

Configuring Cisco VPN 5000 Series Concentrators with Overlapping Networks with LAN-to-LAN Tunnels

Document ID: 14116

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

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This document provides an overview of the configuration required when a Cisco VPN 5000 Series Concentrator has two different Customer Virtual Contexts (CVCs) for different customers with LAN-to-LAN tunnels to different customers' routers. Note that the internal networks of the routers overlap (loopback interfaces were created in this example). The different VPN Clients connect to the VPN Concentrator and to their private networks respectively because they have different VPN groups. The customer 1 VPN group users are sent across the customer 1 CVC to the VPN 3620 router. The customer 2 VPN group users are sent across the customer 2 CVC to the VPN 3640 router.

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(5)T in the routers
- Cisco VPN 5000 Concentrator software version 6.0.16
- Cisco VPN 5002 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.

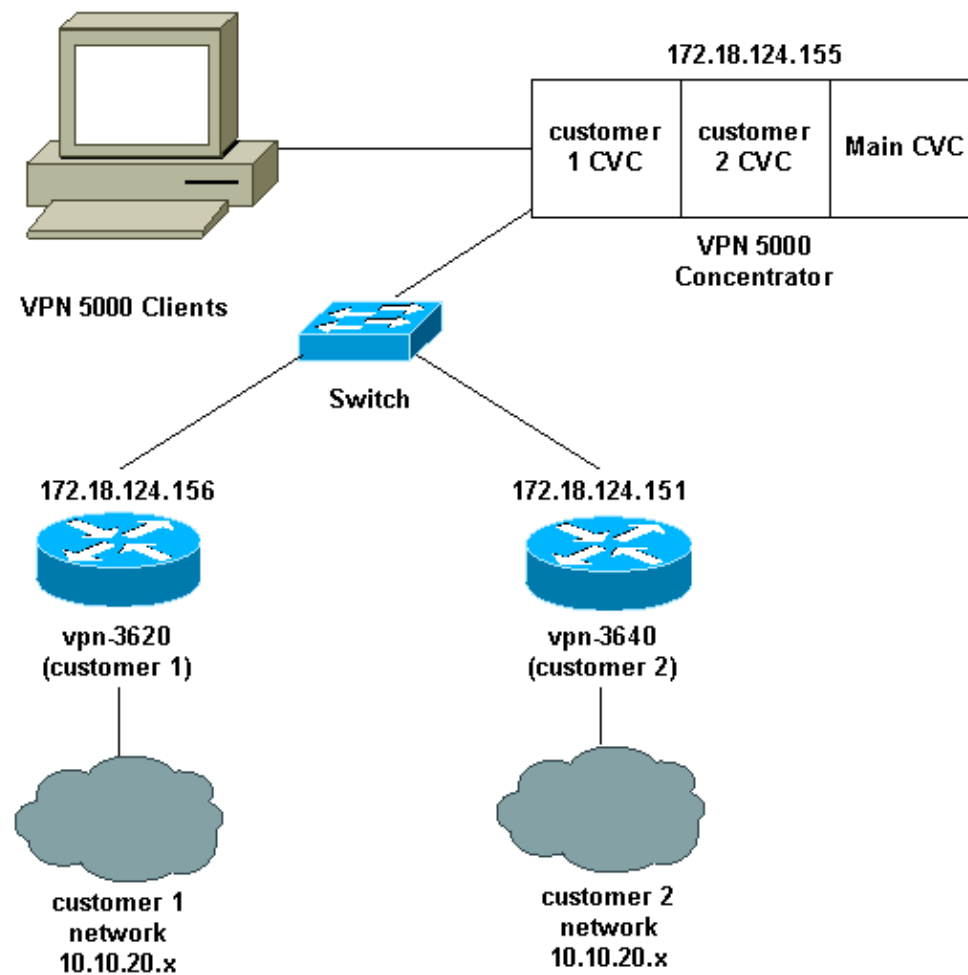
Configure

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 Tool (registered customers only).

Network Diagram

This document uses the network setup shown in this diagram.



Configurations

This document uses these configurations.

- Main CVC
- Customer 1 CVC

- Customer 2 CVC
- VPN 3620 Router (Customer 1)
- VPN 3640 Router (Customer 2)

```

Main CVC
Edited Configuration not Present, using Running
[ General ]
EthernetAddress      = 00:00:a5:e9:c8:00
DeviceType           = VPN 5002/8 Concentrator
ConfiguredOn         = Timeserver not configured
ConfiguredFrom       = Command Line, from Console
EnablePassword       =
Password             =
[ IP Ethernet 0:0 ]
Mode                 = Routed
SubnetMask           = 255.255.255.0
IPAddress            = 172.18.124.155
[ IKE Policy ]
Protection           = MD5_DES_G1
[ IP Static ]
0.0.0.0 0.0.0.0 172.18.124.1 1 redist=none
[ Logging ]
Level                = 7
Enabled              = On
[ Context List ]
flash://customer1.cfg
flash://customer2.cfg
Configuration size is 651 out of 65500 bytes.

```

```

Customer 1 CVC
Edited Configuration not Present, using Running
[ General ]
Context              = customer1
[ Tunnel Partner VPN 0:3 ]
Peer                 = "10.10.20.1"
LocalAccess          = "10.0.0.0/8"
Partner              = 172.18.124.156
KeyManage            = Respond
Mode                 = Main
SharedKey            = "cisco123"
Transform            = esp(md5,des)
BindTo               = "ethernet 0:0"
KeyLifeSecs         = 800
[ IP VPN 0:3 ]
Numbered             = Off
Mode                 = Routed
[ VPN Group "customer1" ]
LocalIPNet           = 10.10.40.0/24
IPNet                = 10.0.0.0/8
Transform            = esp(md5,des)
[ VPN Users ]
omar config="customer1" sharedkey="cisco"
Configuration size is 696 out of 65500 bytes.

