Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM

Contenu

Introduction

La technologie de réseau privé virtuel (VPN) de Secure Socket Layer (SSL) vous permet de vous connecter en toute sécurité depuis n'importe quel emplacement à un réseau d'entreprise interne en utilisant l'une des méthodes suivantes :

- **VPN SSL sans client (WebVPN)** - Fournit un client distant nécessitant un navigateur Web compatible SSL pour accéder à des serveurs Web HTTP ou HTTPS sur un réseau local d'entreprise (LAN). En outre, le VPN SSL sans client permet l'exploration de fichiers Windows via le protocole Common Internet File System (CIFS). Outlook Web Access (OWA) est un exemple d'accès HTTP.Consultez l'Exemple de configuration d'un VPN SSL sans client (WebVPN) sur une ASA afin d'en savoir plus sur le VPN SSL sans client.
- **VPN SSL client léger (redirection de port)** - Fournit un client distant qui télécharge un petit applet basé sur Java et permet l'accès sécurisé aux applications de Protocole de contrôle de transmissions (TCP) qui utilisent des numéros de port statiques. Le Post Office Protocol (POP3), le Simple Mail Transfer Protocol (SMTP), le Protocole de messagerie IMAP, le Secure shell (SSH) et le telnet sont des exemples d'accès sécurisé. Puisque les fichiers sur l'ordinateur local changent, les utilisateurs doivent avoir des privilèges d'administrateur locaux pour utiliser cette méthode. Cette méthode de VPN SSL ne fonctionne pas avec les applications qui utilisent des affectations de ports dynamiques, telles que certaines applications de protocole de transfert de fichiers (FTP).Consultez l'Exemple de configuration d'un VPN SSL client léger (WebVPN) sur une ASA avec ASDM afin d'en savoir plus sur le VPN SSL client léger.**Note**: Le Protocole de datagramme utilisateur (UDP) n'est pas pris en charge.
- **Client VPN SSL (Mode Tunnel)** — Télécharge un petit client sur le poste de travail distant et permet un accès entièrement sécurisé aux ressources d'un réseau d'entreprise interne. Vous pouvez télécharger le client VPN SSL (SVC) sur un poste de travail distant de manière permanente, ou vous pouvez supprimer le client une fois que la session sécurisée est fermée.

Ce document décrit la procédure de configuration du SVC sur un Dispositif de sécurité adaptatif (ASA) à l'aide d'Adaptive Security Device Manager (ASDM). Les lignes de commande résultant de cette configuration sont répertoriées dans la section Résultats.

Conditions préalables

Conditions requises

Assurez-vous de répondre à ces exigences avant d'essayer cette configuration :

- SVC initie le support du logiciel Cisco Adaptive Security Appliance Version 7.1 et ultérieures
- Privilèges d'administrateur locaux sur tous les postes de travail distants
- Commandes Javas et ActiveX sur le poste de travail distant
- Le port 443 n'est pas obstrué à un point quelconque du chemin de connexion

Composants utilisés

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

- Logiciel Cisco Adaptive Security Appliance Version 7.2(1)
- Cisco Adaptive Security Device Manager 5.2(1)
- Dispositif de sécurité adaptatif de la gamme Cisco 5510
- Microsoft Windows XP Professionnel SP 2

Les informations de ce document ont été élaborées dans un environnement de laboratoire. Tous

les périphériques utilisés dans ce document ont été réinitialisés à leur configuration par défaut. Si votre réseau est opérationnel, assurez-vous que vous comprenez l'impact potentiel de toute commande. Toutes les adresses IP utilisées dans cette configuration ont été sélectionnées à partir d'adresses RFC 1918 dans un environnement de laboratoire ; ces adresses IP ne sont pas routables sur Internet et sont utilisées à des fins de test uniquement.

Diagramme du réseau

Ce document utilise la configuration réseau décrite dans cette section.

Un utilisateur distant se connecte à l'adresse IP de l'ASA avec un navigateur Web compatible SSL. Après l'authentification réussie, le SVC est téléchargé sur l'ordinateur client et l'utilisateur peut utiliser une session sécurisée chiffrée pour l'accès complet à toutes les ressources autorisées sur le réseau de l'entreprise.

