PIX 6.x: IPsec-Tunnel-Passthrough an eine PIX-Firewall mit Zugriffsliste und NAT-Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für einen IPSec-Tunnel durch eine Firewall, die die Network Address Translation (NAT) durchführt. **Diese Konfiguration funktioniert nicht mit Port Address Translation (PAT), wenn Sie Cisco IOS® Software Releases vor und ohne 12.2(13)T verwenden.** Diese Konfiguration kann zum Tunnel von IP-Datenverkehr verwendet werden. Dies kann nicht zum Verschlüsseln von Datenverkehr verwendet werden, der nicht über eine Firewall geleitet wird, z. B. IPX oder Routing-Updates. Generic Routing Encapsulation (GRE)-Tunneling ist für diese Konfiguration geeignet. Im Beispiel in diesem Dokument sind die Cisco 2621- und 3660-Router die IPSec-Tunnelendpunkte, die zwei private Netzwerke miteinander verbinden, mit Kanälen oder Zugriffskontrolllisten (ACLs) auf dem dazwischen liegenden PIX, um den IPSec-Datenverkehr zuzulassen.

Hinweis: NAT ist eine Eins-zu-Eins-Adressenumwandlung, die nicht mit PAT verwechselt werden darf. Hierbei handelt es sich um eine viele (innerhalb der Firewall)-zu-Eins-Übersetzung. Weitere Informationen zu NAT-Betrieb und NAT-Basisfehlerbehebung bzw. Funktionsweise von NAT finden Sie unter Verifying NAT Operation and Basic NAT Troubleshooting (NAT-Betrieb und -Konfiguration überprüfen).

Hinweis: IPSec mit PAT funktioniert möglicherweise nicht ordnungsgemäß, da das Endgerät des externen Tunnels nicht mehrere Tunnel von einer IP-Adresse aus verarbeiten kann. Wenden Sie sich an Ihren Anbieter, um festzustellen, ob die Tunnel-Endgeräte mit PAT kompatibel sind. Darüber hinaus kann in Version 12.2(13)T und höher die NAT-Transparenzfunktion auch für PAT

verwendet werden. Weitere Informationen finden Sie unter IPSec NAT Transparency (IPSec NAT-Transparenz). Weitere Informationen zu diesen Funktionen in Version 12.2(13)T und höheren Versionen finden Sie unter Support für IPSec ESP Through NAT. Bevor Sie ein Ticket beim TAC eröffnen, lesen Sie die FAT Frequently Asked Questions (Häufig gestellte Fragen zur NAT), die viele Antworten auf häufige Fragen enthält.

Weitere Informationen zur Konfiguration eines IPSec-Tunnels über eine Firewall mit NAT auf PIX/ASA Version 7.x finden Sie unter IPsec-Tunneldurchleitung unter Verwendung von Zugriffsliste und MPF mit NAT-Konfigurationsbeispiel.

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 Software Release 12.0.7.T [bis einschließlich 12.2(13)T]IPSec NAT Transparency (IPSec-NAT-Transparenz) für neuere Versionen.
- Cisco 2621 Router mit Cisco IOS Software-Version 12.4
- Cisco 3660 Router mit Cisco IOS Software-Version 12.4
- Cisco PIX-Firewall mit 6.x

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).

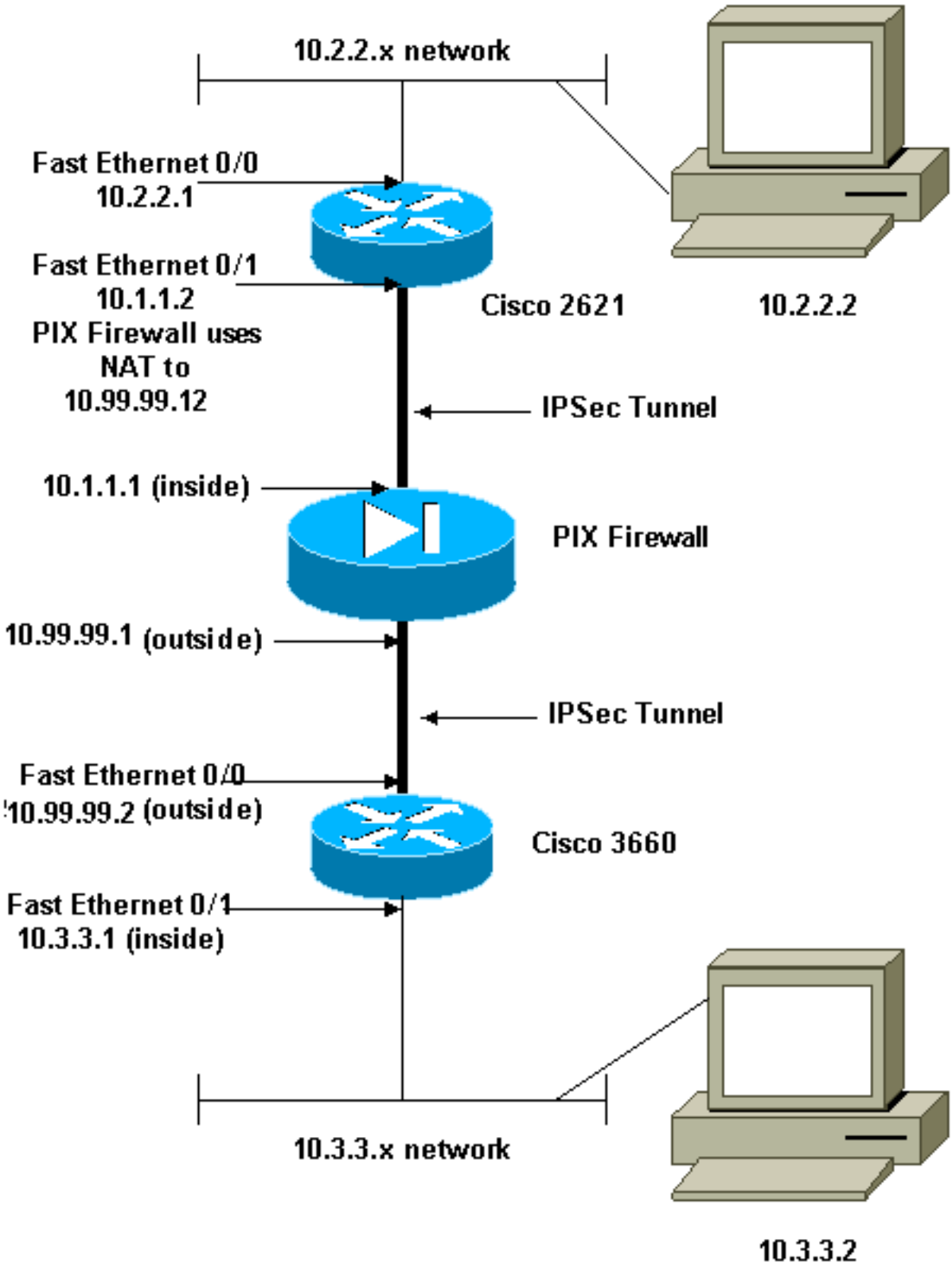
Konfigurieren

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:



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

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Konfiguration des Cisco 2621
- Teilkonfiguration der Cisco PIX-Firewall
- Konfiguration des Cisco 3660

Konfiguration des Cisco 2621

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-2621
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 isdn voice-call-failure 0
 cns event-service server
 !
 !--- IKE Policy crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 10.99.99.2
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/1
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.2
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 controller T1 1/0
 !
 interface FastEthernet0/0
  ip address 10.2.2.1 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !
 interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.1.1
 no ip http server
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 no scheduler allocate
 end
```

Teilkonfiguration der Cisco PIX-Firewall

```
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
!--- The fixup protocol esp-ike command is disabled by
default.

fixup protocol esp-ike

ip address outside 10.99.99.1 255.255.255.0
 ip address inside 10.1.1.1 255.255.255.0
 !--- Range of registered IP addresses for use. global
(outside) 1 10.99.99.50-10.99.99.60 !--- Translate any
internal source address when !--- going out to the
Internet. nat (inside) 1 0.0.0.0 0.0.0.0 0 0
 static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0

 !--- or access-list acl-out permit esp host 10.99.99.2
host 10.99.99.12
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq isakmp
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq 4500
!--- It is important to permit UDP port 4500 for NAT-T
because the PIX is acting !--- as a NAT device between
the routers. access-group acl-out in interface outside
isakmp enable outside isakmp enable inside Command
configured in order to enable NAT-T isakmp nat-traversal
20 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route
inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

Hinweis: Der Befehl **fixup protocol esp-ike** ist standardmäßig deaktiviert. Wenn der Befehl **fixup protocol esp-ike** ausgegeben wird, ist die fixup-Datei aktiviert, und die PIX-Firewall behält den Quellport der Internet Key Exchange (IKE) bei. Außerdem wird eine PAT-Übersetzung für ESP-Datenverkehr erstellt. Wenn die esp-ike fixup-Komponente aktiviert ist, können außerdem Internet Security Association und Key Management Protocol (ISAKMP) für keine Schnittstelle aktiviert werden.

Konfiguration des Cisco 3660

```
version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
 !
 cns event-service server
```

```
!
!--- IKE Policy crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0
!--- IPSec Policy crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.12
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
!
interface FastEthernet0/0
 ip address 10.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
!--- Apply to interface. crypto map mymap
!
interface FastEthernet0/1
 ip address 10.3.3.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 duplex auto
 speed auto
!
interface Ethernet3/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial3/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
interface Ethernet3/1
 no ip address
 no ip directed-broadcast
interface Ethernet4/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface TokenRing4/0
 no ip address
 no ip directed-broadcast
 shutdown
 ring-speed 16
!
!--- Pool from which inside hosts translate to !--- the
globally unique 10.99.99.0/24 network. ip nat pool
OUTSIDE 10.99.99.70 10.99.99.80 netmask 255.255.255.0
!--- Except the private network from the NAT process.
ip nat inside source route-map nonat pool OUTSIDE
ip classless
ip route 0.0.0.0 0.0.0.0 10.99.99.1
no ip http server
```

```
 !
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
 access-list 101 deny   ip 10.3.3.0 0.0.0.255 any
 !--- Except the private network from the NAT process.
access-list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
 access-list 110 permit ip 10.3.3.0 0.0.0.255 any
 route-map nonat permit 10
  match ip address 110
 !
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 end
```

Überprüfen

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

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**.

- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** - Zeigt die Sicherheitszuordnungen für Phase 1 an.
- **show crypto engine connections active** - Benutzen, um die verschlüsselten und entschlüsselten Pakete anzuzeigen.

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Befehle zur Fehlerbehebung

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

- **debug crypto engine** - Zeigt den verschlüsselten Datenverkehr an.
- **debug crypto ipsec** - Zeigen Sie die IPSec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp** - Zeigen Sie die ISAKMP-Verhandlungen von Phase 1 an.

Löschen von Sicherheitszuordnungen

- **clear crypto isakmp** - Löscht IKE-Sicherheitszuordnungen.
- **clear crypto ipsec sa**: Löscht IPSec-Sicherheitszuordnungen.

Zugehörige Informationen

- Cisco Security Appliances der Serie PIX 500
- Cisco Secure PIX Firewall - Befehlsreferenzen
- NAT-Support-Seite
- Request for Comments (RFCs)
- Technischer Support und Dokumentation - Cisco Systems