

Configuring IOS-to-IOS IPSec Using AES Encryption

Document ID: 43069

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Configurations

Verify

Troubleshoot

Troubleshooting Commands

[NetPro Discussion Forums – Featured Conversations](#)

Related Information

Introduction

This document provides a sample configuration for an IOS-to-IOS IPSec tunnel using Advanced Encryption Standard (AES) encryption.

Prerequisites

Requirements

AES encryption support has been introduced in Cisco IOS® 12.2(13)T.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 12.3(10)
- Cisco 1721 routers

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup


```

!--- 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#
```

Router 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#
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

- **show crypto isakmp sa** Displays the state for the Internet Security Association and Key Management Protocol (ISAKMP) SA.

| Router 1721-A | | | | | |
|--------------------------------|--------------|---------|---------|------|--|
| 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 | |

| Router 1721-B | | | | | |
|--------------------------------|--------------|---------|---------|------|--|
| 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** Displays the statistics on the active tunnels.

| Router 1721-A |
|--|
| 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 pcg 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 pcg sas:
```

```
R-1721-A#
```

Router 1721-B

```
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** Displays the total encrypts/decrypts per SA.

| Router 1721-A | | | | | | |
|--|---------------|--------------|-------|--------------------|---------|---------|
| 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 |

| Router 1721-B | | | | | | |
|--|---------------|--------------|-------|--------------------|---------|---------|
| 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 |

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

- **debug crypto ipsec** Displays IPsec events.
- **debug crypto isakmp** Displays messages about IKE events.
- **debug crypto engine** Displays information from the crypto engine.

Additional information on troubleshooting IPsec can be found at IP Security Troubleshooting – Understanding and Using debug commands.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

| |
|---|
| NetPro Discussion Forums – Featured Conversations for VPN |
| Service Providers: VPN Service Architectures |
| Service Providers: Network Management |
| Virtual Private Networks: General |

Related Information

- [Cisco IOS Software Releases 12.2T – Advanced Encryption Standard \(AES\)](#)
- [Configuring IPSec Network Security](#)
- [IPSec Support Page](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Feb 02, 2006

Document ID: 43069
