

使用AES加密配置IOS到IOS 的IPSec

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

简介

本文提供一个使用高级加密标准(AES)加密的IOS到IOS IPSec隧道的配置示例。

先决条件

要求

AES 加密支持已在 Cisco IOS® 12.2(13)T 中引入。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS 软件版本 12.3(10)
- Cisco 1721 路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要查找本文档所用命令的其他信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

配置

本文档使用此处所示的配置。

- [路由器 1721-A](#)
- [路由器 1721-B](#)

路由器 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 aasset 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 aasset  
!--- 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#

路由器 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 aasset 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 aasset
```

```

!--- 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#

```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 **show** 命令，使用此工具可以查看对 **show** 命令输出的分析。

- **show crypto isakmp sa** -显示Internet 安全连接和密钥管理协议 (ISAKMP) SA的状态。
- **show crypto ipsec sa** - 显示有关活动隧道的统计数据。
- **show crypto engine connections active** - 按 SA 显示总加密/解密。

故障排除

本部分提供的信息可用于对配置进行故障排除。

[故障排除命令](#)

注意： 在发出 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- `debug crypto ipsec` — 显示 IPsec 事件。
- `debug crypto isakmp` — 显示关于 IKE 事件的消息。
- `debug crypto engine` - 显示来自加密引擎的信息。

有关 IPsec 故障排除的其他信息，请参阅 [IP 安全故障排除 - 了解和使用 debug 命令](#)。

[相关信息](#)

- [Cisco IOS 软件版本 12.2T - 高级加密标准 \(AES\)](#)
- [配置 IPsec 网络安全](#)
- [IPsec 支持页面](#)
- [技术支持 - Cisco Systems](#)