Configuring an IPSec Tunnel Between a Cisco VPN 3000 Concentrator and a Checkpoint NG Firewall

Document ID: 23786

Contents

Introduction

Prerequisites Requirements Components Used Conventions Network Diagram Configurations Configure the VPN 3000 Concentrator Configure the Checkpoint NG Verify Verify the Network Communication View Tunnel Status on the Checkpoint NG View Tunnel Status on the VPN Concentrator Troubleshoot Network Summarization Debugs for the Checkpoint NG Debugs for the VPN Concentrator

Related Information

This document demonstrates how to configure an IPSec tunnel with pre–shared keys to communicate between two private networks. In this example, the communicating networks are the 192.168.10.x private network inside the Cisco VPN 3000 Concentrator and the 10.32.x.x private network inside the Checkpoint Next Generation (NG) Firewall.

Prerequisites

Requirements

- Traffic from inside the VPN Concentrator and inside the Checkpoint NG to the Internet represented here by the 172.18.124.x networks must flow prior to beginning this configuration.
- Users must be familiar with IPSec negotiation. This process can be broken down into five steps, including two Internet Key Exchange (IKE) phases.
 - 1. An IPSec tunnel is initiated by interesting traffic. Traffic is considered interesting when it travels between the IPSec peers.
 - 2. In IKE Phase 1, the IPSec peers negotiate the established IKE Security Association (SA) policy. Once the peers are authenticated, a secure tunnel is created with the Internet Security Association and Key Management Protocol (ISAKMP).
 - 3. In IKE Phase 2, the IPSec peers use the authenticated and secure tunnel in order to negotiate IPSec SA transforms. The negotiation of the shared policy determines how the IPSec tunnel is established.
 - 4. The IPSec tunnel is created, and data is transferred between the IPSec peers based on the

IPSec parameters configured in the IPSec transform sets.

5. The IPSec tunnel terminates when the IPSec SAs are deleted or when their lifetime expires.

Components Used

This configuration was developed and tested with these software and hardware versions:

- VPN 3000 Series Concentrator 3.5.2
- Checkpoint NG Firewall

Conventions

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

Network Diagram

This document uses this network setup:



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

Configurations

Configure the VPN 3000 Concentrator

Complete these steps in order to configure the VPN 3000 Concentrator:

1. Go to **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** in order to configure the LAN-to-LAN session. Set the options for authentication and IKE algorithms, pre-shared key, peer IP address, and local and remote network parameters. Click **Apply**.

In this configuration, authentication was set as ESP-MD5-HMAC and encryption was set as 3DES.

Configuration System Tunneling Protocols IPSec LAN-to-LAN Modify		
Modify an IPSec LAN-to-LAN connection.		
-		
Name Checkpoint	Enter the name for this LAN-to-LAN connection.	
Interface Ethernet 2 (Public) (172.18.124.131)	Select the interface to put this LAN-to-LAN connection on.	
Peer 172.18.124.157	Enter the IP address of the remote peer for this LAN-to-LAN connection.	
Digital None (Use Preshared Keys) *	Select the Digital Certificate to use.	
Certificate C Entire certificate chain Transmission [®] Identity certificate only	Choose how to send the digital certificate to the IKE peer.	
Preshared Key ciscontproles	Enter the preshared key for this LAN-to-LAN connection.	
Authentication ESP/MD5/HMAC-128 •	Specify the packet authentication mechanism to use.	
Encryption 3DES-168 ·	Specify the encryption mechanism to use.	
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.	
Routing None	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.	
Local Network		
Network List Lise IP Address/Wildcard-mask below	Specify the local network address list or the ID address and wildcard mask	
HELIGIR LAR OVER FREEDOW FREEDOW	for this LAN-to-LAN connection.	
IP Address 192.168.10.0	for this LAN-to-LAN connection.	
IP Address 192.168.10.0 Wildcard Mask 0.0.0.255	for this LAN-to-LAN connection. Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.nnn addresses.	
IP Address 192.168.10.0 Wildcard Mask 0.0.0.255 Remote Network	for this LAN-to-LAN connection. Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.	
IP Address 192.168.10.0 Wildcard Mask 0.0.0.256 Remote Network Network List Use IP Address/Wildcard-mask below •	Specify the rotan network address list of the IP address and white a mask for this LAN-to-LAN connection. Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.nnn addresses. Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.	
IP Address 192.168.10.0 Wildcard Mask 0.0.0.255 Remote Network Network List Use IP Address/Wildcard-mask below • IP Address 10.32.0.0	Specify the remote network address list of the IP address and which a dimask for this LAN-to-LAN connection. Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.nnn addresses. Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection. Note: Enter a wildcard mask, which is the reverse of a subnet mask. A	
IP Address 192.168.10.0 Wildcard Mask 0.0.0.255 Remote Network Network List Use IP Address/Wildcard-mask below • IP Address 10.32.0.0 Wildcard Mask 0.0.127.255	Specify the remote network address list of the IP address and wildcard mask for this LAN-to-LAN connection. Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.nnn addresses. Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection. Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.nnn addresses.	

