Configuration Professional : Site à site IPsec VPN entre l'exemple de configuration de deux Routeurs IOS

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Configuration
Diagramme du réseau
Routeur une configuration de Cisco CP
Configuration du routeur B Cisco CP
Configuration du routeur B CLI
Vérifiez
Ordres de routeur show IOS
Dépannez
Informations connexes

Introduction

Ce document fournit une configuration d'échantillon pour le tunnel d'IPsec d'entre réseaux locaux (site à site) entre deux Routeurs de Cisco IOS® utilisant le Cisco Configuration Professional (Cisco CP). Des routes statiques sont utilisées à des fins de simplicité.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à cette exigence avant que vous tentiez cette configuration :

- La connectivité IP de bout en bout doit être établie avant de commencer cette configuration.

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 2.5 de Cisco CP

Note: Référez-vous à la configuration de base du routeur utilisant le Cisco Configuration Professional afin de permettre le routeur à configurer par 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.

Conventions

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

Configuration

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Note: 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 utilisées dans un environnement de laboratoire.

- Routeur une configuration de Cisco CP
- Configuration du routeur B Cisco CP
- Configuration du routeur B CLI

Routeur une configuration de Cisco CP

Exécutez ces étapes afin de configurer le tunnel VPN de site à site sur le routeur Cisco IOS :

1. Choisissez **configurent > Sécurité > VPN > site à site VPN**, et cliquent sur la case d'option à côté de **créent un site à site VPN**. **Lancement de** clic la **tâche sélectionnée**.
2. Choisissez l'**assistant pas à pas** afin de procéder à la configuration, et cliquez sur Next.
3. Dans la prochaine fenêtre, fournissez les informations de connexion VPN dans les espaces respectifs. Choisissez l'interface du tunnel VPN du menu déroulant. Ici, **FastEthernet0** est choisi. Dans la section **Peer Identity**, choisissez **Peer with static IP address** et fournissez l'adresse IP de l'homologue distant. Puis, fournissez les clés pré-partagées (*cisco123* dans cet exemple) dans la section d'authentification. Pour finir, cliquez sur Next.
4. Cliquez sur Add afin d'ajouter les propositions d'IKE qui spécifient l'algorithme de chiffrement, l'algorithme d'authentification, et la méthode d'échange de clés.
5. Fournissez l'algorithme de chiffrement, l'algorithme d'authentification, et la méthode d'échange de clés, et puis cliquez sur OK. L'algorithme de chiffrement, l'algorithme d'authentification, et les valeurs de méthode d'échange de clés devraient s'assortir avec les données à fournir dans le routeur B.
6. Cliquez sur **Next** (Suivant).
7. Dans cette nouvelle fenêtre, les détails de jeu de transformations sont 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 afin de fournir ces détails. Vous pouvez ajouter un certain nombre de jeux de transformations comme nécessaire à l'aide de cette méthode.
8. Fournissez les détails de jeu de transformations (intégrité et algorithmes de chiffrement), et cliquez sur OK.
9. Choisissez le **jeu de transformations** requis à utiliser du menu déroulant, et cliquez sur Next.
10. Dans la fenêtre suivante, fournissez les détails au sujet du trafic à protéger par le tunnel VPN. Fournissez les **réseaux sources et de destination** du trafic à protéger de sorte que le trafic entre les réseaux sources et de destination spécifiés soit protégé. Dans cet exemple, le réseau de source est *10.10.10.0* et le réseau de destination est *10.20.10.0*. Cliquez sur **Next** (Suivant).
11. Cliquez sur Finish dans la prochaine fenêtre pour se terminer la configuration sur le routeur A.

Configuration du routeur B Cisco CP

Exécutez ces étapes afin de configurer le tunnel VPN de site à site sur le routeur Cisco IOS (routeur B) :

1. Choisissez **configurent > Sécurité > VPN > site à site VPN**, et cliquent sur la case d'option à côté de **créent un site à site VPN**. **Lancement de** clic la **tâche sélectionnée**.
2. Choisissez l'**assistant pas à pas** afin de procéder à la configuration, et cliquez sur Next.
3. Dans la prochaine fenêtre, fournissez les informations de connexion VPN dans les espaces respectifs. Choisissez l'interface du tunnel VPN du menu déroulant. Ici, **FastEthernet0** est choisi. Dans la section **Peer Identity**, choisissez **Peer with static IP address** et fournissez l'adresse IP de l'homologue distant. Puis, fournissez les clés pré-partagées (*cisco123* dans cet exemple) dans la section d'authentification. Pour finir, cliquez sur Next.
4. Cliquez sur Add afin d'ajouter les propositions d'IKE qui spécifient l'algorithme de chiffrement, l'algorithme d'authentification, et la méthode d'échange de clés.
5. Fournissez l'algorithme de chiffrement, l'algorithme d'authentification, et la méthode d'échange de clés, et puis cliquez sur OK. L'algorithme de chiffrement, l'algorithme d'authentification, et les valeurs de méthode d'échange de clés devraient s'assortir avec les données fournies dans le routeur A.
6. Cliquez sur **Next** (Suivant).
7. Dans cette nouvelle fenêtre, les détails de jeu de transformations sont 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 afin de fournir ces détails. Vous pouvez ajouter un certain nombre de jeux de transformations comme nécessaire à l'aide de cette méthode.
8. Fournissez les détails de jeu de transformations (intégrité et algorithmes de chiffrement), et cliquez sur OK.
9. Choisissez le **jeu de transformations** requis à utiliser du menu déroulant, et cliquez sur Next.
10. Dans la fenêtre suivante, fournissez les détails au sujet du trafic à protéger par le tunnel VPN. Fournissez les **réseaux sources et de destination** du trafic à protéger de sorte que le trafic entre les réseaux sources et de destination spécifiés soit protégé. Dans cet exemple, le réseau source est 10.20.10.0 et le réseau de destination est 10.10.10.0. Cliquez sur **Next** (Suivant).

11. Cette fenêtre affiche le résumé de la configuration du VPN de site à site. Vérifiez la **connectivité VPN de test après avoir configuré la** case à cocher si vous voulez tester la connectivité VPN. Ici, la case est cochée car la connectivité doit être vérifiée. Cliquez sur **Finish** (Terminer).
12. **Début de** clic afin de vérifier la connectivité VPN.
13. Dans la prochaine fenêtre, le résultat du test de connectivité VPN est fourni. Ici, vous pouvez voir si le tunnel est activé ou désactivé (**Up ou Down**). En cet exemple de configuration, le tunnel est « vers le haut de », suivant les indications de vert.Ceci se termine la configuration sur le RouterB de Cisco IOS et prouve que le tunnel est.

Configuration du routeur B CLI

routeur B

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- 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 2
 authentication pre-share

!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1
!
!
!--- 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 Router-
IPSEC esp-des esp-sha-hmac
!

!--- Indicates that IKE is used to establish !--- the
IPsec Security Association for protecting the !---
traffic specified by this crypto map entry. crypto map
SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1

!--- Sets the IP address of the remote end. set peer
172.16.1.1

!--- Configures IPsec to use the transform-set !---
"Router-IPSEC" defined earlier in this configuration.
set transform-set Router-IPSEC

!--- Specifies the interesting traffic to be encrypted.
match address 100
!
!
!
!--- Configures the interface to use the !--- crypto map
"SDM_CMAP_1" for IPsec. interface FastEthernet0 ip
address 172.17.1.1 255.255.255.0 duplex auto speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet1
 ip address 10.20.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface
FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!
!--- Configure the access-lists and map them to the
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
!
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
```

```
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

Vérifiez

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

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** .

- Ordres de **routeur show** IOS

Ordres de routeur show IOS

- **show crypto isakmp sa** — Affiche toutes les SA IKE en cours au niveau d'un homologue.

```
RouterB# show crypto isakmp sa

dst             src             state          conn-id slot status
172.17.1.1      172.16.1.1      QM_IDLE              3    0 ACTIVE
```

- **show crypto ipsec sa** — Affiche toutes les SA IPsec en cours au niveau d'un homologue.

```
RouterB# show crypto ipsec sa
interface: FastEthernet0
    Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #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 0

     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)

     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
```

```
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
    sa timing: remaining key lifetime (k/sec): (4578719/3004)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0xB7C1948E(3082917006)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
    sa timing: remaining key lifetime (k/sec): (4578719/3002)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

  outbound ah sas:

  outbound pcp sas:
```

- **active de connexions de show crypto engine** — Connexions en cours et informations d'expositions sur les paquets chiffrés et déchiffrés.

```
RouterB#show crypto engine connections active

   ID Interface        IP-Address    State  Algorithm           Encrypt  Decrypt
    3 FastEthernet0    172.17.1.1    set    HMAC_SHA+DES_56_CB        0        0
 2001 FastEthernet0    172.17.1.1    set    DES+SHA                   0       59
 2002 FastEthernet0    172.17.1.1    set    DES+SHA                  59        0
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

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** .

Note: Référez-vous aux informations importantes sur des commandes de debug et le dépannage de sécurité IP : Comprenant et utilisant des commandes de débogage avant que vous utilisiez des commandes de **débogage**.

- **debug crypto ipsec 7** — Affiche les négociations IPsec de la phase 2.**debug crypto isakmp 7** — Affiche les négociations ISAKMP de la phase 1.
- **debug crypto ipsec** — Affiche les négociations IPsec de la phase 2.**debug crypto isakmp** — affiche les négociations ISAKMP de la phase 1.

Informations connexes

- Guide de démarrage rapide de Cisco Configuration Professional
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems