Exemple de configuration de VPN SSL (WebVPN) client léger sur IOS avec SDM

Contenu

Introduction

La technologie de VPN SSL de client léger peut être utilisée pour permettre l'accès sécurisé pour les applications qui utilisent des prises de pression statique. Les exemples sont le telnet (23), le SSH (22), le POP3 (110), l'IMAP4 (143), et le SMTP (25). Le client léger peut être déterminé par l'utilisateur, motivé par la stratégie, ou tous deux. Access peut être configuré sur une base d'utilisateur-par-utilisateur, ou on peut créer des stratégies de groupe qui incluent un ou plusieurs utilisateurs. La technologie de VPN SSL peut être configurée en trois modes principaux : VPN SSL sans client (webvpn), client de VPN SSL de client léger (transmission du port), et de VPN SSL (Svc-plein tunnel mode).

1. **VPN SSL sans client (webvpn) :**

Un client distant a seulement besoin d'un navigateur Web compatible SSL pour accéder à des serveurs Web HTTP ou HTTPS sur le LAN de l'entreprise. L'accès est également disponible pour parcourir des fichiers Windows avec le système de fichiers Common Internet File System (CIFS). Un bon exemple d'accès HTTP est le client Outlook Web Access (OWA).

Référez-vous au VPN SSL sans client (webvpn) sur le Cisco IOS utilisant l'exemple de configuration SDM afin de se renseigner plus sur le VPN SSL sans client.

2. **VPN SSL de client léger (transmission du port)**

Un client distant doit télécharger un petit applet Javas pour l'accès sécurisé des applications TCP qui utilisent des numéros de port statiques. UDP n'est pas pris en charge. Les exemples incluent l'accès à POP3, SMTP, IMAP, SSH et Telnet. L'utilisateur doit disposer de privilèges d'administration locaux parce que des modifications sont apportées à des fichiers sur l'ordinateur local. Cette méthode de VPN SSL ne fonctionne pas avec les applications qui utilisent des affectations de ports dynamiques, par exemple, plusieurs applications FTP.

3. **Client de VPN SSL (Svc-plein tunnel mode) :**

Le client VPN SSL télécharge un petit client sur le poste de travail distant et permet un accès total et sécurisé aux ressources sur le réseau d'entreprise interne. Le SVC peut être téléchargé de manière permanente sur le poste de travail distant, ou il peut être supprimé après la fin de la session sécurisée.

Référez-vous au client de VPN SSL (SVC) sur l'IOS utilisant l'exemple de configuration SDM afin de se renseigner plus sur le client de VPN SSL.

Ce document explique une configuration simple pour le VPN SSL de client léger sur un routeur de Cisco IOS®. Les passages de VPN SSL de client léger sur ces routeurs Cisco IOS :

- Cisco 870, 1811, 1841, 2801, 2811, 2821, et Routeurs de gamme 2851
- Cisco 3725, 3745, 3825, 3845, 7200, et Routeurs de gamme 7301

Conditions préalables

Conditions requises

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

Conditions requises pour le routeur Cisco IOS

- Les Routeurs énumérés l'uns des ont chargé avec SDM et une image avancée la version IOS de 12.4(6)T ou de plus tard
- Station de Gestion chargée avec SDMCisco expédie de nouveaux Routeurs avec une copie préinstallée de SDM. Si votre routeur ne fait pas installer SDM, vous pouvez obtenir le logiciel au Security Device Manager de Téléchargement-Cisco de logiciel. Vous devez posséder un compte CCO avec un contrat de service. Référez-vous configurent votre routeur avec le Security Device Manager pour le mode d'emploi détaillé.

