ASA 8.3: Herstellen und Beheben von Verbindungen über die Cisco Security Appliance

Inhalt

Einführung

Wenn eine Cisco Adaptive Security Appliance (ASA) anfänglich konfiguriert wird, verfügt sie über eine Standard-Sicherheitsrichtlinie, bei der jeder interne Benutzer herauskommen kann und niemand von außen hereinkommen kann. Wenn für Ihre Site eine andere Sicherheitsrichtlinie erforderlich ist, können Sie externen Benutzern gestatten, über die ASA eine Verbindung zu Ihrem Webserver herzustellen.

Sobald Sie über die Cisco ASA eine grundlegende Verbindung herstellen, können Sie Konfigurationsänderungen an der Firewall vornehmen. Stellen Sie sicher, dass alle Konfigurationsänderungen, die Sie an der ASA vornehmen, den Sicherheitsrichtlinien Ihres Standorts entsprechen.

Weitere Informationen finden Sie unter PIX/ASA: Herstellen und Beheben von Verbindungsproblemen über die Cisco Security Appliance für die identische Konfiguration auf der Cisco ASA mit Version 8.2 oder früher

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass einige grundlegende Konfigurationen bereits auf der Cisco ASA abgeschlossen wurden. Beispiele einer Erstkonfiguration der ASA finden Sie in

diesen Dokumenten:

- ASA 8.3(x): Anschließen eines einzelnen internen Netzwerks an das Internet
- Konfigurieren des PPPoE-Clients auf einer Cisco Adaptive Security Appliance (ASA)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer Cisco Adaptive Security Appliance (ASA), die Version 8.3 und höher ausführt.

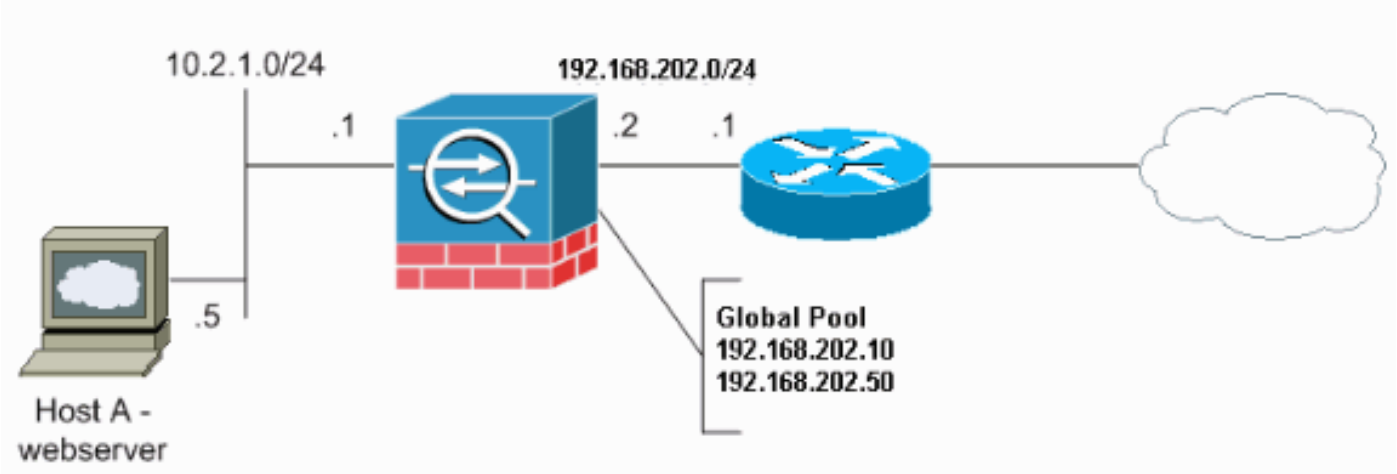
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines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

Konventionen

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

So funktioniert die ASA-Konnektivität

In diesem Netzwerk ist Host A der Webserver mit der internen Adresse 10.2.1.5. Dem Webserver wird die externe (übersetzte) Adresse 192.168.202.5 zugewiesen. Internetbenutzer müssen auf 192.168.202.5 verweisen, um auf den Webserver zugreifen zu können. Der DNS-Eintrag für Ihren Webserver muss diese Adresse sein. Aus dem Internet sind keine anderen Verbindungen zulässig.