2. Go to **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** and set the required parameters.

Select the IKE proposal IKE–3DES–MD5 and verify the parameters selected for the proposal. Click **Apply** in order to configure the LAN–to–LAN session.

These are the parameters for this configuration:

Configuration System Tunneling Protocols IPSec IKE Proposals Modify			
Modify a configured IKE Proposal.			
Proposal Name IKE-3DES-MD5	Specify the name of this IKE Proposal.		
Authentication Mode Preshared Keys	 Select the authentication mode to use. 		
Authentication Algorithm MD5/HMAC-128 •	Select the packet authentication algorithm to use.		
Encryption Algorithm 3DES-168 -	Select the encryption algorithm to use.		
Diffie-Hellman Group Group 2 (1024-bits) 💌	Select the Diffie Hellman Group to use.		
Lifetime Measurement Time 💌	Select the lifetime measurement of the IKE keys.		
Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).		
Time Lifetime 86400	Specify the time lifetime in seconds.		
Apply Cancel			

3. Go to **Configuration > Policy Management > Traffic Management > Security Associations**, select the IPSec SA created for the session, and verify the IPSec SA parameters chosen for the LAN–to–LAN session.

In this configuration the LAN-to-LAN session name was "Checkpoint," so the IPSec SA was created automatically as "L2L: Checkpoint."

Configuration Policy Management Traffic Mana	igement Security Associatio	ns Save Needed
This section lets you add, configure, modify, and negotiate IKE parameters.	delete IPSec Security Assoc	: iations (SAs). Security Associations use $\underline{\rm IKE\ Proposals}$ to
Click Add to add an SA, or select an SA and cli	ck Modify or Delete.	
	IPSec SAs ESP-DES-MD5 ESP-MD5 ESP/ME-3DES-MD5 ESP-3DES-MONE ESP-12TP-TRANSPORT ESP-3DES-MD5-DH7 I2L: Checkpoint	Actions Add Modify Delete

These are the parameters for this SA:

Configuration Policy Management Traffic Management Security Associations Modify		
Modify a configured Security Association.		
SA Name	L2L: Checkpoint	Specify the name of this Security Association (SA).
Inheritance	From Rule *	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	ESP/MD5/HMAC-128	Select the packet authentication algorithm to use.
Encryption Algorithm	3DES-168 •	Select the ESP encryption algorithm to use.
Encapsulation Mode	Tunnel -	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	Disabled •	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	Time •	Select the lifetime measurement of the IPSec keys.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	86400	Specify the time lifetime in seconds.
IKE Parameters		
IKE Peer	172.18.124.157	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
Negotiation Mode	Main 💌	Select the IKE Negotiation mode to use.
Digital Certificate	None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
Certificate Transmission	 Entire certificate chain Identity certificate only 	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	IKE-3DES-MD5	Select the IKE Proposal to use as IKE initiator.
Apply Cancel		

Configure the Checkpoint NG

Network objects and rules are defined on the Checkpoint NG in order to make up the policy that pertains to the VPN configuration to be set up. This policy is then installed with the Checkpoint NG Policy Editor to complete the Checkpoint NG side of the configuration.

1. Create the two network objects for the Checkpoint NG network and VPN Concentrator network that will encrypt the interesting traffic.

in order to create objects, select **Manage > Network Objects**, then select **New > Network**. Enter the appropriate network information, then click OK.

These examples show the set up of network objects called CP_inside (the inside network of the Checkpoint NG) and CONC_INSIDE (the inside network of the VPN Concentrator).

etwork Properties - CP_inside	×
General NAT	
Name: CP_inside	
IP <u>A</u> ddress: 10.32.0.0	
Net <u>M</u> ask: 255.255.128.0	
Comment: CPINSIDE	
Color:	
Broadcast address: Included O Not included	
OK Cancel	Help
OK Cancel	Help
OK Cancel	
OK Cancel Retwork Properties - CONC_INSIDE General NAT	
OK Cancel etwork Properties - CONC_INSIDE General NAT <u>Name: CONC_INSIDE</u>	
OK Cancel etwork Properties - CONC_INSIDE General NAT Name: CONC_INSIDE IP Address: 192.168.10.0	
OK Cancel OK General NAT Name: CONC_INSIDE IP Address: 192.168.10.0 Net Mask: 255.255.255.0	
OK Cancel Concel NAT Mame: CONC_INSIDE IP Address: 192.168.10.0 Net Mask: 255.255.255.0 Concentrator network Concentrator network	
OK Cancel Concel Concel Image: NAT NAT Name: CONC_INSIDE IP Address: 192.168.10.0 IP Address: 192.168.10.0 Net Mask: 255.255.0 Comment: Concentrator network Concentrator network	
OK Cancel OK Cancel Concentration NAT Name: CONC_INSIDE IP Address: 192.168.10.0 Net Mask: 255.255.255.0 Comment: Concentrator network Color: Image: Im	
OK Cancel Idetwork Properties - CONC_INSIDE General NAT Name: CONC_INSIDE IP Address: 192.168.10.0 Net Mask: 255.255.255.0 Concentrator network Color: Broadcast address: Included Ngt included 	
OK Cancel etwork Properties - CONC_INSIDE General NAT Name: CONC_INSIDE IP Address: 192.168.10.0 Net Mask: 255.255.255.0 Concentrator network Color: Broadcast address: Included Included Ngt included	

2. Go to **Manage > Network Objects** and selecting **New > Workstation** in order to create workstation objects for the VPN devices, Checkpoint NG and VPN Concentrator.

Note: You can use the Checkpoint NG workstation object created during initial Checkpoint NG setup. Select the options to set the workstation as Gateway and Interoperable VPN Device, then click **OK**.

These examples show the set up of objects called ciscocp (Checkpoint NG) and CISCO_CONC (VPN 3000 Concentrator):

Workstation Properties - (ciscocp	×
Workstation Properties - General - Topology - NAT - VPN - Authentication - Management - Advanced	General Name: ciscocp IP Address: 172.18.124.157 Gent address: 172.18.124.157 Comment: Checkpoint External IP Color: Image: Color Color: Type: Most Image: Color	×
	Check Boint products installed: Version NG Cet Version VPN-1 & FireWall-1 FloodGate-1 Policy Server Primary Management Station Object Management	
	Managed by another Management Server ([nternal) Managed by another Management Server (External) Secure Internal Communication Communication DN: cn=cp_mgmt,o=ciscocppvzfoa Interoperable VFN Device	
	OK Cancel Help	

Workstation Properties -	CISCO_CONC	×
General	General	
- NAT	Name: CISCO_CONC	
	IP Address: 172.18.124.131 Get address	
	Comment: VPN Concentrator	
	Cojor:	
	Type: C Host C Gateway	
	Check Point Products	
	Check Point products installed: Version NG Cet Version	
	□VPN-1 & FireWall-1 □FloodGate-1 □Policy Server □Management Station	
	Object Management	
	C Managed by this Management Server (Internal)	
	C Managed by another Management Server (External)	
	Interoperable ⊻PN Device	
	OK Cancel Help	

3. Go to **Manage > Network Objects > Edit** in order to open the Workstation Properties window for the Checkpoint NG workstation (ciscocp in this example). Select **Topology** from the choices on the left side of the window, then select the network to be encrypted. Click **Edit** in order to set the interface properties.

In this example, CP_inside is the inside network of the Checkpoint NG.

Workstation Properties -	ciscocp				×
General	Topology Get Interfaces				
	Name	IP Address	Network Mask	IP Addresses behind	
— Management — Advanced	E100B0 E100B1	10.32.50.50 172.18.124.157	255.255.128.0 255.255.255.0	CP_inside External	
	•			•	
	Add Show all IPs behi VPN Domain All IP Addresses information. Manually Define Exportable for S	Edit nd Gateway s behind Gateway be ed	<u>Remove</u>	Show Show	
			ок с	ancel Help	

4. On the Interface Properties window, select the option to designate the workstation as internal, then specify the appropriate IP address. Click **OK**.

The topology selections shown designate the workstation as internal and specify IP addresses behind the CP_inside interface:

Interface Properties	×
General Topology QoS	
Topology	
C External (leads out to the internet)	
 Internal (leads to the local network) 	
IP Addresses behind this interface:	
C Not Defined	
O Network defined by the interface IP and Net Mask	
Anti-Spoofing ✓ Perform Anti-Spoofing based on interface topology Spoof Tracking: ○ None	
OK Cancel Help	

5. From the Workstation Properties window, select the outside interface on the Checkpoint NG that leads out to the Internet, then click **Edit** in order to set the interface properties. Select the option to designate the topology as external, then click **OK**.

Interfa	ace Properties	×
Gene	eral Topology QoS	
Тор	pology	
•	External (leads out to the internet)	
0	Internal (leads to the local network)	
	IP Addresses behind this interface:	
	○ Not Defined	
	${f C}$ Network defined by the interface IP and Net M	ask.
	O <u>S</u> pecific:	-
Anti	i-Spoofing	
	Caref Tracking C. M. C. J. C. M. C.	
	OK Cancel Help	

6. From the Workstation Properties window on the Checkpoint NG, select **VPN** from the choices on the left side of the window, then select the IKE parameters for encryption and authentication algorithms. Click **Edit** in order to configure the IKE properties.

VPN Encryption <u>s</u> chemes	
Image: KE set default [KE properties] Image: FVVZ Edit	
Nickname DN Certificate Authority	
Add Edit Aemove	
	Entrypoint generate Set default [KE properties] Edt Edt Certificate List Nickname DN Certificate Authority Add Edt OK Cancel

7. Set the IKE properties to match the properties on the VPN Concentrator.

In this example, select the encryption option for **3DES** and the hashing option for **MD5**.

IKE Properties	×
General	
Support key exchange encryption w	with:
	□ <u>▼</u> MD <u>5</u>
CAST	
Support authentication methods:	
Pre-Shared Secret	Edit <u>S</u> ecrets
Public Key Signatures	Specify
□ VPN-1 & FireWall-1 authentica	tion for SecuRemote (Hybrid Mode)
<u> </u>	
	<u>A</u> dvanced
 OKCa	ncel Help

8. Select the authentication option for **Pre–Shared Secrets**, then click **Edit Secrets** to set the pre–shared key to be compatible with the pre–shared key on the VPN Concentrator. Click **Edit** in order to enter your key as shown, then click **Set**, **OK**.

Share	ed Secret	×	<
- ۲ ⁹	Shared Secrets List:		
	Peer Name Shared Secret CISCO_CONC ****	<u>E</u> dit	
		<u>R</u> emove	
	Enter secret: ciscortprules Set		
	OK Cancel	<u>H</u> elp	

- 9. From the IKE properties window, click **Advanced...** and change these settings:
 - Deselect the option for **Support aggressive mode**.

• Select the option for **Support key exchange for subnets**. When you are finished, click **OK**.

×
EC_encapsi
3 bit) 24 bit)
36 bit)
1440 🗧 Minutes
3600 🕂 Seconds
y 50000 🕂 KBytes
<u>H</u> elp
3 bit) 24 bit) 36 bit) 1440

10. Go to Manage > Network Objects > Edit in order to open the Workstation Properties window for the VPN Concentrator. Select Topology from the choices on the left side of the window in order to manually define the VPN domain.

In this example, CONC_INSIDE (the inside network of the VPN Concentrator) is defined as the VPN domain.

Workstation Properties - C	ISCO_CONC				×
General Topology NAT	Topology <u>G</u> et Interfaces	1			
VPN	Name	IP Address	Network Mask		1
Advanced	Add Show all IPs before VPN Domain All IP Addresse information. All IP Addresse information.	Edt iind Gateway as behind Gateway b red + CONC_INS SecuRemote	Bernove	how Show Show	

11. Select **VPN** from the choices on the left side of the window, then select **IKE** as the encryption scheme. Click **Edit** in order to configure the IKE properties.

Workstation Properties -	CISCO_CONC			×
General Topology NAT Xim Advanced	VPN Encryption gchemes Image: Image	ΟK	Cancel	Help

12. Set the IKE properties to reflect the current configuration on the VPN Concentrator.

In this example, set the encryption option for **3DES** and the hashing option for **MD5**.

IKE Properties	×				
General					
Support key exchange encryption with	h:				
	✓ MD <u>5</u>				
L li CAST ☑ SDES	E SHA <u>1</u>				
Support authentication methods:					
Pre-Shared Secret	Edit <u>S</u> ecrets				
Public Key Signatures	Aatching Criteria				
	on for SecuRemote (Hybrid Mode)				
	<u>A</u> dvanced				
OK Cano	cel Help				

13. Select the authentication option for **Pre–Shared Secrets**, then click **Edit Secrets** in order to set the pre–shared key. Click **Edit** in order to enter your key as shown, then click **Set**, **OK**.

