

Configuring a Router-to-VPN 5000 Series Concentrator LAN-to-LAN Tunnel

Document ID: 14129

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, please see the End-of-Sales Announcement.

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure Syntax

- IKE Policy
- Tunnel Partner VPN x
- IP VPN x

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document gives an overview of the configuration required to allow a Cisco router and a Cisco VPN 5000 Series Concentrator to open an IPSec LAN-to-LAN tunnel. For information about how to establish basic connectivity, or reference on configuration syntax, please consult the VPN 5000 Concentrator documentation.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco IOS® Software Release 12.1
- VPN 5000 Series Concentrator

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 Syntax

The concentrator configuration groups various components of cryptographic operation together. The Internet Key Exchange (IKE) policy settings, which determine the authentication and encryption mechanisms for Phase 1 (Internet Security Association and Key Management Protocol [ISAKMP]) negotiation, the individual tunnel partner settings (or the global settings, if preferred), and the IP protocol settings are kept in separate areas of the configuration. The remaining sections of the configuration define the functionality of the various LAN and WAN interfaces, external authentication mechanisms (for example, RADIUS, Axent Defender, Secure Computing Safeword, SecurID), and a special keyword called "IPSecGateway." IPSecGateway is found in the General section and provides a default route for VPN traffic (including Point-to-Point Tunneling Protocol [PPTP] and Layer 2 Tunnel Protocol [L2TP]) aside from the standard default route.

The three cryptography-policy configuration section headings are:

- **IKE Policy**
- **Tunnel Partner VPN x** (x is either "Default" or a tunnel number)
- **IP VPN x** (x is either "Default" or a tunnel number. X in "tunnel partner vpn" and "ip vpn" must match to associate configuration settings)

IKE Policy

The **Protection** keyword is the only setting found in the **IKE Policy** section. The **Protection** keyword is equivalent to the **crypto isakmp policy x** command section in Cisco IOS Software configuration. The only additional information that is provided in the **crypto isakmp policy** command section is the type of authentication used, certificate, or shared-key. This discussion focuses on shared-key authentication. This keyword combines three parameters:

1. Authentication method (MD5 or SHA),
2. Encryption mechanism (DES or 3DES), and
3. Diffie-Hellman Group number (G1 or G2) on which to base ISAKMP negotiations.

Several IKE policies can be specified, and each are attempted during an IKE negotiation based on top-to-bottom order. These are keyword examples:

- Protection=SHA_3DES_G1
- Protection=MD5_DES_G2
- Protection=SHA_DES_G1
- Protection=MD5_3DES_G2

Tunnel Partner VPN x

The **Tunnel Partner VPN x** section provides the IPSec Transform value, the Shared Key value, the BindTo parameter, the KeyManage mode, the Mode setting for tunnel type, the Partner address, and the Peer and LocalAccess keywords for IP addresses on the private networks. The (x) is replaced with either a number or the word "default," if fixed tunnel configurations are not set up. Further information for **Tunnel Partner VPN Default** can be found in the VPN 5000 Concentrator documentation.

- The **Transform** value can be set to any combination of authentication (MD5 or SHA) and encryption (DES or 3DES) protection pieces. This value is equivalent to the **crypto ipsec transform-set**

command value in the Cisco IOS configuration. These are examples of VPN Concentrator Transform keywords and the corresponding Cisco IOS command:

- ◆ **Transform=ESP(MD5,DES)** Specifies ESP transport, MD5 packet authentication, and DES payload encryption.
- ◆ **Transform=AH(SHA,3DES)** Specifies AH transport, SHA packet authentication, and 3DES payload encryption.
- ◆ **Transform=ESP(DES)** Specifies ESP transport with only DES payload encryption only, no authentication.
- ◆ **Transform=AH(MD5)** Specifies AH transport with only MD5 packet authentication.
- **SharedKey** defines the value of the IKE password. This value is the component that is used to negotiate the IPsec Security Association. The SharedKey parameter must match the value in the **crypto isakmp key x** command.
- **BindTo** sets the tunnel to operate on a specific interface. The interface that **BindTo** indicates must be a publicly-addressable value, and is the number specified in the IP address keyword set in **IP VPN x**. This keyword roughly equates to the **crypto map x** command applied to a Cisco IOS interface configuration.
- **KeyManage** sets the device's operation for configuring tunnels. The **KeyManage** setting allows a degree of flexibility in how the device manages tunnel establishment. The options for IPsec tunnels are "Auto," "Initiate," and "Respond." Unlike Cisco IOS, which establishes a tunnel based on traffic that matches an access list, the VPN Concentrator establishes a tunnel at boot time if set to "Auto" or "Initiate," or waits for a tunnel initiation request from the other tunnel endpoint if set to "Respond."

Note: If "KeyManage" is set to "Initiate," the 500x ignores tunnel initiation requests from the other tunnel endpoint.

- **Mode** defines the interoperability setting of the tunnel. When running a pair of concentrator devices as the tunnel endpoints, this keyword can be set to "Aggressive." This allows for simplified configuration and greater flexibility for dynamic routing support. In interoperability mode, this parameter must be set to "Main."
- The **Partner** keyword defines the publicly-addressable IP address of the remote tunnel termination device. This keyword parallels the **set peer a.b.c.d** command found in the crypto map configuration in Cisco IOS.
- The **Peer** and **LocalAccess** keywords define the IP subnets that are included in the Security Association. These keywords are equivalent to the Cisco IOS access list that defines traffic associated with the crypto map.

IP VPN x

The **IP VPN x** section defines parameters for IP communication on the site-to-site connection. Two basic parameters are required for IP operation, and are configured identically for all site-to-site connections on a device. These two parameters are:

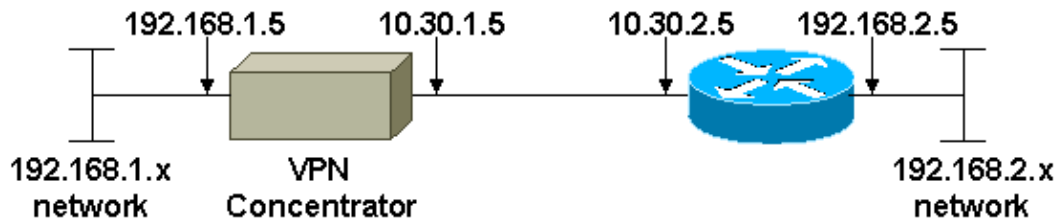
- **Numbered=Off** The **Numbered** value defines that the tunnel will run as an unnumbered connection.
- **Mode=Routed** The **Routed** keyword indicates that this interface is available to pass traffic. The options are bridged, routed, or off.

Configure

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

Network Diagram

This document uses the network setup shown in this diagram.



Configurations

This document uses these configurations.

- VPN 5000 Series Concentrator
- Router

VPN 5000 Series Concentrator	
[General]	
EnablePassword	=
IPSecGateway	= 10.30.1.1
[IP Ethernet 0]	
Mode	= Routed
SubnetMask	= 255.255.255.0
IPAddress	= 192.168.1.5
[IP Ethernet 1]	
SubnetMask	= 255.255.255.0
IPAddress	= 10.30.1.5
Mode	= Routed
[IKE Policy]	
Protection	= MD5_DES_G1
[IP Static]	
[Tunnel Partner VPN 1]	
BindTo	= "ethernet 1"
Peer	= "192.168.2.0/24"
Transform	= esp(md5,des)
SharedKey	= "letmein"
Mode	= Main
KeyManage	= Auto
LocalAccess	= "192.168.1.0/24"
Partner	= 10.30.2.5
[IP VPN 1]	
Numbered	= Off
Mode	= Routed

Router
version 12.1

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco-3640
!
enable password letmein
!
!
!
!
!
ip subnet-zero
ip cef
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
!
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key letmein address 10.30.1.5
!
!
crypto ipsec transform-set compatible esp-des esp-md5-hmac
!
crypto map compatible-crypt 1 ipsec-isakmp
  set peer 10.30.1.5
  set transform-set compatible
  match address 101
!
!
!
!
!
!
!
!
interface FastEthernet0/0
  ip address 10.30.2.5 255.255.255.0
  duplex auto
  speed auto
  crypto map compatible-crypt
!
interface FastEthernet0/1
  ip address 192.168.2.5 255.255.255.0
  duplex auto
  speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.30.2.1
no ip http server
!
access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
tftp-server slot0
tftp-server system
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password letmein
  login
!
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

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 VPN 5000 Series Concentrators End-of-Sales Announcement](#)
- [Cisco VPN 5000 Concentrator Support Page](#)
- [Cisco VPN 5000 Client Support Page](#)
- [IPSec Support Page](#)
- [Technical Support – Cisco Systems](#)