`ASA(config)#class-map tcp_bypass`
2. Employez la commande de paramètre de correspondance afin de spécifier le trafic intéressant dans le class map. En utilisant le cadre de stratégie modulaire, employez la commande de **match access-list** en mode de configuration de class-map afin d'employer une liste d'accès pour identifier le trafic auquel vous voulez s'appliquer des actions. Voici un exemple de cette configuration :`ASA(config)#class-map tcp_bypass ASA(config-cmap)#match access-list tcp_bypass` *les tcp_bypass* est le nom de la liste d'accès utilisée dans cet exemple. Référez-vous à identifier le trafic (class map de couche 3/4) pour plus d'informations sur spécifier le trafic intéressant.
3. Employez la commande de nom de policy-map afin d'ajouter une carte de stratégie ou éditer une carte de stratégie (qui est déjà présente) cette les positionnements les actions de prendre avec le trafic de class map ont spécifié déjà. En utilisant le cadre de stratégie modulaire, employez la commande de **policy-map** (sans mot clé de type) en mode de configuration globale afin d'assigner des actions de trafiquer que vous avez identifié avec un class map de la couche 3/4 (la commande de class-map ou de class-map type management). Dans cet exemple, la carte de stratégie est *tcp_bypass_policy* :`ASA(config-cmap)#policy-map tcp_bypass_policy`
4. Employez la commande de classe en mode de configuration de la carte de stratégie afin d'assigner le class map (*tcp_bypass*) déjà créé à la carte de stratégie (*tcp_bypass_policy*) où vous pouvez assigner des actions au trafic de class map. Dans cet exemple, le class map est des *tcp_bypass* :`ASA(config-cmap)#policy-map tcp_bypass_policy ASA(config-pmap)#class tcp_bypass`
5. Employez la commande de TCP-état-contournement de connection advanced-options de positionnement dans le mode de configuration de classe afin d'activer la caractéristique de contournement d'état de TCP. Cette commande a été introduite dans la version 8.2(1). Le mode de configuration de classe est accessible du mode de configuration de la carte de stratégie suivant les indications de cet exemple :`ASA(config-cmap)#policy-map tcp_bypass_policy ASA(config-pmap)#class tcp_bypass ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass`
6. Utilisez le policymap_name de service-stratégie [global | commande d'*intf d'*interface] en mode de configuration globale afin de lancer une carte de stratégie globalement sur toutes les interfaces ou sur une interface visée. Afin de désactiver la stratégie de service, utilisez le **forme no de** cette commande. Utilisez la commande de service-**stratégie** d'activer un

ensemble de stratégies sur un interface.global applique la carte de stratégie à toutes les interfaces, et l'**interface** s'applique la stratégie à une interface. On permet seulement une stratégie globale. Vous pouvez ignorer la stratégie globale sur une interface en s'appliquant une stratégie de service à cette interface. Vous pouvez appliquer seulement une carte de stratégie à chaque interface.`ASA(config-pmap-c)#service-policy tcp_bypass_policy outside`

Voici une configuration d'échantillon pour le contournement d'état de TCP :

```
!--- Configure the access list to specify the TCP traffic !--- that needs to by-pass inspection
to improve the performance. ASA(config)#access-list tcp_bypass extended permit tcp 10.1.1.0
255.255.255.224 any !--- Configure the class map and specify the match parameter for the !---
class map to match the interesting traffic. ASA(config)#class-map tcp_bypass ASA(config-
cmap)#description "TCP traffic that bypasses stateful firewall" ASA(config-cmap)#match access-
list tcp_bypass !--- Configure the policy map and specify the class map !--- inside this policy
map for the class map. ASA(config-cmap)#policy-map tcp_bypass_policy ASA(config-pmap)#class
tcp_bypass !--- Use the set connection advanced-options tcp-state-bypass !--- command in order
to enable TCP state bypass feature. ASA(config-pmap-c)#set connection advanced-options tcp-
state-bypass !--- Use the service-policy policymap_name [ global | interface intf ] !--- command
in global configuration mode in order to activate a policy map !--- globally on all interfaces
or on a targeted interface. ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
ASA(config-pmap-c)#static (inside,outside) 192.168.1.224 10.1.1.0 netmask 255.255.255.224
```

Vérifiez

La commande de show conn affiche le nombre de connexions actives de TCP et UDP et fournit des informations au sujet des connexions de divers types. Afin d'afficher l'état de connexion pour le type de connexion indiqué, utilisez la commande de show conn dans le mode d'exécution privilégié. Cette commande prend en charge les adresses IPv4 et IPv6. L'affichage de sortie pour les connexions qui utilisent le **contournement d'état de TCP** inclut l'indicateur **B.**

Dépannez

L'ASA affiche ce message d'erreur même après que la caractéristique de TCP-état-contournement est activée.

```
%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface
interface_name to dest_address:no matching session
```

Des paquets d'ICMP ont été lâchés par les dispositifs de sécurité en raison des contrôles de Sécurité ajoutés par la caractéristique d'ICMP d'avec état qui sont habituellement des réponses d'écho d'ICMP sans requête d'écho valide déjà passée à travers les dispositifs de sécurité ou des messages d'erreur ICMP non liés à n'importe quelle session de TCP, d'UDP, ou d'ICMP déjà établie dans les dispositifs de sécurité.

L'ASA affiche ce log même si le contournement d'état de TCP est activé parce que désactiver cette fonctionnalité (c'est-à-dire, en vérifiant l'ICMP renvoyez les entrées pour le type 3 dans la table de connexion) n'est pas possible. Mais la caractéristique de contournement d'état de TCP fonctionne correctement.

Employez cette commande afin d'empêcher ces messages d'apparaître :

```
hostname(config)#no logging message 313004
```

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems