NORTEL

TECHNICAL SUPPORT
TECHNICAL TIP

TT-0602402a | 24-Feb-2006

Nortel VPN Router – Cisco IOS branch office tunnel using pre-shared key authentication

Contents:

Introduction:

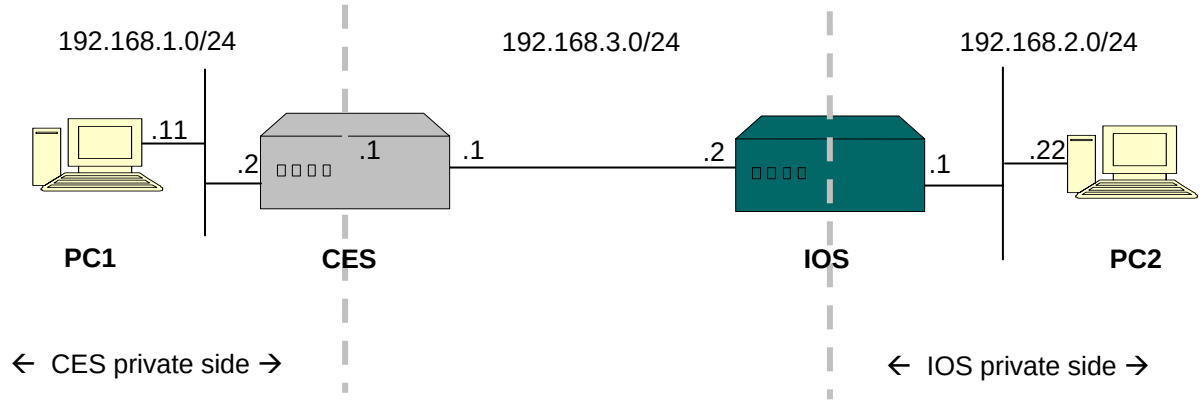
This document shows a sample configuration of an IPSec branch office tunnel between a Cisco IOS Router and a Nortel VPN Router using pre-shared key authentication.

Associated Products:

The information in this document is intended to be used with the following product(s) with the indicated software or hardware revisions:

Product Name or Order Number	Revision Information	
	Potentially Affected	*Corrected*
Nortel VPN Routers (formerly Contivity Secure IP Services Gateways): 1000, 1010, 1050, 1100, 1500, 1600, 1700, 1740, 1750, 2000, 2500, 2600, 2700, 4000, 4500, 4600, 5000, 600	All	N/A

Setup



PC1 – windows XP, IP address 192.168.1.11/24;
PC2 – windows XP, IP address 192.168.2.22/24;
CES – Nortel VPN Router, release version 5_05, management IP 192.168.1.1, private interface 192.168.1.2/24, public IP 192.168.3.1/24;
IOS – Cisco IOS router, version 12.0(28d), private interface IP 192.168.2.1/24, public interface IP 192.168.3.2/24.

The goal of the configuration is to configure a branch office tunnel between the CES and the IOS using pre-shared key authentication.

Configuring PC1

Configure the IP address on PC 1 (192.168.1.11) with CES private interface (192.168.1.2) as a default gateway.

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.11
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.2
```

Configuring PC2

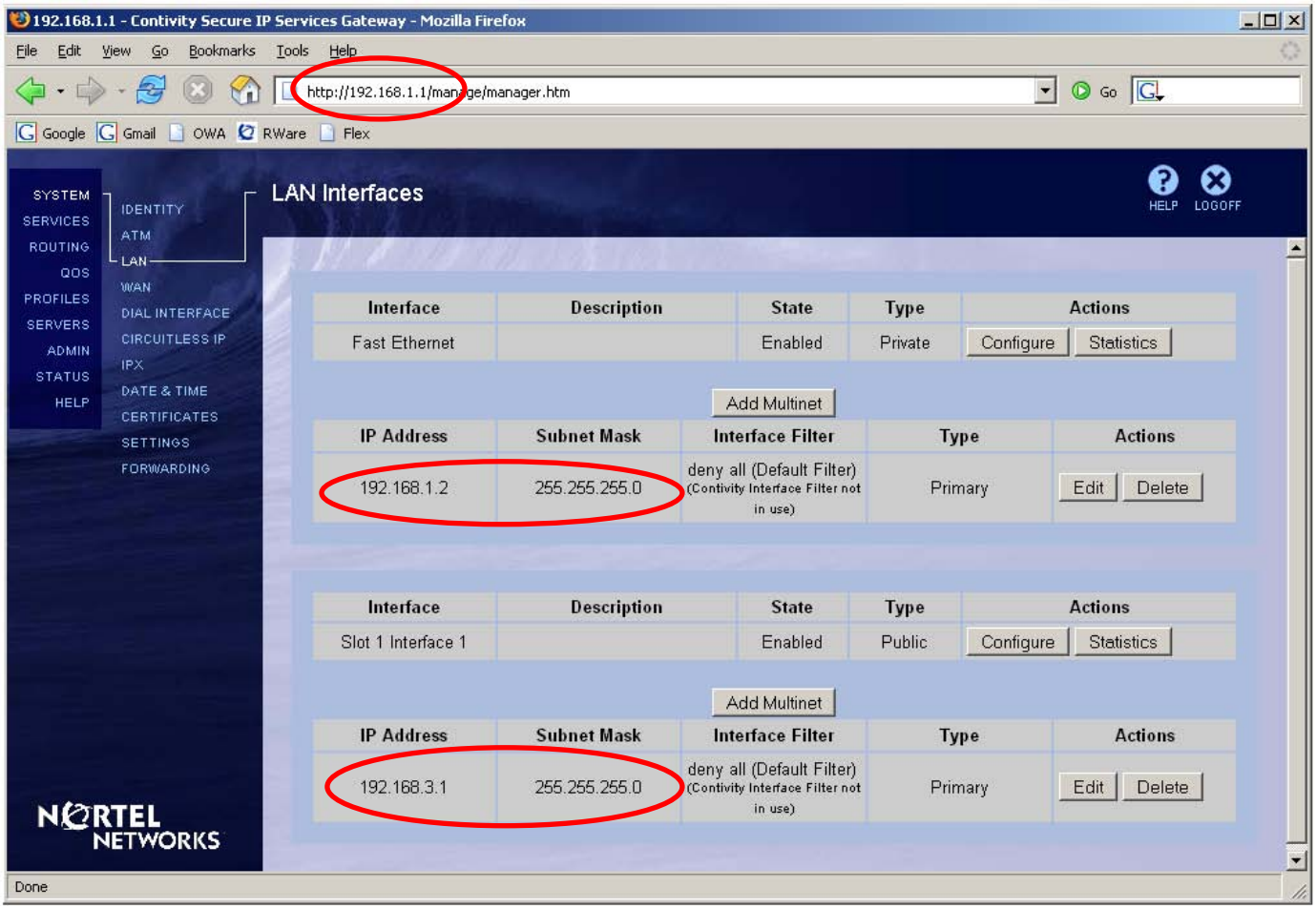
Configure the IP address on PC2 (192.168.2.22) with IOS private interface as a default gateway (192.168.2.1).

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Laptop-Eth:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.22
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.1
```

Configuring CES

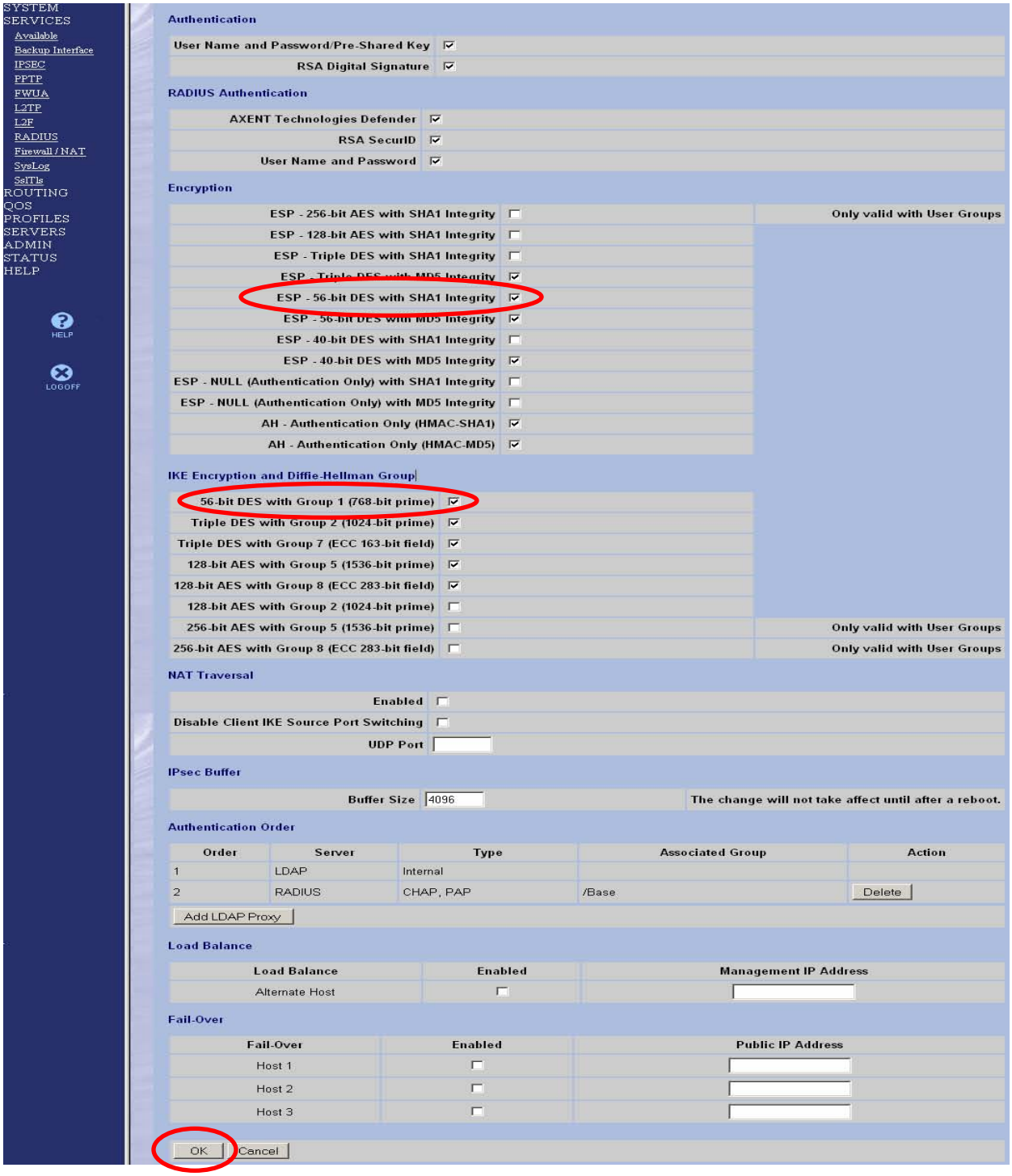
Configuring network parameters

Configure the IP addresses for the management (192.168.1.1), private (192.168.1.2) and public (192.168.3.1) interfaces.



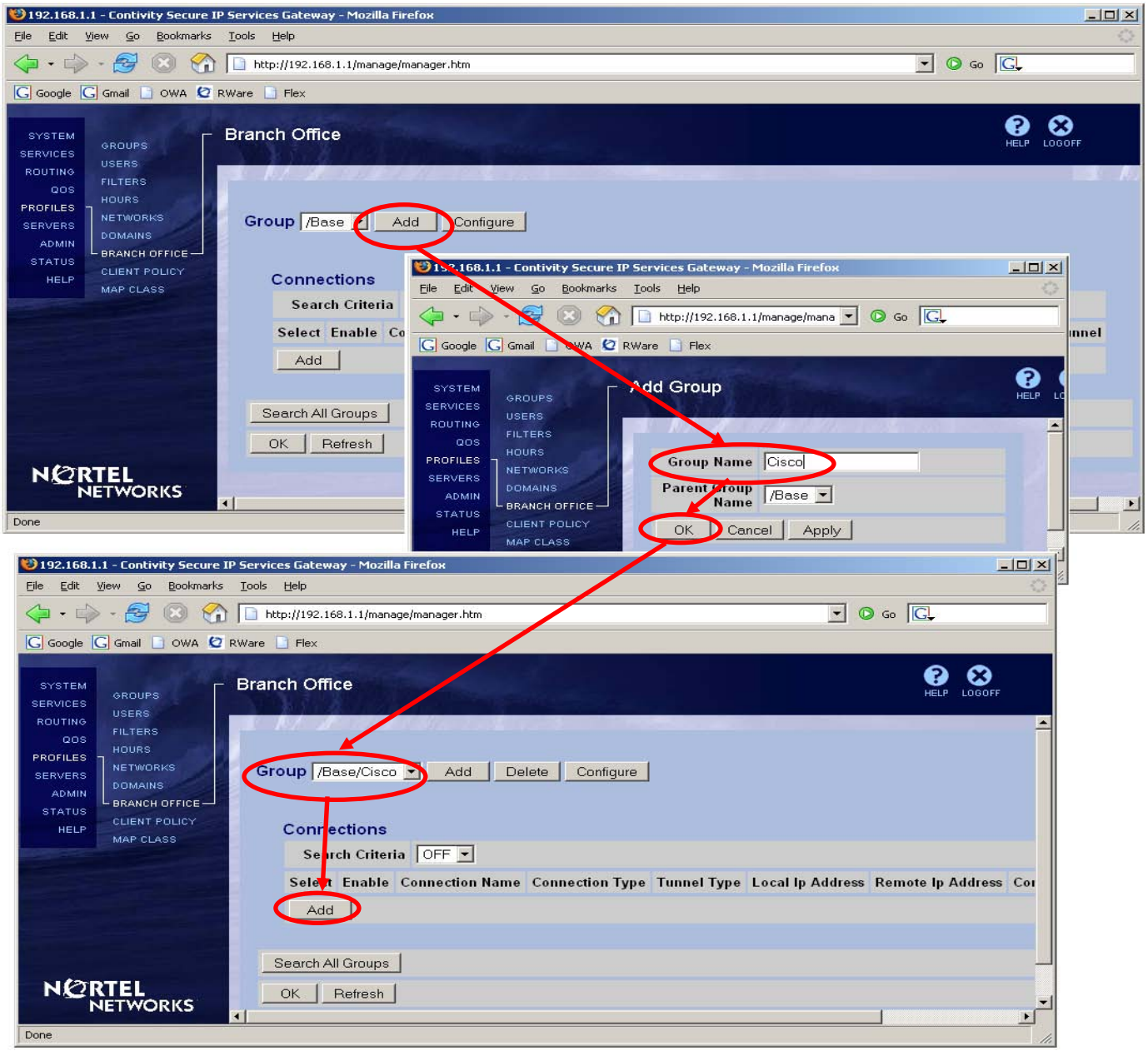
Configuring global IPSec parameters

In this example a tunnel is configured to use DES encryption with SHA-1 hashing algorithm and Diffie-Hellman group 1. In order to enable those parameters for the branch office later on, those parameters should be globally enabled first via the **Services→IPSec** screen. Check the box next to **ESP - 56-bit DES with SHA1 Integrity** and **56-bit DES with Group 1 (768-bit prime)**, once done, click **OK** at the bottom of the screen.

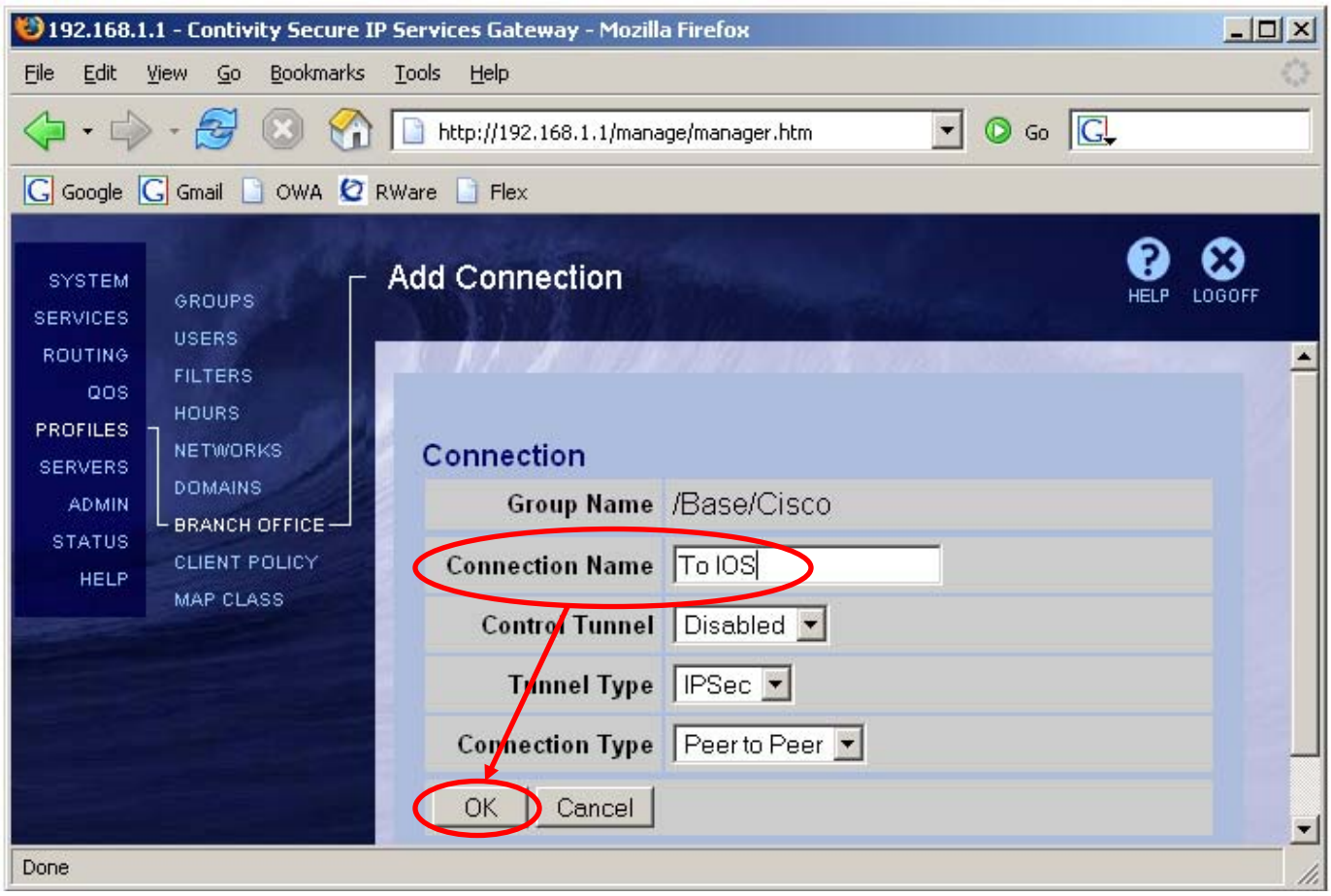


Configuring a branch office connection

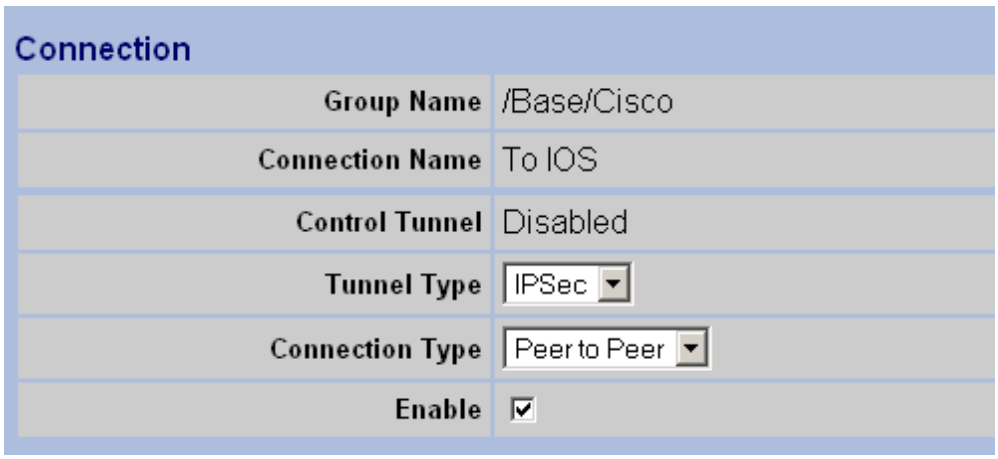
1. Navigate to **Profiles→Branch Office**
2. Create a new group for this tunnel.
   a) Next to **Group** select **Add.**
   b) **`Enter a name for the group`** (Cisco in this case) and click **OK.** A new group is created.
3. To create a new branch office connection for this group, under the **Connections** section select **Add.**



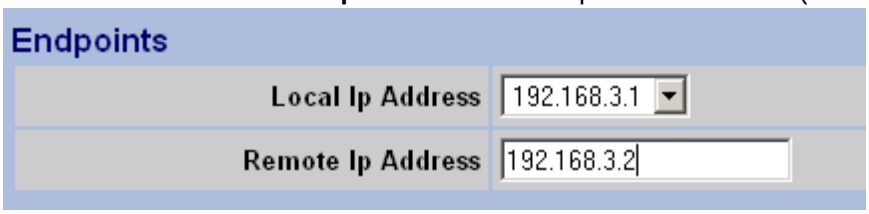
4. **`Enter a name for the connection`** (To IOS in this case), leave the rest of the fields at the default settings and select **OK.**



5. Check the box next to **Enable**.

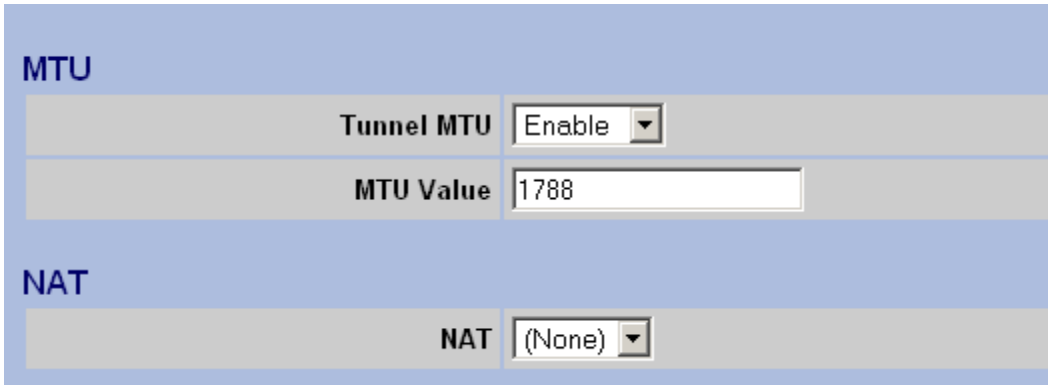


6. For the **Local Endpoint** select the CES public interface IP (192.168.3.1).
7. For the **Remote Endpoint** enter the IOS public interface IP (192.168.3.2).



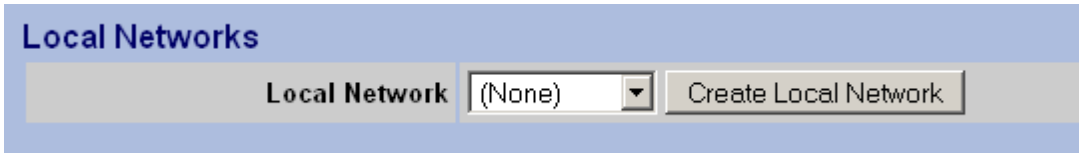
8. Leave the **Filter** as **permit all**.
9. Leave **Authentication** as **Text Pre-Shared Key.**
10. **`Enter and confirm the Text Pre-Shared Key`** ("test" was used in this example. The key should match the one configured on the IOS).

11. Leave **MTU** and **NAT** settings at the default settings.

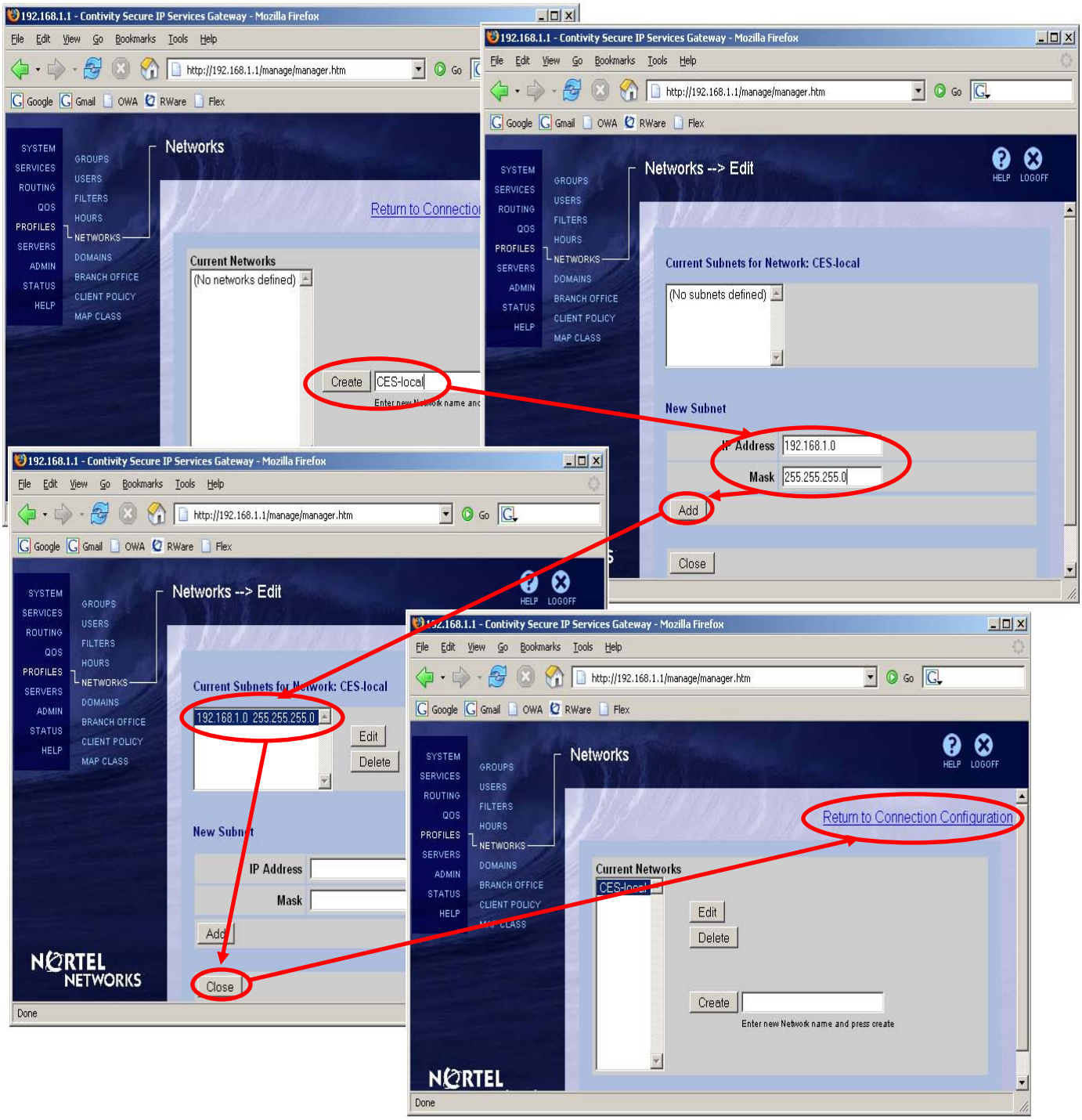


12. **Static** configuration is used in this example.

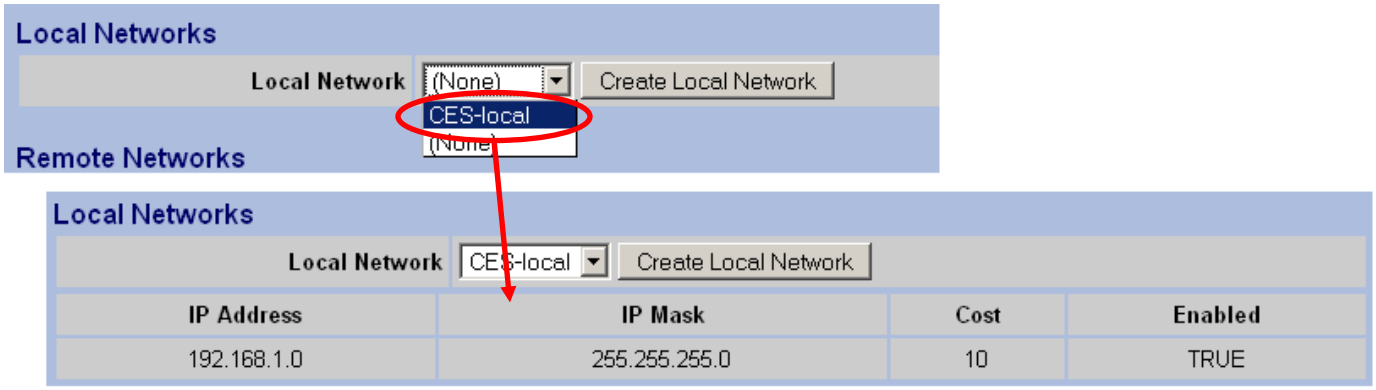
13. To create a local network definition click on **Create Local Network**.



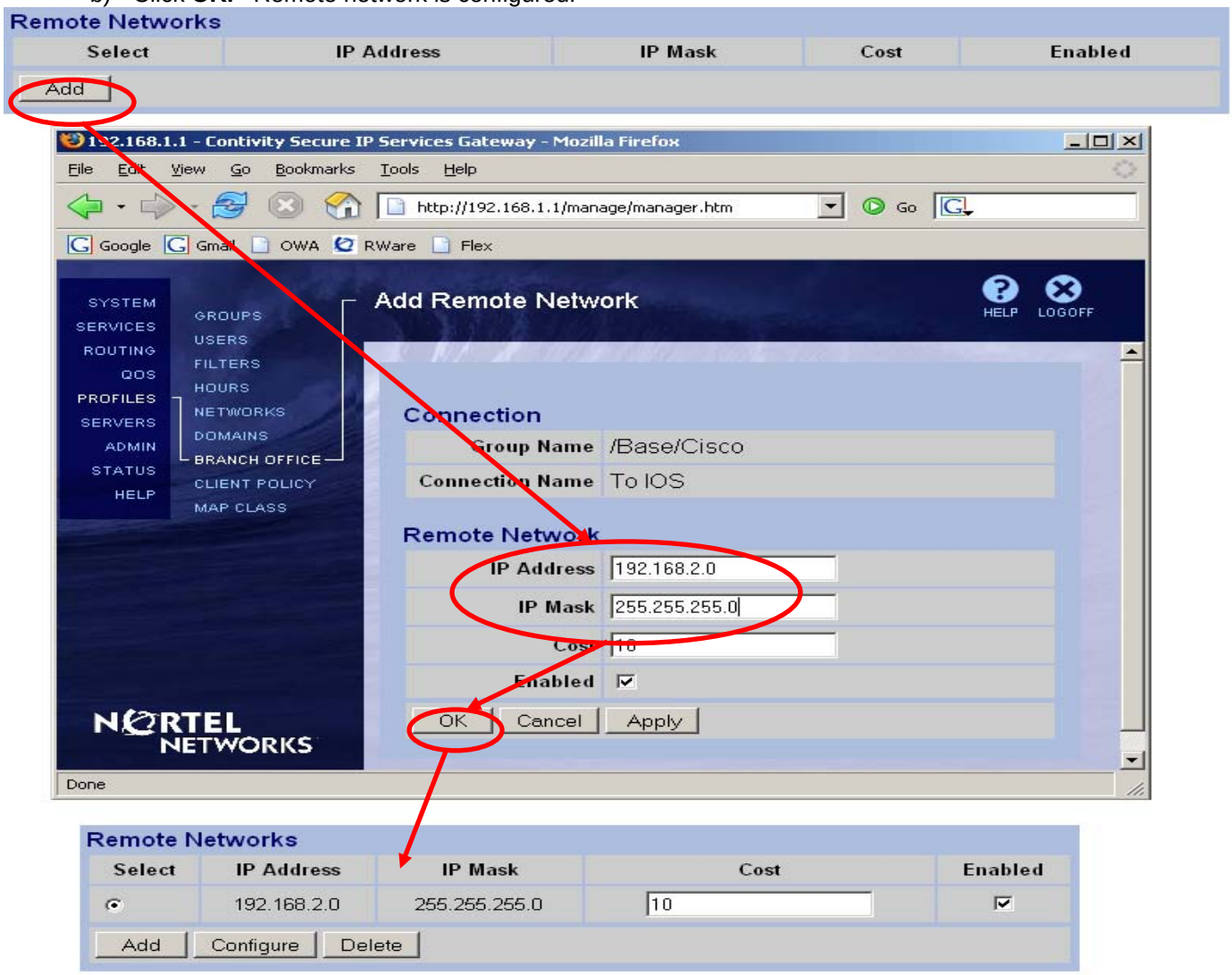
a) **`Enter a name for the local network`** (CES-local in this case) and select **Create**.
b) Enter an **IP Address** (192.168.1.0) and a **Mask** (255.255.255.0) for the private network.
c) Click **Add.**
d) Select **Close.**
e) To return to the branch office configuration, in the top-right corner click on the link.



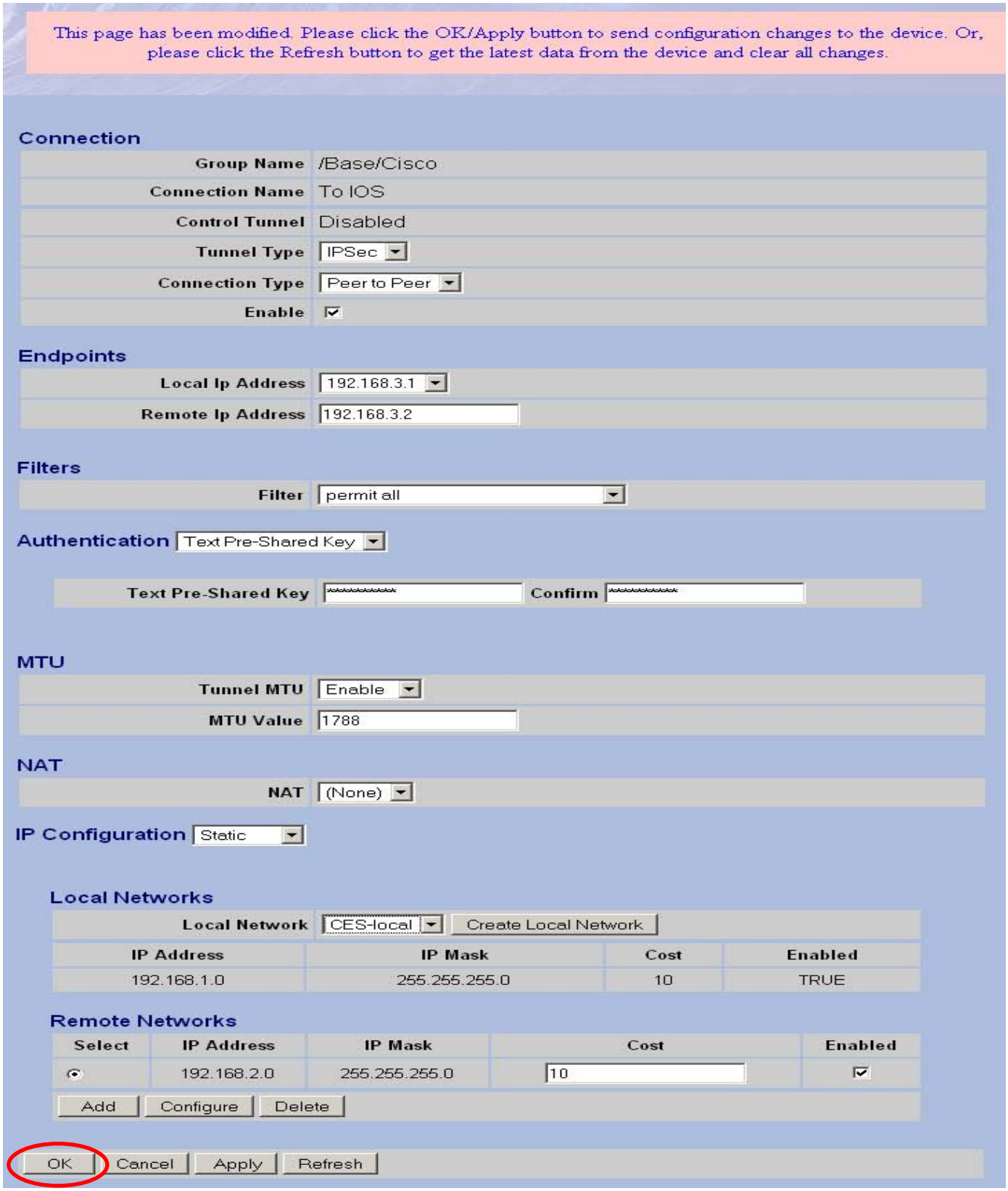
14. From the drop-down list next to **Local Network** select the **created local network**.
15. Screen refreshes showing the configured local network.



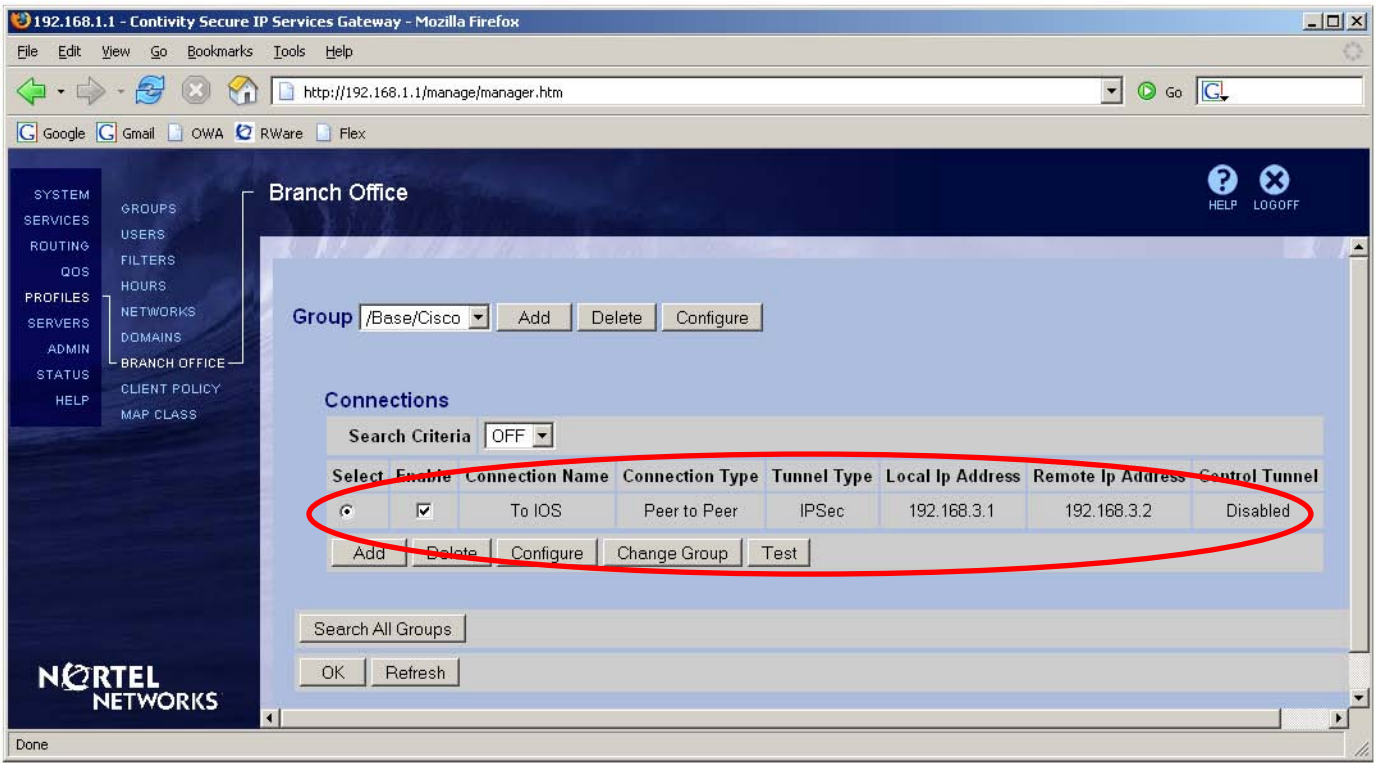
16. Under the **Remote Networks** section select **Add.**
    a) Enter the **IP Address** (192.168.2.0) and **Mask** (255.255.255.0) for the remotely accessible network.
    b) Click **OK.** Remote network is configured.



17. Once all the parameters are configured, at the bottom of the screen click **OK**.



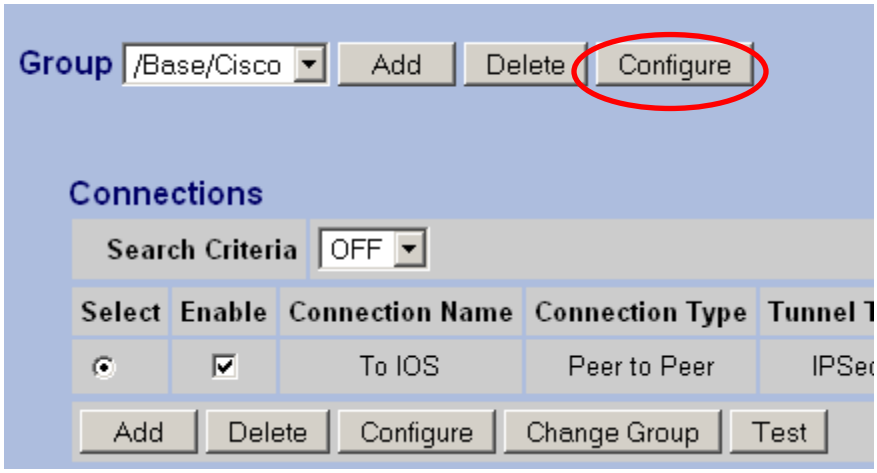
The tunnel connection is configured.



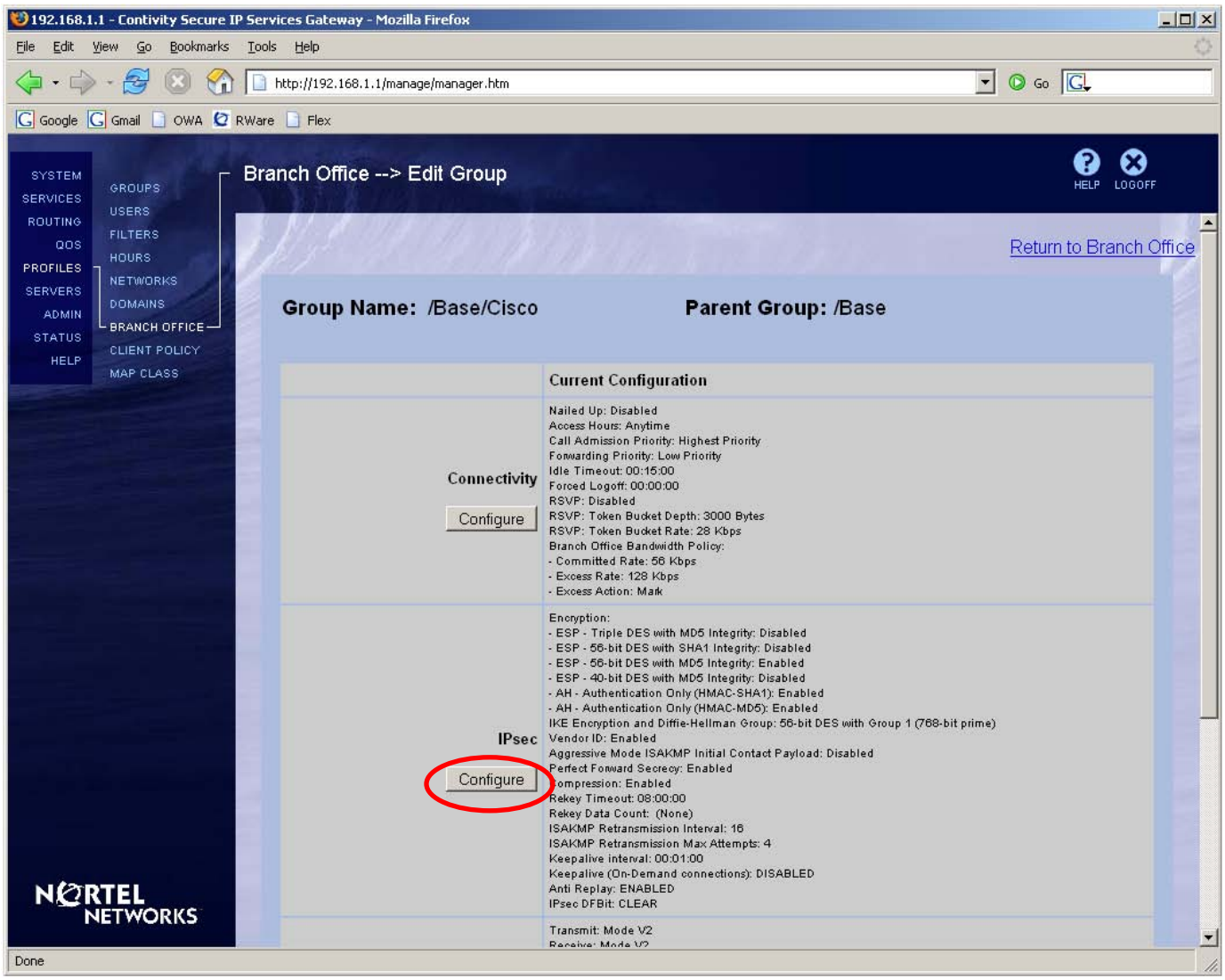
Configuring branch office group settings

This example shows how to establish a tunnel using DES/SHA-1 with Diffie-Hellman group 1, thus appropriate encryption parameters need to be enabled for this branch office group.

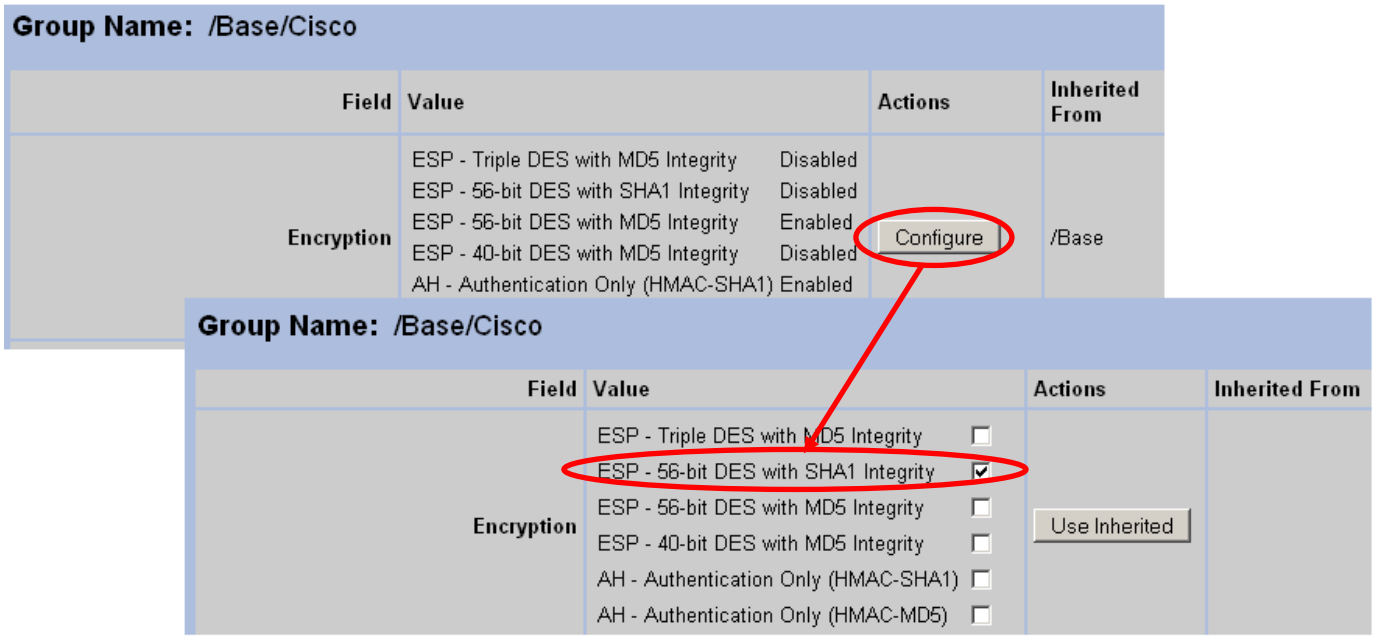
1. Next to the branch office group select**Configure**.



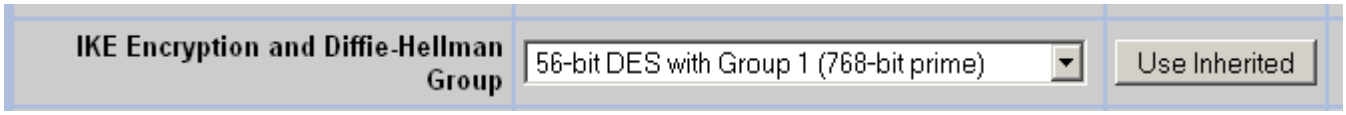
2. Scroll down to the **IPSec** settings and select **Configure**.



3. Next to **Encryption** click on **Configure.**
4. Check the box next to **ESP - 56-bit DES with SHA1 Integrity.**
5. For simplicity, Uncheck the rest.

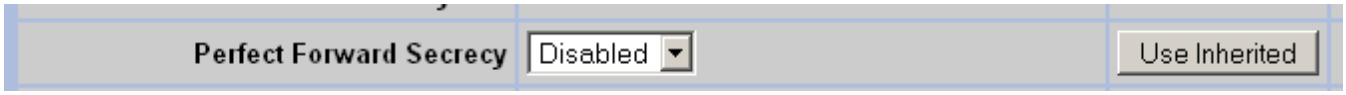


6. Select the appropriate **Diffie-Hellman** group (group 1 in this case).



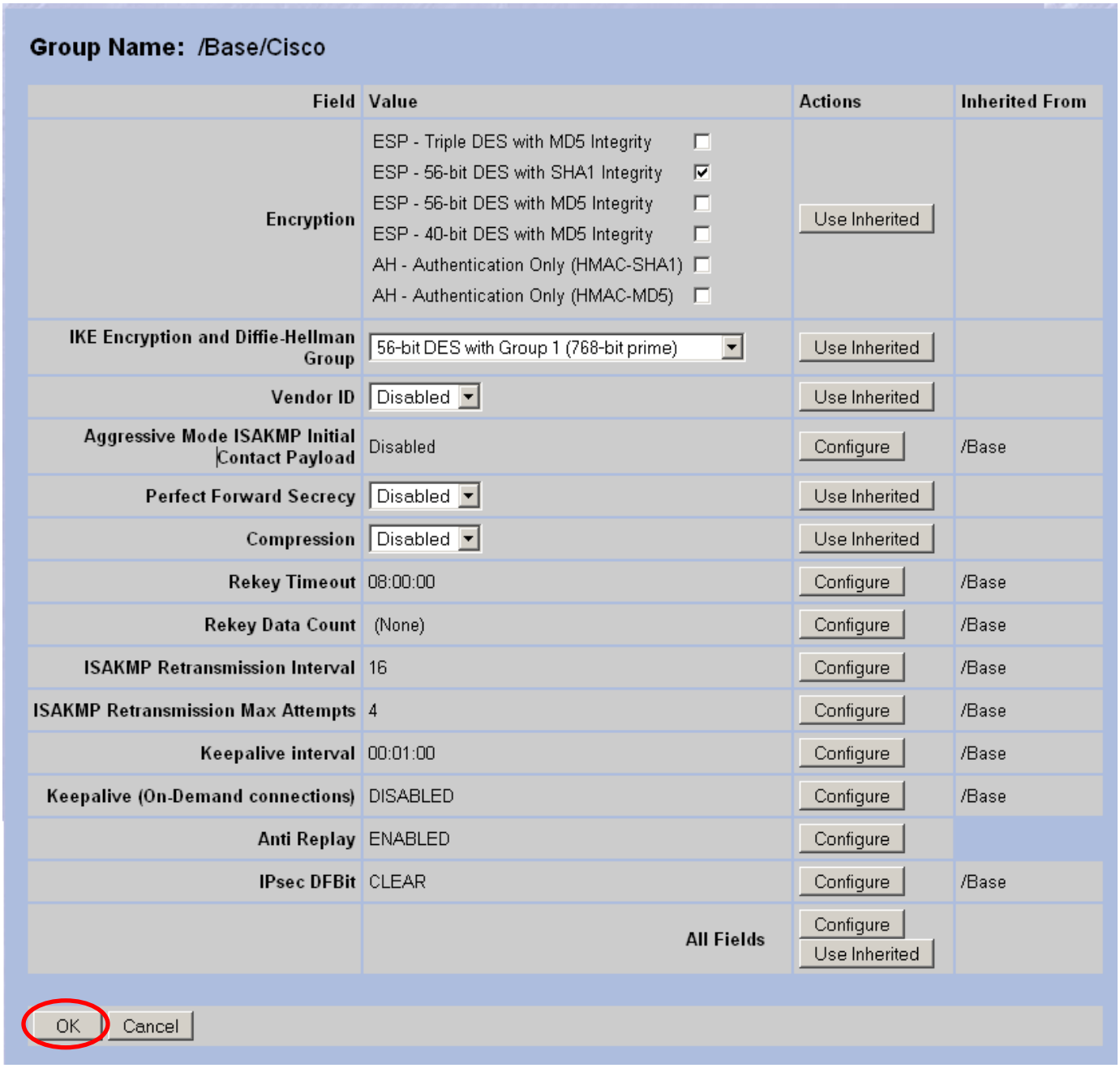
7. Disable the **Vendor ID** to avoid possible interoperability issues. Please note that this is just a sample configuration to get the tunnel going, it could always be adjusted later on to fit specific needs.

8. Disable **Perfect Forward Secrecy**.



9. Disable **Compression**.

10. The rest of the fields including the phase 2 rekey timer and keep-alive interval should be left at their default settings.
11. At the bottom of the screen click **OK**.



Group Name: /Base/Cisco

Field	Value	Actions	Inherited From
Encryption	ESP - Triple DES with MD5 Integrity ☐ ESP - 56-bit DES with SHA1 Integrity ☑ ESP - 56-bit DES with MD5 Integrity ☐ ESP - 40-bit DES with MD5 Integrity ☐ AH - Authentication Only (HMAC-SHA1) ☐ AH - Authentication Only (HMAC-MD5) ☐	Use Inherited	
IKE Encryption and Diffie-Hellman Group	56-bit DES with Group 1 (768-bit prime)	Use Inherited	
Vendor ID	Disabled	Use Inherited	
Aggressive Mode ISAKMP Initial Contact Payload	Disabled	Configure	/Base
Perfect Forward Secrecy	Disabled	Use Inherited	
Compression	Disabled	Use Inherited	
Rekey Timeout	08:00:00	Configure	/Base
Rekey Data Count	(None)	Configure	/Base
ISAKMP Retransmission Interval	16	Configure	/Base
ISAKMP Retransmission Max Attempts	4	Configure	/Base
Keepalive interval	00:01:00	Configure	/Base
Keepalive (On-Demand connections)	DISABLED	Configure	/Base
Anti Replay	ENABLED	Configure	
IPsec DFBit	CLEAR	Configure	/Base
	All Fields	Configure Use Inherited	

OK Cancel

CES is configured.

Configuring IOS

1. Connect to the Cisco router through the console and enter privileged mode.

```
Press RETURN to get started!

cisco>
cisco>en
cisco#
```

2. Enter configuration mode.

```
cisco#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cisco(config)#
```

3. Configure the IP address (192.168.2.1/24) for the private interface (Ethernet 0 in this case) and enable the interface.

```
cisco(config)#interface ethernet 0
cisco(config-if)#ip addr 192.168.2.1 255.255.255.0
cisco(config-if)#no shut
cisco(config-if)#exit
cisco(config)#
00:04:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to
up
```

4. Configure the IP address for the public interface (Ethernet 1 in this case) and enable the interface.

```
cisco(config)#interface ethernet 1
cisco(config-if)#ip address 192.168.3.2 255.255.255.0
cisco(config-if)#no shut
cisco(config-if)#exit
cisco(config)#
00:07:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1, changed state to
up
```

5. Define the IKE policy for phase 1 negotiations. ISAKMP crypto policy with priority number 7 is created in this example.

```
cisco(config)#crypto isakmp policy 7
cisco(config-isakmp)#
```

6. Set authentication to pre-shared key.

```
cisco(config-isakmp)#authentication pre-share
cisco(config-isakmp)#
```

7. Set the encryption level for phase 1. In this example DES encryption is used.

```
cisco(config-isakmp)#encryption des
cisco(config-isakmp)#
```

8. Set the appropriate Diffie-Hellman group to be used for phase 1. Diffie-Hellman group 1 is used in this example.

```
cisco(config-isakmp)#group 1
cisco(config-isakmp)#
```

9. Set the appropriate hashing algorithm. SHA-1 is used in this example:

```
cisco(config-isakmp)#hash sha
cisco(config-isakmp)#
```

10. Use the **lifetime** command to set the appropriate phase 1 SA lifetime. When selecting the value please keep in mind that the Nortel VPN Router does not support phase 1 rekeying. Therefore when it receives phase 1 rekey negotiation messages it will delete the tunnel completely, both phase 1 and phase 2 SAs. Cisco IOS on the other side, will only delete phase 1 SAs and will keep phase 2 SAs until they expire or are cleared manually, which could prevent a new tunnel from being established until the old phase 2 SAs are cleared from the Cisco box. It is recommended to set this timer to the highest possible level or disable it if the IOS version allows it. If there is a need for phase 1 renegotiations due to security reasons, use the **Forced Logoff** feature on the Nortel VPN Router (configured under the **Connectivity** section of branch office group) to ensure that the Nortel VPN Router is the one that initiates tunnel termination to avoid any issues with phase 1 rekeying. When configuring the Forced Logoff timer on the Nortel VPN router select a timer value smaller than the configured Cisco phase 1 lifetime. The goal of this configuration is to bring up the tunnel between Cisco and Nortel only, therefore lifetime is left at the default.

11. Exit the ISAKMP configuration menu.

```
cisco(config-isakmp)#exit
cisco(config)#
```

12. Configure the pre-shared key (“test” in this example) for authentication with the remote end (192.168.3.1).

```
cisco(config)#crypto isakmp key test address 192.168.3.1
cisco(config)#
```

13. Create an IPSec transform set. The transform set defines phase 2 parameters. Crypto set named ios-ces is created in this example with DES encryption and SHA1 hashing algorithm.

```
cisco(config)#crypto ipsec transform-set ios-ces esp-des esp-sha-hmac
cisco(cfg-crypto-trans)#exit
cisco(config)#
```

14. Create a static crypto map to tie together the ISAKMP and IPSec parameters for the tunnel. This map will be assigned to the public interface later in the configuration. Crypto map named ces-map will be created and associated with the earlier created ISAKMP crypto policy 7.

```
cisco(config)#crypto map ces-map 7 ipsec-isakmp
cisco(config-crypto-map)#
```

15. Set the remote peer IP address.

```
cisco(config-crypto-map)#set peer 192.168.3.1
cisco(config-crypto-map)#
```

16. Assign the created transform set to this map.

```
cisco(config-crypto-map)#set transform-set ios-ces
cisco(config-crypto-map)#
```

17. Set the access list to be associated with this tunnel. Access list defines local/remote accessible networks allowed to traverse the tunnel. In this example, networks defined by access list number 111 will be allowed to go through the tunnel. The list itself will be created later in this configuration.

```
cisco(config-crypto-map)#match address 111
cisco(config-crypto-map)#exit
cisco(config)#
```

18. Assign the created crypto map to the public interface.

```
cisco(config)#interface ethernet 1
cisco(config-if)#crypto map ces-map
cisco(config-if)# exit
cisco(config)#
```

19. Create an access list to allow traffic from the IOS private side (192.168.2.0/24) to the CES private side (192.168.1.0/24). Note that the mask is defined as wildcard bits. Significant bits are denoted by 0 and insignificant by 1.

```
cisco(config)#access-list 111 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

20. Add a route for the remote accessible network (192.168.1.0) pointing to the CES public IP and exit the configuration menu.

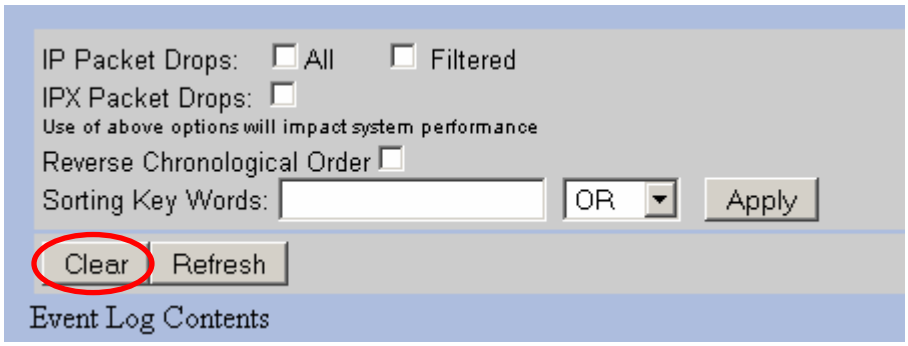
```
cisco(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
cisco(config)#exit
cisco#
03:03:11: %SYS-5-CONFIG_I: Configured from console by console
```

21. Save the configuration.

```
cisco#write mem
Building configuration...
[OK]
cisco#
```

Testing the configuration

1. Clear the log on the CES from the **Status→Event Log** screen.



2. Ping from PC1 to PC2. The first ping is lost as the tunnel is not established yet. The subsequent requests go through as the tunnel gets established.

```
C:\>ping 192.168.2.22

Pinging 192.168.2.22 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.22: bytes=32 time=18ms TTL=254
Reply from 192.168.2.22: bytes=32 time=18ms TTL=254
Reply from 192.168.2.22: bytes=32 time=18ms TTL=254

Ping statistics for 192.168.2.22:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 18ms, Average = 18ms


C:\>
```

3. Check the log on the CES.

```
02/22/2006 09:05:08 0 Branch Office [01] IPSEC branch office connection initiated to
rem[192.168.2.0-255.255.255.0]@[192.168.3.2] loc[192.168.1.0-255.255.255.0]
02/22/2006 09:05:08 0 Security [11] Session: IPSEC[192.168.3.2] attempting login
02/22/2006 09:05:08 0 Security [01] Session: IPSEC[192.168.3.2] has no active sessions
02/22/2006 09:05:08 0 Security [01] Session: IPSEC[192.168.3.2] To IOS has no active
accounts
02/22/2006 09:05:08 0 Security [00] Session: IPSEC - found matching gateway session,
caching parameters from gateway session
02/22/2006 09:05:11 0 Security [01] Session: IPSEC[192.168.3.2]:12 SHARED-SECRET
authenticate attempt...
02/22/2006 09:05:11 0 Security [01] Session: IPSEC[192.168.3.2]:12 attempting
authentication using LOCAL
02/22/2006 09:05:11 0 Security [11] Session: IPSEC[192.168.3.2]:12 authenticated using
LOCAL
02/22/2006 09:05:11 0 Security [11] Session: IPSEC[192.168.3.2]:12 bound to group
/Base/Cisco/To IOS
02/22/2006 09:05:11 0 Security [01] Session: IPSEC[192.168.3.2]:12 Building group
filter permit all
02/22/2006 09:05:12 0 Security [01] Session: IPSEC[192.168.3.2]:12 Applying group
filter permit all
02/22/2006 09:05:12 0 Security [11] Session: IPSEC[192.168.3.2]:12 authorized
02/22/2006 09:05:12 0 Security [11] Session: network IPSEC[192.168.2.0-255.255.255.0]
```

```
attempting login
02/22/2006 09:05:12 0 Security [11] Session: network IPSEC[192.168.2.0-255.255.255.0]
logged in from gateway [192.168.3.2]
02/22/2006 09:05:12 0 ISAKMP [02] ISAKMP SA established with 192.168.3.2
02/22/2006 09:05:12 0 Security [12] Session: IPSEC[192.168.3.2]:12 physical addresses:
remote 192.168.3.2 local 192.168.3.1
02/22/2006 09:05:12 0 Security [12] Session: IPSEC[-]:13 physical addresses: remote
192.168.3.2 local 192.168.3.1
02/22/2006 09:05:12 0 Outbound ESP from 192.168.3.1 to 192.168.3.2 SPI 0x1e200c92 [03]
ESP encap session SPI 0x920c201e bound to s/w on cpu 0
02/22/2006 09:05:12 0 Inbound ESP from 192.168.3.2 to 192.168.3.1 SPI 0xf82eb5aa [03]
ESP decap session SPI 0xaab52ef8 bound to s/w on cpu 0
02/22/2006 09:05:12 0 Branch Office [00] 7451268 BranchOfficeCtxtCls::RegisterTunnel:
rem[192.168.2.0-255.255.255.0]@[192.168.3.2] loc[192.168.1.0-255.255.255.0]
overwriting tunnel context [ffffffff] with [5369cd8]
02/22/2006 09:05:12 0 ISAKMP [03] Established IPsec SAs with 192.168.3.2:
02/22/2006 09:05:12 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA outbound SPI 0x1e200c92
02/22/2006 09:05:12 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA inbound SPI 0xf82eb5aa
```

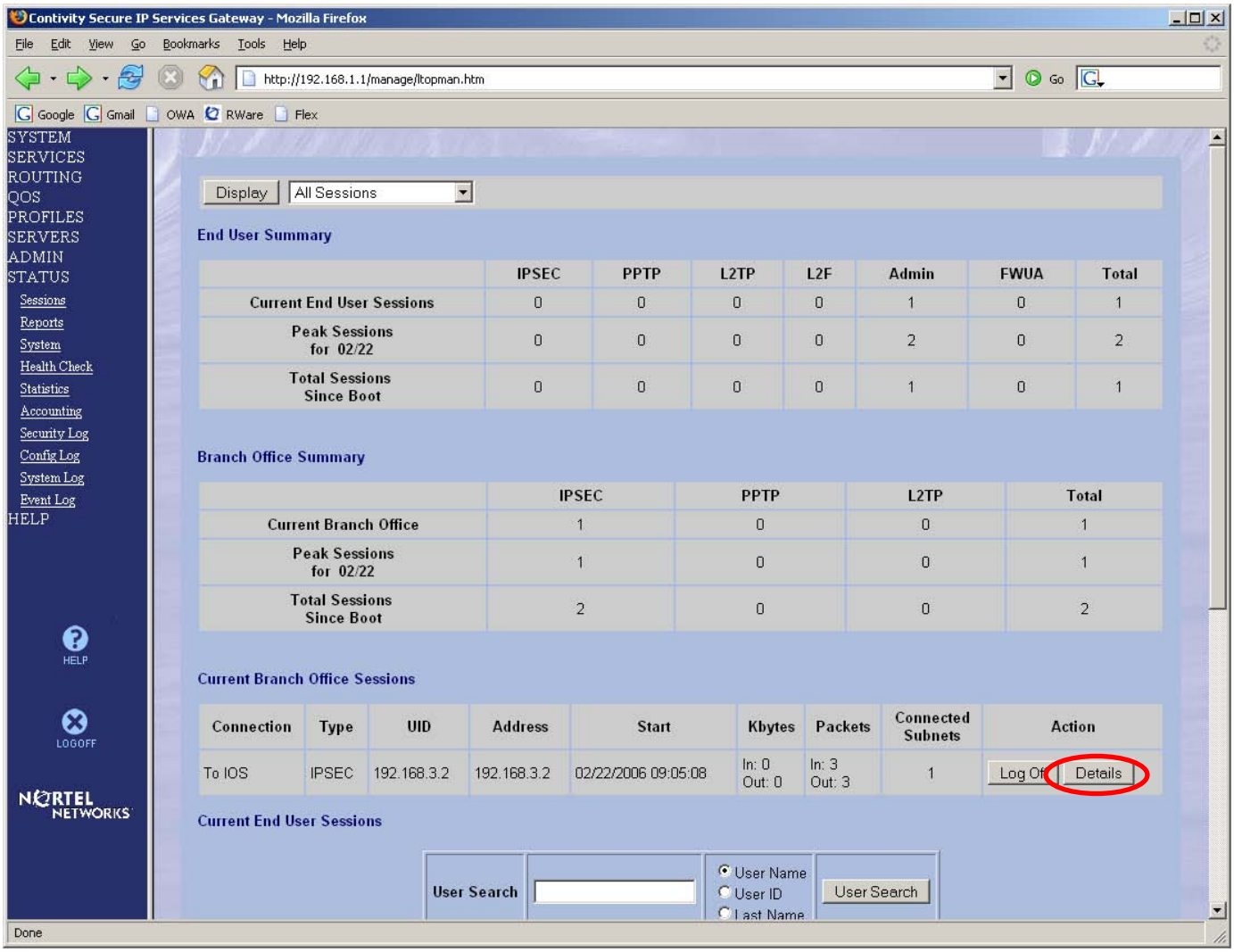
4. Check the established ISAKMP SAs on the IOS.

```
cisco#show crypto isakmp sa
    dst             src          state        conn-id   slot
192.168.3.2    192.168.3.1    QM IDLE           27    0
cisco#
```

5. Check the established IPSec SAs on the IOS.

```
cisco#show crypto ipsec sa

interface: Ethernet0
    Crypto map tag: ces-map, local addr. 192.168.3.2

   local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current peer: 192.168.3.1
     PERMIT, flags={origin is acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
    #pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.3.2, remote crypto endpt.: 192.168.3.1
     path mtu 1500, media mtu 1500
     current outbound spi: F82EB5AA

     inbound esp sas:
      spi: 0x1E200C92(505416850)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 28, crypto map: ces-map
        sa timing: remaining key lifetime (k/sec): (4607999/3362)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:


     outbound esp sas:
      spi: 0xF82EB5AA(4163810730)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 29, crypto map: ces-map
        sa timing: remaining key lifetime (k/sec): (4607999/3362)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:



cisco#
```

6. Check the details for the established tunnel on the CES. On the **Status→Sessions** screen, next to the branch office tunnel select **Details**.



7. Tunnel session details are displayed.

```
Date:  02/22/2006  Time: 09:16:34

  Name:  To IOS
  Account Type:  IPSEC
  Number of Sessions:  1
   Session Subnet:  192.168.2.0 - 255.255.255.0
   Session Start Date:  02/22/2006
   Session Start Time:  09:05:12
   Session Total KBytes In:  0
   Session Total KBytes Out:  0
   Session Total Packets In:  5
   Session Total Packets Out:  5
   Session Filter Drops In:  0
   Session Filter Drops Out:  0
   Session Total QosRandom Drops In:  0
   Session QosRandom Drops Out:  0
   Session QosForced Drops In:  0
   Session Total QosForced Drops Out:  0
   Session IpHdr Drops In:  0
```

```
   Session IpHdr Drops Out:  0
   Session IpFrags In:  0
   Session IpFrags Out:  0
   Session IpFrag Drops In:  0
   Session IpFrag Drops Out:  0
   Session BWM Configured Committed Rate Kbps:  56
   Session BWM Runtime Committed Rate Kbps:  56
   Session BWM In-Profile KBytes:  0
   Session BWM Out-Of-Profile KBytes:  0

ISAKMP security association established with 192.168.3.2
Local address: 192.168.3.1
Local Udp Port:500  Remote port:500
Initiator cookie: CBB32457360A7B03
Responder cookie: EE79234F9285F1AA
IKE encryption: 56-bit DES with Diffie-Hellman group 1 (MODP 768-bit prime)
IKE Keepalive: Disabled.

IPSec tunnel mode security associations established:
Local subnet 192.168.1.0 mask 255.255.255.0
Remote subnet 192.168.2.0 mask 255.255.255.0
  ESP 56-bit DES-CBC-HMAC-SHA outbound SPI 0x1E200C92  software session
    5 packets sent
  ESP 56-bit DES-CBC-HMAC-SHA inbound SPI 0xF82EB5AA  software session
    5 packets successfully received
    0 packets truncated
    0 packets failed replay check
    0 packets failed authentication
    0 packets with invalid pad length (decryption failure)
  Expires on WED FEB 22 10:05:12 2006
```

8. Terminate the tunnel from the CES or the IOS side. The tunnel can be terminated from the CES side by logging off the tunnel from the GUI or CLI. To log off the tunnel from the GUI navigate to the **Status→Sessions** screen, locate the branch office session and next to it select **Log Off** . To log off a tunnel from the CLI use the **forced-logoff bo-conn "connection name" "group"** syntax, for example to log off "To IOS" tunnel that belongs to the /Base/Cisco group.

```
CES#forced-logoff bo-conn "To IOS" "/Base/Cisco"
CES#
```

9. Check the event log messages.

```
02/22/2006 09:20:10 0 ISAKMP [13] 192.168.3.2 logged off by administrator
02/22/2006 09:20:10 0 ISAKMP [03] Deleting IPsec SAs with 192.168.3.2:
02/22/2006 09:20:10 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA outbound SPI 0x1e200c92
02/22/2006 09:20:10 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA inbound SPI 0xf82eb5aa
02/22/2006 09:20:10 0 IPvfy.05369cd8{Tun} [00] destructor called 0x5369cd8
02/22/2006 09:20:10 0 Security [12] Session 6d82d00: IPSEC[-]:13 sib 0 logged out
02/22/2006 09:20:10 0 Security [12] Session 6d82328: IPSEC[192.168.3.2]:12 sib 0
logged out
02/22/2006 09:20:10 0 ISAKMP [02] Deleting ISAKMP SA with 192.168.3.2
```

10. Initiate the tunnel from PC2 to PC1 this time by sending a ping.

```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.11: bytes=32 time=18ms TTL=254
Reply from 192.168.1.11: bytes=32 time=18ms TTL=254
Reply from 192.168.1.11: bytes=32 time=18ms TTL=254

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 18ms, Average = 18ms

C:\>
```

11. Check the event log messages on the CES.

```
02/22/2006 09:23:50 0 Security [11] Session: IPSEC[192.168.3.2] attempting login
02/22/2006 09:23:50 0 Security [01] Session: IPSEC[192.168.3.2] has no active sessions
02/22/2006 09:23:50 0 Security [01] Session: IPSEC[192.168.3.2] To IOS has no active
accounts
02/22/2006 09:23:50 0 Security [00] Session: IPSEC - found matching gateway session,
caching parameters from gateway session
02/22/2006 09:23:50 0 ISAKMP [02] Oakley Main Mode proposal accepted from 192.168.3.2
02/22/2006 09:23:54 0 Security [01] Session: IPSEC[192.168.3.2]:14 SHARED-SECRET
authenticate attempt...
02/22/2006 09:23:54 0 Security [01] Session: IPSEC[192.168.3.2]:14 attempting
authentication using LOCAL
02/22/2006 09:23:54 0 Security [11] Session: IPSEC[192.168.3.2]:14 authenticated using
LOCAL
02/22/2006 09:23:54 0 Security [11] Session: IPSEC[192.168.3.2]:14 bound to group
/Base/Cisco/To IOS
02/22/2006 09:23:54 0 Security [01] Session: IPSEC[192.168.3.2]:14 Building group
filter permit all
02/22/2006 09:23:54 0 Security [01] Session: IPSEC[192.168.3.2]:14 Applying group
filter permit all
02/22/2006 09:23:54 0 Security [11] Session: IPSEC[192.168.3.2]:14 authorized
02/22/2006 09:23:54 0 ISAKMP [02] ISAKMP SA established with 192.168.3.2
02/22/2006 09:23:54 0 Security [11] Session: network IPSEC[192.168.2.0-255.255.255.0]
attempting login
02/22/2006 09:23:54 0 Security [11] Session: network IPSEC[192.168.2.0-255.255.255.0]
logged in from gateway [192.168.3.2]
02/22/2006 09:23:54 0 Security [12] Session: IPSEC[192.168.3.2]:14 physical addresses:
remote 192.168.3.2 local 192.168.3.1
02/22/2006 09:23:54 0 Security [12] Session: IPSEC[-]:15 physical addresses: remote
192.168.3.2 local 192.168.3.1
02/22/2006 09:23:54 0 Outbound ESP from 192.168.3.1 to 192.168.3.2 SPI 0x1be801cf [03]
ESP encap session SPI 0xcf01e81b bound to s/w on cpu 0
02/22/2006 09:23:54 0 Inbound ESP from 192.168.3.2 to 192.168.3.1 SPI 0x457fc722 [03]
ESP decap session SPI 0x22c77f45 bound to s/w on cpu 0
02/22/2006 09:23:54 0 Branch Office [00] 7451268 BranchOfficeCtxtCls::RegisterTunnel:
rem[192.168.2.0-255.255.255.0]@[192.168.3.2] loc[192.168.1.0-255.255.255.0]
overwriting tunnel context [0] with [5369cd8]
02/22/2006 09:23:54 0 ISAKMP [03] Established IPsec SAs with 192.168.3.2:
02/22/2006 09:23:54 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA outbound SPI 0x1be801cf
02/22/2006 09:23:54 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA inbound SPI 0x457fc722
```

12. Check the ISAKMP SA on the IOS.

```
cisco#show crypto isakmp sa
    dst             src          state        conn-id   slot
192.168.3.1    192.168.3.2    QM IDLE           30    0

cisco#
```

13. Check the IPSec SA on the IOS.

```
cisco#show crypto ipsec sa

interface: Ethernet0
    Crypto map tag: ces-map, local addr. 192.168.3.2

   local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer: 192.168.3.1
     PERMIT, flags={origin is acl,}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
    #send errors 3, #recv errors 0

     local crypto endpt.: 192.168.3.2, remote crypto endpt.: 192.168.3.1
     path mtu 1500, media mtu 1500
     current outbound spi: 457FC722

     inbound esp sas:
      spi: 0x1BE801CF(468189647)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 31, crypto map: ces-map
        sa timing: remaining key lifetime (k/sec): (4607999/3383)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:


     outbound esp sas:
      spi: 0x457FC722(1166001954)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 32, crypto map: ces-map
        sa timing: remaining key lifetime (k/sec): (4607999/3383)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:



cisco#
```

14. Terminate the tunnel from the IOS side by clearing all the Sas.

```
cisco#clear crypto sa
cisco#clear crypto isakmp
```

15. Cisco debug functionality can be used to troubleshoot tunnel establishment issues. To view available tunnel debug options type debug crypto followed by a question mark.

```
cisco#debug crypto ?
  engine        Crypto Engine Debug
  ipsec         IPSEC processing
  isakmp        ISAKMP Key Management
  key-exchange  Key Exchanger
  pki           PKI Client
  sessmgmt      Session Management

cisco#
```

Below is a sample output of a successful tunnel establishment when the tunnel was initiated from the CES (**debug crypto ipsec** and **debug crypto isakmp** were enabled on the IOS).

```
22:17:08: ISAKMP (0): received packet from 192.168.3.1 (N) NEW SA
22:17:08: ISAKMP (33): processing SA payload. message ID = 0
22:17:08: ISAKMP (33): Checking ISAKMP transform 1 against priority 7 policy
22:17:08: ISAKMP:      encryption DES-CBC
22:17:08: ISAKMP:      hash SHA
22:17:08: ISAKMP:      auth pre-share
22:17:08: ISAKMP:      default group 1
22:17:08: ISAKMP (33): atts are acceptable. Next payload is 3
22:17:09: ISAKMP (33): SA is doing pre-shared key authentication using id type
ID_IPV4_ADDR
22:17:09: ISAKMP (33): sending packet to 192.168.3.1 (R) MM SA SETUP
22:17:09: ISAKMP (33): received packet from 192.168.3.1 (R) MM SA SETUP
22:17:09: ISAKMP (33): processing KE payload. message ID = 0
22:17:12: ISAKMP (33): processing NONCE payload. message ID = 0
22:17:12: ISAKMP (33): SKEYID state generated
22:17:12: ISAKMP (33): sending packet to 192.168.3.1 (R) MM KEY EXCH
22:17:12: ISAKMP (33): received packet from 192.168.3.1 (R) MM KEY EXCH
22:17:12: ISAKMP (33): processing ID payload. message ID = 0
22:17:12: ISAKMP (33): processing HASH payload. message ID = 0
22:17:12: ISAKMP (33): processing NOTIFY payload 24578 protocol 1
      spi 0, message ID = 0
22:17:12: ISAKMP (33): SA has been authenticated with 192.168.3.1
22:17:12: ISAKMP (33): ID payload
      next-payload : 8
      type         : 1
      protocol     : 17
      port         : 500
      length       : 8
22:17:12: ISAKMP (33): Total payload length: 12
22:17:12: ISAKMP (33): sending packet to 192.168.3.1 (R) QM IDLE
22:17:12: ISAKMP (33): received packet from 192.168.3.1 (R) QM IDLE
22:17:12: ISAKMP (33): processing SA payload. message ID = 716182161
22:17:12: ISAKMP (33): Checking IPSec proposal 1
22:17:12: ISAKMP: transform 1, ESP DES
22:17:12: ISAKMP:   attributes in transform:
22:17:12: ISAKMP:      authenticator is HMAC-SHA
22:17:12: ISAKMP:      encaps is 1
22:17:12: ISAKMP:      SA life type in seconds
22:17:12: ISAKMP:      SA life duration (VPI) of  0x0 0x0 0x70 0x80
22:17:12: ISAKMP (33): atts are acceptable.
22:17:12: IPSEC(validate_proposal_request): proposal part #1,
```

```
  (key eng. msg.) dest= 192.168.3.2, src= 192.168.3.1,
    dest proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    src proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn id= 0, keysize= 0, flags= 0x4
22:17:12: ISAKMP (33): processing NONCE payload. message ID = 716182161
22:17:12: ISAKMP (33): processing ID payload. message ID = 716182161
22:17:12: ISAKMP (33): ID IPV4 ADDR SUBNET src 192.168.1.0/255.255.255.0 prot 0 port 0
22:17:12: ISAKMP (33): processing ID payload. message ID = 716182161
22:17:12: ISAKMP (33): ID IPV4 ADDR SUBNET dst 192.168.2.0/255.255.255.0 prot 0 port 0
22:17:12: IPSEC(key engine): got a queue event...
22:17:12: IPSEC(spi response): getting spi 150932376 for SA
      from 192.168.3.1     to 192.168.3.2     for prot 3
22:17:12: ISAKMP (33): sending packet to 192.168.3.1 (R) QM IDLE
22:17:12: ISAKMP (33): received packet from 192.168.3.1 (R) QM IDLE
22:17:12: ISAKMP (33): Creating IPSec SAs
22:17:12:         inbound SA from 192.168.3.1     to 192.168.3.2     (proxy
192.168.1.0     to 192.168.2.0    )
22:17:12:         has spi 150932376 and conn id 34 and flags 4
22:17:12:         lifetime of 28800 seconds
22:17:12:         outbound SA from 192.168.3.2     to 192.168.3.1     (proxy
192.168.2.0     to 192.168.1.0    )
22:17:12:         has spi 403272119 and conn id 35 and flags 4
22:17:12:         lifetime of 28800 seconds
22:17:12: IPSEC(key engine): got a queue event...
22:17:12: IPSEC(initialize sas): ,
  (key eng. msg.) dest= 192.168.3.2, src= 192.168.3.1,
    dest proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    src proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 28800s and 0kb,
    spi= 0x8FF0B98(150932376), conn id= 34, keysize= 0, flags= 0x4
22:17:12: IPSEC(initialize sas): ,
  (key eng. msg.) src= 192.168.3.2, dest= 192.168.3.1,
    src proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    dest proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 28800s and 0kb,
    spi= 0x180971B7(403272119), conn id= 35, keysize= 0, flags= 0x4
22:17:12: IPSEC(create sa): sa created,
  (sa) sa dest= 192.168.3.2, sa prot= 50,
    sa_spi= 0x8FF0B98(150932376),
    sa trans= esp-des esp-sha-hmac , sa conn id= 34
22:17:12: IPSEC(create sa): sa created,
  (sa) sa dest= 192.168.3.1, sa prot= 50,
    sa spi= 0x180971B7(403272119),
    sa trans= esp-des esp-sha-hmac , sa conn id= 35
cisco#
```

Below are log off messages when the CES initiates tunnel termination.

```
22:18:12: ISAKMP (33): received packet from 192.168.3.1 (R) QM IDLE
22:18:12: ISAKMP (33): processing DELETE payload. message ID = 1150167001
22:18:12: IPSEC(key_engine): got a queue event...
22:18:12: IPSEC(key engine delete sas): rec'd delete notify from ISAKMP
22:18:12: IPSEC(key engine delete sas): delete SA with spi 403272119/50 for
192.168.3.1
22:18:12: IPSEC(delete sa): deleting SA,
  (sa) sa dest= 192.168.3.2, sa prot= 50,
    sa spi= 0x8FF0B98(150932376),
    sa trans= esp-des esp-sha-hmac , sa conn id= 34
22:18:12: IPSEC(delete sa): deleting SA,
  (sa) sa dest= 192.168.3.1, sa prot= 50,
    sa spi= 0x180971B7(403272119),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 35
22:18:12: ISAKMP (33): received packet from 192.168.3.1 (R) QM IDLE
22:18:12: ISAKMP (33): processing DELETE payload. message ID = -1125201820
22:18:12: ISAKMP (33): deleting SA
cisco#
```

Messages below show tunnel establishment initiated from the IOS.

```
22:19:49: IPSEC(sa request): ,
  (key eng. msg.) src= 192.168.3.2, dest= 192.168.3.1,
    src proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    dest proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004
22:19:49: ISAKMP (36): beginning Main Mode exchange
22:19:49: ISAKMP (36): sending packet to 192.168.3.1 (I) MM NO STATE
22:19:49: ISAKMP (36): received packet from 192.168.3.1 (I) MM NO STATE
22:19:49: ISAKMP (36): processing SA payload. message ID = 0
22:19:49: ISAKMP (36): Checking ISAKMP transform 1 against priority 7 policy
22:19:49: ISAKMP:      encryption DES-CBC
22:19:49: ISAKMP:      hash SHA
22:19:49: ISAKMP:      default group 1
22:19:49: ISAKMP:      auth pre-share
22:19:49: ISAKMP (36): atts are acceptable. Next payload is 0
22:19:51: ISAKMP (36): SA is doing pre-shared key authentication using id type
ID IPV4 ADDR
22:19:51: ISAKMP (36): sen.ding packet to 192.168.3.1 (I) MM SA SETUP
22:19:51: ISAKMP (36): received packet from 192.168.3.1 (I) MM SA SETUP
22:19:51: ISAKMP (36): processing KE payload. message ID = 0
22:19:53: ISAKMP (36): processing NONCE payload. message ID = 0
22:19:53: ISAKMP (36): SKEYID state generated
22:19:53: ISAKMP (36): ID payload
      next-payload : 8
      type         : 1
      protocol     : 17
      port         : 500
      length       : 8
22:19:53: ISAKMP (36): Total payload length: 12
22:19:53: ISAKMP (36): sending packet to 192.168.3.1 (I) MM_KEY_EXCH
22:19:53: ISAKMP (36): received packet from 192.168.3.1 (I) MM KEY EXCH
22:19:53: ISAKMP (36): processing ID payload. message ID = 0
22:19:53: ISAKMP (36): processing HASH payload. message ID = 0
22:19:53: ISAKMP (36): processing NOTIFY payload 24578 protocol 1
      spi 0, message ID = 0
22:19:53: ISAKMP (36): SA has been authenticated with 192.168.3.1
22:19:53: ISAKMP (36): beginning Quick Mode exchange, M-ID of 1599802612
```

```
22:19:53: IPSEC(key engine): got a queue event...
22:19:53: IPSEC(spi response): getting spi 510988780 for SA
      from 192.168.3.1     to 192.168.3.2     for prot 3
22:19:54: ISAKMP (36): sending packet to 192.168.3.1 (I) QM IDLE
22:19:54: ISAKMP (36): received packet from 192.168.3.1 (I) QM IDLE
22:19:54: ISAKMP (36): processing SA payload. message ID = 1599802612
22:19:54: ISAKMP (36): Checking IPSec proposal 1
22:19:54: ISAKMP: transform 1, ESP DES
22:19:54: ISAKMP:   attributes in transform:
22:19:54: ISAKMP:      encaps is 1
22:19:54: ISAKMP:      SA life type in seconds
22:19:54: ISAKMP:      SA life duration (basic) of 3600
22:19:54: ISAKMP:      SA life type in kilobytes
22:19:54: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
22:19:54: ISAKMP:      authenticator is HMAC-SHA
22:19:54: ISAKMP (36): atts are acceptable.
22:19:54: IPSEC(validate proposal request): proposal part #1,
  (key eng. msg.) dest= 192.168.3.1, src= 192.168.3.2,
    dest proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn id= 0, keysize= 0, flags= 0x4
22:19:54: ISAKMP (36): processing NONCE payload. message ID = 1599802612
22:19:54: ISAKMP (36): processing ID payload. message ID = 1599802612
22:19:54: ISAKMP (36): unknown error extracting ID
22:19:54: ISAKMP (36): processing ID payload. message ID = 1599802612
22:19:54: ISAKMP (36): unknown error extracting ID
22:19:54: ISAKMP (36): Creating IPSec SAs
22:19:54:         inbound SA from 192.168.3.1     to 192.168.3.2     (proxy
192.168.1.0     to 192.168.2.0    )
22:19:54:           has spi 510988780 and conn_id 37 and flags 4
22:19:54:           lifetime of 3600 seconds
22:19:54:           lifetime of 4608000 kilobytes
22:19:54:           outbound SA from 192.168.3.2     to 192.168.3.1     (proxy
192.168.2.0     to 192.168.1.0    )
22:19:54:           has spi 1419143803 and conn id 38 and flags 4
22:19:54:           lifetime of 3600 seconds
22:19:54:           lifetime of 4608000 kilobytes
22:19:54: IPSEC(key engine): got a queue event...
22:19:54: IPSEC(initialize sas): ,
  (key eng. msg.) dest= 192.168.3.2, src= 192.168.3.1,
    dest_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    src proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x1E7511EC(510988780), conn id= 37, keysize= 0, flags= 0x4
22:19:54: IPSEC(initialize sas): ,
  (key eng. msg.) src= 192.168.3.2, dest= 192.168.3.1,
    src_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    dest proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x54966A7B(1419143803), conn id= 38, keysize= 0, flags= 0x4
22:19:54: IPSEC(create sa): sa created,
  (sa) sa dest= 192.168.3.2, sa prot= 50,
    sa_spi= 0x1E7511EC(510988780),
    sa trans= esp-des esp-sha-hmac , sa conn id= 37
22:19:54: IPSEC(create sa): sa created,
  (sa) sa dest= 192.168.3.1, sa prot= 50,
    sa spi= 0x54966A7B(1419143803),
    sa trans= esp-des esp-sha-hmac , sa conn id= 38
22:19:54: ISAKMP (36): sending packet to 192.168.3.1 (I) QM_IDLE
```

Followed by tunnel termination initiated by the IOS.

```
22:20:20: IPSEC(delete sa): deleting SA,
  (sa) sa dest= 192.168.3.2, sa prot= 50,
    sa spi= 0x1E7511EC(510988780),
    sa trans= esp-des esp-sha-hmac , sa conn id= 37
22:20:20: IPSEC(delete_sa): deleting SA,
  (sa) sa dest= 192.168.3.1, sa prot= 50,
    sa spi= 0x54966A7B(1419143803),
    sa trans= esp-des esp-sha-hmac , sa conn id= 38
22:20:20: ISAKMP (36): sending packet to 192.168.3.1 (I) QM IDLE
22:20:20: IPSEC(delete sa): deleting SA,
  (sa) sa dest= 192.168.3.2, sa prot= 50,
    sa spi= 0x1E7511EC(510988780),
    sa trans= esp-des esp-sha-hmac , sa conn id= 37
22:20:20: IPSEC(delete sa): deleting SA,
  (sa) sa dest= 192.168.3.1, sa prot= 50,
    sa_spi= 0x54966A7B(1419143803),
    sa trans= esp-des esp-sha-hmac , sa conn id= 38
22:20:20: ISAKMP (36): sending packet to 192.168.3.1 (I) QM IDLE
cisco#
cisco#
22:20:57: ISADB: reaper checking SA, conn_id = 33  DELETE IT!
```