Tâches de préconfiguration

Avant de commencer, complétez ces tâches :

- Référez-vous à Permettre l'accès HTTPS pour l'ASDM afin de permettre l'ASA d'être configuré par l'ASDM.Pour accéder à l'application ASDM à partir de votre station de gestion, utilisez un navigateur Web compatible SSL et saisissez l'adresse IP du périphérique ASA. Exemple : **https://inside_ip_address,** où *inside_ip_address* est l'adresse de l'ASA. Une fois que l'ASDM est chargé, vous pouvez commencer la configuration du SVC.
- Téléchargez le package client VPN SSL (sslclient-win*.pkg) depuis le site Web de téléchargement de logiciels Cisco (clients enregistrés seulement) sur le disque dur local de la station de gestion à partir de laquelle vous accédez à l'application ASDM.

Le WebVPN et l'ASDM ne peuvent pas être activés sur la même interface ASA à moins que vous changiez les numéros de port. Si vous voulez que les deux Technologies utilisent le même port (port 443) sur le même périphérique, vous pouvez activer l'ASDM sur l'*interface interne* et activer le WebVPN sur l'*interface externe*.

Conventions

Pour plus d'informations sur les conventions des documents, reportez-vous au document Conventions relatives aux conseils techniques Cisco.

Configurer le Client VPN SSL sur une ASA

Pour configurer le client VPN SSL sur une ASA, complétez ces étapes :

1. Activez l'accès au WebVPN sur l'ASA
2. Installez et activez le client VPN SSL sur l'ASA
3. Activez l'installation de SVC sur les clients
4. Activez les paramètres Rekey

Étape 1. Activer l'accès au WebVPN sur l'ASA

Pour activer l'accès au WebVPN sur l'ASA, complétez ces étapes :

1. Dans l'application ASDM, cliquez sur **Configuration**, puis cliquez sur **VPN**.
2. Développez **WebVPN**, puis sélectionnez **WebVPN Access**.
3. Sélectionnez l'interface pour laquelle vous souhaitez activer WebVPN, puis cliquez sur **Enable.**

Étape 2. Installer et activer le Client VPN SSL sur l'ASA

Pour installer et activer le client VPN SSL sur l'ASA, complétez ces étapes :

1. Cliquez sur **Configuration**, puis cliquez sur **VPN**.
2. Dans le volet de navigation, développez **WebVPN**, puis sélectionnez **SSL VPN Client**.
3. Cliquez sur **Add**.La boîte de dialogue Add SSL VPN Client Image apparaît.
4. Cliquez sur le bouton **Upload**.La boîte de dialogue Upload Image apparaît.
5. Cliquez sur le bouton **Browse Local Files** afin de localiser un fichier sur votre ordinateur local, ou cliquez sur le bouton **Browse Flash** afin de localiser un fichier dans le système de fichiers Flash.
6. Localisez le fichier d'image client à télécharger, puis cliquez sur **OK**.
7. Cliquez sur **Upload File**, puis cliquez sur **Close**.
8. Une fois l'image client téléchargée sur flash, cochez la case **Enable SSL VPN Client**, puis cliquez sur **Apply**.**Note**: Si vous recevez un message d'erreur, vérifiez que l'accès au WebVPN est activé. Dans le volet de navigation, développez **WebVPN**, puis sélectionnez **WebVPN Access**. Sélectionnez l'interface pour laquelle vous souhaitez configurer l'accès, puis cliquez sur **Enable.**
9. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

Étape 3. Activer l'installation des SVC sur les clients

Pour activer l'installation de SVC sur des clients, complétez ces étapes :

1. Dans le volet de navigation, développez **IP Address Management** et choisissez **IP Pools**.
2. Cliquez sur **Add**, saisissez les valeurs dans les champs Name, Starting IP Address, Ending IP Address et Subnet Mask. Les adresses IP saisies dans les champs Starting IP Address et Ending IP Address doivent provenir des sous-réseaux de votre réseau interne.
3. Cliquez sur **OK**, puis sur **Apply**.
4. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.
5. Dans le volet de navigation, développez **IP Address Management**, puis choisissez **Assignment**.
6. Cochez la case **Use internal address pools**, puis désélectionnez les cases **Use authentication server** et **Use DHCP**.
7. Cliquez sur **Apply**.
8. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.
9. Dans le volet de navigation, développez **General** et sélectionnez **Tunnel Group**.
10. Sélectionnez le groupe de tunnels que vous souhaitez gérer, puis cliquez sur **Edit**.
11. Cliquez sur l'onglet **Client Address Assignment**, puis sélectionnez le pool d'adresses IP nouvellement créé dans la liste des pools disponibles.
12. Cliquez sur **Add**, puis cliquez sur **OK**.

