Konfigurationsbeispiel für IPSec/GRE mit NAT auf dem IOS-Router

Inhalt

Einführung
Bevor Sie beginnen
Konventionen
Voraussetzungen
Verwendete Komponenten
Konfigurieren
Netzwerkdiagramm
Konfigurationen
Überprüfen
Fehlerbehebung
Befehle zur Fehlerbehebung
Löschen von Sicherheitszuordnungen (SAs)
Zugehörige Informationen

Einführung

Diese Beispielkonfiguration zeigt, wie eine allgemeine Routing-Kapselung (GRE) über IP Security (IPSec) konfiguriert wird, wenn der GRE/IPSec-Tunnel eine Firewall durchläuft, die Network Address Translation (NAT) ausführt.

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Voraussetzungen

Diese Konfiguration kann zum Tunnel und Verschlüsseln von Datenverkehr verwendet werden, der normalerweise nicht über eine Firewall, wie zum Beispiel IPX (wie in unserem Beispiel hier) oder Routing-Updates, geleitet wird. In diesem Beispiel funktioniert der Tunnel zwischen dem 2621 und dem 3660 nur, wenn Datenverkehr von Geräten in den LAN-Segmenten generiert wird (kein erweiterter IP/IPX-Ping von den IPSec-Routern). Die IP/IPX-Verbindung wurde mit dem IP/IPX-Ping zwischen den Geräten 2513A und 2513B getestet.

Hinweis: Dies funktioniert nicht mit Port Address Translation (PAT).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und Hardwareversionen.

- Cisco IOS® 12.4
- Cisco PIX Firewall 535
- Cisco PIX Firewall Software Release 7.x und höher

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

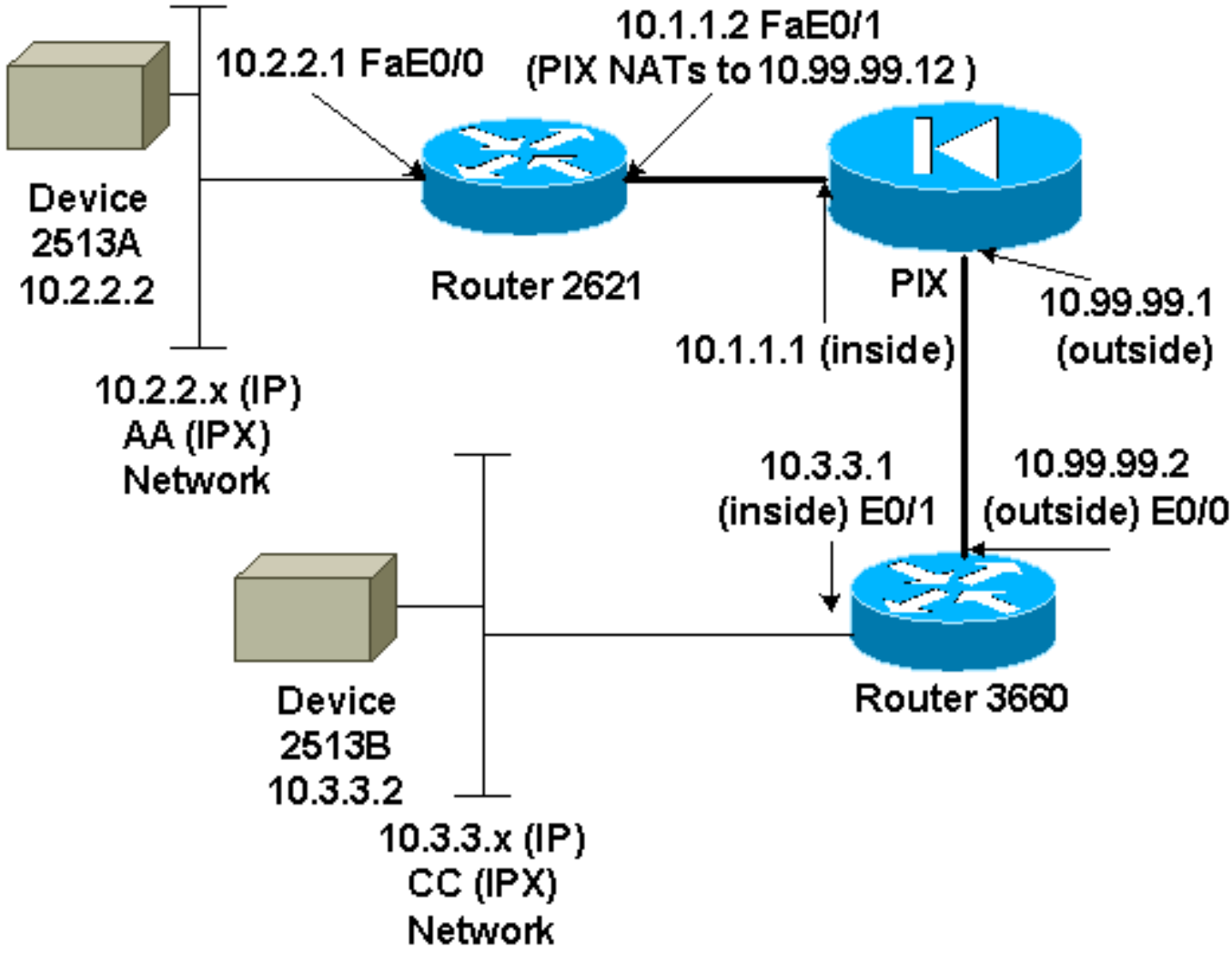
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

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

IOS-Konfigurationshinweis: Bei Cisco IOS 12.2(13)T und höheren Codes (T-Train-Codes mit höherer Nummer, Codes ab 12.3) muss die konfigurierte IPSEC-"crypto map" nur auf die physische Schnittstelle angewendet werden und muss nicht mehr auf die GRE-Tunnelschnittstelle angewendet werden. Die Verwendung der "Crypto Map" auf der physischen Schnittstelle und der Tunnelschnittstelle bei Verwendung der Codes 12.2.(13)T und neuer funktioniert noch. Es wird jedoch dringend empfohlen, diese nur auf die physische Schnittstelle anzuwenden.

Netzwerkdiagramm

In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressen können nicht legal im Internet geroutet werden. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

Hinweise zu Netzwerkdiagrammen

- GRE-Tunnel von 10.2.2.1 bis 10.3.3.1 (IPX-Netzwerk BB)
- IPSec-Tunnel von 10.1.1.2 (10.99.99.12) bis 10.99.99.2

Konfigurationen

Gerät 2513A

```
ipx routing 00e0.b064.20c1
!
interface Ethernet0
 ip address 10.2.2.2 255.255.255.0
 no ip directed-broadcast
 ipx network AA
!
ip route 0.0.0.0 0.0.0.0 10.2.2.1
!--- Output Suppressed
```

2621

```
version 12.4
```

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2621
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ipx routing 0030.1977.8f80
isdn voice-call-failure 0
cns event-service server
!
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
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.2
 set transform-set myset
 match address 101
!
controller T1 1/0
!
interface Tunnel0
 ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/0
 tunnel destination 10.3.3.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 ipx network AA
!
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 crypto map mymap
!
ip classless
ip route 10.3.3.0 255.255.255.0 Tunnel0
ip route 10.3.3.1 255.255.255.255 10.1.1.1
ip route 10.99.99.0 255.255.255.0 10.1.1.1
no ip http server
!
access-list 101 permit gre host 10.2.2.1 host 10.3.3.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
```

```
no scheduler allocate
end

!--- Output Suppressed
```

PIX

```
pixfirewall# sh run
: Saved
:
PIX Version 7.0
!
hostname pixfirewall
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.99.99.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
global (outside) 1 10.99.99.50-10.99.99.60
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
access-list 102 permit esp host 10.99.99.12 host
10.99.99.2
access-list 102 permit udp host 10.99.99.12 host
10.99.99.2 eq isakmp


route outside 0.0.0.0 0.0.0.0 10.99.99.2 1
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1

!--- Output Suppressed
```

3660

```
version 12.4
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname 3660
!
memory-size iomem 30
ip subnet-zero
no ip domain-lookup
!
ipx routing 0030.80f2.2950
cns event-service server
!
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
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.12
 set transform-set myset
 match address 101
!
interface Tunnel0
 ip address 192.168.100.2 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/1
 tunnel destination 10.2.2.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
 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
 ipx network CC
!
ip nat pool 3660-nat 10.99.99.70 10.99.99.80 netmask
255.255.255.0
ip nat inside source list 1 pool 3660-nat
ip classless
ip route 0.0.0.0 0.0.0.0 Tunnel0
ip route 10.2.2.1 255.255.255.255 10.99.99.1
ip route 10.99.99.12 255.255.255.255 10.99.99.1
no ip http server
!
access-list 1 permit 10.3.3.0 0.0.0.255
access-list 101 permit gre host 10.3.3.1 host 10.2.2.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
!--- Output Suppressed
```

Gerät 2513B

```
ipx routing 00e0.b063.e811
!
interface Ethernet0
 ip address 10.3.3.2 255.255.255.0
 no ip directed-broadcast
 ipx network CC
!
ip route 0.0.0.0 0.0.0.0 10.3.3.1
```

```
!--- Output Suppressed
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** - Zeigt die aktuell aktiven verschlüsselten Sitzungsverbindungen für alle Krypto-Engines an.
- *Optional:* **show interfaces tunnel *number*** - Zeigt Tunnelschnittstellendaten an.
- **show ip route** - Zeigt alle statischen IP-Routen oder die mit der AAA-Funktion (Authentifizierung, Autorisierung und Abrechnung) installierten Routen-Downloads an.
- **show ipx route** - Zeigt den Inhalt der IPX-Routing-Tabelle an.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

- **debug crypto engine** - Zeigt den verschlüsselten Datenverkehr an.
- **debug crypto ipsec** - Zeigt die IPSec-Verhandlungen von Phase 2.
- **debug crypto isakmp** - Zeigt die Verhandlungen der Internet Security Association und des Key Management Protocol (ISAKMP) für Phase 1.
- *Optional:* **debug ip routing** - Zeigt Informationen über RIP-Routing (Routing Information Protocol)-Tabellen-Updates und Routen-Cache-Updates.
- **debuggen ipx routing {activity) | events}** - debuggen ipx routing {activity | events} - Zeigt Informationen über IPX-Routing-Pakete an, die der Router sendet und empfängt.

Löschen von Sicherheitszuordnungen (SAs)

- **clear crytpo ipsec sa** - Löscht alle IPSec-Sicherheitszuordnungen.
- **clear crypto isakmp** - Löscht die IKE-Sicherheitszuordnungen.
- *Optional:* **clear ipx route * ** - Löscht alle Routen aus der IPX-Routing-Tabelle.

Zugehörige Informationen

- Support-Seiten für IP Security-Produkte (IPSec)
- GRE-Support-Seiten
- Technischer Support - Cisco Systems