Routeur IOS comme serveur Easy VPN utilisant l'exemple de configuration de Configuration Professional

Contenu

Introduction

Ce document décrit comment configurer un routeur de Cisco IOS® en tant que serveur d'Easy VPN (EzVPN) utilisant le Cisco Configuration Professional (Cisco CP) et le CLI. La caractéristique du serveur Easy VPN permet à un utilisateur final distant de communiquer en utilisant la sécurité IP (IPsec) avec n'importe quelle passerelle de réseau privé virtuel (VPN) Cisco IOS. Des stratégies IPsec centralement gérées sont « dirigées » vers le périphérique de client par le serveur, réduisant la configuration par l'utilisateur final.

Pour plus d'informations sur le serveur Easy VPN référez-vous à la section de serveur Easy VPN de la bibliothèque de guide de configuration de connectivité sécurisée, Cisco IOS version 12.4T.

Conditions préalables

Composants utilisés

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

- Routeur de Cisco 1841 avec la version du logiciel Cisco IOS 12.4(15T)
- Version 2.1 de Cisco CP

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.

Installez Cisco CP

Exécutez ces étapes afin d'installer Cisco CP :

1. Téléchargez Cisco CP V2.1 du centre logiciel Cisco (clients enregistrés seulement) et installez-le sur votre ordinateur local.La dernière version de Cisco CP peut être trouvée au site Web de Cisco CP.
2. Lancez Cisco CP de votre ordinateur local par le **début** > les **programmes** > le **Cisco Configuration Professional (CCP)** et choisissez la **Communauté** qui a le routeur que vous voulez configurer.
3. Afin de découvrir le périphérique que vous voulez configurer, mettre en valeur le routeur et le clic **les découvrent**.

Remarque: Pour les informations sur les modèles de routeur de Cisco et les releases IOS qui sont compatibles à Cisco CP v2.1, référez-vous à la section compatible de releases de Cisco IOS.

Remarque: Pour les informations sur les conditions requises PC qui dirigent Cisco CP v2.1, référez-vous à la section de configurations système requises.

Configuration de routeur pour diriger Cisco CP

Exécutez ces étapes de configuration afin de diriger Cisco CP sur un routeur de Cisco :

1. Connectez à votre routeur utilisant le telnet, SSH, ou par la console.Entrez le mode de configuration globale utilisant cette commande :`Router(config)#`**`enable`** `Router(config)#`
2. Si le HTTP et les HTTPS sont activés et configurés utiliser des numéros du port non standard, vous pouvez ignorer cette étape et simplement utiliser le numéro de port déjà configuré.Activez le serveur de HTTP ou HTTPS de routeur utilisant ces commandes de logiciel de Cisco IOS :`Router(config)#` **`ip http server`** `Router(config)#` **`ip http secure-server`** `Router(config)#` **`ip http authentication local`**
3. Créez un utilisateur avec le niveau de privilège 15 :`Router(config)#` **`username`** *`<username>`* **`privilege 15 password 0`** *`<password>`* **Remarque:** Remplacez le *<username>* et le *<password>* par le nom d'utilisateur et mot de passe que vous voulez configurer.
4. Configurez le SSH et le telnet pour le niveau 15 de procédure de connexion locale et de privilège.`Router(config)#` **`line vty 0 4`** `Router(config-line)#` **`privilege level 15`** `Router(config-line)#` **`login local`** `Router(config-line)#` **`transport input telnet`** `Router(config-line)#` **`transport input telnet ssh`** `Router(config-line)#` **`exit`**
5. (Facultatif) activez les gens du pays se connectant pour prendre en charge la fonction de surveillance de log :`Router(config)#` **`logging buffered 51200 warning`**

Conditions requises

Ce document suppose que le routeur de Cisco est complètement opérationnel et configuré pour

permettre à Cisco CP pour apporter des modifications de configuration.

Pour des informations complètes sur la façon commencer utilisant Cisco CP, référez-vous à obtenir commencé par le Cisco Configuration Professional.

Conventions

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

Configurez

Dans cette section, vous êtes présenté avec les informations pour configurer les paramètres de base pour un routeur dans un réseau.

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 :

Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

Cisco CP - Configuration de serveur Easy VPN

Exécutez ces étapes afin de configurer le routeur Cisco IOS en tant que serveur Easy VPN :

1. Choisissez **configurent > Sécurité > VPN > serveur Easy VPN > créent le serveur Easy VPN** et cliquent sur le **Launch Easy VPN Server Wizard** afin de configurer le routeur Cisco IOS en tant que serveur Easy VPN :
2. Cliquez sur Next afin de procéder à la configuration de **serveur Easy VPN**.
3. Dans la fenêtre en résultant, une **interface virtuelle** sera configurée comme partie de la configuration de serveur Easy VPN. Fournissez l'**adresse IP de l'interface de tunnel virtuelle** et choisissez également la **méthode d'authentification** utilisée pour authentifier les clients vpn. Ici, les **clés pré-partagées** est la méthode d'authentification utilisée. Cliquez sur Next :
4. Spécifiez l'**algorithme de chiffrement, l'algorithme d'authentification et la méthode d'échange de clés** à utiliser par ce routeur en étant en pourparlers avec le périphérique distant. Une stratégie IKE par défaut est présente sur le routeur qui peut être utilisé s'il y a lieu. Si vous voulez ajouter une nouvelle stratégie IKE, cliquez sur Add.
5. Fournissez l'**algorithme de chiffrement**, l'**algorithme d'authentification**, et la **méthode d'échange de clés** comme affiché ici, puis cliquez sur OK :
6. **La stratégie IKE par défaut** est utilisée dans cet exemple. En conséquence, choisissez la stratégie IKE par défaut et cliquez sur Next.
7. Dans la nouvelle fenêtre, les détails de **jeu de transformations** devraient être fournis. Le jeu de transformations (Transform Set) spécifie les algorithmes de **chiffrement** et d'**intégrité**

utilisés pour protéger les **données dans le tunnel VPN**. Cliquez sur Add pour fournir ces détails. Vous pouvez ajouter un certain nombre de jeux de transformations pendant que nécessaire quand vous cliquez sur Add et fournissez les détails.**Remarque: Le CP transfèrent le jeu de transformations** est présent par défaut sur le routeur une fois configuré utilisant **Cisco CP**.

8. Fournissez les détails de **jeu de transformations** (**algorithme de cryptage et d'authentification**) et cliquez sur OK.
9. **Le jeu de transformations par défaut** nommé **jeu de transformations de par défaut CP** est utilisé dans cet exemple. En conséquence, choisissez le jeu de transformations par défaut et cliquez sur Next.
10. Dans la nouvelle fenêtre, choisissez le serveur sur lequel on configurera les stratégies de groupe qui peuvent être les **gens du pays** ou le **RAYON** ou les **gens du pays et le RAYON**. Dans cet exemple, nous utilisons le **serveur local** pour configurer des stratégies de groupe. Choisissez les **gens du pays** et cliquez sur Next.
11. Choisissez le serveur à utiliser pour l'authentification de l'utilisateur dans cette nouvelle fenêtre qui peut être les **gens du pays seulement** ou le **RAYON** ou les **gens du pays seulement et le RAYON**. Dans cet exemple nous utilisons le **serveur local** pour configurer des identifiants utilisateurs pour l'authentification. Assurez-vous que la case à côté de l'**authentification de l'utilisateur d'enable** est cochée. Choisissez les **gens du pays seulement** et cliquez sur Next.
12. Cliquez sur Add pour créer une nouvelle stratégie de groupe et pour ajouter les utilisateurs distants dans ce groupe.
13. Dans la fenêtre de **stratégie de groupe d'ajouter**, fournissez le nom de groupe dans l'espace prévoient le **nom de ce groupe** (**Cisco** dans cet exemple) avec la **clé pré-partagée**, et les informations de **pool d'IP** (l'**adresse IP commençante** et **adresse IP de finir**) comme affiché et cliquent sur OK.**Remarque:** Vous pouvez créer un nouveau pool d'IP ou utiliser un pool d'IP existant si présent.
14. Choisissez maintenant la nouvelle **stratégie de groupe** créée avec le nom **Cisco** et cliquez sur alors la case à côté du du **configurer le temporisateur de veille** au besoin afin de configurer le **temporisateur de veille**. Cliquez sur **Next** (Suivant).
15. Enable **Cisco perçant un tunnel le Control Protocol** (cTCP) s'il y a lieu. Autrement, cliquez sur Next.
16. Examinez le **résumé de la configuration**. Cliquez sur **Finish** (Terminer).
17. Dans la **configuration de livraison à la** fenêtre de **routeur**, le clic **livrent** pour fournir la configuration au routeur. Vous pouvez cliquer sur en fonction la **sauvegarde pour classer** pour sauvegarder la configuration comme fichier sur le PC.
18. La fenêtre d'**état de la livraison de commande** affiche le statut de la livraison des commandes au routeur. Il apparaît comme **configuration fournie au routeur**. Cliquez sur **OK**.
19. Vous pouvez voir le serveur Easy VPN de création récente. Vous pouvez éditer le serveur existant en choisissant **éditez le serveur Easy VPN**. Ceci se termine la configuration de serveur Easy VPN sur le routeur Cisco IOS.

Configuration CLI

Configuration du routeur
Router#**show run** Building configuration... Current configuration : 2069 bytes *!* version 12.4 service timestamps debug datetime msec service timestamps log

```
datetime msec no service password-encryption hostname
Router boot-start-marker boot-end-marker no logging
buffered enable password cisco !---AAA enabled using aaa
newmodel command. Also AAA Authentication and
Authorization are enabled---! aaa new-model ! ! aaa
authentication login ciscocp_vpn_xauth_ml_1 local aaa
authorization network ciscocp_vpn_group_ml_1 local ! !
aaa session-id common ip cef ! ! ! ! ip domain name
cisco.com ! multilink bundle-name authenticated ! ! !---
Configuration for IKE policies. !--- Enables the IKE
policy configuration (config-isakmp) !--- command mode,
where you can specify the parameters that !--- are used
during an IKE negotiation. Encryption and Policy details
are hidden as the default values are chosen. crypto
isakmp policy 1 encr 3des authentication pre-share group
2 crypto isakmp keepalive 10 ! crypto isakmp client
configuration group cisco key cisco123 pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1 match
identity group cisco client authentication list
ciscocp_vpn_xauth_ml_1 isakmp authorization list
ciscocp_vpn_group_ml_1 client configuration address
respond virtual-template 1 ! ! !--- Configuration for
IPsec policies. !--- Enables the crypto transform
configuration mode, !--- where you can specify the
transform sets that are used !--- during an IPsec
negotiation. crypto ipsec transform-set ESP-3DES-SHA
esp-3des esp-sha-hmac ! crypto ipsec profile
CiscoCP_Profile1 set security-association idle-time
86400 set transform-set ESP-3DES-SHA set isakmp-profile
ciscocp-ike-profile-1 ! ! ! !--- RSA certificate
generated after you enable the !--- ip http secure-
server command. crypto pki trustpoint TP-self-signed-
1742995674 enrollment selfsigned subject-name cn=IOS-
Self-Signed-Certificate-1742995674 revocation-check none
rsakeypair TP-self-signed-1742995674 !--- Create a user
account named cisco123 with all privileges. username
cisco123 privilege 15 password 0 cisco123 archive log
config hidekeys ! ! !--- Interface configurations are
done as shown below---! interface Loopback0 ip address
10.10.10.10 255.255.255.0 ! interface FastEthernet0/0 ip
address 10.77.241.111 255.255.255.192 duplex auto speed
auto ! interface Virtual-Template1 type tunnel ip
unnumbered Loopback0 tunnel mode ipsec ipv4 tunnel
protection ipsec profile CiscoCP_Profile1 ! !--- VPN
pool named SDM_POOL_1 has been defined in the below
command---! ip local pool SDM_POOL_1 192.168.1.1
192.168.1.254 !--- This is where the commands to enable
HTTP and HTTPS are configured. ip http server ip http
authentication local ip http secure-server ! ! ! !
control-plane ! line con 0 line aux 0 !--- Telnet
enabled with password as cisco. line vty 0 4 password
cisco transport input all scheduler allocate 20000 1000
! ! ! ! end
```

Vérifiez

Serveur Easy VPN - commandes show

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

- **show crypto isakmp sa** — Affiche toutes les SA IKE en cours au niveau d'un homologue.`Router#show crypto isakmp sa IPv4 Crypto ISAKMP SA dst src state conn-id slot status 10.77.241.111 172.16.1.1 QM_IDLE 1003 0 ACTIVE`
- **show crypto ipsec sa** — Affiche toutes les SA IPsec en cours au niveau d'un homologue.`Router#show crypto ipsec sa interface: Virtual-Access2 Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111 protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0) current_peer 172.16.1.1 port 1086 PERMIT, flags={origin_is_acl,} #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28 #pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 2 local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0 current outbound spi: 0x186C05EF(409732591) inbound esp sas: spi: 0x42FC8173(1123844467) transform: esp-3des esp-sha-hmac`

Dépannez

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** .

Remarque: Reportez-vous à Informations importantes sur les commandes de débogage avant d'émettre des commandes **debug**.

Informations connexes

- Négociation IPSec/Protocoles IKE
- Guide de démarrage rapide de Cisco Configuration Professional
- Page d'assistance de produit Cisco - Routeurs
- Support et documentation techniques - Cisco Systems