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet werden.

Konnektivität über die Cisco ASA konfigurieren

Gehen Sie wie folgt vor, um die Verbindung über die ASA zu konfigurieren:

1. Erstellen Sie ein Netzwerkobjekt, das das interne Subnetz und ein anderes Netzwerkobjekt

für den IP-Pool-Bereich definiert. Konfigurieren Sie die NAT mithilfe der folgenden Netzwerkobjekte:

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. Weisen Sie dem internen Host, auf den Internetbenutzer Zugriff haben, eine statische übersetzte Adresse zu.

```
object network obj-10.2.1.5
  host 10.2.1.5
  nat (inside,outside) static 192.168.202.5
```

3. Verwenden Sie den **Zugriffslisten-**Befehl, um externe Benutzer über die Cisco ASA zuzulassen. Verwenden Sie immer die übersetzte Adresse im Befehl **access-list**.

```
access-list 101 permit tcp any host 192.168.202.5 eq www
  access-group 101 in interface outside
```

ARP-Broadcast-Datenverkehr zulassen

Die Sicherheits-Appliance verbindet dasselbe Netzwerk über die interne und externe Schnittstelle. Da die Firewall kein gerouteter Hop ist, können Sie problemlos eine transparente Firewall in ein bestehendes Netzwerk einführen. IP-Adressierung ist nicht erforderlich. Der IPv4-Datenverkehr wird automatisch von einer höheren Sicherheitsschnittstelle zu einer niedrigeren Sicherheitsschnittstelle ohne Zugriffsliste über die transparente Firewall zugelassen. Adressenauflösungsprotokolle (Address Resolution Protocols, ARPs) sind ohne Zugriffsliste in beide Richtungen durch die transparente Firewall zugelassen. ARP-Datenverkehr kann durch ARP-Inspektion gesteuert werden. Für Layer-3-Datenverkehr, der von einer Schnittstelle mit niedriger bis hin zu einer Schnittstelle mit hoher Sicherheit übertragen wird, ist eine erweiterte Zugriffsliste erforderlich.

Hinweis: Die Security Appliance im transparenten Modus übergibt keine Cisco Discovery Protocol (CDP)-Pakete oder IPv6-Pakete oder Pakete, die keinen gültigen EtherType größer oder gleich 0x600 haben. Zum Beispiel können keine IS-IS-Pakete übergeben werden. Eine Ausnahme bilden BPDUs (Bridge Protocol Data Units), die unterstützt werden.

Zulässige MAC-Adressen

Diese MAC-Zieladressen sind über die transparente Firewall zugelassen. MAC-Adressen, die nicht in dieser Liste aufgeführt sind, werden verworfen:

- WAHRE Broadcast-Ziel-MAC-Adresse gleich FFFF.FFFF.FFFF
- IPv4-Multicast-MAC-Adressen von 0100.5E00.000 bis 0100.5EFE.FFFF
- IPv6-Multicast-MAC-Adressen von 333.000.000 bis 3333.FFFF.FFFF
- BPDU-Multicast-Adresse gleich 0100.0CCC.CCCD

- Appletalk Multicast MAC-Adressen von 0900.0700.000 bis 0900.07FF.FFFF

Datenverkehr darf im Router-Modus nicht weitergeleitet werden

Im Router-Modus können einige Datenverkehrsarten die Sicherheits-Appliance nicht passieren, selbst wenn Sie sie in einer Zugriffsliste zulassen. Die transparente Firewall kann jedoch nahezu jeden Datenverkehr über eine erweiterte Zugriffsliste (für IP-Datenverkehr) oder eine EtherType-Zugriffsliste (für Nicht-IP-Datenverkehr) zulassen.