Shar	ed Secret				×
Г	Shared Secrets List: -				1
	Peer Name	Shared Secr	et		
	ciscocp	****		<u>E</u> dit	
				<u>R</u> emove	
	Enter secret: cisco	rtprules	Set		
	ОК	Cance		<u>H</u> elp	

- 14. From the IKE properties window, click **Advanced...** and change these settings:
 - Select the Diffie–Hellman group appropriate for the IKE properties.
 - Deselect the option for **Support aggressive mode**.
 - Select the option for **Support key exchange for subnets**.

When you are finished, click OK, OK.

Advanced IKE properties			×
☑ Use <u>U</u> DP encapsulation ───			
	UDP VPN1_IPSE	C_encapsi 💌	
Support Diffie-Hellman groups			
	Group 1 (768	bit)	
	Group 2 (1024	bit) Shan	
) DI(J	
Rekeying Parameters			
Renegotiate IKE security associat	ions	1440 🗦	Minutes
Renegotiate IPSEC Security asso	ciations every	3600 🕂	Seconds
Renegotiate IPSEC Security a	ssociations every	50000 🚊	KBytes
Misc			
Support IP compression for Se	cureClient		
Support aggresive mode			
Support key exchange for <u>s</u> ub	nets		
OK Ca	ancel	Help	

15. Select Rules > Add Rules > Top in order to configure the encryption rules for the policy. In the Policy Editor window, insert a rule with source as CP_inside (inside network of the Checkpoint NG) and destination as CONC_INSIDE (inside network of the VPN Concentrator). Set values for Service = Any, Action = Encrypt, and Track = Log. When you have added the Encrypt Action section of the rule, right-click Action and select Edit Properties.

CLISCOCP - Check Point Policy Editor -	Standard				
File Edit View Manage Rules Policy Topology Search Window Help					
」■● X凸前 疊趣夜	▲ 🗉 📲 📲 📲 📲 🗮 🕷 🗎 🖗				
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Q Q 🖸 💊 🗇 🗖				
\$ <u>4</u> 4088808	🗱 Security - Standard 🗮 Address Translation - Standard 🔛 QoS - St	andard 🛛 🎦 Desktop Security - Standard			
B. Workstation	NO. SOURCE DESTINATION SERVICE	ACTION TRACK INSTALL			
	1 CP_inside CONC_NSDE * Any	Edit properties			
-++ CONC_INSIDE	2 4 CP_inside * Any * Any	Add Encryption Gateway:			
Corperate Corperate	4				
- 000 Uyrixanik. UDject	Name IP Comment CISCO_CONC 172.18.124.131 VPN Conce Giscocp 172.18.124.157 Checkpoint	Client Encrypt Client Encrypt Courry Column Cliear Query			

16. Select IKE and click Edit.

Encryption Properties			×
General			
Encryption <u>s</u> chemes defined:			
<u>E</u> dit			
OK Can	cel He	elp	

17. On the IKE Properties window, change the properties to agree with the VPN Concentrator transform.

- ♦ Set the Transform option to **Encryption** + **Data Integrity** (**ESP**).
- Set the Encryption Algorithm to **3DES**.
- Set the Data Integrity to MD5.
- ◆ Set the Allowed Peer Gateway to match the VPN Concentrator (CISCO_CONC).

When you are finished, click **OK**.

IKE Properties	×
General	
Transform	
Encryption + Data Integrity	(ESP)
C Data Integrity Only (AH)	
Encryption Algorithm:	3DES 💌
Data Integrity	MD5
Compression method:	None
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
Use DH <u>G</u> roup:	Group 1 (768 bit)
Perform IP Pool NAT	
OK Car	ncel Help

18. After the Checkpoint NG is configured, save the policy and select **Policy > Install** in order to enable it.

CISCOCP - Check Point Policy	Editor - Standard				1	
File Edit View Manage Rules	Policy Topology Search Window	Help				
Image: Second		' 👞 🗒 🐟 👽 🍰 🍂 년간 [편] ddress Translation - Standard - 📓 QoS - Standard - 10 Desitop Security - Standard -				
Ketwork Objects	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON
B- Workstation	Management High Availability					
ciscorp	Global Properties	CONC_INSIDE	🖈 Any	Encrypt	🔳 Log	Gateways
-++ CONC_INSIDE	2 ++ CP_inside	🗙 Αειγ	* Any	💮 accept	E Log	Gateways
Ormain Ormain Ormain Off Device Embedded Device Group Vigical Server Ugical Server Off Address Range						
Gateway Cluster						<u> </u>
Dynamic Object	Name	IP	Comment			
	CISCO_CONC	172.18.1	24.131 VPN Conc	centrator		
	Ciscocp	172.18.1	24.157 Checkpoi	nt External IP		

The installation window displays progress notes as the policy is compiled.



When the installation window indicates that the policy installation is complete, click **Close** in order to finish the procedure.

Install Policy	×
Standard.W: Security Policy Script generated into Standard.pf Standard: Compiled OK.	4
Installing VPN-1/FireWall-1 policy On: ciscocp	
VPN-1/FireWall-1 policy installed successfully on ciscocp	
VPN-1/FireWall-1 policy Installation for all modules was successful	
[Close]	

Verify

Use this section to confirm that your configuration works properly.

Verify the Network Communication

In order to test communication between the two private networks, you can initiate a ping from one of the private networks to the other private network. In this configuration, a ping was sent from the Checkpoint NG side (10.32.50.51) to the VPN Concentrator network (192.168.10.2).

```
C:\WINNT\System32\cmd.exe
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253
Ping statistics for 192.168.10.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = Oms, Maximum = 10ms, Average =
                                                5ms
C:\>
C:\>
C:\>
C:\>
```

View Tunnel Status on the Checkpoint NG

In order to view the tunnel status, go to the Policy Editor and select **Window > System Status**.

CISCOCP - Check Point System Status			
Ele View Modules Products Iools Window Help			
🗩 🔍 🖻 🐘 🚺 🔌 🎫 🇞 💷 🗳 🛠	R5		
Modules IP Address	VPN-1 Details		
E-12 CISCOCP	Status:	ок	
E-Ciscocp 172.18.124.157	Packets		
FireWal-1	Encrypted:	19	
FloodGate-1	Decrypted:	18	
Management	Errors		
SVN Foundation	Encryption errors:	0	
	Decryption errors:	0	
	IKE events errors:	3	
	Hardware		
	HW Vendor Name:	none	
	HW Status:	none	
For Help, press F1			Last updated:09:34:14 PM

View Tunnel Status on the VPN Concentrator

In order to verify the tunnel status on the VPN Concentrator, go to Administration > Administer Sessions.

his screen shows st formation on a sess onnection to a sessi	atistics for sessions. sion, click on that ses on, click Ping .	To refresh the statis sion's name. To log	tics, click Refre out a session, cl	sh. Sel ick Log	ect a Group gout in the tal	to filter ble belo	the session: w. To test t	Reset @ Refresh s. For more he network
roup [All ogout All: <u>PPTP U</u> Session Summa	ser L2TP User IPS	ec User L2TP/IPSe	ec User IPSec/U	JDP Us	er IPSec/TC	P User	IPSec LAN	N-to-LAN
Active LAN-to- LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak S	Concurrent essions	Con Sessio	current ons Limit	Total Cumulative Sessions
Active LAN-to- LAN Sessions	Active Remote Access Sessions	Active Management Sessions 3	Total Active Sessions	Peak S	Concurrent essions 4	Con Sessio	current ons Limit	Total Cumulative Sessions 17
Active LAN-to- LAN Sessions 1 LAN-to-LAN S	Active Remote Access Sessions	Active Management Sessions 3	Total Active Sessions 4	Peak S	Concurrent essions 4 [Remote Acc	Con Sessio 1	current ons Limit 500 ssions Man	Total Cumulative Sessions 17 agement Sessions
Active LAN-to- LAN Sessions 1 LAN-to-LAN S Connection Nam	Active Remote Access Sessions 0 eessions ne IP Address	Active Management Sessions 3 Protoco	Total Active Sessions 4 Encr	Peak S	Concurrent essions 4 [Remote Acc Login T	Con Sessio 1 cess Ses	current ons Limit 500 ssions Man Duration	Total Cumulative Sessions 17 agement Sessions

Under LAN-to-LAN Sessions, select the connection name for the Checkpoint to view details on the SAs created and the number of packets transmitted/received.

dministration Admini	ster Sessio	ns Det	ail		We	dnesday, 11	September Re	2002 20:37 Iset 🥜 Refresh	
Connection Name	IP Add	dress	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	
Checkpoint	172.18.12	4.157 IPSec/LAN-to-LAN		3DES-168	Sep 11 20:36:03	0:01:55	256	256	
IPSec Sessions: 1	Session ID	1	IK	E Session	Encryption Algori	thum 3DES-1	68		
Hashing Algorithm MD5		MD5			Diffie-Hellman Group		Group 2 (1024-bit)		
Authentication Mode Pre-		Pre-Shared Keys		I	ode Main	Main			
Rekey Time Interval 86400			seconds						
			IPS	ec Session					
Session ID 2				Remote Addr	ess 10.32.0.	10.32.0.0/0.0.127.255			
Local Address 192.		192.168.10.0/0.0.0.255		Encryption Algorithm		hm 3DES-1	n 3DES-168		
Hashing Algorithm MD5		MD5			SEP		P 1		
Encapsula	tion Mode	Tunnel			Rekey Time Interva		d 28800 seconds		
Bytes	Received	256			Bytes Transmit	ted 256			

Troubleshoot

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

Note: The traffic must not be PATed across the IPSec tunnel using the VPN Concentrator public IP address (outside interface). Otherwise, the tunnel fails. So, the IP address used for PATing must be an address other than the address configured on the outside interface.

Network Summarization

When multiple adjacent, inside networks are configured in the encryption domain on the Checkpoint, the device can automatically summarize the networks 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, these networks can be summarized to 10.0.0.0/23.

Debugs for the Checkpoint NG

In order to view the logs, select **Window > Log Viewer**.

🚡 CTSCOCP - Check Point Log Viewer - [fw.log]												X		
E	Ele Mode Edit Selection View Iools Window Help													
1	@/@/\$_Log ▼ # A ▼ ± @ = \$ \$ \$ 0 # 5 \$ \$ @ \$ \$ 0 1													
	Date	Time	Product	<u>.</u>	Inter.	Orig., Type	Action	Source	Destinati	Pr., Rule	S_Port	SrcKeyID	DstKeyID	×
	13Aug2002	21:32:	VPN-1	& FireN.	🖶 dae	. ciscocp 🔳 log	0- key instali	ciscoop	CISCO_CONC					
	13Aug2002	21:32	VPN-1	& FirekV.	. 💽 dae	. ciscocp 🔳 log	Over key install	ciscocp	CISCO_CONC			0x5879f30d	0xt1351129	

Debugs for the VPN Concentrator

In order to enable debugs on the VPN Concentrator, go to **Configuration > System > Events > Classes**. Enable AUTH, AUTHDBG, IKE, IKEDBG, IPSEC, and IPSECDBG for severity to log as 1 - 13. In order to view debugs, select **Monitoring > Filterable Event Log**.

```
1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128
3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157
processing SA payload
4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)
10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1
13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157
Oakley proposal is acceptable
14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157
processing VID payload
15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157
processing IKE SA
16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)
22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513
Phase 1 failure against global IKE proposal # 2:
```

Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1

25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157 IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3

26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157 constructing ISA_SA for isakmp

27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 84

29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157 processing ke payload

34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157 processing ISA_KE

35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157 processing nonce payload

36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157 constructing ke payload

37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157 constructing nonce payload

38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157 constructing Cisco Unity VID payload

39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157 constructing xauth V6 VID payload

40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157 Send IOS VID

41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157 constructing VID payload

44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157 Send Altiga GW VID

45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157 Generating keys for Responder...

46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) ... total length : 256

48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60

50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 Group [172.18.124.157] Processing ID 51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157 Group [172.18.124.157] processing hash 52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157 Group [172.18.124.157] computing hash 53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157 Group [172.18.124.157] Starting group lookup for peer 172.18.124.157 54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10 AUTH_Open() returns 9 55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10 Authentication session opened: handle = 9 56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10 AUTH_PutAttrTable(9, 748174) 57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10 AUTH_GroupAuthenticate(9, 2f1b19c, 49c648) 58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10 AUTH_BindServer(51a6b48, 0, 0) 59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10 Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1 60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10 AUTH CreateTimer(51a6b48, 0, 0) 61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10 Reply timer created: handle = 4B0018 62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10 AUTH_BuildMsg(51a6b48, 0, 0) 63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10 AUTH_StartTimer(51a6b48, 0, 0) 64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10 Reply timer started: handle = 4B0018, timestamp = 1163319, timeout = 3000065 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10 AUTH_SndRequest(51a6b48, 0, 0) 66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19 IntDB_Decode(3825300, 156) 67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19 IntDB_Xmt(51a6b48) 68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10 $xmit_cnt = 1$ 69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20

IntDB_Xmt(51a6b48)

70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10 IntDB Match(51a6b48, 3eb7ab0) 71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10 AUTH_RcvReply(51a6b48, 0, 0) 72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20 IntDB_Decode(3eb7ab0, 298) 73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10 IntDB_Rcv(51a6b48) 74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10 AUTH_DeleteTimer(51a6b48, 0, 0) 75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10 Reply timer stopped: handle = 4B0018, timestamp = 1163329 76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10 AUTH_Callback(51a6b48, 0, 0) 77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157 Authentication successful: handle = 9, server = Internal, group = 172.18.124.15778 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157 Group [172.18.124.157] Found Phase 1 Group (172.18.124.157) 79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10 AUTH_GetAttrTable(9, 748420) 80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157 Group [172.18.124.157] Authentication configured for Internal 81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: IP Compression = disabled 82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: Split Tunneling Policy = Disabled 83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10 AUTH_Close(9) 84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157 Group [172.18.124.157] constructing ID 85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527 Group [172.18.124.157] construct hash payload 86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157 Group [172.18.124.157] computing hash 87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157 Group [172.18.124.157] constructing dpd vid payload 88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157

SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) ... total length : 80 90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157 Group [172.18.124.157] PHASE 1 COMPLETED

91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157 Keep-alive type for this connection: None

92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157 Keep-alives configured on but peer does not support keep-alives (type = None)

93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157 Group [172.18.124.157] Starting phase 1 rekey timer: 64800000 (ms)

94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16 User 172.18.124.157 connected

95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10 AUTH_UnbindServer(51a6b48, 0, 0)

96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10 Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0

97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10 AUTH_Int_FreeAuthCB(51a6b48)

98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10 Authentication session closed: handle = 9

99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 156

102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157 Group [172.18.124.157] processing hash

103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157 Group [172.18.124.157] processing SA payload

104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157 Group [172.18.124.157] processing nonce payload

105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157 Group [172.18.124.157] Processing ID

106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157 Group [172.18.124.157] Received remote IP Proxy Subnet data in ID Payload: Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0

109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157 Group [172.18.124.157] Processing ID

110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157
Group [172.18.124.157]
Received local IP Proxy Subnet data in ID Payload:
Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0

113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534 QM IsRekeyed old sa not found by addr

114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157 Group [172.18.124.157] IKE Remote Peer configured for SA: L2L: Checkpoint

115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157 Group [172.18.124.157] processing IPSEC SA

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157 Group [172.18.124.157] IPSec SA Proposal # 1, Transform # 1 acceptable

117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157 Group [172.18.124.157] IKE: requesting SPI!

118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39 IPSEC key message parse - msgtype 6, len 200, vers 1, pid 0000000, seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300

122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139 Processing KEY_GETSPI msg!

123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10 Reserved SPI 305440147

124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10 IKE got SPI from key engine: SPI = 0x1234a593

125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157 Group [172.18.124.157] oakley constucting quick mode

126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157 Group [172.18.124.157] constructing blank hash

127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157 Group [172.18.124.157] constructing ISA_SA for ipsec

128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157 Group [172.18.124.157] constructing ipsec nonce payload

129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157 Group [172.18.124.157] constructing proxy ID

130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157 Group [172.18.124.157] Transmitting Proxy Id: Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0 Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157 Group [172.18.124.157] constructing qm hash

135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157 SENDING Message (msgid=54796f76) with payloads :

HDR + HASH (8) + SA (1) ... total length : 152

137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + NONE (0) ... total length : 48

139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157 Group [172.18.124.157] processing hash

140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157 Group [172.18.124.157] loading all IPSEC SAs

141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key!

142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key!

143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157 Group [172.18.124.157] Loading subnet: Dst: 192.168.10.0 mask: 255.255.255.0 Src: 10.32.0.0 mask: 255.255.128.0

146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157 Group [172.18.124.157] Security negotiation complete for LAN-to-LAN Group (172.18.124.157) Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959

149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40 IPSEC key message parse - msgtype 1, len 606, vers 1, pid 0000000, seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0, spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140 Processing KEY_ADD msg!

154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141 key_msghdr2secassoc(): Enter

155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142 No USER filter configured

156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143 KeyProcessAdd: Enter

157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144 KeyProcessAdd: Adding outbound SA

158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145 KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255, dst 10.32.0.0 mask 0.0.127.255

159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146 KeyProcessAdd: FilterIpsecAddIkeSa success

160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41 IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0, spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

```
164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147
Processing KEY_UPDATE msg!
165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148
Update inbound SA addresses
166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter
167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150
No USER filter configured
168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151
KeyProcessUpdate: Enter
169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152
KeyProcessUpdate: success
170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0x0df37959
171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547
pitcher: rcv KEY_UPDATE, spi 0x1234a593
172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157
Group [172.18.124.157]
PHASE 2 COMPLETED (msgid=54796f76)
```

Related Information

- Cisco VPN 3000 Series Concentrator Support Page
- Cisco VPN 3000 Series Client Support Page
- IPSec Support Page
- Technical Support 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: Sep 26, 2006

Document ID: 23786