ASA/PIX : Le trafic d'intercommunication expliquant des clients vpn utilisant l'exemple de configuration ACS

Contenu

Introduction

Ce document fournit à une configuration d'échantillon pour expliquer les clients vpn (IPsec/SSL) utilisant PIX/ASA ACS. L'appliance de sécurité adaptable peut envoyer l'information de comptabilité à un serveur de RAYON ou TACACS+ au sujet de n'importe quel TCP ou trafic UDP qui traverse l'appliance de sécurité adaptable. Si ce trafic est également authentifié, alors le serveur d'AAA peut mettre à jour l'information de comptabilité par le nom d'utilisateur. Si le trafic n'est pas authentifié, le serveur d'AAA peut mettre à jour l'information de comptabilité par l'adresse IP. L'information de comptabilité inclut quand les sessions commencent et arrêtent, nom d'utilisateur, le nombre d'octets qui traversent l'appliance de sécurité adaptable pour la session, le service utilisé, et la durée de chaque session.

Avant que vous puissiez utiliser cette commande, vous devez d'abord indiquer un serveur d'AAA avec l'ordre d'AAA-**serveur**. L'information de comptabilité est envoyée seulement au serveur actif à un groupe de serveurs à moins que vous activiez la comptabilité simultanée utilisant la commande de comptabilité-**mode** dans le mode de configuration de protocole d'AAA-serveur.

Vous ne pouvez pas utiliser la **commande match d'aaa accounting** dans la même configuration que l'**aaa accounting incluent** et **excluent des** commandes. Nous proposons que vous utilisiez la **commande match** au lieu de l'**inclusion** et **excluiez des** commandes ; **l'inclure** et **excluent des** commandes ne sont pas pris en charge par ASDM.

Ce document suppose que l'Accès à distance VPN utilisant ASA/PIX avec la configuration de client vpn d'IPsec VPN Client/SSL (Anyconnect) avec ACS pour l'authentification est déjà fait et

fonctionne correctement. Ce document se concentre sur la façon configurer l'AAA expliquant des clients vpn sur des dispositifs de sécurité ASA avec ACS.

Référez-vous à PIX/ASA 7.x et Client VPN Cisco 4.x pour l'exemple de configuration d'authentification de Cisco Secure ACS afin de se renseigner plus sur la façon installer une connexion VPN d'Accès à distance entre un Client VPN Cisco (4.x pour Windows) et l'appliance 7.x de Sécurité de gamme 500 PIX utilisant un Cisco Secure Access Control Server (version 3.2 ACS) pour l'authentification étendue (Xauth).

Référez-vous à ASA 8.x : AnyConnect VPN Client pour l'Internet public VPN sur un exemple de configuration de bâton afin de se renseigner plus sur la façon installer une appliance de sécurité adaptable (ASA) 8.0.2 pour exécuter le VPN SSL sur un bâton avec le Cisco AnyConnect VPN Client.

Conditions préalables

Conditions requises

Assurez-vous que le client vpn peut établir la connexion et atteindre de bout en bout correctement.

Composants utilisés

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

- Gamme de Cisco ASA 5500 qui exécute 7.x et plus tard
- Cisco Secure ACS 4.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.

Produits connexes

Ce document peut également être utilisé avec le Cisco PIX 500 Series Security Appliance avec la version de logiciel 7.x et plus tard.

Conventions

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

Configurez

Configuration ASA

Pour configurer la comptabilité, exécutez ces étapes :

1. Si vous voulez que l'appliance de sécurité adaptable fournisse des données de comptabilité par utilisateur, vous devez activer l'authentification. Si vous voulez que l'appliance de sécurité adaptable fournisse des données de comptabilité par adresse IP, l'activation de l'authentification n'est pas nécessaire et vous pouvez continuer à l'étape 2.
2. Utilisant la **commande access-list**, créez une liste d'accès qui identifie les adresses sources et les adresses de destination du trafic que vous voulez ont rendues compte.**Remarque:** Si vous avez configuré l'authentification et voulez des données de comptabilité pour tout le trafic étant authentifié, vous pouvez utiliser la même liste d'accès que vous avez créée pour l'usage avec la **commande match d'authentification d'AAA**.
3. Afin d'activer la comptabilité, sélectionnez cette commande :`hostname(config)# aaa accounting match acl_name interface_name server_group` Où :L'argument d'*acl_name* est le nom de liste d'accès réglé dans la **commande access-list**.L'argument d'*interface_name* est le nom d'interface réglé dans la commande de **nameif**.L'argument de *server_group* est le nom de groupe de serveurs réglé dans l'ordre d'AAA-**serveur**.**Remarque:** Alternativement, vous pouvez utiliser l'**aaa accounting incluez la** commande (qui identifie le trafic dans la commande), mais vous ne pouvez pas utiliser les deux méthodes dans la même configuration. Voyez le pour en savoir plus de référence de commandes de Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5580.

Ces commandes authentifient, autorisent, et expliquent le trafic sortant :

ASA

```
!--- Using the aaa-server command, identify your AAA
servers. If you have already !--- identified your AAA
servers, continue to the next step. hostname(config)#
aaa-server AuthOutbound protocol RADIUS hostname(config-
aaa-server-group)# exit !--- Identify the server,
including the AAA server group it belongs to and !---
enter the IP address, Shared key of the AAA Server.
hostname(config)# aaa-server AuthOutbound (inside) host
10.1.1.1 hostname(config-aaa-server-host)# key
TACPlusUauthKey hostname(config-aaa-server-host)# exit
!--- Using the access-list command, create an access
list that identifies the source !--- addresses
anddestination addresses of traffic you want to
authenticate. hostname(config)# access-list TELNET_AUTH
extended permit tcp any any eq telnet !--- Using the
access-list command, create an access list that
identifies the source !--- addresses anddestination
addresses of traffic you want to Authorize and
Accounting. hostname(config)# access-list SERVER_AUTH
extended permit tcp any any !--- configure
authentication, enter this command: hostname(config)#
aaa authentication match TELNET_AUTH inside AuthOutbound
!--- configure authorization, enter this command:
hostname(config)# aaa authorization match SERVER_AUTH
inside AuthOutbound
!--- This command causes the PIX Firewall to send !---
RADIUS accounting packets for RADIUS-authenticated
outbound sessions to the AAA !--- server group named
"AuthOutbound": hostname(config)# aaa accounting match
SERVER_AUTH inside AuthOutbound
```

Comptabilité de RAYON utilisant la configuration ACS

L'enregistreur CSV enregistre des données pour se connecter des attributs dans les colonnes séparées par des virgules (,). Vous pouvez importer ce format dans un grand choix d'applications tierces, telles que Microsoft Excel ou Microsoft Access. Après que vous importiez des données à partir d'un fichier CSV dans de telles applications, vous pouvez préparer des tableaux ou exécuter des requêtes, telles que déterminer combien d'heures un utilisateur a été enregistré dans le réseau au cours d'une période donnée. Pour des informations sur la façon utiliser un fichier CSV dans une application tierce telle que Microsoft Excel, voyez la documentation du fournisseur tiers.

Vous pouvez accéder aux fichiers CSV sur le disque dur de serveur ACS ou vous pouvez télécharger le fichier CSV de l'interface web.

Par défaut, ACS maintient des fichiers journal dans les répertoires qui sont seuls au log. Vous pouvez configurer l'emplacement de fichier journal des logs CSV. Les répertoires par défaut pour tous les logs résident dans **sysdrive : \ Fichiers de programme \ CiscoSecure ACS vx.x.**

Afin de configurer la CiscoSecure ACS pour exécuter la comptabilité de RAYON utilisant CSV, exécutez ces étapes :

1. Dans la barre de navigation, **configuration système de** clic.
2. **Se connecter de** clic. La page de configuration de journalisation paraît.
3. **Comptabilité** choisie de **RAYON CSV**.
4. Confirmez que le **log dans la** case d'**état de comptabilité de RAYON CSV** est sélectionné. S'il n'est pas sélectionné, sélectionnez-le maintenant.
5. Dans les **attributs choisis pour se connecter la** table, assurez-vous que les attributs RADIUS que vous voulez voir dans le journal de traçabilité de RAYON apparaissent dans la liste d'**attributs loggée**. En plus des attributs RADIUS standard, il y a plusieurs offre spéciale se connectant des attributs fournis par CiscoSecure ACS, telle que le nom réel, les informations d'ExtDB, et connectés à distance.
6. (Facultatif) si vous utilisez la CiscoSecure ACS pour des Windows Server, vous pouvez spécifier la Gestion de fichier journal, qui détermine à quel point les grands fichiers de compte de RAYON peuvent être, combien sont retenus, pendant combien de temps, et où ils sont enregistrés.
7. Si vous avez apporté des modifications à la configuration de comptabilité de RAYON, cliquez sur Submit. La CiscoSecure ACS enregistre et implémente les modifications que vous avez apportées à sa configuration de comptabilité de RAYON.

Ces thèmes décrivent comment visualiser et télécharger ACS CSV signale :

- Noms de fichier journal CSV
- Visionnement d'un état CSV
- Télécharger un état CSV

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide utilisateur pour le Cisco Secure Access Control Server 4.2 - Se connecter et états
- Page d'assistance des appliances de sécurité adaptables de la gamme Cisco ASA 5500
- PIX/ASA : Exemple de configuration d'un proxy à coupure pour l'accès réseau à l'aide d'un serveur TACACS+ et RADIUS
- Cisco Secure Access Control Server pour Windows
- Dispositifs de sécurité de la gamme Cisco PIX 500
- Support et documentation techniques - Cisco Systems