Tech Tip
Contivity Secure IP Services Gateway

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Contents

Overview

This document shows a sample configuration of an IPSec Asymmetric Branch Office Tunnel (ABOT) between Contivity Secure IP Services Gateway and Cisco PIX using pre-shared key authentication.

For more information on Branch Office peer-to-peer configuration consult Configuration Guide – Configuring Peer-to-Peer Branch Office Tunnel.

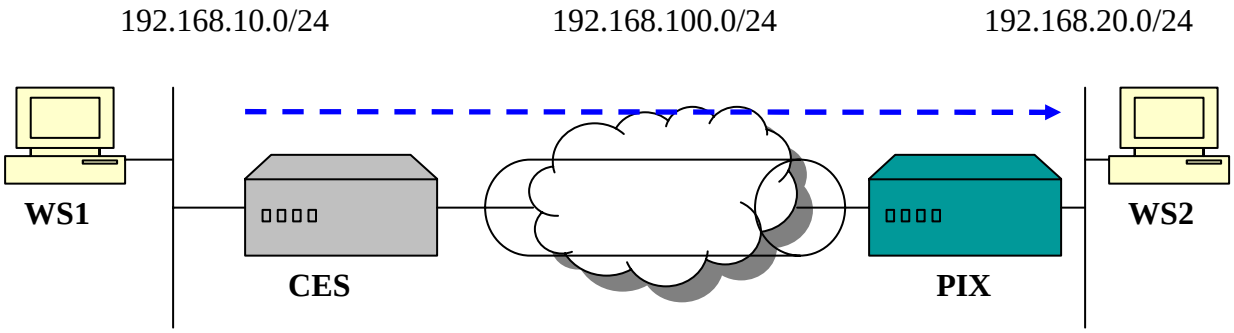
For more information on Cisco PIX consult http://www.cisco.com

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Sample Configurations

1. CES - Initiator

1.1. Setup



WS1 – Windows 2000 workstation, IP 192.168.10.11.24;
WS2 - Windows 2000 workstation, IP 192.168.20.22/24;
CES – Contivity Secure IP Services Gateway, code version V04_85, management IP 192.168.10.1/24, private IP 192.168.10.10/24, public IP 192.168.100.1/24;
PIX – Cisco PIX firewall 515, code version 6.3(1), private IP (Ethernet 0) 192.168.20.20/24, Public IP (Ethernet 1) 192.168.100.2/24.

The goal of the configuration is to setup an IPSec ABOT branch office tunnel between the CES and the PIX box using DES with SHA integrity and pre-shared key authentication. CES will act as an initiator of the tunnel and PIX as a responder.

1.2. Configuring WS1

Configure the IP address (192.168.10.11/24) on the WS1 and the CES private interface (192.168.10.10) as a default gateway:

```
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.10.11
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.10.10
```

1.3. Configuring WS2

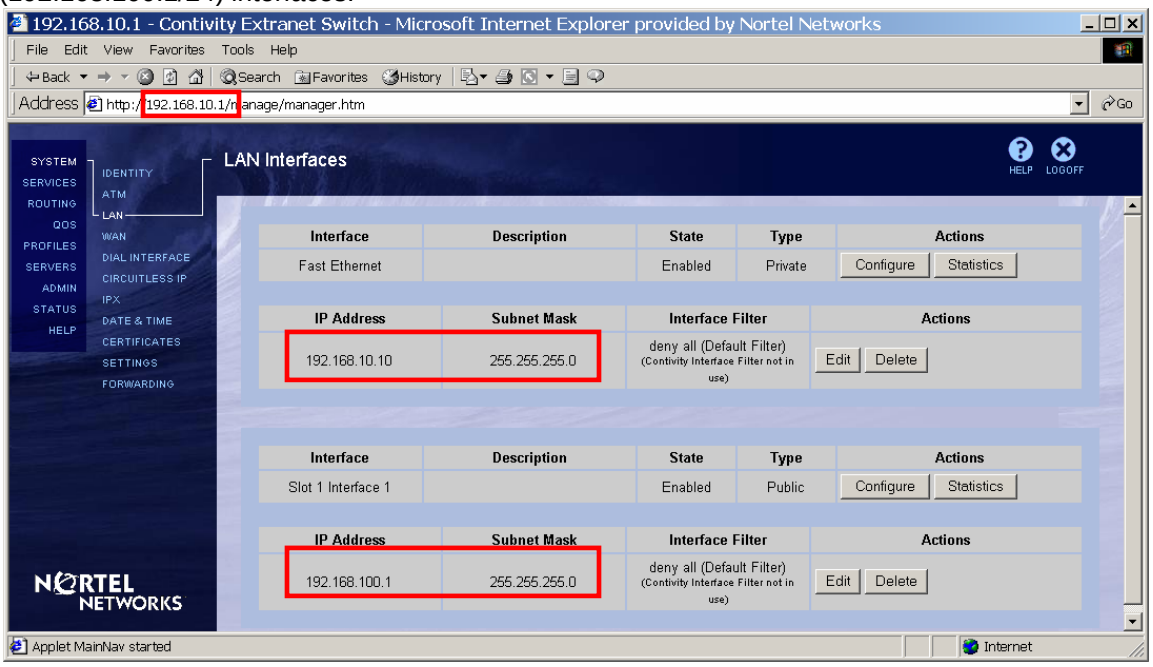
Configure the IP address (192.168.20.22/24) on the WS2 and the Cisco private interface (192.168.20.20) as a default gateway:

```
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.20.22
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.20.20
```

1.4. Configuring CES

1.4.1. Configuring network parameters

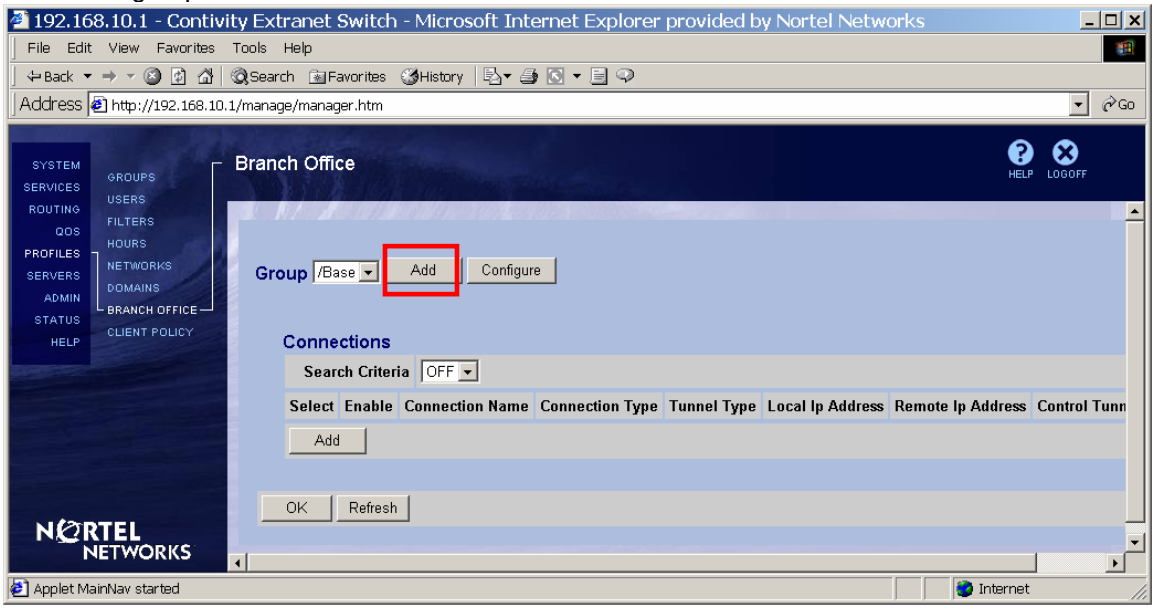
Configure IP address for management (192.268.10.1/24), private (192.168.10.10/24) and public (192.168.100.1/24) interfaces:



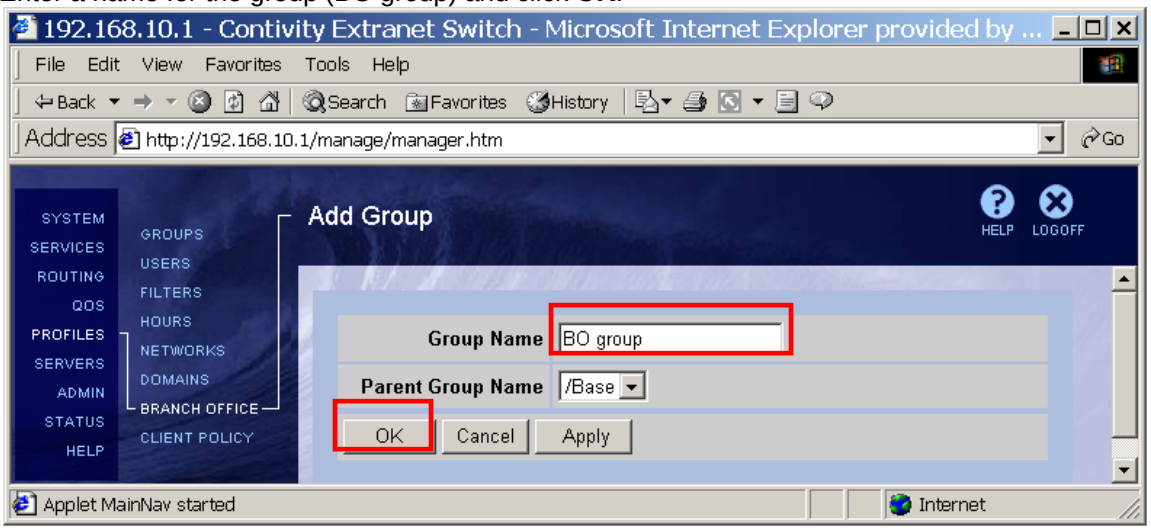
In this configuration CES and PIX are connected directly, if router is used between CES and PIX public default gateway must be configured on **Routing→Static Routes** screen by clicking **Add Public Route** and specifying the address of a public default router.

1.4.2. Configuring Branch Office connection

Configure the BO connection. Navigate **Profiles→Branch Office**. Click **Add** next to **Group** to add a new group for the branch office:

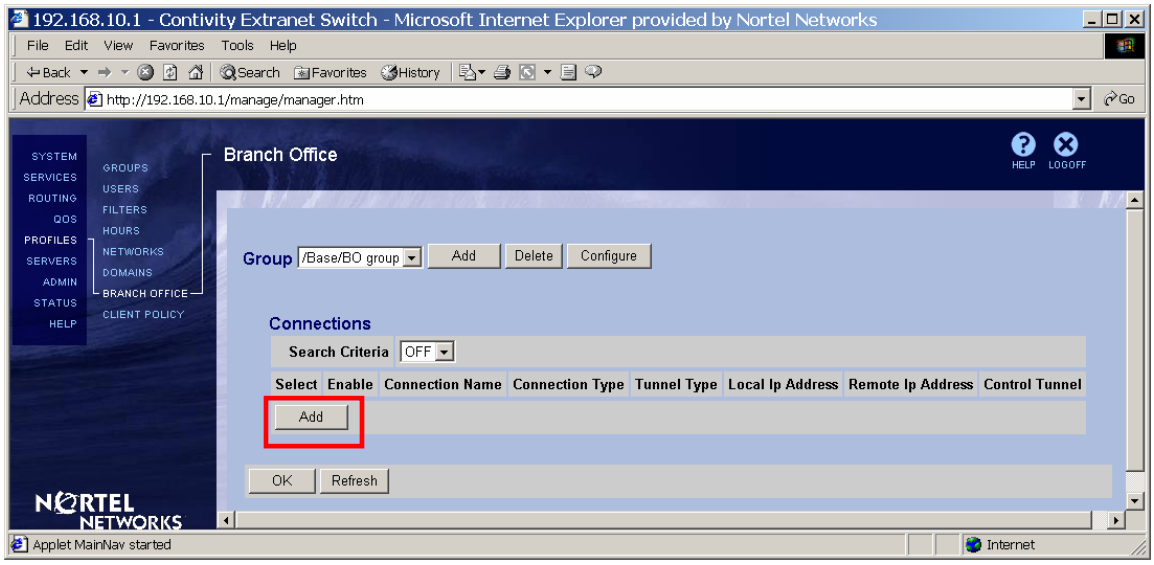


Enter a name for the group (BO group) and click **OK**:

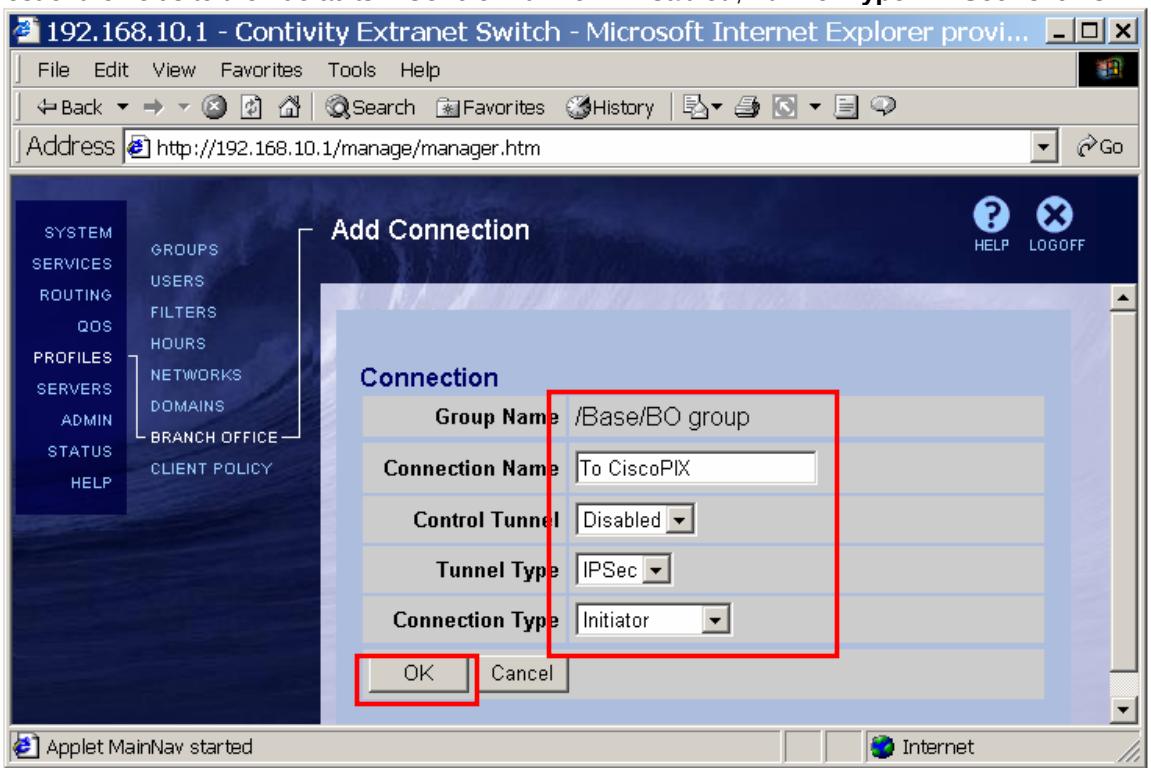


Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Select the newly created group from the menu next to **Group** and **Add** under the **Connections** field to add a new branch office connection:

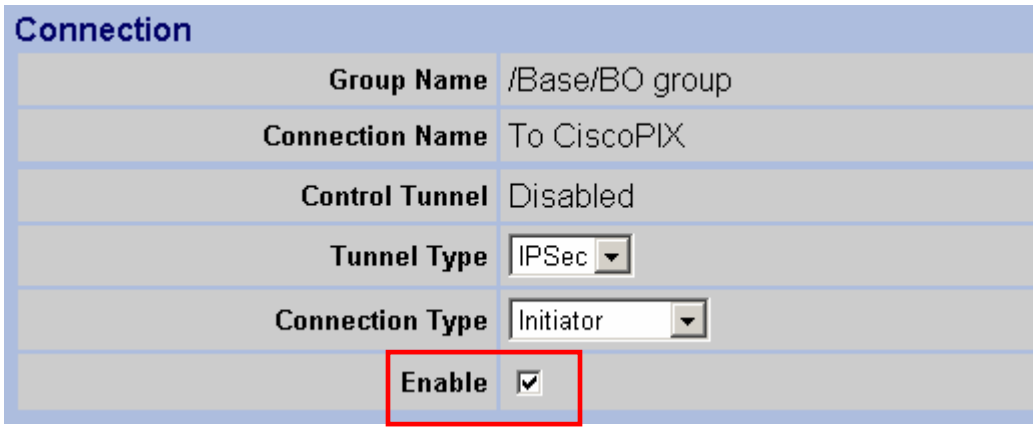


Enter a **Name** for the **Connection** (To CiscoPIX), set **Connection Type** to **Initiator**, leave the rest of the fields to their defaults – **Control Tunnel** – **Disabled**, **Tunnel Type** – **IPSec**. Click **OK**:

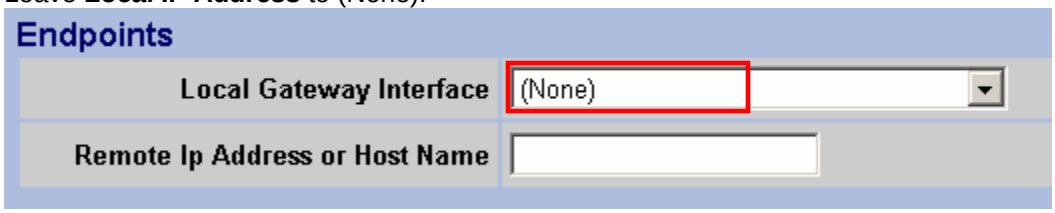


Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

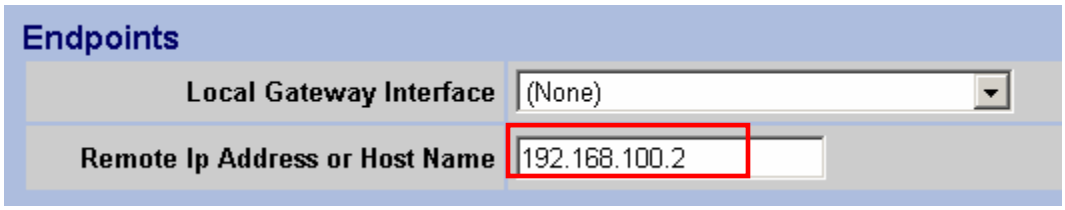
The **Connection Configuration** screen appears.
Check the box next to **Enable**:



Leave **Local IP Address** to (None):

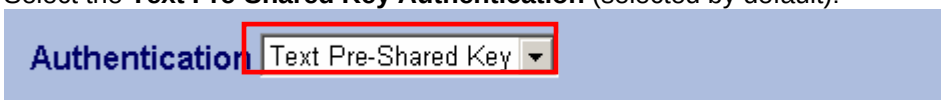


Enter **Remote IP Address** (Cisco PIX public IP – 192.168.100.2) for the remote endpoint of the tunnel:



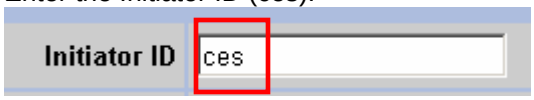
Leave the **Filter** to **Permit All**:

Select the **Text Pre-Shared Key Authentication** (selected by default):



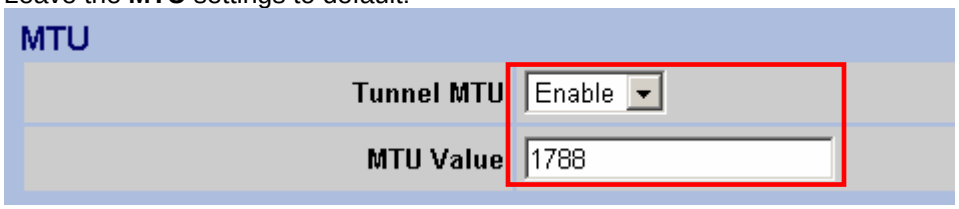
Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Enter the Initiator ID (ces):

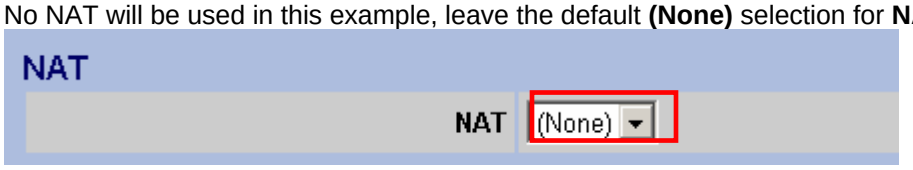


Enter the **Text Pre-Shared Key** (test):

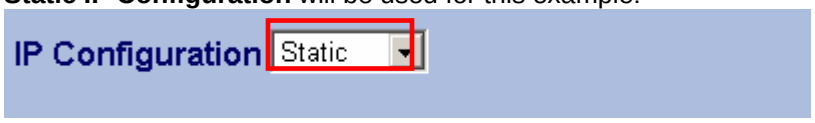
Leave the **MTU** settings to default:



No NAT will be used in this example, leave the default **(None)** selection for **NAT**:



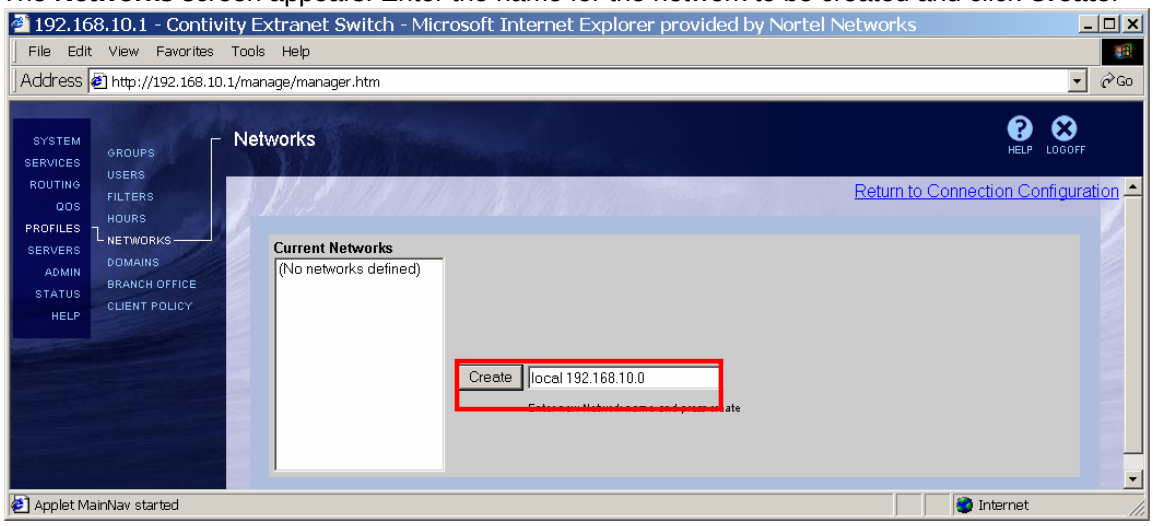
Static IP Configuration will be used for this example:



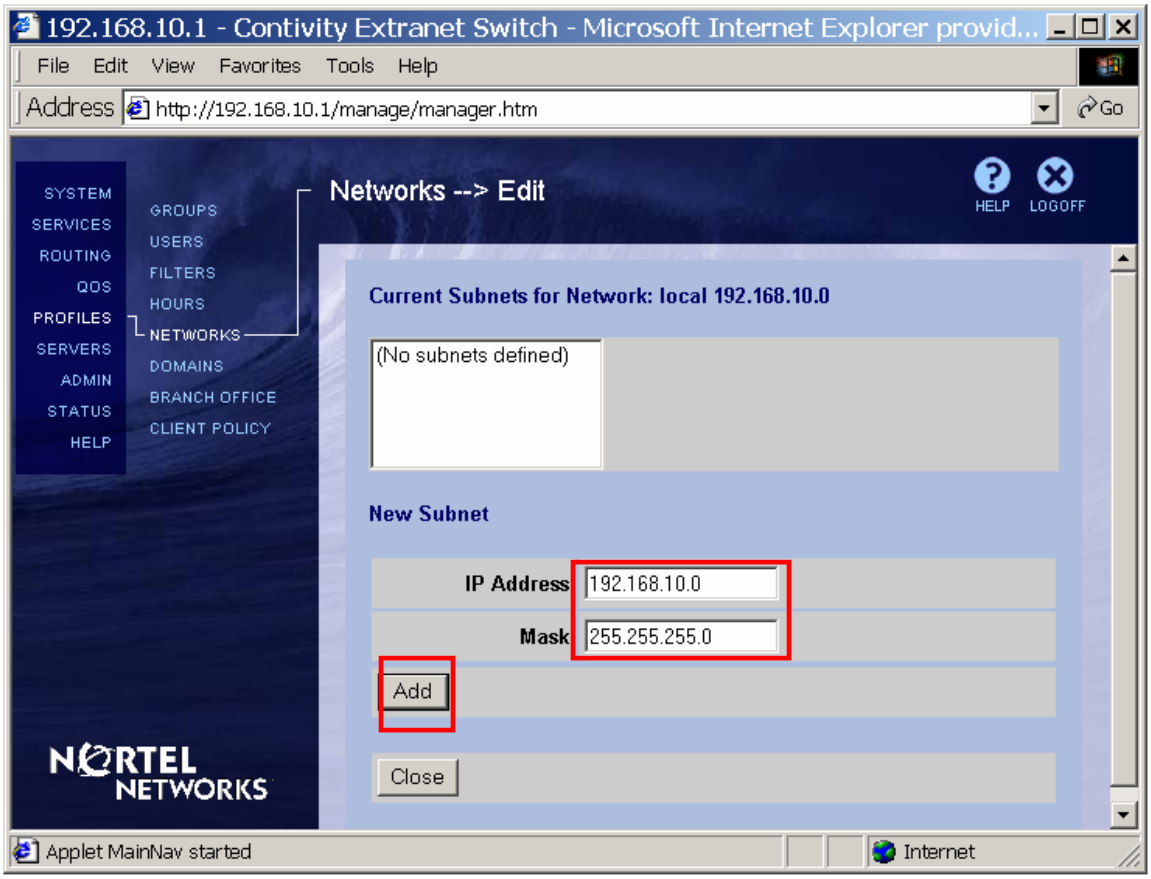
Define local accessible networks. Click **Create Local Network** next to **Local Network**:

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

The **Networks** screen appears. Enter the name for the network to be created and click **Create**:

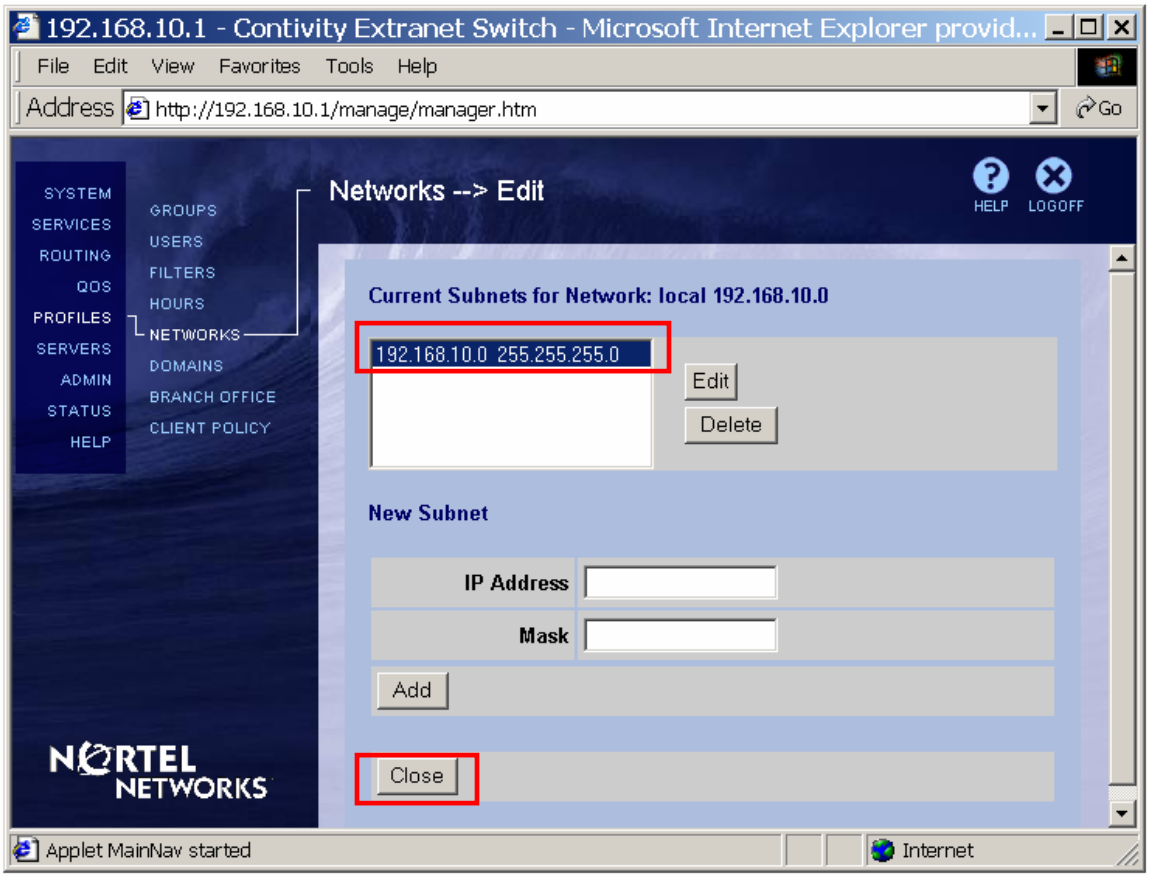


Enter **IP Address** for the local network (192.168.10.0), **Mask** associated with the address (255.255.255.0) and click **Add**:



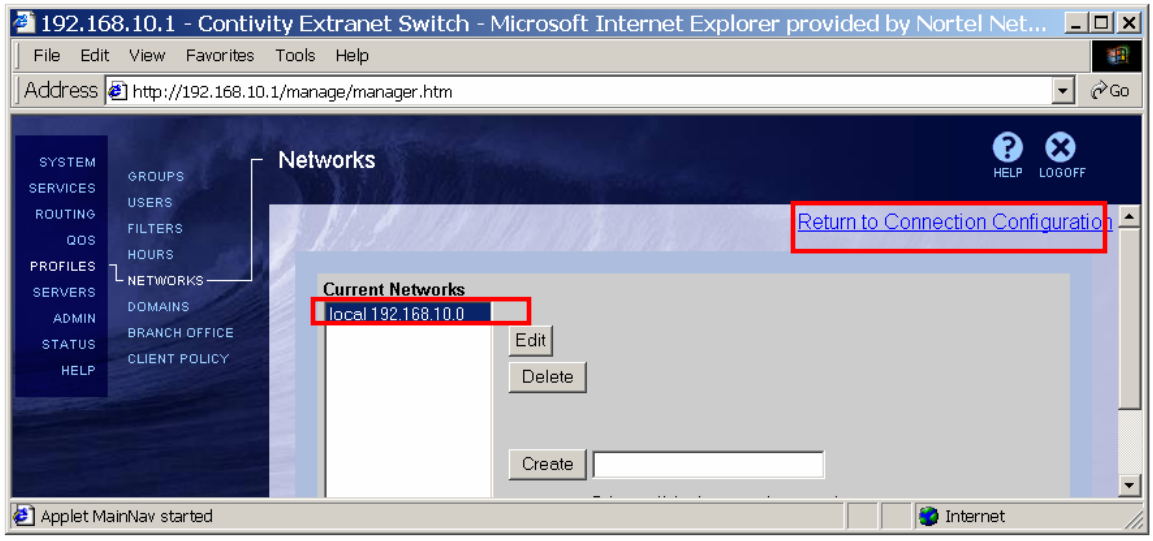
Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

The configured subnet for the network is listed under the **Current Subnets for Network** window. Click **Close**:

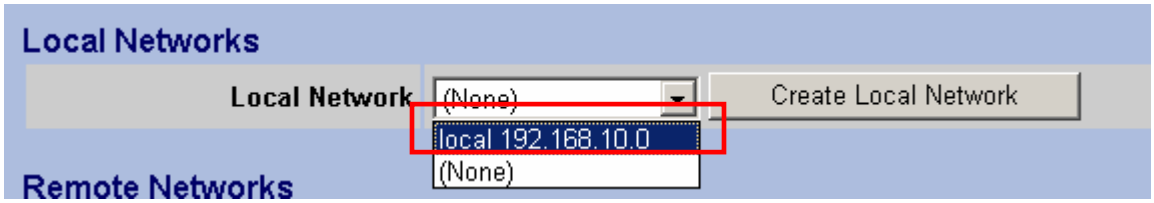


Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

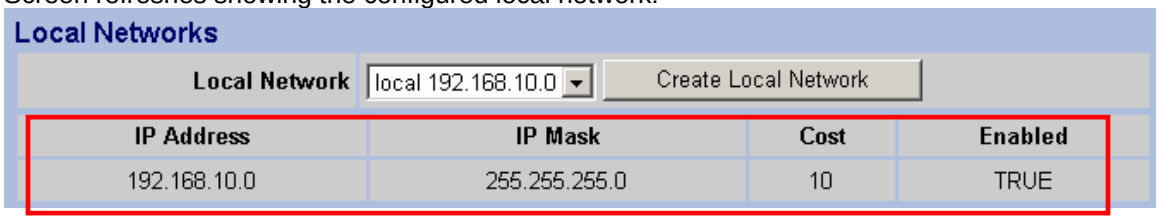
The configured network is listed under the **Current Networks**. Follow the link in the top right corner to return to the branch office configuration:



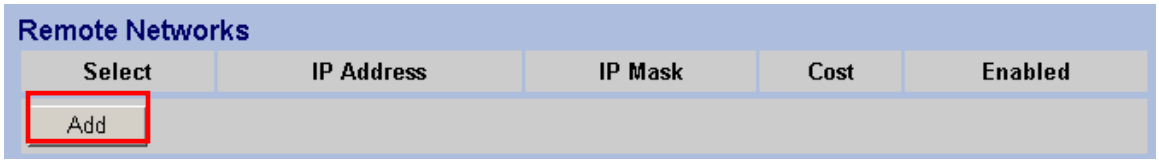
Select the newly configured local network (local 192.168.10.0) from the drop-down list next to **Local Network**:



Screen refreshes showing the configured local network:

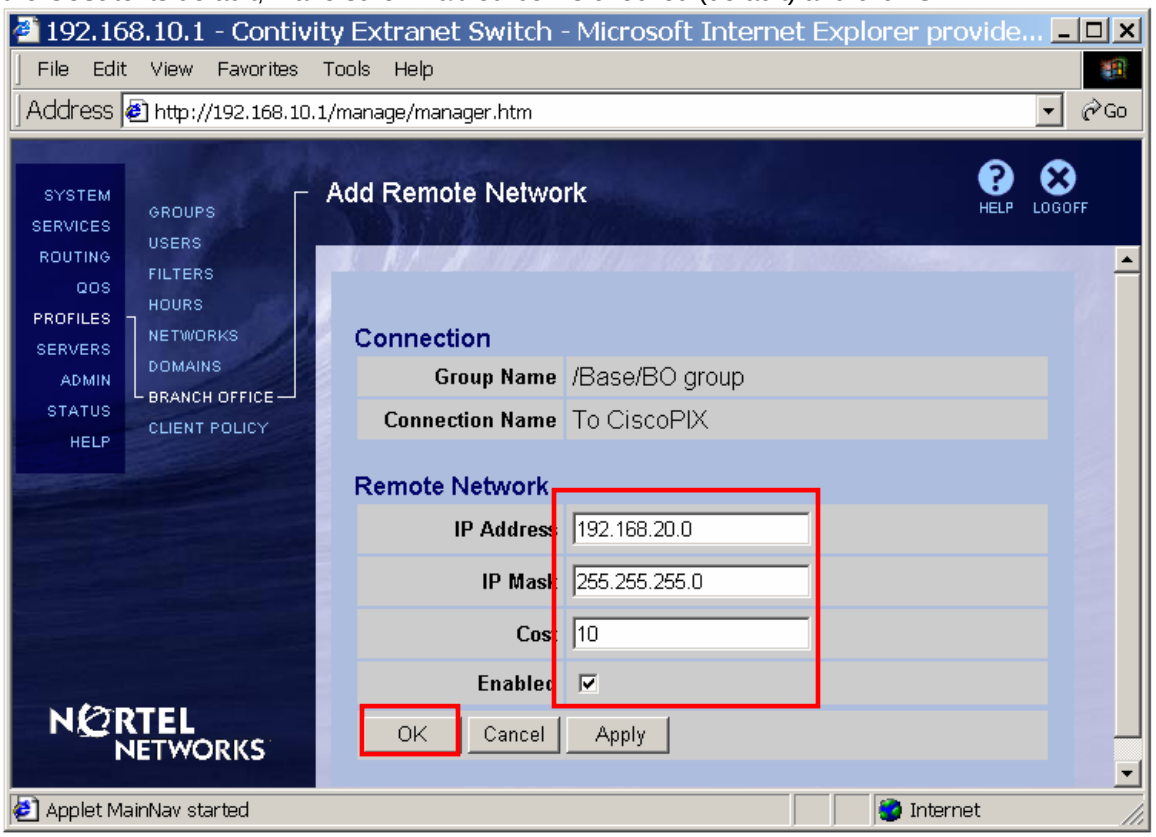


Define the remote accessible networks. Click **Add** under the **Remote Networks**:

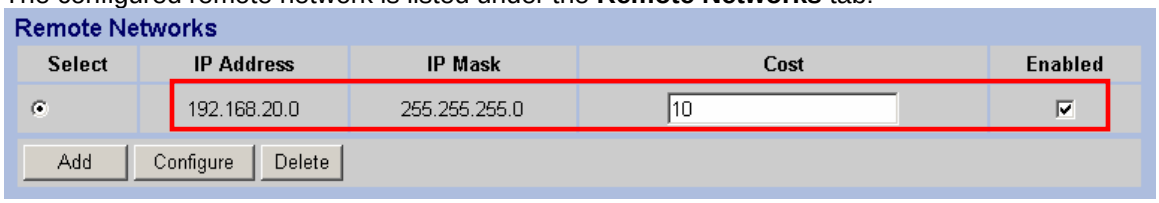


Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

The **Add Remote Network** screen appears. Enter the **IP Address** of the remote network (Cisco PIX private network – 192.168.20.0), **Mask** (255.255.255.0) associated with the address, leave the **Cost** to its default, make sure **Enabled** box is checked (default) and click **OK**:

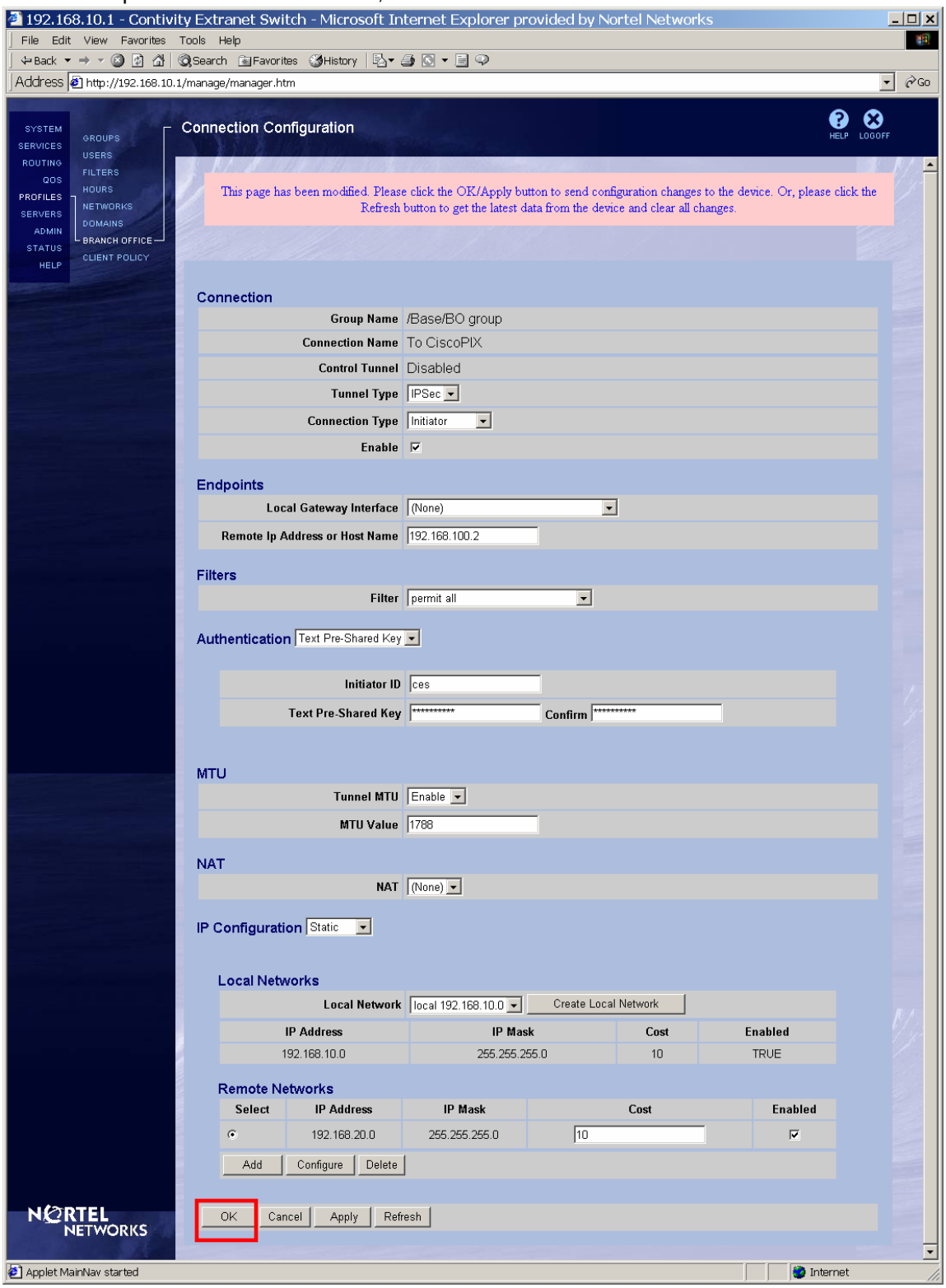


The configured remote network is listed under the **Remote Networks** tab:



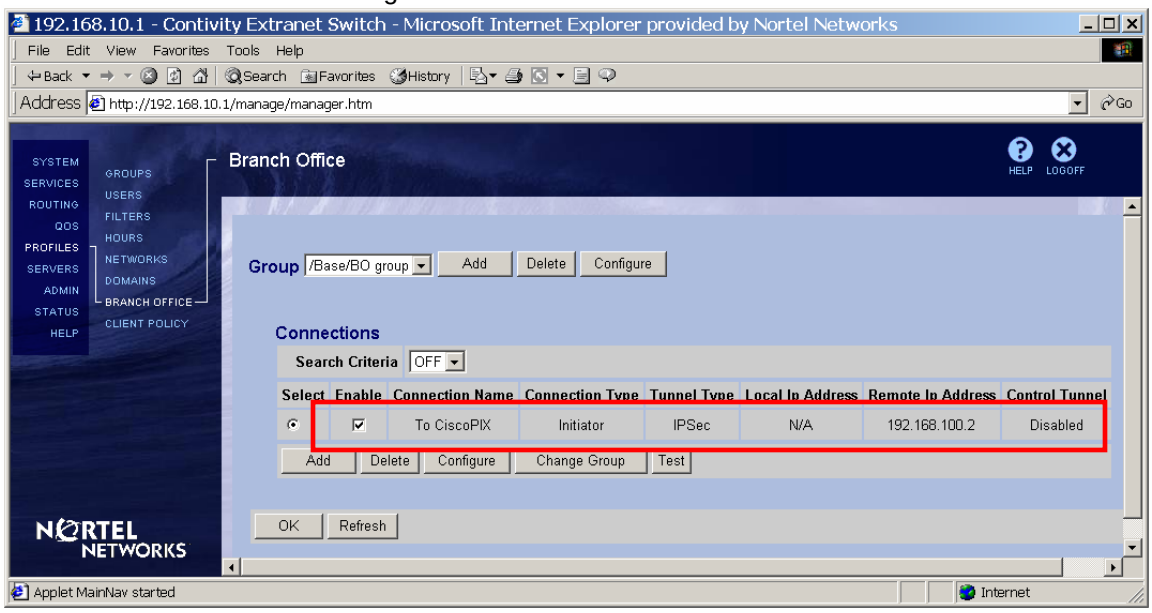
Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Once all the parameters have been set, click **OK** at the bottom of the screen:



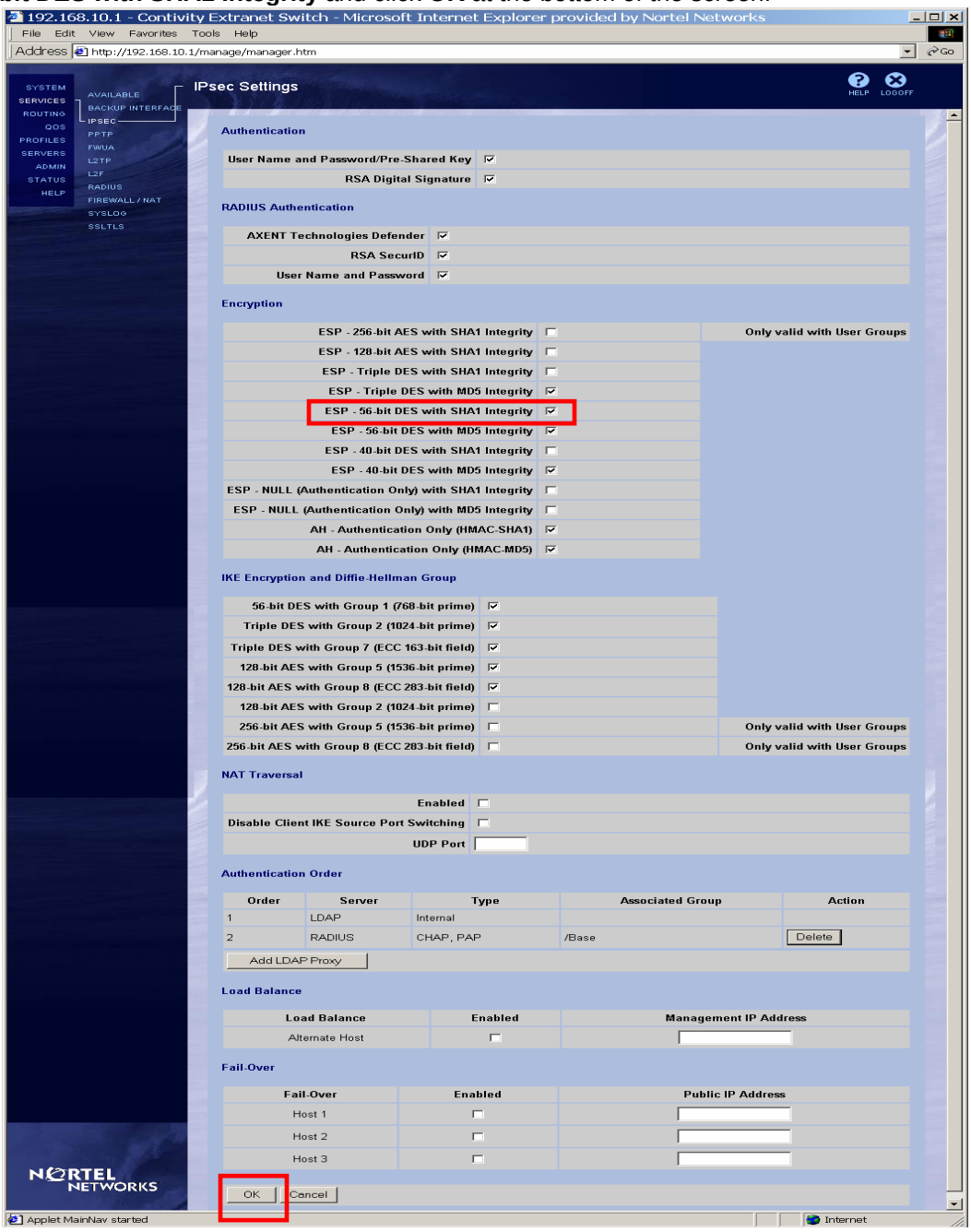
Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Branch office connection is configured:



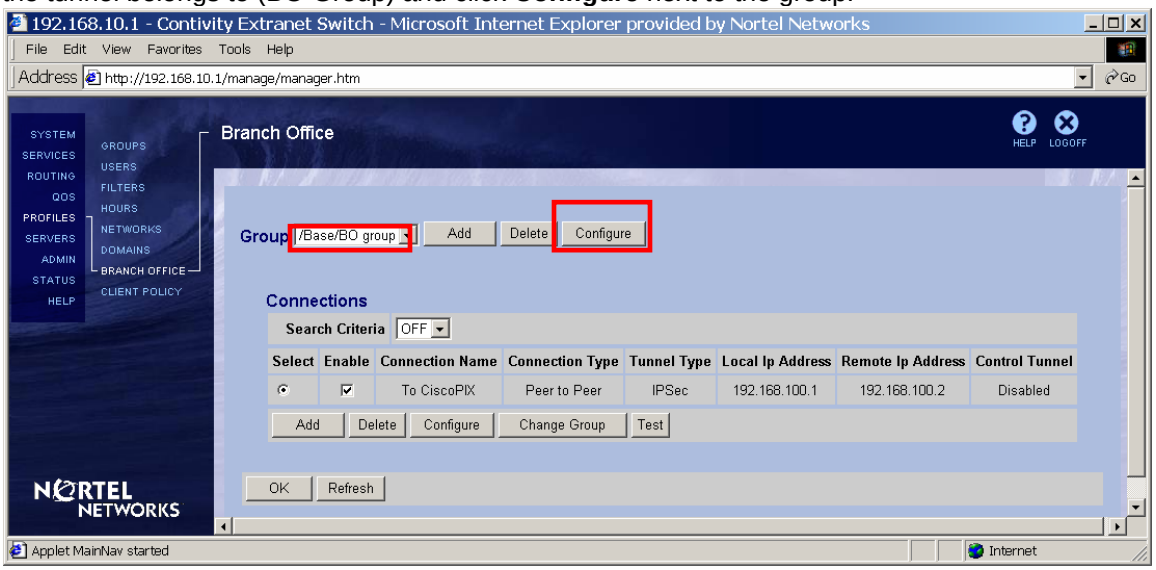
1.4.3. Configuring Global IPSec parameters

Configure IPSec parameters globally. DES with SHA1 integrity is disabled globally on Contivity by default. To enable DES with SHA1 navigate **Services→IPSec**. Check the box next to **ESP - 56-bit DES with SHA1 Integrity** and click **OK** at the bottom of the screen:



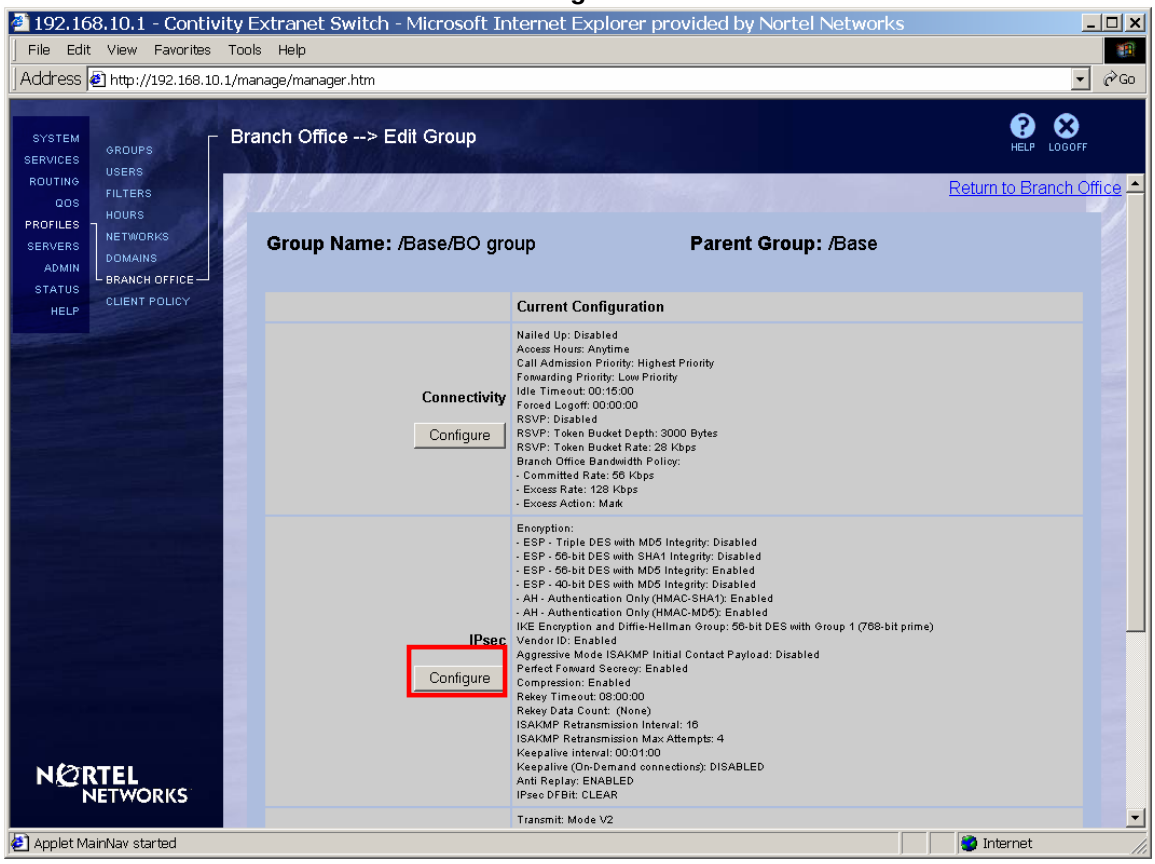
1.4.4. Configuring Branch Office IPSec parameters

Navigate **Profiles→Branch Office** to configure branch office IPSec parameters. Select a group the tunnel belongs to (BO Group) and click **Configure** next to the group:

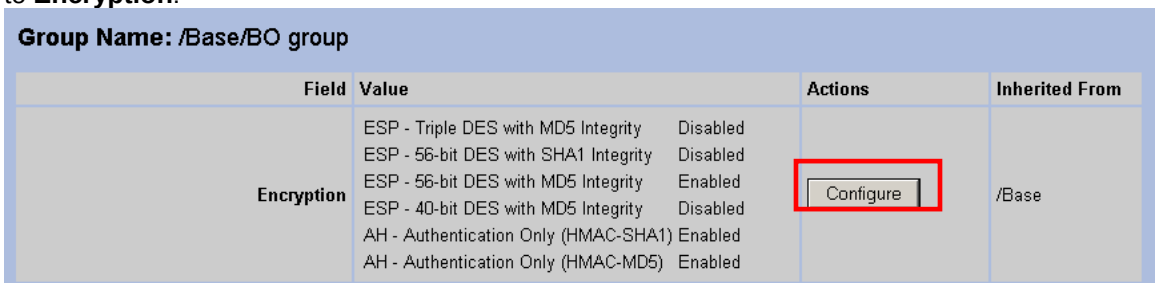


Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Scroll down to the IPSec section and click **Configure**:

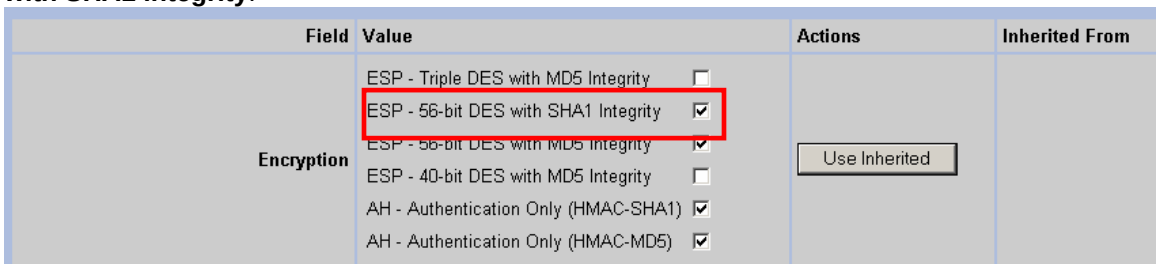


We need to enable DES with SHA1for the branch office tunnel in this group. Click **Configure** next to **Encryption**:

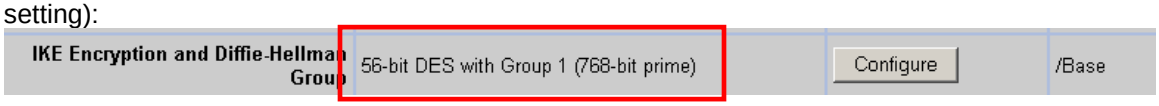


Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Screen refreshes allowing us to select encryption types. Check the box next to **ESP – 56-bit DES with SHA1 integrity**:

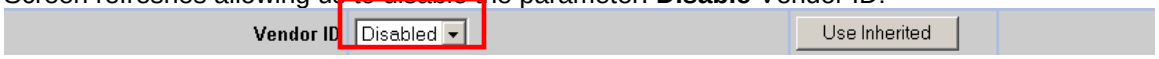


Make sure the correct **Diffie-Hellman** group is selected, for 56 bit DES it's group 1 (default setting):



To interoperate with Cisco PIX **Vendor ID** must be disabled for the group. Click **Configure** next to **Vendor ID**:

Screen refreshes allowing us to disable the parameter. **Disable** Vendor ID:



Disable the PFS, click **Configure** next to **Perfect Forward Secrecy**:

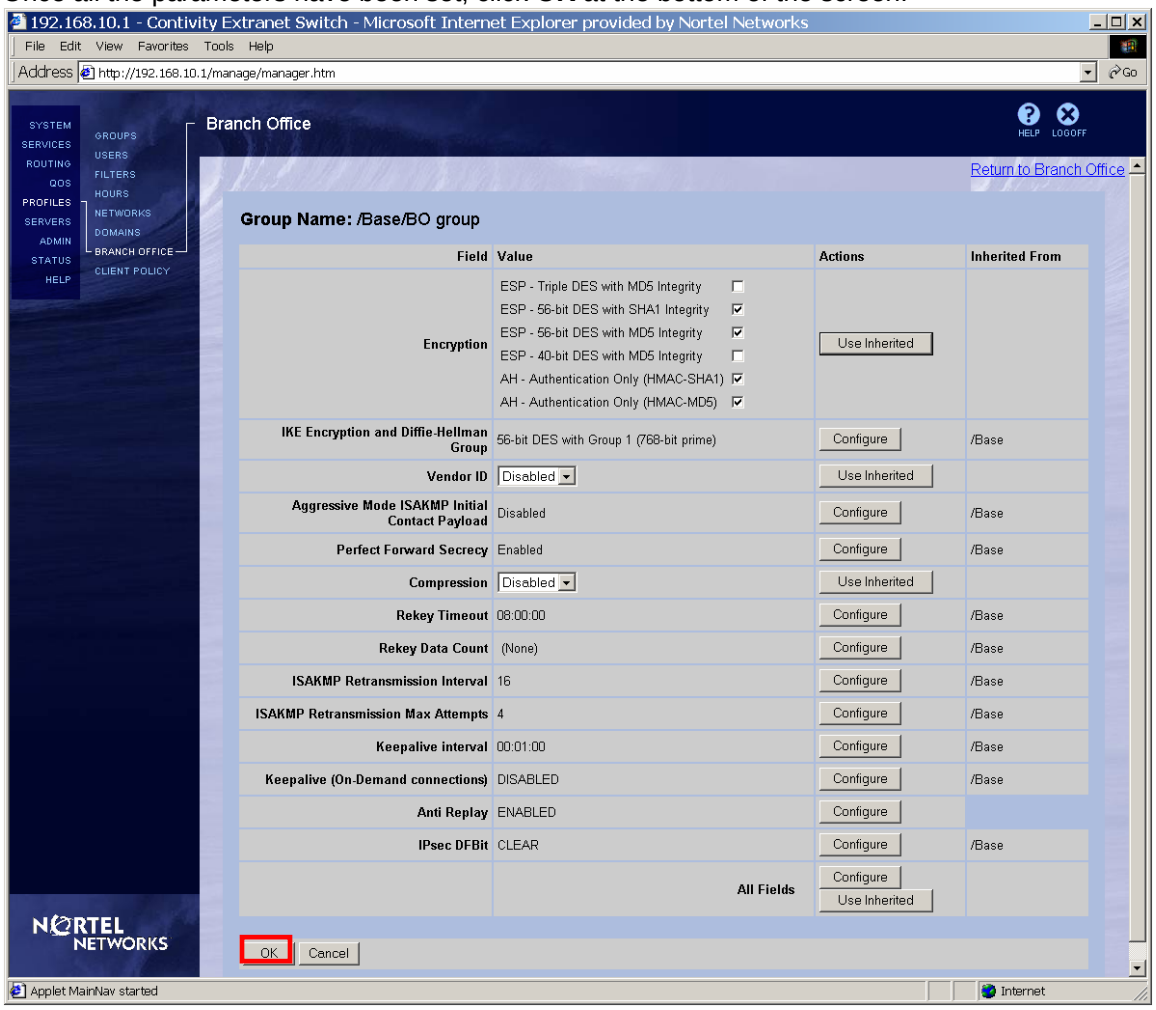
Select **Disabled** option:

Compression must be disabled to interoperate with Cisco PIX. Click **Configure** next to **Compression**:

Disable the **Compression** parameter:

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Once all the parameters have been set, click **OK** at the bottom of the screen:



At this point CES is configured.

1.5. Configuring PIX

The configuration of the Cisco PIX will be done via console in this example. Connect to the Cisco PIX via console and enter the privileged mode, by default PIX does not have a password set, press Enter when prompted for password:

```
pixfirewall> enable
Password:
pixfirewall#
```

Enter configuration mode:

```
pixfirewall# configure terminal
pixfirewall(config)#
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Configure and enable interfaces eth0 and eth1, in this example auto speed selection will be used for interfaces:

```
cisco-side(config)# interface ethernet1 auto
cisco-side(config)# interface ethernet0 auto
```

We will configure Ethernet 0 to be private interface and Ethernet 1 to be public interface. Configure eth 0 to be private (by default eth 0 is public and eth1 is private), this will swap the interfaces and will automatically make eth1 public:

```
pixfirewall(config)# nameif ethernet0 inside security100
interface 1 name "inside" swapped with interface 0 name "outside"
```

Configure hostname (cisco-side) on PIX:

```
pixfirewall(config)# hostname cisco-side
cisco-side(config)#
```

Create an access list that will be used with crypto algorithm to define what traffic will be encrypted and what will be sent in clear text. The permitted traffic will be encrypted and denied traffic will be sent in clear. We need to permit traffic from Cisco PIX private side (192.168.20.0/24) to CES private side (192.168.10.0/24) this will force all the traffic between private networks to go through the tunnel. 15 is the access list number we are creating:

```
cisco-side(config)# access-list 15 permit ip 192.168.20.0 255.255.255.0
192.168.10.0 255.255.255.0
```

Configure the IP address for the PIX private interface or inside address (192.168.20.20/24):

```
cisco-side(config)# ip address inside 192.168.20.20 255.255.255.0
```

Configure the IP address for the PIX public interface or outside address (192.168.100.2/24):

```
cisco-side(config)# ip address outside 192.168.100.2 255.255.255.0
```

We do not need to NAT over IPSec tunnel:

```
cisco-side(config)# nat (inside) 0 access-list 15
cisco-side(config)# nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Configure an outside route. In this configuration CES and PIX are directly connected, so CES public IP (192.168.100.1) will be used as a default public gateway. If a router is used between CES and PIX use routers IP as a gateway:

```
cisco-side(config)# route outside 0.0.0.0 0.0.0.0 192.168.100.1 1
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Configure Cisco PIX to accept IPSec traffic. This assures that traffic through the tunnel is not blocked by other access lists that might exist on the PIX box. Alternatively, access lists explicitly allowing particular traffic across PIX need to be configured via access list or conduit commands. In this example we will allow all IPSec traffic:

```
cisco-side(config)# sysopt connection permit-ipsec
```

Create an IPSec transform set to define what encryption and authentication algorithms will be used for the tunnel. We need to create a transform set (myset) for the DES with SHA integrity:

```
cisco-side(config)# crypto ipsec transform-set myset esp-des esp-sha-
hmac
```

Create an IPSec dynamic crypto map (map number 1, named cisco) and associate created transform set with the dynamic map:

```
cisco-side(config)# crypto dynamic-map cisco 1 set transform-set myset
```

Create a static map (map number 20, named dyn-map) and associate the created earlier dynamic map (cisco) with the static map:

```
cisco-side(config)# crypto map dyn-map 20 ipsec-isakmp dynamic cisco
```

Associate static map with the interface:

```
cisco-side(config)# crypto map dyn-map interface outside
```

Enable ISAKMP service for the outside interface:

```
cisco-side(config)# isakmp enable outside
```

Configure a pre-shared key (test) for authentication with initiator (note, address 0.0.0.0 netmask 0.0.0.0 means that any remote peer that knows the secret password will be authenticated):

```
cisco-side(config)# isakmp key test address 0.0.0.0 netmask 0.0.0.0
```

Configure Cisco PIX to use IP address as peer ID (by default PIX uses domain name as an ID):

```
cisco-side(config)# isakmp identity address
```

Configure Cisco PIX to use pre-shared key authentication:

```
cisco-side(config)# isakmp policy 20 authentication pre-share
```

Configure Cisco to use DES for encryption:

```
cisco-side(config)# isakmp policy 20 encryption des
```

Configure Cisco to use SHA1 for authentication:

```
cisco-side(config)# isakmp policy 20 hash sha
```

Configure Cisco to use Diffie-Hellman group 1:

```
cisco-side(config)# isakmp policy 20 group 1
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Check the config to make sure everything is correct:

```
cisco-side# show runn
: Saved
:
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 inside security100
nameif ethernet1 outside security0
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco-side
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 15 permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
pager lines 24
mtu inside 1500
mtu outside 1500
ip address inside 192.168.20.20 255.255.255.0
ip address outside 192.168.100.2 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 15
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 192.168.100.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto dynamic-map cisco 1 set transform-set myset
crypto map dyn-map 20 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
isakmp enable outside
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash sha
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d89c6e150ce28f659b61214df4af9d5e
: end
```

Save the configuration:

```
cisco-side(config)# write mem
Building configuration...
Cryptochecksum: dddab1ea a1b442f4 c0d1c3ae d1f2ae69
[OK]
```

Exit the configuration mode:

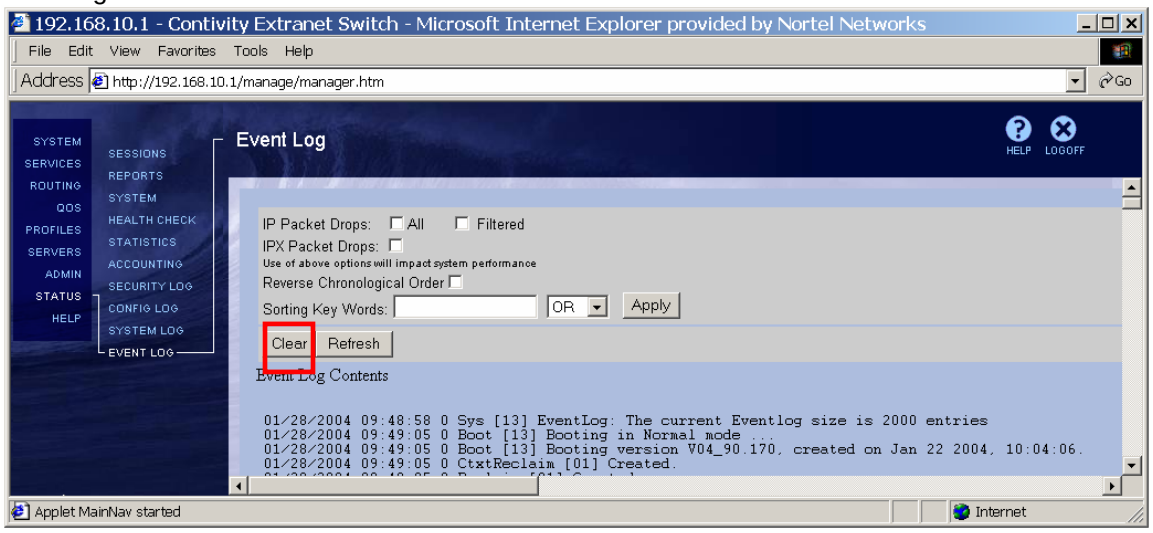
```
cisco-side(config)# exit
cisco-side#
```

A reboot might be required to activate the settings:

```
cisco-side# reload
```

1.6. Testing the configuration

Clear log on CES:



Enable debug on Cisco PIX to see the connection establishment:

```
cisco-side# debug crypto isakmp 2
cisco-side# debug crypto ipsec 2
```

Ping from WS2 (192.168.20.22) to WS1 (192.168.10.11) to make sure responder (PIX) does not try to establish the tunnel:

```
C:\>ping 192.168.10.11
Pinging 192.168.10.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

The ping is lost as the tunnel could not be initiated by the responder.

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Ping from WS1 (192.168.10.11) to WS2 (192.168.20.22) to bring up the tunnel from the CES side:

```
C:\>ping 192.168.20.22
Pinging 192.168.20.22 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.22: bytes=32 time=230ms TTL=29
Reply from 192.168.20.22: bytes=32 time<10ms TTL=29
Reply from 192.168.20.22: bytes=32 time<10ms TTL=29

Ping statistics for 192.168.20.22:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  230ms, Average =  57ms
```

The first ping is lost as tunnel has not yet been established; all the following pings went through as the tunnel has been established.

Check the log on CES:

```
02/09/2004 11:14:00 0 DCLog [00] DCManager flushing data to stat file
'20040209.DC'
02/09/2004 11:14:35 0 Branch Office [01] IPSEC branch office connection
initiated to rem[192.168.20.0-255.255.255.0]@[192.168.100.2]
loc[192.168.10.0-255.255.255.0]
02/09/2004 11:14:35 0 Security [11] Session: IPSEC[192.168.100.2]
attempting login
02/09/2004 11:14:35 0 Security [01] Session: IPSEC[192.168.100.2] has no
active sessions
02/09/2004 11:14:35 0 Security [01] Session: IPSEC[192.168.100.2] To
CiscoPIX has no active accounts
02/09/2004 11:14:35 0 Security [00] Session: IPSEC - found matching
gateway session, caching parameters from gateway session
02/09/2004 11:14:36 0 Security [01] Session: IPSEC[192.168.100.2]:11
SHARED-SECRET authenticate attempt...
02/09/2004 11:14:36 0 Security [01] Session: IPSEC[192.168.100.2]:11
attempting authentication using LOCAL
02/09/2004 11:14:36 0 Security [11] Session: IPSEC[192.168.100.2]:11
authenticated using LOCAL
02/09/2004 11:14:36 0 Security [11] Session: IPSEC[192.168.100.2]:11
bound to group /Base/BO group/To CiscoPIX
02/09/2004 11:14:36 0 Security [01] Session: IPSEC[192.168.100.2]:11
Building group filter permit all
02/09/2004 11:14:36 0 Security [01] Session: IPSEC[192.168.100.2]:11
Applying group filter permit all
02/09/2004 11:14:36 0 Security [11] Session: IPSEC[192.168.100.2]:11
authorized
02/09/2004 11:14:36 0 ISAKMP [02] ISAKMP SA (aggressive-mode)
established with 192.168.100.2
02/09/2004 11:14:36 0 ISAKMP [13] Unknown Notify message (24578)
received from 192.168.100.2
02/09/2004 11:14:36 0 ISAKMP [13] Unknown Notify message (24576)
received from 192.168.100.2
02/09/2004 11:14:37 0 Security [11] Session: network IPSEC[192.168.20.0-
255.255.255.0] attempting login
02/09/2004 11:14:37 0 Security [11] Session: network IPSEC[192.168.20.0-
255.255.255.0] logged in from gateway [192.168.100.2]
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
02/09/2004 11:14:37 0 Security [12] Session: IPSEC[192.168.100.2]:11
physical addresses: remote 192.168.100.2 local 192.168.100.1
02/09/2004 11:14:37 0 Security [12] Session: IPSEC[-]:12 physical
addresses: remote 192.168.100.2 local 192.168.100.1
02/09/2004 11:14:37 0 Outbound ESP from 192.168.100.1 to 192.168.100.2
SPI 0x9df931b4 [03] ESP encap session SPI 0xb431f99d bound to cpu 0
02/09/2004 11:14:37 0 Inbound ESP from 192.168.100.2 to 192.168.100.1
SPI 0x00239a0a [03] ESP decap session SPI 0xa9a2300 bound to cpu 0
02/09/2004 11:14:37 0 Branch Office [00] 52b80d8
BranchOfficeCtxtCls::RegisterTunnel: rem[192.168.20.0-
255.255.255.0]@[192.168.100.2] loc[192.168.10.0-255.255.255.0]
overwriting tunnel context [ffffffff] with [4fc3a88]
02/09/2004 11:14:37 0 ISAKMP [03] Established IPsec SAs with
192.168.100.2:
02/09/2004 11:14:37 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA outbound
SPI 0x9df931b4
02/09/2004 11:14:37 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA inbound
SPI 0x239a0a
```

Tunnel has been successfully established from the CES side.

```
Take a look at the ISAKMP and IPSec debug messages on the Cisco Pix:
crypto_isakmp_process_block:src:192.168.100.1, dest:192.168.100.2
spt:500 dpt:500
crypto_isakmp_init_phase1_fields: responder
name_addr2string: no name service
OAK_AG exchange
process_isakmp_packet:
process_sa: mess_id 0x0
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      auth pre-share
ISAKMP:      default group 1
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 20 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      auth pre-share
ISAKMP:      default group 1
ISAKMP (0): atts are acceptable. Next payload is 0
crypto_generate_DH_parameters: dhset 0xdd6b1c, phase 0
DH_ALG_PHASE1
process_ke:
ISAKMP (0): processing KE payload. message ID = 0

crypto_generate_DH_parameters: dhset 0xdd6b1c, phase 1
DH_ALG_PHASE2
process_nonce:
ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
construct_header: message_id 0x0
construct_isakmp_sa: auth 7
construct_xauthv6_vendor_id:
construct_dpd_vendor_id:
construct_unity_vendor_id:
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
construct_vendor_id:
construct_ke:
need_cert_from_peer:
ISAKMP (0): ID payload
        next-payload : 10
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
construct_nonce:
construct_hash:
compute_hash:
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:192.168.100.1, dest:192.168.100.2
spt:500 dpt:500
OAK_AG exchange
process_isakmp_packet:
process_hash:
ISAKMP (0): processing HASH payload. message ID = 0
compute_hash:
ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
construct_header: message_id 0x46e6a133
construct_blank_hash:
construct_notify:
construct_qm_hash:
ISAKMP (0): sending phase 1 RESPONDER_LIFETIME notify
ISAKMP (0): sending NOTIFY message 24576 protocol 1
construct_header: message_id 0x807d3dd
construct_blank_hash:
construct_notify:
construct_qm_hash:
VPN Peer: ISAKMP: Added new peer: ip:192.168.100.1/500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:192.168.100.1/500 Ref cnt incremented to:1
Total VPN P
eers:1
crypto_isakmp_process_block:src:192.168.100.1, dest:192.168.100.2
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
verify_qm_hash:
OAK_QM_IDLE
process_isakmp_packet:
process_sa: mess_id 0x4eb52f2d
ISAKMP (0): processing SA payload. message ID = 1320496941

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x0 0x70 0x80
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 2
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x0 0x70 0x80
ISAKMP (0): atts are acceptable.
snoop_id_payloads:IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.168.100.2, src= 192.168.100.1,
    dest_proxy= 192.168.20.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

process_nonce:
ISAKMP (0): processing NONCE payload. message ID = 1320496941

ISAKMP (0): processing ID payload. message ID = 1320496941
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 192.168.10.0/255.255.255.0 prot 0
port 0
ISAKMP (0): processing ID payload. message ID = 1320496941
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 192.168.20.0/255.255.255.0 prot 0
port 0IPSE
C(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x9df931b4(2650354100) for SA
        from   192.168.100.1 to   192.168.100.2 for prot 3

return status is IKMP_NO_ERROR
oakley_const_qm:
construct_header: message_id 0x4eb52f2d
construct_blank_hash:
construct_ipsec_sa:
construct_ipsec_nonce:
construct_proxy_id:
construct_proxy_id:
construct_notify:
construct_qm_hash:
crypto_isakmp_process_block:src:192.168.100.1, dest:192.168.100.2
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
verify_qm_hash:
OAK_QM_AUTH_AWAIT
prepare_ipsec_sas:
CREATE IPSEC KEY:
CREATE IPSEC KEY:
ISAKMP (0): Creating IPSec SAs
        inbound SA from   192.168.100.1 to   192.168.100.2 (proxy
192.168.10.0 to    192.168.20.0)
        has spi 2650354100 and conn_id 1 and flags 4
        lifetime of 28800 seconds
        outbound SA from   192.168.100.2 to   192.168.100.1 (proxy
192.168.20.0 to    192.168.10.0)
        has spi 2333194 and conn_id 2 and flags 4
        lifetime of 28800 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 192.168.100.2, src= 192.168.100.1,
    dest_proxy= 192.168.20.0/255.255.255.0/0/0 (type=4),
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
    src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 28800s and 0kb,
    spi= 0x9df931b4(2650354100), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 192.168.100.2, dest= 192.168.100.1,
    src_proxy= 192.168.20.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 28800s and 0kb,
    spi= 0x239a0a(2333194), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:192.168.100.1/500 Ref cnt incremented to:2
Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:192.168.100.1/500 Ref cnt incremented to:3
Total VPN Peers:1
return status is IKMP_NO_ERROR
```

Check ISAKMP SAs on PIX:

```
cisco-side(config)# show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src         state     pending     created
   192.168.100.2    192.168.100.1    QM_IDLE           0           1
```

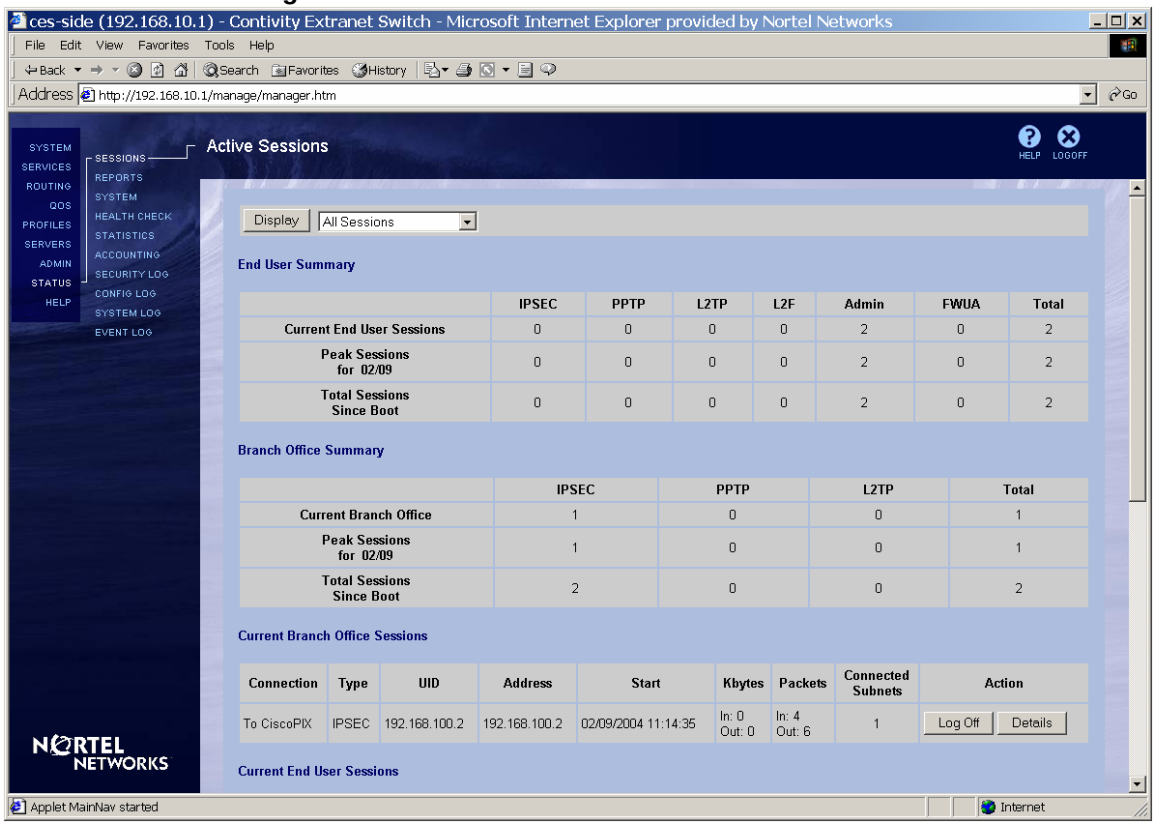
Check IPSec SAs on PIX:

```
cisco-side(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: dyn-map, local addr. 192.168.100.2

   local  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current peer: 192.168.100.1:500
     PERMIT, flags={}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.100.2, remote crypto endpt.:
192.168.100.1
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 239a0a

     inbound esp sas:
      spi: 0x9df931b4(2650354100)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: dyn-map
        sa timing: remaining key lifetime (k/sec): (4607999/28707)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
     inbound pcp sas:
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
outbound esp sas:
 spi: 0x239a0a(2333194)
   transform: esp-des esp-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2, crypto map: dyn-map
   sa timing: remaining key lifetime (k/sec): (4607999/28707)
   IV size: 8 bytes
   replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Check the branch office session statistics on **Status→Statistics** screen. Note the presence of branch office tunnel. **Log off** the connection:



Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Check the log on CES:

```
02/09/2004 11:18:38 0 ISAKMP [13] 192.168.100.2 logged off by
administrator
02/09/2004 11:18:38 0 ISAKMP [03] Deleting IPsec SAs with 192.168.100.2:
02/09/2004 11:18:38 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA outbound
SPI 0x9df931b4
02/09/2004 11:18:38 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA inbound
SPI 0x239a0a
02/09/2004 11:18:38 0 IPvfy.04fc3a88{Tun} [00] destructor called
0x4fc3a88
02/09/2004 11:18:38 0 Security [12] Session 6c7fb20: IPSEC[-]:12 sib 0
logged out
02/09/2004 11:18:38 0 Security [12] Session 6c80a48:
IPSEC[192.168.100.2]:11 sib 0 logged out
02/09/2004 11:18:38 0 ISAKMP [02] Deleting ISAKMP SA with 192.168.100.2
```

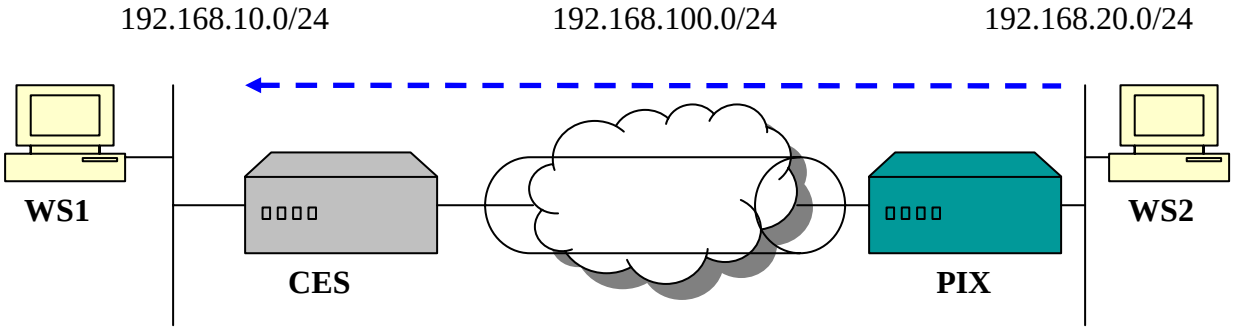
Check the debug messages on PIX:

```
crypto_isakmp_process_block:src:192.168.100.1, dest:192.168.100.2
spt:500 dpt:500
process_isakmp_info:
verify_qm_hash:
process_isakmp_packet:
ISAKMP (0): processing DELETE payload. message ID = 51597287, spi size =
4IPSEC(key_engine): got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP

VPN Peer: IPSEC: Peer ip:192.168.100.1/500 Decrementing Ref cnt to:2
Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:192.168.100.1/500 Decrementing Ref cnt to:1
Total VPN Peers:1
return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:192.168.100.1, dest:192.168.100.2
spt:500 dpt:500
process_isakmp_info:
verify_qm_hash:
process_isakmp_packet:
ISAKMP (0): processing DELETE payload. message ID = 2829118539, spi size
= 16
ISAKMP (0): deleting SA: src 192.168.100.1, dst 192.168.100.2
return status is IKMP_NO_ERR_NO_TRANS
ISADB: reaper checking SA 0xdd6864, conn_id = 0  DELETE IT!

VPN Peer: ISAKMP: Peer ip:192.168.100.1/500 Ref cnt decremented to:0
Total VPN Peers:1
VPN Peer: ISAKMP: Deleted peer: ip:192.168.100.1/500 Total VPN peers:0
```

2. CES – Responder

2.1. Setup

The same setup as in first example will be used.



WS1 – Windows 2000 workstation, IP 192.168.10.11.24;
WS2 - Windows 2000 workstation, IP 192.168.20.22/24;
CES – Contivity Secure IP Services Gateway, code version V04_85, management IP 192.168.10.1/24, private IP 192.168.10.10/24, public IP 192.168.100.1/24;
PIX – Cisco PIX firewall 515, code version 6.3(1), private IP (Ethernet 0) 192.168.20.20/24, Public IP (Ethernet 1) 192.168.100.2/24.

The goal of the configuration is to setup an IPSec ABOT branch office tunnel between the CES and the PIX box using DES with SHA integrity and pre-shared key authentication. CES will act as a responder of the tunnel and PIX as an initiator.

2.2. Configuring WS1

Configure WS1 the same way it was configured for the first example.

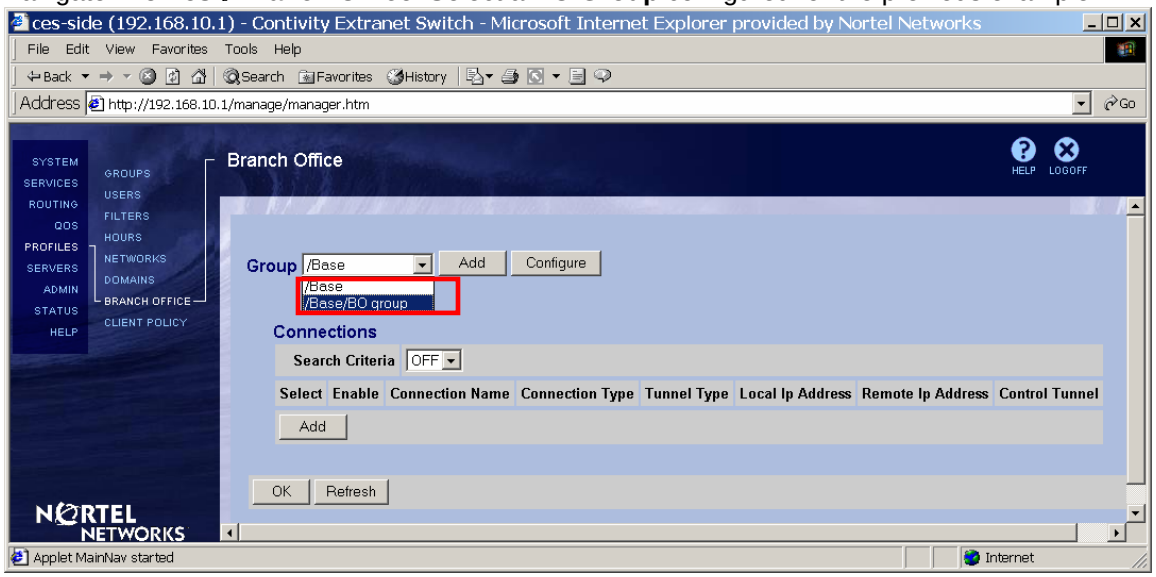
2.3. Configuring WS2

Configure WS2 the same way it was configured for the first example.

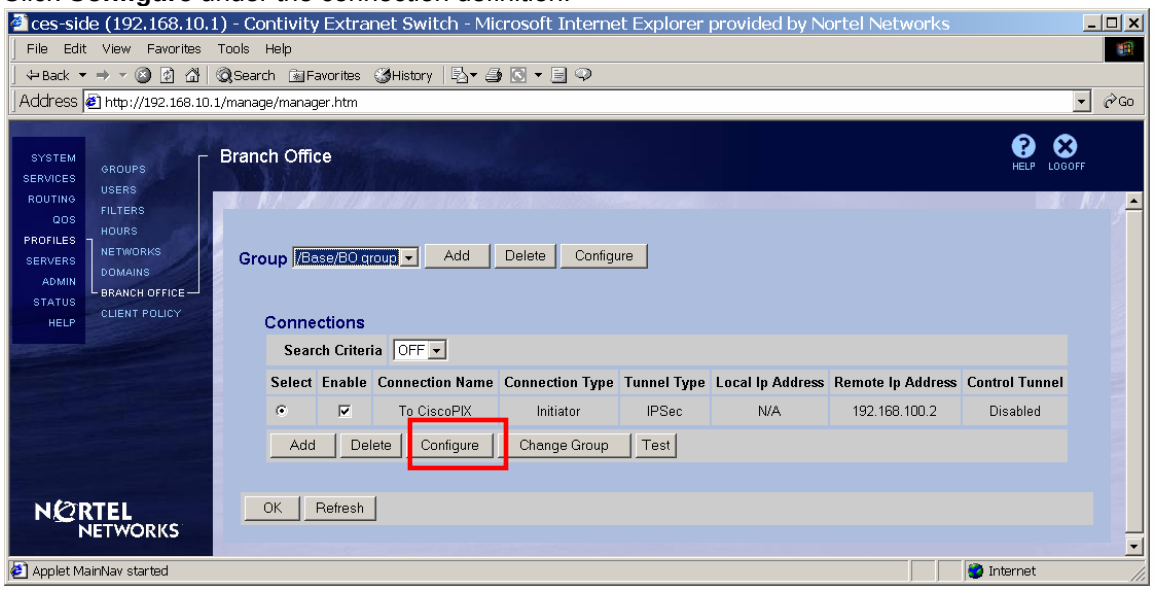
2.4. Configuring CES

The configuration of CES in this example is based on the configuration of CES in previous example. Only the difference will be noted.

Navigate **Profiles→Branch Office**. Select a **BO Group** configured for the previous example:

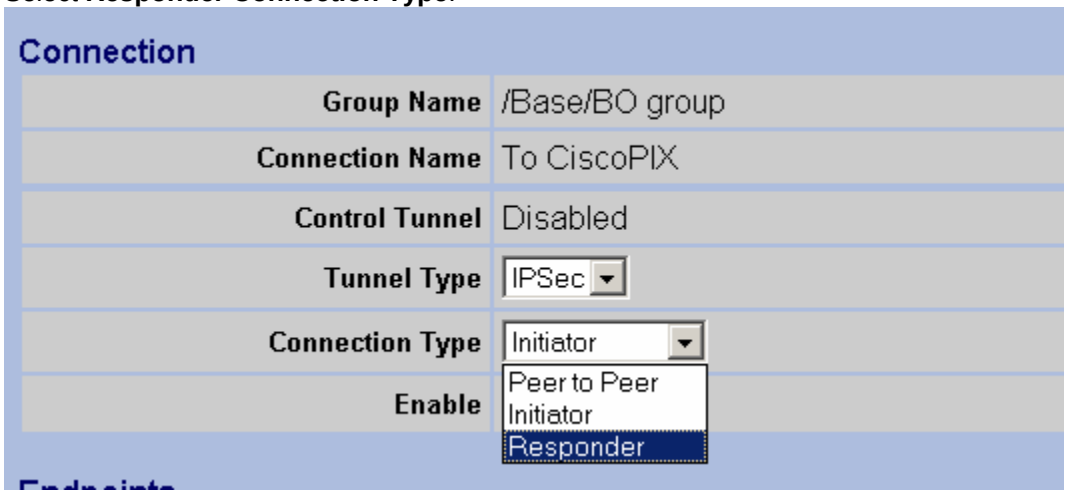


Click **Configure** under the connection definition:

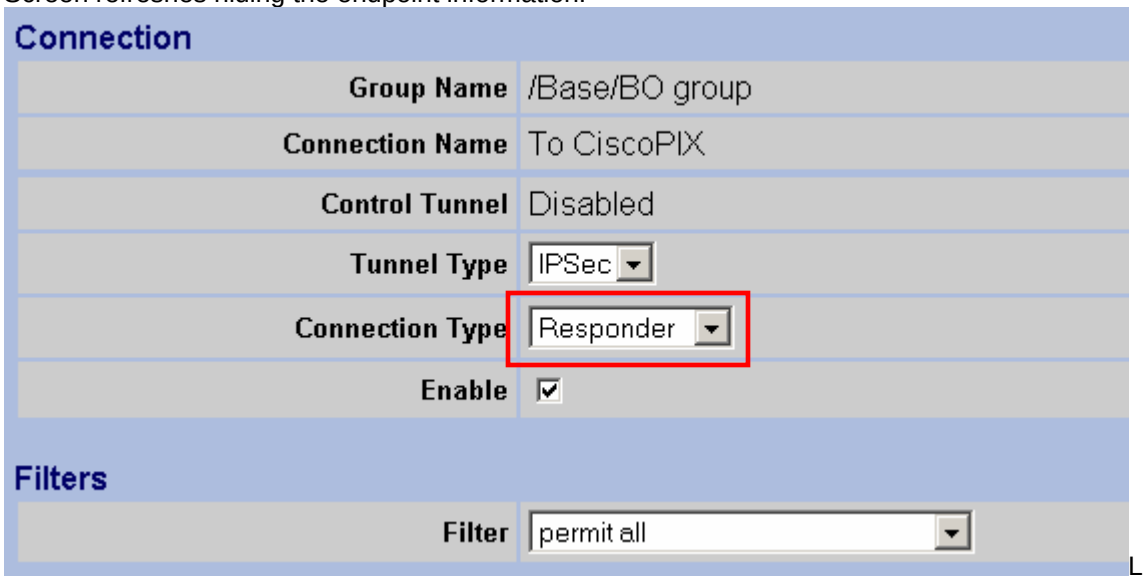


Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Select **Responder Connection Type**:



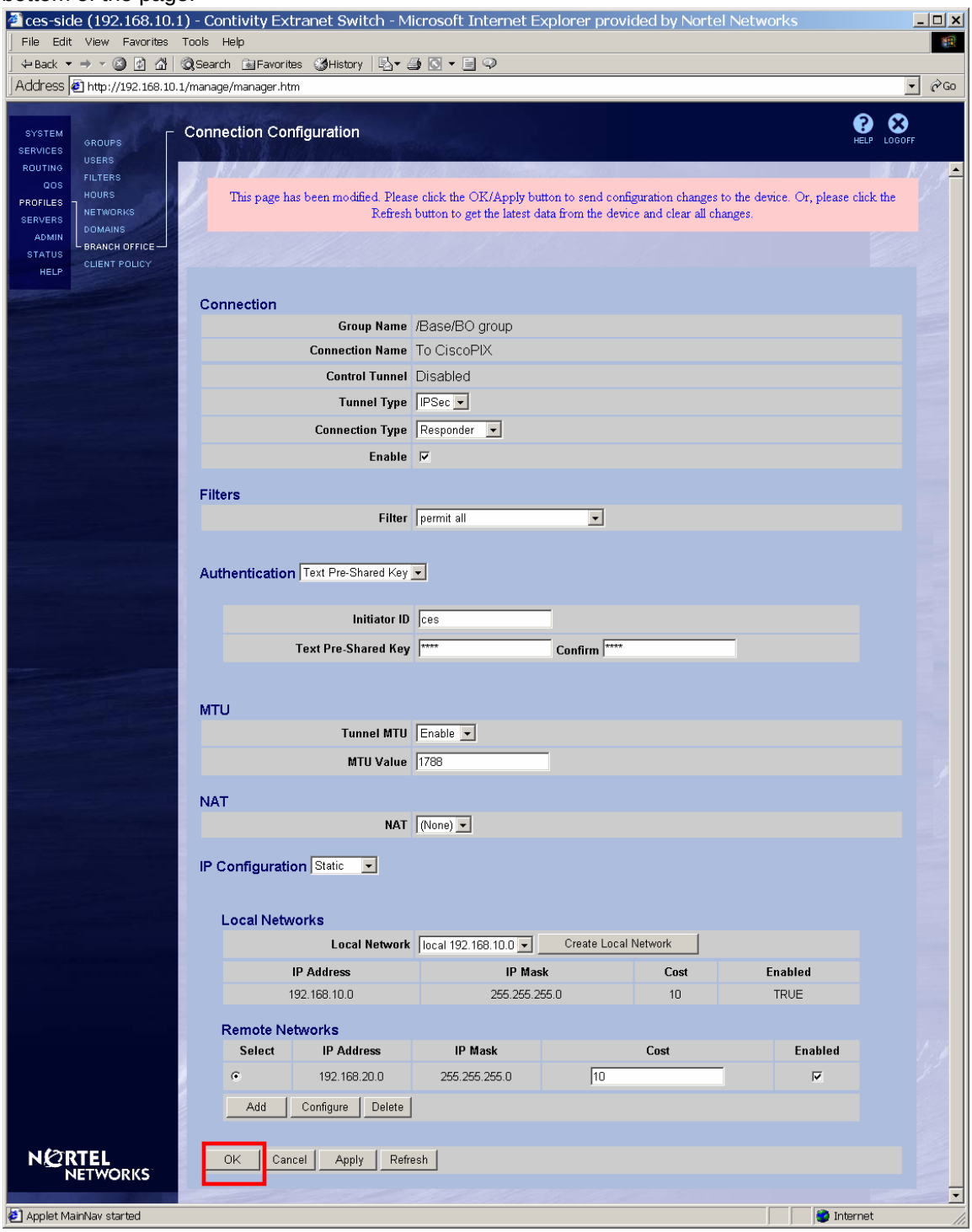
Screen refreshes hiding the endpoint information:



L

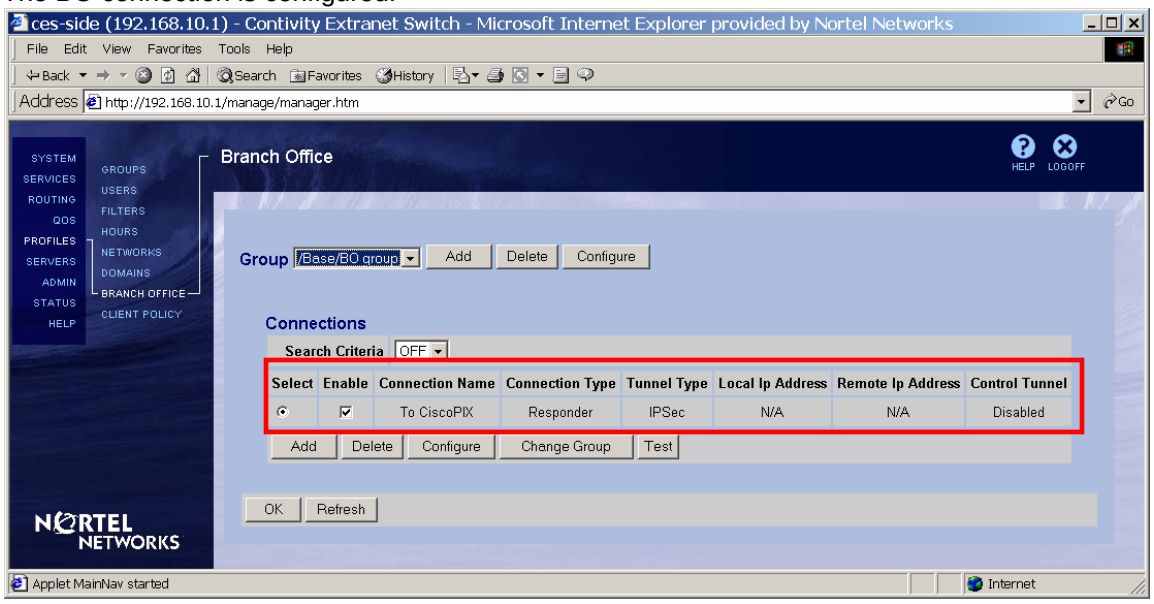
Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Leave the rest of the fields as they were configured for the previous example and click **OK** at the bottom of the page:



Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

The BO connection is configured:



2.5. Configuring PIX

Erase config on PIX to remove config from the previous example:

```
cisco-side(config)#write erase
Erase PIX configuration in flash memory? [confirm]
```

Reload PIX to start configuration from a scratch:

```
pixfirewall(config)# reload
Proceed with reload? [confirm]
Rebooting....
```

Enter **NO** when prompted to configure PIX through the interactive prompts:

```
Pre-configure PIX Firewall now through interactive prompts [yes]? no
Type help or '?' for a list of available commands.
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Enter privileged mode:

```
pixfirewall> en
Password:
```

Enter configuration mode:

```
pixfirewall# conf t
pixfirewall(config)#
```

Configure and enable interfaces eth0 and eth1, in this example auto speed selection will be used for interfaces:

```
cisco-side(config)# interface ethernet1 auto
cisco-side(config)# interface ethernet0 auto
```

We will configure Ethernet 0 to be private interface and Ethernet 1 to be public interface. Configure eth 0 to be private (by default eth 0 is public and eth1 is private), this will swap the interfaces and will automatically make eth1 public:

```
pixfirewall(config)# nameif ethernet0 inside security100
interface 1 name "inside" swapped with interface 0 name "outside"
```

Configure hostname (cisco-side) on PIX:

```
pixfirewall(config)# hostname cisco-side
cisco-side(config)#
```

Create an access list that will be used with crypto algorithm to define what traffic will be encrypted and what will be sent in clear text. The permitted traffic will be encrypted and denied traffic will be sent in clear. We need to permit traffic from Cisco PIX private side (192.168.20.0/24) to CES private side (192.168.10.0/24) this will force all the traffic between private networks to go through the tunnel. 15 is the access list number we are creating:

```
cisco-side(config)# access-list 15 permit ip 192.168.20.0 255.255.255.0
192.168.10.0 255.255.255.0
```

Configure the IP address for the PIX private interface or inside address (192.168.20.20/24):

```
cisco-side(config)# ip address inside 192.168.20.20 255.255.255.0
```

Configure the IP address for the PIX public interface or outside address (192.168.100.2/24):

```
cisco-side(config)# ip address outside 192.168.100.2 255.255.255.0
```

We do not need to NAT over IPSec tunnel:

```
cisco-side(config)# nat (inside) 0 access-list 15
cisco-side(config)# nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Configure default outside gateway pointing to CES public interface (1921.68.100.1) (**Note**: In this example CES and PIX public interfaces are directly connected, if a router is used between CES and PIX enter the routers address as a default gateway):

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
cisco-side(config)# route outside 0.0.0.0 0.0.0.0 192.168.100.1 1
```

Configure Cisco PIX to accept IPSec traffic. This assures that traffic through the tunnel is not blocked by other access lists that might exist on the PIX box. Alternatively, access lists explicitly allowing particular traffic across PIX need to be configured via access list or conduit commands. In this example we will allow all IPSec traffic:

```
cisco-side(config)# sysopt connection permit-ipsec
```

Create an IPSec transform set to define what encryption and authentication algorithms will be used for the tunnel. We need to create a transform set (pix) for the DES with SHA integrity:

```
cisco-side(config)# crypto ipsec transform-set pix esp-des esp-sha-hmac
```

Create an IPSec crypto map (map number 1, named pixmap) that will use IPSec ISAKMP:

```
cisco-side(config)# crypto map pixmap 1 ipsec-isakmp
```

Associate a crypto map with the created access list:

```
cisco-side(config)# crypto map pixmap 1 match address 15
```

Set peer address (CES public address – 192.168.100.1) for the crypto map:

```
cisco-side(config)# crypto map pixmap 1 set peer 192.168.100.1
```

Associate crypto map with the created transform set (pix):

```
cisco-side(config)# crypto map pixmap 1 set transform-set pix
```

Bind crypto map with the outside interface:

```
cisco-side(config)# crypto map pixmap interface outside
```

Enable ISAKMP service for the outside interface:

```
cisco-side(config)# isakmp enable outside
```

Configure a pre-shared key (test) for authentication with CES (192.168.100.1):

```
cisco-side(config)# isakmp key test address 192.168.100.1 netmask
255.255.255.255
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

When initiating a connection Cisco PIX will use main mode negotiation by default just like in regular peer-to-peer tunnel. For Contivity to recognize ABOT initiator aggressive mode should be used for tunnel negotiation. To make PIX use aggressive mode the isakmp identity must be set to key id. Push PIX to use aggressive mode when initiating a connection to CES. For that set identity to key-id (ces):

```
cisco-side(config)# isakmp identity key-id ces
```

Configure Cisco PIX to use pre-shared key authentication:

```
cisco-side(config)# isakmp policy 1 authentication pre-share
```

Configure Cisco to use DES for encryption:

```
cisco-side(config)# isakmp policy 1 encryption des
```

Configure Cisco to use SHA1 for authentication:

```
cisco-side(config)# isakmp policy 1 hash sha
```

Configure Cisco to use Diffie-Hellman group 1:

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

View the configuration:

```
cisco-side(config)# show run
: Saved
:
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 inside security100
nameif ethernet1 outside security0
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco-side
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 15 permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
pager lines 24
mtu inside 1500
mtu outside 1500
ip address inside 192.168.20.20 255.255.255.0
ip address outside 192.168.100.2 255.255.255.0
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 15
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 192.168.100.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
no snmp-server contact
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set pix esp-des esp-sha-hmac
crypto map pixmap 1 ipsec-isakmp
crypto map pixmap 1 match address 15
crypto map pixmap 1 set peer 192.168.100.1
crypto map pixmap 1 set transform-set pix
crypto map pixmap interface outside
isakmp enable outside
isakmp key ******** address 192.168.100.1 netmask 255.255.255.255
isakmp identity key-id ces
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash sha
isakmp policy 1 group 1
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:c94d4849677031bfb4007c614e46ba07
: end
```

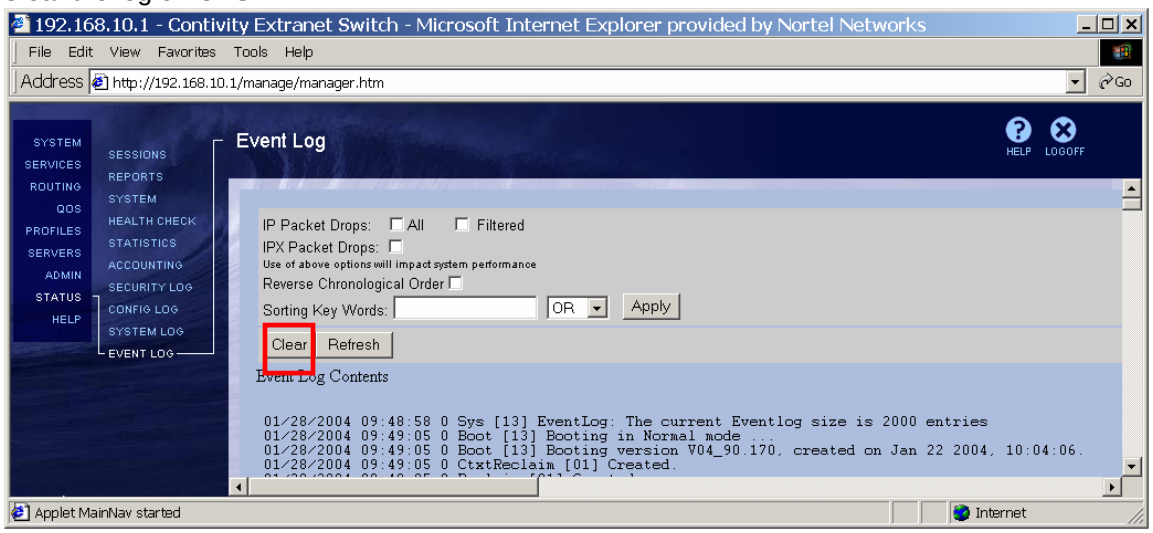
Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Save the configuration:

```
cisco-side(config)# write mem
Building configuration...
Cryptochecksum: bc663e92 4b3c7b02 8fe04442 bafb3abe
[OK]
```

2.6. Testing the configuration

Clear the log on CES:



Enable debug on Cisco PIX to see the connection establishment:

```
cisco-side# debug crypto isakmp 2
cisco-side# debug crypto ipsec 2
```

Ping from WS1 (192.168.10.11) to WS2 (192.168.20.22) to make sure responder could not initiate the connection:

```
C:\>ping 192.168.20.22
Pinging 192.168.20.22 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.22:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

The ping is lost as the tunnel could not be initiated by the responder.

Ping from WS2 (192.168.20.22) to WS1 (192.168.10.11):

```
C:\>ping 192.168.10.11
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
Pinging 192.168.20.22 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.11: bytes=32 time=230ms TTL=29
Reply from 192.168.10.11: bytes=32 time<10ms TTL=29
Reply from 192.168.10.11: bytes=32 time<10ms TTL=29

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  230ms, Average =  57ms
```

Check the log on CES:

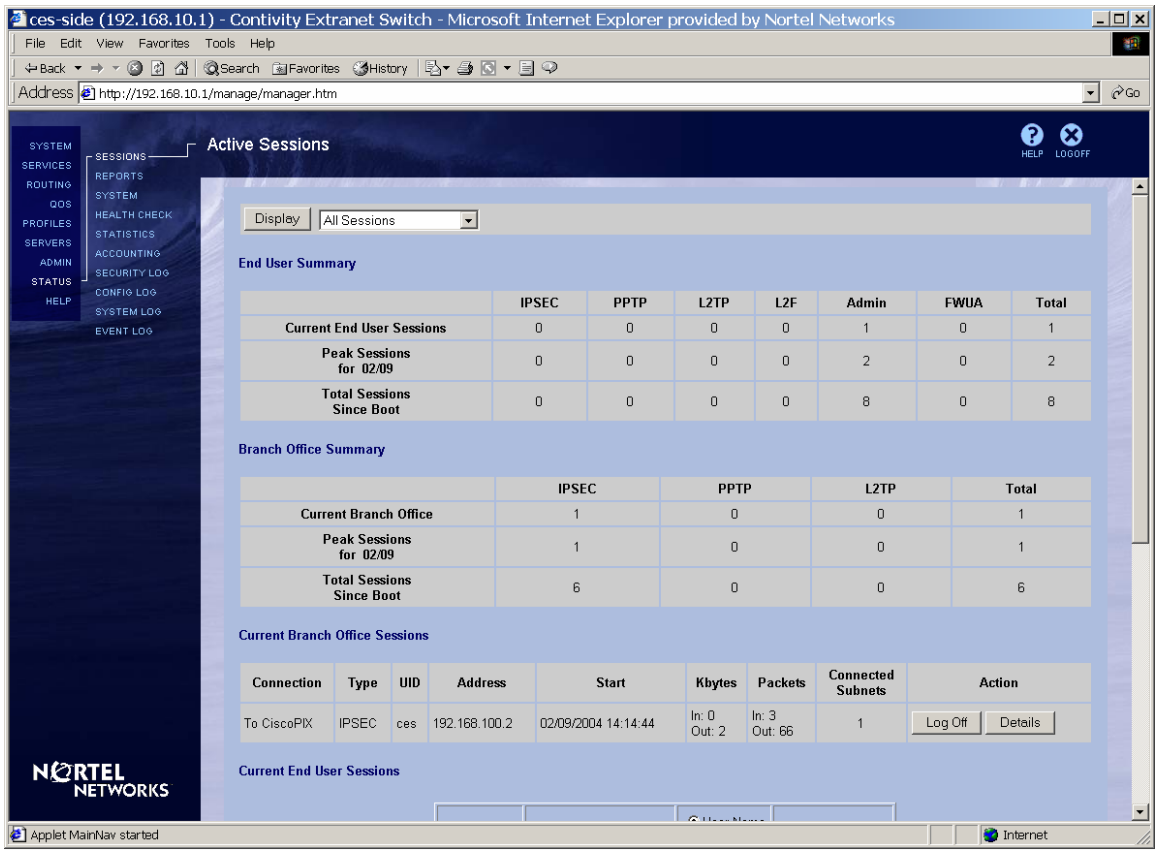
```
02/09/2004 14:11:42 0 Security [11] Session: IPSEC[ces] attempting login
02/09/2004 14:11:42 0 Security [01] Session: IPSEC[ces] has no active
sessions
02/09/2004 14:11:42 0 Security [01] Session: IPSEC[ces] To CiscoPIX has
no active accounts
02/09/2004 14:11:42 0 Security [00] Session: IPSEC - did not find
matching gateway session
02/09/2004 14:11:42 0 ISAKMP [02] Oakley Aggressive Mode proposal
accepted from ces (192.168.100.2)
02/09/2004 14:11:42 0 ISAKMP [02] Initial Contact Payload Received
02/09/2004 14:11:42 0 ISAKMP [02] Group settings set to ignore Initial
Contact Payload.
02/09/2004 14:11:42 0 Security [01] Session: IPSEC[ces]:31 SHARED-SECRET
authenticate attempt...
02/09/2004 14:11:42 0 Security [01] Session: IPSEC[ces]:31 attempting
authentication using LOCAL
02/09/2004 14:11:42 0 Security [11] Session: IPSEC[ces]:31 authenticated
using LOCAL
02/09/2004 14:11:42 0 Security [11] Session: IPSEC[ces]:31 bound to
group /Base/BO group/To CiscoPIX
02/09/2004 14:11:42 0 Security [01] Session: IPSEC[ces]:31 Building
group filter permit all
02/09/2004 14:11:42 0 Security [01] Session: IPSEC[ces]:31 Applying
group filter permit all
02/09/2004 14:11:42 0 Security [11] Session: IPSEC[ces]:31 authorized
02/09/2004 14:11:42 0 Branch Office [01] Setting up branch office
gateway [192.168.100.2] uid:[ces]
02/09/2004 14:11:42 0 Branch Office [01] InstallBOSession:
IPSEC[192.168.100.2] routing [STATIC]
02/09/2004 14:11:42 0 RTM [10] netWrite RTM_RouteDef: N 192.168.20.0 M
255.255.255.0 NumNH 1 NH 192.168.100.2 CM 0x744d7e8
02/09/2004 14:11:42 0 RTM [00] writeNewEntry: adding new: 192.168.20.0
to 192.168.20.255
02/09/2004 14:11:42 0 RTM [00] NextHop:newEntry NextHop: 192.168.100.2
NHI 192.168.100.1 C 66 CM 0x744d7e8 PR (6c18e84) 192.168.100.1
02/09/2004 14:11:42 0 Branch Office [01] 744c978
BranchOfficeCtxtCls::InstallRoute: Route installed for rem[192.168.20.0-
255.255.255.0]@192.168.100.2
02/09/2004 14:11:42 0 McRelay [00] Received circuit up for circuit num =
66. local 192.168.20.0
02/09/2004 14:11:42 0 McRelay [00] MC circuit enabled. circuit num = 66,
ifp 1881e34
02/09/2004 14:11:42 0 RTM [00] Best::nextRoute fini for 0x40
02/09/2004 14:11:42 0 ISAKMP [02] ISAKMP SA established with ces
(192.168.100.2)
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
02/09/2004 14:11:42 0 Security [11] Session: network IPSEC[192.168.20.0-
255.255.255.0] attempting login
02/09/2004 14:11:42 0 Security [11] Session: network IPSEC[192.168.20.0-
255.255.255.0] logged in from gateway [192.168.100.2]
02/09/2004 14:11:42 0 Security [12] Session: IPSEC[ces]:31 physical
addresses: remote 192.168.100.2 local 192.168.100.1
02/09/2004 14:11:42 0 Security [12] Session: IPSEC[-]:34 physical
addresses: remote 192.168.100.2 local 192.168.100.1
02/09/2004 14:11:42 0 BaseCmsClient [00] RipCmsClient::New() : handling
new circuit event for circuit 66 [0x5975438].
02/09/2004 14:11:42 0 BaseCmsClient [00] RipCmsClient::New() : handling
new circuit event for circuit 66 [0x5975438].
02/09/2004 14:11:42 0 RTM [00] Best::nextRoute fini for 0x1
02/09/2004 14:11:42 0 DHCP Relay Table [00] Circuit config node for
interface 192.168.20.0 inserted
02/09/2004 14:11:42 0 Outbound ESP from 192.168.100.1 to 192.168.100.2
SPI 0x08d531cc [03] ESP encap session SPI 0xcc31d508 bound to cpu 0
02/09/2004 14:11:42 0 Inbound ESP from 192.168.100.2 to 192.168.100.1
SPI 0x0015f641 [03] ESP decap session SPI 0x41f61500 bound to cpu 0
02/09/2004 14:11:42 0 Branch Office [00] 744c978
BranchOfficeCtxtCls::RegisterTunnel: rem[192.168.20.0-
255.255.255.0]@[192.168.100.2] loc[192.168.10.0-255.255.255.0]
overwriting tunnel context [0] with [6fa7c18]
02/09/2004 14:11:42 0 ISAKMP [03] Established IPsec SAs with ces
(192.168.100.2):
02/09/2004 14:11:42 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA outbound
SPI 0x8d531cc
02/09/2004 14:11:42 0 ISAKMP [03] ESP 56-bit DES-CBC-HMAC-SHA inbound
SPI 0x15f641
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

Check the status of the connection on **Status→Sessions** screen. Note the presence of the BO connection:



Check the IPSec Sas on PIX:

```
cisco-side(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: pixmap, local addr. 192.168.100.2

   local  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current peer: 192.168.100.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
    #pkts decaps: 66, #pkts decrypt: 66, #pkts verify 66
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.100.2, remote crypto endpt.:
192.168.100.1
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 527a6

     inbound esp sas:
      spi: 0x37e084d5(937460949)
```

Contivity – Cisco PIX IPSec ABOT using pre-shared key authentication

```
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: pixmap
        sa timing: remaining key lifetime (k/sec): (4607995/28578)
        IV size: 8 bytes
        replay detection support: Y

    inbound ah sas:
    inbound pcp sas:

   outbound esp sas:
      spi: 0x527a6(337830)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: pixmap
        sa timing: remaining key lifetime (k/sec): (4607999/28578)
        IV size: 8 bytes
        replay detection support: Y

    outbound ah sas:
    outbound pcp sas:
```

Check the ISAKMP Sas on PIX:

```
cisco-side(config)# show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending     created
   192.168.100.1    192.168.100.2    QM_IDLE           0           1
```


To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Networks Technical Support on the web at: http://www.nortel.com/support

If after following this guide you are still having problems, please ensure you have carried out the steps exactly as in this document. If problems still persist, please contact Nortel Networks Technical Support (contact information is available online at: http://www.nortel.com/cgi-bin/comments/comments.cgi?key=techsupport_cu).

We welcome you comments and suggestions on the quality and usefulness of this document. If you would like to leave a feedback please send your comments to: CRCONT@nortel.com

Author: Kristina Senkova