13. Dans la fenêtre d'application ASDM, cliquez sur **Apply**.
14. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

Étape 4. Activer le paramètre Rekey

Pour activer les paramètres de Rekey :

1. Dans le volet de navigation, développez **General**, puis sélectionnez **Group Policy**.
2. Sélectionnez la stratégie que vous souhaitez appliquer à ce groupe de clients, puis cliquez sur **Edit**.
3. Sous l'onglet General, désélectionnez la case **Tunneling Protocols Inherit**, puis cochez la case **WebVPN**.
4. Cliquez sur l'onglet **WebVPN**, cliquez sur l'onglet **SSLVPN Client**, puis sélectionnez ces options :Pour l'option Use SSL VPN Client, désélectionnez la case à cocher **Inherit**, puis cliquez sur la case d'option **Optional**.Ce choix permet au client distant de télécharger ou non le SVC. Le choix *Always* permet de s'assurer que le SVC est téléchargé sur le poste de travail distant pendant chaque connexion VPN SSL.Pour l'option Keep Installer on Client System, désélectionnez la case à cocher **Inherit**, puis cliquez sur le bouton radio **Yes**.Cette action permet au logiciel SVC de demeurer sur l'ordinateur client. Par conséquent, il n'est pas nécessaire que l'ASA télécharge le logiciel SVC sur le client chaque fois qu'une connexion est établie. Cette option est un bon choix pour les utilisateurs distants qui accèdent souvent au réseau de l'entreprise.Pour l'option Renegotiation Interval, décochez la case **Inherit**, décochez la case à cocher **Unlimited** et saisissez le nombre de minutes jusqu'à une nouvelle saisie.La sécurité est améliorée en fixant des limites à la durée de validité d'une clé.Pour l'option Renegotiation Method, décochez la case à cocher **Inherit** et cliquez la case d'option **SSL**. La renégociation peut utiliser le tunnel SSL actuel ou un nouveau tunnel créé expressément pour la renégociation.Vos attributs client VPN SSL doivent être configurés tel qu´indiqué sur cette image :
5. Cliquez sur **OK**, puis sur **Apply**.
6. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

Résultats

L'ASDM crée les configurations de ligne de commande suivantes :

ciscoasa

```
ciscoasa(config)#show run
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
```

```
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask
255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 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 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 Statements group-policy GroupPolicy1
internal group-policy GroupPolicy1 attributes vpn-
tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the
SVC for WebVPN webvpn svc enable svc keep-installer
installed svc rekey time 30 svc rekey method ssl !
username cisco password 53QNetqK.Kqqfshe encrypted
privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart !--- Tunnel
Group and Group Policy using the defaults here tunnel-
group DefaultWEBVPNGroup general-attributes address-pool
CorporateNet default-group-policy GroupPolicy1 ! no vpn-
addr-assign aaa no vpn-addr-assign dhcp ! telnet timeout
5 ssh 172.22.1.0 255.255.255.0 outside 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 rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global !--- Enable webvpn
and the select the SVC client webvpn enable outside svc
image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !-
-- Provide list for access to resources url-list
ServerList "E-Commerce Server1" http://10.2.2.2 1 url-
list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-
group-list enable prompt hostname context
Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

Personnaliser votre configuration

Les procédures décrites dans Configurer le Client VPN SSL sur une ASA utilisent les noms d´ASA par défaut names pour la stratégie de groupe (*GroupPolicy1*) et le groupe de tunnels (*DefaultWebVPNGroup*), tel qu´indiqué sur cette image :

Cette procédure décrit comment créer vos propres stratégies de groupe et groupes de tunnels et comment les relier selon les stratégies de sécurité de votre organisation.

Pour personnaliser votre configuration, complétez ces étapes :

1. Créez une stratégie de groupe personnalisée
2. Créez un groupe de tunnels personnalisé
3. Créez un utilisateur et ajouter-le à votre stratégie de groupe personnalisée

Étape 1. Créer une stratégie de groupe personnalisée

Pour créer une stratégie de groupe personnalisée, complétez ces étapes :

1. Cliquez sur **Configuration**, puis cliquez sur **VPN**.
2. Développez **General**, puis choisissez **Group Policy**.
3. Cliquez sur **Add**, puis sélectionnez **Internal Group Policy**.
4. Dans le champ Name, saisissez un nom pour votre stratégie de groupe.Dans cet exemple, le nom de stratégie de groupe a été modifié à *SalesGroupPolicy*.
5. Sous l'onglet General, désélectionnez la case **Tunneling Protocols Inherit**, puis cochez la case **WebVPN**.
6. Cliquez sur l'onglet **WebVPN**, puis cliquez sur l'onglet **SSLVPN Client**.Dans cette boîte de dialogue, vous pouvez également faire des choix concernant le comportement du client VPN SSL.
7. Cliquez sur **OK**, puis sur **Apply**.
8. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

Étape 2. Créer un groupe de tunnels personnalisé

Pour créer un groupe de tunnels personnalisé, complétez ces étapes :

1. Cliquez sur le **bouton Configuration**, puis cliquez sur **VPN**.
2. Développez **General**, puis sélectionnez **Tunnel Group**.
3. Cliquez sur **Add**, puis sélectionnez **WebVPN Access**.
4. Dans le champ Name, entrez un nom pour votre groupe de tunnels.Dans cet exemple, le nom du groupe de tunnels a été modifié à *SalesForceGroup*.
5. Cliquez sur la flèche de défilement **Group Policy**, puis sélectionnez votre stratégie de groupe nouvellement créée.Votre stratégie de groupe et votre groupe de tunnels sont désormais reliés.
6. Cliquez sur l'onglet **Client Address Assignment**, puis entrez les informations relatives au serveur DHCP ou sélectionnez-les à partir du pool IP créé localement.
7. Cliquez sur **OK**, puis sur **Apply**.
8. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

Étape 3. Créer un utilisateur et l'ajouter à votre stratégie de groupe personnalisée

Pour créer un utilisateur et l´ajouter à votre stratégie de groupe personnalisée, complétez ces étapes :

1. Cliquez sur **Configuration**, puis cliquez sur **VPN**.
2. Développez **General**, puis choisissez **Users**.
3. Cliquez sur **Add**, puis saisissez les informations relatives au nom d´utilisateur et au mot de passe.
4. Cliquez sur l'onglet **VPN Policy**. Assurez-vous que votre stratégie de groupe nouvellement créée s'affiche dans le champs Group Policy.Cet utilisateur hérite de toutes les caractéristiques de la nouvelle stratégie de groupe.
5. Cliquez sur **OK**, puis sur **Apply**.
6. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

Vérifiez

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

Authentification

L'authentification des clients VPN SSL et réalisée en utilisant l´une de ces méthodes :

- Serveur Cisco Secure ACS (Radius)
- Domaine NT
- Active Directory
- Mots de passe à usage unique
- Certificats numériques
- Cartes à puce
- Authentification AAA locale

Cette documentation utilise un compte local créé sur le périphérique ASA.

Note: Si un dispositif de sécurité adaptatif dispose de certificats multiples partageant le même CA, seul un de ces certificats peut être utilisé pour valider des certificats utilisateurs.

Configuration

Pour vous connecter à l'ASA avec un client distant, saisissez **https://ASA_outside_address** dans le champ Adresse d'un navigateur Web compatible SSL. *ASA_outside_address* est l'adresse IP externe de votre ASA. Si votre configuration est réussie, la fenêtre Cisco Systems SSL VPN Client apparaît.

Note: La fenêtre Cisco Systems SSL VPN Client apparaît uniquement après que vous avez accepté le certificat de l'ASA et après que le client VPN SSL a été téléchargé sur le poste de travail distant. Si la fenêtre n'apparaît pas, assurez-vous qu'elle n'est pas réduite.

Commandes

Plusieurs commandes **show** sont associées au WebVPN. Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Pour obtenir des informations détaillées à propos des **commandes show**, reportez-vous à la section Vérification des Configurations WebVPN.

Note: 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** .

Dépannez

Utilisez cette section pour dépanner votre configuration.

Erreur SVC

Problème

Il se peut que vous receviez ce message d'erreur pendant l'authentification :

```
ciscoasa(config)#show run
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 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 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 Statements group-policy GroupPolicy1 internal group-policy GroupPolicy1
attributes vpn-tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the SVC for WebVPN webvpn svc
enable svc keep-installer installed svc rekey time 30 svc rekey method ssl ! username cisco
password 53QNetqK.Kqqfshe encrypted privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !--- Tunnel Group and Group Policy using the
defaults here tunnel-group DefaultWEBVPNGroup general-attributes address-pool CorporateNet
default-group-policy GroupPolicy1 ! no vpn-addr-assign aaa no vpn-addr-assign dhcp ! telnet
timeout 5 ssh 172.22.1.0 255.255.255.0 outside 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 rsh inspect rtsp
inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp ! service-policy global_policy global !--- Enable webvpn and the select the
SVC client webvpn enable outside svc image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !---
Provide list for access to resources url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
url-list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-group-list enable prompt hostname
context Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

Solution

Si un service de pare-feu est exécuté sur votre PC, celui-ci peut perturber l'authentification. Arrêtez le service et reconnectez le client.

Le SVC a-t-il établi une session sécurisée avec l'ASA ?

Afin de vous assurer que le Client VPN SSL a établi une session sécurisée avec l'ASA :

1. Cliquez sur **Monitoring**.
2. Développez **VPN Statistics**, puis choisissez **Sessions**.
3. En utilisant le filtre du menu déroulant, choisissez **SSL VPN Client**, puis cliquez sur le bouton **Filter**.Votre configuration devrait apparaître dans la liste de sessions.

Des sessions sécurisées sont-elles établies et terminées avec succès ?

Vous pouvez afficher les journaux en temps réel afin de vous assurer que des sessions sont établies et terminées avec succès. Pour afficher des journaux de session :

1. Cliquez sur **Monitoring**, puis sur **Logging**.
2. Choisissez le **Real-time Log Viewer** ou **Log Buffer**, puis cliquez sur **View**.**Note**: Pour afficher uniquement des sessions à partir d´une adresse spécifique, filtrez par adresse.

Vérifier le pool IP dans le profil WebVPN

```
ciscoasa(config)#show run
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
```

```
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 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 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 Statements group-policy GroupPolicy1 internal group-policy GroupPolicy1
attributes vpn-tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the SVC for WebVPN webvpn svc
enable svc keep-installer installed svc rekey time 30 svc rekey method ssl ! username cisco
password 53QNetqK.Kqqfshe encrypted privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !--- Tunnel Group and Group Policy using the
defaults here tunnel-group DefaultWEBVPNGroup general-attributes address-pool CorporateNet
default-group-policy GroupPolicy1 ! no vpn-addr-assign aaa no vpn-addr-assign dhcp ! telnet
timeout 5 ssh 172.22.1.0 255.255.255.0 outside 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 rsh inspect rtsp
inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp ! service-policy global_policy global !--- Enable webvpn and the select the
SVC client webvpn enable outside svc image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !---
Provide list for access to resources url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
url-list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-group-list enable prompt hostname
context Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

Aucune adresse ne peut être attribuée à la connexion SVC. Par conséquent, vous devez attribuer l'adresse de pool IP au profil.

Si vous créez le nouveau profil de connexion, configurez alors un pseudonyme ou un groupe-url afin d'accéder à ce profil de connexion. Sinon, toutes les tentatives SSL s´appliqueront au profil de connexion WebVPN par défaut ne disposant pas d´un pool IP associé. Configurez ceci afin d´utiliser le profil de connexion par défaut et l´associer à un pool IP.

Conseils

- Assurez-vous que le routage fonctionne correctement avec le pool d'adresses IP que vous avez affecté à vos clients distants. Ce pool d'adresses IP devrait provenir d'un sous-réseau sur votre LAN. Vous pouvez également utiliser un serveur DHCP ou un serveur d'authentification pour attribuer des addresses IP.
- L'ASA crée un groupe de tunnels par défaut (*DefaultWebVPNGroup*) et une stratégie de groupe par défaut (*GroupPolicy1*). Si vous créez de nouveaux groupes et de nouvelles stratégies, veillez à appliquer les valeurs selon les stratégies de sécurité de votre réseau.
- Si vous souhaitez activer l´exploration de fichiers Windows via CIFS, saisissez un serveur WINS (NBNS) sous **Configuration > VPN > WebVPN > Servers and URLs**. Cette technologie utilise la sélection CIFS.

Commandes

Plusieurs commandes **debug** sont associées à WebVPN. Pour obtenir des informations détaillées à propos de ces commandes, reportez-vous à Utilisation des commandes Debug WebVPN.

Note: L'utilisation des commandes **debug** peut avoir un impact négatif sur votre périphérique Cisco. Avant d'utiliser les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

Informations connexes

- Exemple de configuration d'un VPN SSL sans client (WebVPN) sur ASA
- Exemple de configuration d'un VPN SSL client léger (WebVPN) sur ASA avec ASDM
- Exemple de configuration d'ASA avec WebVPN et authentification unique à l'aide d'ASDM et de NTLMv1
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems