PIX 6.x: Dynamische IPsec zwischen einer statisch adressierten PIX-Firewall und dem dynamisch adressierten IOS-Router mit NAT-Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration, wie das PIX so konfiguriert wird, dass es dynamische IPsec-Verbindungen akzeptiert. Der Remote-Router führt Network Address Translation (NAT) aus, wenn das private Netzwerk 10.1.1.x auf das Internet zugreift. Der hinter dem PIX liegende Datenverkehr von 10.1.1.x zum privaten Netzwerk 192.168.1.x ist vom NAT-Prozess ausgeschlossen. Der Router kann Verbindungen zum PIX initiieren, aber der PIX kann keine Verbindungen zum Router initiieren.

Diese Konfiguration verwendet eine PIX-Firewall, um dynamische IPsec-LAN-to-LAN (L2L)-Tunnel mit einem Cisco IOS®-Router zu erstellen, der dynamische IP-Adressen an der öffentlichen Schnittstelle (externe Schnittstelle) empfängt. Dynamic Host Configuration Protocol (DHCP) bietet einen Mechanismus für die dynamische Zuweisung von IP-Adressen vom Service Provider (ISP). Dadurch können IP-Adressen wiederverwendet werden, wenn Hosts sie nicht mehr benötigen.

Weitere Informationen zu einem Szenario, in dem der Router dynamische IPsec-Verbindungen von einer PIX Security Appliance mit 6.x akzeptiert, finden Sie unter Router-to-PIX Dynamic-to-Static IPsec with NAT Configuration Example (Beispiel für NAT-Konfiguration).

Informationen zum Akzeptieren dynamischer IPsec-Verbindungen vom Cisco IOS-Router finden Sie unter IPsec Between a Static IOS Router and a Dynamic PIX/ASA 7.x with NAT Configuration Example, damit die PIX/ASA Security Appliance dynamische IPsec-Verbindungen vom Cisco IOS-

Router annehmen kann.

Unter IPsec Between a Static PIX/ASA 7.x and a Dynamic IOS Router with NAT Configuration Example (IPsec Between a Static PIX/ASA 7.x und ein dynamischer IOS Router mit NAT-Konfigurationsbeispiel erfahren Sie mehr über dasselbe Szenario, in dem die PIX/ASA Security Appliance die Softwareversion 7.x oder höher ausführt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Softwareversion 12.4
- Cisco PIX Firewall Softwareversion 6.3.1
- Cisco Secure PIX Firewall 515E
- Cisco Router 7206

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

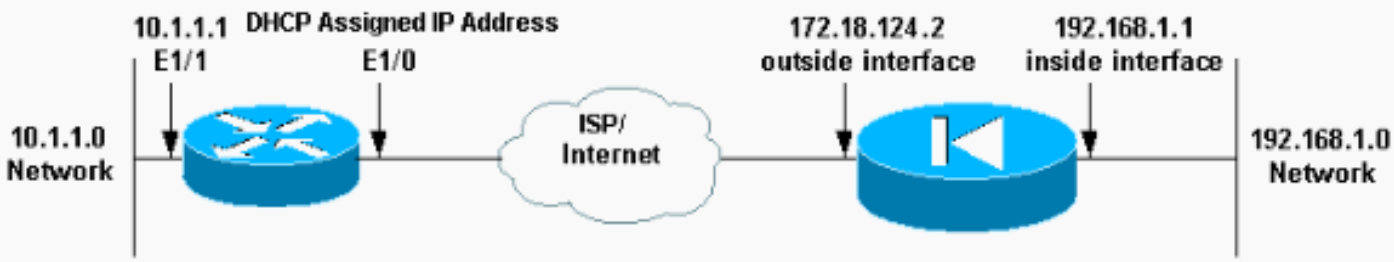
Konfigurieren

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

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

Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

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

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 Router 7204)

```
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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Sie können diese **show**-Befehle auf dem PIX und dem Router ausführen.

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an.
- **show crypto ipsec sa**: Zeigt die von aktuellen (IPsec)-SAs verwendeten Einstellungen.
- **show crypto engine connections active** - Zeigt aktuelle Verbindungen und Informationen über verschlüsselte und entschlüsselte Pakete (nur Router).

Sie müssen SAs auf beiden Peers löschen.

- Die PIX-Befehle werden im Konfigurationsmodus ausgeführt.**clear crypto isakmp sa**: Löscht die SAs der Phase 1.**clear crypto ipsec sa**: Löscht die SAs der Phase 2.
- Die Router-Befehle werden im Aktivierungsmodus ausgeführt.**clear crypto isakmp** - Löscht die SAs der Phase 1.**clear crypto sa**: Löscht die SAs der Phase 2.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE-SAs in einem Peer an.
- **show crypto ipsec sa**: Zeigt die von aktuellen (IPsec)-SAs verwendeten Einstellungen.
- **show crypto engine connections active** - Zeigt aktuelle Verbindungen und Informationen über verschlüsselte und entschlüsselte Pakete (nur Router).

Zugehörige Informationen

- Support-Seite für IPsec-Aushandlung/IKE-Protokolle
- Security Appliances der Serie PIX 500

- Cisco Secure PIX Firewall - Befehlsreferenzen
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems