PIX 6.x : Esempio di tunnel IPsec passato attraverso un firewall PIX con elenco degli accessi e configurazione NAT

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per un tunnel IPSec con un firewall che esegue NAT (Network Address Translation). **Questa configurazione non funziona con Port Address Translation (PAT) se si utilizza il software Cisco IOS® versioni precedenti alla 12.2(13)T esclusa.** Questo tipo di configurazione può essere utilizzata per eseguire il tunnel del traffico IP. Non può essere utilizzato per crittografare il traffico che non attraversa un firewall, ad esempio gli aggiornamenti di routing o IPX. Il tunneling GRE (Generic routing encapsulation) è appropriato per questo tipo di configurazione. Nell'esempio di questo documento, i router Cisco 2621 e 3660 sono gli endpoint del tunnel IPSec che si uniscono a due reti private, con condotti o elenchi di controllo di accesso (ACL) sul PIX in mezzo per consentire il traffico IPSec.

Nota: NAT è una traduzione di indirizzi uno a uno, da non confondere con PAT, che è una traduzione molti (all'interno del firewall)-a-uno. Per ulteriori informazioni sul funzionamento e la configurazione NAT, fare riferimento a Verifica del funzionamento NAT e risoluzione dei problemi NAT di base o Funzionamento di NAT.

Nota: è possibile che IPSec con PAT non funzioni correttamente perché il dispositivo endpoint del tunnel esterno non è in grado di gestire più tunnel da un unico indirizzo IP. Per stabilire se i dispositivi dell'endpoint del tunnel funzionano con PAT, è necessario contattare il fornitore. Inoltre, nelle versioni 12.2(13)T e successive, la funzione di trasparenza NAT può essere utilizzata anche per PAT. per ulteriori informazioni, fare riferimento a Trasparenza NAT IPSec. per ulteriori informazioni su queste funzionalità, fare riferimento a Supporto per IPSec ESP tramite NAT nelle

versioni 12.2(13)T e successive. Inoltre, prima di aprire una richiesta con TAC, fare riferimento alle domande frequenti NAT, che contengono molte risposte alle domande frequenti.

Per ulteriori informazioni su come configurare un tunnel IPSec attraverso un firewall con NAT su PIX/ASA versione 7.x, fare riferimento a Tunnel Pass Through a Security Appliance With Use of Access List e MPF with NAT to NAT Configuration Example (Passaggio del tunnel IPSec tramite un firewall con NAT su PIX/ASA versione 7.x).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS release 12.0.7.T [fino a 12.2(13)T escluso]Per ulteriori informazioni, fare riferimento a Trasparenza NAT IPSec.
- Router Cisco 2621 con software Cisco IOS versione 12.4
- Router Cisco 3660 con software Cisco IOS versione 12.4
- Cisco PIX Firewall con versione 6.x

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.

Convenzioni

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

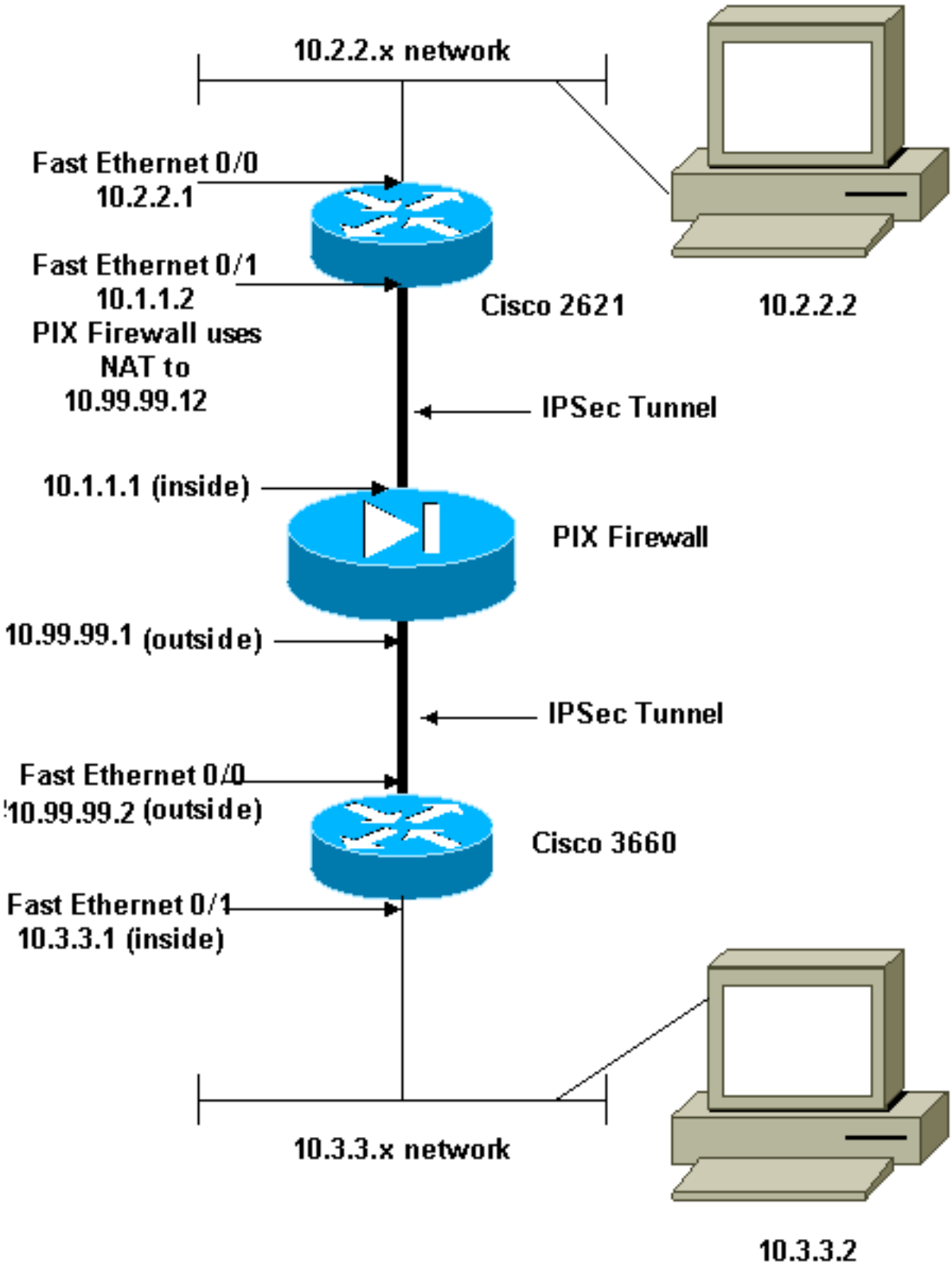
Configurazione

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).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Questi sono indirizzi RFC 1918 usati in un ambiente lab.

Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione di Cisco 2621
- Configurazione parziale di Cisco PIX Firewall
- Configurazione di Cisco 3660

Configurazione di 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
```

Configurazione parziale di 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
```

Nota: il comando **fixup protocol esp-ike** è disabilitato per impostazione predefinita. Se viene emesso un comando **fixup protocol esp-ike**, la correzione viene attivata e il firewall PIX mantiene la porta di origine di Internet Key Exchange (IKE). Crea inoltre una traduzione PAT per il traffico ESP. Inoltre, se la correzione esp-ike è attivata, non sarà possibile abilitare Internet Security Association and Key Management Protocol (ISAKMP) su nessuna interfaccia.

Configurazione di 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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per 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 associazioni di sicurezza della fase 1.
- **show crypto engine connections active**: consente di visualizzare i pacchetti crittografati e decrittografati.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

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

- **debug crypto engine**: visualizza il traffico crittografato.
- **debug crypto ipsec**: da utilizzare per visualizzare le negoziazioni IPSec della fase 2.
- **debug crypto isakmp**: da utilizzare per visualizzare le negoziazioni ISAKMP della fase 1.

Cancellazione delle associazioni di protezione

- **clear crypto isakmp**: cancella le associazioni di sicurezza IKE.
- **clear crypto ipsec sa**: cancella le associazioni di protezione IPSec.

Informazioni correlate

- Cisco PIX serie 500 Security Appliance

- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Pagina di supporto NAT
- RFC (Request for Comments)
- Documentazione e supporto tecnico – Cisco Systems