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

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration, in der veranschaulicht wird, wie der IOS®-Router die Annahme dynamischer IPsec-Verbindungen von einer PIX-Firewall ermöglicht. Der Remote-Router führt Network Address Translation (NAT) aus, wenn das private Netzwerk 10.0.0.x auf das Internet zugreift. Der hinter dem PIX liegende Datenverkehr von 10.0.0.x zum privaten Netzwerk 10.1.0.x ist vom NAT-Prozess ausgeschlossen. Die PIX-Firewall kann Verbindungen zum Router initiieren, der Router kann jedoch keine Verbindungen zum PIX initiieren.

Bei dieser Konfiguration wird ein Cisco IOS-Router verwendet, um dynamische IPsec-LAN-to-LAN (L2L)-Tunnel mit einer PIX-Firewall zu erstellen, die dynamische IP-Adressen an ihrer öffentlichen Schnittstelle (externen Schnittstelle) empfängt. Dynamic Host Configuration Protocol (DHCP) bietet einen Mechanismus für die dynamische Zuweisung von IP-Adressen vom Internet Service Provider (ISP). Dadurch können IP-Adressen wiederverwendet werden, wenn Hosts sie nicht mehr benötigen.

Siehe PIX 6.x: Dynamische IPsec zwischen einer statisch adressierten PIX-Firewall und dem dynamisch adressierten IOS-Router mit NAT-Konfigurationsbeispiel für weitere Informationen über das Szenario, in dem das PIX dynamische IPsec-Verbindungen vom Router akzeptiert.

Weitere Informationen finden Sie unter PIX/ASA 7.x und höher: Dynamische IPsec zwischen einem statisch adressierten PIX und einem dynamisch adressierten IOS-Router mit NAT-

Konfigurationsbeispiel, um die PIX/ASA Security Appliance in die Lage zu versetzen, dynamische IPsec-Verbindungen vom IOS-Router zu akzeptieren.

Weitere Informationen finden Sie unter PIX/ASA 7.x und höher: Dynamische IPsec zwischen einem statisch adressierten IOS-Router und einem dynamisch adressierten PIX mit NAT-Konfigurationsbeispiel, um mehr über dasselbe Szenario zu erfahren, 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 6.3.4
- Cisco Secure PIX Firewall 515E
- Cisco Router 2811

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).

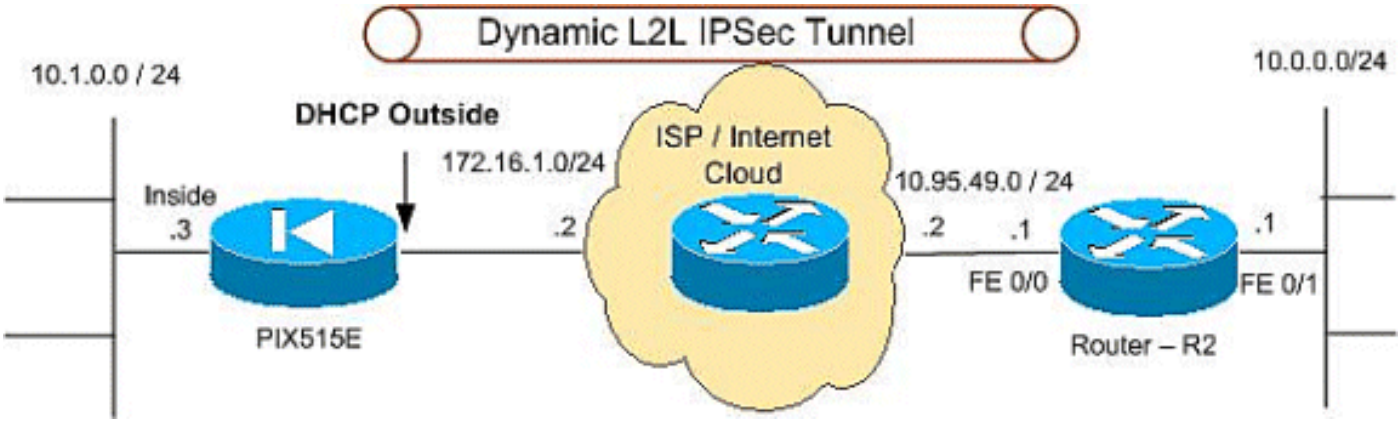
Konfigurieren

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 die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- 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
```

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**.

- **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.

Führen Sie diese PIX-Befehle im Konfigurationsmodus aus.

- **clear crypto isakmp sa**: Löscht die SAs der Phase 1.

- **clear crypto ipsec sa**: Löscht die SAs der Phase 2.

Führen Sie diese Router-Befehle im Aktivierungsmodus aus.

- **clear crypto isakmp** - Löscht die SAs der Phase 1.
- **clear crypto sa**: Löscht die SAs der Phase 2.

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre 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** - Zeigen Sie alle aktuellen IKE-SAs unter 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

- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Anforderungen für Kommentare (RFCs)
- IPsec-Aushandlung/IKE-Protokolle