Exemple de configuration de PIX/ASA et d'un client VPN pour un VPN Internet public sur un stick

Contenu

Introduction

Ce document décrit comment installer des dispositifs de sécurité 7.2 ASA et plus tard pour exécuter IPsec sur un bâton. Cette configuration s'applique à un cas spécifique dans lequel l'ASA n'autorise pas la transmission tunnel partagée et où les utilisateurs se connectent directement à l'ASA avant d'être autorisés à accéder à Internet.

Remarque: Dans la version 7.2 et ultérieures PIX/ASA, le mot clé *intra-interface* permet à tout le trafic pour écrire et quitter la même interface, et pas simplement le trafic d'IPsec.

Référez-vous au routeur et au client vpn pour l'Internet public sur un exemple de configuration de bâton pour se terminer une configuration semblable sur un routeur de lieu d'exploitation principal.

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 concentrateur PIX réoriente le trafic du client vpn au rai PIX.

Remarque: Afin d'éviter une superposition des adresses IP dans le réseau, affectez un groupe

complètement différent d'adresses IP au client vpn (par exemple, 10.x.x.x, 172.16.x.x, et 192.168.x.x). Ce schéma d'adressage IP est utile afin de dépanner votre réseau.

Conditions préalables

Conditions requises

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

- L'appliance de Sécurité du pivot PIX/ASA doit exécuter la version 7.2 ou ultérieures
- Version 5.x de Client VPN Cisco

Composants utilisés

Les informations dans ce document sont basées version 8.0.2 d'appareils sur PIX ou ASA Sécurité et version 5.0 de Client VPN Cisco.

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.

Produits connexes

Cette configuration peut également être utilisée avec la version 7.2 et ultérieures d'appareils de Sécurité de Cisco PIX.

Conventions

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

Informations générales

Hairpinning ou demi-tour

Cette fonctionnalité est utile pour le trafic VPN qui entre dans interface, mais qui est ensuite routé hors de cette même interface. Par exemple, si vous avez un réseau VPN d'en étoile, où les dispositifs de sécurité sont le hub, et les réseaux VPN distants êtes des rais, afin d'un parliez pour communiquer avec un autre rai, trafiquez devez entrer dans les dispositifs de sécurité et alors de nouveau à l'autre parlait.

Utilisez la commande du même-Sécurité-**trafic** de permettre au trafic pour écrire et quitter la même interface.

```
securityappliance(config)#same-security-traffic permit intra-interface
```

Remarque: Le hairpinning ou le demi-tour s'applique pour le client vpn à la transmission de client vpn, aussi bien.

Configurations

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 obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configuration CLI de PIX/ASA

- PIX/ASA

Exécutez la configuration sur PIX/ASA

```
PIX Version 8.0(2)
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
```

```
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface access-list 100 extended permit icmp any
any echo-reply pager lines 24 logging enable logging
buffered debugging mtu outside 1500 mtu inside 1500 ip
local pool vpnpool 192.168.10.1-192.168.10.254 mask
255.255.255.0 no failover monitor-interface outside
monitor-interface inside icmp permit any outside no asdm
history enable arp timeout 14400 nat-control !--- The
address pool for the VPN Clients. !--- The global
address for Internet access used by VPN Clients. !---
Note: Uses an RFC 1918 range for lab setup. !--- Apply
an address from your public range provided by your ISP.
global (outside) 1 172.18.124.166 !--- The NAT statement
to define what to encrypt (the addresses from the vpn-
pool). nat (outside) 1 192.168.10.0 255.255.255.0 nat
(inside) 1 0.0.0.0 0.0.0.0 static (inside,outside)
172.16.3.102 172.16.3.102 netmask 255.255.255.255
access-group 100 in interface outside route outside
0.0.0.0 0.0.0.0 172.18.124.98 1 timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
!--- The configuration of group-policy for VPN Clients.
group-policy clientgroup internal group-policy
clientgroup attributes vpn-idle-timeout 20 !--- Forces
VPN Clients over the tunnel for Internet access. split-
tunnel-policy tunnelall no snmp-server location no snmp-
server contact snmp-server enable traps snmp !---
Configuration of IPsec Phase 2. crypto ipsec transform-
set myset esp-3des esp-sha-hmac !--- Crypto map
configuration for VPN Clients that connect to this PIX.
crypto dynamic-map rtpdynmap 20 set transform-set myset
!--- Binds the dynamic map to the crypto map process.
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap !---
Crypto map applied to the outside interface. crypto map
mymap interface outside !--- Enable ISAKMP on the
outside interface. isakmp identity address isakmp enable
outside !--- Configuration of ISAKMP policy. isakmp
policy 10 authentication pre-share isakmp policy 10
encryption 3des isakmp policy 10 hash sha isakmp policy
10 group 2 isakmp policy 10 lifetime 86400 isakmp policy
65535 authentication pre-share isakmp policy 65535
encryption 3des isakmp policy 65535 hash sha isakmp
policy 65535 group 2 isakmp policy 65535 lifetime 86400
telnet timeout 5 ssh timeout 5 console timeout 0 !---
Configuration of tunnel-group with group information for
VPN Clients. tunnel-group rtptacvpn type ipsec-ra !---
Configuration of group parameters for the VPN Clients.
tunnel-group rtptacvpn general-attributes address-pool
vpnpool !--- Disable user authentication.
authentication-server-group none !--- Bind group-policy
parameters to the tunnel-group for VPN Clients. default-
group-policy clientgroup tunnel-group rtptacvpn ipsec-
attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !
service-policy global_policy global
```

```
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0 : end
```

Configurer ASA/PIX avec ASDM

Terminez-vous ces étapes afin de configurer Cisco ASA en tant que serveur VPN distant avec l'ASDM :

1. Choisissez les **assistants > l'assistant d'IPsec VPN de la** fenêtre d'accueil.
2. Choisissez le type de tunnel VPN d'**Accès à distance**, et assurez-vous que l'interface de tunnel VPN est placée comme désirée.
3. Le seul type de client vpn disponible est déjà choisi. Cliquez sur **Next** (Suivant).
4. Écrivez un nom pour le nom du groupe tunnel. Fournissez les informations d'authentification à utiliser.**La clé pré-partagée** est choisie dans cet exemple.**Remarque:** Il n'y a pas de moyen de cacher/crypter la clé pré-partagée sur l'ASDM. La raison est que l'ASDM doit seulement être utilisé par les personnes qui configurent l'ASA ou par les personnes qui aident le client avec cette configuration.
5. Choisissez si vous voulez que des utilisateurs distants soient authentifiés à la base de données des utilisateurs locaux ou à un groupe de serveurs AAA externe.**Remarque:** Vous ajoutez des utilisateurs à la base de données des utilisateurs locaux dans l'étape 6.**Remarque:** Référez-vous aux groupes de serveurs d'authentification et d'autorisation PIX/ASA 7.x pour des utilisateurs VPN par l'intermédiaire de l'exemple de configuration ASDM pour les informations sur la façon dont configurer un Groupe de serveurs AAA externe par l'ASDM.
6. Ajoutez les utilisateurs à la base de données locale, s'il y a lieu.**Remarque:** Ne retirez pas les utilisateurs courants de cette fenêtre. Choisissez le **Configuration > Device Administration > Administration > User Accounts dans la fenêtre principale ASDM** pour éditer les entrées existantes dans la base de données ou pour les retirer de la base de données.
7. Définissez un pool des adresses locales à assigner dynamiquement aux clients VPN distants quand elles se connectent.
8. *Facultatif :* Spécifiez les informations du serveur DNS et WINS et un nom de Domaine par défaut à diffuser aux clients VPN distants.
9. Spécifiez les paramètres pour l'IKE, également connus sous le nom de IKE phase 1.Les configurations des deux côtés du tunnel doivent s'assortir exactement, mais le Client VPN Cisco choisit automatiquement la configuration correcte pour elle-même. Aucune configuration d'IKE n'est nécessaire sur le PC client.
10. Spécifiez les paramètres pour IPSec, également connus sous le nom de IKE phase 2.Les configurations des deux côtés du tunnel doivent s'assortir exactement, mais le Client VPN Cisco choisit automatiquement la configuration correcte pour elle-même. Aucune configuration d'IKE n'est nécessaire sur le PC client.
11. Spécifiez que, le cas échéant, des hôtes internes ou les réseaux peuvent être exposé aux utilisateurs distants VPN.Si vous laissez cette liste vide, elle permet à des utilisateurs distants de VPN d'accéder au réseau interne en entier de l'ASA.Vous pouvez également activer split tunneling sur cette fenêtre. Split tunneling crypte le trafic aux ressources définies précédemment dans cette procédure et fournit un accès non crypté à l'ensemble de l´Internet en ne tunnellisant pas ce trafic. Si la Transmission tunnel partagée n'est *pas* activée, tout le trafic des utilisateurs distants de VPN est tunnellisé à l'ASA. Ceci peut devenir très intensif en largeur de bande et processeur intensif, basé sur votre configuration.