Beispielsweise können Sie Routing-Protokoll-Adjacencies über eine transparente Firewall einrichten. Sie können auf Basis einer erweiterten Zugriffsliste Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) oder Border Gateway Protocol (BGP)-Datenverkehr zulassen. Ebenso können Protokolle wie Hot Standby Router Protocol (HSRP) oder Virtual Router Redundancy Protocol (VRRP) die Sicherheits-Appliance passieren.

Nicht-IP-Datenverkehr (z. B. AppleTalk, IPX, BPDUs und MPLS) kann mithilfe einer EtherType-Zugriffsliste für den Durchlauf konfiguriert werden.

Bei Funktionen, die nicht direkt von der transparenten Firewall unterstützt werden, können Sie die Durchleitung des Datenverkehrs zulassen, sodass Upstream- und Downstream-Router die Funktionalität unterstützen. Mithilfe einer erweiterten Zugriffsliste können Sie beispielsweise DHCP-Datenverkehr (Dynamic Host Configuration Protocol) (anstelle der nicht unterstützten DHCP-Relay-Funktion) oder Multicast-Datenverkehr wie IP/TV zulassen.

Beheben von Verbindungsproblemen

Wenn Internetbenutzer nicht auf Ihre Website zugreifen können, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie die Konfigurationsadressen korrekt eingegeben haben:Gültige externe AdresseRichtige interne AdresseExterner DNS hat übersetzte Adresse
2. Überprüfen Sie die externe Schnittstelle auf Fehler.Die Cisco Security Appliance ist vorkonfiguriert, um die Geschwindigkeit- und Duplexeinstellungen einer Schnittstelle automatisch zu erkennen. Es gibt jedoch mehrere Situationen, die zu einem Fehlschlagen des automatischen Aushandlungsprozesses führen können. Dies führt entweder zu Geschwindigkeits- oder Duplex-Diskrepanzen (und Leistungsproblemen). In geschäftskritischen Netzwerkinfrastrukturen werden Geschwindigkeit und Duplex auf jeder Schnittstelle von Cisco manuell hardcodiert, sodass keine Fehlerquelle besteht. Diese Geräte bewegen sich im Allgemeinen nicht. Wenn Sie sie also richtig konfigurieren, sollten Sie sie nicht ändern müssen.**Beispiel:**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex full
   asa(config-if)#speed 100
   asa(config-if)#exit
   ```

   In einigen Situationen führt die Hardwarekodierung der Geschwindigkeit und der Duplexeinstellungen zu Fehlern. Daher müssen Sie die Schnittstelle auf die Standardeinstellung des Auto-Detection-Modus konfigurieren, wie im folgenden Beispiel gezeigt:**Beispiel:**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex auto
   ```

```
asa(config-if)#speed auto
asa(config-if)#exit
```

3. Wenn der Datenverkehr nicht über die ASA-Schnittstelle oder den Headend-Router gesendet oder empfangen wird, versuchen Sie, die ARP-Statistiken zu löschen.
```
asa#clear arp
```

4. Verwenden Sie das **show run object** und **show run static** Commands, um sicherzustellen, dass die statische Übersetzung aktiviert ist.**Beispiel:**

```
object service www
service tcp source eq www
object network 192.168.202.2
host 192.168.202.2
object network 10.2.1.5
host 10.2.1.5
object service 1025
service tcp source eq 1025
nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
```

In diesem Szenario wird die externe IP-Adresse als zugeordnete IP-Adresse für den Webserver verwendet.

```
nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
```

5. Überprüfen Sie, ob die Standardroute auf den Webserver auf die interne Schnittstelle der ASA verweist.
6. Überprüfen Sie die Übersetzungstabelle mit dem Befehl **show xlate**, um festzustellen, ob die Übersetzung erstellt wurde.
7. Verwenden Sie den Befehl **logging puffered** , um die Protokolldateien zu überprüfen, um festzustellen, ob eine Verweigerung auftritt. (Suchen Sie nach der übersetzten Adresse, und prüfen Sie, ob Sie eine Ablehnung sehen.)
8. Verwenden Sie den Befehl **capture**:

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

Hinweis: Dieser Befehl generiert eine große Menge an Ausgabe. Dies kann dazu führen, dass ein Router bei starker Datenverkehrslast hängen oder neu geladen wird.

9. Wenn Pakete an die ASA gesendet werden, stellen Sie sicher, dass Ihre Route zum Webserver von der ASA richtig ist. (Überprüfen Sie die **Route-**Befehle in Ihrer ASA-Konfiguration.)
10. Überprüfen Sie, ob die Proxy-ARP deaktiviert ist. Geben Sie den Befehl **show running-config sysopt** in ASA 8.3 ein.In diesem Fall wird die Proxy-ARP durch den **externen** Befehl **sysopt noproxyarp** deaktiviert:
```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
```

```
sysopt connection permit-vpn
```

Geben Sie den folgenden Befehl im globalen Konfigurationsmodus ein, um den Proxy-ARP erneut zu aktivieren:

```
ciscoasa(config)#no sysopt noproxyarp outside
```

Wenn ein Host IP-Datenverkehr an ein anderes Gerät im gleichen Ethernet-Netzwerk sendet, muss der Host die MAC-Adresse des Geräts kennen. ARP ist ein Layer-2-Protokoll, das eine IP-Adresse in eine MAC-Adresse auflöst. Ein Host sendet eine ARP-Anfrage und fragt: "Wer ist diese IP-Adresse?" Das Gerät, dem die IP-Adresse gehört, antwortet: "Ich besitze diese IP-Adresse. Hier ist meine MAC-Adresse."Proxy-ARP ermöglicht der Sicherheits-Appliance, eine ARP-Anfrage im Namen von Hosts zu beantworten, die sich dahinter befinden. Hierzu antwortet sie auf ARP-Anfragen für die statischen zugeordneten Adressen dieser Hosts. Die Sicherheits-Appliance antwortet auf die Anfrage mit einer eigenen MAC-Adresse und leitet die IP-Pakete dann an den entsprechenden internen Host weiter.Wenn beispielsweise im Diagramm in diesem Dokument eine ARP-Anfrage für die globale IP-Adresse des Webservers (192.168.202.5) erfolgt, antwortet die Sicherheits-Appliance mit ihrer eigenen MAC-Adresse. Wenn Proxy-ARP in dieser Situation nicht aktiviert ist, können Hosts im externen Netzwerk der Sicherheits-Appliance den Webserver nicht erreichen, indem sie eine ARP-Anfrage für die Adresse 192.168.202.5 senden. Weitere Informationen zum sysopt-Befehl finden Sie in der Befehlsreferenz.

11. Wenn alles korrekt angezeigt wird und Benutzer immer noch nicht auf den Webserver zugreifen können, erstellen Sie ein Ticket beim technischen Support von Cisco.

Fehlermeldung - %ASA-4-407001:

Einige Hosts können keine Verbindung zum Internet herstellen und die `Fehlermeldung - %ASA-4-407001: Der Datenverkehr für die Schnittstelle_Name des lokalen Hosts:inside_address, die` Fehlermeldung`, dass die Lizenzgrenze der Anzahl überschritten wurde,` wird im Syslog empfangen. Wie wird dieser Fehler behoben?

Diese Fehlermeldung wird angezeigt, wenn die Anzahl der Benutzer die Benutzergrenze der verwendeten Lizenz überschreitet. Um diesen Fehler zu beheben, aktualisieren Sie die Lizenz auf eine höhere Anzahl von Benutzern. Dabei kann es sich je nach Bedarf um eine Lizenz für 50, 100 oder eine unbegrenzte Anzahl von Benutzern handeln.

Zugehörige Informationen

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