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

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour que la façon permette au PIX de recevoir les connexions dynamiques d'IPsec. Le routeur à distance exécute la Traduction d'adresses de réseau (NAT) si le réseau privé 10.1.1.x accède à l'Internet. Le trafic de 10.1.1.x au réseau privé 192.168.1.x derrière le PIX est exclu du processus NAT. Le routeur peut initier des connexions au dispositif de sécurité PIX, mais ce dernier ne peut pas initier de connexion au routeur.

Cette configuration emploie un Pare-feu PIX afin de créer les tunnels dynamiques de l'entre réseaux locaux d'IPsec (L2L) avec un routeur de Cisco IOS® 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 (ISP). Ceci permet des adresses IP à réutiliser quand les hôtes n'ont besoin plus de elles.

Référez-vous Routeur--PIX à IPsec Dynamique-à-statique avec l'exemple NAT de configuration pour plus d'informations sur un scénario où le routeur reçoit les connexions dynamiques d'IPsec des dispositifs de sécurité PIX qui exécutent 6.x.

Référez-vous à IPsec entre un routeur statique IOS et un PIX/ASA dynamique 7.x avec l'exemple NAT de configuration afin de permettre aux dispositifs de sécurité PIX/ASA de recevoir les connexions dynamiques d'IPsec du routeur Cisco IOS.

Référez-vous à IPsec entre un PIX/ASA statique 7.x et un routeur dynamique IOS 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 du logiciel Cisco IOS 12.4
- Version de logiciel de Logiciels pare-feu Cisco PIX 6.3.1
- Pare-feu Cisco Secure PIX 515E
- **Routeur Cisco 7206**

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.

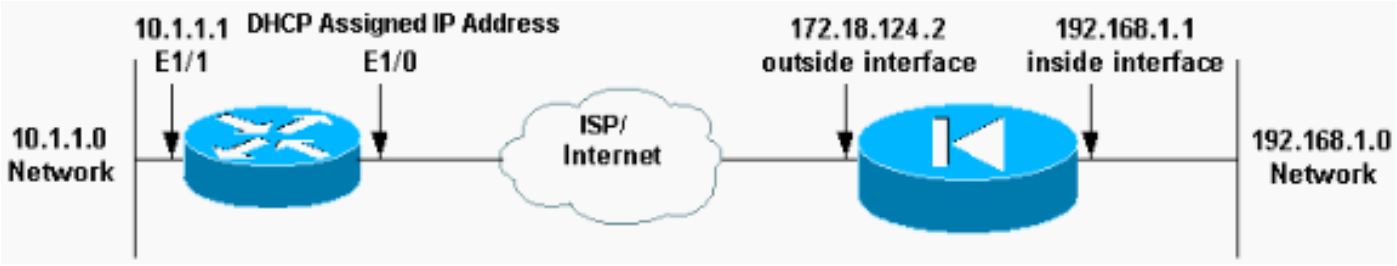
Configurez

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 cette configuration du réseau.



Configurations

Ce document utilise les configurations suivantes.

- Elf (PIX)
- Balai (Routeur Cisco 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#
```

Balai (Routeur Cisco 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
```

Vérifiez

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** .

Vous pouvez exécuter ces **commandes show** sur le PIX et sur le routeur.

- **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.

- Les commandes PIX sont exécutées en mode de config.**clear crypto isakmp sa** - Efface la Phase 1 SAS.**clear crypto ipsec sa** — Efface le Phase 2 SAS.
- Les commandes de routeur sont exécutées dans le mode enable.**clear crypto isakmp** — Efface le Phase 1 SAS.**clear crypto sa** — Efface le Phase 2 SAS.

Dépannez

Cette section fournit des informations que vous pouvez utiliser 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** — Affiche toutes les SA IKE en cours au niveau d'un homologue.
- **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

- Page de support de la négociation IPSec/des protocoles IKE
- Appliances de sécurité de la gamme PIX 500
- Références des commandes du pare-feu Cisco Secure PIX
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems