ASA 8.4(x) verbindet ein einzelnes internes Netzwerk mit dem Konfigurationsbeispiel für das Internet

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Cisco Adaptive Security Appliance (ASA) mit Version 8.4(1) für die Verwendung in einem internen Netzwerk einrichten.

Weitere Informationen finden Sie unter PIX/ASA: Anschließen eines internen Netzwerks mit Internetkonfigurationsbeispiel für dieselbe Konfiguration auf der ASA mit Version 8.2 und früher.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der ASA mit Version 8.4(1).

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

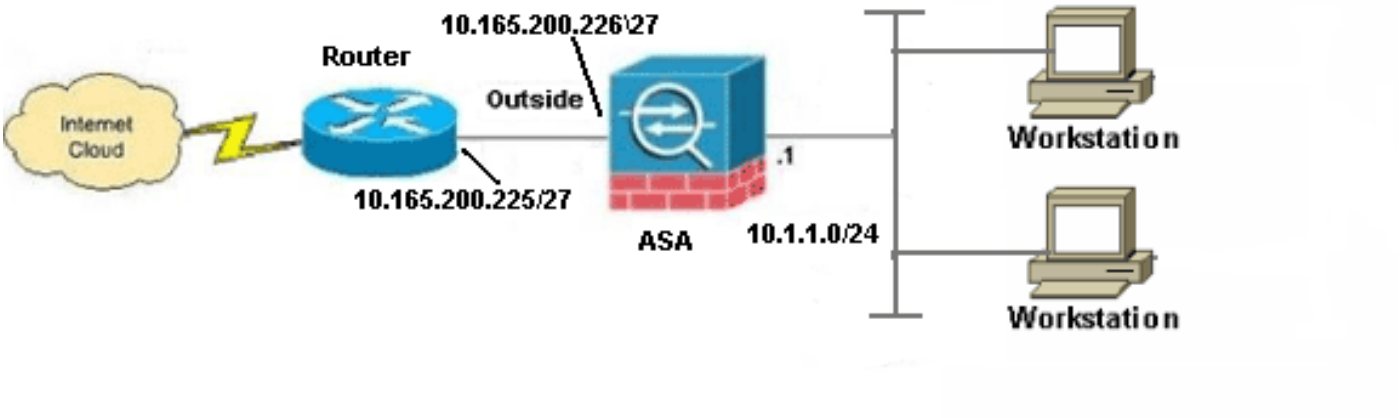
Konfigurieren

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

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

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



> **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.

ASA 8.4-Konfiguration

In diesem Dokument werden folgende Konfigurationen verwendet:

- Routerkonfiguration
- ASA 8.4 und spätere Konfiguration

Routerkonfiguration

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

ASA 8.4 und spätere Konfiguration

```
ASA#show run
: Saved
:
ASA Version 8.4(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface.

!
```

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.165.200.226 255.255.255.224

!--- Configure the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (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
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
```

```
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

Hinweis: Weitere Informationen zur Konfiguration von Network Address Translation (NAT) und Port Address Translation (PAT) auf ASA Version 8.4 finden Sie unter Informationen zu NAT.

Weitere Informationen zur Konfiguration von Zugriffslisten auf ASA Version 8.4 finden Sie unter Informationen zu Zugriffslisten.

Überprüfen

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 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, idle 0:00:06, bytes 937,
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 bereits vorhandenen Verbindung übereinstimmt, wird durch die Firewall zugelassen, ohne durch eine Schnittstelle-ACL blockiert zu werden.

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 | in 10.1.1.154

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.1.1.154/58799 to outside:10.165.200.226/58799

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:10.1.1.154/58799 (10.165.200.226/58799)
```

Die ASA-Firewall erzeugt im Normalbetrieb Syslogs. Die Syslogs sind abhängig von der Protokollierungskonfiguration ausführlich dargestellt. Die Ausgabe zeigt zwei Syslogs, die auf Ebene 6 angezeigt werden, bzw**. "informational"**.

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 (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 für diesen spezifischen Datenverkehr zwischen Client und Server eine **Verbindung** in der Verbindungstabelle 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 (Xlate)

```
ASA(config)# show xlate local 10.1.1.154
3 in use, 80 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:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 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 "Übersetzung" 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 pro Konfiguration in die Adresse 10.165.200.226 übersetzt. Die aufgeführten Flags r i **geben** an, dass die Übersetzung **dynamisch** und eine **Portmap** ist. Weitere Informationen zu verschiedenen NAT-Konfigurationen finden Sie hier: Informationen zu NAT.

Fehlerbehebung

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 10.1.1.154 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 weitergeleitet werden *sollte*, und diese 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 **10.1.1.154**.
- 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 in Tracing-Paketen mit Packet Tracer.

Erfassung

```
ASA# capture capin interface inside match tcp host 10.1.1.154 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       10.1.1.154.58799 > 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 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       10.165.200.226.58799 > 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 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       10.165.200.226.58799 > 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 haben Sie angegeben**,** dass Sie den auf der internen Schnittstelle (Eingang oder Ausgang) sichtbaren Datenverkehr, der mit **TCP-Host 10.1.1.154 Host 198.51.100.100** übereinstimmt, **abgleichen möchten**. Mit anderen Worten, Sie möchten jeden TCP-Datenverkehr erfassen, der von **Host 10.1.1.154** 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, würden Sie erneut versuchen, eine Verbindung herzustellen, und die Captures mit dem Befehl **show capture** ***<capture_name>*** anzeigen. In diesem Beispiel sehen Sie, dass der Client eine Verbindung zum Server herstellen konnte, wie der TCP-3-Way-Handshake in den Erfassungen zeigt.

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