Exemple de configuration d'un tunnel IPSec entre PIX 7.x et un concentrateur VPN 3000

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour que la façon établisse un tunnel VPN d'IPsec d'entre réseaux locaux entre un Pare-feu 7.x PIX et un concentrateur de Cisco VPN 3000.

Référez-vous au Rai-à-client amélioré par 7.x VPN PIX/ASA avec l'exemple de configuration d'authentification TACACS+ afin de se renseigner plus sur le scénario où le tunnel entre réseaux locaux entre le PIXes tient compte également pour qu'un client vpn accède au rai PIX par le concentrateur PIX.

Référez-vous aux dispositifs de sécurité PIX/ASA 7.x à un exemple de configuration de tunnel d'IPsec d'entre réseaux locaux de routeur IOS afin de se renseigner plus sur le scénario où le tunnel entre réseaux locaux entre le PIX/ASA et un routeur IOS.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Ce document exige une compréhension de base de protocole IPsec. Référez-vous à une introduction au cryptage d'IPsec pour se renseigner plus sur IPsec.

Composants utilisés

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

- Cisco PIX 500 Series Security Appliance avec la version de logiciel 7.1(1)
- Concentrateur Cisco VPN 3060 avec la version de logiciel 4.7.2(B)

Note: PIX 506/506E ne prend en charge pas 7.x.

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.

Afin de configurer PIX 6.x, référez-vous au tunnel d'IPSec d'entre réseaux locaux entre l'exemple de configuration de concentrateur de Cisco VPN 3000 et de Pare-feu PIX.

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.

- Configurez le PIX
- Configurez le concentrateur VPN 3000

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurez le PIX

PIX

```
PIX7#show running-config
: Saved
:
PIX Version 7.1(1)
!
hostname PIX7
enable password 8Ry2YjIyt7RRXU24 encrypted
```

```
names
!
!--- Configures the outside interface of the PIX. !---
By default, the security level for the outside interface
is 0. interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
!--- Configures the inside interface of the PIX. !--- By
default, the security level for the inside interface is
100. interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
!--- Defines the IP addresses that should not be NATed.
access-list nonat extended permit ip 192.168.1.0
255.255.255.0 172.16.0.0 255.255.0.0
access-list outside extended permit icmp any any
!--- Defines the IP addresses that can communicate via
the IPsec tunnel. access-list 101 extended permit ip
192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0
access-list OUT extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-504.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list nonat
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1
!--- Output is suppressed. !--- These are the IPsec
parameters that are negotiated with the client. crypto
ipsec transform-set my-set esp-aes-256 esp-sha-hmac
crypto map mymap 20 match address 101
crypto map mymap 20 set peer 172.30.1.1
crypto map mymap 20 set transform-set my-set
crypto map mymap interface outside
!--- These are the Phase I parameters negotiated by the
two peers. isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- A tunnel group consists of a set of records !---
that contain tunnel connection policies. The two
attributes !--- are General and IPsec. Use the remote
peer IP address as the !--- name of the Tunnel group. In
this example 172.30.1.1 is the peer IP address. !---
Refer to Tunnel Group for more information. tunnel-group
172.30.1.1 type ipsec-l2l
tunnel-group 172.30.1.1 ipsec-attributes
 pre-shared-key *
!--- Output is suppressed. ! : end PIX7#
```

Configurez le concentrateur VPN 3000

Des concentrateurs VPN ne sont pas préprogrammés avec des adresses IP dans leurs

configurations d'usine. Vous devez employer le port de console afin de configurer les configurations initiales qui sont une interface de ligne de commande pilotée par menu (CLI). Référez-vous à configurer des concentrateurs VPN par la console pour les informations sur la façon dont configurer par la console.

Après que vous configuriez l'adresse IP sur l'interface (privée) d'Ethernet 1, vous pouvez configurer le repos avec le CLI ou par l'intermédiaire de l'interface du navigateur. L'interface du navigateur prend en charge le HTTP et le HTTP au-dessus du Protocole SSL (Secure Socket Layer).

Ces paramètres sont configurés par la console :

- **Heure/date** — La date et heure correcte sont très importante. Ils aident à s'assurer que se connecter et entrées de traçabilité sont précis, et que le système peut créer un Security Certificate valide.
- **Interface (privée) d'Ethernet 1** — L'adresse IP et le masque (de la topologie du réseau 172.16.5.100/16).

Le concentrateur VPN est maintenant accessible par un navigateur HTML du réseau intérieur. Référez-vous utilisant l'interface de ligne de commande pour la configuration rapide pour les informations sur la façon dont configurer le concentrateur VPN dans le mode CLI.

Tapez l'adresse IP de l'interface privée du navigateur Web afin d'activer l'interface gui.

Cliquez sur l'icône **nécessaire par sauvegarde** pour sauvegarder des modifications à la mémoire. Le nom d'utilisateur et mot de passe de par défaut d'usine sont l'**admin**, qui distingue les majuscules et minuscules.

1. Lancez le GUI et sélectionnez le **Configuration > Interfaces** pour configurer l'adresse IP pour l'interface publique et la passerelle par défaut.
2. **La configuration > la Gestion des stratégies > la gestion de trafic > les listes des réseaux** choisies **> ajoutent ou modifient** pour créer les listes des réseaux qui définissent le trafic à chiffrer.Ajoutez les gens du pays et les réseaux distants ici. Les adresses IP devraient refléter ceux dans la liste d'accès configurée sur le distant PIX.Dans cet exemple, les deux listes des réseaux sont **RÉSEAU LOCAL de gens du pays de remote_network** et de **client vpn**.
3. **La configuration > les protocoles de système > de Tunnellisation > l'entre réseaux locaux** choisis d'**IPSec > ajoutent** pour configurer le tunnel entre réseaux locaux d'IPsec. Cliquez sur Apply quand vous êtes de finition.Écrivez l'adresse IP de pair, les listes des réseaux créées dans l'étape 2, les paramètres d'IPsec et d'ISAKMP, et la clé pré-partagée.Dans cet exemple l'adresse IP de pair est **10.1.1.1**, les listes des réseaux sont **RÉSEAU LOCAL local de remote_network** et de **client vpn**, et **Cisco** est la clé pré-partagée.
4. **Le Configuration > User Management > Groups** choisi **> modifient 10.1.1.1** pour visualiser l'information du groupe automatiquement générée.**Note**: Ne modifiez pas ces configurations de groupe.

Vérifiez

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

- Vérifiez le PIX
- Vérifiez le concentrateur VPN 3000

Vérifiez le PIX

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** .

- affichez ISAKMP SA — Affiche toutes les associations de sécurité en cours d'IKE (SAS) à un pair. L'état MM_ACTIVE dénote que le mode principal est utilisé pour installer le tunnel VPN d'IPsec.Dans cet exemple le Pare-feu PIX initie la connexion d'IPsec. L'adresse IP de pair est 172.30.1.1 et emploie le mode principal pour établir la connexion.

```
PIX7#show isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.30.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

- show ipsec sa — Affiche les paramètres utilisés par les SA en cours. Recherchez les adresses IP de l'homologue, les réseaux accessibles aux niveaux local et distant et le jeu de transformations utilisé. Il y a deux SAS ESP, une dans chaque direction.

```
PIX7#show ipsec sa
interface: outside
    Crypto map tag: mymap, seq num: 20, local addr: 10.1.1.1

      access-list 101 permit ip 192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0

      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
      current_peer: 172.30.1.1

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.1.1.1, remote crypto endpt.: 172.30.1.1

      path mtu 1500, ipsec overhead 76, media mtu 1500
      current outbound spi: 136580F6

    inbound esp sas:
      spi: 0xF24F4675 (4065281653)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel,}
         slot: 0, conn_id: 1, crypto-map: mymap
         sa timing: remaining key lifetime (kB/sec): (3824999/28747)
         IV size: 16 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x136580F6 (325419254)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel,}
         slot: 0, conn_id: 1, crypto-map: mymap
```

```
sa timing: remaining key lifetime (kB/sec): (3824999/28745)
IV size: 16 bytes
replay detection support: Y
```

Utilisez ipsec clair SA et commandes claires d'ISAKMP SA de remettre à l'état initial le tunnel.

Vérifiez le concentrateur VPN 3000

Surveillance > statistiques > IPsec choisis à vérifier si le tunnel a monté dans le concentrateur VPN 3000. Ceci contient les statistiques pour l'IKE et les paramètres d'IPsec.

Vous pouvez surveillez activement la session au **Monitoring > Sessions**. Vous pouvez remettre à l'état initial le tunnel d'IPsec ici.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Dépannez le PIX
- Dépannez le concentrateur VPN 3000
- PFS

Dépannez le PIX

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** .

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

Les commandes de **débogage** sur PIX pour des tunnels VPN sont :

- debug crypto isakmp — Négociations de SA ISAKMP de debugs.
- debug crypto ipsec — Négociations d'IPsec SA de debugs.

Dépannez le concentrateur VPN 3000

Semblable aux commandes de débogage sur les Routeurs de Cisco, vous pouvez configurer des classes d'événement pour visualiser toutes les alarmes. **La configuration > le système > les événements > les classes** choisis **> ajoutent** pour activer se connecter des classes d'événement.

Surveillance > journal d'événements filtrables choisis pour surveiller les événements activés.

PFS

Dans des négociations IPsec, le Perfect Forward Secrecy (PFS) assure que chacune nouvelle clé cryptographique est indépendante de toute clé précédente. Le PFS d'enable ou de débronchement sur le les deux le tunnel scrute, autrement le tunnel d'IPsec de l'entre réseaux locaux (L2L) n'est pas établi dans le PIX/ASA.

PFS est désactivé par défaut. Afin d'activer PFS, utilisez la commande **pfs** avec le mot clé **enable**

en mode de configuration de stratégie de groupe. Afin de désactiver PFS, saisissez le mot clé **disable**.

```
hostname(config-group-policy)#pfs {enable | disable}
```

Afin de retirer l'attribut PFS de la configuration en cours, saisissez la forme **no** de cette commande. Une stratégie de groupe peut hériter d'une valeur pour PFS d'une autre stratégie de groupe. Saisissez la forme **no** de cette commande afin d'éviter d'hériter d'une valeur.

```
hostname(config-group-policy)#no pfs
```

Informations connexes

- Dispositifs de sécurité de la gamme Cisco PIX 500 - Page de support
- Concentrateur de la série Cisco VPN 3000 - Page de support
- Référence de commandes de Cisco PIX 500 Series Security Appliance
- Support et documentation techniques - Cisco Systems