Esempio di configurazione di IPSec/GRE con NAT su router IOS

Sommario

Introduzione

In questa configurazione di esempio viene mostrato come configurare GRE (Generic Routing Encapsulation) su IPSec (IP Security) in cui il tunnel GRE/IPSec sta attraversando un firewall con Network Address Translation (NAT).

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti

Questo tipo di configurazione può essere utilizzata per eseguire il tunnel e crittografare il traffico che normalmente non attraversa un firewall, ad esempio IPX (come nell'esempio riportato qui) o per aggiornare il routing. Nell'esempio, il tunnel tra gli switch 2621 e 3660 funziona solo quando il traffico viene generato dai dispositivi sui segmenti LAN (non un ping IP/IPX esteso dai router IPSec). La connettività IP/IPX è stata testata con il ping IP/IPX tra i dispositivi 2513A e 2513B.

Nota: questa operazione non è possibile con Port Address Translation (PAT).

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Cisco IOS® 12.4
- Cisco PIX Firewall 535
- Software Cisco PIX Firewall release 7.x e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

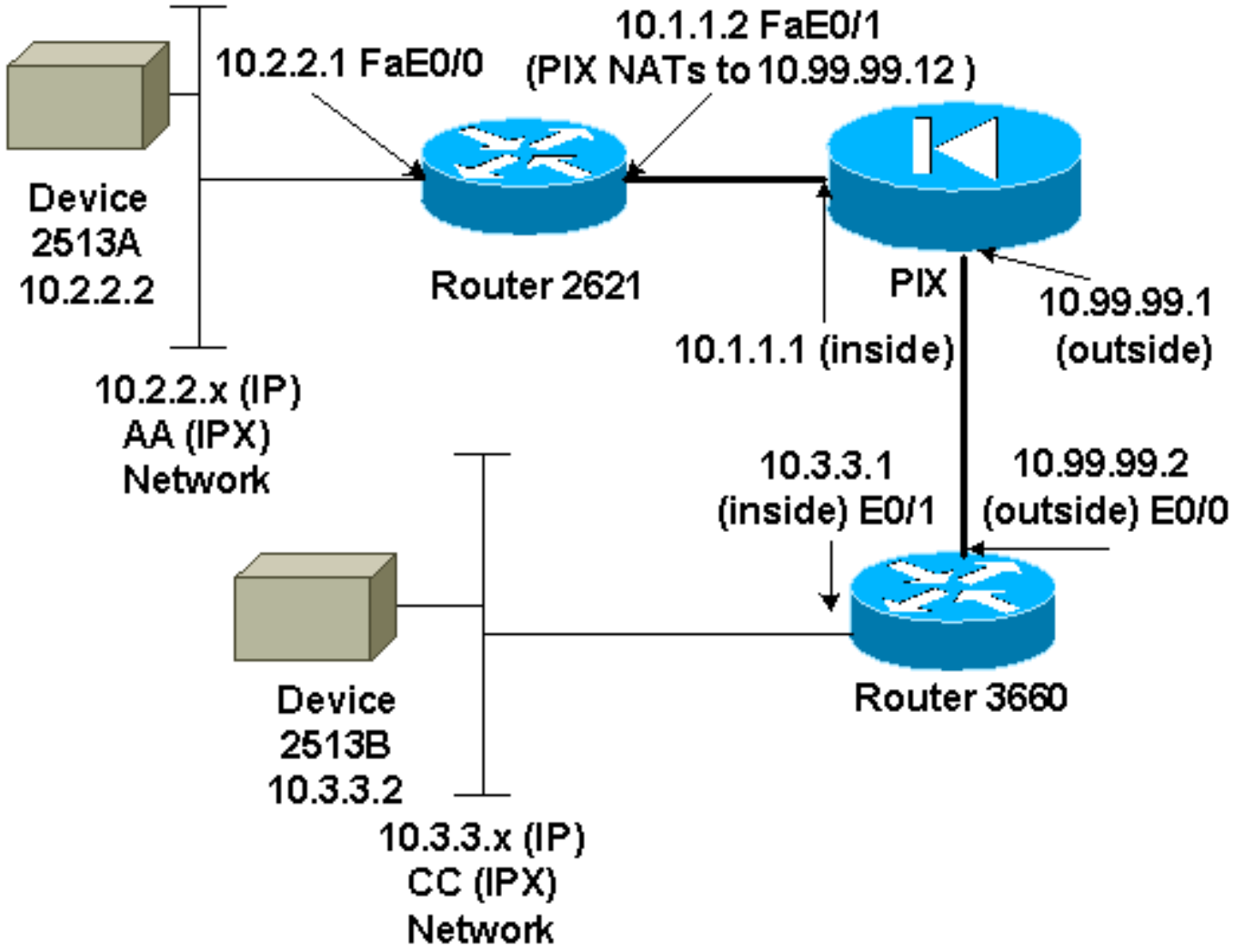
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Nota sulla configurazione di IOS: Con i codici Cisco IOS versione 12.2(13)T e successive (codici T-train con numerazione superiore, 12.3 e successivi), la "mappa crittografica" IPSEC configurata deve essere applicata solo all'interfaccia fisica e non è più necessario applicarla all'interfaccia del tunnel GRE. Mantenere la "mappa crittografica" sull'interfaccia fisica e sull'interfaccia del tunnel quando si usano i codici 12.2.2(13)T e successivi funziona ancora. Tuttavia, si consiglia di applicarlo solo sull'interfaccia fisica.

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Nota: gli indirizzi IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Note diagramma reticolare

- Tunnel GRE da 10.2.2.1 a 10.3.3.1 (rete IPX BB)
- Tunnel IPSec da 10.1.1.2 (10.99.99.12) a 10.99.99.2

Configurazioni

Dispositivo 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
```

Dispositivo 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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **show crypto ipsec sa**: visualizza le associazioni di sicurezza della fase 2.
- **show crypto isakmp sa**: visualizza le connessioni delle sessioni crittografate attive correnti per tutti i motori di crittografia.
- *Facoltativamente:* **show interfaces tunnel *number*: visualizza le informazioni sull'interfaccia del tunnel.**
- **show ip route**: visualizza tutte le route IP statiche o quelle installate utilizzando la funzione di download delle route AAA (autenticazione, autorizzazione e accounting).
- **show ipx route**: visualizza il contenuto della tabella di routing IPX.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

- **debug crypto engine**: visualizza il traffico crittografato.
- **debug crypto ipsec**: visualizza le negoziazioni IPSec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1.
- *Facoltativamente:* **debug ip routing**: visualizza le informazioni sugli aggiornamenti della tabella di routing RIP (Routing Information Protocol) e sugli aggiornamenti della route-cache.
- **debug ipx routing {activity | events}** - debug ipx routing {activity | events} - Mostra informazioni sui pacchetti di routing IPX che il router invia e riceve.

Cancellazione delle associazioni di sicurezza

- **clear crypto ipsec sa**: cancella tutte le associazioni di protezione IPSec.
- **clear crypto isakmp**: cancella le associazioni di sicurezza IKE.
- *Facoltativamente:* **clear ipx route ***: elimina tutte le route dalla tabella di routing IPX.

Informazioni correlate

- Pagine di supporto dei prodotti IP Security (IPSec)
- Pagine di supporto GRE
- Supporto tecnico – Cisco Systems