PIX 6.x : Exemple de configuration d'IPsec dynamique entre un routeur IOS à adresse statique et le pare-feu PIX à adresse dynamique avec NAT

Contenu

Introduction

Ce document fournit une configuration d'échantillon qui t'affiche comment permettre au routeur de ® IOS de recevoir les connexions dynamiques d'IPsec d'un Pare-feu PIX. Le routeur distant exécute le Traduction d'adresses de réseau (NAT) si le réseau privé 10.0.0.x accède à l'Internet. Le trafic de 10.0.0.x au réseau privé 10.1.0.x derrière le PIX est exclu du processus NAT. Le Pare-feu PIX peut initier des connexions au routeur, mais le routeur ne peut pas initier des connexions au PIX.

Cette configuration utilise un routeur Cisco IOS afin de créer les tunnels dynamiques de l'entre réseaux locaux d'IPsec (L2L) avec un Pare-feu PIX qui reçoit des adresses IP dynamiques sur leur interface publique (interface d'extérieur). Le protocole DHCP (DHCP) fournit un mécanisme afin d'allouer des adresses IP dynamiquement du fournisseur de services Internet (ISP). Ceci permet des adresses IP à réutiliser quand les hôtes n'ont besoin plus de elles.

Consultez PIX 6.x : IPsec dynamique entre un Pare-feu statiquement adressé PIX et le routeur dynamiquement adressé IOS avec l'exemple NAT de configuration pour plus d'informations sur le scénario où le PIX reçoit les connexions dynamiques d'IPsec du routeur.

Consultez PIX/ASA 7.x et versions ultérieures : IPsec dynamique entre un PIX statiquement adressé et un routeur dynamiquement adressé IOS avec l'exemple NAT de configuration afin de permettre aux dispositifs de sécurité PIX/ASA de recevoir les connexions dynamiques d'IPsec du

routeur IOS.

Consultez PIX/ASA 7.x et versions ultérieures : IPsec dynamique entre un routeur statiquement adressé IOS et un PIX dynamiquement adressé avec l'exemple NAT de configuration afin d'apprendre un scénario plus à peu près identique où l'appliance de Sécurité PIX/ASA exécute la version de logiciel 7.x et plus tard.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version de logiciel 12.4 de Cisco IOS®
- Version de logiciel de Logiciels pare-feu Cisco PIX 6.3.4
- Pare-feu Cisco Secure PIX 515E
- Routeur de Cisco 2811

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

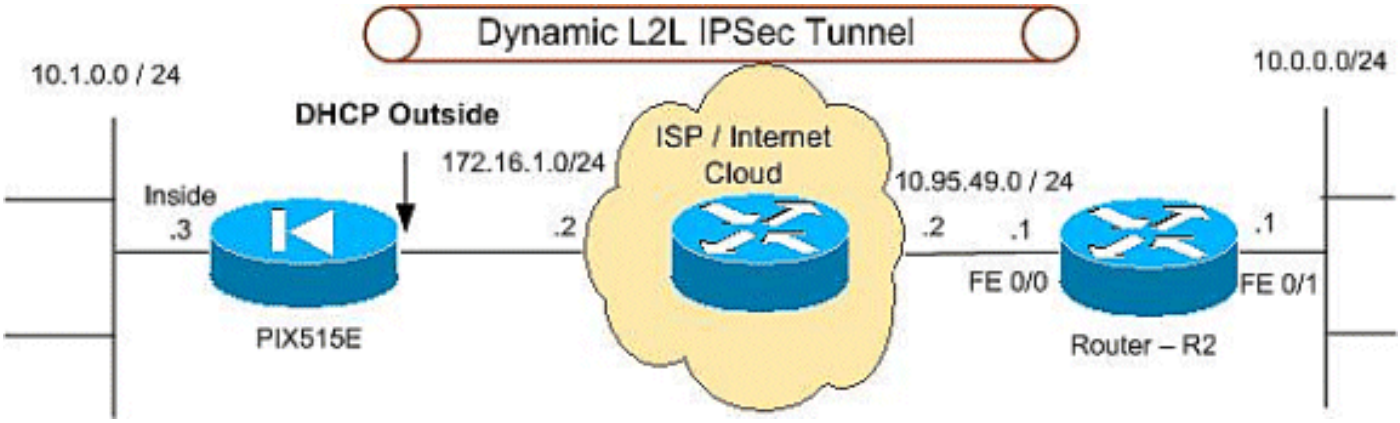
Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- PIX 515E
- R2 (routeur de Cisco 2811)

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 (routeur de Cisco 2811)

```
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
```

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **show crypto isakmp sa** — Affiche toutes les associations de sécurité en cours d'IKE (SAS) à un pair.
- **show crypto ipsec sa** — Affiche les configurations utilisées par le courant (IPsec) SAS.
- **active de connexions de show crypto engine** — Connexions en cours et informations d'expositions concernant les paquets chiffrés et déchiffrés (routeur seulement).

Vous devez effacer SAS sur les deux pairs.

Exécutez ces commandes PIX en mode de config.

- **clear crypto isakmp sa** - Efface la Phase 1 SAS.

- **clear crypto ipsec sa** — Efface le Phase 2 SAS.

Exécutez ces commandes de routeur dans le mode enable.

- **clear crypto isakmp** — Efface le Phase 1 SAS.
- **clear crypto sa** — Efface le Phase 2 SAS.

Dépanner

Utilisez cette section pour dépanner votre configuration.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **show crypto isakmp sa** — Visualisez tout l'IKE en cours SAS à un pair.
- **show crypto ipsec sa** — Affiche les configurations utilisées par le courant (IPsec) SAS.
- **active de connexions de show crypto engine** — Connexions en cours et informations d'expositions concernant les paquets chiffrés et déchiffrés (routeur seulement).

Informations connexes

- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Demandes de commentaires (RFC)
- Négociation IPSec/Protocoles IKE