Conditions requises pour des ordinateurs client

- Les clients distants devraient avoir des privilèges d'administrateur locaux ; on ne l'exige pas, mais on lui suggère fortement.
- Les clients à distance doivent avoir la version 1.4 ou ultérieures de Java Runtime Environment (JRE).
- Navigateurs de client distant : Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, safari 1.2.2, ou Firefox 1.0
- Témoins activés et Popups permis sur des clients distants

Composants utilisés

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

- Cisco a avancé l'image logicielle 12.4(9)T d'entreprise
- Routeur à services intégrés Cisco 3825
- Version 2.3.1 du Cisco Router and Security Device Manager (SDM)

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 commencé par une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande. Les adresses IP utilisées pour cette configuration proviennent l'espace d'adressage RFC 1918. Ils ne sont pas juridiques sur l'Internet.

Conventions

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

Configurez

Tâche

Cette section contient les informations requises pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurez le VPN SSL de client léger

Utilisez l'assistant fourni dans l'interface du Security Device Manager (SDM) pour configurer le VPN SSL de client léger sur le Cisco IOS, ou configurez-le à l'interface de ligne de commande (CLI) ou manuellement dans l'application SDM. Cet exemple utilise l'assistant.

1. Choisissez l'onglet de **configurer**.Du volet de navigation, choisissez **VPN > webvpn**.Cliquez sur l'onglet de **webvpn de création**.Cliquez sur la case d'option à côté de **créent un nouveau webvpn**.Cliquez sur le **lancement le** bouton de **tâche sélectionnée**.
2. Les lancements d'assistant de webvpn. Cliquez sur **Next** (Suivant).Écrivez l'adresse IP et un nom unique pour ce webvpn gateway. Cliquez sur **Next** (Suivant).
3. L'écran d'authentification de l'utilisateur permet l'occasion de prévoir l'authentification des utilisateurs. Cette configuration utilise un compte créé localement sur le routeur. Vous pouvez également utiliser un serveur d'Authentification, autorisation et comptabilité (AAA).Pour ajouter un utilisateur, cliquez sur Add.Écrivez les informations utilisateur sur l'ajouter un écran de compte, et cliquez sur OK.Cliquez sur Next sur l'écran d'authentification de l'utilisateur.L'écran des Assistant de webvpn tient compte de la configuration des sites

Web d'intranet, mais cette étape est omise parce que la transmission du port est utilisée pour cet accès d'application. Si vous voulez permettre l'accès aux sites Web, utilisez les configurations sans client ou pleines de VPN SSL de client, qui ne sont pas à portée de ce document.Cliquez sur **Next** (Suivant). L'assistant affiche un écran qui permet la configuration du client de Full Tunnel. Ceci ne s'applique pas au VPN SSL de client léger (transmission du port).Décochez l'**enable Full Tunnel**. Cliquez sur **Next** (Suivant).

4. Personnalisez l'apparence de la page du portail de webvpn ou recevez l'apparence par défaut.Cliquez sur **Next** (Suivant).Visionnez le résumé de la configuration et cliquez sur Finish préalablement **> sauvegarde**.
5. Vous avez créé un webvpn gateway et un contexte de webvpn avec une stratégie de groupe jointe. Configurez les ports de client léger, qui sont rendus disponibles quand les clients se connectent au webvpn.Choisissez **configurent**.Choisissez **VPN > webvpn**.Choisissez **créent le webvpn**.Choisissez la case d'option **configurent la fonctionnalité avancée pour un webvpn existant** et cliquent sur le **lancement la tâche sélectionnée**.L'écran de bienvenue offre des points culminants des capacités de l'assistant. Cliquez sur **Next** (Suivant).Choisissez le contexte et le groupe d'utilisateurs de webvpn des menus déroulants. Cliquez sur **Next** (Suivant).Choisissez le **client léger (transmission du port)** et cliquez sur Next.Inscrivez les ressources que vous voulez pour faire la transmission du port traversante disponible. Le port de service doit être une prise de pression statique, mais vous pouvez recevoir le port par défaut sur le PC client assigné par l'assistant. Cliquez sur **Next** (Suivant).Visionnez votre résumé de configuration et cliquez sur Finish préalablement **> CORRECT > sauvegarde**.

Configuration

Résultats de la configuration SDM.

ausnml-3825-01

```
Building configuration...

Current configuration : 4343 bytes
!
! Last configuration change at 15:55:38 UTC Thu Jul 27
2006 by ausnml
! NVRAM config last updated at 21:30:03 UTC Wed Jul 26
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
!
aaa new-model
!
aaa authentication login default local
```

```
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 !---------------------- !--- cut for
brevity quit ! username ausnml privilege 15 password 7
15071F5A5D292421 username fallback privilege 15 password
7 08345818501A0A12 username austin privilege 15 secret 5
$1$3xFv$W0YUsKDx1adDc.cVQF2Ei0 username sales_user1
privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
username admin0321 privilege 15 secret 5
$1$FxzG$cQUJeUpBWgZ.scSzOt8Ro1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! ip route
0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http
authentication local ip http secure-server ip http
timeout-policy idle 600 life 86400 requests 100 !
control-plane ! line con 0 stopbits 1 line aux 0
stopbits 1 line vty 0 4 exec-timeout 40 0 privilege
level 15 password 7 071A351A170A1600 transport input
telnet ssh line vty 5 15 exec-timeout 40 0 password 7
001107505D580403 transport input telnet ssh ! scheduler
allocate 20000 1000 !--- the WebVPN Gateway webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint ausnml-3825-
01_Certificate inservice !--- the WebVPN Context webvpn
context webvpn title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all !---
resources available to the thin-client port-forward
"portforward_list_1" local-port 3002 remote-server
"172.22.1.20" remote-port 110 description "Pop3 Email"
local-port 3001 remote-server "172.22.1.30" remote-port
23 description "Router1" local-port 3000 remote-server
"172.22.1.50" remote-port 25 description "Email" local-
port 3003 remote-server "172.22.1.10" remote-port 22
description "Router2 SSH" !--- the group policy policy
group policy_1 port-forward "portforward_list_1"
default-group-policy policy_1 aaa authentication list
sdm_vpn_xauth_ml_2 gateway gateway_1 domain webvpn max-
users 2 inservice ! end
```

Vérifiez

Vérifiez votre configuration

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

1. Utilisez un ordinateur client pour accéder au webvpn gateway chez **https://gateway_ip_address.** Souvenez-vous pour inclure le nom de domaine de webvpn si vous créez de seuls contextes de webvpn. Par exemple, si vous avez créé un domaine appelé les ventes, entrez dans **https://gateway_ip_address/sales**.
2. Ouvrez une session et recevez le certificat offert par le webvpn gateway. **Application de début de** clic **Access**.
3. Affichages de l'écran d'Access d'une application. Vous pouvez accéder à une application avec le nombre de port local et votre adresse IP de bouclage locale. Par exemple, au telnet au routeur 1, entrez dans le **telnet 127.0.0.1 3001**. Le petit applet Java envoie ces informations au webvpn gateway, qui attache alors les deux fins de la session ensemble d'une mode sécurisée. Les connexions réussies peuvent faire augmenter les **octets** et des **octets dans les** colonnes.

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 voir l'utilisation des **commandes show** en détail, référez-vous à vérifier la configuration de webvpn.

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.

Des ordinateurs client doivent être chargés avec la version 1.4 ou ultérieures de Javas de SUN. Obtenez une copie de ce logiciel du téléchargement logiciel de Javas

Commandes utilisées pour dépanner

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

- **show webvpn ?** — Beaucoup de commandes **show** sont associées avec WebVPN. Ceux-ci peuvent être exécutés au CLI pour afficher des statistiques et d'autres informations. Afin de voir l'utilisation des **commandes show** en détail, référez-vous à vérifier la configuration de webvpn.
- **debug webvpn ?** — L'utilisation des commandes de **débogage** peut défavorablement affecter le routeur. Afin de voir l'utilisation des commandes de **débogage** plus en détail, référez-vous en utilisant des commandes de debug de webvpn.

Informations connexes

- Cisco IOS SSLVPN
- VPN SSL - WebVPN
- Webvpn Q&A de Cisco IOS
- Support et documentation techniques - Cisco Systems