Configuration de la fonction TCP State Bypass sur la gamme ASA 5500

Contenu

Introduction

Ce document décrit comment configurer la fonctionnalité de contournement de l'état TCP, qui permet au trafic sortant et entrant de circuler via des appareils de sécurité adaptatifs (ASA) de la gamme Cisco ASA 5500 distincts.

Conditions préalables

Conditions requises

La licence de base de Cisco ASA doit être installée au moins pour que vous puissiez poursuivre la configuration décrite dans ce document.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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 une vue d'ensemble de la fonctionnalité de contournement de l'état TCP et des informations de support associées.

Vue d'ensemble de la fonction de contournement de l'état TCP

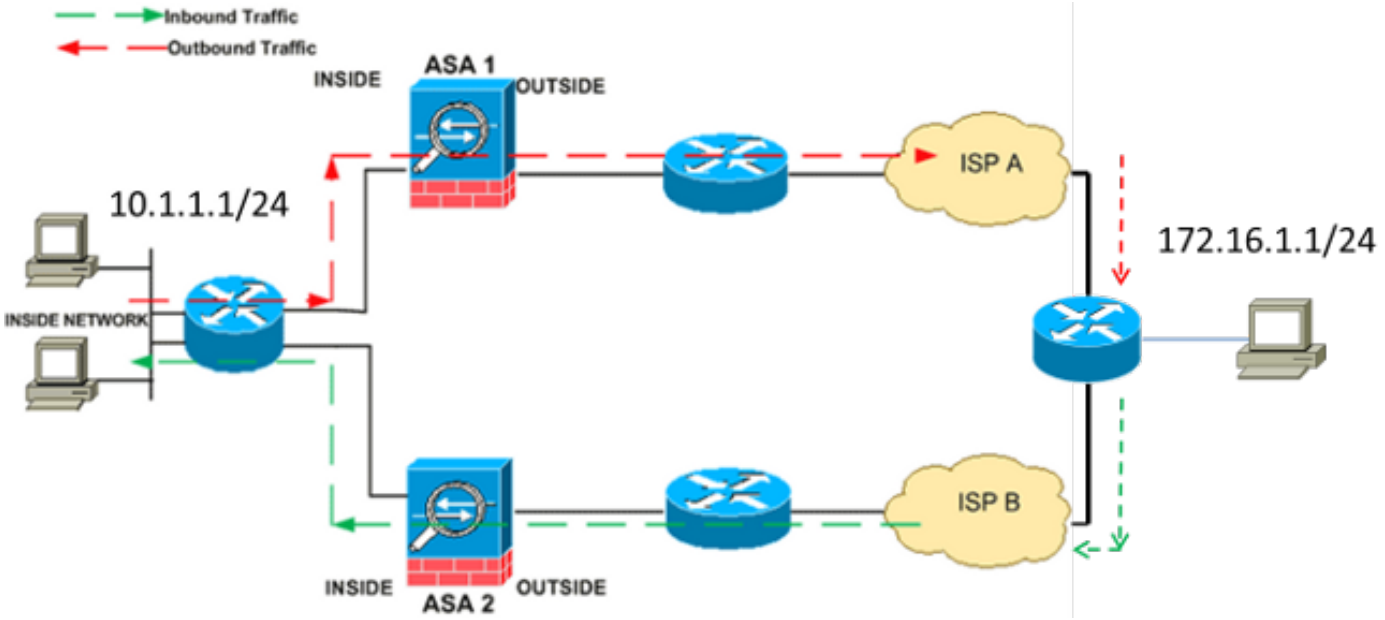
Par défaut, tout le trafic qui passe par l'ASA est inspecté via l'algorithme de sécurité adaptatif et est autorisé à traverser ou abandonné en fonction de la stratégie de sécurité. Afin d'optimiser les performances du pare-feu, l'ASA vérifie l'état de chaque paquet (par exemple, il vérifie s'il s'agit d'une nouvelle connexion ou d'une connexion établie) et l'attribue soit au chemin de gestion de session (un paquet SYN (new connection Synchronize)), soit au chemin rapide (une connexion établie), soit au chemin du plan de contrôle (inspection avancée).

Les paquets TCP qui correspondent aux connexions actuelles dans le chemin rapide peuvent traverser l'ASA sans avoir à vérifier à nouveau tous les aspects de la stratégie de sécurité. Cette fonction optimise les performances. Cependant, la méthode utilisée pour établir la session dans le chemin rapide (qui utilise le paquet SYN) et les vérifications qui se produisent dans le chemin rapide (comme le numéro de séquence TCP) peuvent entraver les solutions de routage asymétrique ; les flux sortants et entrants d'une connexion doivent passer par le même ASA.

Par exemple, une nouvelle connexion va à *ASA 1*. Le paquet SYN passe par le chemin de gestion de session et une entrée pour la connexion est ajoutée à la table de chemins rapides. Si les paquets suivants sur cette connexion passent par *ASA 1*, les paquets correspondent à l'entrée dans le chemin rapide et sont transmis. Si les paquets suivants vont à *ASA 2*, où il n'y avait pas de paquet SYN qui passait 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 abandonnés.

Si le routage asymétrique est configuré sur les routeurs en amont et que le trafic alterne entre deux ASA, vous pouvez configurer la fonction de contournement de l'état TCP pour un trafic spécifique. La fonctionnalité de contournement d'état TCP modifie la façon dont les sessions sont établies dans le chemin rapide et désactive les vérifications de chemin rapide. Cette fonctionnalité traite le trafic TCP comme il traite une connexion UDP : lorsqu'un paquet non SYN qui correspond aux réseaux spécifiés entre dans l'ASA et qu'il n'y a pas d'entrée de chemin rapide, 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 contourne les contrôles de chemin rapide.

Cette image fournit un exemple de routage asymétrique, où le trafic sortant passe par un ASA différent du trafic entrant :



Note: La fonctionnalité de contournement d'état TCP est désactivée par défaut sur la gamme Cisco ASA 5500. En outre, la configuration de contournement de l'état TCP peut entraîner un nombre élevé de connexions si elle n'est pas correctement implémentée.

Informations d'assistance

Cette section décrit les informations de prise en charge de la fonctionnalité de contournement d'état TCP.

- **Mode contexte** - - La fonction de contournement d'état TCP est prise en charge en mode contexte unique et multiple.

- **Mode pare-feu** - - La fonction de contournement de l'état TCP est prise en charge en mode routé et transparent.

- **Basculement** - - La fonction de contournement d'état TCP prend en charge le basculement.

Ces fonctionnalités ne sont pas prises en charge lorsque vous utilisez la fonction de contournement d'état TCP :

- **Inspection d'application** - - L'inspection d'application nécessite que le trafic entrant et sortant passe par le même ASA, de sorte que l'inspection d'application n'est pas prise en charge avec la fonctionnalité de contournement d'état TCP.

- **Authentification, autorisation et comptabilité (AAA) sessions authentifiées** - - Lorsqu'un utilisateur s'authentifie auprès d'un ASA, le trafic qui revient via l'autre ASA est refusé car l'utilisateur ne s'est pas authentifié auprès de cet ASA.

- **Interception TCP, limite maximale de connexion embryonnaire, randomisation du numéro de séquence TCP** âÂ â L'ASA ne suit pas l'état de la connexion, donc ces fonctionnalités ne sont pas appliquées.

- **Normalisation TCP** - - Le normalisateur TCP est désactivé.
- **Fonctionnalité Security Services Module (SSM) et Security Services Card (SSC)** - - Vous ne pouvez pas utiliser la fonctionnalité TCP State Bypass avec les applications qui s'exécutent sur un SSM ou un SSC, telles que IPS ou Content Security (CSC).

Note: Comme la session de traduction est établie séparément pour chaque ASA, assurez-vous de configurer la traduction d'adresses de réseau statique (NAT) sur les deux ASA pour le trafic de contournement de l'état TCP. Si vous utilisez la NAT dynamique, l'adresse choisie pour la session sur *ASA 1* diffère de l'adresse choisie pour la session sur *ASA 2*.

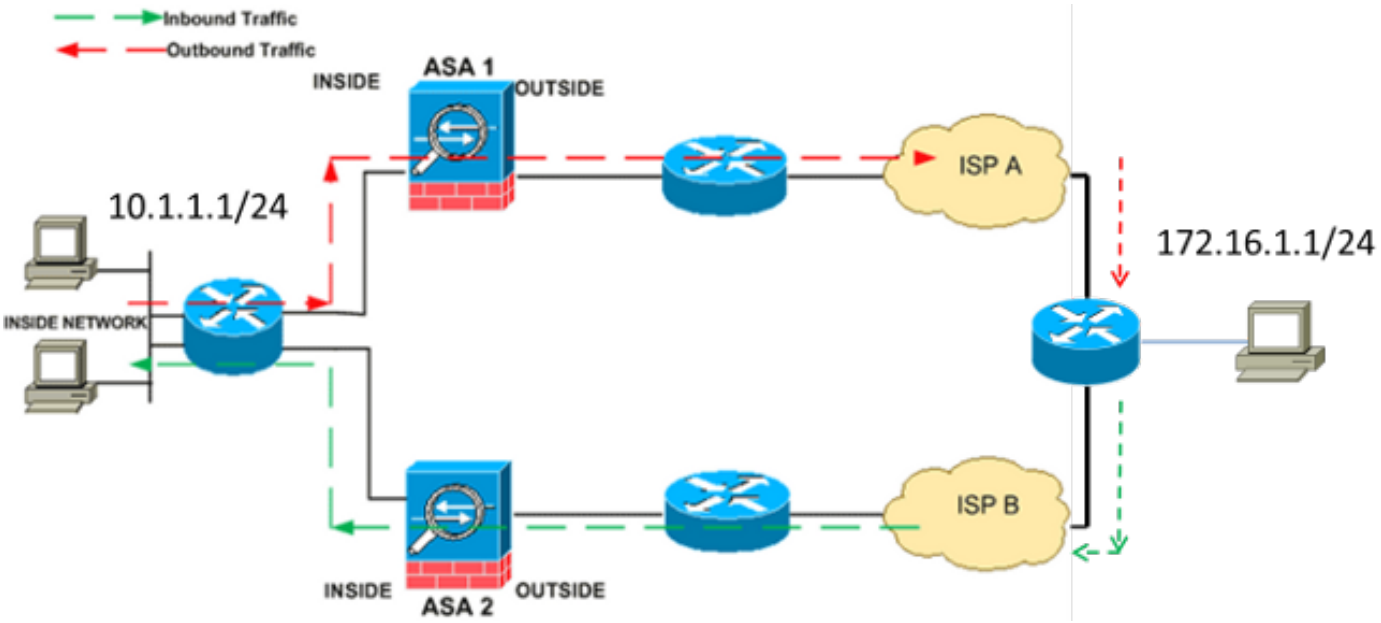
Configuration

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

Note: Utilisez l'outil de recherche de commandes (clients enregistrés seulement) pour en savoir plus sur les commandes employées dans cette section.

Scénario 1

Voici la topologie utilisée pour le premier scénario :



Note: Vous devez appliquer la configuration décrite dans cette section aux deux ASA.

Complétez ces étapes afin de configurer la fonctionnalité de contournement d'état TCP :

1. Entrez la commande class-map class_map_name afin de créer une *carte de classe*. La carte de classe est utilisée afin d'identifier le trafic pour lequel vous voulez désactiver l'inspection avec état du pare-feu.**Note**: La carte de classe utilisée dans cet exemple est **tcp_bypass**.

```
ASA(config)#class-map tcp_bypass
```

2. Entrez la commande match paramètre afin de spécifier le trafic d'intérêt dans la carte de classe. Lorsque vous utilisez le Cadre de stratégie modulaire, utilisez la commande **match access-list** en mode *de configuration class-map* afin d'utiliser une liste d'accès pour identifier le trafic auquel vous voulez appliquer des actions. Voici un exemple de cette configuration :

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```

Note: Le **tcp_bypass** est le nom de la liste d'accès utilisée dans cet exemple. Référez-vous à la section Identification du trafic (carte de classe de couche 3/4) du *Guide de configuration de la gamme Cisco ASA 5500 à l'aide de l'interface de ligne de commande, 8.2* pour plus d'informations sur la façon de spécifier le trafic intéressant.

3. Entrez la commande policy-map name afin d'ajouter un mappage de stratégie ou de modifier un mappage de stratégie (déjà présent) qui attribue les actions à entreprendre en ce qui concerne le trafic de mappage de classe spécifié. Lorsque vous utilisez le Cadre de stratégie modulaire, utilisez la commande policy-map (sans le mot clé *type*) en mode de *configuration globale* afin d'affecter des actions au trafic que vous avez identifié avec une carte de classe de couche 3/4 (la **carte-classe** ou **gestion de type de carte-classe**). Dans cet exemple, la carte de stratégie est **tcp_bypass_policy** :

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

4. Entrez la commande class en mode de *configuration policy-map* afin d'affecter la carte de classe créée (*tcp_bypass*) à la carte de stratégie (*tcp_bypass_policy*) afin que vous puissiez affecter les actions au trafic de la carte de classe. Dans cet exemple, la carte de classe est **tcp_bypass** :

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

5. Entrez la commande set connection advanced-options tcp-state-bypass en mode *de configuration de classe* afin d'activer la fonctionnalité de contournement d'état TCP. Cette commande a été introduite dans la version 8.2(1). Le mode de *configuration de classe* est accessible depuis le mode de *configuration policy-map*, comme illustré dans 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. Entrez le nom de la politique de service [global | interface *intf*] commande en mode de *configuration globale* afin d'activer une carte de stratégie globale sur toutes les interfaces ou sur une interface ciblée. Afin de désactiver la stratégie de service, utilisez la forme **no** de cette commande. Entrez la commande **service-policy** 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 **interface** applique la carte de stratégie à une seule interface. Une seule politique globale est autorisée. Afin de remplacer la stratégie globale sur une interface, vous pouvez appliquer une stratégie de service à cette interface. Vous ne pouvez appliquer qu'une seule 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 fonctionnalité de contournement d'état 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 fonctionnalité de contournement d'état TCP sur *ASA2* :

