PIX 6.x Esempio di IPsec dinamico tra un router IOS con indirizzo statico e il firewall PIX con indirizzo dinamico con configurazione NAT

Sommario

Introduzione

In questo documento viene fornito un esempio di configurazione che mostra come abilitare il router IOS® ad accettare connessioni IPsec dinamiche da un firewall PIX. Il router remoto esegue NAT (Network Address Translation) se la rete privata 10.0.0.x accede a Internet. Il traffico dalla versione 10.0.0.x alla rete privata 10.1.0.x dietro il PIX è escluso dal processo NAT. Il firewall PIX può avviare connessioni al router, ma il router non può avviare connessioni al PIX.

Questa configurazione utilizza un router Cisco IOS per creare tunnel IPsec LAN-to-LAN (L2L) dinamici con un firewall PIX che riceve indirizzi IP dinamici sull'interfaccia pubblica (interfaccia esterna). Il protocollo DHCP (Dynamic Host Configuration Protocol) fornisce un meccanismo per allocare dinamicamente indirizzi IP dal provider di servizi Internet (ISP). Questo consente di riutilizzare gli indirizzi IP quando gli host non ne hanno più bisogno.

Per ulteriori informazioni, fare riferimento al documento PIX 6.x: IPSec dinamico tra un firewall PIX con indirizzo statico e il router IOS con indirizzo dinamico con configurazione NAT Esempio per ulteriori informazioni sullo scenario in cui il PIX accetta connessioni IPsec dinamiche dal router.

Fare riferimento a PIX/ASA 7.x e versioni successive: IPSec dinamico tra un PIX con indirizzo statico e un router IOS con indirizzo dinamico con configurazione NAT di esempio per consentire a PIX/ASA Security Appliance di accettare connessioni IPsec dinamiche dal router IOS.

Fare riferimento a PIX/ASA 7.x e versioni successive: IPSec dinamico tra un router IOS con indirizzo statico e un PIX con indirizzo dinamico con configurazione NAT di esempio per ulteriori

informazioni sullo stesso scenario in cui l'appliance di sicurezza PIX/ASA esegue il software versione 7.x e successive.

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® versione 12.4
- Software Cisco PIX Firewall release 6.3.4
- Cisco Secure PIX Firewall 515E
- Cisco 2811 Router

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.

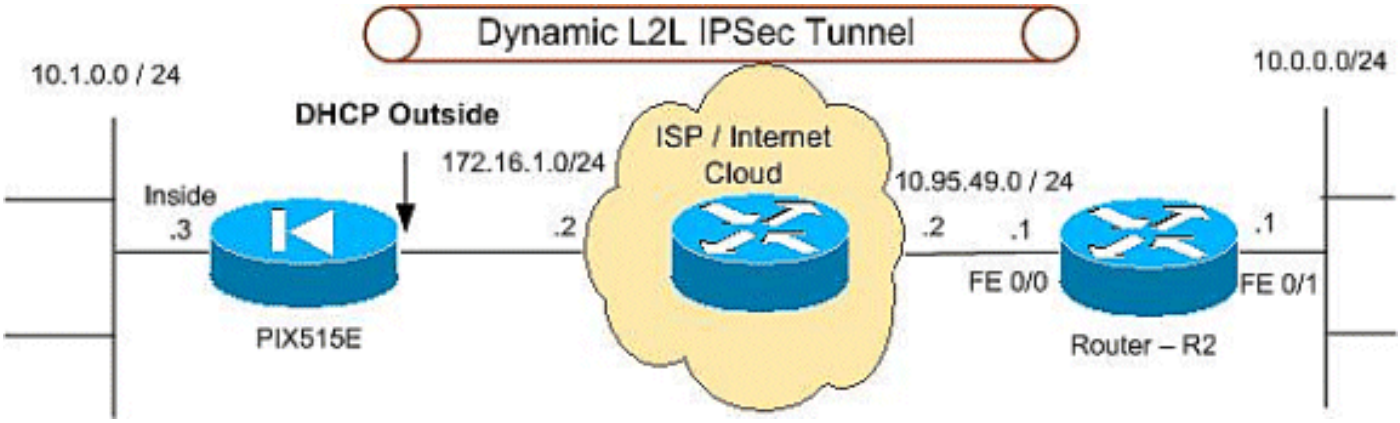
Configurazione

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:



