# Configuring an IPsec Tunnel – Cisco VPN 5000 Concentrator to Checkpoint 4.1 Firewall

Document ID: 14105

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. Refer to the End–of–Sales Announcement for more information.

# Contents

Introduction **Prerequisites** Requirements Components Used Conventions Configure Network Diagram Configurations Checkpoint 4.1 Firewall Verify Troubleshoot VPN 5000 Concentrator Troubleshooting Commands Network Summarization Checkpoint 4.1 Firewall Debug Sample Debug Output **Related Information** 

# Introduction

This document demonstrates how to form an IPsec tunnel with pre–shared keys to join two private networks. It joins a private network inside the Cisco VPN 5000 Concentrator (192.168.1.x) to a private network inside the Checkpoint 4.1 Firewall (10.32.50.x). It is assumed that traffic from inside the VPN Concentrator and inside the Checkpoint to the Internet (represented in this document by the 172.18.124.x networks) flows before you start this configuration.

# 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 VPN 5000 Concentrator
- Cisco VPN 5000 Concentrator software version 5.2.19.0001
- Checkpoint 4.1 Firewall

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 Cisco Technical Tips Conventions for more information on document conventions.

# Configure

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

**Note:** Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

### **Network Diagram**

This document uses this network setup:



### Configurations

This document uses this configuration.

Cisco VPN 5000 Concentrator				
[ IP Ethernet 0:0 ]				
Mode	= Routed			
SubnetMask	= 255.255.255.0			
IPAddress	= 192.168.1.1			
[ General ]				
EthernetAddress	= 00:00:a5:e9:c8:00			
DeviceType	= VPN 5002/8 Concentrator			
ConfiguredOn	= Timeserver not configured			
ConfiguredFrom	= Command Line, from Console			
DeviceName	= "cisco_endpoint"			
IPSecGateway	= 172.18.124.34			

```
[ IKE Policy ]
Protection = SHA_DES_G2
[ Tunnel Partner VPN 1 ]
I numer Partner VPN I JKeyLifeSecs= 28800LocalAccess= "192.168.1.0/24"Peer= "10.32.50.0/24"BindTo= "ethernet 1:0"SharedKey= "ciscorules"KeyManage= AutoTransform= esp(sha,des)Partner= 172 18 124 157
Partner
                                 = 172.18.124.157
Mode
                                 = Main
[ IP VPN 1 ]
Numbered
                                 = Off
Mode
                                 = Routed
[ IP Ethernet 1:0 ]
IPAddress
                                = 172.18.124.35
SubnetMask
                                = 255.255.255.240
Mode
                                = Routed
[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1
Configuration size is 1131 out of 65500 bytes.
```

### **Checkpoint 4.1 Firewall**

Complete these steps to configure the Checkpoint 4.1 Firewall.

1. Select **Properties > Encryption** to set the Checkpoint IPsec lifetimes to agree with the **KeyLifeSecs** = **28800** VPN Concentrator command.

Note: Leave the Checkpoint Internet Key Exchange (IKE) lifetimes at the default.

Properties Setup	×
High Availability   IP Pool NAT   Acces Security Policy   Traffic Control   Services   L Authentication   SYNDefender   LDAP	ss Lists Desktop Security Log and Alert Security Servers Encryption ConnectControl
SKIP Enable Exportable SKIP Change SKIP Session Key :	Manual IPSEC SPI allocation range (hex):
Every     120     Seconds (0 for infinity)       or     Every     10485760     Bytes (0 for infinity)	Erom 100 Lo ffff
Renegotiate I <u>K</u> E Security Associations every	1440 minutes
Renegotiate I <u>P</u> SEC Security Associations every	28800 seconds
OK Cancel	Help

Select Manage > Network objects > New (or Edit) > Network to configure the object for the internal ("cpinside") network behind the Checkpoint. This should agree with the Peer = "10.32.50.0/24" VPN Concentrator command.

Network Properties	×
General NAT	
<u>N</u> ame: Cpinside	<u>G</u> et address
Net <u>M</u> ask: 255.255.255.0	
Comment:	Color:
Location: <u>Internal</u> <u>External</u>	Broadcast: <u>Allowed</u> <u>Disallowed</u>
OK Ca	ncel Help

- 3. Select Manage > Network objects > Edit to edit the object for the gateway ("RTPCPVPN" Checkpoint) endpoint that the VPN Concentrator points to in the Partner = <ip> command.
  - Select **Internal** under Location.
  - Select **Gateway** for Type.
  - ◆ Check VPN-1 & FireWall-1 and Management Station under Modules Installed.

Workstation Properti	ties 🤰
General Interfaces	SNMP NAT Certificates VPN Authe
<u>N</u> ame: RTP	2CPVPN
IP <u>A</u> ddress: 172.1	.18.124.157 <u>G</u> et address
<u>Comment:</u> Firew	walled gateway to internet
Location: Internal O	Type: External O Host O Gateway
Modules Installed	J
VPN-1 & Eire	eWall-1 Version: 4.1 💌 Ge <u>t</u>
FloodGate-1	Version: 4.1
Compre <u>s</u> sion	n Version: 4.1
Managemer	ent Station Color:
OK	Cancel Help

4. Select Manage > Network objects > New (or Edit) > Network to configure the object for the external ("inside\_cisco") network behind the VPN Concentrator.

This should agree with the LocalAccess = <192.168.1.0/24> VPN Concentrator command.

Network Properties	×
General NAT	
Name:       Inside_cisco         IP Address:       192.168.1.0         Net Mask:       255.255.255.0         Comment:       Color:	
O Internal         € External         € Allowed         D isallowed	
OK Cancel Help	

5. Select Manage > Network objects > New > Workstation to add an object for the external ("cisco\_endpoint") VPN Concentrator gateway.

This is the "outside" interface of the VPN Concentrator with connectivity to the Checkpoint (in this document, 172.18.124.35 is the IP address in the **IPAddress** =  $\langle ip \rangle$  command).

Select External under Location. Select Gateway for Type.

**Note:** Do not check VPN–1/FireWall–1.

Wo	rkstation Properties	x		
G	General Interfaces SNMP NAT VPN			
	Name: cisco_endpoint			
	IP Address: 172.18.124.35 Get address			
	Comment:			
	Location:Type: ○ Internal ○ External ○ Host ○ Gateway			
	Modules Installed			
	VPN-1 & FireWall-1 Version: 4.1 💌 Get			
	FloodGate-1 Version: 4.1			
	Compression Version: 4.1			
	□ <u>M</u> anagement Station Co <u>l</u> or: □			
	OK Cancel Help			

6. Select **Manage > Network objects > Edit** to edit the Checkpoint gateway endpoint (called "RTPCPVPN") VPN tab. Under Domain, select **Other** and then select the inside of the Checkpoint network (called "cpinside") from the drop–down list. Under Encryption schemes defined, select **IKE**, and then click **Edit**.

Workstation Properties	×				
General Interfaces SNMP NAT	Certificates VPN Authe				
Domain:       Encryption schemes defined:         Disabled       Valid Addresses(of Interfaces)         ① Dither:       Manual IPSEC         □ Dither:       Image: Commission Skip         □ Exportable for SecuRemote       Edit					
Traffic Control Logging					
OK Car	ncel Help				

7. Change the IKE properties to **DES** encryption and **SHA1** hashing to agree with the **SHA\_DES\_G2** VPN Concentrator command.

**Note:** The "G2" refers to Diffie–Hellman group 1 or 2. In testing, it was discovered that the Checkpoint accepts either "G2" or "G1."

Change these settings:

\_

a. I	De-sel	ect A	ggressiv	<i>v</i> e	Mode.
------	--------	-------	----------	------------	-------

b. Check Supports Subnets.

c. Check Pre-Shared Secret under Authentication Method				
General Interfaces SNMP NAT Certificates VPN Authe				
YE Properties N				
General				
Key <u>N</u> egotiation Encryption Method(s): <u>H</u> ash Method:				
D 🖾 3DES				
Authentication Method:				
Pre-Shared Secret Edit Secrets				
Public Key Signatures     Configure				
Supports Aggresive <u>M</u> ode  Supports Subnets				
OK Cancel Help				

8. Click **Edit Secrets** to set the pre–shared key to agree with the **SharedKey** = <**key**> VPN Concentrator command.

\_

Workstation Properties 🛛 🔀
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties
General
Shared Secret
Shared Secrets List:
Peer Name Shared Secret
cisco_endpoint
<u>H</u> emove
OK Cancel Help

9. Select **Manage > Network objects > Edit** to edit the "cisco\_endpoint" VPN tab. Under Domain, select **Other**, and then select the inside of the VPN Concentrator network (called "inside\_cisco"). Under Encryption schemes defined, select **IKE**, and then click **Edit**.

Workstation Properties	×			
General Interfaces SNMP NAT	VPN			
Domain:	Encryption schemes defined:			
O <u>D</u> isabled	Manual IPSEC			
C ⊻alid Addresses(of Interfaces)				
	🗆 🔝 SKIP			
💂 inside_cisco 🔻				
Egportable for SecuFremote	<u>E</u> dit			
Traffic Control Logging				
Lum on Traffic Control Logging				
OK Car	ncel Help			

10. Change the IKE properties to **DES** encryption and **SHA1** hashing to agree with the **SHA\_DES\_G2** VPN Concentrator command.