12. Cette fenêtre montre un résumé des actions que vous avez prises. Cliquez sur **Finish** si vous êtes satisfait de votre configuration.
13. Configurez le même-Sécurité-**trafic de** commande pour activer le trafic entre deux hôtes ou plus connectés à la même interface quand vous cliquez sur la case à cocher comme affichée :
14. Choisissez les **règles de configuration > de Pare-feu >NAT**, et cliquez sur Add la **règle NAT dynamique** afin de créer cette traduction dynamique avec l'utilisation de l'ASDM.
15. Choisissez l'**intérieur** comme interface de source, et introduisez les adresses que vous voulez à NAT. Pour l'adresse Translate sur l'interface, choisissez **dehors** et cliquez sur OK.
16. Choisissez l'**extérieur** comme interface de source, et introduisez les adresses que vous voulez à NAT. Pour l'adresse Translate sur l'interface, choisissez **dehors** et cliquez sur OK.
17. La traduction apparaît dans les Règles de traduction aux **règles de configuration > de Pare-feu >NAT**.

Note 1 : La commande d'autorisation-VPN de connexion de sysopt doit être configurée. La commande de sysopt de show running-config vérifie si elle est configurée.

Note 2 : Ajoutez cette sortie pour le transport facultatif d'UDP :

```
group-policy clientgroup attributes vpn-idle-timeout 20 ipsec-udp enable ipsec-udp-port 10000
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

Note 3 : Configurez cette commande en configuration globale de l'appliance PIX pour que les clients vpn se connectent par l'intermédiaire d'IPsec au-dessus de TCP :

```
isakmp ipsec-over-tcp port 10000
```

Remarque: Référez-vous à Cheveu-goupiller sur le vidéo de Cisco ASA pour plus d'informations sur différents scénarios où cheveu-goupiller peut être utilisé.

Configuration du client VPN

Terminez-vous ces étapes pour configurer le client vpn :

1. Choisissez **nouveau**.
2. Écrivez le PIX en dehors de l'IP address d'interface et du nom de groupe de tunnels avec le mot de passe pour l'authentification.
3. (*Facultatif*) cliquez sur le **Tunnellisation transparent d'enable** sous le transport tableau (c'est facultatif et exige la configuration supplémentaire PIX/ASA mentionnée dans la note 2.)
4. Sauvegardez le profil.

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** .

- show crypto isakmp sa - Affiche toutes les associations de sécurité actuelles d'IKE (SA) sur un pair.

- show crypto ipsec sa — Affiche tout le courant SAS. Look for chiffrent et déchiffrent les paquets sur SA qui définissent le trafic de client vpn.

Tentative de cingler ou parcourir à une adresse IP publique du client (par exemple, www.cisco.com).

Remarque: L'interface interne du PIX ne peut pas être cinglée pour la formation d'un tunnel à moins que la commande de Gestion-Access soit configurée en mode de configuration globale.

```
PIX1(config)#management-access inside PIX1(config)# show management-access management-access
inside
```

Vérification de client vpn

Terminez-vous ces étapes afin de vérifier le client vpn.

1. Cliquez avec le bouton droit sur l'icône de verrouillage de client vpn actuelle à la barre d'état système après une connexion réussie et choisissez l'option pour que les **statistiques** visualisent chiffre et déchiffre.
2. Cliquez sur en fonction l'onglet de détails d'artère afin de ne vérifier l'aucune liste de tunnel partagé passée vers le bas de l'appliance.

Dépannez

Remarque: Pour plus d'informations sur la façon dépanner des questions VPN, référez-vous aux solutions de dépannage VPN.

Informations connexes

- Exemple amélioré de configuration du VPN de Rai-à-client pour la version 7.0 d'appareils de Sécurité PIX
- Client VPN Cisco
- Négociation IPSec/Protocoles IKE
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Cheveu-goupiller sur Cisco ASA
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems