AES 暗号化を使用した IOS-IOS 間 IPSec の設定

内容

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暗号化のサポートは、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いています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメントの表記法の詳細は、「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

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザのみ）。

コンフィギュレーション

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

```
<#root>

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 associatio


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

<#root>

```
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

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

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。

ルータ 1721-A

```
<#root>

R-1721-A#

show crypto isakmp sa


dst             src             state          conn-id slot
10.48.66.147    10.48.66.146    QM_IDLE              1    0
```

ルータ 1721-B

```
<#root>

R-1721-B#

show crypto isakmp sa


dst             src             state          conn-id slot
10.48.66.147    10.48.66.146    QM_IDLE              1    0
```

- 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。

ルータ 1721-A

```
<#root>

R-1721-A#

show crypto ipsec sa


interface: FastEthernet0
    Crypto map tag: aesmap, local addr. 10.48.66.147

   protected vrf:


local  ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)

   current_peer: 10.48.66.146:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 30, #pkts encrypt: 30, #pkts digest 30
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify 30
    #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.: 10.48.66.147, remote crypto endpt.: 10.48.66.146

     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 2EB0BA1A

     inbound esp sas:
      spi: 0xFECA28BC(4274661564)


transform: esp-256-aes esp-sha-hmac ,

        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: aesmap
        sa timing: remaining key lifetime (k/sec): (4554237/2895)
        IV size: 16 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x2EB0BA1A(783333914)


transform: esp-256-aes esp-sha-hmac ,

        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: aesmap
        sa timing: remaining key lifetime (k/sec): (4554237/2894)
        IV size: 16 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
R-1721-A#
```

ルータ 1721-B

```
<#root>

R-1721-B#

show crypto ipsec sa


interface: FastEthernet0
    Crypto map tag: aesmap, local addr. 10.48.66.146

   protected vrf:
```

```
local  ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)

   current_peer: 10.48.66.147:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 30, #pkts encrypt: 30, #pkts digest 30
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify 30
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 5, #recv errors 0



local crypto endpt.: 10.48.66.146, remote crypto endpt.: 10.48.66.147

     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: FECA28BC

     inbound esp sas:
      spi: 0x2EB0BA1A(783333914)


transform: esp-256-aes esp-sha-hmac ,

        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: aesmap
        sa timing: remaining key lifetime (k/sec): (4583188/2762)
        IV size: 16 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xFECA28BC(4274661564)


transform: esp-256-aes esp-sha-hmac ,

        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: aesmap
        sa timing: remaining key lifetime (k/sec): (4583188/2761)
        IV size: 16 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
R-1721-B#
```

- show crypto engine connections active：SA ごとの暗号化と復号化の総計を表示します。

ルータ 1721-A

```
<#root>

R-1721-A#

show crypto engine connections active



  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
   1 FastEthernet0   10.48.66.147    set    HMAC_SHA+AES_256_C        0        0
2000 FastEthernet0   10.48.66.147    set    HMAC_SHA+AES_256_C        0       30
2001 FastEthernet0   10.48.66.147    set    HMAC_SHA+AES_256_C       30        0
```

ルータ 1721-B

```
<#root>

R-1721-B#

show crypto engine connections active


  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
   1 FastEthernet0   10.48.66.146    set    HMAC_SHA+AES_256_C        0        0
2000 FastEthernet0   10.48.66.146    set    HMAC_SHA+AES_256_C        0       30
2001 FastEthernet0   10.48.66.146    set    HMAC_SHA+AES_256_C       30        0
```

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

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に関する詳細については、IP セキュリティのトラブルシューティング：デバッグ コマンドの詳細と使用法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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。