Konfigurieren eines IPsec-Tunnel-Private-to-Private-Netzwerks des Routers mit NAT und einem statischen

Inhalt

Einführung

In dieser Beispielkonfiguration erfahren Sie, wie Sie:

- Verschlüsselung des Datenverkehrs zwischen zwei privaten Netzwerken (10.1.1.x und 172.16.1.x)
- Weisen Sie einem Netzwerkgerät unter 10.1.1.3 eine statische IP-Adresse (externe Adresse 200.1.1.25) zu.

Sie weisen den Router mithilfe von Zugriffskontrolllisten (ACLs) an, keine Network Address Translation (NAT) für den Datenverkehr zwischen privaten und privaten Netzwerken auszuführen. Diese wird dann verschlüsselt und beim Verlassen des Routers im Tunnel platziert. In dieser Beispielkonfiguration gibt es auch eine statische NAT für einen internen Server im 10.1.1.x-Netzwerk. Bei dieser Beispielkonfiguration wird die Option route-map auf dem NAT-Befehl verwendet, um zu verhindern, dass NAT verwendet wird, wenn der entsprechende Datenverkehr auch über den verschlüsselten Tunnel geleitet wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® Softwareversion 12.3(14)T
- Zwei Cisco Router

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 unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Warum wird in der Anweisung 'Verweigern' in der ACL der NAT-Datenverkehr angegeben?

Sie ersetzen ein Netzwerk prinzipiell durch einen Tunnel, wenn Sie Cisco IOS IPsec oder ein VPN verwenden. Sie ersetzen die Internet-Cloud durch einen Cisco IOS IPsec-Tunnel, der von 200.1.1.1 bis 100.1.1.1 in diesem Diagramm verläuft. Machen Sie dieses Netzwerk aus Sicht der beiden privaten LANs transparent, die durch den Tunnel miteinander verbunden sind. Aus diesem Grund sollten Sie normalerweise keine NAT für den Datenverkehr verwenden, der von einem privaten LAN zum privaten Remote-LAN fließt. Sie möchten die Pakete sehen, die vom Router-2-Netzwerk mit einer Quell-IP-Adresse aus dem Netzwerk 10.1.1.0/24 kommen, anstatt 200.1.1.1, wenn die Pakete das interne Router-3-Netzwerk erreichen.

Weitere Informationen zur Konfiguration einer NAT finden Sie in der NAT-Reihenfolge der Vorgänge. Dieses Dokument zeigt, dass die NAT vor der Überprüfung der Verschlüsselung erfolgt, wann das Paket von innen nach außen übertragen wird. Aus diesem Grund müssen Sie diese Informationen in der Konfiguration angeben.

```
ip nat inside source list 122 interface Ethernet0/1 overload
```

```
access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

Hinweis: Es ist auch möglich, den Tunnel zu erstellen und noch NAT zu verwenden. In diesem Szenario geben Sie den NAT-Datenverkehr als "interessanten Datenverkehr für IPsec" (in anderen Abschnitten dieses Dokuments als ACL 101 bezeichnet) an. Weitere Informationen zum Erstellen eines Tunnels bei aktivem NAT finden Sie unter Konfigurieren eines IPsec-Tunnels zwischen Routern mit doppelten LAN-Subnetzen.

Wie sieht es mit der statischen NAT aus? Warum kann ich diese Adresse nicht über den IPsec-Tunnel erreichen?

Diese Konfiguration enthält auch eine statische One-to-One NAT für einen Server mit 10.1.1.3. Dies ist NAT'd to 200.1.1.25, damit Internetbenutzer darauf zugreifen können. Geben Sie den folgenden Befehl ein:

```
ip nat inside source static 10.1.1.3 200.1.1.25
```

Diese statische NAT verhindert, dass Benutzer im Netzwerk 172.16.1.x über den verschlüsselten Tunnel 10.1.1.3 erreichen. Dies liegt daran, dass Sie verhindern müssen, dass der verschlüsselte Datenverkehr mit der ACL 122 NAT erhält. Der statische NAT-Befehl hat jedoch Vorrang vor der generischen NAT-Anweisung für alle Verbindungen zu und von 10.1.1.3. Die statische NAT-Anweisung verhindert nicht ausdrücklich, dass verschlüsselter Datenverkehr auch NAT'd wird. Die Antworten von 10.1.1.3 sind NAT'd to 200.1.1.25, wenn ein Benutzer im Netzwerk 172.16.1.x eine Verbindung zu 10.1.1.3 herstellt und daher nicht über den verschlüsselten Tunnel zurückkehrt (NAT erfolgt vor Verschlüsselung).

Sie müssen verhindern, dass der verschlüsselte Datenverkehr NAT'd (auch statisch one-to-one NAT'd) ist, wenn Sie auf der statischen NAT-Anweisung **einen route-map**-Befehl eingeben.

Hinweis: Die **route-map**-Option auf einer statischen NAT wird nur von der Cisco IOS Software, Version 12.2(4)T und höher, unterstützt. Weitere Informationen finden Sie unter NAT - Möglichkeit, Routenzuordnungen mit statischen Übersetzungen zu verwenden.

Sie müssen diese zusätzlichen Befehle ausgeben, um den verschlüsselten Zugriff auf 10.1.1.3 zu ermöglichen, den statisch gehosteten NAT'd:

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

Diese Anweisungen weisen den Router an, die statische NAT nur auf Datenverkehr anzuwenden, der mit ACL 150 übereinstimmt. Laut ACL 150 darf die NAT nicht auf Datenverkehr angewendet werden, der von 10.1.1.3 stammt und über den verschlüsselten Tunnel an 172.16.1.x gerichtet ist. Wenden Sie sie jedoch auf den gesamten anderen Datenverkehr an, der von 10.1.1.3 stammt (internetbasierter Datenverkehr).

Konfigurieren

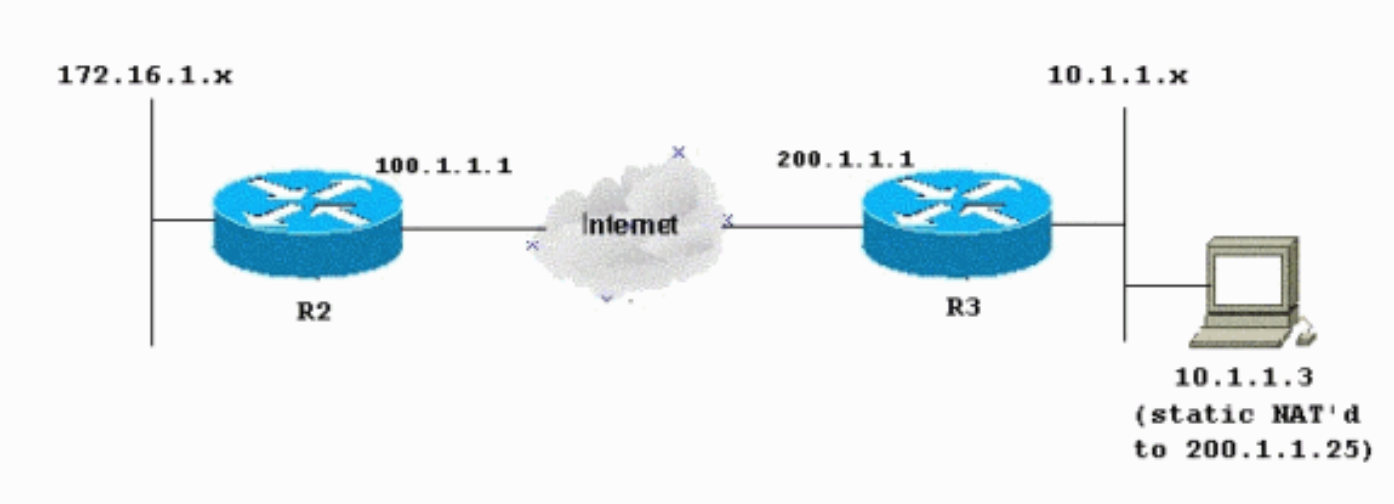
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere

Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Router 2
- Router 3

R2 - Router-Konfiguration

```
R2#write terminal
Building configuration...
Current configuration : 1412 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
crypto isakmp policy 10
 authentication pre-share
!
```

```
crypto isakmp key ciscokey address 200.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 100.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
!
ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 175 interface Ethernet1/0
overload
!
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 101
permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
!--- Except the private network from the NAT process:
access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

R3 - Router-Konfiguration

```
R3#write terminal
Building configuration...
Current configuration : 1630 bytes
!
version 12.3
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 200.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
!
no ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 122 interface Ethernet1/0
overload
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: ip nat
inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
!--- Except the private network from the NAT process:
access-list 122 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
```

```
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: access-list
150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Weitere Informationen finden Sie unter IP Security Troubleshooting - Understanding and Using debug Commands for additional information.

Befehle zur Fehlerbehebung

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

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug crypto ipsec sa**: Zeigt die IPsec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp sa** —Siehe ISAKMP-Verhandlungen von Phase 1.
- **debug crypto engine**: Zeigt die verschlüsselten Sitzungen an.

Zugehörige Informationen

- IPsec-Verhandlung/IKE-Protokolle - Cisco Systems
- Technischer Support und Dokumentation - Cisco Systems