Exemple de configuration de PIX/ASA en tant que serveur VPN distant avec authentification étendue à l'aide de l'interface CLI et d'ASDM

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Produits connexes
Conventions
Informations générales
Configurations
Configurez l'ASA/PIX comme serveur de VPN distant utilisant l'ASDM
Configurez l'ASA/PIX comme serveur de VPN distant utilisant la CLI
Configuration du stockage de mot de passe pour Client VPN Cisco
Désactivez l'authentification étendue
Vérifiez
Dépannez
ACL de cryptage incorrect
Informations connexes

Introduction

Ce document décrit comment configurer le dispositif de sécurité adaptatif (ASA) de la gamme Cisco 5500 pour agir en tant que serveur de VPN distant utilisant l´Adaptative Security Device Manager (ASDM) ou la CLI. L'ASDM fournit la gestion et la surveillance de la sécurité de classe mondiale par une interface de gestion basée sur le Web, intuitive et facile à utiliser. Une fois que la configuration Cisco ASA est complète, elle peut être vérifiée en utilisant le Client VPN Cisco.

Référez-vous à Exemple de configuration d'authentification PIX/ASA 7.x et Client VPN Cisco 4.x avec Windows 2003 RADIUS IAS (sur Active Directory) afin de configurer la connexion VPN d'accès à distance entre un client VPN Cisco (4.x pour Windows) et le dispositif de sécurité 7.x de le gamme PIX 500. L'utilisateur distant du Client VPN authentifie contre l'Active Directory en utilisant un serveur RADIUS du service d'authentification Internet (IAS) de Microsoft Windows 2003.

Référez-vous à PIX/ASA 7.x et Client VPN Cisco 4.x pour un exemple de configuration d'authentification Cisco secure ACS afin d´établir une connexion VPN d'accès à distance entre un Client VPN Cisco (4.x pour Windows) et le dispositif de sécurité 7.x de le gamme PIX 500 à l´aide d´un Cisco Secure Access Control Server (ACS version 3.2) pour l'authentification étendue

(Xauth).

Conditions préalables

Conditions requises

Ce document suppose que l´ASA est complètement opérationnel et configuré pour permettre au Cisco ASDM ou CLI d'apporter des modifications de configuration.

Remarque: Référez-vous à Permettre l'accès HTTPS pour l'ASDM ou PIX/ASA 7.x : SSH dans l'exemple de configuration d'interface interne et externe pour permettre au périphérique d´être configuré à distance par l'ASDM ou Secure Shell (SSH).

Composants utilisés

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

- Logiciel Cisco Adaptive Security Appliance versions 7.x et ultérieures
- Adaptive Security Device Manager Versions 5.x et ultérieures
- Client VPN Cisco Versions 4.x et ultérieures

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

Vous pouvez également utiliser cette configuration avec le dispositif de sécurité Cisco PIX Versions 7.x et ultérieures.

Conventions

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

Informations générales

Les configurations d'accès à distance fournissent un accès à distance sécurisé pour les Clients VPN Cisco, tels que les utilisateurs mobiles. Un VPN d'accès à distance permet aux utilisateurs distants d´accéder sécuritairement aux ressources réseau centralisées. Le Client VPN Cisco se conforme au protocole IPSec et est spécifiquement conçu pour fonctionner avec l'appareil de sécurité. Cependant, l'appareil de sécurité peut établir des connexions d'IPSec avec beaucoup de clients protocol-conformes. Référez-vous aux Guides de configuration ASA pour plus d'informations sur IPSec.

Les groupes et les utilisateurs sont des concepts de noyau en Gestion de la Sécurité des VPN et dans la configuration de l'appareil de sécurité. Ils spécifient les attributs qui déterminent l'accès d'utilisateurs et l'utilisation du VPN. Un groupe est une collection d'utilisateurs traités comme entité

unique. Les utilisateurs obtiennent leurs attributs dans les politiques de groupe. Les groupes de tunnel identifient la politique de groupe pour des connexions spécifiques. Si vous n'affectez pas une politique de groupe particulière à des utilisateurs, la politique de groupe par défaut s'applique pour la connexion.

Un groupe de tunnel se compose d'un ensemble d´enregistrements qui détermine les politiques de connexion de tunnel. Ces enregistrements identifient les serveurs auxquels les utilisateurs du tunnel sont authentifiés, aussi bien que les serveurs de gestion des comptes, le cas échéant, auxquels les informations de connexions sont envoyées. Ils identifient également une politique de groupe par défaut pour les connexions, et ils contiennent des paramètres protocol-spécifiques de connexion. Les groupes de tunnel incluent un nombre restreint d'attributs qui concernent la création du tunnel lui-même. Les groupes de tunnel incluent un pointeur à une politique de groupe qui définit des attributs adaptés à l'utilisateur.

Remarque: Dans l´exemple de configuration de ce document, des comptes d'utilisateur local sont utilisés pour l'authentification. Si vous voudriez utiliser un autre service, tel que le LDAP et RADIUS, référez-vous à Configurer un serveur RADIUS externe pour l'autorisation et l'authentification.

Le protocole Internet Security Association and Key Management Protocol (ISAKMP), également appelé IKE, est le protocole de négociation que les serveurs conviennent sur la façon d´établir une association de sécurité IPSec. Chaque négociation ISAKMP est divisée en deux sections, Phase1 et Phase2. Phase1 crée le premier tunnel pour protéger par la suite les messages de négociation ISAKMP. Phase2 crée tunnel qui protège les données qui voyagent à travers la connexion sécurisée. Référez-vous à Mots clés de la politique ISAKMP pour les commandes de CLI pour plus d'informations sur ISAKMP.

Configurations

Configurez l'ASA/PIX comme serveur de VPN distant utilisant l'ASDM

Complétez ces étapes afin de configurer Cisco ASA comme serveur de VPN distant utilisant l'ASDM :

1. Sélectionnez **Assistants > Assistant de VPN** de la fenêtre Accueil.
2. Sélectionnez le type de tunnel VPN **Accès à distance** et assurez-vous que l´interface tunnel VPN est définie comme désiré.
3. Le seul client VPN type disponible est déjà sélectionné. 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 sélectionnée 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 devrait seulement être utilisé par des personnes qui configurent l'ASA ou par des 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 à Authentification et autorisation aux groupes de serveurs PIX/ASA 7.x pour des utilisateurs de VPN par l'intermédiaire de l'exemple de configuration ASDM pour des informations sur la façon de configurer un groupe de serveurs AAA externe par l'intermédiaire de l'ASDM.

6. Ajoutez des utilisateurs à la base de données locale s'il y a lieu.**Remarque:** Ne pas supprimer les utilisateurs existants de cette fenêtre. Sélectionnez **configuration > gestion de périphérique > administration > comptes d'utilisateur dans la fenêtre principale ASDM** pour modifier les entrées existantes dans la base de données ou les supprimer 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 correspondre exactement. Cependant, le Client VPN Cisco sélectionne automatiquement la configuration appropriée pour lui-même. Par conséquent, aucun 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 correspondre exactement. Cependant, le Client VPN Cisco sélectionne automatiquement la configuration appropriée pour lui-même. Par conséquent, aucun configuration d´IKE n'est nécessaire sur le PC Client.
11. Spécifiez lequel, le cas échéant, des hôtes ou des réseaux internes devraient être exposés aux utilisateurs distants de 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.

Configurez l'ASA/PIX comme serveur de VPN distant utilisant la CLI

Complétez ces étapes afin de configurer un serveur VPN Access distant à partir de la ligne de commande. Référez-vous à Configurer les vpn d'accès à distance ou Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5505-Références de commande pour plus d'informations sur chaque commande qui est utilisée.

