Configurez la caractéristique de contournement d'état de TCP sur la gamme ASA 5500

Contenu

Introduction

Ce document décrit comment configurer la caractéristique de contournement d'état de TCP, qui permet au trafic en partance et d'arrivée pour traverser le Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 distinct (ASA).

Conditions préalables

Conditions requises

Cisco ASA doit avoir au moins le permis de base installé avant que vous puissiez poursuivre la configuration qui est décrite dans ce document.

Composants utilisés

Les informations dans ce document sont basées sur la gamme de Cisco ASA 5500 qui exécutent la version de logiciel 9.x.

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Cette section fournit un aperçu de la caractéristique de contournement d'état de TCP et des informations de support relatives.

Vue d'ensemble des fonctionnalités de contournement d'état de TCP

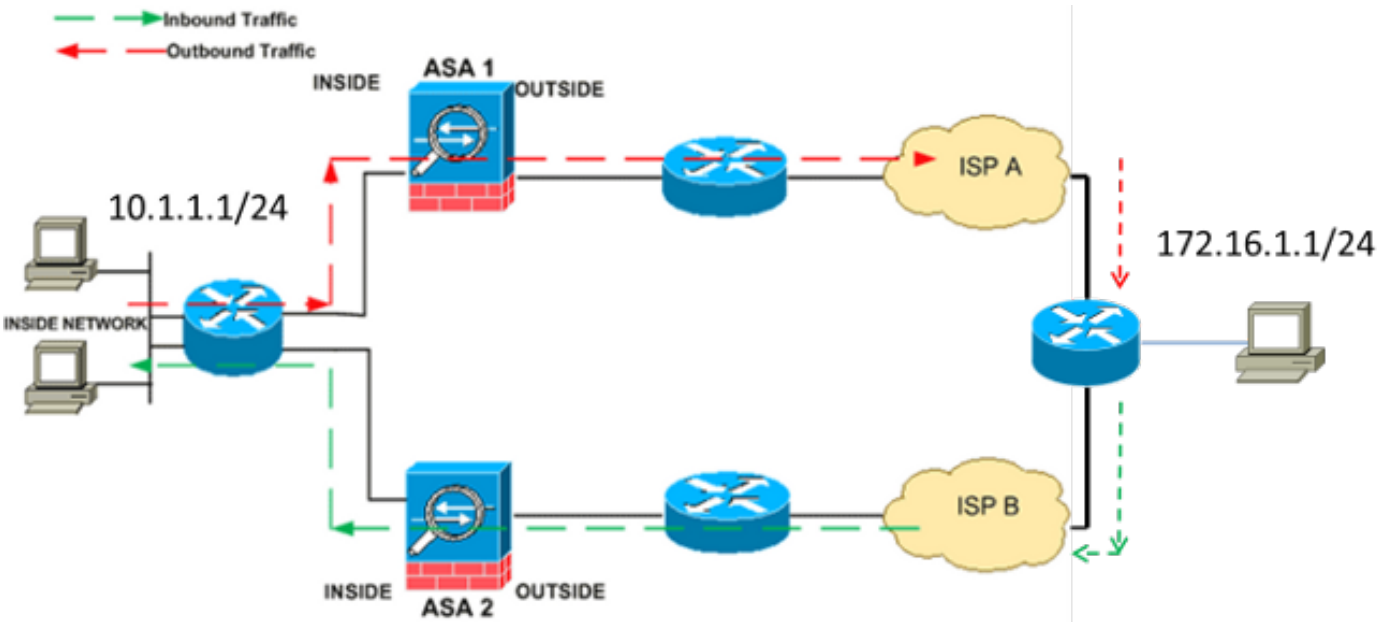
Par défaut, tout les trafic qui traverse l'ASA est examiné par l'intermédiaire d'Adaptive Security Algorithm et est laissé ou abandonné basé sur la stratégie de sécurité. Afin de maximiser la représentation de Pare-feu, l'ASA vérifie l'état de chaque paquet (par exemple, elle vérifie si c'est une nouvelle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

Les paquets TCP qui apparient les connexions en cours dans le chemin rapide peuvent traverser l'ASA sans revérification de chaque aspect de la stratégie de sécurité. Cette caractéristique maximise la représentation. Cependant, la méthode qui est utilisée afin d'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 ; les écoulements sortants et d'arrivée d'une connexion doivent 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 sur cette connexion passent par *ASA 1*, les paquets apparient 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 la caractéristique de contournement d'état de TCP pour le trafic spécifique. La caractéristique de 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 qui apparie les réseaux spécifiés écrit l'ASA, et là n'est aucune entrée de chemin rapide, alors le paquet passe par le chemin de Gestion de session afin d'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 la gamme de Cisco ASA 5500. Supplémentaire, la configuration de contournement d'état de TCP peut entraîner un nombre élevé de connexions si elle n'est pas correctement mise en application.

Les informations de support

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

- Le du Â d'âÂ de **mode de contexte la** caractéristique de contournement d'état de TCP est pris en charge dans simple et des modes de contexte multiple.
- Le du Â d'âÂ de **mode de Pare-feu la** caractéristique de contournement d'état de TCP est pris en charge en modes conduits et transparents.
- du Â d'âÂ de **Basculement le** Basculement de prises en charge de fonctionnalité de contournement d'état de TCP.

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

- L'inspection d'application de du Â d'âÂ d'**inspection d'application** exige que chacun des deux le trafic en entrée et en sortie traversent la même ASA, ainsi l'inspection d'application n'est pas prise en charge avec la configuration de contournement d'état de TCP.
- **L'Authentification, autorisation et comptabilité (AAA) a authentifié le** du Â d'âÂ de **sessions** quand un utilisateur authentifie avec une ASA, le trafic que des retours par l'intermédiaire de l'autre ASA est refusé parce que l'utilisateur n'a pas authentifié avec cette ASA.

- **L'Interception TCP, limite embryonnaire maximum de connexion,** du Â d'âÂ de **randomisation de numéro de séquence de TCP L'**ASA ne fait pas piste de l'état de la connexion, ainsi ces caractéristiques ne sont pas appliquées.

- Le du Â d'âÂ de **normalisation de TCP le** normalisateur de TCP est désactivé.

- **Module de Services de sécurité (SSM) et** du Â d'âÂ de **fonctionnalité de carte de Services de sécurité (SSC)** vous ne pouvez pas utiliser la caractéristique de contournement d'état de TCP avec aucune application qui fonctionnent sur un SSM ou SSC, tel qu'IPS ou sécurité du contenu (CSC).

  Remarque: Puisque la session de traduction est établie séparément pour chaque ASA, assurez-vous que vous configurez la traduction d'adresses de réseau statique (NAT) sur chacun des deux ASA pour le trafic de contournement d'état de TCP. Si vous utilisez NAT dynamique, l'adresse qui est choisie pour la session sur *ASA 1* différera de l'adresse qui est choisie pour la session sur *ASA 2.*

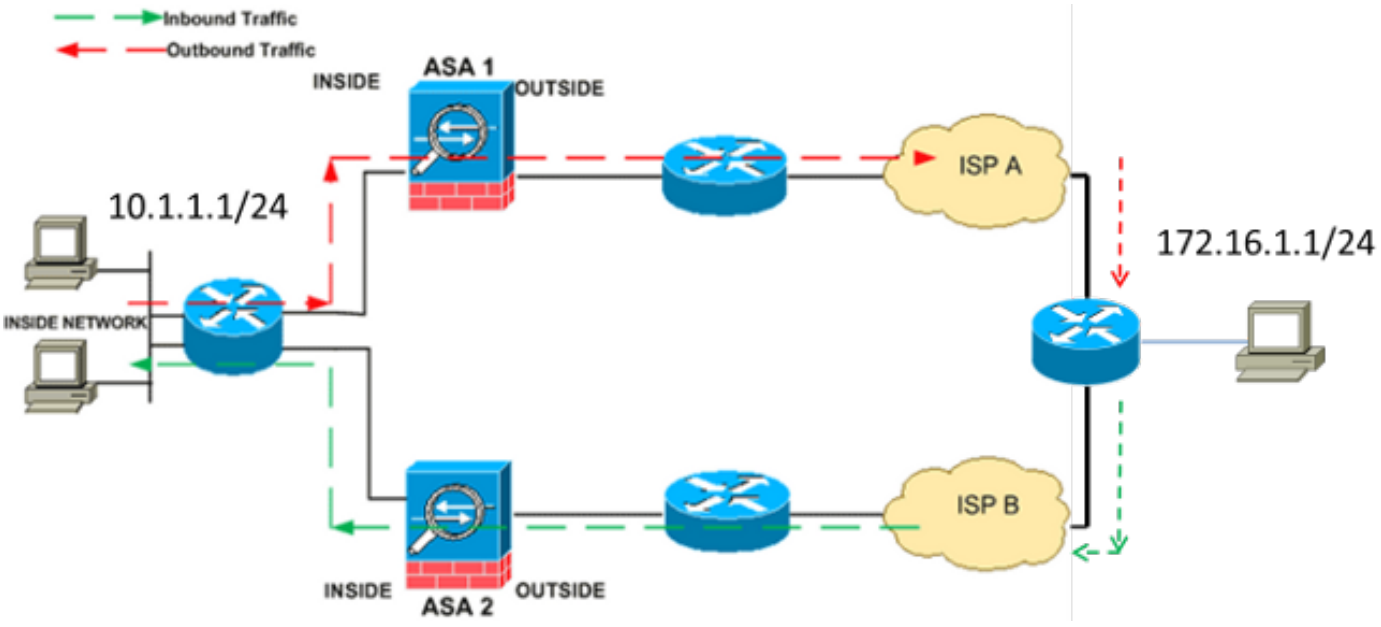
Configurez

Cette section décrit comment configurer la caractéristique de contournement d'état de TCP sur la gamme ASA 5500 dans deux scénarios différents.

Remarque: Utilisez le Command Lookup Tool (clients enregistrés seulement) afin d'obtenir plus d'informations sur les commandes qui sont utilisées dans cette section.

Scénario 1

C'est la topologie qui est utilisée pour le premier scénario :



Remarque: Vous devez appliquer la configuration qui est décrite dans cette section à chacun

des deux ASA.

Terminez-vous ces étapes afin de configurer la caractéristique de contournement d'état de TCP :

1. Sélectionnez la commande de class_map_name de class-map afin de créer un *class map*. Le class map est utilisé afin d'identifier le trafic pour lequel vous voulez désactiver l'inspection de pare-feu dynamique.Remarque: Le class map qui est utilisé dans cet exemple est des **tcp_bypass**.`ASA(config)#class-map tcp_bypass`
2. Sélectionnez la commande de paramètre de correspondance afin de spécifier le trafic d'intérêt dans le class map. Quand vous utilisez le cadre de stratégie modulaire, employez la commande de **match access-list** en mode de *configuration de class-map* afin d'utiliser une liste d'accès pour l'identification du 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
   ```
   Remarque: **Les tcp_bypass** est le nom de la liste d'accès qui est utilisée dans cet exemple. Référez-vous à la section l'identifiant du trafic (class map de couche 3/4) du *guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, 8.2* pour plus d'informations sur la façon spécifier le trafic d'intérêt.
3. Sélectionnez la commande de nom de policy-map afin d'ajouter une carte de stratégie ou éditer une carte de stratégie (qu'est à dire déjà présent) qui assigne les actions d'être respect rentré au trafic spécifié de class map. Quand vous utilisez 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 au trafic 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. Sélectionnez la commande de classe en mode de *configuration de la carte de stratégie* afin d'assigner le class map créé (*tcp_bypass*) à la carte de stratégie (*tcp_bypass_policy*) de sorte que vous puissiez assigner les 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. Sélectionnez 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. Écrivez 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. Sélectionnez la commande de service-**stratégie** afin d'activer un ensemble de stratégies sur une interface. Le mot clé **global** applique la carte de stratégie à toutes les interfaces, et le mot clé d'**interface** applique la carte de stratégie à seulement une interface. On permet seulement une stratégie globale. Afin d'ignorer la stratégie globale sur une interface, vous pouvez s'appliquer une stratégie de service à cette interface. Vous

pouvez appliquer seulement une carte de stratégie à chaque interface. Voici un exemple :

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
```

Voici un exemple de configuration pour la caractéristique de contournement d'état de TCP sur *ASA1* :

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA1(config)#access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA1(config)#class-map tcp_bypass
ASA1(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA1(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA1(config-cmap)#policy-map tcp_bypass_policy
ASA1(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA1(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.

ASA1(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA1(config)#object network obj-10.1.1.0
ASA1(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

Voici un exemple de configuration pour la caractéristique de contournement d'état de TCP sur *ASA2* :

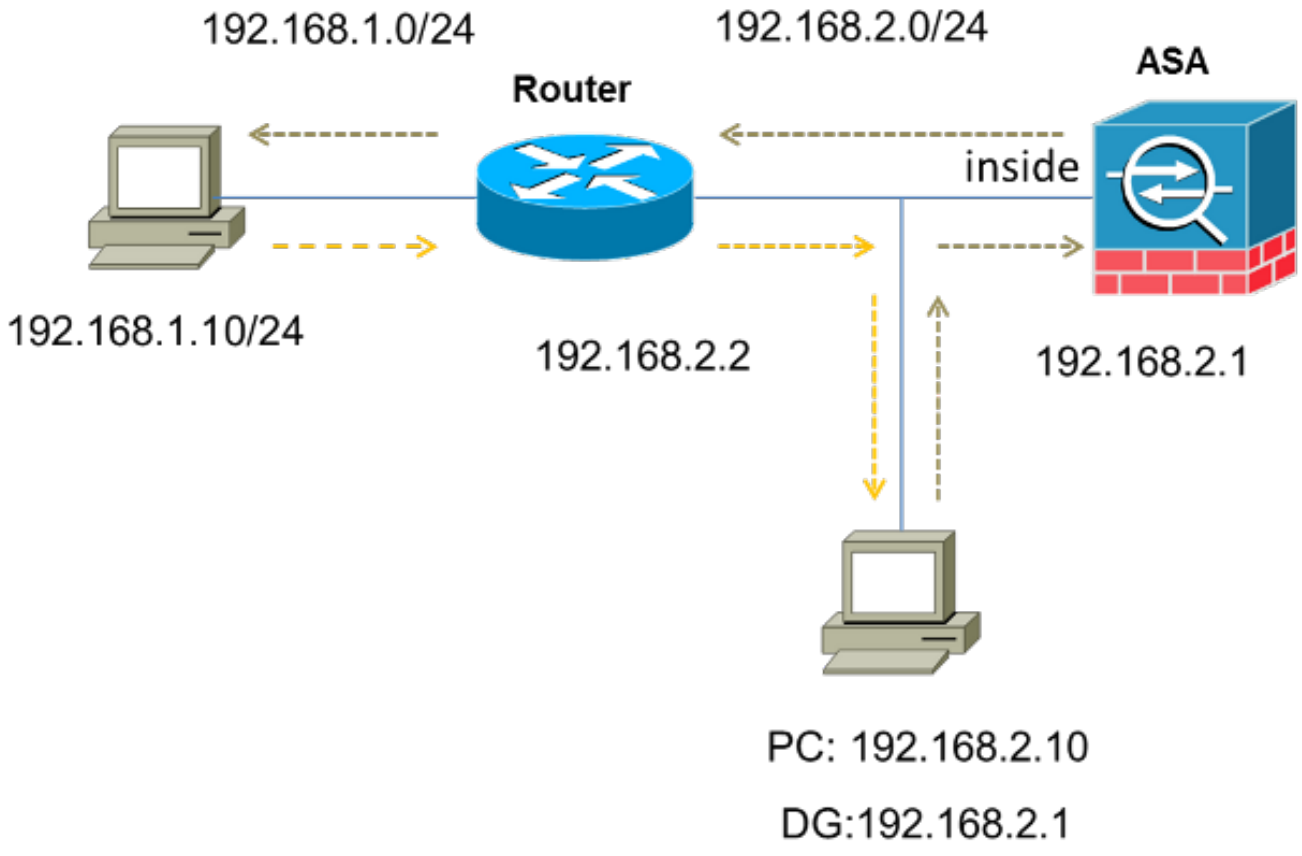
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA2(config)#access-list tcp_bypass extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA2(config)#class-map tcp_bypass
ASA2(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA2(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.
```

```
ASA2(config-cmap)#policy-map tcp_bypass_policy
ASA2(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA2(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.

ASA2(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA2(config)#object network obj-10.1.1.0
ASA2(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

Scénario 2

Cette section décrit comment configurer la caractéristique de contournement d'état de TCP sur l'ASA pour les scénarios qui utilisent le routage asymétrique, où le trafic écrit et part de l'ASA de la même interface (u-*rotation*).

Voici la topologie qui est utilisée dans ce scénario :



Terminez-vous ces étapes afin de configurer la caractéristique de contournement d'état de TCP :

1. Créez une *liste d'accès* afin d'apparier le trafic qui devrait sauter l'inspection de TCP :
   ```
   ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
   192.168.1.0 255.255.255.0
   ```
2. Sélectionnez la commande de class_map_name de class-map afin de créer un *class map*. Le class map est utilisé afin d'identifier le trafic pour lequel vous voulez désactiver l'inspection de pare-feu dynamique.Remarque: Le class map qui est utilisé dans cet exemple est des **tcp_bypass**.
   ```
   ASA(config)#class-map tcp_bypass
   ```
3. Sélectionnez la commande de paramètre de correspondance afin de spécifier le trafic de l'intérêt pour le class map. Quand vous utilisez le cadre de stratégie modulaire, employez la commande de **match access-list** en mode de *configuration de class-map* afin d'utiliser une liste d'accès pour l'identification du 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
   ```
   Remarque: **Les tcp_bypass** est le nom de la liste d'accès qui est utilisée dans cet exemple. Référez-vous à identifier la section du trafic (class map de couche 3/4) du *guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, 8.2* pour plus d'informations sur la façon spécifier le trafic d'intérêt.
4. Sélectionnez la commande de nom de policy-map afin d'ajouter une carte de stratégie ou éditer une carte de stratégie (qu'est à dire déjà présent) cette des positionnements les actions d'être respect rentré au trafic spécifié de class map. Quand vous utilisez le cadre de stratégie modulaire, employez la commande de **policy-map** (sans mot clé de *type*) en mode de *configuration globale* afin d'assigner les actions au trafic 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
   ```
5. Sélectionnez la commande de classe en mode de *configuration de la carte de stratégie* afin d'assigner le class map créé (*tcp_bypass*) à la carte de stratégie (*tcp_bypass_policy*) de sorte que vous puissiez 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
   ```
6. Sélectionnez 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
   ```
7. Écrivez 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. Sélectionnez la commande de service-**stratégie** afin d'activer un ensemble de stratégies sur une interface. Le mot clé **global** applique la carte de stratégie à toutes les interfaces, et le mot clé d'**interface** s'applique la stratégie à seulement une interface. On permet seulement une stratégie globale. Afin d'ignorer la stratégie globale sur une interface, vous pouvez s'appliquer une stratégie de service à cette interface. Vous pouvez appliquer seulement une carte de stratégie à chaque interface. Voici un exemple :
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy inside
   ```
8. Permettez le même niveau de Sécurité pour le trafic sur l'ASA :

```
ASA(config)#same-security-traffic permit intra-interface
```

Voici un exemple de configuration pour la caractéristique de contournement d'état de TCP sur l'ASA :

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to bypass inspection to improve the performance.

ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0

!--- 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 inside

!--- Permit same security level traffic on the ASA to support U-turning

ASA(config)#same-security-traffic permit intra-interface
```

Vérifiez

Sélectionnez la commande de **show conn** afin de visualiser le nombre de connexions actives de TCP et UDP et des informations sur les connexions de divers types. Afin d'afficher l'état de connexion pour le type de connexion indiqué, sélectionnez la commande de **show conn** dans le *mode d'exécution privilégié*.

> Remarque: Cette commande prend en charge les adresses IPv4 et IPv6. La sortie qui est affichée pour les connexions qui utilisent la caractéristique de contournement d'état de TCP inclut l'indicateur **B.**

Voici un exemple de sortie :

```
ASA(config)show conn
1 in use, 3 most used
TCP tcp 10.1.1.1:49525 tcp 172.16.1.1:21, idle 0:01:10, bytes 230, flags b
```

Dépannez

Il n'y a aucune information de dépannage spécifique pour cette caractéristique. Référez-vous à ces documents pour l'information de dépannage générale de Connectivité :

- Captures de paquet ASA avec l'exemple de configuration CLI et ASDM
- ASA 8.2 : Le paquet traversent le Pare-feu de Cisco ASA

  Remarque: Les connexions de contournement d'état de TCP ne sont pas répliquées vers l'équipement de réserve dans une paire de Basculement.

Messages d'erreur

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

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

Les paquets de Protocole ICMP (Internet Control Message Protocol) sont lâchés par l'ASA en raison des contrôles de Sécurité qui sont ajoutés par la caractéristique d'ICMP d'avec état. Ce sont habituellement des *réponses d'écho d'*ICMP sans *requête d'écho* valide déjà passée à travers l'ASA, ou des messages d'erreur ICMP qui ne sont liés à aucune session de TCP, d'UDP, ou d'ICMP actuellement établie dans l'ASA.

L'ASA affiche ce log même si la caractéristique de contournement d'état de TCP est activée parce que la désactivation de cette fonctionnalité (c'est-à-dire, vérifie des entrées de *retour d'*ICMP pour le type 3 dans la table de connexion) n'est pas possible. Cependant, la caractéristique de contournement d'état de TCP fonctionne correctement.

Sélectionnez cette commande afin d'empêcher l'apparence de ces messages :

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

Informations connexes

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