```

```

Customer 2 CVC
Edited Configuration not Present, using Running
[ General ]
Context              = customer2
[ Tunnel Partner VPN 0:4 ]
Peer                 = "10.10.20.1"
LocalAccess          = "10.0.0.0/8"

```

```

Partner                = 172.18.124.151
KeyManage              = Respond
Mode                  = Main
SharedKey              = "cisco123"
Transform              = esp(md5,des)
BindTo                = "ethernet 0:0"
[ VPN Group "customer2" ]
LocalIPNet             = 10.10.40.0/24
IPNet                 = 10.0.0.0/8
Transform              = esp(md5,des)
[ IP VPN 0:4 ]
Numbered               = Off
Mode                  = Routed
[ VPN Users ]
omar2 config="customer2" sharedkey="cisco"

```

VPN 3620 Router (Customer 1)

```

show running-config
Building configuration...
Current configuration : 1187 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn-3620
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
no ip dhcp-client network-discovery

!--- IKE policy:

crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 172.18.124.155
!

!--- IPsec policy:

crypto ipsec transform-set compatible esp-des esp-md5-hmac
!
crypto map compatible-crypt 1 ipsec-isakmp
set peer 172.18.124.155
set transform-set compatible
match address 101
!
!
!
!
!
interface Loopback0
ip address 10.10.20.1 255.255.255.0
!

```

```

interface Ethernet1/0
ip address 172.18.124.156 255.255.255.0
no ip route-cache
no ip mroute-cache
half-duplex
crypto map compatible-crypt
!
interface TokenRing1/0
no ip address
shutdown
ring-speed 16
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip http server

!--- Traffic to encrypt:

access-list 101 permit ip 10.10.20.0 0.0.0.255 10.0.0.0 0.255.255.255
!
!
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

```

VPN 3640 Router (Customer 2)

```

Current configuration : 1669 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn-3640
!
boot system flash flash://c3640-jo3s56i-mz.121-5.T
logging rate-limit console 10 except errors
!
ip subnet-zero
!
!
no ip finger
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100

!--- IKE policy:

crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 172.18.124.155
!

!--- IPSec policy:

crypto ipsec transform-set compatible esp-des esp-md5-hmac

```

```

!
crypto map compatible-crypt 1 ipsec-isakmp
set peer 172.18.124.155
set transform-set compatible
match address 101
!
call rsvp-sync
cns event-service server
!
!
interface Loopback0
ip address 10.10.20.1 255.255.255.0
!
interface Ethernet0/0
ip address 172.18.124.151 255.255.255.0
half-duplex
crypto map compatible-crypt
!
interface Serial0/0
no ip address
shutdown
no fair-queue
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
no ip http server

!--- Traffic to encrypt:

access-list 101 permit ip 10.10.20.0 0.0.0.255 10.0.0.0 0.255.255.255
!
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

```

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 syslog buffer** Allows you to view previously buffered events on the VPN Concentrator.
- **show version** Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images on the VPN Concentrator.
- **show vpn statistics** and **show vpn statistics verbose** Shows this information for users and Partners, and the total for both on the VPN Concentrator:
 - ◆ Current active connections.
 - ◆ Currently negotiating connections.
 - ◆ The highest number of concurrent active connections since the last reboot.
 - ◆ The total number of successful connections since the last reboot.
 - ◆ The number of tunnel starts.
 - ◆ The number of tunnels for which there were no errors.
 - ◆ The number of tunnels with errors.

- **show crypto ipsec sa** Shows the settings used by current [IPSec] security associations (SAs) on the router.
- **show crypto isakmp sa** Shows all current IKE (SAs) at a peer on the router.

This is sample output of the **show version** command.

```

Software Version:      VPN 5002/8 Concentrator V6.0.16.0001 (dalecki) US
SW Build Date:        1/18/01 13:27
Hardware Revision:    3
BootBlock Version:    V2.09
Memory:               4096K Flash ROM, 128K CFG Flash, 262144K RAM
Last Configuration Date: none
Configuration File:   none
Configuration:        Running saved config, buffer unmodified
Ethernet 0:00 Address: 00:00:a5:e9:c8:00
Ethernet 1:00 Address: 00:00:a5:be:c8:00
Up Time:              20 hours 9 minutes 33 secs
Terminal settings:    80x24, Erase , Non-Enhanced Parser, More On
Time Server:          disabled

```

Troubleshoot

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

Troubleshooting Commands

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

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

- **vpn trace dump all** Shows information about all matching VPN connections. This includes information about the time, the VPN number, the real IP address of the peer, which scripts have been run, and in the case of an error, the routine and line number of the software code where the error occurred on the VPN Concentrator.
- **debug crypto ipsec** Shows the IPSec negotiations of phase 2 on the router.
- **debug crypto isakmp** Shows the ISAKMP negotiations of phase 1 on the router.
- **debug crypto engine** Shows the traffic that is encrypted on the router.
- **clear crypto isakmp** Clears the SAs related to phase 1 on the router.
- **clear crypto sa** Clears the SAs related to phase 2 on the router.

Related Information

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

Contacts & Feedback | Help | Site Map

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