1. Saisissez la commande **ip local pool** en mode de configuration globale afin de configurer les pools d´adresses IP à utiliser pour les tunnels d'accès à distance de VPN. Afin de supprimer les pools d´adresses, saisissez la forme non de cette commande.L´appliance de sécurité utilise des pools d'adresses basés sur le groupe de tunnels pour la connexion. Si vous configurez plus d´un pool d'adresses pour un groupe de tunnels, l'appliance de sécurité les utilise dans l´ordre dans lequel ils sont configurés. Émettez cette commande afin de créer un pool d´adresses locales qui peuvent être utilisées pour assigner des adresses dynamiques aux clients VPN d'accès à distance :`ASA-AIP-CLI(config)#`**`ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0`**
2. Émettez la commande suivante :`ASA-AIP-CLI(config)#`**`username marty password 12345678`**
3. Émettez cet ensemble de commandes afin de configurer le tunnel spécifique :Asa-AIP-CLI(config)#isakmp **politique 1 authentification pré-partagée**Asa-AIP-CLI(config)#isakmp

politique 1 cryptage 3desASA-AIP-CLI(config)#isakmp **politique 1 hash sha**ASA-AIP-CLI(config)#isakmp **politique 1 groupe 2**ASA-AIP-CLI(config)#isakmp **politique 1 durée de vie 43200**ASA-AIP-CLI(config)#isakmp **activez extérieur**ASA-AIP-CLI(config)#crypto **ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac**ASA-AIP-CLI(config)#crypto **dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHASet reverse-route de l'outside_dyn_map 10 de la dynamique-MAP ASA-**AIP-CLI(config)#cryptoASA-AIP-CLI(config)#crypto **dynamic-map outside_dyn_map 10 set security-association durée de vie secondes 288000Outside_dyn_map dynamique d'ipsec-ISAKMP de l'outside_map 10 de la carte ASA-**AIP-CLI(config)#cryptoASA-AIP-CLI(config)#crypto **map outside_map interface extérieure**ASA-AIP-CLI(config)#crypto **isakmp nat-traversal**

4. *Facultatif :* Si vous voulez que la connexion ignore l'access-list qui est appliquée à l´interface, émettez cette commande :`ASA-AIP-CLI(config)#`**`sysopt connection permit-ipsec`**
   Remarque: Cette commande fonctionne sur les images 7.x avant 7.2(2). Si vous utilisez l'image 7.2(2), émettez la commande ASA-AIP-CLI(config)#sysopt connection permit-vpn.
5. Émettez la commande suivante :`ASA-AIP-CLI(config)#`**`group-policy hillvalleyvpn internal`**
6. Émettez ces commandes afin de configurer les paramètres de la connexion du client :ASA-AIP-CLI(config)#group-policy **hillvalleyvpn attributes**ASA-AIP-CLI(config)#(config-group-policy)#dns-server **value 172.16.1.11**ASA-AIP-CLI(config)#(config-group-policy)#vpn-tunnel-protocol **IPSec**ASA-AIP-CLI(config)#(config-group-policy)#default-domain **value test.com**
7. Émettez la commande suivante :`ASA-AIP-CLI(config)#`**`tunnel-group hillvalleyvpn ipsec-ra`**
8. Émettez la commande suivante :`ASA-AIP-CLI(config)#`**`tunnel-group hillvalleyvpn ipsec-attributes`**
9. Émettez la commande suivante :`ASA-AIP-CLI(config-tunnel-ipsec)#`**`pre-shared-key cisco123`**
10. Émettez la commande suivante :`ASA-AIP-CLI(config)#`**`tunnel-group hillvalleyvpn general-attributes`**
11. Émettez cette commande afin de référer la base de données des utilisateurs locaux pour l'authentification.`ASA-AIP-CLI(config-tunnel-general)#`**`authentication-server-group LOCAL`**
12. Associez la stratégie de groupe au groupe de tunnels`ASA-AIP-CLI(config-tunnel-ipsec)#` **`default-group-policy hillvalleyvpn`**
13. Émettez cette commande tandis qu´en mode general-attributes du tunnel-group hillvalleyvpn afin d'assigner le vpnpool créé dans l'étape 1 au groupe hillvalleyvpn.`ASA-AIP-CLI(config-tunnel-general)#`**`address-pool vpnpool`**

Exécution de Config sur le périphérique ASA

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASAwAIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted names !
interface Ethernet0/0 nameif outside security-level 0 ip
address 10.10.10.2 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 172.16.1.2
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive dns server-group DefaultDNS domain-name
corp.com pager lines 24 mtu outside 1500 mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 no asdm history enable arp timeout 14400
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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
```

```
group-policy hillvalleyvpn1 internal group-policy
hillvalleyvpn1 attributes dns-server value 172.16.1.11
vpn-tunnel-protocol IPSec default-domain value test.com
username marty password 6XmYwQOO9tiYnUDN encrypted no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart crypto ipsec transform-set ESP-3DES-SHA esp-
3des esp-sha-hmac crypto dynamic-map outside_dyn_map 10
set transform-set ESP-3DES-SHA crypto dynamic-map
outside_dyn_map 10 set security-association lifetime
seconds 288000 crypto map outside_map 10 ipsec-isakmp
dynamic outside_dyn_map crypto map outside_map interface
outside crypto isakmp enable outside crypto isakmp
policy 10 authentication pre-share encryption 3des hash
sha group 2 lifetime 86400 crypto isakmp nat-traversal
20 tunnel-group hillvalleyvpn type ipsec-ra tunnel-group
hillvalleyvpn general-attributes address-pool vpnpool
default-group-policy hillvalleyvpn tunnel-group
hillvalleyvpn ipsec-attributes pre-shared-key * telnet
timeout 5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
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
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192 : end
ASA-AIP-CLI(config)#
```

Configuration du stockage de mot de passe pour Client VPN Cisco

Si vous avez de nombreux Clients VPN Cisco, il est très difficile de se rappeler tous les noms utilisateurs et mots de passe des Clients VPN. Afin d'enregistrer les mots de passe dans la machine du Client VPN, configurez l'ASA/PIX et le Client VPN comme décrit dans cette section.

ASA/PIX

Utilisez la commande **group-policy attributes** en mode de configuration globale :

```
group-policy VPNusers attributes password-storage enable
```

Client VPN Cisco

Modifiez **.pcf file** et modifiez ces paramètres :

```
SaveUserPassword=1 UserPassword= <type your password>
```

Désactivez l'authentification étendue

En mode groupe de tunnels, entrez cette commande afin de désactiver l'authentification étendue, qui est activée par défaut, sur le PIX/ASA 7.x :

```
asa(config)#tunnel-group client ipsec-attributes asa(config-tunnel-ipsec)#isakmp ikev1-user-
authentication none
```

Après avoir désactivé l'authentification étendue, les Clients VPN ne font pas apparaître un nom

utilisateur/mot de passe pour une authentification (Xauth). Par conséquent, l'ASA/PIX n'exige pas la configuration du nom utilisateur et du mot de passe pour authentifier les Clients VPN.

Vérifiez

Essayez de vous connecter à Cisco ASA en utilisant le Client VPN Cisco afin de vérifier que l'ASA est configuré avec succès.

1. Sélectionnez **Connection Entries > New**.
2. Complétez les détails de votre nouvelle connexion.Le champ Host devrait contenir l'adresse IP ou le nom d´hôte du Cisco ASA précédemment configuré. Les informations d'authentification de groupe devraient correspondre à cela utilisé dans la **sauvegarde de** clic d'étape 4. quand vous êtes de finition.
3. Sélectionnez la connexion de création récente, et cliquez sur **Connect**.
4. Saisissez un nom utilisateur et un mot de passe pour l'authentification étendue. Cette information devrait correspondre à celle spécifiée dans les étapes 5 et 6.
5. Une fois que la connexion est établie avec succès, sélectionnez **Statistics** dans le menu Status pour vérifier les données du tunnel.Cette fenêtre montre les informations de trafic et de cryptage :Cette fenêtre montre les informations de split tunneling :

Dépannez

Utilisez cette section pour dépanner votre configuration.

ACL de cryptage incorrect

ASDM 5.0(2) est connu pour créer et appliquer une liste de contrôle d'accès (ACL) de cryptage qui peut poser des problèmes pour les Clients VPN qui utilisent le split tunneling, aussi bien que pour des clients matériels en mode de network-extension. Utilisez l´ASDM version 5.0(4.3) ou ultérieure afin d'éviter ce problème. Référez-vous au bug Cisco ayant l'ID CSCsc10806 (clients enregistrés uniquement) pour plus de détails.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Dépannage et alertes des dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems