AES 暗号化を使用した IOS-IOS 間 IPSec の設定

目次

はじめに

この文書では、Advanced Encryption Standard（AES）暗号化を使用した、IOS-IOS 間 IPSec トンネルの設定例を説明します。

前提条件

要件

AES 暗号化サポートは Cisco IOS® 12.2(13)T で導入されました。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 12.3(10)
- Cisco 1721 ルータ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定

このドキュメントでは、次に示す設定を使用しています。

- ルータ 1721-A
- ルータ 1721-B

ルータ 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#
```

ルータ 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#
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- show crypto isakmp sa：Internet Security Association and Key Management Protocol（ISAKMP）SA の状態を表示します。
- show crypto ipsec sa：アクティブなトンネルの統計情報を表示します。
- show crypto engine connections active：SA ごとの合計の暗号化/復号化を表示します。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティングのためのコマンド

注: debug コマンドを使用する前に、『debug コマンドに関する重要な情報』を参照してください。

- **debug crypto ipsec**：IPSec イベントを表示します。
- **debug crypto isakmp**：IKE イベントに関するメッセージを表示します。
- **debug crypto engine**：暗号化エンジンからの情報を表示します。

IPSec のトラブルシューティングの詳細については、「IP Security のトラブルシューティング - debug コマンドの理解と使用」を参照してください。

関連情報

- Cisco IOS ソフトウェア リリース 12.2T ： Advanced Encryption Standard（AES）
- IPsec ネットワーク セキュリティの設定
- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems