Configuration Professional: Site–to–Site IPsec VPN Between Two IOS Routers Configuration Example

Document ID: 113337

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configuration
Network Diagram
Router A Cisco CP Configuration
Router B Cisco CP Configuration
Router B CLI Configuration
Verify
IOS Router – show Commands
Troubleshoot
Related Information

Introduction

This document provides a sample configuration for the LAN–to–LAN (Site–to–Site) IPsec tunnel between two Cisco IOS® Routers using Cisco Configuration Professional (Cisco CP). Static routes are used for simplicity.

Prerequisites

Requirements

Make sure that you meet this requirement before you attempt this configuration:

• End–to–End IP connectivity must be established before starting this configuration.

Components Used

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

• Cisco 1841 Router with Cisco IOS Software Release 12.4(15T)
• Cisco CP version 2.5

Note: Refer to Basic Router Configuration Using Cisco Configuration Professional in order to allow the router to be configured by Cisco CP.

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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configuration

Network Diagram

This document uses this network setup:

![Network Diagram](image)

Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses, which have been used in a lab environment.

- Router A Cisco CP Configuration
- Router B Cisco CP Configuration
- Router B CLI Configuration

Router A Cisco CP Configuration

Perform these steps in order to configure Site-to-Site VPN Tunnel on the Cisco IOS Router:

1. Choose Configure > Security > VPN > Site-to-Site VPN, and click the radio button next to Create a Site-to-Site VPN. Click Launch the selected task.
Choose **Step by step wizard** in order to proceed with the configuration, and click **Next**.
In the next window, provide the VPN Connection Information in the respective spaces. Choose the interface of the VPN Tunnel from the drop-down menu. Here, FastEthernet0 is chosen. In the Peer Identity section, choose Peer with static IP address and provide the remote peer IP address. Then, provide the Pre-shared Keys (cisco123 in this example) in the Authentication section. Lastly, click Next.
4. Click **Add** in order to add IKE proposals which specify the Encryption Algorithm, Authentication Algorithm, and the Key Exchange Method.

5. Provide the Encryption Algorithm, Authentication Algorithm, and Key Exchange method, and then click **OK**. The Encryption Algorithm, Authentication Algorithm, and the Key Exchange method values should match with the data to be provided in the Router B.

6. Click **Next**.
In this new window, the Transform Set details are provided. The Transform Set specifies the Encryption and Authentication algorithms used to protect Data in VPN Tunnel. Click **Add** in order to provide these details. You can add any number of Transform Sets as needed by using this method.

7. In this new window, the Transform Set details are provided. The Transform Set specifies the Encryption and Authentication algorithms used to protect Data in VPN Tunnel. Click **Add** in order to provide these details. You can add any number of Transform Sets as needed by using this method.

8. Provide the Transform Set details (Integrity and Encryption Algorithms), and click **OK**.
9. Choose the required **Transform Set** to be used from the drop-down menu, and click **Next**.

10. In the following window, provide the details about the Traffic to be protected through the VPN Tunnel. Provide the Source and Destination Networks of the traffic to be protected so that the traffic between the specified source and destination networks are protected. In this example, the Source network is **10.10.10.0** and the Destination network is **10.20.10.0**. Click **Next**.
11. Click **Finish** in the next window to complete the configuration on Router A.

### Router B Cisco CP Configuration

Perform these steps in order to configure Site-to-Site VPN Tunnel on the Cisco IOS Router (Router B):

1. Choose **Configure > Security > VPN > Site-to-Site VPN**, and click the radio button next to **Create a Site-to-Site VPN**. Click **Launch the selected task**.
Choose Step by step wizard in order to proceed with the configuration, and click Next.
3. In the next window, provide the VPN Connection Information in the respective spaces. Choose the interface of the VPN Tunnel from the drop-down menu. Here, FastEthernet0 is chosen. In the Peer Identity section, choose Peer with static IP address and provide the remote peer IP address. Then, provide the Pre-shared Keys (cisco123 in this example) in the Authentication section. Lastly, click Next.
4. Click **Add** in order to add IKE proposals which specify the Encryption Algorithm, Authentication Algorithm, and the Key Exchange Method.

5. Provide the Encryption Algorithm, Authentication Algorithm, and Key Exchange method, and then click **OK**. The Encryption Algorithm, Authentication Algorithm, and the Key Exchange method values should match with the data provided in the Router A.

6. Click **Next**.
7. In this new window, the Transform Set details are provided. The Transform Set specifies the Encryption and Authentication algorithms used to protect Data in VPN Tunnel. Click **Add** in order to provide these details. You can add any number of Transform Sets as needed by using this method.

8. Provide the Transform Set details (Integrity and Encryption Algorithms), and click **OK**.
9. Choose the required **Transform Set** to be used from the drop-down menu, and click **Next**.

10. In the following window, provide the details about the Traffic to be protected through the VPN Tunnel. Provide the Source and Destination Networks of the traffic to be protected so that the traffic between the specified source and destination networks are protected. In this example, the Source network is 10.20.10.0 and the Destination network is 10.10.10.0. Click **Next**.
11. This window shows the summary of the Site–to–Site VPN configuration. Check the Test VPN Connectivity after configuring checkbox if you want to test the VPN connectivity. Here, the box is checked as the connectivity needs to be checked. Click Finish.

12. Click Start in order to check the VPN connectivity.
In the next window, the result of the VPN connectivity Test is provided. Here, you can see if the tunnel is Up or Down. In this example configuration, the Tunnel is "Up", as shown in green.
This completes the configuration on the Cisco IOS RouterB and shows that the tunnel is up.

**Router B CLI Configuration**

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7 1511021F07257A767B
no aaa new-model
ip subnet-zero
```
ip cef
ip ips po max-events 100
no ftp-server write-enable

!--- Configuration for IKE policies.
!--- Enables the IKE policy configuration (config-isakmp)
!--- command mode, where you can specify the parameters that
!--- are used during an IKE negotiation. Encryption and Policy details are hidden
!--- as the default values are chosen.

crypto isakmp policy 2
  authentication pre-share

!--- Specifies the pre-shared key "cisco123" which should
!--- be identical at both peers. This is a global
!--- configuration mode command.

crypto isakmp key cisco123 address 172.16.1.1

!--- Configuration for IPsec policies.
!--- Enables the crypto transform configuration mode,
!--- where you can specify the transform sets that are used
!--- during an IPsec negotiation.

crypto ipsec transform-set Router-IPSEC esp-des esp-sha-hmac

!--- Indicates that IKE is used to establish
!--- the IPsec Security Association for protecting the
!--- traffic specified by this crypto map entry.

crypto map SDM_CMAP_1 1 ipsec-isakmp
description Tunnel to172.16.1.1

!--- Sets the IP address of the remote end.

  set peer 172.16.1.1

!--- Configures IPsec to use the transform-set
!--- "Router-IPSEC" defined earlier in this configuration.

  set transform-set Router-IPSEC

!--- Specifies the interesting traffic to be encrypted.

  match address 100

! !

!--- Configures the interface to use the
!--- crypto map "SDM_CMAP_1" for IPsec.
interface FastEthernet0
  ip address 172.17.1.1 255.255.255.0
duplex auto
  speed auto
  crypto map SDM_CMAP_1
!
interface FastEthernet1
  ip address 10.20.10.2 255.255.255.0
duplex auto
  speed auto
!
interface FastEthernet2
  no ip address
!
interface Vlan1
  ip address 10.77.241.109 255.255.255.192
  !
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!
!  Configure the access-lists and map them to the Crypto map configured.

access-list 100 remark SDM_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
!
!
!  This ACL 110 identifies the traffic flows using route map

access-list 110 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
  match ip address 110
!
control-plane
!
!
line con 0
  login local
line aux 0
line vty 0 4
  privilege level 15
  login local
  transport input telnet ssh
!
end

Verify

Use this section to confirm that your configuration works properly.
The Output Interpreter Tool (registered customers only) (OIT) supports certain `show` commands. Use the OIT to view an analysis of `show` command output.

- **IOS Router – show Commands**

**IOS Router – show Commands**

- `show crypto isakmp sa` Shows all current IKE SAs at a peer.

  RouterB# `show crypto isakmp sa`
  
<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.17.1.1</td>
<td>172.16.1.1</td>
<td>QM_IDLE</td>
<td>3</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

- `show crypto ipsec sa` Shows all current IPsec SAs at a peer.

  RouterB# `show crypto ipsec sa`
  
  interface: FastEthernet0
  
  Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1
  
  protected vrf: (none)
  
  local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  
  remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  
  current_peer 172.16.1.1 port 500
  
  PERMIT, flags={origin_is_acl,}
  
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
  
  #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
  
  #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.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
  
  path mtu 1500, ip mtu 1500
  
  current outbound spi: 0xB7C1948E(3082917006)
  
  inbound esp sas:
  
  spi: 0x434C4A7F(1129073279)
  
  transform: esp-des esp-sha-hmac ,
  
  in use settings ={Tunnel, }
  
  conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
  
  sa timing: remaining key lifetime (k/sec): (4578719/3004)
  
  IV size: 8 bytes
  
  replay detection support: Y
  
  Status: ACTIVE
  
  inbound ah sas:
  
  inbound pcp sas:
  
  outbound esp sas:
  
  spi: 0xB7C1948E(3082917006)
  
  transform: esp-des esp-sha-hmac ,
  
  in use settings ={Tunnel, }
  
  conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
  
  sa timing: remaining key lifetime (k/sec): (4578719/3002)
  
  IV size: 8 bytes
  
  replay detection support: Y
  
  Status: ACTIVE
  
  outbound ah sas:
  
  outbound pcp sas:
show crypto engine connections active

 RouterB#show crypto engine connections active

<table>
<thead>
<tr>
<th>ID</th>
<th>Interface</th>
<th>IP-Address</th>
<th>State</th>
<th>Algorithm</th>
<th>Encrypt</th>
<th>Decrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>FastEthernet0</td>
<td>172.17.1.1</td>
<td>set</td>
<td>HMAC_SHA+DES_56_CB</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2001</td>
<td>FastEthernet0</td>
<td>172.17.1.1</td>
<td>set</td>
<td>DES+SHA</td>
<td>0</td>
<td>59</td>
</tr>
<tr>
<td>2002</td>
<td>FastEthernet0</td>
<td>172.17.1.1</td>
<td>set</td>
<td>DES+SHA</td>
<td>59</td>
<td>0</td>
</tr>
</tbody>
</table>

Troubleshoot

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

The Output Interpreter Tool (registered customers only) (OIT) supports certain show commands. Use the OIT to view an analysis of show command output.

Note: Refer to Important Information on Debug Commands and IP Security Troubleshooting: Understanding and Using debug Commands before you use debug commands.

- **debug crypto ipsec 7** Displays the IPsec negotiations of phase 2.
- **debug crypto isakmp 7** Displays the ISAKMP negotiations of phase 1.
- **debug crypto ipsec** Displays the IPsec negotiations of phase 2.
- **debug crypto isakmp** Displays the ISAKMP negotiations of phase 1.

Related Information

- Cisco Configuration Professional Quick Start Guide
- Requests for Comments (RFCs)
- Technical Support & Documentation – Cisco Systems