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

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Configurazione
Esempio di rete
Configurazioni
Verifica
Risoluzione dei problemi
Comandi per la risoluzione dei problemi
Informazioni correlate

Introduzione

In questo documento viene fornita una configurazione di esempio per consentire al PIX di accettare connessioni IPsec dinamiche. Il router remoto esegue NAT (Network Address Translation) se la rete privata 10.1.1.x accede a Internet. Il traffico dalla versione 10.1.1.x alla rete privata 192.168.1.x dietro il PIX è escluso dal processo NAT. Il router può avviare connessioni al PIX, ma il PIX non può avviare connessioni al router.

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

Per ulteriori informazioni su uno scenario in cui il router accetta connessioni IPsec dinamiche da un'appliance di sicurezza PIX con versione 6.x, fare riferimento all'esempio di configurazione NAT di IPsec da router a PIX.

Per abilitare le appliance di sicurezza PIX/ASA ad accettare le connessioni IPsec dinamiche dal router Cisco IOS, fare riferimento alla sezione IPsec tra un router IOS statico e un'appliance PIX/ASA 7.x dinamica con configurazione NAT.

Per ulteriori informazioni sullo stesso scenario in cui la protezione PIX/ASA esegue la versione software 7.x e successive, fare riferimento all'esempio di IPsec tra un PIX/ASA 7.x statico e un

router IOS dinamico con configurazione NAT.

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 12.4
- Software Cisco PIX Firewall release 6.3.1
- Cisco Secure PIX Firewall 515E
- Cisco 7206 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.

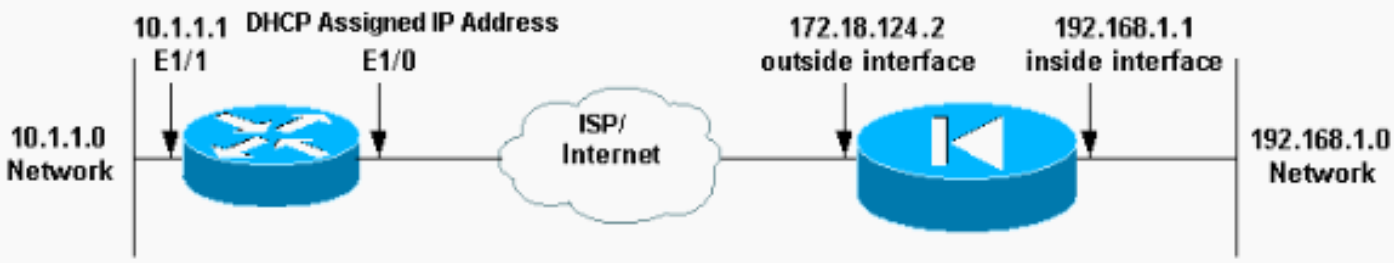
Configurazione

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.

- Elf (PIX)
- Mop (Cisco 7204 Router)

Elf (PIX)

```
Building configuration...
: Saved
:
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname elf
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Access control list (ACL) to avoid NAT on the IPsec
packets. access-list nonat permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.18.124.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 interface
!-- Binds ACL nonat to the NAT statement to avoid NAT on
the IPsec packets nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Permits Internet Control Message Protocol (ICMP)
traffic for testing. !--- Do not enable it in a live
network. conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00
h323 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 RADIUS protocol radius
aaa-server LOCAL protocol tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
!--- IPsec configuration crypto ipsec transform-set
router-set esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set router-set
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
isakmp enable outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy for accepting dynamic
connections from remote PIX. !--- Note: In real show run
output, the pre-shared key appears as *******. isakmp
key cisco123 address 0.0.0.0 netmask 0.0.0.0
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
terminal width 80
Cryptochecksum:eeb67d5df47045f7e6ac4aa090aab683
: end
[OK]
elf#
```

Mop (Cisco 7204 Router)

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

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mop
!
!
ip subnet-zero
!
!
no ip domain-lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) policies crypto isakmp
```

```
policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 172.18.124.2
!
!
!--- IPsec policies crypto ipsec transform-set pix-set
esp-des esp-md5-hmac
!
crypto map pix 10 ipsec-isakmp
 set peer 172.18.124.2
 set transform-set pix-set
 match address 101
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
ip address dhcp
ip nat outside
duplex half
crypto map pix
!
interface Ethernet1/1
ip address 10.1.1.1 255.255.255.0
ip nat inside
duplex half
!
!--- Except the private network from the NAT process. ip
nat inside source route-map nonat interface Ethernet1/0
overload
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1/0
no ip http server
ip pim bidir-enable
!
!--- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
!--- Except the private network from the NAT process.
access-list 110 deny ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 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**.

Èpossibile eseguire questi comandi **show** sul PIX e sul router.

- **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.

- I comandi PIX vengono eseguiti in modalità di configurazione.**clear crypto isakmp sa**: cancella le SA della fase 1.**clear crypto ipsec sa**: cancella le SA di fase 2.
- I comandi del router vengono eseguiti in modalità abilitazione.**clear crypto isakmp**: cancella le SA di fase 1.**clear crypto sa**: cancella le SA di fase 2.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di 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

- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- PIX serie 500 Security Appliance
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems