Konfigurieren der Funktion zum Umgehen des TCP-Zustands auf der Serie ASA 5500

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Funktion zur Umgehung des TCP-Zustands konfiguriert wird, mit der der ausgehende und der eingehende Datenverkehr über separate Cisco Adaptive Security Appliances (ASAs) der Serie ASA 5500 fließen kann.

Voraussetzungen

Anforderungen

Bevor Sie mit der in diesem Dokument beschriebenen Konfiguration fortfahren können, muss auf der Cisco ASA mindestens die Basislizenz installiert sein.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Serie ASA 5500, auf der die Software Version 9.x ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Dieser Abschnitt bietet eine Übersicht über die Funktion zur Umgehung des TCP-Zustands und die zugehörigen Support-Informationen.

Übersicht über die Funktion zur Umgehung des TCP-Zustands

Standardmäßig wird der gesamte Datenverkehr, der über die ASA geleitet wird, über den Adaptive Security Algorithm geprüft und entweder anhand der Sicherheitsrichtlinie zugelassen oder verworfen. Um die Firewall-Leistung zu maximieren, prüft die ASA den Status jedes Pakets (z. B. prüft sie, ob es sich um eine neue Verbindung oder eine etablierte Verbindung handelt) und weist es entweder dem Sitzungs-Managementpfad (ein neues SYN-Paket), dem schnellen Pfad (eine etablierte Verbindung) oder dem Pfad der Kontrollebene (erweiterte Überprüfung) zu.

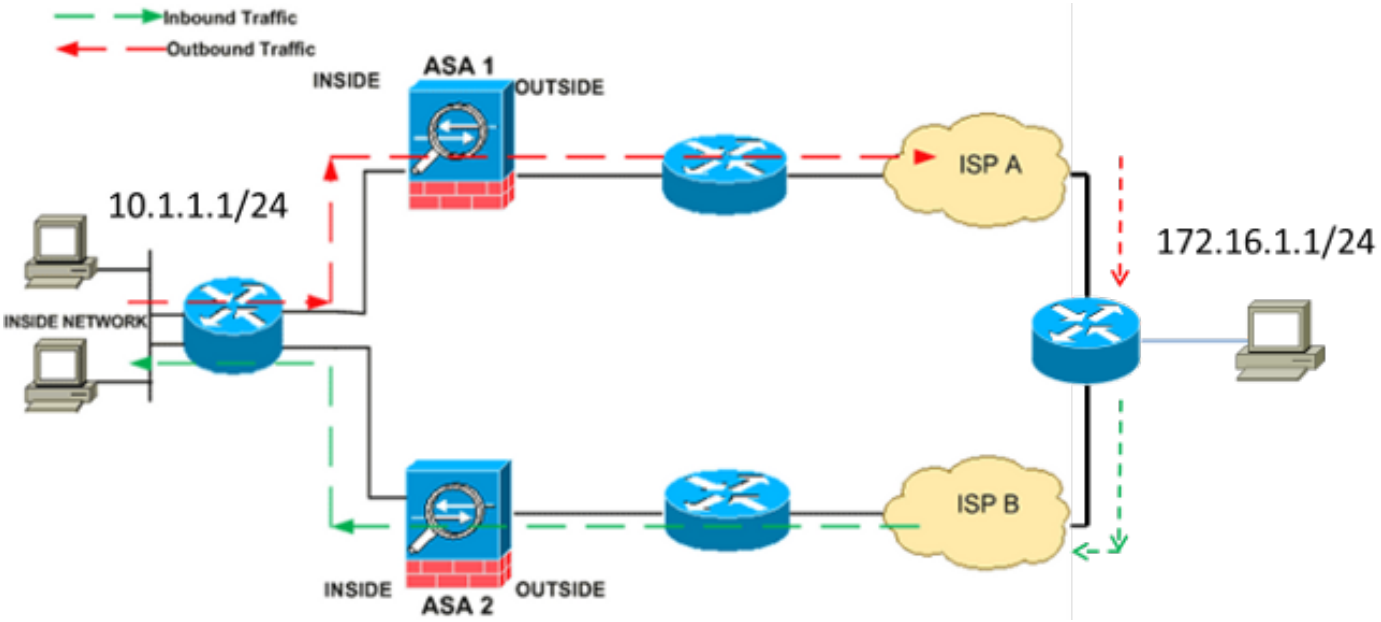
Die TCP-Pakete, die mit den aktuellen Verbindungen im schnellen Pfad übereinstimmen, können die ASA passieren, ohne jeden Aspekt der Sicherheitsrichtlinien erneut zu überprüfen. Diese Funktion maximiert die Leistung. Die Methode, die zum Herstellen der Sitzung im schnellen Pfad (bei der das SYN-Paket verwendet wird) und die Prüfungen im schnellen Pfad (z. B. die TCP-Sequenznummer) verwendet wird, kann jedoch asymmetrischen Routing-Lösungen im Wege stehen. Sowohl die ausgehenden als auch die eingehenden Datenflüsse einer Verbindung müssen über dieselbe ASA geleitet werden.

Beispielsweise wird eine neue Verbindung zur *ASA 1 hergestellt*. Das SYN-Paket durchläuft den Sitzungsverwaltungspfad, und der Fast Path-Tabelle wird ein Eintrag für die Verbindung hinzugefügt. Wenn nachfolgende Pakete auf dieser Verbindung über *ASA 1* laufen, stimmen die Pakete mit dem Eintrag im schnellen Pfad überein und werden weitergeleitet. Wenn nachfolgende Pakete an *ASA 2* gesendet werden, wo kein SYN-Paket über den Sitzungsverwaltungspfad vorhanden war, gibt es keinen Eintrag im schnellen Pfad für die Verbindung, und die Pakete werden verworfen.

Wenn auf den Upstream-Routern asymmetrisches Routing konfiguriert ist und der Datenverkehr zwischen zwei ASAs wechselt, können Sie die Funktion zur Umgehung des TCP-Zustands für bestimmten Datenverkehr konfigurieren. Die Funktion zur Umgehung des TCP-Zustands ändert die Art und Weise, wie Sitzungen im schnellen Pfad eingerichtet werden, und deaktiviert die Schnellpfadprüfungen. Diese Funktion behandelt TCP-Datenverkehr ähnlich wie UDP-Verbindungen: Wenn ein Paket ohne SYN-Verbindung, das mit den angegebenen Netzwerken übereinstimmt, in die ASA gelangt und es keinen schnellen Pfadeintrag gibt, dann durchläuft das Paket den Sitzungsverwaltungspfad, um die Verbindung im schnellen Pfad herzustellen. Wenn der

Datenverkehr im schnellen Pfad ist, umgeht er die Schnellpfadprüfungen.

Dieses Bild zeigt ein Beispiel für asymmetrisches Routing, bei dem der ausgehende Datenverkehr eine andere ASA durchläuft als der eingehende Datenverkehr:



Hinweis: Die Funktion zur Umgehung des TCP-Zustands ist auf der Cisco Serie ASA 5500 standardmäßig deaktiviert. Darüber hinaus kann die Konfiguration der TCP-Zustandsumgehung eine hohe Anzahl von Verbindungen verursachen, wenn sie nicht ordnungsgemäß implementiert ist.

Support-Informationen

In diesem Abschnitt werden die Support-Informationen für die Funktion zur Umgehung des TCP-Zustands beschrieben.

- **Context Mode** âÂ Â Die Funktion zur Umgehung des TCP-Zustands wird in Einzel- und Mehrfachkontext-Modi unterstützt.

- **Firewall Mode** âÂ Â Die Funktion zur Umgehung des TCP-Zustands wird in gerouteten und transparenten Modi unterstützt.

- **Failover** â Â Die Funktion zur Umgehung des TCP-Zustands unterstützt Failover.

Diese Funktionen werden bei Verwendung der Funktion zur Umgehung des TCP-Zustands nicht unterstützt:

- **Anwendungsinspektion** - Â Anwendungsprüfung erfordert, dass sowohl der ein- als auch der ausgehende Datenverkehr dieselbe ASA durchläuft, sodass die Anwendungsinspektion nicht mit der Funktion zur Umgehung des TCP-Zustands unterstützt wird.

- **Authentifizierungs-, Autorisierungs- und Abrechnungssitzungen (AAA)** Â Wenn ein Benutzer sich bei einer ASA authentifiziert, wird der Datenverkehr, der über die andere ASA zurückgegeben wird, abgelehnt, da der Benutzer sich nicht bei dieser ASA authentifiziert hat.

- **TCP-Intercept, maximale embryonale Verbindungsgrenze, TCP-Sequenznummer randomisierung** âÂ Â Die ASA verfolgt nicht den Zustand der Verbindung, sodass diese Funktionen nicht angewendet werden.

- **TCP Normalisierung** âÂ Â Der TCP-Normalisierer ist deaktiviert.

- **Security Services Module (SSM) und Security Services Card (SSC)-Funktionalität** - Â Â Sie können die Funktion zur Umgehung des TCP-Zustands bei Anwendungen, die auf einem SSM oder SSC ausgeführt werden, nicht verwenden, z. B. IPS oder Content Security (CSC).

Hinweis: Da die Übersetzungssitzung für jede ASA separat eingerichtet wird, stellen Sie sicher, dass Sie die statische Network Address Translation (NAT) auf beiden ASAs für den TCP-Status-Umgehungsverkehr konfigurieren. Wenn Sie dynamische NAT verwenden, unterscheidet sich die für die Sitzung auf der *ASA 1* gewählte Adresse von der Adresse, die für die Sitzung auf der *ASA 2* gewählt wurde.

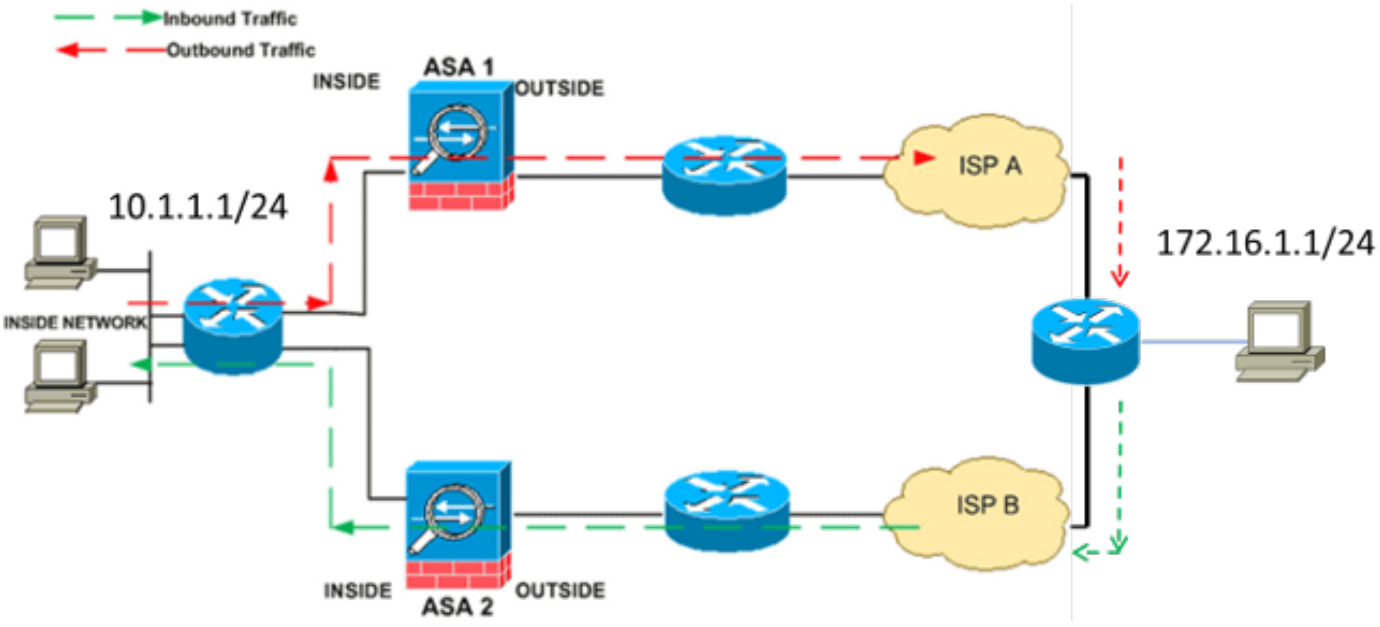
Konfigurieren

In diesem Abschnitt wird beschrieben, wie die Funktion zur Umgehung des TCP-Zustands auf der Serie ASA 5500 in zwei verschiedenen Szenarien konfiguriert wird.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen über die Befehle zu erhalten, die in diesem Abschnitt verwendet werden.

Szenario 1

Dies ist die Topologie, die für das erste Szenario verwendet wird:



Hinweis: Sie müssen die in diesem Abschnitt beschriebene Konfiguration auf beide ASAs

anwenden.

Gehen Sie wie folgt vor, um die Funktion zur TCP-Zustandsumgehung zu konfigurieren:

1. Geben Sie den Befehl **class-map class_map_name** ein, um eine *Klassenzuordnung* zu erstellen. Die Klassenzuordnung wird verwendet, um den Datenverkehr zu identifizieren, für den Sie die Stateful Firewall Inspection deaktivieren möchten.**Hinweis**: Die in diesem Beispiel verwendete Klassenzuordnung ist **tcp_bypass**.
   ```
   ASA(config)#class-map tcp_bypass
   ```
2. Geben Sie den Befehl **match**-Parameter ein, um den relevanten Datenverkehr in der Klassenzuordnung anzugeben. Wenn Sie das modulare Richtlinien-Framework verwenden, verwenden Sie den Befehl **match access-list** im *Klassenzuordnungs-Konfigurationsmodus*, um eine Zugriffsliste zur Identifizierung des Datenverkehrs zu verwenden, auf den Sie Aktionen anwenden möchten. Hier ein Beispiel für diese Konfiguration:

   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```
   Hinweis: Der **tcp_bypass** ist der Name der Zugriffsliste, die in diesem Beispiel verwendet wird. Weitere Informationen zur Angabe des Datenverkehrs finden Sie im Abschnitt Identifying Traffic (Layer 3/4 Class Map) im *Konfigurationshandbuch zur Cisco Serie ASA 5500 unter Verwendung der CLI 8.2*.
3. Geben Sie den Befehl **policy-map name** ein, um eine Richtlinienzuordnung hinzuzufügen oder eine (bereits vorhandene) Richtlinienzuordnung zu bearbeiten, die die für den angegebenen Klassenzuordnungs-Datenverkehr durchzuführenden Aktionen zuweist. Wenn Sie das modulare Richtlinien-Framework verwenden, verwenden Sie den Befehl **policy-map** (ohne das *type*-Schlüsselwort) im *globalen Konfigurationsmodus*, um dem Datenverkehr, den Sie mit einer Layer-3/4-Klassenzuordnung (**Class-Map** oder **Class-Map-Managementbefehl) identifiziert haben, Aktionen zuzuweisen.** In diesem Beispiel lautet die Richtlinienzuordnung **tcp_bypass_policy**:

   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```
4. Geben Sie den Befehl **class** im *Richtlinienzuordnungskonfigurationsmodus ein*, um die erstellte Klassenzuordnung (*tcp_bypass*) der Richtlinienzuordnung (*tcp_bypass_policy*) zuzuweisen, damit Sie die Aktionen dem Klassenzuweisungsverkehr zuweisen können. In diesem Beispiel lautet die Klassenzuordnung **tcp_bypass**:

   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
5. Geben Sie den Befehl **set connection advanced-options tcp-state-bypass** im *class configuration*-Modus ein, um die Funktion zur Umgehung des TCP-Zustands zu aktivieren. Dieser Befehl wurde in Version 8.2(1) eingeführt. Der *Klassenkonfigurationsmodus* ist über den *Richtlinienzuordnungs-Konfigurationsmodus* zugänglich, wie im folgenden Beispiel gezeigt:

   ```
   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. Geben Sie den **Service-Policy policy policy_map_name [global | interface *intf*]** im *globalen Konfigurationsmodus*, um eine Richtlinienzuordnung global auf allen Schnittstellen

oder auf einer Zielschnittstelle zu aktivieren. Um die Dienstrichtlinie zu deaktivieren, verwenden Sie die **no**-Form dieses Befehls. Geben Sie den Befehl **service-policy** ein, um eine Reihe von Richtlinien für eine Schnittstelle zu aktivieren. Das **globale** Schlüsselwort wendet die Richtlinienzuordnung auf alle Schnittstellen an, und das **interface**-Schlüsselwort wendet die Richtlinienzuordnung auf nur eine Schnittstelle an. Es ist nur eine globale Richtlinie zulässig. Um die globale Richtlinie für eine Schnittstelle zu überschreiben, können Sie eine Dienstrichtlinie auf diese Schnittstelle anwenden. Sie können auf jede Schnittstelle nur eine Richtlinienzuordnung anwenden. Hier ein Beispiel:

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

Nachfolgend finden Sie eine Beispielkonfiguration für die Funktion zur Umgehung des TCP-Zustands auf *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
```

Nachfolgend finden Sie eine Beispielkonfiguration für die Funktion zur Umgehung des TCP-Zustands auf *ASA2*:

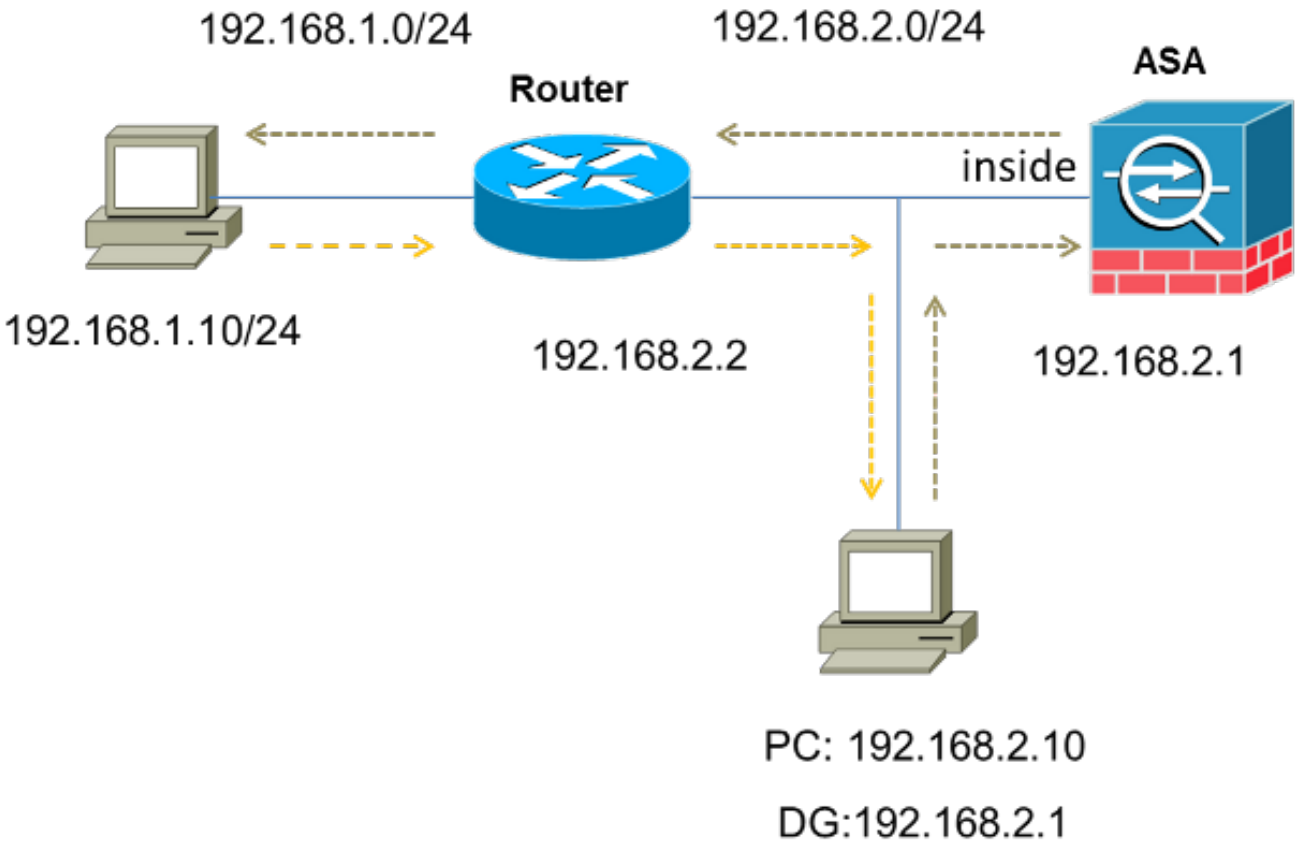
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.
```

```
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
```

Szenario 2

In diesem Abschnitt wird beschrieben, wie Sie die Funktion zur Umgehung des TCP-Zustands auf der ASA für Szenarien konfigurieren, die asymmetrisches Routing verwenden, bei dem der Datenverkehr über dieselbe Schnittstelle ein- und ausläuft (*u-Turn*).

Die folgende Topologie wird in diesem Szenario verwendet:



Gehen Sie wie folgt vor, um die Funktion zur TCP-Zustandsumgehung zu konfigurieren:

1. Erstellen Sie eine *Zugriffsliste*, um den Datenverkehr abzugleichen, der die TCP-Prüfung umgehen soll:

   ```
   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. Geben Sie den Befehl class-map class_map_name ein, um eine *Klassenzuordnung* zu erstellen. Die Klassenzuordnung wird verwendet, um den Datenverkehr zu identifizieren, für den Sie die Stateful Firewall Inspection deaktivieren möchten.**Hinweis**: Die in diesem Beispiel verwendete Klassenzuordnung ist **tcp_bypass**.
   ```
   ASA(config)#class-map tcp_bypass
   ```
3. Geben Sie den Befehl match-Parameter ein, um den für die Klassenzuordnung relevanten Datenverkehr anzugeben. Wenn Sie das modulare Richtlinien-Framework verwenden, verwenden Sie den Befehl **match access-list** im *Klassenzuordnungs-Konfigurationsmodus*, um eine Zugriffsliste zur Identifizierung des Datenverkehrs zu verwenden, auf den Sie Aktionen anwenden möchten. Hier ein Beispiel für diese Konfiguration:

   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```
   Hinweis: Der **tcp_bypass** ist der Name der Zugriffsliste, die in diesem Beispiel verwendet wird. Weitere Informationen zur Angabe des relevanten Datenverkehrs finden Sie im Abschnitt Identifizieren von Datenverkehr (Layer 3/4 Class Map) im *Konfigurationshandbuch zur Cisco Serie ASA 5500 unter Verwendung der CLI 8.2*.
4. Geben Sie den Befehl policy-map name ein, um eine Richtlinienzuordnung hinzuzufügen oder eine (bereits vorhandene) Richtlinienzuordnung zu bearbeiten, die die für den angegebenen Klassenzuordnungs-Datenverkehr zu ergreifenden Maßnahmen festlegt. Wenn Sie das Modular Policy Framework verwenden, verwenden Sie den Befehl **policy-map**

(ohne das *type*-Schlüsselwort) im *globalen Konfigurationsmodus*, um dem Datenverkehr, den Sie mit einer Layer-3/4-Klassenzuordnung identifiziert haben, die Aktionen zuzuweisen (**class-map** oder **class-map type management-Befehl).** In diesem Beispiel lautet die Richtlinienzuordnung **tcp_bypass_policy**:

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

5. Geben Sie den Befehl **class** im *Richtlinienzuordnungskonfigurationsmodus ein*, um die erstellte Klassenzuordnung (*tcp_bypass*) der Richtlinienzuordnung (*tcp_bypass_policy*) zuzuweisen, damit Sie dem Klassenzuordnungsdatenverkehr Aktionen zuweisen können. In diesem Beispiel lautet die Klassenzuordnung **tcp_bypass**:

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

6. Geben Sie den Befehl **set connection advanced-options tcp-state-bypass** im *class configuration*-Modus ein, um die Funktion zur Umgehung des TCP-Zustands zu aktivieren. Dieser Befehl wurde in Version 8.2(1) eingeführt. Der *Klassenkonfigurationsmodus* ist über den *Richtlinienzuordnungs-Konfigurationsmodus* zugänglich, wie im folgenden Beispiel gezeigt:

```
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. Geben Sie den **Service-Policy policy policy_map_name [global | interface *intf*]** Befehl im *globalen Konfigurationsmodus*, um eine Richtlinienzuordnung global auf allen Schnittstellen oder auf einer Zielschnittstelle zu aktivieren. Um die Dienstrichtlinie zu deaktivieren, verwenden Sie die **no-**Form dieses Befehls. Geben Sie den Befehl **service-policy** ein, um eine Reihe von Richtlinien für eine Schnittstelle zu aktivieren. Das **globale** Schlüsselwort wendet die Richtlinienzuordnung auf alle Schnittstellen an, und das **interface**-Schlüsselwort wendet die Richtlinie auf nur eine Schnittstelle an. Es ist nur eine globale Richtlinie zulässig. Um die globale Richtlinie für eine Schnittstelle zu überschreiben, können Sie eine Dienstrichtlinie auf diese Schnittstelle anwenden. Sie können auf jede Schnittstelle nur eine Richtlinienzuordnung anwenden. Hier ein Beispiel:

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

8. Geben Sie die gleiche Sicherheitsstufe für den Datenverkehr auf der ASA an:

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

Im Folgenden finden Sie ein Beispiel für eine Konfiguration der Funktion zur Umgehung des TCP-Zustands auf der 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
```

Überprüfen

Geben Sie Show Conn , um die Anzahl der aktiven TCP- und UDP-Verbindungen sowie Informationen über die Verbindungen verschiedener Typen anzuzeigen. Um den Verbindungsstatus für den festgelegten Verbindungstyp anzuzeigen, geben Sie die Show Conn im *privilegierten EXEC*-Modus.

> **Hinweis**: Dieser Befehl unterstützt IPv4- und IPv6-Adressen. Die Ausgabe, die für die Verbindungen angezeigt wird, die die Funktion zur Umgehung des TCP-Zustands verwenden, enthält das Flag **b**.

Hier ein Beispiel für die Ausgabe:

```
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
```

Fehlerbehebung

Für diese Funktion liegen keine spezifischen Informationen zur Fehlerbehebung vor. Allgemeine Informationen zur Behebung von Verbindungsproblemen finden Sie in diesen Dokumenten:

- ASA-Paketerfassung mit CLI- und ASDM-Konfigurationsbeispiel
- ASA 8.2: Paketfluss durch die Cisco ASA Firewall

  Hinweis: Die Verbindungen zum TCP-Status-Bypass werden nicht in einem Failover-Paar auf die Standby-Einheit repliziert.

Fehlermeldungen

Die ASA zeigt diese Fehlermeldung an, selbst wenn die Funktion zur Umgehung des TCP-Zustands aktiviert ist:

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

Die ICMP-Pakete (Internet Control Message Protocol) werden von der ASA aufgrund der Sicherheitsüberprüfungen verworfen, die durch die Stateful ICMP-Funktion hinzugefügt werden. Dabei handelt es sich in der Regel entweder um ICMP-*Echoantworten* ohne eine gültige *Echoanfrage*, die bereits über die ASA übergeben wurde, oder um ICMP-Fehlermeldungen, die sich nicht auf eine derzeit in der ASA eingerichtete TCP-, UDP- oder ICMP-Sitzung beziehen.

Die ASA zeigt dieses Protokoll an, selbst wenn die Funktion zur Umgehung des TCP-Zustands aktiviert ist, da die Deaktivierung dieser Funktion (d. h. die Überprüfung der ICMP-*Rückgabeeinträge* für Typ 3 in der Verbindungstabelle) nicht möglich ist. Die Funktion zur Umgehung des TCP-Zustands funktioniert jedoch ordnungsgemäß.

Geben Sie den folgenden Befehl ein, um die Darstellung dieser Meldungen zu verhindern:

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

Zugehörige Informationen

- Cisco Adaptive Security Device Manager
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems