

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Exigences de licence](#)

[Components Used](#)

[Conventions](#)

[Contournement d'état TCP](#)

[Informations d'assistance](#)

[Configuration](#)

[Configuration de la fonction de contournement de l'état TCP](#)

[Vérification](#)

[Dépannage](#)

[Message d'erreur](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer la caractéristique de contournement d'état de TCP. Cette fonctionnalité permet des flux sortants et entrants via des appliances de sécurité adaptatives de la gamme Cisco ASA 5500 distinctes.

[Conditions préalables](#)

[Exigences de licence](#)

Les appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 doivent avoir au moins la licence de base.

[Components Used](#)

Les informations de ce document sont basées sur Cisco Adaptive Security Appliance (ASA) avec la version 8.2(1) et ultérieure.

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](#)

Reportez-vous aux [Conventions des conseils techniques de Cisco](#) pour plus d'informations sur les conventions du document.

Contournement d'état TCP

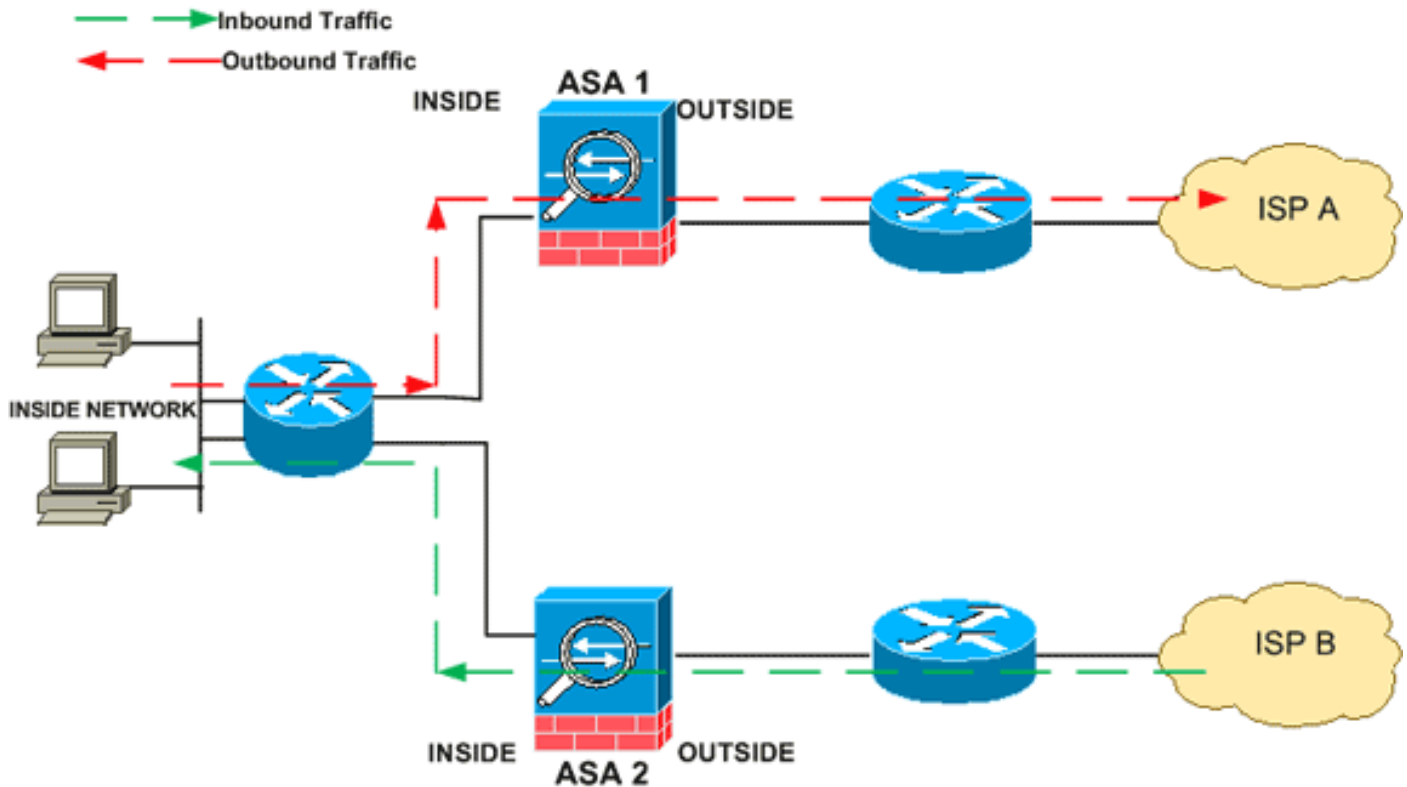
Par défaut, tout le trafic qui passe par l'appareil de sécurité adaptatif Cisco (ASA) est inspecté à l'aide de l'algorithme de sécurité adaptatif et est autorisé à traverser ou abandonné en fonction de la stratégie de sécurité. Afin d'optimiser les performances du pare-feu, l'ASA vérifie l'état de chaque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

Les paquets TCP qui correspondent aux connexions existantes dans le chemin rapide peuvent passer par l'appareil de sécurité adaptatif sans révéifier 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 empêcher les solutions de routage asymétrique : le flux sortant et le flux entrant 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 de 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 le contournement de l'état TCP pour un trafic spécifique. Le 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 correspondant 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 pour 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 :



Remarque : la fonction de contournement de l'état TCP est désactivée par défaut sur les appliances de sécurité adaptatives de la gamme Cisco ASA 5500.

