ASA Version 9.(x) Verbindung von drei internen Netzwerken mit Internet-Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält Informationen zum Einrichten der Cisco Adaptive Security Appliance (ASA) Version 9.1(5) für die Verwendung in drei internen Netzwerken. Zur Vereinfachung werden auf den Routern statische Routen verwendet.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance (ASA) Version 9.1(5).

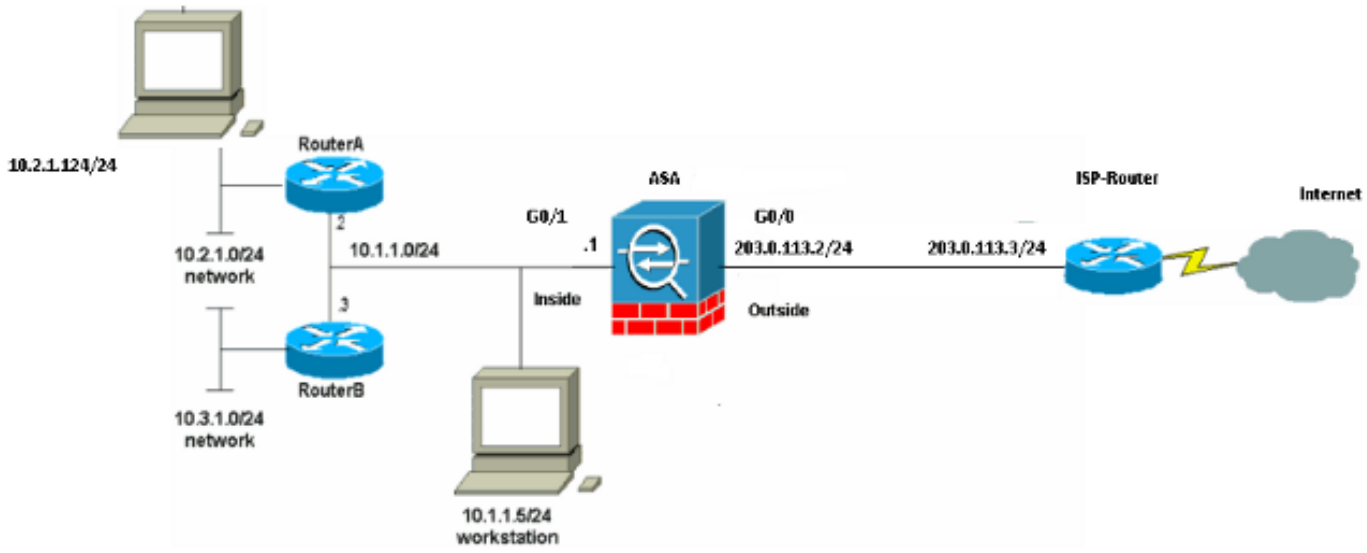
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines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

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



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

ASA 9.1-Konfiguration

In diesem Dokument werden diese Konfigurationen verwendet. Wenn Sie die Ausgabe eines **Write Terminal**-Befehls von Ihrem Cisco Gerät haben, können Sie Output Interpreter (nur registrierte Kunden) verwenden, um potenzielle Probleme und Fixes anzuzeigen.

Konfigurationen

- Router A-Konfiguration
- Router B-Konfiguration
- ASA Version 9.1 und spätere Konfiguration

Router A-Konfiguration

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
```

```
line con 0
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password ww
login
!
!
end

RouterA#
```

Router B-Konfiguration

```
RouterB#show running-config
Building configuration...

Current configuration : 1132 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
```

```
duplex auto
speed auto
no cdp enable
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#
```

ASA Version 9.1 und spätere Konfiguration

```
ASA#show run
: Saved
:
ASA Version 9.1(5)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
```

```
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa915-k8.bin

ftp mode passive

!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- Output Suppressed

!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- object will get PAT to the outside interface IP
!--- on the ASA (or 10.165.200.226) for internet bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface

!--- Output Suppressed

!--- Define a default route to the ISP router.


route outside 0.0.0.0 0.0.0.0 203.0.113.3 1

!--- Define a route to the INTERNAL router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Versuchen Sie, über HTTP mit einem Webbrowser auf eine Website zuzugreifen. In diesem Beispiel wird eine Site verwendet, die unter 198.51.100.100 gehostet wird. Wenn die Verbindung erfolgreich hergestellt wurde, wird diese Ausgabe in der ASA CLI angezeigt.

Verbindung

```
ASA(config)# show connection address 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
```

```
flags UIO
```

Die ASA ist eine Stateful-Firewall, und der Rückverkehr vom Webserver wird durch die Firewall zugelassen, da er mit einer ***Verbindung*** in der Firewall-Verbindungstabelle übereinstimmt. Datenverkehr, der mit einer vorbestehenden Verbindung übereinstimmt, wird durch die Firewall zugelassen und nicht durch eine Schnittstellen-ACL blockiert.

In der vorherigen Ausgabe hat der Client auf der internen Schnittstelle eine Verbindung zum Host 198.51.100.100 der externen Schnittstelle hergestellt. Diese Verbindung wird mit dem TCP-Protokoll hergestellt und ist seit sechs Sekunden inaktiv. Die Verbindungsflags zeigen den aktuellen Status dieser Verbindung an. Weitere Informationen zu Verbindungsflags finden Sie in den ASA TCP-Verbindungsflags.

Syslog

```
ASA(config)# show log | include 10.2.1.124

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.2.1.124/18711 (203.0.113.2/18711)
```

Die ASA-Firewall erzeugt im Normalbetrieb Syslogs. Die Syslogs sind abhängig von der Protokollierungskonfiguration ausführlich dargestellt. Die Ausgabe zeigt zwei Syslogs, die auf Stufe 6 angezeigt werden, oder 'informational' Level.

In diesem Beispiel werden zwei Syslogs generiert. Die erste ist eine Protokollmeldung, die anzeigt, dass die Firewall eine Übersetzung erstellt hat, insbesondere eine dynamische TCP-Übersetzung (Dynamic TCP Translation, PAT). Es gibt die Quell-IP-Adresse und den Port sowie die übersetzte IP-Adresse und den übersetzten Port an, wenn der Datenverkehr von innen zu den externen Schnittstellen verläuft.

Das zweite Syslog gibt an, dass die Firewall eine Verbindung in ihrer Verbindungstabelle für diesen spezifischen Datenverkehr zwischen Client und Server erstellt hat. Wenn die Firewall konfiguriert wurde, um diesen Verbindungsversuch zu blockieren, oder ein anderer Faktor die Erstellung dieser Verbindung behinderte (Ressourcenbeschränkungen oder eine mögliche Fehlkonfiguration), würde die Firewall kein Protokoll generieren, das angibt, dass die Verbindung hergestellt wurde. Stattdessen wird ein Grund für die Ablehnung der Verbindung oder ein Hinweis darauf angegeben, welcher Faktor die Verbindung verhindert.

NAT-Übersetzungen

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 timeout 0:00:30
```

Im Rahmen dieser Konfiguration wird PAT so konfiguriert, dass die internen Host-IP-Adressen in Adressen übersetzt werden, die im Internet routbar sind. Um zu bestätigen, dass diese Übersetzungen erstellt wurden, können Sie die Tabelle NAT-Übersetzungen (Xlate) überprüfen. Der Befehl **show xlate** zeigt in Kombination mit dem **lokalen** Schlüsselwort und der IP-Adresse des internen Hosts alle Einträge, die in der Übersetzungstabelle für diesen Host enthalten sind. Die

vorherige Ausgabe zeigt, dass für diesen Host derzeit eine Übersetzung zwischen der internen und der externen Schnittstelle erstellt wird. Die interne Host-IP-Adresse und der interne Port werden in die Adresse 203.0.113.2 pro Konfiguration übersetzt. Die aufgeführten Flags r i geben an, dass die Übersetzung **dynamisch** und eine **Portmap** ist. Weitere Informationen zu verschiedenen NAT-Konfigurationen finden Sie in Information About NAT.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Die ASA bietet mehrere Tools zur Behebung von Verbindungsproblemen. Wenn das Problem weiterhin besteht, nachdem Sie die Konfiguration überprüft und die zuvor aufgelistete Ausgabe überprüft haben, können diese Tools und Techniken dabei helfen, die Ursache für den Verbindungsfehler zu ermitteln.

Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 10.2.1.124 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Mit der Packet Tracer-Funktion auf der ASA können Sie ein simuliertes Paket angeben und alle Schritte, Überprüfungen und Funktionen anzeigen, die die Firewall durchläuft, wenn sie Datenverkehr verarbeitet. Mit diesem Tool ist es hilfreich, ein Beispiel für Datenverkehr zu identifizieren, der Ihrer Meinung nach über die Firewall passieren darf, und diesen 5-Tupel zu verwenden, um Datenverkehr zu simulieren. Im vorherigen Beispiel wird der Paket-Tracer verwendet, um einen Verbindungsversuch zu simulieren, der die folgenden Kriterien erfüllt:

- Das simulierte Paket kommt **innen** an.
- Das verwendete Protokoll ist **TCP**.
- Die simulierte Client-IP-Adresse ist **10.2.1.124**.
- Der Client sendet Datenverkehr, der von Port **1234 stammt**.
- Der Datenverkehr ist für einen Server mit der IP-Adresse **198.51.100.100** bestimmt.
- Der Datenverkehr ist für Port **80** bestimmt.

Beachten Sie, dass die Schnittstelle **außerhalb** des Befehls nicht erwähnt wurde. Dies erfolgt über das Paket-Tracer-Design. Das Tool erklärt Ihnen, wie die Firewall diesen Verbindungsversuch verarbeitet, einschließlich der Art der Weiterleitung und der Schnittstelle. Weitere Informationen zu Packet Tracer finden Sie unter Tracing Packets with Packet Tracer.

Erfassung

```
ASA# capture capin interface inside match tcp host 10.2.1.124 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#   show capture capin

3 packets captured

  1: 11:31:23.432655       10.2.1.124.18711 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518       198.51.100.100.80 > 10.2.1.124.18711: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.18711 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472       198.51.100.100.80 > 203.0.113.2.18711: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       203.0.113.2.18711 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

Die ASA-Firewall kann den ein- oder ausgehenden Datenverkehr der Schnittstellen erfassen. Diese Erfassungsfunktion ist fantastisch, da sie definitiv belegen kann, ob der Datenverkehr eine Firewall erreicht oder verlässt. Im vorherigen Beispiel wurde die Konfiguration von zwei Aufnahmen mit dem Namen **capin** und **capout** auf der Innen- und Außenschnittstelle veranschaulicht. Die Erfassungsbefehle verwenden das **match**-Schlüsselwort, mit dem Sie festlegen können, welcher Datenverkehr erfasst werden soll.

Für die **Capin** der Erfassung wurde angegeben**,** dass Sie den auf der internen Schnittstelle (ein- oder ausgehend) sichtbaren Datenverkehr, der mit dem **TCP-Host 10.2.1.124 Host 198.51.100.100** übereinstimmt, **abgleichen möchten**. Mit anderen Worten, Sie möchten jeden TCP-Datenverkehr erfassen, der von **Host 10.2.1.124** an **Host 198.51.100.100** gesendet wird oder **umgekehrt**. Durch die Verwendung des **match**-Schlüsselworts kann die Firewall diesen Datenverkehr bidirektional erfassen. Der für die externe Schnittstelle definierte Erfassungsbefehl verweist nicht auf die interne Client-IP-Adresse, da die Firewall PAT für diese Client-IP-Adresse durchführt. Infolgedessen können Sie nicht mit dieser Client-IP-Adresse **übereinstimmen**. Stattdessen wird in diesem Beispiel **jeder** verwendet, um anzugeben, dass alle möglichen IP-Adressen mit dieser Bedingung übereinstimmen.

Nachdem Sie die Captures konfiguriert haben, versuchen Sie erneut, eine Verbindung herzustellen, und zeigen die Captures mit dem Befehl **show capture *<capture_name>*** an. In diesem Beispiel sehen Sie, dass der Client eine Verbindung zum Server herstellen konnte, wie der TCP-3-Way-Handshake in den Erfassungen zeigt.