ASA 8.2.X-Beispiel für eine Bypass-Funktion im TCP-Status

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Funktion zur Umgehung des TCP-Zustands konfiguriert wird. Diese Funktion ermöglicht ausgehende und eingehende Datenflüsse über separate Cisco Adaptive Security Appliances der Serie ASA 5500.

Voraussetzungen

Lizenzanforderungen

Die Cisco Adaptive Security Appliances der Serie ASA 5500 sollten über mindestens die Basislizenz verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance (ASA) mit Version 8.2(1) und höher.

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

Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Umgehung des TCP-Zustands

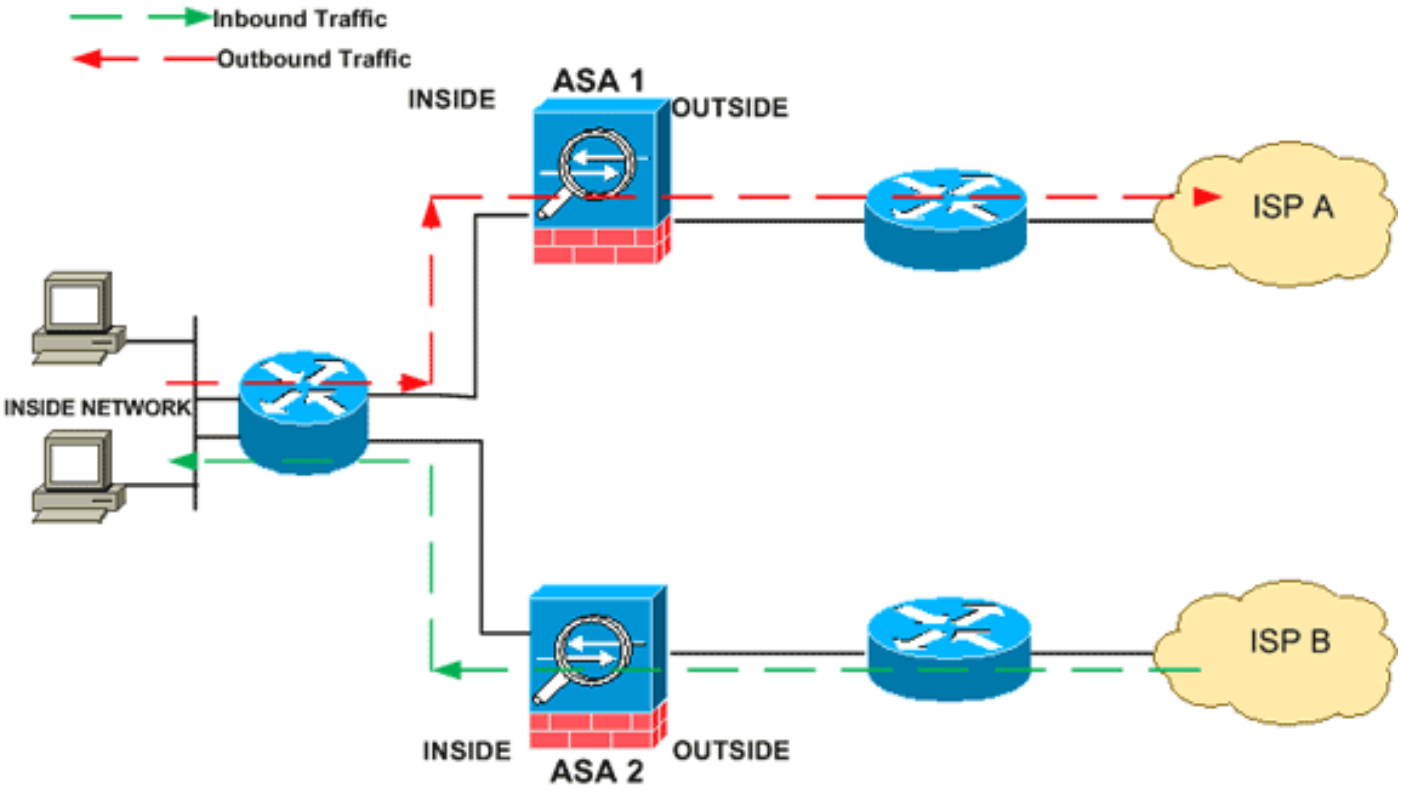
Standardmäßig wird der gesamte Datenverkehr, der über die Cisco Adaptive Security Appliance (ASA) geleitet wird, mit dem Adaptive Security Algorithm geprüft und entweder anhand der Sicherheitsrichtlinie zugelassen oder verworfen. Um die Firewall-Leistung zu maximieren, prüft die ASA den Zustand jedes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

TCP-Pakete, die mit vorhandenen Verbindungen im schnellen Pfad übereinstimmen, können die Adaptive Security Appliance passieren, ohne jeden Aspekt der Sicherheitsrichtlinie erneut zu überprüfen. Diese Funktion maximiert die Leistung. Die Methode 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) können jedoch asymmetrischen Routing-Lösungen im Wege stehen: sowohl der ausgehende als auch der eingehende Datenfluss 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 dieser Verbindung die *ASA 1* durchlaufen, stimmen die Pakete mit dem Eintrag im schnellen Pfad überein und werden durchgeleitet. 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 Upstream-Routern asymmetrisches Routing konfiguriert ist und der Datenverkehr zwischen zwei ASAs wechselt, können Sie die Umgehung des TCP-Zustands für bestimmten Datenverkehr konfigurieren. Der TCP-Status umgeht Änderungen an der 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 kein schneller Pfadeintrag vorhanden ist, 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 den Adaptive Security Appliances der Serie Cisco ASA 5500 standardmäßig deaktiviert.

Support-Informationen

Dieser Abschnitt enthält die Support-Informationen für die Funktion zur Umgehung des TCP-Zustands.

- Kontextmodus - Wird im Ein- und Mehrfachkontextmodus unterstützt.
- Firewall Mode (Firewall-Modus): Wird im Routing- und Transparenz-Modus unterstützt.
- Failover - Unterstützt Failover.

Diese Funktionen werden bei Verwendung der TCP-Zustandsumgehung nicht unterstützt:

- Anwendungsinspektion - Bei der Anwendungsinspektion muss sowohl ein- als auch ausgehender Datenverkehr dieselbe ASA passieren, sodass die Anwendungsinspektion nicht durch eine TCP-Zustandsumgehung unterstützt wird.
- AAA-authentifizierte Sitzungen - Wenn sich ein Benutzer bei einer ASA authentifiziert, wird der Datenverkehr, der über die andere ASA zurückgeleitet wird, abgelehnt, da sich der Benutzer nicht bei dieser ASA authentifiziert hat.
- TCP Intercept, maximale embryonale Verbindungsgrenze, Randomisierung der TCP-Sequenznummer - Die ASA verfolgt den Verbindungsstatus nicht. Daher werden diese Funktionen nicht angewendet.
- TCP normalization (TCP-Normalisierung): Der TCP-Normalisierer ist deaktiviert.
- SSM- und SSC-Funktionen - Sie können keine TCP-Zustandsumgehung und keine Anwendung verwenden, die auf einem SSM oder SSC ausgeführt wird, z. B. IPS oder CSC.

NAT-Richtlinien: Da die Übersetzungssitzung für jede ASA separat eingerichtet wird, müssen Sie für den TCP-Status-Bypass-Verkehr auf beiden ASAs eine statische NAT konfigurieren. Wenn Sie dynamische NAT verwenden, unterscheidet sich die für die Sitzung auf der *ASA 1* gewählte Adresse von der für die Sitzung auf der *ASA 2* gewählten Adresse.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie die Funktion zur Umgehung des TCP-Zustands auf der Cisco Adaptive Security Appliance (ASA) der Serie ASA 5500 konfiguriert wird.

Konfiguration der Funktion zur Umgehung des TCP-Zustands

Gehen Sie wie folgt vor, um die Funktion zur Umgehung des TCP-Zustands auf der Cisco Adaptive Security Appliance der Serie ASA 5500 zu konfigurieren:

1. Verwenden Sie den **Befehl** class-map class_map_name, um eine *Klassenzuordnung* zu erstellen. Die Klassenzuordnung wird verwendet, um den Datenverkehr zu identifizieren, für den Sie die Stateful Firewall Inspection deaktivieren möchten. Die in diesem Beispiel verwendete Klassenzuordnung ist *tcp_bypass*.
   ```
   ASA(config)#class-map tcp_bypass
   ```

2. Verwenden Sie den **Befehl match-Parameter**, um interessanten Datenverkehr in der Klassenzuordnung anzugeben. Verwenden Sie beim Verwenden des modularen Richtlinien-Framework den Befehl **match access-list** im Klassenzuordnungs-Konfigurationsmodus, um mithilfe einer Zugriffsliste den Datenverkehr zu identifizieren, 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
   ```

   tcp_bypass ist der Name der in diesem Beispiel verwendeten Zugriffsliste. Weitere Informationen zur Angabe des interessanten Datenverkehrs finden Sie in der Klassenübersicht zu Identifizieren (Layer 3/4).
3. Verwenden Sie den **Befehl policy-map name, um eine Richtlinienzuordnung hinzuzufügen oder eine (bereits vorhandene) Richtlinienzuordnung zu bearbeiten, die die Aktionen für den bereits angegebenen Klassenzuordnungsdatenverkehr festlegt.** Verwenden Sie bei Verwendung des modularen Richtlinien-Framework den Befehl **policy-map** (ohne das Schlüsselwort type) im globalen Konfigurationsmodus, um Aktionen für Datenverkehr zuzuweisen, der mit einer Layer-3/4-Klassenzuordnung (dem Befehl class-map oder class-map type management) identifiziert wurde. In diesem Beispiel lautet die Richtlinienzuordnung *tcp_bypass_policy*:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```

4. Verwenden Sie den Befehl **class im Richtlinienzuweisungskonfigurationsmodus, um der** Richtlinienzuordnung (*tcp_bypass_policy*) die bereits erstellte Klassenzuordnung (*tcp_bypass_policy*) zuzuweisen, in der Sie dem Klassenzuordnungs-Datenverkehr 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
   ```

5. Verwenden Sie den Befehl **set connection advanced-options tcp-state-bypass-bypass im** class configuration mode, um die Funktion zur Umgehung des TCP-Zustands zu aktivieren. Dieser Befehl wurde in Version 8.2(1) eingeführt. Auf den Klassenkonfigurationsmodus kann vom Konfigurationsmodus der Richtlinienzuordnung aus zugegriffen werden, wie in diesem 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. Verwenden Sie die **Dienstrichtlinienrichtlinie "policyMap_name" [global | interface *intf*] im globalen Konfigurationsmodus verwenden, 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. Verwenden Sie den Befehl **service-policy**, um eine Gruppe von Richtlinien für eine Schnittstelle zu aktivieren.**global** wendet die Richtlinienzuordnung auf alle Schnittstellen an und **Schnittstelle** wendet die Richtlinie auf eine Schnittstelle an. Es ist nur eine globale Richtlinie zulässig. Sie können die globale Richtlinie für eine Schnittstelle überschreiben, indem Sie eine Dienstrichtlinie auf diese Schnittstelle anwenden. Sie können auf jede Schnittstelle nur eine Richtlinienzuordnung anwenden.
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
   ```

Im Folgenden finden Sie eine Beispielkonfiguration für die Umgehung des TCP-Zustands:

```
!--- 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
```

Überprüfen

Der **Befehl show conn zeigt die Anzahl der aktiven TCP- und UDP-Verbindungen an und liefert Informationen über Verbindungen verschiedener Typen.** Um den Verbindungsstatus für den angegebenen Verbindungstyp anzuzeigen, verwenden Sie den **Befehl show conn im privilegierten EXEC-Modus.** Dieser Befehl unterstützt IPv4- und IPv6-Adressen. Die Ausgabe-Anzeige für Verbindungen, die **TCP-Zustandsumgehung** verwenden, enthält das Flag **b**.

Fehlerbehebung

Fehlermeldung

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
```

ICMP-Pakete wurden von der Sicherheits-Appliance verworfen, weil die Stateful ICMP-Funktion Sicherheitsüberprüfungen hinzugefügt hat, bei denen es sich in der Regel entweder um ICMP-Echo-Antworten ohne gültige Echo-Anfrage handelt, die bereits über die Sicherheits-Appliance weitergegeben wurden, oder um ICMP-Fehlermeldungen, die sich nicht auf bereits in der Sicherheits-Appliance eingerichtete TCP-, UDP- oder ICMP-Sitzungen beziehen.

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

Verwenden Sie diesen Befehl, um zu verhindern, dass diese Meldungen angezeigt werden:

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

Zugehörige Informationen

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