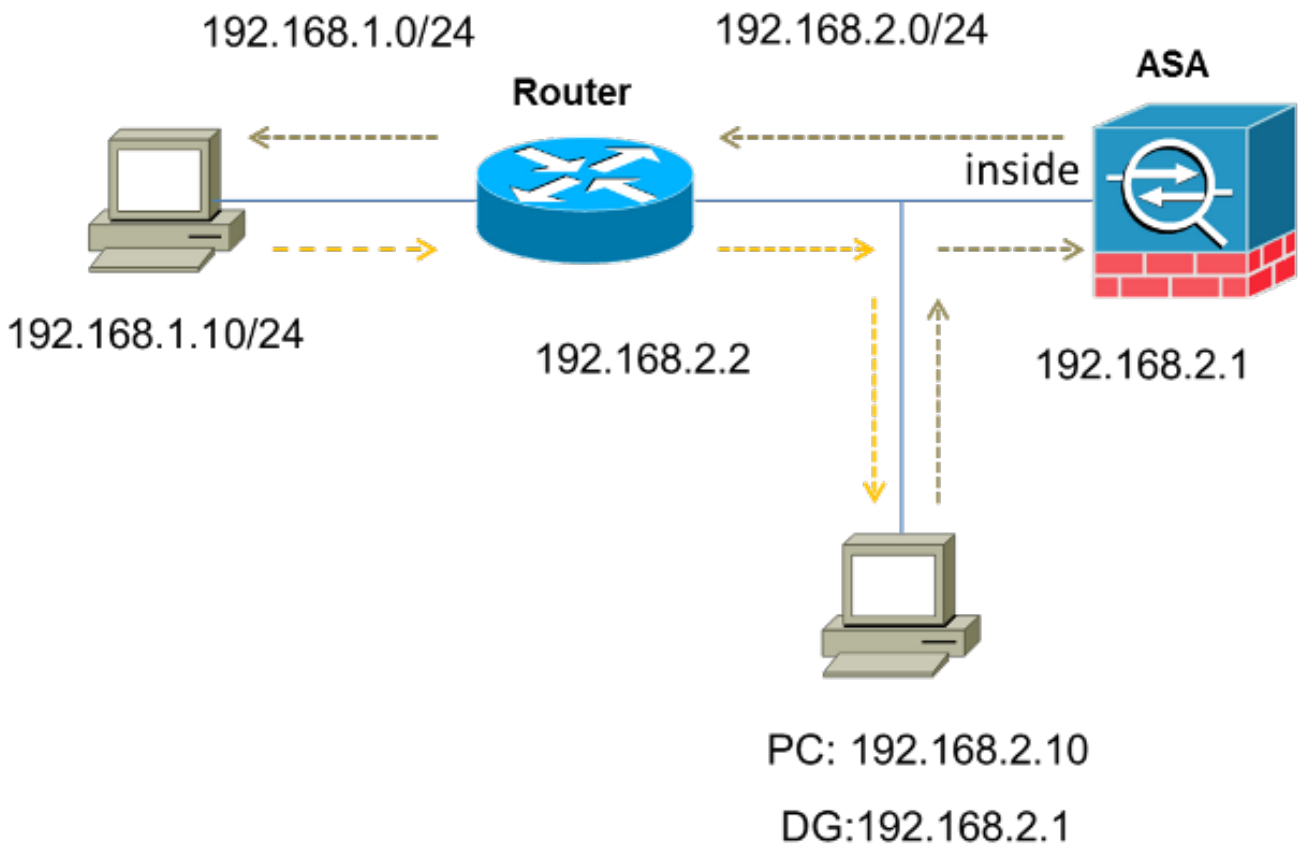
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

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 fonctionnalité de contournement d'état TCP sur l'ASA pour les scénarios qui utilisent le routage asymétrique, où le trafic entre et quitte l'ASA de la même interface (*tournage*).

Voici la topologie utilisée dans ce scénario :



Complétez ces étapes afin de configurer la fonctionnalité de contournement d'état TCP :

1. Créez une *liste d'accès* afin de faire correspondre le trafic qui doit contourner l'inspection 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. Entrez la commande class-map class_map_name afin de créer une *carte de classe*. La carte de classe est utilisée afin d'identifier le trafic pour lequel vous voulez désactiver l'inspection avec état du pare-feu.**Note**: La carte de classe utilisée dans cet exemple est **tcp_bypass**.
```
ASA(config)#class-map tcp_bypass
```
3. Entrez la commande match paramètre afin de spécifier le trafic d'intérêt dans la carte de classe. Lorsque vous utilisez le Cadre de stratégie modulaire, utilisez la commande **match access-list** en mode *de configuration class-map* afin d'utiliser une liste d'accès pour identifier le trafic auquel vous voulez appliquer des actions. Voici un exemple de cette configuration :

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```
Note: Le **tcp_bypass** est le nom de la liste d'accès utilisée dans cet exemple. Référez-vous à la section Identification du trafic (carte de classe de couche 3/4) du *Guide de configuration de la gamme Cisco ASA 5500 à l'aide de l'interface de ligne de commande, 8.2* pour plus d'informations sur la façon de spécifier le trafic intéressant.
4. Entrez la commande policy-map name afin d'ajouter un mappage de stratégie ou de modifier un mappage de stratégie (déjà présent) qui définit les actions à entreprendre en ce qui concerne le trafic de mappage de classe spécifié. Lorsque vous utilisez le Cadre de stratégie modulaire, utilisez la commande policy-map (sans le mot clé *type*) en mode *de configuration globale* afin d'affecter les actions au trafic que vous avez identifié avec une carte de classe de couche 3/4 (la commande **class-map** ou **class-map type management**). Dans cet exemple, la carte de stratégie est **tcp_bypass_policy** :

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```
5. Entrez la commande class en mode de *configuration policy-map* afin d'affecter la carte de classe créée (*tcp_bypass*) à la carte de stratégie (*tcp_bypass_policy*) afin que vous puissiez affecter des actions au trafic de la carte de classe. Dans cet exemple, la carte de classe est **tcp_bypass** :

```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
```
6. Entrez la commande set connection advanced-options tcp-state-bypass en mode *de configuration de classe* afin d'activer la fonctionnalité de contournement d'état TCP. Cette commande a été introduite dans la version 8.2(1). Le mode *de configuration de classe* est accessible depuis le mode *de configuration policy-map*, comme illustré dans 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. Entrez le nom de la politique de service [global | interface *intf*] commande en mode *de configuration globale* afin d'activer une carte de stratégie globale sur toutes les interfaces ou sur une interface ciblée. Afin de désactiver la stratégie de service, utilisez la forme **no** de cette commande. Entrez la commande **service-policy** 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 **interface** applique la stratégie à une seule interface. Une seule politique globale est autorisée. Afin de remplacer la stratégie globale sur une interface, vous pouvez appliquer une stratégie de service à cette interface. Vous ne pouvez appliquer qu'une seule carte de stratégie à chaque interface. Voici un exemple :

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

8. Autoriser 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 fonctionnalité de contournement d'état 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
```

Vérification

Saisissez le **show conn** afin d'afficher le nombre de connexions TCP et UDP actives et des informations sur les connexions de différents types. Afin d'afficher l'état de la connexion pour le type de connexion désigné, saisissez **show conn** en mode *d'exécution privilégié*.

> **Note**: Cette commande prend en charge les adresses IPv4 et IPv6. Le résultat affiché pour les connexions qui utilisent la fonction de contournement d'état TCP inclut l'indicateur **b**.

Voici un exemple de résultat :

```
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
```

Dépannage

Il n'existe aucune information de dépannage spécifique pour cette fonctionnalité. Reportez-vous aux documents suivants pour obtenir des informations générales sur le dépannage de la connectivité :

- Exemple de configuration des captures de paquets ASA avec CLI et ASDM
- ASA 8.2 : Flux de paquets via le pare-feu Cisco ASA

  Note: Les connexions de contournement d'état TCP ne sont pas répliquées sur l'unité de secours dans une paire de basculement.

Messages d'erreur

L'ASA affiche ce message d'erreur même après l'activation de la fonctionnalité de contournement de l'état TCP :

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

Les paquets ICMP (Internet Control Message Protocol) sont abandonnés par l'ASA en raison des contrôles de sécurité ajoutés par la fonctionnalité ICMP avec état. Il s'agit généralement de réponses *d'écho* ICMP sans *requête d'écho* valide déjà transmise sur l'ASA, ou de messages d'erreur ICMP qui ne sont liés à aucune session TCP, UDP ou ICMP actuellement établie dans l'ASA.

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

Entrez cette commande afin d'empêcher l'affichage 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