Configuration IPSec IOS à IOS à l'aide du cryptage AES

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Configurez
Configurations
Vérifiez
Dépannez
Dépannage des commandes
Informations connexes

Introduction

Ce document fournit un exemple de configuration pour un tunnel IPsec IOS-à-IOS utilisant le chiffrement d'Advanced Encryption Standard (AES).

Conditions préalables

Conditions requises

La prise en charge du chiffrement AES a été introduite dans le Cisco IOS® 12.2(13)T.

Composants utilisés

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

- Logiciel Cisco IOS version 12.3(10)
- Cisco 1721 Routeurs

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 aux Conventions relatives aux conseils techniques Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Configurations

Ce document utilise les configurations indiquées ici.

- Routeur 1721-A
- Routeur 1721-B

Routeur 1721-A

```
R-1721-A#show run Building configuration... Current
configuration : 1706 bytes ! ! Last configuration change
at 00:46:32 UTC Fri Sep 10 2004 ! NVRAM config last
updated at 00:45:48 UTC Fri Sep 10 2004 ! version 12.3
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname R-1721-A ! boot-start-marker boot-
end-marker ! ! memory-size iomem 15 mmi polling-interval
60 no mmi auto-configure no mmi pvc mmi snmp-timeout 180
no aaa new-model ip subnet-zero ip cef ! ! ! ip audit po
max-events 100 no ip domain lookup no ftp-server write-
enable ! ! ! ! !--- Define Internet Key Exchange (IKE)
policy. crypto isakmp policy 10 !--- Specify the 256-bit
AES as the !--- encryption algorithm within an IKE
policy. encr aes 256 !--- Specify that pre-shared key
authentication is used. authentication pre-share !---
Specify the shared secret. crypto isakmp key cisco123
address 10.48.66.146 ! ! !--- Define the IPSec transform
set. crypto ipsec transform-set aesset esp-aes 256 esp-
sha-hmac ! !--- Define crypto map entry name "aesmap"
that will use !--- IKE to establish the security
associations (SA). crypto map aesmap 10 ipsec-isakmp !--
- Specify remote IPSec peer. set peer 10.48.66.146 !---
Specify which transform sets !--- are allowed for this
crypto map entry. set transform-set aesset !--- Name the
access list that determines which traffic !--- should be
protected by IPSec. match address acl_vpn ! ! !
interface ATM0 no ip address shutdown no atm ilmi-
keepalive dsl equipment-type CPE dsl operating-mode
GSHDSL symmetric annex A dsl linerate AUTO ! interface
Ethernet0 ip address 192.168.100.1 255.255.255.0 ip nat
inside half-duplex ! interface FastEthernet0 ip address
10.48.66.147 255.255.254.0 ip nat outside speed auto !--
- Apply crypto map to the interface. crypto map aesmap !
ip nat inside source list acl_nat interface
FastEthernet0 overload ip classless ip route 0.0.0.0
0.0.0.0 10.48.66.1 ip route 192.168.200.0 255.255.255.0
FastEthernet0 no ip http server no ip http secure-server
```

```
! ip access-list extended acl_nat !--- Exclude protected
traffic from being NAT'ed. deny ip 192.168.100.0
0.0.0.255 192.168.200.0 0.0.0.255 permit ip
192.168.100.0 0.0.0.255 any !--- Access list that
defines traffic protected by IPSec. ip access-list
extended acl_vpn permit ip 192.168.100.0 0.0.0.255
192.168.200.0 0.0.0.255 ! ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 ! end R-1721-A#
```

Routeur 1721-B

```
R-1721-B#show run Building configuration... Current
configuration : 1492 bytes ! ! Last configuration change
at 14:11:41 UTC Wed Sep 8 2004 ! version 12.3 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
R-1721-B ! boot-start-marker boot-end-marker ! ! memory-
size iomem 15 mmi polling-interval 60 no mmi auto-
configure no mmi pvc mmi snmp-timeout 180 no aaa new-
model ip subnet-zero ip cef ! ! ! ip audit po max-events
100 no ip domain lookup no ftp-server write-enable ! ! !
! ! !--- Define IKE policy. crypto isakmp policy 10 !---
Specify the 256-bit AES as the !--- encryption algorithm
within an IKE policy. encr aes 256 !--- Specify that
pre-shared key authentication is used. authentication
pre-share !--- Specify the shared secret. crypto isakmp
key cisco123 address 10.48.66.147 ! ! !--- Define the
IPSec transform set. crypto ipsec transform-set aesset
esp-aes 256 esp-sha-hmac ! !--- Define crypto map entry
name "aesmap" that uses !--- IKE to establish the SA.
crypto map aesmap 10 ipsec-isakmp !--- Specify remote
IPSec peer. set peer 10.48.66.147 !--- Specify which
transform sets !--- are allowed for this crypto map
entry. set transform-set aesset !--- Name the access
list that determines which traffic !--- should be
protected by IPSec. match address acl_vpn ! ! !
interface Ethernet0 ip address 192.168.200.1
255.255.255.0 ip nat inside half-duplex ! interface
FastEthernet0 ip address 10.48.66.146 255.255.254.0 ip
nat outside speed auto !--- Apply crypto map to the
interface. crypto map aesmap ! ip nat inside source list
acl_nat interface FastEthernet0 overload ip classless ip
route 0.0.0.0 0.0.0.0 10.48.66.1 ip route 192.168.100.0
255.255.255.0 FastEthernet0 no ip http server no ip http
secure-server ! ip access-list extended acl_nat !---
Exclude protected traffic from being NAT'ed. deny ip
192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255 permit
ip 192.168.200.0 0.0.0.255 any !--- Access list that
defines traffic protected by IPSec. ip access-list
extended acl_vpn permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255 ! ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 ! end R-1721-B#
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto isakmp sa** — Affiche l'état pour Protocole ISAKMP (Internet Security Association and Key Management Protocol) SA.
- **show crypto ipsec sa** — Affiche les statistiques sur les tunnels actifs.
- **active de connexions de show crypto engine** — Affiche le total chiffre/déchiffre par SA.

Dépannez

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

Dépannage des commandes

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

- **debug crypto ipsec** — Affiche des événements IPsec.
- **debug crypto isakmp**—Affichage de messages d'événements IKE.
- **debug crypto engine** — Affiche des informations du moteur de chiffrement.

Vous trouverez les informations supplémentaires pour dépanner IPSec à la section Dépannage de sécurité IP - Présentation et utilisation des commandes de débogage.

Informations connexes

- Versions du logiciel Cisco IOS 12.2T - Norme AES (Advanced Encryption Standard)
- Sécurité des réseaux de configuration d'IPSec
- Page d'assistance IPsec
- Support technique - Cisco Systems