Configurazioni

Nel documento vengono usate queste configurazioni:

- PIX 515E
- R2 (Cisco 2811 Router)

PIX 515E

```
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 shut
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX515E
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
names

!--- The access control list (ACL) to avoid NAT on the
IPsec packets. access-list NO-NAT permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
!--- The ACL to apply on crypto map. !--- Include the
private-network-to-private-network traffic !--- in the
encryption process. access-list 101 permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
mtu intf2 1500
!--- ISP will providthe the Outside IP address.
```

```
ip address outside dhcp

ip address inside 10.1.0.3 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list NO-NAT
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 10.0.0.0 255.255.255.0 172.16.1.5 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec

!--- IPsec configuration, Phase 2. crypto ipsec
transform-set DYN-TS esp-des esp-md5-hmac
crypto map IPSEC 10 ipsec-isakmp
crypto map IPSEC 10 match address 101
crypto map IPSEC 10 set peer 10.95.49.1
crypto map IPSEC 10 set transform-set DYN-TS
crypto map IPSEC interface outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy, Phase 1. !--- Note: In
real show run output, the pre-shared key appears as
*******.

isakmp enable outside
isakmp key cisco123 address 10.95.49.1 netmask
255.255.255.255
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400

telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:f0294298e214a947fc2e03f173e4a405
: end
```

R2 (Cisco 2811 Router)

```
R2#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname r1800
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
!--- ISAKMP policy, Phase 1. crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
!
!
!--- IPsec policy, Phase 2. crypto ipsec transform-set
DYN-TS esp-des esp-md5-hmac
!
crypto dynamic-map DYN 10
set transform-set DYN-TS
match address 101
!
!
crypto map IPSEC 10 ipsec-isakmp dynamic DYN
!
!
!
interface FastEthernet0/0
ip address 10.95.49.1 255.255.255.0
ip nat outside
ip virtual-reassembly
load-interval 30
duplex auto
speed auto
```

```
crypto map IPSEC
!
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
ip classless
ip route 10.1.0.0 255.255.255.0 10.95.49.2
!
ip http server
no ip http secure-server
!--- Except the private network from the NAT process. ip
nat inside source list 102 interface FastEthernet0/0
overload
!
!--- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255

!--- Except the private network from the NAT process.
access-list 102 deny ip 10.0.0.0 0.0.0.255 10.1.0.0
0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
login
!
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 isakmp sa**: visualizza tutte le associazioni di sicurezza (SA) IKE correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione (SA) correnti (IPsec).
- **show crypto engine connections active**: visualizza le connessioni correnti e le informazioni relative ai pacchetti crittografati e decrittografati (solo router).

Ènecessario cancellare le associazioni di protezione su entrambi i peer.

Eseguire questi comandi PIX in modalità di configurazione.

- **clear crypto isakmp sa**: cancella le SA della fase 1.
- **clear crypto ipsec sa**: cancella le SA di fase 2.

Eseguire questi comandi del router in modalità abilitazione.

- **clear crypto isakmp**: cancella le SA di fase 1.
- **clear crypto sa**: cancella le SA di fase 2.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

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

- **show crypto isakmp sa**: visualizza tutte le associazioni di protezione IKE correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione (SA) correnti (IPsec).
- **show crypto engine connections active**: visualizza le connessioni correnti e le informazioni relative ai pacchetti crittografati e decrittografati (solo router).

Informazioni correlate

- Soluzioni per la risoluzione dei problemi più comuni di VPN IPSec di L2L e ad accesso remoto
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- RFC (Requests for Comments)
- Negoziazione IPSec/protocolli IKE