**Note:** The "G2" refers to Diffie–Hellman group 1 or 2. In testing, it was found that the Checkpoint accepts either "G2" or "G1."

Change these settings:

- a. De-select Aggressive Mode.
- b. Check **Supports Subnets**.
- c. Check **Pre–Shared Secret** under Authentication Method.

General Interfaces SNMP NAT Certifica	ates VPN Authe
KE Properties	
General	
Key <u>N</u> egotiation Encryption Method(s):	– – <u>H</u> ash Method: –
DES DES	□ MD <u>5</u>
CAST	SHA1
Die Soles	
<u>A</u> uthentication Method:	
Pre-Shared Secret	dit <u>S</u> ecrets
Public <u>K</u> ey Signatures	Configure
Supports Aggresive Mode 🔽 Sup	oports Subnets
OK Cancel	Help

11. Click **Edit Secrets** to set the pre–shared key to agree with the **SharedKey** = <**key**> VPN Concentrator command.

IKE Properties
General
Shared Secret
Shared Secrets List:
Peer Name Shared Secret
RTPCPVPN **** Edit
Barray
OK Cancel
OK Cancel Help

12. In the Policy Editor window, insert a rule with both Source and Destination as "inside\_cisco" and "cpinside" (bidirectional). Set **Service=Any**, **Action=Encrypt**, and **Track=Long**.

File F	PCPVPN - Check P	oint Policy Editor	eln				- O ×
	i 🔔 🔾   🕺 🖻			ž   😭   📒 🖪	·	u 👡 🗩	🖶 🐻 🎹 🚯
🚔 Se	curity Policy - Standard	l 🛅 Address Trans	slation - Standa	rd 🛛 😿 Bandwidt	h Policy - St	andard	
No.	Source	Destination	Servio	e Ac	tion	Track	In
1	inside_cisco	nside_cisco	Any	E E	ncrypt	Long	<b>6</b>
For Help	), press F1			RTPCPVPN	Read	/Write	

13. Under the Action heading, click the green **Encrypt** icon and select **Edit properties** to configure encryption policies.

rrity Policy - Standard	🛃 Address Translation	- Standard 🛛 👬 Ban	dwidth Policy - Standard	-0
∼ FW1 Host	∼ Ldap-Servers	😰 Idap	accept	
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept	
🖶 inside_cisco	문고 cpinside 문고 inside_cisco	Any	Mit properties	ng .
		icmp dest-unreach	Edit Encryption	
		echo-reply	accept	am r
		icmp icmp-proto	drop	
Any	Any	imp mask-reply	reject	hg l

14. Select **IKE**, and click **Edit**.

Encryption Properties	×
General	
Encryption schemes defined:	
Edit	
OK Cancel Help	

15. On the IKE Properties window, change these properties to agree with the **Transform = esp(sha,des)** VPN Concentrator command.

Under Transform, select **Encryption + Data Integrity (ESP)**. The Encryption Algorithm should be **DES**, Data Integrity should be **SHA1**, and the Allowed Peer Gateway should be the external VPN Concentrator gateway (called "cisco\_endpoint"). Click **OK**.

IKE Properties	×
General	
Turn form	
• Encryption + Data Integrity (ESP)	
Data Integrity Only (AH)	
Encuration Algorithm:	
Data Integrity SHA1	
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
OK Cancel Help	

16. After you configure the Checkpoint, select **Policy > Install** on the Checkpoint menu to have the changes take effect.

# Verify

There is currently no verification procedure available for this configuration.

# Troubleshoot

### **VPN 5000 Concentrator Troubleshooting Commands**

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 before you use debug commands.

- **vpn trace dump all** Shows information about all matching VPN connections, including 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.
- show system log buffer Shows the contents of the internal log buffer.
- **show vpn statistics** Shows this information for users, partners, and the total for both. (For modular models, the display includes a section for each module slot. Refer to the Sample Debug Output section.)
  - ♦ Current Active The current active connections.
  - In Negot The currently negotiating connections.
  - ♦ High Water The highest number of concurrent active connections since the last reboot.
  - Running Total The total number of successful connections since the last reboot.
  - Tunnel OK The number of tunnels for which there were no errors.
  - Tunnel Starts The number of tunnel starts.
  - ♦ Tunnel Error The number of tunnels with errors.
- **show vpn statistics verbose** Shows ISAKMP negotiation statistics, and many more active connection statistics.

#### **Network Summarization**

When multiple adjacent inside networks are configured in the encryption domain on the Checkpoint, the device might automatically summarize them with regard to interesting traffic. If the VPN Concentrator is not configured to match, the tunnel is likely to fail. For example, if the inside networks of 10.0.0.0 /24 and 10.0.1.0 /24 are configured to be included in the tunnel, they might be summarized to 10.0.0.0 /23.

### **Checkpoint 4.1 Firewall Debug**

This was a Microsoft Windows NT installation. Because the tracking was set for Long in the Policy Editor window (as seen in Step 12), denied traffic should appear in red in the Log Viewer. More verbose debug can be obtained by:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

and in another window:

 $C:\WINNT\FW1\4.1\fwstart$ 

Issue these commands to clear the Security Associations (SAs) on the checkpoint:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

Answer yes at the Are you sure? prompt.

#### Sample Debug Output

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
  new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
  new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
  next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
  new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
```

39 seconds doing ihp2\_process\_pkt\_2, (0 @ 0) 39 seconds doing iph2\_build\_pkt\_3, (0 @ 0) 39 seconds doing iph2\_config\_SAs, (0 @ 0) 39 seconds doing iph2\_send\_pkt\_3, (0 @ 0) 39 seconds doing iph2\_last\_op, (0 @ 0) end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0) next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0) 39 seconds doing l2lp\_open\_tunnel, (0 @ 0) 39 seconds doing l2lp\_start\_i\_maint, (0 @ 0) new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start) 39 seconds doing imnt\_init, (0 @ 0) manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)

cisco\_endpoint#**show vpn stat** 

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0

IOP slot 1:

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0

#### cisco\_endpoint#show vpn stat verb

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0
Stats		VPN0:1					
Wrapped		13					
Unwrapped		9					
BadEncap		0					
BadAuth		0					
BadEncrypt	-	0					
rx IP		9					
rx IPX		0					

rx	Other	0	
tx	IP	13	
tx	IPX	0	
tx	Other	0	
IKE	l rekey	0	

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats Admin packets in 4 Fastswitch packets in 0 No cookie found 0 Can't insert cookie 0 Inserted cookie(L) 1 Inserted cookie(R) 0

Cookie not inserted(L) 0 Cookie not inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 Deleted cookie(L) 0 Deleted cookie(R) 0 Cookie not deleted(L) 0 Cookie not deleted(R) 0 0 Forwarded to RP 0 Forwarded to IOP Bad UDP checksum 0 Not fastswitched 0 Bad Initiator cookie 0 Bad Responder cookie 0 Has Responder cookie 0 No Responder cookie 0 No SA 0 Bad find conn 0 Admin queue full 0 0 Priority queue full Bad IKE packet 0 No memory 0 Bad Admin Put 0 IKE pkt dropped 0 No UDP PBuf 0 No Manager 0 Mgr w/ no cookie 0 Cookie Scavenge Add 1 Cookie Scavenge Rem 0 Cookie Scavenged 0 Cookie has mgr err 0 New conn limited 0

IOP slot 1:

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0

Stats Wrapped Unwrapped BadEncap BadAuth BadEncrypt rx IP rx IPX rx Other tx IP tx IPX tx Other IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats Admin packets in 0 Fastswitch packets in 3 No cookie found 0 Can't insert cookie 0 Inserted cookie(L) 0

Inserted cookie(R) 1 Cookie not inserted(L) 0 Cookie not inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 Deleted cookie(L) 0 Deleted cookie(R) 0 Cookie not deleted(L) 0 Cookie not deleted(R) 0 Forwarded to RP 0 Forwarded to IOP 3 Bad UDP checksum 0 Not fastswitched 0 Bad Initiator cookie 0 Bad Responder cookie 0 Has Responder cookie 0 No Responder cookie 0 No SA 0 Bad find conn 0 Admin queue full 0 Priority queue full 0 Bad IKE packet 0 No memory 0 Bad Admin Put 0 IKE pkt dropped 0 No UDP PBuf 0 No Manager Mgr w/ no cookie Cookie Scavenge Add No Manager 0 0 1 Cookie Scavenge Rem 0 Cookie Scavenged 0 Cookie has mgr err 0 New conn limited 0

## **Related Information**

- Cisco VPN 5000 Series Concentrators End-of-Sales Announcement
- IPsec Negotiation/IKE Protocols
- Technical Support & Documentation Cisco Systems

Contacts & Feedback | Help | Site Map

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: May 02, 2008

Document ID: 14105