Informations d'assistance

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

- Context Mode : pris en charge en mode de contexte unique et multiple.
- Mode pare-feu : pris en charge en mode routé et transparent.
- Basculement : prend en charge le basculement.

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

- Inspection des applications : l'inspection des applications nécessite que le trafic entrant et sortant passe par le même ASA, de sorte que l'inspection des applications n'est pas prise en charge avec le contournement de l'état TCP.
- Sessions authentifiées AAA : lorsqu'un utilisateur s'authentifie auprès d'un ASA, le trafic revenant via l'autre ASA sera 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 : l'ASA ne suit pas l'état de la connexion, de sorte que ces fonctionnalités ne sont pas appliquées.
- Normalisation TCP : le normalisateur TCP est désactivé.
- Fonctionnalité SSM et SSC : vous ne pouvez pas utiliser le contournement de l'état TCP ni aucune application exécutée sur un SSM ou un SSC, tel qu'IPS ou CSC.

Directives NAT : Étant donné que la session de traduction est établie séparément pour chaque ASA, veillez à configurer la NAT statique sur les deux ASA pour le trafic de contournement d'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 le dispositif de sécurité adaptatif (ASA) de la gamme Cisco ASA 5500.

Configuration de la fonction de contournement de l'état TCP

Complétez ces étapes afin de configurer la fonctionnalité de contournement d'état TCP sur l'appareil de sécurité adaptatif de la gamme Cisco ASA 5500 :

1. Utilisez la commande [class-map class_map_name](#) afin de créer une *carte de classe*. La carte de classe est utilisée pour identifier le trafic pour lequel vous voulez désactiver l'inspection avec état du pare-feu. La carte de classe utilisée dans cet exemple est *tcp_bypass*.

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

2. Utilisez la commande [match paramètre](#) afin de spécifier le trafic intéressant dans la carte de classe. Lors de l'utilisation du 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
```

tcp_bypass est le nom de la liste d'accès utilisée dans cet exemple. Référez-vous à [Identification du trafic \(carte de classe de couche 3/4\)](#) pour plus d'informations sur la spécification du trafic intéressant.

3. Utilisez la commande [policy-map name](#) afin d'ajouter un mappage de stratégie ou de modifier un mappage de stratégie (qui est déjà présent) qui définit les actions à entreprendre avec le trafic de mappage de classe déjà spécifié. Lors de l'utilisation du 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 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
```

4. Utilisez la commande [class](#) en mode de configuration policy-map afin d'assigner la carte de classe (*tcp_bypass*) déjà créée à la carte de stratégie (*tcp_bypass_policy*) où vous pouvez assigner 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
```

5. Utilisez 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 à partir du 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. Utiliser le [nom](#) de la [politique de service \[global | interface *intf*\]](#) 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. Utilisez la commande **service-policy** pour activer un ensemble de stratégies sur une interface. **global** applique la carte de stratégie à toutes les interfaces et **interface** applique la stratégie à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la stratégie globale sur une interface en appliquant une stratégie de service à cette interface. Vous ne pouvez appliquer qu'une seule carte de stratégie à chaque interface.

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

Voici un exemple de configuration pour le contournement d'état 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
```

Vérification

La commande [show conn](#) affiche le nombre de connexions TCP et UDP actives et fournit des informations sur les connexions de différents types. Afin d'afficher l'état de la connexion pour le type de connexion désigné, utilisez la commande [show conn](#) en 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 TCP** inclut l'indicateur **b**.

Dépannage

Message d'erreur

ASA affiche ce message d'erreur même après l'activation de la fonctionnalité de contournement d'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 ont été abandonnés par l'appliance de sécurité en raison des contrôles de sécurité ajoutés par la fonctionnalité ICMP avec état qui sont généralement des réponses d'écho ICMP sans demande d'écho valide déjà passée sur l'appliance de sécurité ou des messages d'erreur ICMP non liés à une session TCP, UDP ou ICMP déjà établie dans l'appliance de sécurité.

ASA affiche ce journal même si le contournement de l'état TCP est activé car la désactivation de cette fonctionnalité (c'est-à-dire la vérification des entrées de retour ICMP pour le type 3 dans la table de connexion) n'est pas possible. Mais la fonction de contournement de l'état TCP fonctionne correctement.

Utilisez cette commande afin d'empêcher l'affichage de ces messages :

```
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](#)