Allied Telesis

AlliedWare™ OS

How To | Create Concurrent VPNs with Remote Routers, Microsoft Windows Vista Clients and XP Clients, over NAT-T

Contents

Introduction

This document describes how to provide secure remote access through IP security (IPsec) Virtual Private Networks (VPNs), with an emphasis on using an Allied Telesis router at a head office and roaming Vista clients.

This VPN solution is suitable for any business deployment and provides your office with secure Internet access and firewall protection, plus remote encrypted VPN access for your travelling staff. The solution includes an office-to-office VPN as well, so that a remote office can securely access the head office.

The solution allows for IPsec NAT Traversal, which permits VPN clients to communicate through Network Address Translation (NAT) gateways over the Internet. For example, business travellers (road warriors) commonly use IPsec on their laptop to gain remote VPN access to the central office. When working off-site, these users sometimes need to connect to the Internet through a NAT gateway such as from a hotel. Also, NAT gateways are often part of a company's firewall and let its Local Area Network (LAN) appear as one IP address to the world.

For more information about NAT gateways, see RFC 1631 *The IP Network Address Translator (NAT)*, and the Network Address Translation section in the Firewall chapter of your device's Software Reference.

What information will you find in this How To Note?

This How To Note starts with the configuration for a head office router on page 5. This configuration allows the head office to create concurrent VPN tunnels with:

- a remote office router. The configuration for this starts on page 10.
- Windows Vista roaming clients. The configuration for these starts on page 12.
- Windows XP roaming clients. This Note does not include the configuration for these—see the How To Note *How To Create a VPN between an Allied Telesis Router and a Microsoft Windows XP Client, over NAT-T.*

Then the How To Note displays debugging output from when:

- the remote office router initiates a tunnel
  - output from the head office router, from page 27
  - output from the remote office router, from page 39
- a Vista client initiates a tunnel, from page 50
- an XP client initiates a tunnel, from page 65
- you disconnect an XP client, from page 81
- you disconnect a Vista client, from page 83

Color coding For your convenience, the configuration and debugging output pages are color-coded:

head office	remote office	Vista client	XP client

Related How To Notes

Allied Telesis offers How To Notes with a wide range of VPN solutions, from quick and simple solutions for connecting home and remote offices, to advanced multi-feature setups. Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors.

For a complete list of VPN How To Notes, see the *Overview of VPN Solutions in How To Notes* in the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx.

The collection includes Notes that describe how to interoperate with Windows 2000 and XP clients.

Which products and software version does this apply to?

This How To Note applies to the following routers and switches, running AlliedWare software version 291-08 or later:

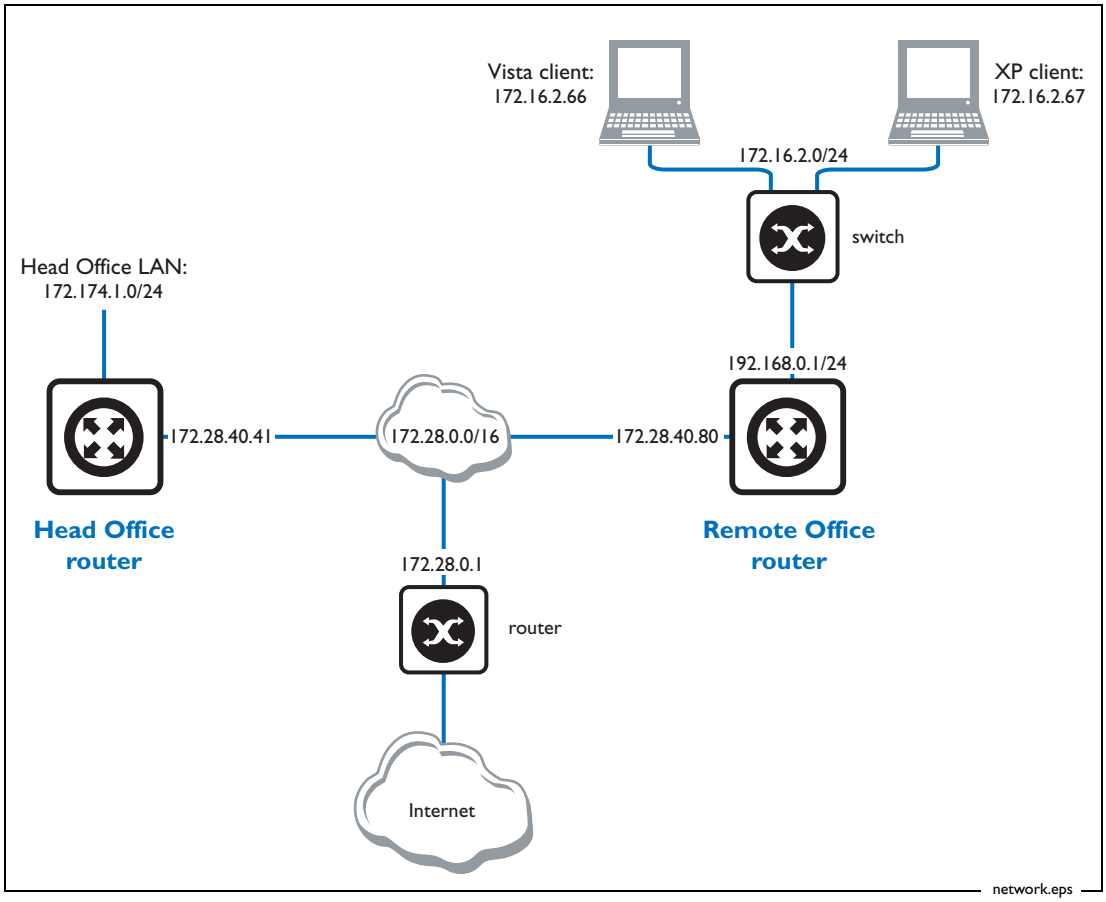
- AR400 Series routers
- AR750S and AR770S routers
- Rapier i Series switches
- AT-8800 Series switches

It requires firewall and 3DES licenses. If these licenses are not already installed on your device, you can purchase them from your Allied Telesis distributor.

The network

Network diagram

We set up the three solutions in a lab, using the network shown in the following figure.



The figure shows a head office and a remote office.

The head office router is connected to a LAN (through 172.174.1.0/24), and to the Internet and the remote office (through 172.28.0.0/16).

The remote office router is also connected to a LAN, the head office and the Internet. However, the remote office router performs two completely separate roles in this How To Note:

- in the remote office configuration (page 10), the remote office router acts as a VPN peer to the head office.
- in the Vista client configuration (page 12) and with the XP client, the remote office router acts as a NAT gateway. In a real-world setting, the clients would be roaming and the NAT gateway would be at a location such as a hotel.

Configure the head office router

Initial security setup

Before adding the ISAKMP and IPSec configuration, set up the router with the following important details.

1. Create two keys to use for Secure Shell (SSH)

Use the commands:

```
create enco key=1 description="Server Key" type=rsa length=768 format=ssh
create enco key=2 description="Host Key" type=rsa length=1024 format=ssh
```

After each of these commands, the router displays the following information.

```
Info (1073278): RSA Key Generation process started.
Manager >
Info (1073279): RSA Key generation process completed.
```

2. Create a third key for ISAKMP to use as a preshared key

For security reasons, **do not use the same value as this example.**

Use the command:

```
create enco key=3 description="ISAKMP PSK" type=general value=secret
```

We use this encryption key on the Vista clients (see step 5 on page 21).

3. Check the key configuration

Use the command:

```
show enco key
```

This results in the following output.

```
 ID  Type       Length Digest   Description              Mod   IP
---------------------------------------------------------------------------
  1  RSA-PRIVATE  768 A40EB1F4 Server Key                -     -
  2  RSA-PRIVATE 1024 2BB712B4 Host Key                  -     -
  3  GENERAL        6 EE635A9D ISAKMP PSK                -     -
```

4. Check feature licences

Check that you have a 3DES feature licence for the ISAKMP policy.

```
show feature
```

You can purchase feature licences from your Allied Telesis distributor.

If necessary, install the licence, using the password provided by your distributor.

```
enable feature=3des pass=<licence-number>
```

5. Add a security officer

Add a security officer. This step is important because a security officer must exist before you enable system security (which you do in the next step).

```
add user=secoff pass=<password> priv=securityOfficer telnet=yes login=yes
```

After this command, the router displays the following information.

```
Number of Radius-backup users..... 0

User Authentication Database
-------------------------------------------------------------------------
Username: secoff ()
   Status: enabled    Privilege: Sec Off   Telnet: yes   Login: yes   RBU: no
   Logins: 0          Fails: 0        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
-------------------------------------------------------------------------
```

6. Enable system security

Enable system security so that the newly created keys will be stored permanently. They would otherwise be deleted if the router restarted.

```
enable system security
```

Once security mode is enabled, you need to log in as the security officer to enter most configuration-altering commands.

7. Save the configuration and set the router to use it at startup

Use the command:

```
create config=vpn.cfg set
```

Configuration template

This section contains a configuration script for the head office. You can copy and paste the script to an editor on your PC, modify addresses, passwords and any other requirements for all your individual sites, and then use TFTP, HTTP or ZMODEM to transfer the files to your routers.

Please refer to the "Managing Configuration Files and Software Versions" chapter in the *Software Reference* for more information about loading files onto the router.

For detailed explanations about the CLI configuration, see the How To Note *How To Configure VPNs In A Corporate Network, With Optional Prioritisation Of VoIP.*

```
set system name="Head Office"

#  User configuration
add user=secoff pass=<your-secoff-password> priv=securityOfficer lo=yes
set user=secoff telnet=yes netmask=255.255.255.255
add user=vista_user pass=<user-password> lo=no
#  Specify the IP address that L2TP will issue to the VPN user who logs in
#  as vista_user.
set user=vista_user telnet=no ipaddr=192.168.254.99 netmask=255.255.255.255
add user=xp_user pass=<user-password> lo=no
set user=xp_user telnet=no ipaddr=192.168.254.66 netmask=255.255.255.255

#  PPP templates configuration
create ppp template=1
set ppp template=1 bap=off ippool="myippool" authentication=chap
   mssheader=120 echo=30

#  L2TP configuration
enable l2tp
enable l2tp server=both
add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1

#  VLAN general configuration
create vlan="vlan100" vid=100

#  VLAN port configuration
add vlan="100" port=1-5

#  IP configuration
enable ip
add ip int=eth0 ip=172.28.40.41
add ip int=vlan100 ip=172.174.1.254 mask=255.255.255.0
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=172.28.0.1
create ip pool="myippool" ip=192.168.66.66-192.168.66.77
add ip dns prim=10.32.16.105 seco=202.49.72.50
```

head office

```
# Firewall configuration
enable firewall
enable firewall notify=mail to=<administrator-email-address>
create firewall policy="fw"
create firewall policy="fw" dy=dynamic
add firewall policy="fw" dy=dynamic us=ANY
enable firewall policy="fw" icmp_f=all
add firewall policy="fw" int=vlan100 type=private
add firewall policy="fw" int=dyn-dynamic type=private
add firewall policy="fw" int=eth0 type=public
# NAT for local users
add firewall poli="fw" nat=enhanced int=vlan100 gblin=eth0
# NAT for the IPSec users
add firewall poli="fw" nat=enhanced int=dyn-dynamic gblin=eth0
# Permit incoming SSH
add firewall poli="fw" ru=1 ac=allo int=eth0 prot=tcp po=22 ip=172.28.40.41
   gblip=172.28.40.41 gblp=22
# Permit incoming ISAKMP
add firewall poli="fw" ru=2 ac=allo int=eth0 prot=udp po=500 ip=172.28.40.41
   gblip=172.28.40.41 gblp=500
# Permit ESP over UDP (for IPSec NAT-T)
add firewall poli="fw" ru=3 ac=allo int=eth0 prot=udp po=4500 ip=172.28.40.41
   gblip=172.28.40.41 gblp=4500
# Permit L2TP specifically over IPSec
add firewall poli="fw" ru=4 ac=allo int=eth0 prot=udp po=1701 ip=172.28.40.41
   gblip=172.28.40.41 gblp=1701 encap=ipsec
# Do not apply NAT on incoming traffic destined for private LAN addresses;
# send to IPSec instead
add firewall poli="fw" ru=5 ac=non int=eth0 prot=ALL ip=172.174.1.0-
   172.174.1.254 enc=ips
# Do not apply NAT to traffic from LAN destined for remote office
add fire poli=fw ru=6 int=vlan100 act=nonat proto=all ip=172.174.1.1-
   172.174.1.254 remoteip=192.168.0.1-192.168.0.254

# SSH configuration
enable ssh server serverkey=1 hostkey=2 expirytime=0 logintimeout=60
add ssh user=secoff password=secoff

# IPSEC configuration
create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha
set ipsec sas=1 mod=transport
create ipsec sas=2 key=isakmp prot=esp enc=3desouter hasha=md5
set ipsec sas=2 mod=transport
create ipsec sas=3 key=isakmp prot=esp enc=des hasha=sha
set ipsec sas=3 mod=transport
create ipsec sas=4 key=isakmp prot=esp enc=des hasha=md5
set ipsec sas=4 mod=transport
create ipsec bund=1 key=isakmp string="1 or 2 or 3 or 4"
```

head office

```
# IPSec is interested in the following traffic types
create ipsec pol="isakmp" int=eth0 ac=permit lp=500 rp=500
create ipsec pol="natt_udp" int=eth0 ac=permit lp=4500
# Windows (Vista/XP) hosts will match the following policy
create ipsec pol="windows_warriors" int=eth0 ac=ipsec key=isakmp bund=1
   peer=ANY isa="windows_isakmp" lp=1701 tra=UDP
create ipsec sas=10 key=isakmp prot=esp enc=3desouter hasha=sha
create ipsec bund=10 key=isakmp string="10"
create ipsec pol="office" int=eth0 ac=ipsec key=isakmp bund=10 peer=any
   isa="office" lad=172.174.1.0 lma=255.255.255.0 rad=192.168.0.0
   rmas=255.255.255.0
# All other traffic is defined here.
create ipsec pol="internet" int=eth0 ac=permit
enable ipsec

# ISAKMP configuration
# Vista and XP definition, don't define localid or remoteid
create isakmp pol="windows_isakmp" pe=any enc=3desouter key=3 natt=true gro=2
# Remote office definition
create isakmp pol="office" pe=any key=3 natt=true
enable isakmp
```

Configure the remote office router

Initial security setup

Before adding the ISAKMP and IPSec configuration, set up the router with the following important details:

- create a security officer (this needs to be in the script as well)

```
add user=secoff pass=<your-secoff-password> priv=securityofficer lo=yes
   telnet=yes
```

- enable system security

```
enable system security
```

- log in as the security officer

```
login secoff
```

- enable the 3DES feature licence if it is not factory-enabled

```
enable feature=3des pass=<licence-number>
```

- define preshared encryption keys for SSH and ISAKMP

```
cre enco key=1 type=rsa length=768 desc="server key" format=ssh
cre enco key=2 type=rsa length=1024 desc="host key" format=ssh
cre enco key=3 type=general desc="ISAKMP PSK" value=<alphanumeric>
```

Configuration template

This section contains a configuration script for the remote office router. You can copy and paste the script to an editor on your PC, modify addresses, passwords and any other requirements for all your individual sites, and then use TFTP, HTTP or ZMODEM to transfer the files to your routers.

Note that this router does not have a firewall configuration. A firewall configuration is not necessary for IPSec, but you should always configure a firewall on routers with public-facing interfaces.

```
#  System configuration
set system name="Remote Office"

#  User configuration
add user=secoff pass=secoff priv=securityOfficer lo=yes
set user=secoff telnet=yes netmask=255.255.255.255

#  VLAN configuration
create vlan="vlan2" vid=2
add vlan=2 port=1-5

#  IP configuration
enable ip
add ip int=vlan1 ip=172.28.40.80
add ip int=vlan2 ip=192.168.0.1

#  SSH configuration
enable ssh server serverkey=1 hostkey=2 expirytime=0 logintimeout=60
add ssh user=secoff password=secoff

#  IPSEC configuration
create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha
create ipsec bund=1 key=isakmp string="1"
create ipsec pol="isakmp" int=vlan1 ac=permit
set ipsec pol="isakmp" lp=500 rp=500
create ipsec pol="remote_office" int=vlan1 ac=ipsec key=isakmp bund=1
   peer=172.28.40.41 isa="remote_office"
set ipsec pol="remote_office" lad=192.168.0.0 lma=255.255.255.0
   rad=172.174.1.0 rma=255.255.255.0
create ipsec pol="internet" int=vlan1 ac=permit
enable ipsec

#  ISAKMP configuration
create isakmp pol="remote_office" pe=172.28.40.41 key=3 natt=true
enable isakmp
```

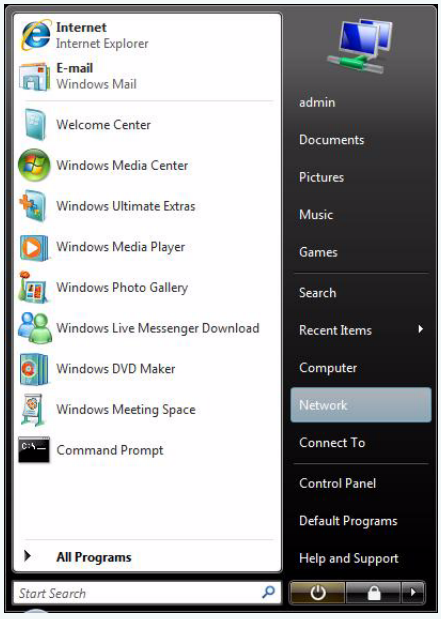
Configure a Microsoft Windows Vista client

This section describes how to set up a VPN between a Vista client and the Head Office. Note that no registry hacks, special patches or service packs are required.

Create the connection

1. Open the Network and Sharing Center

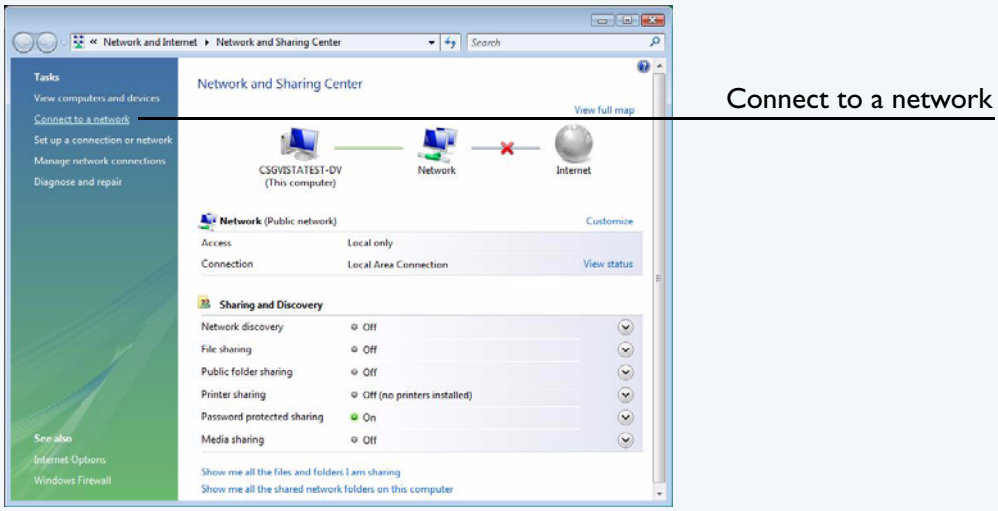
Open the Start menu, as shown in the following figure, right-click on Network, and select Properties.



This opens the Network and Sharing Center.

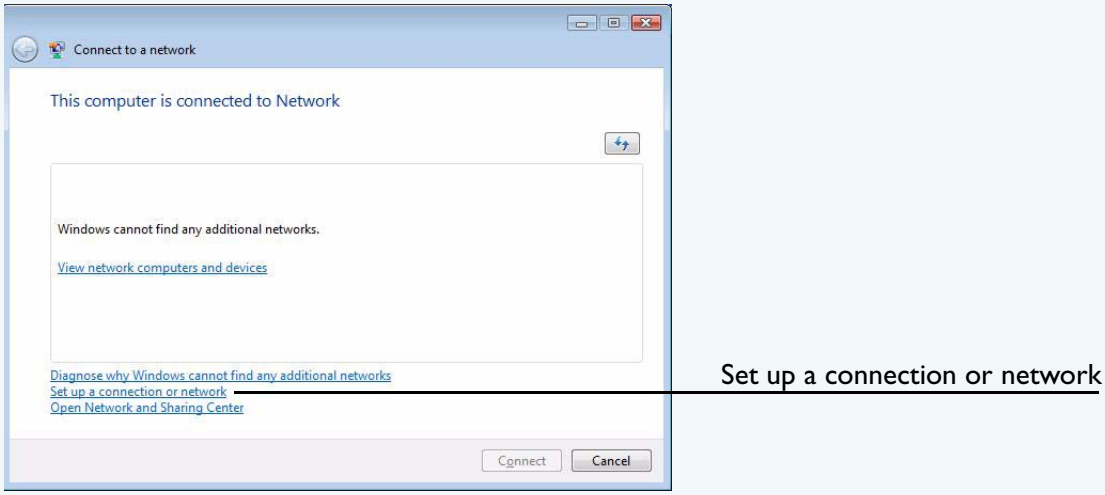
2. Connect to the network

In the left-hand menu of the Network and Sharing Center, click on "Connect to a network", as shown in the following figure.



3. Start creating the new connection

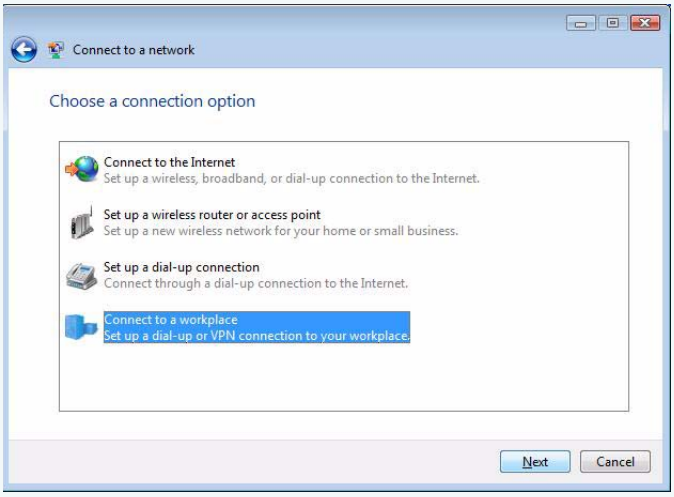
At the bottom of the resulting window, click on "Set up a connection or network", as shown in the following figure.



This opens the connection wizard.

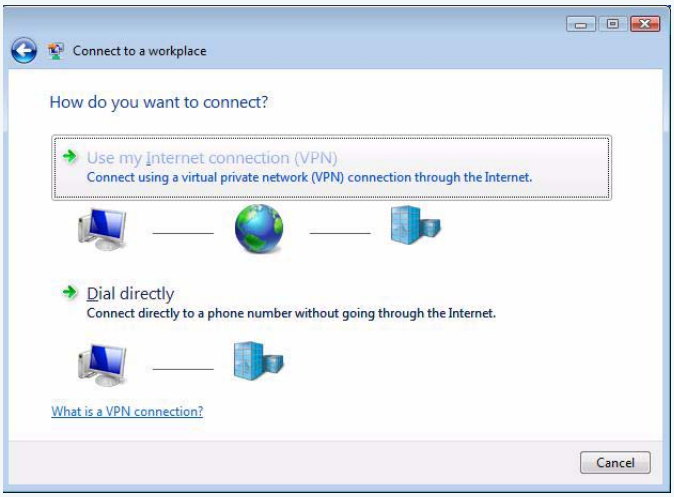
4. Select the connection option

On the first page of the wizard, select "Connect to a workplace" and click the Next button.



5. Select to connect through a VPN

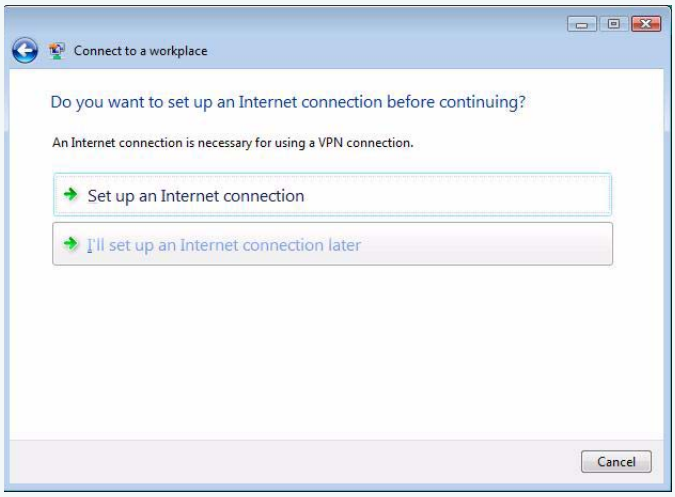
Select "Use my Internet connection (VPN)" and click the Next button.



6. Choose not to set up an Internet connection

Select "I'll set up an Internet connection later" and click the Next button.

In this example, we assume that the VPN will be initiated over the user's cable modem at home or (when the user is travelling) from a hotel local area network. Therefore the VPN will be initiated over a connection that is already up. If you are instead connecting via dial-up, you might need to set up a dial-up connection. You can do that at this stage, or later.



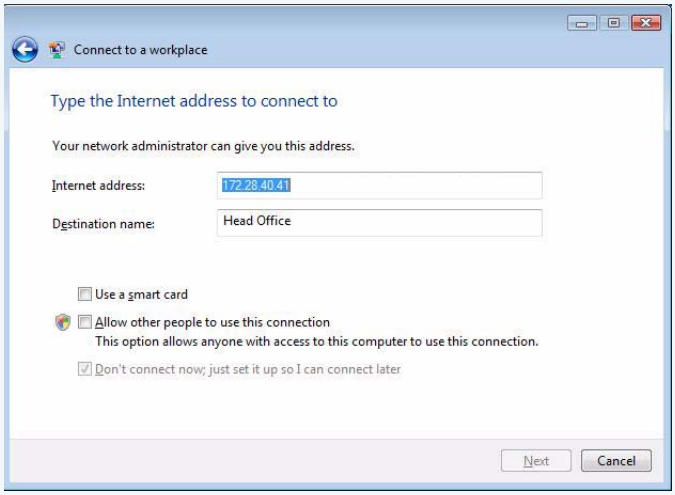
7. Type in the Internet address to connect to

In the "Internet address" field, type in the IP address of the Head Office. In this example, the IP is 172.28.40.41.

In the "Destination name" field, give the connection a meaningful name. The name has no effect on the operation of the VPN; it is just the connection name that appears in the list of network connections.

In this example, we do not use the smart card option. As administrator, you need to decide whether to use the smart card, and whether to allow other people who use this Vista PC to access this VPN connection.

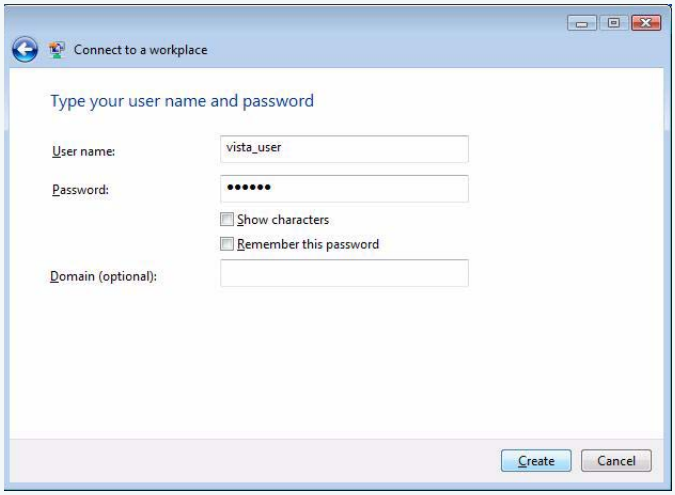
Then click the Next button.



8. Choose a user name and password

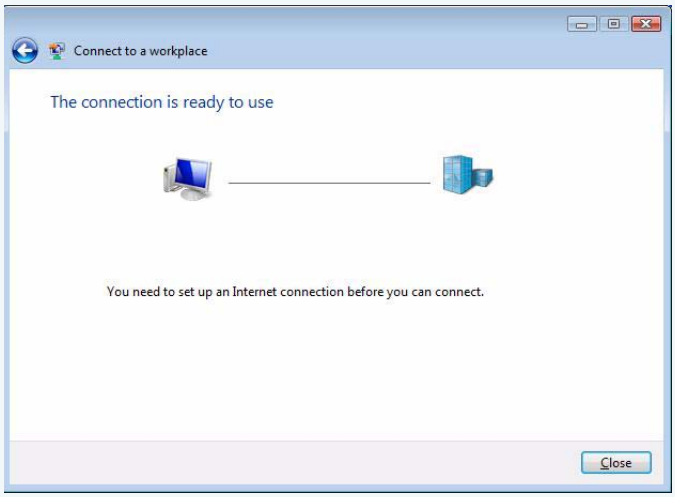
Enter a user name and password, and choose whether to have Vista remember the password. We recommend **not** letting Vista remember passwords, particularly on a laptop. If the laptop is stolen, the VPN connection could be initiated by the thieves.

Then click the Create button.



9. Close the wizard

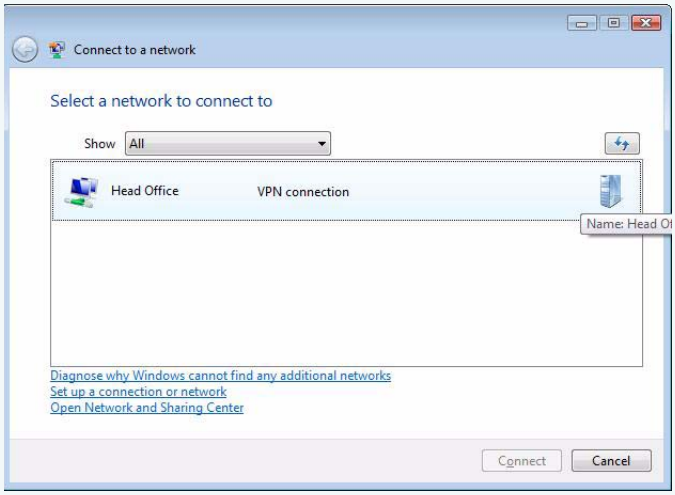
Vista informs you that the connection is ready to use, but it is not yet ready. Ignore the message about setting up an Internet connection and click the Close button.



Modify the connection

1. Open the Head office connection properties

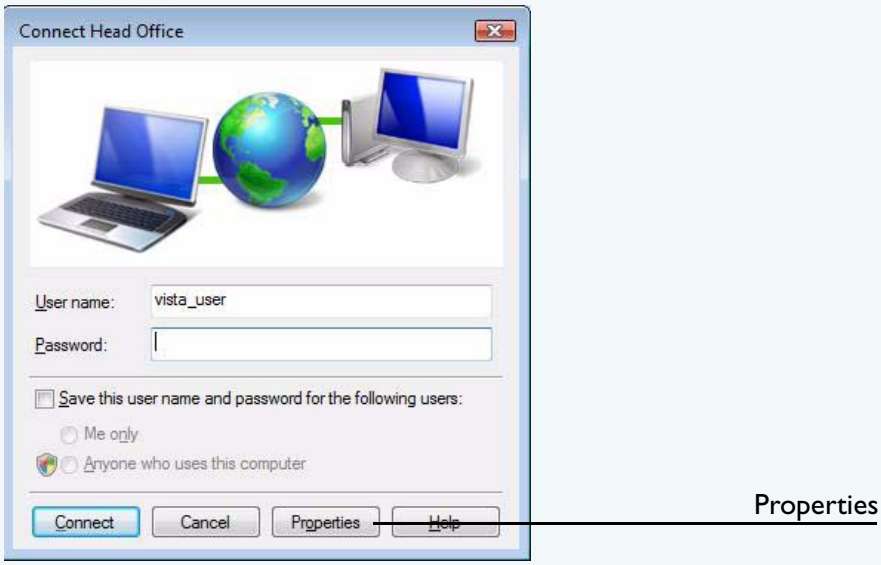
From the Networking and Sharing Center, click on "Connect to a network". This time, the resulting window shows the Head Office connection, as shown in the following figure.



Open the Head Office properties by either

- double-clicking on it. This is possible if there is network connectivity, which you can see by looking for a PC shaped icon to the right of the connection name.
- right-clicking on it and choosing Properties. If there is no connectivity, you have to do this.

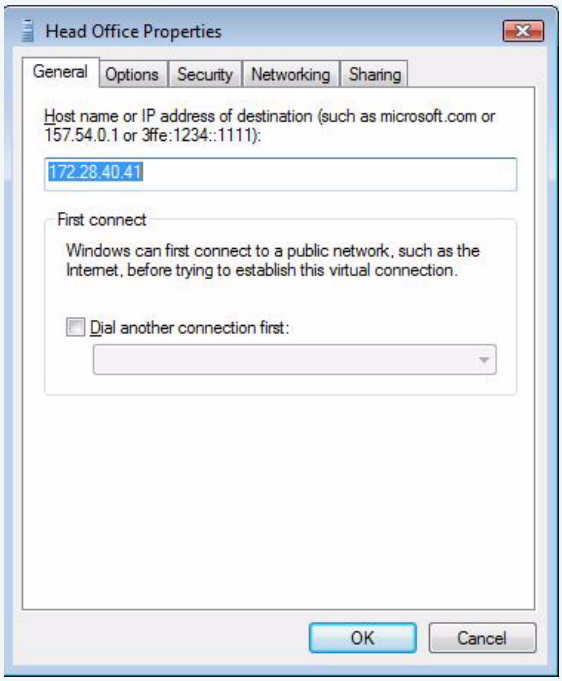
In this example, the connection is present, so we are able to double-click. This displays the following window.



Press the "Properties" button, as shown in the above figure.

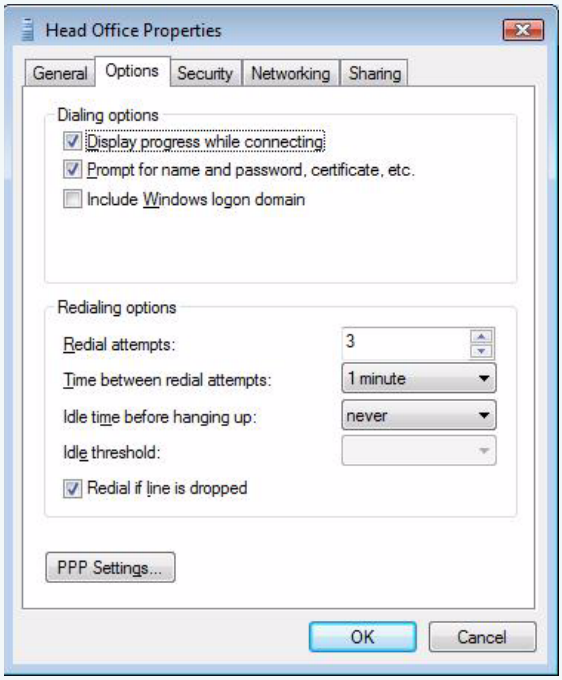
2. Check the destination address

On the General tab, the destination address should be the IP address of the Head Office router, as shown in the following figure.



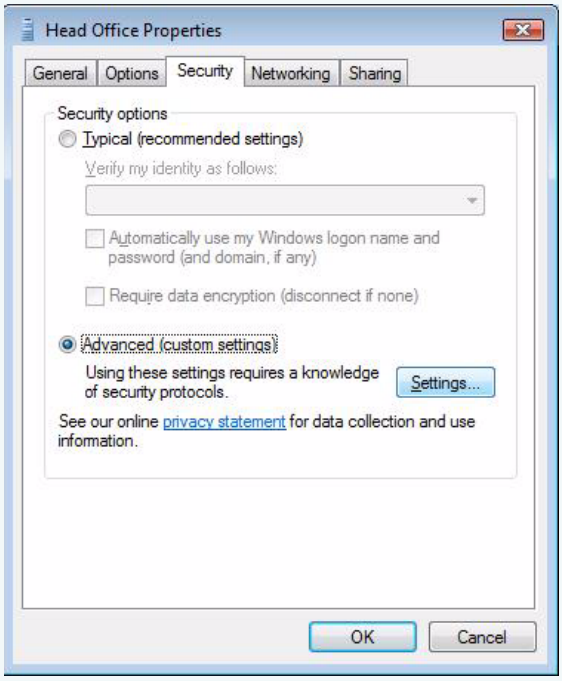
3. Configure the options settings

On the Options tab, deselect the "Include Windows logon domain" checkbox if you do not need it or do not know what it is.



4. Configure the security settings

On the Security tab, select "Advanced (custom settings)" and click on the Settings button.



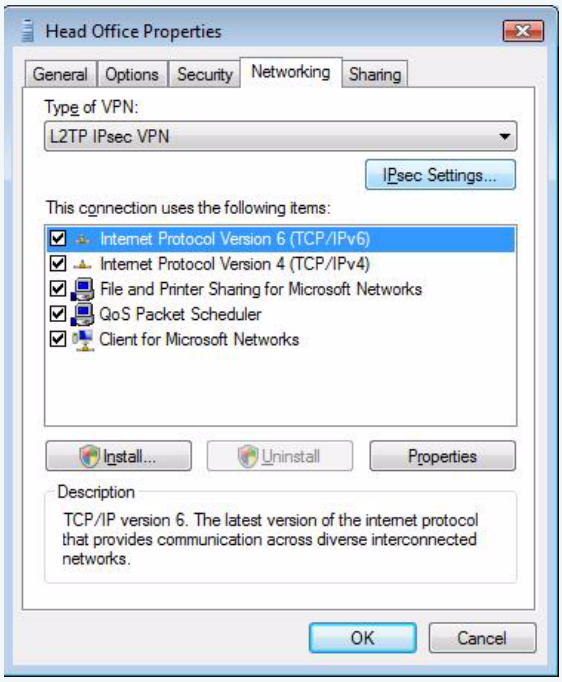
This opens the Advanced Settings window, as shown in the following figure. In "Data encryption", select "Maximum strength encryption". In "Allow these protocols", deselect the "Automatically use my Windows logon name and password (and domain, if any)" checkbox, because this example does not use this option. CHAP v2 is also unnecessary so you can optionally deselect it.

Click on the OK button to return to the Head Office properties.

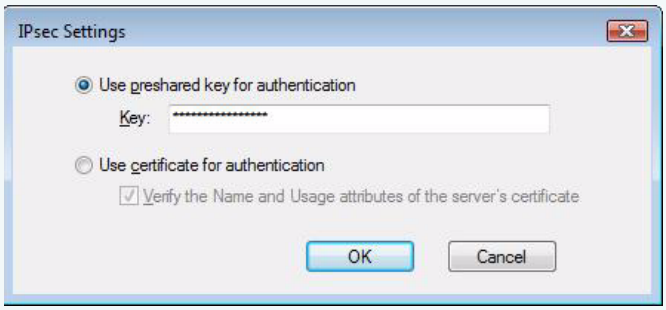
5. Configure the networking settings

On the Networking tab, set the "Type of VPN" to "L2TP IPsec VPN".

You may also deselect any of the protocols and networks in the box below except for "Internet Protocol Version 4 (TCP/IPv4)". The IPSec tunnel will complete faster if you turn off unnecessary protocols and networks.



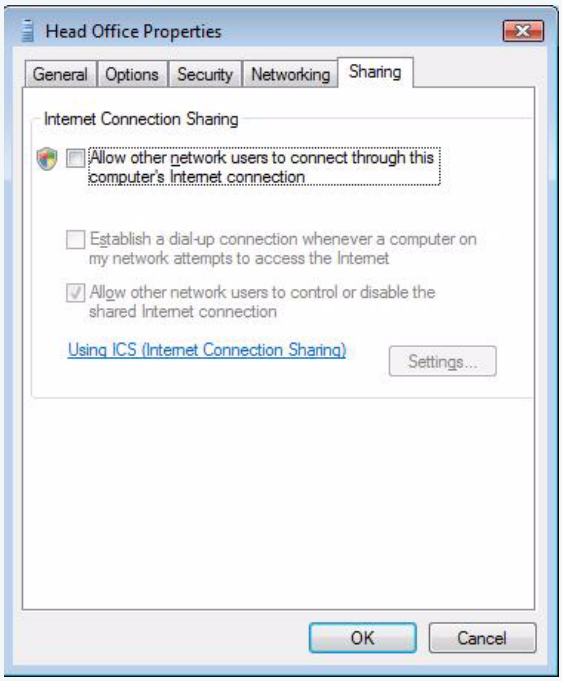
Then click on the "IPSec Settings …" button. This opens the IPsec Settings window, as shown in the following figure. Enter the preshared key. On the Head Office router this is encryption key number 3 (see step 2 on page 5) and has a value of "secret".



Click on the OK button to return to the Head Office properties.

6. Check the sharing settings

No changes need to be made on the Sharing tab. Click OK to close the connection properties.



Connect

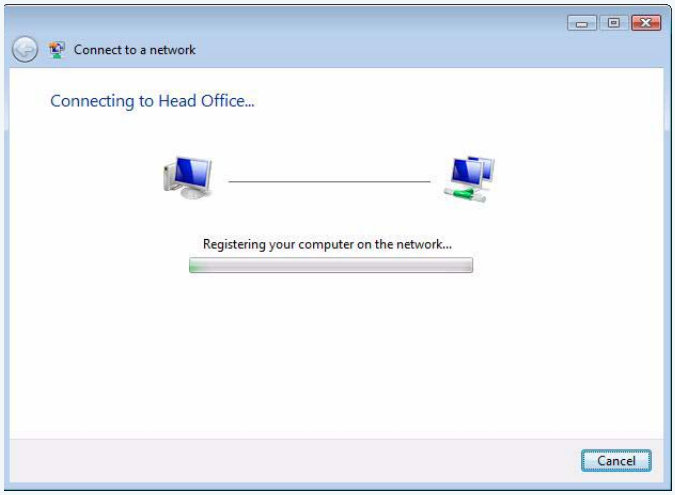
1. If necessary, start the connection that the VPN will initiate over

If you are not connected to a LAN, start the connection that the VPN will initiate over (such as dialup).

2. Start the VPN

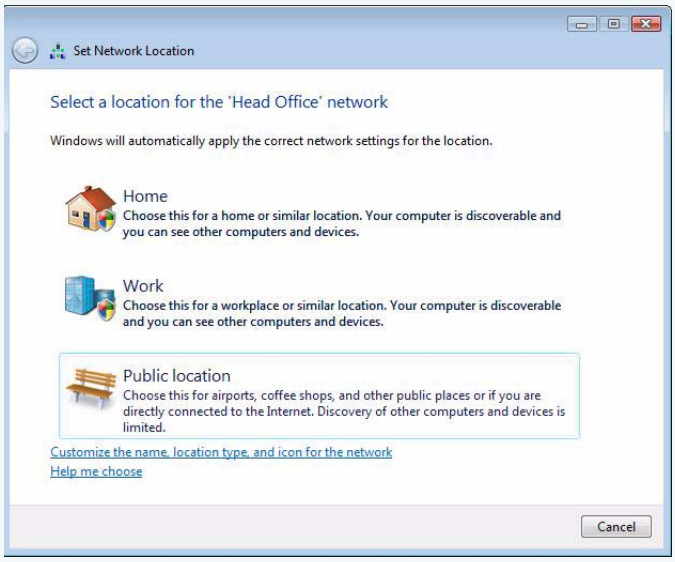
Open the "Connect Head Office" window and enter the username and password. Click on the Connect button.

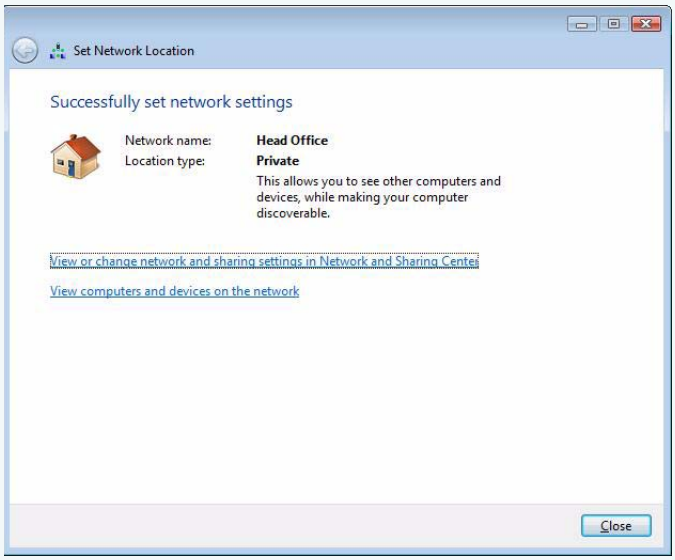
The IPSec tunnel should come up and the following window should display. This indicates that the tunnel is up. Windows may spend some time "registering" if you did not deselect the networks mentioned in step 5 on page 21.



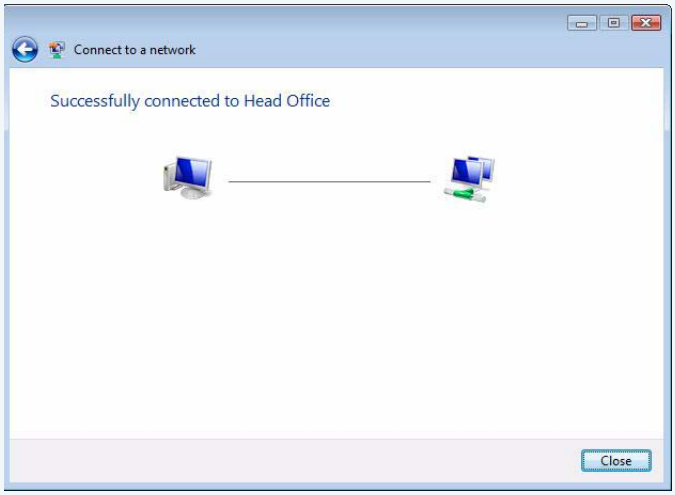
3. Answer Vista's questions

Because this is the first time that the connection has been started, Vista will ask you some security and location-related details about it. Answer appropriately for your situation.





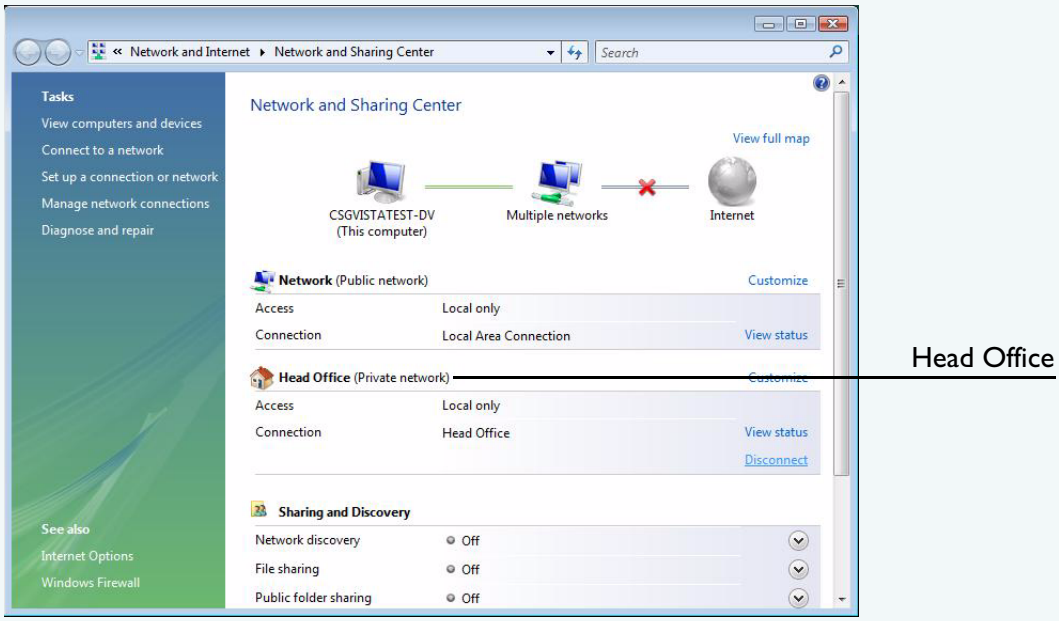
Once the connection is successful, you will see the following window.



Click Close to close the window.

4. Check the Network and Sharing Center

The Head Office network now appears in the Network and Sharing Center, as shown in the following figure. You can disconnect the VPN here when required.



Example debugging output

This section provides a snapshot of the debugging output when tunnels are working properly, in the following situations:

If you encounter problems initiating tunnels, this section may be a useful reference. It also illustrates the following three useful debug tools:

- **enable isakmp debug=all**

  This command provides real time debugging of ISAKMP and IPSec packets. It shows every step that the router follows when setting up and maintaining the ISAKMP and IPSec Security Associations (SAs).

- **show isakmp sa**

  This command's output shows the status and characteristics of ISAKMP Security Associations.

- **show ipsec sa**

  This command's output shows the status and characteristics of IPsec Security Associations.

A remote office initiates a tunnel

This section contains the following:

ISAKMP debug output on the head office router

The following debug is the output from the command **enable isakmp debug=all** on the Head Office router.

```
SecOff Head Office> ena isakmp debug=all

Info (1082057): ISAKMP Debugging has been enabled.
```

raw ISAKMP payload

```
SecOff Head Office> ISAKMP Network Rx:
     remotePort=9882 localPort=500
     af 98 24 b4 96 c1 59 52 00 00 00 00 00 00 00 00 01 10 02 00
     00 00 00 00 00 00 00 7c 0d 00 00 38 00 00 00 01 00 00 00 01
     00 00 00 2c 01 01 00 01 00 00 00 24 01 01 00 00 80 01 00 01
     80 02 00 02 80 03 00 01 80 04 00 01 80 0b 00 01 00 0c 00 04
     00 01 51 80 0d 00 00 14 90 cb 80 91 3e bb 69 6e 08 63 81 b5
     ec 42 7b 1f 00 00 00 14 8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4
     28 c1 1d e8
ISAKMP MAIN exchange 19: New State: IDLE

ISAKMP MAIN: RESP: xchg 19: Started with peer 172.28.40.80
```

decoded ISAKMP payload

```
ISAKMP Rx Message
     Cookies:   af9824b496c15952:0000000000000000
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 124
     Payload #:  0  Length: 56  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 1  SPI:
           Transform#: 1
             Transform Id ................... IKE(1)
             Encryption Algorithm........... DES(1)
             Authentication Algorithm....... SHA(2)
             Authentication Method.......... PRESHARED(1)
             Group Description.............. 768(1)
             Group Type..................... MODP
             Expiry Seconds................. 86400
     Payload #:  1  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-02\n
       90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     Payload #:  2  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-08
       8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4 28 c1 1d e8
ISAKMP MAIN: RESP: xchg 19: Rx NAT-T version 2 vendor ID
ISAKMP MAIN: RESP: xchg 19: Rx NAT-T version 8 vendor ID
ISAKMP MAIN exchange 19: New State: SARECV

ISAKMP MAIN: RESP: xchg 19: Found matching policy = office
```

```
ISAKMP Tx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 184
     Payload #:  0  Length: 56  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 1  SPI:
           Transform#: 1
             Transform Id ................. IKE(1)
             Encryption Algorithm........... DES(1)
             Authentication Algorithm....... SHA(2)
             Authentication Method.......... PRESHARED(1)
             Group Description.............. 768(1)
             Group Type..................... MODP
             Expiry Seconds................. 86400
     Payload #:  1  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-02\n
       90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     Payload #:  2  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-02 (no \n)
       cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
     Payload #:  3  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-03
       7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
     Payload #:  4  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-08
       8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4 28 c1 1d e8
     Payload #:  5  Length: 20  Type: Vendor ID (VID)
       string=NAT-T RFC3947
       4a 13 1c 81 07 03 58 45 5c 57 28 f2 0e 95 45 2f
ISAKMP Tx Unencrypted
ISAKMP Network Tx:
     localPort=500 remotePort=9882
     af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 01 10 02 00
     00 00 00 00 00 00 00 b8 0d 00 00 38 00 00 00 01 00 00 00 01
     00 00 00 2c 01 01 00 01 00 00 00 24 01 01 00 00 80 01 00 01
     80 02 00 02 80 03 00 01 80 04 00 01 80 0b 00 01 00 0c 00 04
     00 01 51 80 0d 00 00 14 90 cb 80 91 3e bb 69 6e 08 63 81 b5
     ec 42 7b 1f 0d 00 00 14 cd 60 46 43 35 df 21 f8 7c fd b2 fc
     68 b6 a4 48 0d 00 00 14 7d 94 19 a6 53 10 ca 6f 2c 17 9d 92
     15 52 9d 56 0d 00 00 14 8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4
     28 c1 1d e8 00 00 00 14 4a 13 1c 81 07 03 58 45 5c 57 28 f2
     0e 95 45 2f
ISAKMP MAIN exchange 19: New State: SASENT

ISAKMP Network Rx:
     remotePort=9882 localPort=500
     af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 04 10 02 00
     00 00 00 00 00 00 00 c8 0a 00 00 64 8e 35 b7 16 0c 64 93 4d
     56 fb b3 e8 7f 94 84 b6 b2 cc 30 fd 9c 77 e7 0b 80 05 e8 a3
     32 b7 97 4e 3b 15 13 05 64 58 43 c7 c0 cd f0 15 bb 8e e5 f5
     0a 87 3d 0f b1 33 dc a9 57 f8 f4 c9 47 cf b6 d2 6b ef 4a 1a
     25 4d 91 28 e2 eb a6 bb 1f 02 12 c2 d0 b7 e6 63 8e 89 b2 53
     f7 3a 16 b2 74 0a d5 3c 0f 00 00 18 2b 88 9c b8 e9 d4 37 f1
     c6 75 9c 10 a6 7b 0d 7b cf f1 cf 6a 0f 00 00 18 bd 35 90 fe
     6a 8c d9 62 7f 76 d3 8d 4a 68 29 d4 e2 45 97 d0 00 00 00 18
     e5 88 fc 6e 06 1d a0 e4 b5 23 0f 6e c6 d3 23 92 8c 24 cd 97
```

```
ISAKMP Rx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 200
     Payload #:  0  Length: 100  Type: Key Exchange (KE)
       8e 35 b7 16 0c 64 93 4d 56 fb b3 e8 7f 94 84 b6 b2 cc 30 fd
       9c 77 e7 0b 80 05 e8 a3 32 b7 97 4e 3b 15 13 05 64 58 43 c7
       c0 cd f0 15 bb 8e e5 f5 0a 87 3d 0f b1 33 dc a9 57 f8 f4 c9
       47 cf b6 d2 6b ef 4a 1a 25 4d 91 28 e2 eb a6 bb 1f 02 12 c2
       d0 b7 e6 63 8e 89 b2 53 f7 3a 16 b2 74 0a d5 3c
     Payload #:  1  Length: 24  Type: Nonce (NONCE)
       2b 88 9c b8 e9 d4 37 f1 c6 75 9c 10 a6 7b 0d 7b cf f1 cf 6a
     Payload #:  2  Length: 24  Type: NAT-T Discovery (NAT-D)
       bd 35 90 fe 6a 8c d9 62 7f 76 d3 8d 4a 68 29 d4 e2 45 97 d0
     Payload #:  3  Length: 24  Type: NAT-T Discovery (NAT-D)
       e5 88 fc 6e 06 1d a0 e4 b5 23 0f 6e c6 d3 23 92 8c 24 cd 97
ISAKMP MAIN: RESP: xchg 19: NAT-D detected a remote NAT
ISAKMP MAIN exchange 19: New State: KERECV

ISAKMP MAIN: RESP: xchg 19: x l=20 v=df5bfb9cb0d928a56fc47a1b5af215c5c025c06d
ISAKMP MAIN: RESP: xchg 19: g^x l=96
   v=8e35b7160c64934d56fbb3e87f9484b6b2cc30fdc
ISAKMP MAIN: RESP: xchg 19: g^y l=96
   v=af898c37776e55d97ac0728b83126cd3ea0805107
ISAKMP MAIN: RESP: xchg 19: g^xy l=96
   v=a02ce1469a10aec0bf50aa75b3c1c13c4b937d51
ISAKMP MAIN: RESP: xchg 19: Ni l=20
   v=2b889cb8e9d437f1c6759c10a67b0d7bcff1cf6a
ISAKMP MAIN: RESP: xchg 19: Nr l=20
   v=9a0a0b8faac22cc1d66bc569aee1f71c5d4e9581
ISAKMP MAIN: RESP: xchg 19: COOKIE_I l=8 v=af9824b496c15952
ISAKMP MAIN: RESP: xchg 19: COOKIE_R l=8 v=5328549750db971e
ISAKMP MAIN: RESP: xchg 19: Key l=6 v=667269656e64
ISAKMP MAIN: RESP: xchg 19: SKEYID l=20
   v=03fe34c0cebe46f4b36f1e1a119da71e8d7f84
ISAKMP MAIN: RESP: xchg 19: SKEYID_d l=20
   v=0740c8f80b1d43c99e30ac7ed8c896925e50
ISAKMP MAIN: RESP: xchg 19: SKEYID_a l=20
   v=83c7f8305a07f531e32a4a64981727ad0c04
ISAKMP MAIN: RESP: xchg 19: SKEYID_e l=20
   v=27722ea1825f68d248b0507a594a3af57344
ISAKMP MAIN: RESP: xchg 19: EncKey l=8 v=27722ea1825f68d2
ISAKMP MAIN: RESP: xchg 19: IV l=8 v=15d302f818b44c04
ISAKMP Tx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 200
     Payload #:  0  Length: 100  Type: Key Exchange (KE)
       af 89 8c 37 77 6e 55 d9 7a c0 72 8b 83 12 6c d3 ea 08 05 10
       88 9d 64 86 18 36 06 9d 3c cc 5a 18 df 73 2b d9 5d f4 0c 69
       be e5 01 91 50 04 30 49 ac 7b 79 d9 6a 2e 6c 2f 00 17 6f 34
       61 2b 51 fa b3 24 ca d5 e4 fd 7c e1 ab b6 96 3e bb 79 8a 49
       67 88 5c 26 2d 48 d7 e8 1f 83 33 0e 65 fd e4 97
     Payload #:  1  Length: 24  Type: Nonce (NONCE)
       9a 0a 0b 8f aa c2 2c c1 d6 6b c5 69 ae e1 f7 1c 5d 4e 95 81
     Payload #:  2  Length: 24  Type: NAT-T Discovery (NAT-D)
       79 03 40 7e 9c dc fc e4 f4 e5 5f c3 8f c6 d8 e1 f6 45 af d1
     Payload #:  3  Length: 24  Type: NAT-T Discovery (NAT-D)
       bd 35 90 fe 6a 8c d9 62 7f 76 d3 8d 4a 68 29 d4 e2 45 97 d0
```

```
ISAKMP Tx Unencrypted
ISAKMP Network Tx:
     localPort=500 remotePort=9882
     af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 04 10 02 00
     00 00 00 00 00 00 00 c8 0a 00 00 64 af 89 8c 37 77 6e 55 d9
     7a c0 72 8b 83 12 6c d3 ea 08 05 10 88 9d 64 86 18 36 06 9d
     3c cc 5a 18 df 73 2b d9 5d f4 0c 69 be e5 01 91 50 04 30 49
     ac 7b 79 d9 6a 2e 6c 2f 00 17 6f 34 61 2b 51 fa b3 24 ca d5
     e4 fd 7c e1 ab b6 96 3e bb 79 8a 49 67 88 5c 26 2d 48 d7 e8
     1f 83 33 0e 65 fd e4 97 0f 00 00 18 9a 0a 0b 8f aa c2 2c c1
     d6 6b c5 69 ae e1 f7 1c 5d 4e 95 81 0f 00 00 18 79 03 40 7e
     9c dc fc e4 f4 e5 5f c3 8f c6 d8 e1 f6 45 af d1 00 00 00 18
     bd 35 90 fe 6a 8c d9 62 7f 76 d3 8d 4a 68 29 d4 e2 45 97 d0
```

encrypted raw ISAKMP payload

```
ISAKMP MAIN exchange 19: New State: KESENT
ISAKMP Network Rx:
     remotePort=20438 localPort=4500
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     05 10 02 01 00 00 00 00 00 00 00 44 93 76 4d 16 c4 44 67 dc
     be 9e 57 77 09 09 0d 33 39 b7 72 78 e2 55 15 7e f8 44 8f a6
     1f ed 64 e6 31 6c 12 96 e1 dd eb a7
ISAKMP Network Rx: Removed Non-ESP Marker.
```

decrypted raw ISAKMP payload

```
ISAKMP Rx (decrypted)<---
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 05 10 02 01
00 00 00 00 00 00 00 44 08 00 00 0c 01 00 00 00 ac 10 02 44
00 00 00 18 07 9e 0b 5b 0a 0d d8 18 81 83 26 a3 04 f4 c6 cc
17 88 0d 51 00 00 00 03
```

decrypted decoded ISAKMP payload

```
ISAKMP Rx Message (decrypted)
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 01
     MessageID:  00000000   Total Length: 64
     Payload #:  0  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 0  Port: 0
       Value: 172.16.2.68
     Payload #:  1  Length: 24  Type: Hash (HASH)
       07 9e 0b 5b 0a 0d d8 18 81 83 26 a3 04 f4 c6 cc 17 88 0d 51
ISAKMP CORE: Info: exchange 19 local port changed from 500 to 4500

ISAKMP CORE: Info: exchange 19 remote port changed from 9882 to 20438

ISAKMP MAIN exchange 19: New State: AUTHRECV

ISAKMP MAIN: RESP: xchg 19: RemoteID=172.16.2.68 OR 172.28.40.80 for NAT-T
ISAKMP MAIN: RESP: xchg 19: Hi l=20
   v=079e0b5b0a0dd818818326a304f4c6cc17880d51
ISAKMP MAIN: RESP: xchg 19: Hr l=20
   v=0532e1272f4474db54947a680eb54529af6947fe
ISAKMP Encrypt:
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 05 10 02 00
00 00 00 00 00 00 00 40 08 00 00 0c 01 00 00 00 ac 1c 28 29
00 00 00 18 05 32 e1 27 2f 44 74 db 54 94 7a 68 0e b5 45 29
af 69 47 fe
```

```
ISAKMP Tx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 64
     Payload #:  0  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 0  Port: 0
       Value: 172.28.40.41
     Payload #:  1  Length: 24  Type: Hash (HASH)
       05 32 e1 27 2f 44 74 db 54 94 7a 68 0e b5 45 29 af 69 47 fe
ISAKMP Tx Encrypted
ISAKMP Network Tx:
     localPort=4500 remotePort=20438
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     05 10 02 01 00 00 00 00 00 00 00 44 8e 60 41 35 ff 2d fe 8a
     85 11 68 ef 22 79 2a fd b1 12 9f 42 7e 97 ac 93 f6 54 52 ae
     14 e9 23 73 85 61 db ae 72 e5 70 88
ISAKMP MAIN exchange 19: New State: AUTHSENT

ISAKMP MAIN exchange 19: New State: UP

ISAKMP CORE: Exchange 19 done

ISAKMP Network Rx:
     remotePort=20438 localPort=4500
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     08 10 20 01 29 4b f4 82 00 00 00 9c eb c0 ff 5f 16 de 10 53
     af c6 56 3d 2d 83 0f 97 6c 54 66 6c 8d 0b 80 34 c5 07 55 30
     2f 6e 5f 06 6b 16 7d 93 e2 dc 8a 57 08 dd c4 28 d8 54 89 04
     b8 ee 38 5e e5 df f8 96 20 be b0 3d 6a b0 bb 85 43 49 57 d3
     ca 65 1b 79 bc 80 43 29 cd 43 98 a0 af ef 9f 7f 6a 0e e5 14
     f7 9b 25 ee af 47 ee a2 39 c9 1d d0 82 14 21 99 c7 78 28 a5
     0c db 04 1c b6 27 5a b1 d9 29 c3 8c 00 91 e8 af 42 05 a7 37

ISAKMP Network Rx: Removed Non-ESP Marker.

ISAKMP QUICK: RESP: xchg 20: Started with peer 172.28.40.80
ISAKMP QUICK exchange 20: New State: WAIT_HASH_SA_NONCE
ISAKMP QUICK: RESP: xchg 20: COOKIE_I l=8 v=af9824b496c15952
ISAKMP QUICK: RESP: xchg 20: COOKIE_R l=8 v=5328549750db971e
ISAKMP QUICK: RESP: xchg 20: MessageID=294bf482
ISAKMP QUICK: RESP: xchg 20: IV l=8 v=b3ae9834d91f35f9
ISAKMP Rx (decrypted)<---
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 08 10 20 01
29 4b f4 82 00 00 00 9c 01 00 00 18 86 79 19 ff 7a a4 e0 81
10 37 48 c3 3a 05 07 73 ee 3a eb 73 0a 00 00 28 00 00 00 01
00 00 00 01 00 00 00 1c 01 03 04 01 e2 1b ae 85 00 00 00 10
01 03 00 00 80 04 00 03 80 05 00 02 05 00 00 18 ea ca e0 85
0a 8f 8c 93 53 a6 f9 1d 6b 06 46 c5 2b 99 fe 71 05 00 00 10
04 00 00 00 c0 a8 00 00 ff ff ff 00 00 00 00 10 04 00 00 00
ac ae 01 00 ff ff ff 00 00 00 00 00 00 00 00 07
```

```
ISAKMP Rx Message (decrypted)
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 01
     MessageID:  294bf482   Total Length: 148
     Payload #:  0  Length: 24  Type: Hash (HASH)
       86 79 19 ff 7a a4 e0 81 10 37 48 c3 3a 05 07 73 ee 3a eb 73
     Payload #:  1  Length: 40  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ESP(3)  #Trans: 1  SPI: e21bae85
           Transform#: 1
             Transform Id .................. 3DESOUTER(3)
             Group Description ............. MODP768(1)
             Encapsulation Mode ............ UDP_ENCAP_TUNNEL(3)
             Authentication Algorithm ...... SHA(2)
     Payload #:  2  Length: 24  Type: Nonce (NONCE)
       ea ca e0 85 0a 8f 8c 93 53 a6 f9 1d 6b 06 46 c5 2b 99 fe 71
     Payload #:  3  Length: 16  Type: Identification (ID)
       Type: IPV4_ADDR_SUBNET  ProtocolId: 0  Port: 0
       Value: 192.168.0.0:255.255.255.0
     Payload #:  4  Length: 16  Type: Identification (ID)
       Type: IPV4_ADDR_SUBNET  ProtocolId: 0  Port: 0
       Value: 172.174.1.0:255.255.255.0

ISAKMP QUICK: RESP: xchg 20: rx msg 1: start
ISAKMP QUICK exchange 20: New State: RECEIVING_MESSAGE
ISAKMP QUICK: RESP: xchg 20: rx msg 1: rec PROP 0: # 1, protid 3, outspi
   e21bae
ISAKMP QUICK: RESP: xchg 20: rx msg 1: PROP 0 transforms good
ISAKMP QUICK: RESP: xchg 20: rx msg 1: SA proposals good
ISAKMP QUICK: RESP: xchg 20: rx msg 1: payloads good:
ISAKMP QUICK: RESP: xchg 20: rx msg 1: good

ISAKMP QR 20: HASH1: 01d5c114 100
294bf4820a000028000000010000000010000001c01030401e21bae8500000010
0103000080040003800500020500001 8eacae0850a8f8c9353a6f91d6b0646c5
2b99fe71050000100400000c0a80000ffffff000000001004000000acae0100
ffffff00

ISAKMP QR 20: HASH1: result 867919ff7aa4e081103748c33a050773ee3aeb73

ISAKMP DOI: IPSEC: resp match pol:
   peerIP=172.28.40.80
   filtEnableFlag=00000005
   filtOpaqueFlag=00000000
   selectorsFromPktFlag=00000000
   lAddr=172.174.1.0
   lMask=255.255.255.0
   lAddrLow=0.0.0.0
   lAddrHigh=0.0.0.0
   rAddr=192.168.0.0
   rMask=255.255.255.0
   rAddrLow=0.0.0.0
   rAddrHigh=0.0.0.0
   lPort=0
   rPort=0
   lName=
   rName=
   lAddrVer=4
   rAddrVer=4
```

```
ISAKMP DOI: IPSEC: Aquire Info -> Local Policy
  number of proposals 1
  proposal 0: # 1, protId 3, #transforms 1
    transform 0: # 1, id 3, sas 10
                 expiry: b 0-4294967295, s 0-28800
                 gr 1, mode 1, auth 2, keylen 0
ISAKMP QUICK: RESP: xchg 20: Match Pol: 2 Local (prot 1) found - 0
ISAKMP QUICK: RESP: xchg 20: Match Pol: 2 Remote (prot 1) found - 0
ISAKMP QUICK: RESP: xchg 20: Match Pol: prop match try: l
   00000000000000001d5bc
ISAKMP QUICK: RESP: xchg 20: Match Pol: matching (prot 2) props 1
ISAKMP QUICK: RESP: xchg 20: Match Pol: (prot 2) tran match try: loc 0 - rem 0
ISAKMP QUICK: RESP: xchg 20: Match Tran: match good
ISAKMP QUICK: RESP: xchg 20: Match Pol: matched
ISAKMP QUICK: RESP: xchg 20: proc 1: done good

ISAKMP QI 20: HASH INK1: 01d60214 45
03b0f1c51feacae0850a8f8c9353a6f91d6b0646c52b99fe71ff4676ba2172ba
52ce6e602c53f9cb82e4a4a467

ISAKMP QI 20: HASH INK1: result dde98e71ff3b3bad106ddf6c78f7555b3976cb2e

ISAKMP QI 20: HASH OUTK1: 01d60214 45
03e21bae85eacae0850a8f8c9353a6f91d6b0646c52b99fe71ff4676ba2172ba
52ce6e602c53f9cb82e4a4a467

ISAKMP QI 20: HASH OUTK1: result 86581c245ae656a295b0f470bc01065c3357bf1a

ISAKMP QI 20: HASH INK2: 01d60200 65
dde98e71ff3b3bad106ddf6c78f7555b3976cb2e03b0f1c51feacae0850a8f8c
9353a6f91d6b0646c52b99fe71ff4676ba2172ba52ce6e602c53f9cb82e4a4a4
67

ISAKMP QI 20: HASH INK2: result 46e6dbab8f6c681fde7107e07b1534c685d5337a

ISAKMP QI 20: HASH OUTK2: 01d60200 65
86581c245ae656a295b0f470bc01065c3357bf1a03e21bae85eacae0850a8f8c
9353a6f91d6b0646c52b99fe71ff4676ba2172ba52ce6e602c53f9cb82e4a4a4
67

ISAKMP QI 20: HASH INK3: 01d60200 65
46e6dbab8f6c681fde7107e07b1534c685d5337a03b0f1c51feacae0850a8f8c
9353a6f91d6b0646c52b99fe71ff4676ba2172ba52ce6e602c53f9cb82e4a4a4
67

ISAKMP QI 20: HASH INK3: result 9a2379eb25ccb2c0cd32f3fb0b4abf3e6da7aad9

ISAKMP QI 20: HASH OUTK3: 01d60200 65
3e02b94fb270da5c0fde4fce4d829ece7f3b450803e21bae85eacae0850a8f8c
9353a6f91d6b0646c52b99fe71ff4676ba2172ba52ce6e602c53f9cb82e4a4a4
67

ISAKMP QI 20: HASH OUTK3: result 425ee9c2644877e1ce34329092dfa8af13dd6076
```

```
ISAKMP QUICK exchange 20: New State: SENDING_HASH_SA_NONCE
ISAKMP DOI: IPSEC: Exchange IDs not default:
  initiatorAddress      172.28.40.80
  IDi: type             IPV4_ADDR_SUBNET
       protocol Id      0
       port             0
       data             c0a80000ffffff00
  responderAddress      172.28.40.41
  IDr: type             IPV4_ADDR_SUBNET
       protocol Id      0
       port             0
       data             acae0100ffffff00

ISAKMP QR 20: HASH1: ID Payload Created

ISAKMP QR 20: HASH2: 01d61254 120
294bf482eacae0850a8f8c9353a6f91d6b0646c52b99fe710a00002800000001
000000010000001c01030401b0f1c51f000000100103000080040003800500 02
05000018ff4676ba2172ba52ce6e602c53f9cb82e4a4a4670500001004000000
c0a80000ffffff00000000001004000000acae0100ffffff00

ISAKMP QR 20: HASH2: result 6356ea28e5179dc271c29c6a87a7d4fd4dbb3f30
ISAKMP Encrypt:
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 08 10 20 00
29 4b f4 82 00 00 00 94 01 00 00 18 63 56 ea 28 e5 17 9d c2
71 c2 9c 6a 87 a7 d4 fd 4d bb 3f 30 0a 00 00 28 00 00 00 01
00 00 00 01 00 00 00 1c 01 03 04 01 b0 f1 c5 1f 00 00 00 10
01 03 00 00 80 04 00 03 80 05 00 02 05 00 00 18 ff 46 76 ba
21 72 ba 52 ce 6e 60 2c 53 f9 cb 82 e4 a4 a4 67 05 00 00 10
04 00 00 00 c0 a8 00 00 ff ff ff 00 00 00 00 10 04 00 00 00
ac ae 01 00 ff ff ff 00
ISAKMP Tx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 00
     MessageID:  294bf482   Total Length: 148
     Payload #:  0  Length: 24  Type: Hash (HASH)
       63 56 ea 28 e5 17 9d c2 71 c2 9c 6a 87 a7 d4 fd 4d bb 3f 30
     Payload #:  1  Length: 40  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ESP(3)  #Trans: 1  SPI: b0f1c51f
           Transform#: 1
             Transform Id ................... 3DESOUTER(3)
             Group Description .............. MODP768(1)
             Encapsulation Mode ............. UDP_ENCAP_TUNNEL(3)
             Authentication Algorithm ...... SHA(2)
     Payload #:  2  Length: 24  Type: Nonce (NONCE)
       ff 46 76 ba 21 72 ba 52 ce 6e 60 2c 53 f9 cb 82 e4 a4 a4 67
     Payload #:  3  Length: 16  Type: Identification (ID)
       Type: IPV4_ADDR_SUBNET  ProtocolId: 0  Port: 0
       Value: 192.168.0.0:255.255.255.0
     Payload #:  4  Length: 16  Type: Identification (ID)
       Type: IPV4_ADDR_SUBNET  ProtocolId: 0  Port: 0
       Value: 172.174.1.0:255.255.255.0
ISAKMP Tx Encrypted
```

```
ISAKMP Network Tx:
     localPort=4500 remotePort=20438
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     08 10 20 01 29 4b f4 82 00 00 00 9c 81 b1 63 1a d9 67 15 b6
     95 14 e0 66 d9 3b ef 41 3c 83 43 e8 8b 59 4b 23 cd 12 89 bc
     0d 05 d0 da b0 82 9c 2c ef e0 4f 48 a7 9f d4 d7 c4 62 58 d9
     82 0b 12 99 82 87 cf 12 93 3c 1f 4d 47 6c 20 58 fd 31 12 ab
     7e 5a b0 ec 22 b0 4e c5 00 d4 b7 af fe f8 7f ac a5 db dd 37
     14 20 80 90 8d ae 63 1a 37 31 7a 76 72 d0 31 65 e2 9d da 2d
     f2 ce 62 d1 c3 cb a2 c3 99 fc 3e 46 98 2f c6 d4 77 a3 0c d7

ISAKMP Network Rx:
     remotePort=20438 localPort=4500
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     08 10 20 01 29 4b f4 82 00 00 00 3c f8 83 c6 7b 36 f8 27 89
     f3 5d a0 57 89 88 b7 87 4f 5a 1d 51 0f ef 42 e1 96 8f 37 3c
     dc 1c 9f c2
ISAKMP Network Rx: Removed Non-ESP Marker.
ISAKMP Rx (decrypted)<---
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 08 10 20 01
29 4b f4 82 00 00 00 3c 00 00 00 18 57 8e f2 bc 80 aa 26 88
cb b5 55 f1 4e 31 14 df 92 e2 26 d0 00 00 00 00 00 00 00 07

ISAKMP Rx Message (decrypted)
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 01
     MessageID:  294bf482   Total Length: 52
     Payload #:  0  Length: 24  Type: Hash (HASH)
       57 8e f2 bc 80 aa 26 88 cb b5 55 f1 4e 31 14 df 92 e2 26 d0

ISAKMP QUICK: RESP: xchg 20: rx msg 1: start
ISAKMP QUICK exchange 20: New State: RECEIVING_MESSAGE
ISAKMP QUICK: RESP: xchg 20: rx msg 2: payloads good:
ISAKMP QUICK: RESP: xchg 20: rx msg 2: good

ISAKMP QR 20: HASH3: 01d6b4d4 45
00294bf482eacae0850a8f8c9353a6f91d6b0646c52b99fe71ff4676ba2172ba
52ce6e602c53f9cb82e4a4a467

ISAKMP QR 20: HASH3: result 578ef2bc80aa2688cbb555f14e3114df92e226d0
ISAKMP CORE: Exchange 20 done

ISAKMP QUICK exchange 20: New State: DONE

SecOff AR450S> dis isakmp debug=all

Info (1082056): ISAKMP Debugging has been disabled.
```

IPSec and ISAKMP SAs on the head office router

This section shows the output of the commands **show ipsec sa** and **show isakmp sa** on the head office router. For each command, specifying the SA number gives much more detail.

show ipsec sa

```
SA Id  Policy                Bundle  State     Protocol    OutSPI       InSPI
-------------------------------------------------------------------------------
    5  office                    10  Valid     ESP     3793464965  2968634655
```

show ipsec sa=5

```
SA Id ................................ 5
  Policy ............................. office
  Bundle ............................. 1
  SA Specification Used ............... 10
  State .............................. Valid
  Protocol ........................... ESP
  Role ............................... RESPONDER
  Mode ............................... UDP_ENCAP_TUNNEL
  Outbound SPI ....................... 3793464965
  Inbound SPI ........................ 2968634655
  Local tunnel IP address ............ 172.28.40.41
  Remote tunnel IP address ........... 172.28.40.80
  Encryption algorithm ............... 3DESOUTER
  Encryption ENCO channel............. 1
  Hash algorithm ..................... SHA
  Hash ENCO channel................... 2
  NAT-Traversal NAT-OA
    Peer original source IP address ..... n/a in tunnel mode
    Peer original destination IP address  n/a in tunnel mode
  Filters
    Local IP address ................... 172.174.1.0
    Local IP address mask .............. 255.255.255.0
    Remote IP address .................. 192.168.0.0
    Remote IP address mask ............. 255.255.255.0
    NAPT remote port number ............ n/a in tunnel mode
    Local Name ......................... ANY
    Remote Name ........................ ANY
  DF Bit ............................. CLEAR
  Last sent sequence number .......... 1
  Anti-replay checking enabled ....... FALSE
  Debug device ....................... 16
  Filter debug flags ................. 00000000
  Packet debug flags ................. 00000000
  Trace debug flags .................. 00000000
  Packet debug length ................ 72
```

show isakmp sa

```
                                    Expiry Limits - hard/soft/used
SA Id PeerAddress     EncA.  HashA. Bytes                Seconds
-----------------------------------------------------------------------------
1     172.28.40.80    DES    SHA    -/-/-               86400/75593/19521
```

show isakmp sa=1

```
SA Id ................................ 1
  Initiator Cookie ..................... af9824b496c15952
  Responder Cookie ..................... 5328549750db971e
  DOI .................................. IPSEC
  Policy name .......................... office
  State ................................ ACTIVE
  Local address ........................ 172.28.40.41
  Remote Address ....................... 172.28.40.80
  Remote Port .......................... 20438
  Time of establishment ................ 18-May-2007:08:15:35
  Commit bit set ....................... FALSE
  Send notifies ........................ FALSE
  Send deletes ......................... FALSE
  Always send ID ....................... FALSE
  Message Retry Limit .................. 8
  Initial Message Retry Timeout (s) ... 4
  Message Back-off ..................... Incremental
  Exchange Delete Delay (s) ........... 30
  Do Xauth ............................ FALSE
    Xauth Finished ..................... TRUE
  Expiry Limit (bytes) ................ -
  Soft Expiry Limit (bytes) ........... -
  Bytes seen ........................... -
  Expiry Limit (seconds) .............. 86400
  Soft Expiry Limit (seconds) ......... 75593
  Seconds since creation .............. 19523
  Number of Phase 2 exchanges allowed . 4294967294
  Number of acquires queued ........... 0

Sa Definition Information:
  Authentication Type .................. PRESHARED
  Encryption Algorithm ................ DES - 56 bit
  Hash Algorithm ....................... SHA
  group Type ........................... MODP
  group Description .................... MODP768
  DH Private Exponent Bits ............ 160
  expiry seconds ....................... 86400
  expiry kilobytes ..................... -
```

continued on next page

continued from previous page

```
Sa Definition Information:
  Authentication Type ................. PRESHARED
  Encryption Algorithm ................ DES - 56 bit
  Hash Algorithm ...................... SHA
  group Type .......................... MODP
  group Description ................... MODP768
  DH Private Exponent Bits ............ 160
  expiry seconds ...................... 86400
  expiry kilobytes .................... -

XAuth Information:
  Id .................................. 0
  Next Message ........................ UNKNOWN
  Status .............................. FAIL
  Type ................................ Generic
  Max Failed Attempts.................. 0
  Failed Attempts...................... 0

NAT-Traversal Information:
  NAT-T enabled ....................... YES
  Peer NAT-T capable .................. YES (v8)
  NAT discovered ...................... REMOTE

Heartbeat Information:
  Send Heartbeats ..................... NO
  Next sequence number tx ............. 1
  Receive Heartbeats .................. NO
  Last sequence number rx ............. 0
```

ISAKMP debug output on the remote office router

The following debug is the output from the command **enable isakmp debug=all** captured on the Remote Office router.

```
SecOff Remote Office> ena isakmp debug=all

Info (1082057): ISAKMP Debugging has been enabled.

SecOff Remote Office> ping 172.174.1.254 sipaddress=192.168.0.1 num=1
ISAKMP: acquire - Create Phase 1 Exchange
ISAKMP MAIN exchange 3: New State: IDLE

ISAKMP MAIN: INIT: xchg 3: Started with peer 172.28.40.41
ISAKMP Tx Message
     Cookies:   af9824b496c15952:0000000000000000
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 124
     Payload #:  0  Length: 56  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 1  SPI:
           Transform#: 1
             Transform Id ................... IKE(1)
             Encryption Algorithm........... DES(1)
             Authentication Algorithm....... SHA(2)
             Authentication Method.......... PRESHARED(1)
             Group Description.............. 768(1)
             Group Type..................... MODP
             Expiry Seconds................. 86400
     Payload #:  1  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-02\n
       90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     Payload #:  2  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-08
       8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4 28 c1 1d e8
ISAKMP Tx Unencrypted
ISAKMP Network Tx:
     localPort=500 remotePort=500
     af 98 24 b4 96 c1 59 52 00 00 00 00 00 00 00 00 01 10 02 00
     00 00 00 00 00 00 00 7c 0d 00 00 38 00 00 00 01 00 00 00 01
     00 00 00 2c 01 01 00 01 00 00 00 24 01 01 00 00 80 01 00 01
     80 02 00 02 80 03 00 01 80 04 00 01 80 0b 00 01 00 0c 00 04
     00 01 51 80 0d 00 00 14 90 cb 80 91 3e bb 69 6e 08 63 81 b5
     ec 42 7b 1f 00 00 00 14 8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4
     28 c1 1d e8
ISAKMP MAIN exchange 3: New State: SASENT


ISAKMP: acquire - Queue the acquire struct
 ISAKMP Network Rx:
     remotePort=500 localPort=500
     af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 01 10 02 00
     00 00 00 00 00 00 00 b8 0d 00 00 38 00 00 00 01 00 00 00 01
     00 00 00 2c 01 01 00 01 00 00 00 24 01 01 00 00 80 01 00 01
     80 02 00 02 80 03 00 01 80 04 00 01 80 0b 00 01 00 0c 00 04
     00 01 51 80 0d 00 00 14 90 cb 80 91 3e bb 69 6e 08 63 81 b5
     ec 42 7b 1f 0d 00 00 14 cd 60 46 43 35 df 21 f8 7c fd b2 fc
     68 b6 a4 48 0d 00 00 14 7d 94 19 a6 53 10 ca 6f 2c 17 9d 92
```

```
     15 52 9d 56 0d 00 00 14 8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4
     28 c1 1d e8 00 00 00 14 4a 13 1c 81 07 03 58 45 5c 57 28 f2
     0e 95 45 2f
ISAKMP Rx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 184
     Payload #:  0  Length: 56  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 1  SPI:
           Transform#: 1
             Transform Id ................... IKE(1)
             Encryption Algorithm........... DES(1)
             Authentication Algorithm....... SHA(2)
             Authentication Method.......... PRESHARED(1)
             Group Description.............. 768(1)
             Group Type..................... MODP
             Expiry Seconds................. 86400
     Payload #:  1  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-02\n
       90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     Payload #:  2  Length: 20  Type: Vendor ID (VID)
       string=UNKNOWN
       cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
     Payload #:  3  Length: 20  Type: Vendor ID (VID)
       string=UNKNOWN
       7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
     Payload #:  4  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-08
       8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4 28 c1 1d e8
     Payload #:  5  Length: 20  Type: Vendor ID (VID)
       string=UNKNOWN
       4a 13 1c 81 07 03 58 45 5c 57 28 f2 0e 95 45 2f
ISAKMP MAIN: INIT: xchg 3: Rx NAT-T version 2 vendor ID
ISAKMP MAIN: INIT: xchg 3: Rx NAT-T version 8 vendor ID
ISAKMP MAIN exchange 3: New State: SARECV

ISAKMP Tx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 200
     Payload #:  0  Length: 100  Type: Key Exchange (KE)
       8e 35 b7 16 0c 64 93 4d 56 fb b3 e8 7f 94 84 b6 b2 cc 30 fd
       9c 77 e7 0b 80 05 e8 a3 32 b7 97 4e 3b 15 13 05 64 58 43 c7
       c0 cd f0 15 bb 8e e5 f5 0a 87 3d 0f b1 33 dc a9 57 f8 f4 c9
       47 cf b6 d2 6b ef 4a 1a 25 4d 91 28 e2 eb a6 bb 1f 02 12 c2
       d0 b7 e6 63 8e 89 b2 53 f7 3a 16 b2 74 0a d5 3c
     Payload #:  1  Length: 24  Type: Nonce (NONCE)
       2b 88 9c b8 e9 d4 37 f1 c6 75 9c 10 a6 7b 0d 7b cf f1 cf 6a
     Payload #:  2  Length: 24  Type: NAT-T Discovery (NAT-D)
       bd 35 90 fe 6a 8c d9 62 7f 76 d3 8d 4a 68 29 d4 e2 45 97 d0
     Payload #:  3  Length: 24  Type: NAT-T Discovery (NAT-D)
       e5 88 fc 6e 06 1d a0 e4 b5 23 0f 6e c6 d3 23 92 8c 24 cd 97
ISAKMP Tx Unencrypted
ISAKMP Network Tx:
     localPort=500 remotePort=500
     af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 04 10 02 00
     00 00 00 00 00 00 00 c8 0a 00 00 64 8e 35 b7 16 0c 64 93 4d
```

```
     56 fb b3 e8 7f 94 84 b6 b2 cc 30 fd 9c 77 e7 0b 80 05 e8 a3
     32 b7 97 4e 3b 15 13 05 64 58 43 c7 c0 cd f0 15 bb 8e e5 f5
     0a 87 3d 0f b1 33 dc a9 57 f8 f4 c9 47 cf b6 d2 6b ef 4a 1a
     25 4d 91 28 e2 eb a6 bb 1f 02 12 c2 d0 b7 e6 63 8e 89 b2 53
     f7 3a 16 b2 74 0a d5 3c 0f 00 00 18 2b 88 9c b8 e9 d4 37 f1
     c6 75 9c 10 a6 7b 0d 7b cf f1 cf 6a 0f 00 00 18 bd 35 90 fe
     6a 8c d9 62 7f 76 d3 8d 4a 68 29 d4 e2 45 97 d0 00 00 00 18
     e5 88 fc 6e 06 1d a0 e4 b5 23 0f 6e c6 d3 23 92 8c 24 cd 97

ISAKMP MAIN exchange 3: New State: KESENT

ISAKMP Network Rx:
     remotePort=500 localPort=500
     af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 04 10 02 00
     00 00 00 00 00 00 00 c8 0a 00 00 64 af 89 8c 37 77 6e 55 d9
     7a c0 72 8b 83 12 6c d3 ea 08 05 10 88 9d 64 86 18 36 06 9d
     3c cc 5a 18 df 73 2b d9 5d f4 0c 69 be e5 01 91 50 04 30 49
     ac 7b 79 d9 6a 2e 6c 2f 00 17 6f 34 61 2b 51 fa b3 24 ca d5
     e4 fd 7c e1 ab b6 96 3e bb 79 8a 49 67 88 5c 26 2d 48 d7 e8
     1f 83 33 0e 65 fd e4 97 0f 00 00 18 9a 0a 0b 8f aa c2 2c c1
     d6 6b c5 69 ae e1 f7 1c 5d 4e 95 81 0f 00 00 18 79 03 40 7e
     9c dc fc e4 f4 e5 5f c3 8f c6 d8 e1 f6 45 af d1 00 00 00 18
     bd 35 90 fe 6a 8c d9 62 7f 76 d3 8d 4a 68 29 d4 e2 45 97 d0

ISAKMP Rx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 200
     Payload #:  0  Length: 100  Type: Key Exchange (KE)
       af 89 8c 37 77 6e 55 d9 7a c0 72 8b 83 12 6c d3 ea 08 05 10
       88 9d 64 86 18 36 06 9d 3c cc 5a 18 df 73 2b d9 5d f4 0c 69
       be e5 01 91 50 04 30 49 ac 7b 79 d9 6a 2e 6c 2f 00 17 6f 34
       61 2b 51 fa b3 24 ca d5 e4 fd 7c e1 ab b6 96 3e bb 79 8a 49
       67 88 5c 26 2d 48 d7 e8 1f 83 33 0e 65 fd e4 97
     Payload #:  1  Length: 24  Type: Nonce (NONCE)
       9a 0a 0b 8f aa c2 2c c1 d6 6b c5 69 ae e1 f7 1c 5d 4e 95 81
     Payload #:  2  Length: 24  Type: NAT-T Discovery (NAT-D)
       79 03 40 7e 9c dc fc e4 f4 e5 5f c3 8f c6 d8 e1 f6 45 af d1
     Payload #:  3  Length: 24  Type: NAT-T Discovery (NAT-D)
       bd 35 90 fe 6a 8c d9 62 7f 76 d3 8d 4a 68 29 d4 e2 45 97 d0
ISAKMP MAIN: INIT: xchg 3: NAT-D detected a local NAT
ISAKMP MAIN: INIT: xchg 3: NAT-T switched to UDP port 4500
ISAKMP MAIN exchange 3: New State: KERECV

ISAKMP MAIN: INIT: xchg 3: x l=20 v=789743986bcbf31c89d05f5f8edcabf4692a7b9e
ISAKMP MAIN: INIT: xchg 3: g^x l=96
   v=8e35b7160c64934d56fbb3e87f9484b6b2cc30fd9c
ISAKMP MAIN: INIT: xchg 3: g^y l=96
   v=af898c37776e55d97ac0728b83126cd3ea08051087
ISAKMP MAIN: INIT: xchg 3: g^xy l=96
   v=a02ce1469a10aec0bf50aa75b3c1c13c4b937d5e1
ISAKMP MAIN: INIT: xchg 3: Ni l=20 v=2b889cb8e9d437f1c6759c10a67b0d7bcff1cf6a
ISAKMP MAIN: INIT: xchg 3: Nr l=20 v=9a0a0b8faac22cc1d66bc569aee1f71c5d4e9581
ISAKMP MAIN: INIT: xchg 3: COOKIE_I l=8 v=af9824b496c15952
ISAKMP MAIN: INIT: xchg 3: COOKIE_R l=8 v=5328549750db971e
ISAKMP MAIN: INIT: xchg 3: Key l=6 v=667269656e64
ISAKMP MAIN: INIT: xchg 3: SKEYID l=20
   v=03fe34c0cebe46f4b36f1e1a119da71e8d7f8e4
```

```
ISAKMP MAIN: INIT: xchg 3: SKEYID_d l=20
   v=0740c8f80b1d43c99e30ac7ed8c896925e5f0
ISAKMP MAIN: INIT: xchg 3: SKEYID_a l=20
   v=83c7f8305a07f531e32a4a64981727ad0c0f4
ISAKMP MAIN: INIT: xchg 3: SKEYID_e l=20
   v=27722ea1825f68d248b0507a594a3af5734a4
ISAKMP MAIN: INIT: xchg 3: EncKey l=8 v=27722ea1825f68d2
ISAKMP MAIN: INIT: xchg 3: IV l=8 v=15d302f818b44c04
ISAKMP MAIN: INIT: xchg 3: Hi l=20 v=079e0b5b0a0dd818818326a304f4c6cc17880d51
ISAKMP Encrypt:
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 05 10 02 00
00 00 00 00 00 00 00 40 08 00 00 0c 01 00 00 00 ac 10 02 44
00 00 00 18 07 9e 0b 5b 0a 0d d8 18 81 83 26 a3 04 f4 c6 cc
17 88 0d 51
ISAKMP Tx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 64
     Payload #:  0  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 0  Port: 0
       Value: 172.16.2.68
     Payload #:  1  Length: 24  Type: Hash (HASH)
       07 9e 0b 5b 0a 0d d8 18 81 83 26 a3 04 f4 c6 cc 17 88 0d 51
ISAKMP Tx Encrypted
ISAKMP Network Tx:
     localPort=4500 remotePort=4500
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     05 10 02 01 00 00 00 00 00 00 00 44 93 76 4d 16 c4 44 67 dc
     be 9e 57 77 09 09 0d 33 39 b7 72 78 e2 55 15 7e f8 44 8f a6
     1f ed 64 e6 31 6c 12 96 e1 dd eb a7
ISAKMP MAIN exchange 3: New State: AUTHSENT

ISAKMP Network Rx:
     remotePort=4500 localPort=4500
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     05 10 02 01 00 00 00 00 00 00 00 44 8e 60 41 35 ff 2d fe 8a
     85 11 68 ef 22 79 2a fd b1 12 9f 42 7e 97 ac 93 f6 54 52 ae
     14 e9 23 73 85 61 db ae 72 e5 70 88
ISAKMP Network Rx: Removed Non-ESP Marker.
ISAKMP Rx (decrypted)<---
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 05 10 02 01
00 00 00 00 00 00 00 44 08 00 00 0c 01 00 00 00 ac 1c 28 29
00 00 00 18 05 32 e1 27 2f 44 74 db 54 94 7a 68 0e b5 45 29
af 69 47 fe 00 00 00 03
ISAKMP Rx Message (decrypted)
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 01
     MessageID:  00000000   Total Length: 64
     Payload #:  0  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 0  Port: 0
       Value: 172.28.40.41
     Payload #:  1  Length: 24  Type: Hash (HASH)
       05 32 e1 27 2f 44 74 db 54 94 7a 68 0e b5 45 29 af 69 47 fe
ISAKMP MAIN exchange 3: New State: AUTHRECV

ISAKMP MAIN: INIT: xchg 3: RemoteID=172.28.40.41
ISAKMP MAIN: INIT: xchg 3: Hr l=20 v=0532e1272f4474db54947a680eb54529af6947fe
ISAKMP MAIN exchange 3: New State: UP
```

```
ISAKMP CORE: Exchange 3 done

ISAKMP DOI: IPSEC: Exchange IDs from selectors:
  IDi: type             IPV4_ADDR_SUBNET
       protocol Id      0
       port             0
       data             c0a80000ffffff00
  IDr: type             IPV4_ADDR_SUBNET
       protocol Id      0
       port             0
       data             acae0100ffffff00
ISAKMP DOI: IPSEC: Aquire Info -> Local Policy
  number of proposals 1
  proposal 0: # 1, protId 3, #transforms 1
    transform 0: # 1, id 3, sas 1
                  expiry: b 0-4294967295, s 0-28800
                  gr 1, mode 3, auth 2, keylen 0
ISAKMP QUICK: INIT: xchg 4: Started with peer 172.28.40.41
ISAKMP QUICK: INIT: xchg 4: COOKIE_I l=8 v=af9824b496c15952
ISAKMP QUICK: INIT: xchg 4: COOKIE_R l=8 v=5328549750db971e
ISAKMP QUICK: INIT: xchg 4: MessageID=294bf482
ISAKMP QUICK: INIT: xchg 4: IV l=8 v=b3ae9834d91f35f9

ISAKMP QUICK exchange 4: New State: SENDING_HASH_SA_NONCE
ISAKMP DOI: IPSEC: Exchange IDs not default:
  initiatorAddress      172.16.2.68
  IDi: type             IPV4_ADDR_SUBNET
       protocol Id      0
       port             0
       data             c0a80000ffffff00
  responderAddress      172.28.40.41
  IDr: type             IPV4_ADDR_SUBNET
       protocol Id      0
       port             0
       data             acae0100ffffff00

ISAKMP QI 4: HASH1: ID Payload Created

ISAKMP QI 4: HASH1: 012f5334 100
294bf4820a000028000000010000000010000001c01030401e21bae8500000010
0103000080040003800500020500001 8eacae0850a8f8c9353a6f91d6b0646c5
2b99fe71050000100400000c0a80000ffffff00000000100400000acae0100
ffffff00

ISAKMP QI 4: HASH1: result 867919ff7aa4e081103748c33a050773ee3aeb73
ISAKMP Encrypt:
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 08 10 20 00
29 4b f4 82 00 00 00 94 01 00 00 18 86 79 19 ff 7a a4 e0 81
10 37 48 c3 3a 05 07 73 ee 3a eb 73 0a 00 00 28 00 00 00 01
00 00 00 01 00 00 00 1c 01 03 04 01 e2 1b ae 85 00 00 00 10
01 03 00 00 80 04 00 03 80 05 00 02 05 00 00 18 ea ca e0 85
0a 8f 8c 93 53 a6 f9 1d 6b 06 46 c5 2b 99 fe 71 05 00 00 10
04 00 00 00 c0 a8 00 00 ff ff ff 00 00 00 00 10 04 00 00 00
ac ae 01 00 ff ff ff 00
```

```
ISAKMP Tx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 00
     MessageID:  294bf482   Total Length: 148
     Payload #:  0  Length: 24  Type: Hash (HASH)
       86 79 19 ff 7a a4 e0 81 10 37 48 c3 3a 05 07 73 ee 3a eb 73
     Payload #:  1  Length: 40  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ESP(3)  #Trans: 1  SPI: e21bae85
           Transform#: 1
             Transform Id ................... 3DESOUTER(3)
             Group Description .............. MODP768(1)
             Encapsulation Mode ............ UDP_ENCAP_TUNNEL(3)
             Authentication Algorithm ...... SHA(2)
     Payload #:  2  Length: 24  Type: Nonce (NONCE)
       ea ca e0 85 0a 8f 8c 93 53 a6 f9 1d 6b 06 46 c5 2b 99 fe 71
     Payload #:  3  Length: 16  Type: Identification (ID)
       Type: IPV4_ADDR_SUBNET  ProtocolId: 0  Port: 0
       Value: 192.168.0.0:255.255.255.0
     Payload #:  4  Length: 16  Type: Identification (ID)
       Type: IPV4_ADDR_SUBNET  ProtocolId: 0  Port: 0
       Value: 172.174.1.0:255.255.255.0
ISAKMP Tx Encrypted
ISAKMP Network Tx:
     localPort=4500 remotePort=4500
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     08 10 20 01 29 4b f4 82 00 00 00 9c eb c0 ff 5f 16 de 10 53
     af c6 56 3d 2d 83 0f 97 6c 54 66 6c 8d 0b 80 34 c5 07 55 30
     2f 6e 5f 06 6b 16 7d 93 e2 dc 8a 57 08 dd c4 28 d8 54 89 04
     b8 ee 38 5e e5 df f8 96 20 be b0 3d 6a b0 bb 85 43 49 57 d3
     ca 65 1b 79 bc 80 43 29 cd 43 98 a0 af ef 9f 7f 6a 0e e5 14
     f7 9b 25 ee af 47 ee a2 39 c9 1d d0 82 14 21 99 c7 78 28 a5
     0c db 04 1c b6 27 5a b1 d9 29 c3 8c 00 91 e8 af 42 05 a7 37

ISAKMP Network Rx:
     remotePort=4500 localPort=4500
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     08 10 20 01 29 4b f4 82 00 00 00 9c 81 b1 63 1a d9 67 15 b6
     95 14 e0 66 d9 3b ef 41 3c 83 43 e8 8b 59 4b 23 cd 12 89 bc
     0d 05 d0 da b0 82 9c 2c ef e0 4f 48 a7 9f d4 d7 c4 62 58 d9
     82 0b 12 99 82 87 cf 12 93 3c 1f 4d 47 6c 20 58 fd 31 12 ab
     7e 5a b0 ec 22 b0 4e c5 00 d4 b7 af fe f8 7f ac a5 db dd 37
     14 20 80 90 8d ae 63 1a 37 31 7a 76 72 d0 31 65 e2 9d da 2d
     f2 ce 62 d1 c3 cb a2 c3 99 fc 3e 46 98 2f c6 d4 77 a3 0c d7

ISAKMP Network Rx: Removed Non-ESP Marker.
ISAKMP Rx (decrypted)<---
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 08 10 20 01
29 4b f4 82 00 00 00 9c 01 00 00 18 63 56 ea 28 e5 17 9d c2
71 c2 9c 6a 87 a7 d4 fd 4d bb 3f 30 0a 00 00 28 00 00 00 01
00 00 00 01 00 00 00 1c 01 03 04 01 b0 f1 c5 1f 00 00 00 10
01 03 00 00 80 04 00 03 80 05 00 02 05 00 00 18 ff 46 76 ba
21 72 ba 52 ce 6e 60 2c 53 f9 cb 82 e4 a4 a4 67 05 00 00 10
04 00 00 00 c0 a8 00 00 ff ff ff 00 00 00 00 10 04 00 00 00
ac ae 01 00 ff ff ff 00 00 00 00 00 00 00 00 07
```

```
ISAKMP Rx Message (decrypted)
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 01
     MessageID:  294bf482   Total Length: 148
     Payload #:  0  Length: 24  Type: Hash (HASH)
       63 56 ea 28 e5 17 9d c2 71 c2 9c 6a 87 a7 d4 fd 4d bb 3f 30
     Payload #:  1  Length: 40  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ESP(3)  #Trans: 1  SPI: b0f1c51f
           Transform#: 1
             Transform Id ................. 3DESOUTER(3)
             Group Description ............ MODP768(1)
             Encapsulation Mode ........... UDP_ENCAP_TUNNEL(3)
             Authentication Algorithm ...... SHA(2)
     Payload #:  2  Length: 24  Type: Nonce (NONCE)
       ff 46 76 ba 21 72 ba 52 ce 6e 60 2c 53 f9 cb 82 e4 a4 a4 67
     Payload #:  3  Length: 16  Type: Identification (ID)
       Type: IPV4_ADDR_SUBNET  ProtocolId: 0  Port: 0
       Value: 192.168.0.0:255.255.255.0
     Payload #:  4  Length: 16  Type: Identification (ID)
       Type: IPV4_ADDR_SUBNET  ProtocolId: 0  Port: 0
       Value: 172.174.1.0:255.255.255.0

ISAKMP QUICK: INIT: xchg 4: rx msg 1: start
ISAKMP QUICK exchange 4: New State: RECEIVING_MESSAGE
ISAKMP QUICK: INIT: xchg 4: rx msg 1: prop policy done
ISAKMP QUICK: INIT: xchg 4: rx msg 1: TRAN 0,1 attributes good
ISAKMP QUICK: INIT: xchg 4: rx msg 1: TRAN 0,1 match
ISAKMP QUICK: INIT: xchg 4: rx msg 1: prop 0 match
ISAKMP QUICK: INIT: xchg 4: rx msg 1: All proposals matched:  (lpn 1)
ISAKMP QUICK: INIT: xchg 4: rx msg 1: payloads good:
ISAKMP QUICK: INIT: xchg 4: rx msg 1: good

ISAKMP QI 4: HASH2: 012fed94 120
294bf482eacae0850a8f8c9353a6f91d6b0646c52b99fe710a00002800000001
000000010000001c01030401b0f1c51f000000100103000080040003800500 02
05000018ff4676ba2172ba52ce6e602c53f9cb82e4a4a467050000100400000 0
c0a80000ffffff000000001004000000acae0100ffffff00

ISAKMP QI 4: HASH2: result 6356ea28e5179dc271c29c6a87a7d4fd4dbb3f30

ISAKMP QI 4: HASH INK1: 013005f4 45
03e21bae85eacae0850a8f8c9353a6f91d6b0646c52b99fe71ff4676ba2172ba
52ce6e602c53f9cb82e4a4a467

ISAKMP QI 4: HASH INK1: result 86581c245ae656a295b0f470bc01065c3357bf1a

ISAKMP QI 4: HASH OUTK1: 013005f4 45
03b0f1c51feacae0850a8f8c9353a6f91d6b0646c52b99fe71ff4676ba2172ba
52ce6e602c53f9cb82e4a4a467

ISAKMP QI 4: HASH OUTK1: result dde98e71ff3b3bad106ddf6c78f7555b3976cb2e

ISAKMP QI 4: HASH INK2: 013005e0 65
86581c245ae656a295b0f470bc01065c3357bf1a03e21bae85eacae0850a8f8c
9353a6f91d6b0646c52b99fe71ff4676ba2172ba52ce6e602c53f9cb82e4a4a4
67
```

```
ISAKMP QI 4: HASH INK2: result 3e02b94fb270da5c0fde4fce4d829ece7f3b4508

ISAKMP QI 4: HASH OUTK2: 013005e0 65
dde98e71ff3b3bad106ddf6c78f7555b3976cb2e03b0f1c51feacae0850a8f8c
9353a6f91d6b0646c52b99fe71ff4676ba2172ba52ce6e602c53f9cb82e4a4a4
67

ISAKMP QI 4: HASH INK3: 013005e0 65
3e02b94fb270da5c0fde4fce4d829ece7f3b450803e21bae85eacae0850a8f8c
9353a6f91d6b0646c52b99fe71ff4676ba2172ba52ce6e602c53f9cb82e4a4a4
67

ISAKMP QI 4: HASH INK3: result 425ee9c2644877e1ce34329092dfa8af13dd6076

ISAKMP QI 4: HASH OUTK3: 013005e0 65
46e6dbab8f6c681fde7107e07b1534c685d5337a03b0f1c51feacae0850a8f8c
9353a6f91d6b0646c52b99fe71ff4676ba2172ba52ce6e602c53f9cb82e4a4a4
67

ISAKMP QI 4: HASH OUTK3: result 9a2379eb25ccb2c0cd32f3fb0b4abf3e6da7aad9

ISAKMP QUICK exchange 4: New State: SENDING_HASH

ISAKMP QI 4: HASH3: 01301634 45
00294bf482eacae0850a8f8c9353a6f91d6b0646c52b99fe71ff4676ba2172ba
52ce6e602c53f9cb82e4a4a467

ISAKMP QI 4: HASH3: result 578ef2bc80aa2688cbb555f14e3114df92e226d0
ISAKMP Encrypt:
af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e 08 10 20 00
29 4b f4 82 00 00 00 34 00 00 00 18 57 8e f2 bc 80 aa 26 88
cb b5 55 f1 4e 31 14 df 92 e2 26 d0
ISAKMP Tx Message
     Cookies:   af9824b496c15952:5328549750db971e
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 00
     MessageID:  294bf482   Total Length: 52
     Payload #:  0  Length: 24  Type: Hash (HASH)
       57 8e f2 bc 80 aa 26 88 cb b5 55 f1 4e 31 14 df 92 e2 26 d0
ISAKMP Tx Encrypted
ISAKMP Network Tx:
     localPort=4500 remotePort=4500
     00 00 00 00 af 98 24 b4 96 c1 59 52 53 28 54 97 50 db 97 1e
     08 10 20 01 29 4b f4 82 00 00 00 3c f8 83 c6 7b 36 f8 27 89
     f3 5d a0 57 89 88 b7 87 4f 5a 1d 51 0f ef 42 e1 96 8f 37 3c
     dc 1c 9f c2
ISAKMP CORE: Exchange 4 done

ISAKMP QUICK exchange 4: New State: DONE

Echo reply 1 from 172.174.1.254 time delay 48 ms

SecOff Remote Office> dis isakmp debug=all

Info (1082056): ISAKMP Debugging has been disabled.
```

IPSec and ISAKMP SAs on the remote office router

This section shows the output of the commands **show ipsec sa** and **show isakmp sa** on the remote office. For each command, specifying the SA number gives much more detail.

show ipsec sa

```
SA Id  Policy                Bundle  State     Protocol    OutSPI       InSPI
-------------------------------------------------------------------------------
    1  remote_office             1  Valid     ESP     2968634655  3793464965
```

show ipsec sa=1

```
SA Id ................................ 1
  Policy ............................. remote_office
  Bundle ............................. 1
  SA Specification Used ............... 1
  State .............................. Valid
  Protocol ........................... ESP
  Role ............................... INITIATOR
  Mode ............................... UDP_ENCAP_TUNNEL
  Outbound SPI ....................... 2968634655
  Inbound SPI ........................ 3793464965
  Local tunnel IP address ............ 172.16.2.68
  Remote tunnel IP address ........... 172.28.40.41
  Encryption algorithm ............... 3DESOUTER
  Encryption ENCO channel............. 1
  Hash algorithm ..................... SHA
  Hash ENCO channel................... 2
  NAT-Traversal NAT-OA
    Peer original source IP address ..... n/a in tunnel mode
    Peer original destination IP address  n/a in tunnel mode
  Filters
    Local IP address ................... 192.168.0.0
    Local IP address mask .............. 255.255.255.0
    Remote IP address .................. 172.174.1.0
    Remote IP address mask ............. 255.255.255.0
    NAPT remote port number ............ n/a in tunnel mode
    Local Name ......................... ANY
    Remote Name ........................ ANY
  DF Bit ............................. CLEAR
  Last sent sequence number .......... 1
  Anti-replay checking enabled ....... FALSE
  Debug device ....................... 16
  Filter debug flags ................. 00000000
  Packet debug flags ................. 00000000
  Trace debug flags .................. 00000000
  Packet debug length ................ 72
```

show isakmp sa

```
                                    Expiry Limits - hard/soft/used
SA Id PeerAddress     EncA.  HashA. Bytes                Seconds
-----------------------------------------------------------------------
1     172.28.40.41    DES    SHA    -/-/-               86400/75600/23622
```

show isakmp sa=1

```
SA Id ................................ 1
  Initiator Cookie .................... af9824b496c15952
  Responder Cookie .................... 5328549750db971e
  DOI ................................. IPSEC
  Policy name ......................... remote_office
  State ............................... ACTIVE
  Local address ....................... 172.16.2.68
  Remote Address ...................... 172.28.40.41
  Remote Port ......................... 4500
  Time of establishment ............... **-***-****:**:**:**
  Commit bit set ...................... FALSE
  Send notifies ....................... FALSE
  Send deletes ........................ FALSE
  Always send ID ...................... FALSE
  Message Retry Limit ................. 8
  Initial Message Retry Timeout (s) ... 4
  Message Back-off .................... Incremental
  Exchange Delete Delay (s) ........... 30
  Do Xauth ............................ FALSE
    Xauth Finished .................... TRUE
  Expiry Limit (bytes) ................ -
  Soft Expiry Limit (bytes) ........... -
  Bytes seen .......................... -
  Expiry Limit (seconds) .............. 86400
  Soft Expiry Limit (seconds) ......... 75600
  Seconds since creation .............. 23624
  Number of Phase 2 exchanges allowed . 4294967293
  Number of acquires queued ........... 0

Sa Definition Information:
  Authentication Type ................. PRESHARED
  Encryption Algorithm ................ DES - 56 bit
  Hash Algorithm ...................... SHA
  group Type .......................... MODP
  group Description ................... MODP768
  DH Private Exponent Bits ............ 160
  expiry seconds ...................... 86400
  expiry kilobytes .................... -
```

continued on next page

continued from previous page

```
XAuth Information:
  Id ................................ 0
  Next Message ....................... UNKNOWN
  Status ............................ FAIL
  Type ............................... Generic
  Max Failed Attempts................. 0
  Failed Attempts..................... 0

NAT-Traversal Information:
  NAT-T enabled ...................... YES
  Peer NAT-T capable ................. YES (v8)
  NAT discovered ..................... LOCAL

Heartbeat Information:
  Send Heartbeats .................... NO
  Next sequence number tx ............ 1
  Receive Heartbeats ................. NO
  Last sequence number rx ............ 0
```

A Vista client initiates a tunnel

This section contains the following:

- "ISAKMP debug output on the head office router" on page 50
- "IPSec and ISAKMP SAs on the head office router" on page 62

ISAKMP debug output on the head office router

The following debug is the output from the command **enable isakmp debug=all** captured on the Head Office router.

```
SecOff Head Office> ena isakmp debug=all

Info (1082057): ISAKMP Debugging has been enabled.

SecOff Head Office> ISAKMP Network Rx:
     remotePort=44973 localPort=500
     db b8 0f 0a a0 ab df a1 00 00 00 00 00 00 00 00 01 10 02 00
     00 00 00 00 00 00 01 58 0d 00 00 ac 00 00 00 01 00 00 00 01
     00 00 00 a0 01 01 00 04 03 00 00 28 01 01 00 00 80 01 00 07
     80 0e 01 00 80 02 00 02 80 04 00 14 80 03 00 01 80 0b 00 01
     00 0c 00 04 00 00 70 80 03 00 00 28 02 01 00 00 80 01 00 07
     80 0e 00 80 80 02 00 02 80 04 00 13 80 03 00 01 80 0b 00 01
     00 0c 00 04 00 00 70 80 03 00 00 24 03 01 00 00 80 01 00 05
     80 02 00 02 80 04 00 0e 80 03 00 01 80 0b 00 01 00 0c 00 04
     00 00 70 80 00 00 00 24 04 01 00 00 80 01 00 05 80 02 00 02
     80 04 00 02 80 03 00 01 80 0b 00 01 00 0c 00 04 00 00 70 80
     0d 00 00 18 1e 2b 51 69 05 99 1c 7d 7c 96 fc bf b5 87 e4 61
     00 00 00 05 0d 00 00 14 4a 13 1c 81 07 03 58 45 5c 57 28 f2
     0e 95 45 2f 0d 00 00 14 90 cb 80 91 3e bb 69 6e 08 63 81 b5
     ec 42 7b 1f 0d 00 00 14 40 48 b7 d5 6e bc e8 85 25 e7 de 7f
     00 d6 c2 d3 0d 00 00 14 fb 1d e3 cd f3 41 b7 ea 16 b7 e5 be
     08 55 f1 20 0d 00 00 14 26 24 4d 38 ed db 61 b3 17 2a 36 e3
     d0 cf b8 19 00 00 00 14 e3 a5 96 6a 76 37 9f e7 07 22 82 31
     e5 ce 86 52
ISAKMP MAIN exchange 21: New State: IDLE

ISAKMP MAIN: RESP: xchg 21: Started with peer 172.28.40.80
ISAKMP Rx Message
     Cookies:   dbb80f0aa0abdfa1:0000000000000000
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 344
     Payload #:  0  Length: 172  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 4  SPI:
           Transform#: 1
             Transform Id ................... IKE(1)
             Encryption Algorithm........... AES(7)
             Key Length ..................... 256 bits
             Authentication Algorithm....... SHA(2)
             Authentication Method.......... PRESHARED(1)
             Group Description.............. UNKNOWN(20)
             Group Type..................... MODP
             Expiry Seconds................. 28800
```

```
                Transform#: 2
                  Transform Id ................... IKE(1)
                  Encryption Algorithm........... AES(7)
                  Key Length ..................... 128 bits
                  Authentication Algorithm....... SHA(2)
                  Authentication Method.......... PRESHARED(1)
                  Group Description.............. UNKNOWN(19)
                  Group Type..................... MODP
                  Expiry Seconds................. 28800
                Transform#: 3
                  Transform Id ................... IKE(1)
                  Encryption Algorithm........... 3DESOUTER(5)
                  Authentication Algorithm....... SHA(2)
                  Authentication Method.......... PRESHARED(1)
                  Group Description.............. UNKNOWN(14)
                  Group Type..................... MODP
                  Expiry Seconds................. 28800
                Transform#: 4
                  Transform Id ................... IKE(1)
                  Encryption Algorithm........... 3DESOUTER(5)
                  Authentication Algorithm....... SHA(2)
                  Authentication Method.......... PRESHARED(1)
                  Group Description.............. 1024(2)
                  Group Type..................... MODP
                  Expiry Seconds................. 28800
        Payload #:  1  Length: 24  Type: Vendor ID (VID)
          string=UNKNOWN
          1e 2b 51 69 05 99 1c 7d 7c 96 fc bf b5 87 e4 61 00 00 00 05
        Payload #:  2  Length: 20  Type: Vendor ID (VID)
          string=NAT-T RFC3947
          4a 13 1c 81 07 03 58 45 5c 57 28 f2 0e 95 45 2f
        Payload #:  3  Length: 20  Type: Vendor ID (VID)
          string=draft-ietf-ipsec-nat-t-ike-02\n
          90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
        Payload #:  4  Length: 20  Type: Vendor ID (VID)
          string=Microsoft L2TP/IPsec VPN Client
          40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
        Payload #:  5  Length: 20  Type: Vendor ID (VID)
          string=UNKNOWN
          fb 1d e3 cd f3 41 b7 ea 16 b7 e5 be 08 55 f1 20
        Payload #:  6  Length: 20  Type: Vendor ID (VID)
          string=UNKNOWN
          26 24 4d 38 ed db 61 b3 17 2a 36 e3 d0 cf b8 19
        Payload #:  7  Length: 20  Type: Vendor ID (VID)
          string=UNKNOWN
          e3 a5 96 6a 76 37 9f e7 07 22 82 31 e5 ce 86 52
      ISAKMP MAIN: RESP: xchg 21: Rx RFC3947 NAT-T vendor ID
      ISAKMP MAIN: RESP: xchg 21: Rx NAT-T version 2 vendor ID
      ISAKMP MAIN exchange 21: New State: SARECV

      ISAKMP DOI: IPSEC: Compare transform fail: encAlg l=DES(1) r=AES(7)
      ISAKMP DOI: IPSEC: Compare transform fail: encAlg l=DES(1) r=AES(7)
      ISAKMP DOI: IPSEC: Compare transform fail: encAlg l=DES(1) r=3DESOUTER(5)
      ISAKMP DOI: IPSEC: Compare transform fail: encAlg l=DES(1) r=3DESOUTER(5)
      ISAKMP MAIN: RESP: xchg 21: Policy 'office' does not match
      ISAKMP DOI: IPSEC: Compare transform fail: encAlg l=3DESOUTER(5) r=AES(7)
```

```
ISAKMP DOI: IPSEC: Compare transform fail: encAlg l=3DESOUTER(5) r=AES(7)
ISAKMP DOI: IPSEC: Compare transform fail: groupDescription l=2 r=14
ISAKMP MAIN: RESP: xchg 21: Found matching policy = windows_isakmp
ISAKMP Tx Message
     Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 180
     Payload #:  0  Length: 52  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 1  SPI:
           Transform#: 4
             Transform Id ................... IKE(1)
             Encryption Algorithm........... 3DESOUTER(5)
             Authentication Algorithm....... SHA(2)
             Authentication Method.......... PRESHARED(1)
             Group Description.............. 1024(2)
             Group Type..................... MODP
             Expiry Seconds................. 28800
     Payload #:  1  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-02\n
       90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     Payload #:  2  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-02 (no \n)
       cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
     Payload #:  3  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-03
       7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
     Payload #:  4  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-08
       8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4 28 c1 1d e8
     Payload #:  5  Length: 20  Type: Vendor ID (VID)
       string=NAT-T RFC3947
       4a 13 1c 81 07 03 58 45 5c 57 28 f2 0e 95 45 2f
ISAKMP Tx Unencrypted
ISAKMP Network Tx:
     localPort=500 remotePort=44973
     db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 01 10 02 00
     00 00 00 00 00 00 00 b4 0d 00 00 34 00 00 00 01 00 00 00 01
     00 00 00 28 01 01 00 01 00 00 00 20 04 01 00 00 80 01 00 05
     80 02 00 02 80 03 00 01 80 04 00 02 80 0b 00 01 80 0c 70 80
     0d 00 00 14 90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     0d 00 00 14 cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
     0d 00 00 14 7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
     0d 00 00 14 8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4 28 c1 1d e8
     00 00 00 14 4a 13 1c 81 07 03 58 45 5c 57 28 f2 0e 95 45 2f

ISAKMP MAIN exchange 21: New State: SASENT

ISAKMP Network Rx:
     remotePort=44973 localPort=500
     db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 04 10 02 00
     00 00 00 00 00 00 01 04 0a 00 00 84 11 cc 22 eb f5 35 b8 20
     38 51 2b 9a d7 8d 92 2e ae 7e db 2d cf 6c 34 a5 15 6c 49 a6
     72 16 d2 4e e1 5c e7 0a 98 c9 78 1c fa 2b c0 c0 d9 a2 2d de
     b2 8d c0 33 3d a9 03 2e 65 7d 6d b4 ad 8c 76 73 9f 21 e5 44
     b7 b2 46 c0 9c be 44 92 01 3b a5 ab a2 72 c9 80 d3 a4 1f 8f
     41 03 98 62 7b 0f 9d 93 e2 49 4e 33 ec 25 e8 02 4b 0c 2c 77
```

```
        a6 7c 4c 5f bd 97 df ac 86 23 aa 57 b0 31 6a 04 cc 77 ad cc
        14 00 00 34 3e ea fe 57 64 19 87 06 eb b9 d9 01 78 aa 51 20
        57 7e 55 68 e9 3f dc fa 39 b6 70 3b 02 5a e1 c7 d7 1c 3c 40
        b2 0c 18 2d ee 04 b8 c6 e9 ed 6a 0e 14 00 00 18 a6 43 60 00
        bf 27 0d f7 5c 83 9f d9 10 2f 6b 01 88 1d 8f 30 00 00 00 18
        1e 25 1e d6 91 57 c3 94 96 d3 6e 55 6c 4a b9 22 47 9b ec bb

ISAKMP Rx Message
        Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
        Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
        MessageID:  00000000   Total Length: 260
        Payload #:  0  Length: 132  Type: Key Exchange (KE)
          11 cc 22 eb f5 35 b8 20 38 51 2b 9a d7 8d 92 2e ae 7e db 2d
          cf 6c 34 a5 15 6c 49 a6 72 16 d2 4e e1 5c e7 0a 98 c9 78 1c
          fa 2b c0 c0 d9 a2 2d de b2 8d c0 33 3d a9 03 2e 65 7d 6d b4
          ad 8c 76 73 9f 21 e5 44 b7 b2 46 c0 9c be 44 92 01 3b a5 ab
          a2 72 c9 80 d3 a4 1f 8f 41 03 98 62 7b 0f 9d 93 e2 49 4e 33
          ec 25 e8 02 4b 0c 2c 77 a6 7c 4c 5f bd 97 df ac 86 23 aa 57
          b0 31 6a 04 cc 77 ad cc
        Payload #:  1  Length: 52  Type: Nonce (NONCE)
          3e ea fe 57 64 19 87 06 eb b9 d9 01 78 aa 51 20 57 7e 55 68
          e9 3f dc fa 39 b6 70 3b 02 5a e1 c7 d7 1c 3c 40 b2 0c 18 2d
          ee 04 b8 c6 e9 ed 6a 0e
        Payload #:  2  Length: 24  Type: NAT-T(rfc) Discovery (NAT-D)
          a6 43 60 00 bf 27 0d f7 5c 83 9f d9 10 2f 6b 01 88 1d 8f 30
        Payload #:  3  Length: 24  Type: NAT-T(rfc) Discovery (NAT-D)
          1e 25 1e d6 91 57 c3 94 96 d3 6e 55 6c 4a b9 22 47 9b ec bb
ISAKMP MAIN: RESP: xchg 21: NAT-D detected a remote NAT
ISAKMP MAIN exchange 21: New State: KERECV

ISAKMP MAIN: RESP: xchg 21: x l=20 v=2e0052e6cc317369595449e8ce5c3fa3ee0fbe8f
ISAKMP MAIN: RESP: xchg 21: g^x l=128
   v=11cc22ebf535b82038512b9ad78d922eae7edb2c
ISAKMP MAIN: RESP: xchg 21: g^y l=128
   v=20c3f192fe7e9f4a15c1d178a93f39c3a3b1e28b
ISAKMP MAIN: RESP: xchg 21: g^xy l=128
   v=f4ef20640f4ce83b04c8d885c7f113a232d3b8b
ISAKMP MAIN: RESP: xchg 21: Ni l=48
   v=3eeafe5764198706ebb9d90178aa5120577e5568ee
ISAKMP MAIN: RESP: xchg 21: Nr l=20
   v=795379cecb606a1e6b67a589ad510815ba011b5c
ISAKMP MAIN: RESP: xchg 21: COOKIE_I l=8 v=dbb80f0aa0abdfa1
ISAKMP MAIN: RESP: xchg 21: COOKIE_R l=8 v=3e39ebd4724db839
ISAKMP MAIN: RESP: xchg 21: Key l=6 v=667269656e64
ISAKMP MAIN: RESP: xchg 21: SKEYID l=20
   v=ad9d900330a44b42a3bb65eae13dd6d70b4eda
ISAKMP MAIN: RESP: xchg 21: SKEYID_d l=20
   v=1458a675592419144b9acc2e457d1ea95efe
ISAKMP MAIN: RESP: xchg 21: SKEYID_a l=20
   v=0ca53774203dc64b1345989ece0c509b82d1
ISAKMP MAIN: RESP: xchg 21: SKEYID_e l=20
   v=e62f9a40fb32dd3126bfee37a500251b8f56
ISAKMP MAIN: RESP: xchg 21: EncKey l=24
   v=c4c569127928715d4d3c8ca2d8bab0079c2e94
ISAKMP MAIN: RESP: xchg 21: IV l=8 v=19a43ac51d4be2b4
```

```
ISAKMP Tx Message
     Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 232
     Payload #:  0  Length: 132  Type: Key Exchange (KE)
       20 c3 f1 92 fe 7e 9f 4a 15 c1 d1 78 a9 3f 39 c3 a3 b1 e2 87
       6a 63 08 2a 5d b7 85 d2 38 8b db 60 14 69 74 ae cf e5 ff 9a
       ff 1c 90 44 40 4f 80 38 5b 9e 7c d1 ec bf 3a 48 90 0a 15 a9
       47 c8 8f 26 c4 f7 09 17 13 fa 7e 7d 26 45 53 08 8d 75 5a 6c
       0f ae ac e1 f4 00 e3 5f 2d 41 18 55 a6 a6 2e 09 5f b9 84 0c
       39 0c ac 9d 24 e0 34 a5 de dd 0e b2 f3 cb 3d e4 04 cf 36 f5
       82 20 a6 ed 58 1b 94 3b
     Payload #:  1  Length: 24  Type: Nonce (NONCE)
       79 53 79 ce cb 60 6a 1e 6b 67 a5 89 ad 51 08 15 ba 01 1b 5c
     Payload #:  2  Length: 24  Type: NAT-T(rfc) Discovery (NAT-D)
       2b 9a 20 d1 1d e1 88 03 78 59 14 13 74 5a d0 87 8b d6 1c 63
     Payload #:  3  Length: 24  Type: NAT-T(rfc) Discovery (NAT-D)
       a6 43 60 00 bf 27 0d f7 5c 83 9f d9 10 2f 6b 01 88 1d 8f 30
ISAKMP Tx Unencrypted
ISAKMP Network Tx:
     localPort=500 remotePort=44973
     db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 04 10 02 00
     00 00 00 00 00 00 00 e8 0a 00 00 84 20 c3 f1 92 fe 7e 9f 4a
     15 c1 d1 78 a9 3f 39 c3 a3 b1 e2 87 6a 63 08 2a 5d b7 85 d2
     38 8b db 60 14 69 74 ae cf e5 ff 9a ff 1c 90 44 40 4f 80 38
     5b 9e 7c d1 ec bf 3a 48 90 0a 15 a9 47 c8 8f 26 c4 f7 09 17
     13 fa 7e 7d 26 45 53 08 8d 75 5a 6c 0f ae ac e1 f4 00 e3 5f
     2d 41 18 55 a6 a6 2e 09 5f b9 84 0c 39 0c ac 9d 24 e0 34 a5
     de dd 0e b2 f3 cb 3d e4 04 cf 36 f5 82 20 a6 ed 58 1b 94 3b
     14 00 00 18 79 53 79 ce cb 60 6a 1e 6b 67 a5 89 ad 51 08 15
     ba 01 1b 5c 14 00 00 18 2b 9a 20 d1 1d e1 88 03 78 59 14 13
     74 5a d0 87 8b d6 1c 63 00 00 00 18 a6 43 60 00 bf 27 0d f7
     5c 83 9f d9 10 2f 6b 01 88 1d 8f 30
ISAKMP MAIN exchange 21: New State: KESENT

ISAKMP Network Rx:
     remotePort=48348 localPort=4500
     00 00 00 00 db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39
     05 10 02 01 00 00 00 00 00 00 00 44 4d 41 16 ff b5 83 3b ee
     03 48 3d 36 9b fc 88 b6 93 d5 23 93 6e d9 2c db 36 05 78 bb
     b3 59 89 49 12 31 49 6d 2a 55 08 a2
ISAKMP Network Rx: Removed Non-ESP Marker.
ISAKMP Rx (decrypted)<---
db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 05 10 02 01
00 00 00 00 00 00 00 44 08 00 00 0c 01 00 00 00 ac 10 02 42
00 00 00 18 1b 1b 0b bf 9c 72 05 36 72 39 43 67 e1 95 4b 46
48 6c a2 4b 00 00 00 00
ISAKMP Rx Message (decrypted)
     Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 01
     MessageID:  00000000   Total Length: 64
     Payload #:  0  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 0  Port: 0
       Value: 172.16.2.66
```

```
     Payload #:  1  Length: 24  Type: Hash (HASH)
       1b 1b 0b bf 9c 72 05 36 72 39 43 67 e1 95 4b 46 48 6c a2 4b
ISAKMP CORE: Info: exchange 21 local port changed from 500 to 4500

ISAKMP CORE: Info: exchange 21 remote port changed from 44973 to 48348

ISAKMP MAIN exchange 21: New State: AUTHRECV

ISAKMP MAIN: RESP: xchg 21: RemoteID=172.16.2.66 OR 172.28.40.80 for NAT-T
ISAKMP MAIN: RESP: xchg 21: Hi l=20
   v=1b1b0bbf9c72053672394367e1954b46486ca24b
ISAKMP MAIN: RESP: xchg 21: Hr l=20
   v=c8a41ad957323d9934c4766d69031900e1941224
ISAKMP Encrypt:
db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 05 10 02 00
00 00 00 00 00 00 00 40 08 00 00 0c 01 00 00 00 ac 1c 28 29
00 00 00 18 c8 a4 1a d9 57 32 3d 99 34 c4 76 6d 69 03 19 00
e1 94 12 24
ISAKMP Tx Message
     Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 64
     Payload #:  0  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 0  Port: 0
       Value: 172.28.40.41
     Payload #:  1  Length: 24  Type: Hash (HASH)
       c8 a4 1a d9 57 32 3d 99 34 c4 76 6d 69 03 19 00 e1 94 12 24
ISAKMP Tx Encrypted
ISAKMP Network Tx:
     localPort=4500 remotePort=48348
     00 00 00 00 db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39
     05 10 02 01 00 00 00 00 00 00 00 44 2d b4 f6 be cd 7f b1 2c
     cf 34 63 a6 b5 cb e5 4c 4c 0b da 68 12 54 ce 67 83 45 a0 01
     0b a5 93 de 23 5c 78 b2 28 a5 e4 ce
ISAKMP MAIN exchange 21: New State: AUTHSENT

ISAKMP MAIN exchange 21: New State: UP

ISAKMP CORE: Exchange 21 done

ISAKMP Network Rx:
     remotePort=48348 localPort=4500
     00 00 00 00 db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39
     08 10 20 01 00 00 00 01 00 00 01 3c 24 4c fd 0e 1c 94 a3 6f
     58 ae ca 92 b3 5b 92 05 1d f3 52 66 64 62 40 38 90 f5 7b af
     5e 8f f0 3b a0 a0 07 2a 40 6e 01 9d c4 a1 86 64 8a fc 85 97
     84 4b 32 ef 1a 65 0c 25 7b 5a d0 e8 21 94 33 39 f3 ca 04 dd
     1a 11 d2 05 2f 9a cf 7b 91 0a 15 51 87 d3 8a 2c 49 39 8d 25
     43 e5 58 44 c3 28 6d 89 24 f5 9e 4c 60 3c 4c 07 c0 e1 17 25
     32 83 92 cc 4b ca 08 6e f4 a6 18 0c 04 46 ea 97 4b a7 3b 4b
     7d d7 85 1b c4 3a 9d 4c cc be e9 da 50 bb b6 a4 46 d1 77 8b
     9d 4b bb 59 5d 70 61 08 e2 70 18 b6 f5 7c a7 61 3f d7 ad c7
     e1 33 58 2f 2e 84 ff 8c 7b 2e e3 42 cc 97 50 d9 f0 f6 7f 92
     28 0a 90 f8 f9 fd 60 4d c5 b4 95 a7 12 d3 c1 0d b3 23 3b 23
     92 de 42 c6 b4 99 fc f1 00 fa ac 90 ec 1d d6 67 95 a5 25 8c
     c8 90 99 c9 ad d4 d6 f3 ea 06 fd 2e 9e 2d 55 f1 12 c5 4f 2f
     3c b5 d7 f8 ec 4e 57 04 6d 52 fa 80 86 83 26 f5 9e 78 20 07
     a3 f3 16 ab 44 ad f6 fc a7 ae 1f ce 6d a2 e0 06 c1 35 53 21
```

```
ISAKMP Network Rx: Removed Non-ESP Marker.

ISAKMP QUICK: RESP: xchg 22: Started with peer 172.28.40.80
ISAKMP QUICK exchange 22: New State: WAIT_HASH_SA_NONCE
ISAKMP QUICK: RESP: xchg 22: COOKIE_I l=8 v=dbb80f0aa0abdfa1
ISAKMP QUICK: RESP: xchg 22: COOKIE_R l=8 v=3e39ebd4724db839
ISAKMP QUICK: RESP: xchg 22: MessageID=00000001
ISAKMP QUICK: RESP: xchg 22: IV l=8 v=3eb8f1ee317e087b
ISAKMP Rx (decrypted)<---
db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 08 10 20 01
00 00 00 01 00 00 01 3c 01 00 00 18 f4 1b 6d 52 d0 ba 58 ca
de 7e d2 b3 19 84 c8 6b 9d e4 86 fb 0a 00 00 ac 00 00 00 01
00 00 00 01 02 00 00 38 01 03 04 01 fb 83 82 4c 00 00 00 2c
01 0c 00 00 80 04 00 04 80 06 00 80 80 05 00 02 80 01 00 01
00 02 00 04 00 00 0e 10 80 01 00 02 00 02 00 04 00 03 d0 90
02 00 00 34 02 03 04 01 fb 83 82 4c 00 00 00 28 01 03 00 00
80 04 00 04 80 05 00 02 80 01 00 01 00 02 00 04 00 00 0e 10
80 01 00 02 00 02 00 04 00 03 d0 90 00 00 00 34 03 03 04 01
fb 83 82 4c 00 00 00 28 01 0b 00 00 80 04 00 04 80 05 00 02
80 01 00 01 00 02 00 04 00 00 0e 10 80 01 00 02 00 02 00 04
00 03 d0 90 05 00 00 34 3d a1 c1 8b 22 e7 3f 9d 75 62 10 7f
d1 4b 8a 90 7e 00 98 88 ef eb 61 38 5e a6 5a 4a 97 ec aa 2e
2a 68 ac 81 68 96 86 c0 2f 4f 14 52 49 87 fd a3 05 00 00 0c
01 11 06 a5 ac 10 02 42 15 00 00 0c 01 11 06 a5 ac 1c 28 29
00 00 00 0c 01 00 00 00 ac 10 02 42 00 00 00 00
ISAKMP Rx Message (decrypted)
     Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 01
     MessageID:  00000001   Total Length: 312
     Payload #:  0  Length: 24  Type: Hash (HASH)
       f4 1b 6d 52 d0 ba 58 ca de 7e d2 b3 19 84 c8 6b 9d e4 86 fb
     Payload #:  1  Length: 172  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ESP(3)  #Trans: 1  SPI: fb83824c
           Transform#: 1
             Transform Id .................. AES(12)
             Group Description ............. MODP768(1)
             Encapsulation Mode ............ UDP_ENCAP_TRANSPORT(4)
             Authentication Algorithm ...... SHA(2)
             Expiry KBytes ................. 250000
             Expiry Seconds ................ 3600
             Key Length .................... 128 bits
         Proposal#: 2  Protocol: ESP(3)  #Trans: 1  SPI: fb83824c
           Transform#: 1
             Transform Id .................. 3DESOUTER(3)
             Group Description ............. MODP768(1)
             Encapsulation Mode ............ UDP_ENCAP_TRANSPORT(4)
             Authentication Algorithm ...... SHA(2)
             Expiry KBytes ................. 250000
             Expiry Seconds ................ 3600
         Proposal#: 3  Protocol: ESP(3)  #Trans: 1  SPI: fb83824c
           Transform#: 1
             Transform Id .................. NULL(11)
             Group Description ............. MODP768(1)
             Encapsulation Mode ............ UDP_ENCAP_TRANSPORT(4)
             Authentication Algorithm ...... SHA(2)
             Expiry KBytes ................. 250000
             Expiry Seconds ................ 3600
```

```
        Payload #:  2  Length: 52  Type: Nonce (NONCE)
          3d a1 c1 8b 22 e7 3f 9d 75 62 10 7f d1 4b 8a 90 7e 00 98 88
          ef eb 61 38 5e a6 5a 4a 97 ec aa 2e 2a 68 ac 81 68 96 86 c0
          2f 4f 14 52 49 87 fd a3
        Payload #:  3  Length: 12  Type: Identification (ID)
          Type: IPV4_ADDR  ProtocolId: 17  Port: 1701
          Value: 172.16.2.66
        Payload #:  4  Length: 12  Type: Identification (ID)
          Type: IPV4_ADDR  ProtocolId: 17  Port: 1701
          Value: 172.28.40.41
        Payload #:  5  Length: 12  Type: NAT-T(rfc) Original Address (NAT-OA)
          ID Type=IPv4 IP=172.16.2.66
ISAKMP QUICK: RESP: xchg 22: rx msg 1: start
ISAKMP QUICK exchange 22: New State: RECEIVING_MESSAGE
ISAKMP QUICK: RESP: xchg 22: rx msg 1: rec PROP 0: # 1, protid 3, outspi
   fb8382
ISAKMP QUICK: RESP: xchg 22: rx msg 1: PROP 0 transforms good
ISAKMP QUICK: RESP: xchg 22: rx msg 1: rec PROP 1: # 2, protid 3, outspi
   fb8382
ISAKMP QUICK: RESP: xchg 22: rx msg 1: PROP 1 transforms good
ISAKMP QUICK: RESP: xchg 22: rx msg 1: rec PROP 2: # 3, protid 3, outspi
   fb8382
ISAKMP QUICK: RESP: xchg 22: rx msg 1: PROP 2 transforms good
ISAKMP QUICK: RESP: xchg 22: rx msg 1: SA proposals good
ISAKMP QUICK: RESP: xchg 22: rx msg 1: payloads good:
ISAKMP QUICK: RESP: xchg 22: rx msg 1: good

ISAKMP QR 22: HASH1: 012708f4 264
000000010a0000ac0000000100000001020000380103040 1fb83824c0000002c
010c000080040004800600808005000280010001000200040000e1080010002
000200040003d09002000034020304 01fb83824c00000028010300008004000 4
8005000280010001000200040000e1080010002000200040003d09000000034


ISAKMP QR 22: HASH1: result f41b6d52d0ba58cade7ed2b31984c86b9de486fb

ISAKMP DOI: IPSEC: resp match pol:
   peerIP=172.28.40.80
   filtEnableFlag=00000075
   filtOpaqueFlag=00000000
   selectorsFromPktFlag=00000000
   lAddr=172.28.40.41
   lMask=255.255.255.255
   lAddrLow=0.0.0.0
   lAddrHigh=0.0.0.0
   rAddr=172.16.2.66
   rMask=255.255.255.255
   rAddrLow=0.0.0.0
   rAddrHigh=0.0.0.0
   lPort=1701
   rPort=1701
   lName=
   rName=
   lAddrVer=4
   rAddrVer=4
```

```
ISAKMP DOI: IPSEC: Aquire Info -> Local Policy
  number of proposals 1
  proposal 0: # 1, protId 3, #transforms 4
    transform 0: # 1, id 3, sas 1
                  expiry: b 0-4294967295, s 0-28800
                  gr 1, mode 2, auth 2, keylen 0
    transform 0: # 2, id 3, sas 2
                  expiry: b 0-4294967295, s 0-28800
                  gr 1, mode 2, auth 1, keylen 0
    transform 0: # 3, id 2, sas 3
                  expiry: b 0-4294967295, s 0-28800
                  gr 1, mode 2, auth 2, keylen 0
    transform 0: # 4, id 2, sas 4
                  expiry: b 0-4294967295, s 0-28800
                  gr 1, mode 2, auth 1, keylen 0
ISAKMP QUICK: RESP: xchg 22: Match Pol: 2 Local (prot 1) found - 0
ISAKMP QUICK: RESP: xchg 22: Match Pol: 2 Remote (prot 1) found - 0
ISAKMP QUICK: RESP: xchg 22: Match Pol: prop match try: l
   00000000000000001270c
ISAKMP QUICK: RESP: xchg 22: Match Pol: matching (prot 2) props 1
ISAKMP QUICK: RESP: xchg 22: Match Pol: (prot 2) tran match try: loc 0 - rem 0
ISAKMP QUICK: RESP: xchg 22: Match Tran: id match failed (3:12)
ISAKMP QUICK: RESP: xchg 22: Match Pol: (prot 2) tran match try: loc 1 - rem 0
ISAKMP QUICK: RESP: xchg 22: Match Tran: id match failed (3:12)
ISAKMP QUICK: RESP: xchg 22: Match Pol: (prot 2) tran match try: loc 2 - rem 0
ISAKMP QUICK: RESP: xchg 22: Match Tran: id match failed (2:12)
ISAKMP QUICK: RESP: xchg 22: Match Pol: (prot 2) tran match try: loc 3 - rem 0
ISAKMP QUICK: RESP: xchg 22: Match Tran: id match failed (2:12)
ISAKMP QUICK: RESP: xchg 22: Match Pol: rem prop number 1 no match
ISAKMP QUICK: RESP: xchg 22: Match Pol: 2 Remote (prot 2) found - 1
ISAKMP QUICK: RESP: xchg 22: Match Pol: prop match try: l
   00000000000000012700
ISAKMP QUICK: RESP: xchg 22: Match Pol: matching (prot 2) props 1
ISAKMP QUICK: RESP: xchg 22: Match Pol: (prot 2) tran match try: loc 0 - rem 0
ISAKMP QUICK: RESP: xchg 22: Match Tran: match good
ISAKMP QUICK: RESP: xchg 22: Match Pol: matched
ISAKMP QUICK: RESP: xchg 22: proc 1: done good

ISAKMP QI 22: HASH INK1: 01277294 73
03b40c57b53da1c18b22e73f9d7562107fd14b8a907e009888efeb61385ea65a
4a97ecaa2e2a68ac81689686c02f4f14524987fda3d7cc3e5e4f8ff25dade2bb
81fedbb5f206b1b7f9

ISAKMP QI 22: HASH INK1: result 2ab7f346585bb8ff63269bca5c8fcae7cdfa5e5f

ISAKMP QI 22: HASH OUTK1: 01277294 73
03fb83824c3da1c18b22e73f9d7562107fd14b8a907e009888efeb61385ea65a
4a97ecaa2e2a68ac81689686c02f4f14524987fda3d7cc3e5e4f8ff25dade2bb
81fedbb5f206b1b7f9

ISAKMP QI 22: HASH OUTK1: result 371974e6186cfee068e29a0fc82155775280a5a5

ISAKMP QI 22: HASH INK2: 01277280 93
2ab7f346585bb8ff63269bca5c8fcae7cdfa5e5f03b40c57b53da1c18b22e73f
9d7562107fd14b8a907e009888efeb61385ea65a4a97ecaa2e2a68ac81689686
c02f4f14524987fda3d7cc3e5e4f8ff25dade2bb81fedbb5f206b1b7f9
```

```
ISAKMP QI 22: HASH INK2: result b7aca20d27d4f98a944ccce8225da17ddf0fa3e6

ISAKMP QI 22: HASH OUTK2: 01277280 93
371974e6186cfee068e29a0fc82155775280a5a503fb83824c3da1c18b22e73f
9d7562107fd14b8a907e009888efeb61385ea65a4a97ecaa2e2a68ac81689686
c02f4f14524987fda3d7cc3e5e4f8ff25dade2bb81fedbb5f206b1b7f9

ISAKMP QI 22: HASH INK3: 01277280 93
b7aca20d27d4f98a944ccce8225da17ddf0fa3e603b40c57b53da1c18b22e73f
9d7562107fd14b8a907e009888efeb61385ea65a4a97ecaa2e2a68ac81689686
c02f4f14524987fda3d7cc3e5e4f8ff25dade2bb81fedbb5f206b1b7f9

ISAKMP QI 22: HASH INK3: result 2610622d2fa3a9bbe2c8643be79f150150ff4e3b

ISAKMP QI 22: HASH OUTK3: 01277280 93
ef250a4fa192c790bd85acd460362b36caaa4c2203fb83824c3da1c18b22e73f
9d7562107fd14b8a907e009888efeb61385ea65a4a97ecaa2e2a68ac81689686
c02f4f14524987fda3d7cc3e5e4f8ff25dade2bb81fedbb5f206b1b7f9

ISAKMP QI 22: HASH OUTK3: result 21aa1dd1be0edc6ef5e9cd12553d7faf201f6846

ISAKMP QUICK exchange 22: New State: SENDING_HASH_SA_NONCE
ISAKMP DOI: IPSEC: Exchange IDs not default:
  initiatorAddress      172.28.40.80
  IDi: type             IPV4_ADDR
       protocol Id      17
       port             1701
       data             ac100242
  responderAddress      172.28.40.41
  IDr: type             IPV4_ADDR
       protocol Id      17
       port             1701
       data             ac1c2829

ISAKMP QR 22: HASH1: ID Payload Created

ISAKMP QR 22: HASH2: 012782d4 188
000000013da1c18b22e73f9d7562107fd14b8a907e009888efeb61385ea65a4a
97ecaa2e2a68ac81689686c02f4f14524987fda30a000040000000100000001
0000003402030401b40c57b500000028010300008004000480050002800100 01
0002000400000e1080010002000200040003d09005000018d7cc3e5e4f8ff25d


ISAKMP QR 22: HASH2: result dc0ac22e507dbff6779e2ee640adaa9260d8de33
ISAKMP Encrypt:
db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 08 10 20 00
00 00 00 01 00 00 00 bc 01 00 00 18 dc 0a c2 2e 50 7d bf f6
77 9e 2e e6 40 ad aa 92 60 d8 de 33 0a 00 00 40 00 00 00 01
00 00 00 01 00 00 00 34 02 03 04 01 b4 0c 57 b5 00 00 00 28
01 03 00 00 80 04 00 04 80 05 00 02 80 01 00 01 00 02 00 04
00 00 0e 10 80 01 00 02 00 02 00 04 00 03 d0 90 05 00 00 18
d7 cc 3e 5e 4f 8f f2 5d ad e2 bb 81 fe db b5 f2 06 b1 b7 f9
05 00 00 0c 01 11 06 a5 ac 10 02 42 15 00 00 0c 01 11 06 a5
ac 1c 28 29 15 00 00 0c 01 00 00 00 ac 1c 28 50 00 00 00 0c
01 00 00 00 ac 1c 28 29
```

```
ISAKMP Tx Message
     Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 00
     MessageID:  00000001   Total Length: 188
     Payload #:  0  Length: 24  Type: Hash (HASH)
       dc 0a c2 2e 50 7d bf f6 77 9e 2e e6 40 ad aa 92 60 d8 de 33
     Payload #:  1  Length: 64  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 2  Protocol: ESP(3)  #Trans: 1  SPI: b40c57b5
           Transform#: 1
             Transform Id ................... 3DESOUTER(3)
             Group Description .............. MODP768(1)
             Encapsulation Mode ............. UDP_ENCAP_TRANSPORT(4)
             Authentication Algorithm ...... SHA(2)
             Expiry KBytes .................. 250000
             Expiry Seconds ................. 3600
     Payload #:  2  Length: 24  Type: Nonce (NONCE)
       d7 cc 3e 5e 4f 8f f2 5d ad e2 bb 81 fe db b5 f2 06 b1 b7 f9
     Payload #:  3  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 17  Port: 1701
       Value: 172.16.2.66
     Payload #:  4  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 17  Port: 1701
       Value: 172.28.40.41
     Payload #:  5  Length: 12  Type: NAT-T(rfc) Original Address (NAT-OA)
       ID Type=IPv4 IP=172.28.40.80
     Payload #:  6  Length: 12  Type: NAT-T(rfc) Original Address (NAT-OA)
       ID Type=IPv4 IP=172.28.40.41
ISAKMP Tx Encrypted
ISAKMP Network Tx:
     localPort=4500 remotePort=48348
     00 00 00 00 db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39
     08 10 20 01 00 00 00 01 00 00 00 c4 8f 3a 6b 52 30 69 9c 12
     d5 2c ee f4 f3 16 06 16 b8 ce 0b 55 0e 50 03 a8 0e 83 b3 0a
     d0 7d b7 f9 00 2a 1d 56 64 01 48 0e d6 73 ed 94 af 89 31 2a
     f5 23 23 e9 b5 c4 12 87 ec 6c 82 ab 0c aa e4 87 b2 f0 dd d7
     da 30 d1 a6 91 44 e7 2a 91 01 e2 c5 8d 86 27 cc 70 00 28 71
     2f db 06 78 57 56 8e 15 29 89 2f e4 de bc 19 5b b7 dd bb da
     e2 3f 72 b1 4b 7f 31 39 6a 02 22 8c 04 58 96 28 54 2f 3b cd
     27 2c 34 eb c0 9f 3c 48 70 d8 55 3b 20 91 a9 c1 dc 17 f7 6f
     e9 a7 c1 20 64 00 bb 2b e0 7c 98 88 e0 c9 cb 97 4e 84 17 d3

ISAKMP Network Rx:
     remotePort=48348 localPort=4500
     b4 0c 57 b5 00 00 00 01 6a c2 67 fd 17 fd a8 5d 68 87 3f 39
     a9 7d 43 d6 34 b3 62 34 43 19 27 6c f8 6a ba 14 4d 48 e6 4b
     c0 25 bb c0 1d f0 22 35 75 39 2e 2e 5c 42 73 d9 71 b3 25 21
     62 dd 07 cd 85 7d 20 e9 c6 4b 7b 38 17 d7 af 18 cc 75 38 2b
     a4 8a d0 99 03 26 49 0f 8f 9b c8 7c 5d ee b0 c5 a7 09 95 56
     2b 3a 12 bd fd 5e 21 15 25 5b 3c fe 46 e4 36 d3 21 3a 79 bc
     c2 b3 5d e2 a4 7e 68 84 d5 58 34 03 8a 2f 7c bd f6 d0 aa 2c
     0d 18 93 5f 34 8a 65 ec
ISAKMP Network Rx: Missing Non-ESP Marker.
```

```
ISAKMP Network Rx:
     remotePort=48348 localPort=4500
     00 00 00 00 db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39
     08 10 20 01 00 00 00 01 00 00 00 3c 43 1c fd 9c 2d 33 8b 93
     13 8c 6b 61 3a 09 f4 48 ea 03 14 55 2b 6e f2 af d5 98 0f 7c
     5c 51 d8 72
ISAKMP Network Rx: Removed Non-ESP Marker.
ISAKMP Rx (decrypted)<---
db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 08 10 20 01
00 00 00 01 00 00 00 3c 00 00 00 18 c9 81 77 45 4d 36 0b 8a
1e 30 ba 36 71 f2 5d 7b c9 3d db 8b 00 00 00 00 00 00 00 00
ISAKMP Rx Message (decrypted)
     Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 01
     MessageID:  00000001   Total Length: 52
     Payload #:  0  Length: 24  Type: Hash (HASH)
       c9 81 77 45 4d 36 0b 8a 1e 30 ba 36 71 f2 5d 7b c9 3d db 8b

ISAKMP QUICK: RESP: xchg 22: rx msg 1: start
ISAKMP QUICK exchange 22: New State: RECEIVING_MESSAGE
ISAKMP QUICK: RESP: xchg 22: rx msg 2: payloads good:
ISAKMP QUICK: RESP: xchg 22: rx msg 2: good

ISAKMP QR 22: HASH3: 01281d34 73
00000000013da1c18b22e73f9d7562107fd14b8a907e009888efeb61385ea65a
4a97ecaa2e2a68ac81689686c02f4f14524987fda3d7cc3e5e4f8ff25dade2bb
81fedbb5f206b1b7f9

ISAKMP QR 22: HASH3: result c98177454d360b8a1e30ba3671f25d7bc93ddb8b
ISAKMP CORE: Exchange 22 done

ISAKMP QUICK exchange 22: New State: DONE
```

IPSec and ISAKMP SAs on the head office router

This section shows the output of the commands **show ipsec sa** and **show isakmp sa** on the head office. For each command, specifying the SA number gives much more detail.

show ipsec sa

```
SA Id  Policy                Bundle  State     Protocol    OutSPI       InSPI
-------------------------------------------------------------------------------
    5  office                   10  Valid     ESP     3793464965  2968634655
    6  windows_warriors          1  Valid     ESP     4219699788  3020707765
```

show ipsec sa=6

```
SA Id ................................ 6
  Policy ............................. windows_warriors
  Bundle ............................. 1
  SA Specification Used ............... 1
  State .............................. Valid
  Protocol ........................... ESP
  Role ............................... RESPONDER
  Mode ............................... UDP_ENCAP_TRANSPORT
  Outbound SPI ....................... 4219699788
  Inbound SPI ........................ 3020707765
  Encryption algorithm ............... 3DESOUTER
  Encryption ENCO channel............. 3
  Hash algorithm ..................... SHA
  Hash ENCO channel................... 4
  NAT-Traversal NAT-OA
    Peer original source IP address ..... 172.16.2.66
    Peer original destination IP address  -
  Filters
    Local IP address ................... 172.28.40.41
    Local IP address mask .............. 255.255.255.255
    Remote IP address .................. 172.16.2.66
    Remote IP address mask ............. 255.255.255.255
    Local port number .................. 1701
    Remote port number ................. 1701
    NAPT remote port number ............ 6
    Transport protocol ................. UDP
    Local Name ......................... ANY
    Remote Name ........................ ANY
  DF Bit ............................. CLEAR
  Last sent sequence number ........... 21
  Anti-replay checking enabled ........ FALSE
  Debug device ....................... 16
  Filter debug flags ................. 00000000
  Packet debug flags ................. 00000000
  Trace debug flags .................. 00000000
  Packet debug length ................ 72
```

show isakmp sa

```
                                    Expiry Limits - hard/soft/used
SA Id PeerAddress     EncA.  HashA. Bytes                Seconds
-----------------------------------------------------------------------
1     172.28.40.80    DES    SHA    -/-/-               86400/75593/23726
2     172.28.40.80    3DES   SHA    -/-/-               28800/25188/38
```

sh isakmp sa=2

```
SA Id ................................ 2
  Initiator Cookie .................... dbb80f0aa0abdfa1
  Responder Cookie .................... 3e39ebd4724db839
  DOI ................................. IPSEC
  Policy name ......................... windows_isakmp
  State ............................... ACTIVE
  Local address ....................... 172.28.40.41
  Remote Address ...................... 172.28.40.80
  Remote Port ......................... 48348
  Time of establishment ............... 18-May-2007:14:50:26
  Commit bit set ...................... FALSE
  Send notifies ....................... FALSE
  Send deletes ........................ FALSE
  Always send ID ...................... FALSE
  Message Retry Limit ................. 8
  Initial Message Retry Timeout (s) ... 4
  Message Back-off .................... Incremental
  Exchange Delete Delay (s) ........... 30
  Do Xauth ............................ FALSE
    Xauth Finished .................... TRUE
  Expiry Limit (bytes) ................ -
  Soft Expiry Limit (bytes) ........... -
  Bytes seen .......................... -
  Expiry Limit (seconds) .............. 28800
  Soft Expiry Limit (seconds) ......... 25188
  Seconds since creation .............. 42
  Number of Phase 2 exchanges allowed . 4294967294
  Number of acquires queued ........... 0
```

continued on next page

continued from previous page

```
Sa Definition Information:
  Authentication Type ................. PRESHARED
  Encryption Algorithm ................ 3DES - 168 bit - outer CBC
  Hash Algorithm ...................... SHA
  group Type .......................... MODP
  group Description ................... MODP1024
  DH Private Exponent Bits ............ 160
  expiry seconds ...................... 28800
  expiry kilobytes .................... -

XAuth Information:
  Id .................................. 0
  Next Message ........................ UNKNOWN
  Status .............................. FAIL
  Type ................................ Generic
  Max Failed Attempts.................. 0
  Failed Attempts...................... 0

NAT-Traversal Information:
  NAT-T enabled ....................... YES
  Peer NAT-T capable .................. YES (rfc)
  NAT discovered ...................... REMOTE

Heartbeat Information:
  Send Heartbeats ..................... NO
  Next sequence number tx ............. 1
  Receive Heartbeats .................. NO
  Last sequence number rx ............. 0
```

An XP client initiates a tunnel

This section contains the following:

- "ISAKMP debug output on the head office router" on page 65
- "IPSec and ISAKMP SAs on the head office router" on page 78

ISAKMP debug output on the head office router

The following debug is the output from the command **enable isakmp debug=all** captured on the Head Office router.

```
SecOff Head Office> ISAKMP Network Rx:
     remotePort=54351 localPort=500
     a9 18 5a ba 7f 5c 85 99 00 00 00 00 00 00 00 00 01 10 02 00
     00 00 00 00 00 00 01 38 0d 00 00 c8 00 00 00 01 00 00 00 01
     00 00 00 bc 01 01 00 05 03 00 00 24 01 01 00 00 80 01 00 05
     80 02 00 02 80 04 00 0e 80 03 00 01 80 0b 00 01 00 0c 00 04
     00 00 70 80 03 00 00 24 02 01 00 00 80 01 00 05 80 02 00 02
     80 04 00 02 80 03 00 01 80 0b 00 01 00 0c 00 04 00 00 70 80
     03 00 00 24 03 01 00 00 80 01 00 05 80 02 00 01 80 04 00 02
     80 03 00 01 80 0b 00 01 00 0c 00 04 00 00 70 80 03 00 00 24
     04 01 00 00 80 01 00 01 80 02 00 02 80 04 00 01 80 03 00 01
     80 0b 00 01 00 0c 00 04 00 00 70 80 00 00 00 24 05 01 00 00
     80 01 00 01 80 02 00 01 80 04 00 01 80 03 00 01 80 0b 00 01
     00 0c 00 04 00 00 70 80 0d 00 00 18 1e 2b 51 69 05 99 1c 7d
     7c 96 fc bf b5 87 e4 61 00 00 00 04 0d 00 00 14 40 48 b7 d5
     6e bc e8 85 25 e7 de 7f 00 d6 c2 d3 0d 00 00 14 90 cb 80 91
     3e bb 69 6e 08 63 81 b5 ec 42 7b 1f 00 00 00 14 26 24 4d 38
     ed db 61 b3 17 2a 36 e3 d0 cf b8 19
ISAKMP MAIN exchange 23: New State: IDLE

ISAKMP MAIN: RESP: xchg 23: Started with peer 172.28.40.80
ISAKMP Rx Message
     Cookies:   a9185aba7f5c8599:0000000000000000
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 312
     Payload #:  0  Length: 200  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 5  SPI:
           Transform#: 1
             Transform Id ................... IKE(1)
             Encryption Algorithm........... 3DESOUTER(5)
             Authentication Algorithm....... SHA(2)
             Authentication Method.......... PRESHARED(1)
             Group Description.............. UNKNOWN(14)
             Group Type..................... MODP
             Expiry Seconds................. 28800
```

```
        Transform#: 2
                    Transform Id ................... IKE(1)
                    Encryption Algorithm........... 3DESOUTER(5)
                    Authentication Algorithm....... SHA(2)
                    Authentication Method.......... PRESHARED(1)
                    Group Description.............. 1024(2)
                    Group Type..................... MODP
                    Expiry Seconds................. 28800
                  Transform#: 3
                    Transform Id ................... IKE(1)
                    Encryption Algorithm........... 3DESOUTER(5)
                    Authentication Algorithm....... MD5(1)
                    Authentication Method.......... PRESHARED(1)
                    Group Description.............. 1024(2)
                    Group Type..................... MODP
                    Expiry Seconds................. 28800
                  Transform#: 4
                    Transform Id ................... IKE(1)
                    Encryption Algorithm........... DES(1)
                    Authentication Algorithm....... SHA(2)
                    Authentication Method.......... PRESHARED(1)
                    Group Description.............. 768(1)
                    Group Type..................... MODP
                    Expiry Seconds................. 28800
                  Transform#: 5
                    Transform Id ................... IKE(1)
                    Encryption Algorithm........... DES(1)
                    Authentication Algorithm....... MD5(1)
                    Authentication Method.......... PRESHARED(1)
                    Group Description.............. 768(1)
                    Group Type..................... MODP
                    Expiry Seconds................. 28800
          Payload #:  1  Length: 24  Type: Vendor ID (VID)
            string=UNKNOWN
            1e 2b 51 69 05 99 1c 7d 7c 96 fc bf b5 87 e4 61 00 00 00 04
          Payload #:  2  Length: 20  Type: Vendor ID (VID)
            string=Microsoft L2TP/IPsec VPN Client
            40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
          Payload #:  3  Length: 20  Type: Vendor ID (VID)
            string=draft-ietf-ipsec-nat-t-ike-02\n
            90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
          Payload #:  4  Length: 20  Type: Vendor ID (VID)
            string=UNKNOWN
            26 24 4d 38 ed db 61 b3 17 2a 36 e3 d0 cf b8 19
        ISAKMP MAIN: RESP: xchg 23: Rx NAT-T version 2 vendor ID
        ISAKMP MAIN exchange 23: New State: SARECV

        ISAKMP DOI: IPSEC: Compare transform fail: encAlg l=DES(1) r=3DESOUTER(5)
        ISAKMP DOI: IPSEC: Compare transform fail: encAlg l=DES(1) r=3DESOUTER(5)
        ISAKMP DOI: IPSEC: Compare transform fail: encAlg l=DES(1) r=3DESOUTER(5)
```

```
ISAKMP MAIN: RESP: xchg 23: Found matching policy = office
ISAKMP Tx Message
     Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 180
     Payload #:  0  Length: 52  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 1  SPI:
           Transform#: 4
             Transform Id ................... IKE(1)
             Encryption Algorithm........... DES(1)
             Authentication Algorithm....... SHA(2)
             Authentication Method.......... PRESHARED(1)
             Group Description.............. 768(1)
             Group Type..................... MODP
             Expiry Seconds................. 28800
     Payload #:  1  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-02\n
       90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     Payload #:  2  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-02 (no \n)
       cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
     Payload #:  3  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-03
       7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
     Payload #:  4  Length: 20  Type: Vendor ID (VID)
       string=draft-ietf-ipsec-nat-t-ike-08
       8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4 28 c1 1d e8
     Payload #:  5  Length: 20  Type: Vendor ID (VID)
       string=NAT-T RFC3947
       4a 13 1c 81 07 03 58 45 5c 57 28 f2 0e 95 45 2f
ISAKMP Tx Unencrypted
ISAKMP Network Tx:
     localPort=500 remotePort=54351
     a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 01 10 02 00
     00 00 00 00 00 00 00 b4 0d 00 00 34 00 00 00 01 00 00 00 01
     00 00 00 28 01 01 00 01 00 00 00 20 04 01 00 00 80 01 00 01
     80 02 00 02 80 03 00 01 80 04 00 01 80 0b 00 01 80 0c 70 80
     0d 00 00 14 90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     0d 00 00 14 cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
     0d 00 00 14 7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
     0d 00 00 14 8f 8d 83 82 6d 24 6b 6f c7 a8 a6 a4 28 c1 1d e8
     00 00 00 14 4a 13 1c 81 07 03 58 45 5c 57 28 f2 0e 95 45 2f

ISAKMP MAIN exchange 23: New State: SASENT

ISAKMP Network Rx:
     remotePort=54351 localPort=500
     a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 04 10 02 00
     00 00 00 00 00 00 00 c8 0a 00 00 64 c6 a5 a7 9d 7b 49 90 bf
```

```
        c0 a7 5f da 9f 59 5d f8 76 d3 d5 bf 0f 0f bb 13 b3 3a ff bb
        35 6d 33 f1 95 bc d6 8a 33 6e 5d 41 69 50 e1 35 b1 fc 28 c4
        41 d4 06 b1 a6 f7 97 b6 52 ed 9e 3a ba 18 79 59 8c d3 c6 52
        8c a4 7c 9d a0 14 33 f5 ee 7f 48 20 8e bb 45 c7 ed 88 87 8d
        a4 5b 92 4d 5e fb 53 de 82 00 00 18 46 bb 7f 2f 15 61 68 f6
        16 8c 81 be 18 0f 71 99 30 f0 78 5b 82 00 00 18 ff ea dc f1
        90 c0 fd 84 c5 69 4c 4b f8 1b 23 75 f7 b1 e7 7a 00 00 00 18
        ef 1b 3e 9a ec ca a5 b3 94 7e 75 4f 3c 0e d0 57 c4 ba 5c b9

ISAKMP Rx Message
        Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
        Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
        MessageID:  00000000   Total Length: 200
        Payload #:  0  Length: 100  Type: Key Exchange (KE)
          c6 a5 a7 9d 7b 49 90 bf c0 a7 5f da 9f 59 5d f8 76 d3 d5 bf
          0f 0f bb 13 b3 3a ff bb 35 6d 33 f1 95 bc d6 8a 33 6e 5d 41
          69 50 e1 35 b1 fc 28 c4 41 d4 06 b1 a6 f7 97 b6 52 ed 9e 3a
          ba 18 79 59 8c d3 c6 52 8c a4 7c 9d a0 14 33 f5 ee 7f 48 20
          8e bb 45 c7 ed 88 87 8d a4 5b 92 4d 5e fb 53 de
        Payload #:  1  Length: 24  Type: Nonce (NONCE)
          46 bb 7f 2f 15 61 68 f6 16 8c 81 be 18 0f 71 99 30 f0 78 5b
        Payload #:  2  Length: 24  Type: NAT-T(v2) Discovery (NAT-D)
          ff ea dc f1 90 c0 fd 84 c5 69 4c 4b f8 1b 23 75 f7 b1 e7 7a
        Payload #:  3  Length: 24  Type: NAT-T(v2) Discovery (NAT-D)
          ef 1b 3e 9a ec ca a5 b3 94 7e 75 4f 3c 0e d0 57 c4 ba 5c b9
ISAKMP MAIN: RESP: xchg 23: NAT-D detected a remote NAT
ISAKMP MAIN exchange 23: New State: KERECV

ISAKMP MAIN: RESP: xchg 23: x l=20 v=6b07794d8c0d84e0e87ce57af806faba5de578f3
ISAKMP MAIN: RESP: xchg 23: g^x l=96
   v=c6a5a79d7b4990bfc0a75fda9f595df876d3d5bfe
ISAKMP MAIN: RESP: xchg 23: g^y l=96
   v=cfc22e62592574f1b2e334b72d0f3336f48d6b8bb
ISAKMP MAIN: RESP: xchg 23: g^xy l=96
   v=d7bf531b4979f29b81810e3047646c73a464e63c
ISAKMP MAIN: RESP: xchg 23: Ni l=20 v=46bb7f2f156168f6168c81be180f719930f0785b
ISAKMP MAIN: RESP: xchg 23: Nr l=20 v=18c4aba924ac22a9ab9e5d935cec29e9e40a9038
ISAKMP MAIN: RESP: xchg 23: COOKIE_I l=8 v=a9185aba7f5c8599
ISAKMP MAIN: RESP: xchg 23: COOKIE_R l=8 v=7d74dae5cbf5eb8b
ISAKMP MAIN: RESP: xchg 23: Key l=6 v=667269656e64
ISAKMP MAIN: RESP: xchg 23: SKEYID l=20
   v=bcfd7c1560b1b37b6a4710ae27fecda3eb789f
ISAKMP MAIN: RESP: xchg 23: SKEYID_d l=20
   v=c09ac3f458dd80fb98cbe2a5ec153cadf902
ISAKMP MAIN: RESP: xchg 23: SKEYID_a l=20
   v=8e87975b9af188caa871641eb2132c93a1f8
ISAKMP MAIN: RESP: xchg 23: SKEYID_e l=20
   v=920453255ef072890ce1afdb60341f88c8bc
ISAKMP MAIN: RESP: xchg 23: EncKey l=8 v=920453255ef07289
ISAKMP MAIN: RESP: xchg 23: IV l=8 v=206c8f57acb474c9
```

```
ISAKMP Tx Message
     Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 200
     Payload #:  0  Length: 100  Type: Key Exchange (KE)
       cf c2 2e 62 59 25 74 f1 b2 e3 34 b7 2d 0f 33 36 f4 8d 6b 8b
       b7 5f 0e f5 e6 b3 14 68 c3 13 2e 5f c4 4c c4 c6 fb 8f ca d4
       f3 14 24 b1 89 2d db 24 7e 68 0c c5 35 74 93 12 c9 4a aa c2
       e7 eb 21 d2 03 eb 79 9a 57 bb c3 66 9c 8a 98 d6 d1 bf e8 13
       f5 23 25 2a 74 55 6f 13 99 47 f0 52 66 ec 36 4b
     Payload #:  1  Length: 24  Type: Nonce (NONCE)
       18 c4 ab a9 24 ac 22 a9 ab 9e 5d 93 5c ec 29 e9 e4 0a 90 38
     Payload #:  2  Length: 24  Type: NAT-T(v2) Discovery (NAT-D)
       e7 5b 40 95 b1 36 0c 2b 0e d8 0d 14 58 74 35 60 1b 22 3c 82
     Payload #:  3  Length: 24  Type: NAT-T(v2) Discovery (NAT-D)
       ff ea dc f1 90 c0 fd 84 c5 69 4c 4b f8 1b 23 75 f7 b1 e7 7a
ISAKMP Tx Unencrypted
ISAKMP Network Tx:
     localPort=500 remotePort=54351
     a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 04 10 02 00
     00 00 00 00 00 00 00 c8 0a 00 00 64 cf c2 2e 62 59 25 74 f1
     b2 e3 34 b7 2d 0f 33 36 f4 8d 6b 8b b7 5f 0e f5 e6 b3 14 68
     c3 13 2e 5f c4 4c c4 c6 fb 8f ca d4 f3 14 24 b1 89 2d db 24
     7e 68 0c c5 35 74 93 12 c9 4a aa c2 e7 eb 21 d2 03 eb 79 9a
     57 bb c3 66 9c 8a 98 d6 d1 bf e8 13 f5 23 25 2a 74 55 6f 13
     99 47 f0 52 66 ec 36 4b 82 00 00 18 18 c4 ab a9 24 ac 22 a9
     ab 9e 5d 93 5c ec 29 e9 e4 0a 90 38 82 00 00 18 e7 5b 40 95
     b1 36 0c 2b 0e d8 0d 14 58 74 35 60 1b 22 3c 82 00 00 00 18
     ff ea dc f1 90 c0 fd 84 c5 69 4c 4b f8 1b 23 75 f7 b1 e7 7a

ISAKMP MAIN exchange 23: New State: KESENT

ISAKMP Network Rx:
     remotePort=58248 localPort=4500
     00 00 00 00 a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b
     05 10 02 01 00 00 00 00 00 00 00 44 65 80 82 be 9c 7f 1d 8f
     e9 3b 2f 01 66 45 ce 84 6e c8 6c be 52 5f f5 e6 bd e6 c6 34
     fa 68 b0 89 61 75 10 4b 50 00 e2 6b
ISAKMP Network Rx: Removed Non-ESP Marker.
ISAKMP Rx (decrypted)<---
a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 05 10 02 01
00 00 00 00 00 00 00 44 08 00 00 0d 02 00 00 00 73 6c 69 6d
79 00 00 00 18 77 36 af cf 95 30 d1 b4 26 77 57 1d 5c 65 c3
74 99 42 de 5c 00 00 00
```

```
ISAKMP Rx Message (decrypted)
     Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 01
     MessageID:  00000000   Total Length: 65
     Payload #:  0  Length: 13  Type: Identification (ID)
       Type: FQDN  ProtocolId: 0  Port: 0
       Value: slimy
     Payload #:  1  Length: 24  Type: Hash (HASH)
       77 36 af cf 95 30 d1 b4 26 77 57 1d 5c 65 c3 74 99 42 de 5c
ISAKMP CORE: Info: exchange 23 local port changed from 500 to 4500

ISAKMP CORE: Info: exchange 23 remote port changed from 54351 to 58248

ISAKMP MAIN exchange 23: New State: AUTHRECV

ISAKMP MAIN: RESP: xchg 23: RemoteID=FQDN:slimy OR :: for NAT-T
ISAKMP MAIN: RESP: xchg 23: Hi l=20 v=7736afcf9530d1b42677571d5c65c3749942de5c
ISAKMP MAIN: RESP: xchg 23: Hr l=20 v=85fc260ab49cf7bd05e791aac1b272c3449a5288
ISAKMP Encrypt:
a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 05 10 02 00
00 00 00 00 00 00 00 40 08 00 00 0c 01 00 00 00 ac 1c 28 29
00 00 00 18 85 fc 26 0a b4 9c f7 bd 05 e7 91 aa c1 b2 72 c3
44 9a 52 88
ISAKMP Tx Message
     Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
     Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
     MessageID:  00000000   Total Length: 64
     Payload #:  0  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 0  Port: 0
       Value: 172.28.40.41
     Payload #:  1  Length: 24  Type: Hash (HASH)
       85 fc 26 0a b4 9c f7 bd 05 e7 91 aa c1 b2 72 c3 44 9a 52 88
ISAKMP Tx Encrypted
ISAKMP Network Tx:
     localPort=4500 remotePort=58248
     00 00 00 00 a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b
     05 10 02 01 00 00 00 00 00 00 00 44 5c de f7 b9 7c eb 85 39
     35 67 3f 45 f4 19 1c 50 83 2a 05 2a 2b 6d ed 89 fb 2f 0f a9
     cd e4 96 91 4e 3b 84 ba 8b be 2b 48
ISAKMP MAIN exchange 23: New State: AUTHSENT

ISAKMP MAIN exchange 23: New State: UP

ISAKMP CORE: Exchange 23 done

ISAKMP Network Rx:
     remotePort=58248 localPort=4500
     00 00 00 00 a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b
     08 10 20 01 66 e9 36 20 00 00 01 7c 1e b4 26 86 61 38 7f ea
     2c 0c a3 fb 21 85 37 df d1 f5 03 22 64 e5 b1 2f bb b9 0c 34
```

```
        f5 10 7f 1a 04 33 45 3c 38 49 d3 19 0f 2d e8 c0 71 bc 0b 43
        5a 34 28 5d d0 f4 04 bb cc 34 3d e7 6b 79 d2 40 00 88 02 4c
        64 70 bc 4e 16 2b 46 9d a2 00 4d 12 1a 17 08 d6 ba 4e 65 cd
        f9 3a 23 96 fd 55 64 84 55 1e b2 0e 86 0f ed 3b 06 16 b2 e8
        c7 4b 7a 46 cd 8d c4 0e 99 b3 ca ea 8d 8c 7d b1 06 77 1b 0a
        81 00 f1 f0 e0 ae be 07 7a 9c 0b da 27 fe 25 68 dd 28 45 83
        8d 72 f5 20 e0 19 4c 55 e5 64 18 4f 2e ee f4 d9 75 07 6c 25
        35 b9 d4 50 60 1d 07 d7 93 6c 09 e4 10 97 6e f2 54 2b 77 e3
        5a 82 87 ea 81 d7 58 54 a4 3b 32 92 2b 18 13 2f 8b 21 12 b6
        2c b1 74 dd 66 11 35 e2 45 92 a9 ab a5 a7 c5 ee fe 1a e0 44
        78 bf 4b 66 7c 1b fc 9c fa 9d c0 8e f3 dd 76 20 03 7b 50 cd
        49 6a 48 54 3d 19 75 9d be 58 bd d8 8c 54 bf 3b 55 40 b6 6c
        64 ed 21 51 41 1d 9e f5 c0 39 d5 d6 e3 e9 00 7d a4 29 82 ba
        78 de 9c d8 83 a2 f6 62 1f 67 d9 93 d9 b0 4f d1 16 50 ac 9d
        07 ca e8 b0 f4 62 ec 9d bf 52 58 fc 9f d0 65 3d 8d e5 5b a3
        5e 8c 03 c0 8c 82 44 8e d9 50 d6 f5 30 04 bf b4 37 a6 55 30
        98 74 21 3b
ISAKMP Network Rx: Removed Non-ESP Marker.

ISAKMP QUICK: RESP: xchg 24: Started with peer 172.28.40.80
ISAKMP QUICK exchange 24: New State: WAIT_HASH_SA_NONCE
ISAKMP QUICK: RESP: xchg 24: COOKIE_I l=8 v=a9185aba7f5c8599
ISAKMP QUICK: RESP: xchg 24: COOKIE_R l=8 v=7d74dae5cbf5eb8b
ISAKMP QUICK: RESP: xchg 24: MessageID=66e93620
ISAKMP QUICK: RESP: xchg 24: IV l=8 v=ec0a6b64a3d306cd
ISAKMP Rx (decrypted)<---
a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 08 10 20 01
66 e9 36 20 00 00 01 7c 01 00 00 18 fc fe a0 fa f2 c8 c1 81
92 bb 6e 70 c3 26 78 3e 5e 44 5a e5 0a 00 01 08 00 00 00 01
00 00 00 01 00 00 00 fc 01 03 04 06 74 43 a8 90 03 00 00 28
01 03 00 00 80 01 00 01 00 02 00 04 00 00 0e 10 80 01 00 02
00 02 00 04 00 03 d0 90 80 04 f0 04 80 05 00 01 03 00 00 28
02 03 00 00 80 01 00 01 00 02 00 04 00 00 0e 10 80 01 00 02
00 02 00 04 00 03 d0 90 80 04 f0 04 80 05 00 02 03 00 00 28
03 02 00 00 80 01 00 01 00 02 00 04 00 00 0e 10 80 01 00 02
00 02 00 04 00 03 d0 90 80 04 f0 04 80 05 00 01 03 00 00 28
04 02 00 00 80 01 00 01 00 02 00 04 00 00 0e 10 80 01 00 02
00 02 00 04 00 03 d0 90 80 04 f0 04 80 05 00 02 03 00 00 28
05 0b 00 00 80 01 00 01 00 02 00 04 00 00 0e 10 80 01 00 02
00 02 00 04 00 03 d0 90 80 04 f0 04 80 05 00 02 00 00 00 28
06 0b 00 00 80 01 00 01 00 02 00 04 00 00 0e 10 80 01 00 02
00 02 00 04 00 03 d0 90 80 04 f0 04 80 05 00 01 05 00 00 18
40 4d b6 b7 0b 41 e3 a5 7c 62 4a d1 b1 30 93 96 60 fb 82 38
05 00 00 0d 02 11 06 a5 73 6c 69 6d 79 83 00 00 0c 01 11 06
a5 ac 1c 28 29 00 00 00 0c 01 00 00 00 ac 10 02 43 00 00 00
```

```
ISAKMP Rx Message (decrypted)
     Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 01
     MessageID:  66e93620   Total Length: 377
     Payload #:  0  Length: 24  Type: Hash (HASH)
       fc fe a0 fa f2 c8 c1 81 92 bb 6e 70 c3 26 78 3e 5e 44 5a e5
     Payload #:  1  Length: 264  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ESP(3)  #Trans: 6  SPI: 7443a890
           Transform#: 1
             Transform Id ................... 3DESOUTER(3)
             Group Description .............. MODP768(1)
             Encapsulation Mode ............. UDP_ENCAP_TRANSPORT(v2)(61444)
             Authentication Algorithm ...... MD5(1)
             Expiry KBytes ................. 250000
             Expiry Seconds ................ 3600
           Transform#: 2
             Transform Id ................... 3DESOUTER(3)
             Group Description .............. MODP768(1)
             Encapsulation Mode ............. UDP_ENCAP_TRANSPORT(v2)(61444)
             Authentication Algorithm ...... SHA(2)
             Expiry KBytes ................. 250000
             Expiry Seconds ................ 3600
           Transform#: 3
             Transform Id ................... DES(2)
             Group Description .............. MODP768(1)
             Encapsulation Mode ............. UDP_ENCAP_TRANSPORT(v2)(61444)
             Authentication Algorithm ...... MD5(1)
             Expiry KBytes ................. 250000
             Expiry Seconds ................ 3600
           Transform#: 4
             Transform Id ................... DES(2)
             Group Description .............. MODP768(1)
             Encapsulation Mode ............. UDP_ENCAP_TRANSPORT(v2)(61444)
             Authentication Algorithm ...... SHA(2)
             Expiry KBytes ................. 250000
             Expiry Seconds ................ 3600
           Transform#: 5
             Transform Id ................... NULL(11)
             Group Description .............. MODP768(1)
             Encapsulation Mode ............. UDP_ENCAP_TRANSPORT(v2)(61444)
             Authentication Algorithm ...... SHA(2)
             Expiry KBytes ................. 250000
             Expiry Seconds ................ 3600
```

```
                Transform#: 6
                  Transform Id ................... NULL(11)
                  Group Description ............. MODP768(1)
                  Encapsulation Mode ............ UDP_ENCAP_TRANSPORT(v2)(61444)
                  Authentication Algorithm ...... MD5(1)
                  Expiry KBytes ................. 250000
                  Expiry Seconds ................ 3600
        Payload #:  2  Length: 24  Type: Nonce (NONCE)
          40 4d b6 b7 0b 41 e3 a5 7c 62 4a d1 b1 30 93 96 60 fb 82 38
        Payload #:  3  Length: 13  Type: Identification (ID)
          Type: FQDN  ProtocolId: 17  Port: 1701
          Value: slimy
        Payload #:  4  Length: 12  Type: Identification (ID)
          Type: IPV4_ADDR  ProtocolId: 17  Port: 1701
          Value: 172.28.40.41
        Payload #:  5  Length: 12  Type: NAT-T(v2) Original Address (NAT-OA)
          ID Type=IPv4 IP=172.16.2.67

ISAKMP QUICK: RESP: xchg 24: rx msg 1: start
ISAKMP QUICK exchange 24: New State: RECEIVING_MESSAGE
ISAKMP QUICK: RESP: xchg 24: rx msg 1: rec PROP 0: # 1, protid 3, outspi 7443a8
ISAKMP QUICK: RESP: xchg 24: rx msg 1: PROP 0 transforms good
ISAKMP QUICK: RESP: xchg 24: rx msg 1: SA proposals good
ISAKMP QUICK: RESP: xchg 24: rx msg 1: payloads good:
ISAKMP QUICK: RESP: xchg 24: rx msg 1: good

ISAKMP QR 24: HASH1: 014578d4 329
66e936200a000108000000010000000001000000fc010304067443a89003000028
0103000080010001000200040000e1080010002000200040003d0908004f004
8005000103000028020300008001000100020004000000e108001000200020004
0003d0908004f00480050002030000280302000080010001000200040000e10


ISAKMP QR 24: HASH1: result fcfea0faf2c8c18192bb6e70c326783e5e445ae5

ISAKMP DOI: IPSEC: resp match pol:
   peerIP=172.28.40.80
   filtEnableFlag=00000171
   filtOpaqueFlag=00000000
   selectorsFromPktFlag=00000000
   lAddr=172.28.40.41
   lMask=255.255.255.255
   lAddrLow=0.0.0.0
   lAddrHigh=0.0.0.0
   rAddr=0.0.0.0
   rMask=255.255.255.255
   rAddrLow=0.0.0.0
   rAddrHigh=0.0.0.0
   lPort=1701
   rPort=1701
```

```
   lName=
   rName=slimy
   lAddrVer=4
   rAddrVer=4
ISAKMP DOI: IPSEC: Aquire Info -> Local Policy
  number of proposals 1
  proposal 0: # 1, protId 3, #transforms 4
    transform 0: # 1, id 3, sas 1
                 expiry: b 0-4294967295, s 0-28800
                 gr 1, mode 2, auth 2, keylen 0
    transform 0: # 2, id 3, sas 2
                 expiry: b 0-4294967295, s 0-28800
                 gr 1, mode 2, auth 1, keylen 0
    transform 0: # 3, id 2, sas 3
                 expiry: b 0-4294967295, s 0-28800
                 gr 1, mode 2, auth 2, keylen 0
    transform 0: # 4, id 2, sas 4
                 expiry: b 0-4294967295, s 0-28800
                 gr 1, mode 2, auth 1, keylen 0
ISAKMP QUICK: RESP: xchg 24: Match Pol: 2 Local (prot 1) found - 0
ISAKMP QUICK: RESP: xchg 24: Match Pol: 2 Remote (prot 1) found - 0
ISAKMP QUICK: RESP: xchg 24: Match Pol: prop match try: 1
   00000000000000001457c
ISAKMP QUICK: RESP: xchg 24: Match Pol: matching (prot 2) props 1
ISAKMP QUICK: RESP: xchg 24: Match Pol: (prot 2) tran match try: loc 0 - rem 0
ISAKMP DOI: IPSEC: ATTR match fail: authAlg 2 1
ISAKMP QUICK: RESP: xchg 24: Match Tran: match fail
ISAKMP QUICK: RESP: xchg 24: Match Pol: (prot 2) tran match try: loc 0 - rem 1
ISAKMP QUICK: RESP: xchg 24: Match Tran: match good
ISAKMP QUICK: RESP: xchg 24: Match Pol: matched
ISAKMP QUICK: RESP: xchg 24: proc 1: done good

ISAKMP QI 24: HASH INK1: 0145b9d4 45
03f05d087f404db6b70b41e3a57c624ad1b130939660fb823859c56af9ea23b5
82b53959f8eabe471d397e1b19

ISAKMP QI 24: HASH INK1: result 33ed6f75bcc651aba6479149fd94e0f8800414b4

ISAKMP QI 24: HASH OUTK1: 0145b9d4 45
037443a890404db6b70b41e3a57c624ad1b130939660fb823859c56af9ea23b5
82b53959f8eabe471d397e1b19

ISAKMP QI 24: HASH OUTK1: result b9a9b7493554497412a9055a29b931013d2d3740

ISAKMP QI 24: HASH INK2: 0145b9c0 65
33ed6f75bcc651aba6479149fd94e0f8800414b403f05d087f404db6b70b41e3
a57c624ad1b130939660fb823859c56af9ea23b582b53959f8eabe471d397e1b
19

ISAKMP QI 24: HASH INK2: result 2252400e179200a597197752e65ba69eba335c4f
```

```
ISAKMP QI 24: HASH OUTK2: 0145b9c0 65
b9a9b7493554497412a9055a29b931013d2d3740037443a890404db6b70b41e3
a57c624ad1b130939660fb823859c56af9ea23b582b53959f8eabe471d397e1b
19

ISAKMP QI 24: HASH INK3: 0145b9c0 65
2252400e179200a597197752e65ba69eba335c4f03f05d087f404db6b70b41e3
a57c624ad1b130939660fb823859c56af9ea23b582b53959f8eabe471d397e1b
19

ISAKMP QI 24: HASH INK3: result 7859356abba96501ee79af407817e85c65110e1a

ISAKMP QI 24: HASH OUTK3: 0145b9c0 65
cdda73d44dbae1340877245a152b47d3e7dfbdd7037443a890404db6b70b41e3
a57c624ad1b130939660fb823859c56af9ea23b582b53959f8eabe471d397e1b
19

ISAKMP QI 24: HASH OUTK3: result e706a3e4a458fd9c3131b1d48410957a14fe2965

ISAKMP QUICK exchange 24: New State: SENDING_HASH_SA_NONCE
ISAKMP DOI: IPSEC: Exchange IDs not default:
  initiatorAddress      172.28.40.80
  IDi: type             FQDN
       protocol Id      17
       port             1701
       data             736c696d79
  responderAddress      172.28.40.41
  IDr: type             IPV4_ADDR
       protocol Id      17
       port             1701
       data             ac1c2829

ISAKMP QR 24: HASH1: ID Payload Created

ISAKMP QR 24: HASH2: 0145ca14 149
66e93620404db6b70b41e3a57c624ad1b130939660fb82380a00004000000001
0000000100000034010304 01f05d087f0000002802030000800100010002000 4
00000e10800100020002000400 03d0908004f0048005000205000018 59c56af9
ea23b582b53959f8eabe471d397e1b190500000d021106a5736c696d79830000


ISAKMP QR 24: HASH2: result fa1b4f8ed7adc97176000ca5bb3058b2fb33c7ca
ISAKMP Encrypt:
a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 08 10 20 00
66 e9 36 20 00 00 00 b1 01 00 00 18 fa 1b 4f 8e d7 ad c9 71
76 00 0c a5 bb 30 58 b2 fb 33 c7 ca 0a 00 00 40 00 00 00 01
00 00 00 01 00 00 00 34 01 03 04 01 f0 5d 08 7f 00 00 00 28
02 03 00 00 80 01 00 01 00 02 00 04 00 00 0e 10 80 01 00 02
00 02 00 04 00 03 d0 90 80 04 f0 04 80 05 00 02 05 00 00 18
```

```
59 c5 6a f9 ea 23 b5 82 b5 39 59 f8 ea be 47 1d 39 7e 1b 19
05 00 00 0d 02 11 06 a5 73 6c 69 6d 79 83 00 00 0c 01 11 06
a5 ac 1c 28 29 00 00 00 0c 01 00 00 00 ac 1c 28 29
ISAKMP Tx Message
     Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 00
     MessageID:  66e93620   Total Length: 177
     Payload #:  0  Length: 24  Type: Hash (HASH)
       fa 1b 4f 8e d7 ad c9 71 76 00 0c a5 bb 30 58 b2 fb 33 c7 ca
     Payload #:  1  Length: 64  Type: Security Association (SA)
       DOI: IPSEC(0)  Situation: 00000001
         Proposal#: 1  Protocol: ESP(3)  #Trans: 1  SPI: f05d087f
           Transform#: 2
             Transform Id ................. 3DESOUTER(3)
             Group Description ............ MODP768(1)
             Encapsulation Mode ........... UDP_ENCAP_TRANSPORT(v2)(61444)
             Authentication Algorithm ...... SHA(2)
             Expiry KBytes ................ 250000
             Expiry Seconds ............... 3600
     Payload #:  2  Length: 24  Type: Nonce (NONCE)
       59 c5 6a f9 ea 23 b5 82 b5 39 59 f8 ea be 47 1d 39 7e 1b 19
     Payload #:  3  Length: 13  Type: Identification (ID)
       Type: FQDN  ProtocolId: 17  Port: 1701
       Value: slimy
     Payload #:  4  Length: 12  Type: Identification (ID)
       Type: IPV4_ADDR  ProtocolId: 17  Port: 1701
       Value: 172.28.40.41
     Payload #:  5  Length: 12  Type: NAT-T(v2) Original Address (NAT-OA)
       ID Type=IPv4 IP=172.28.40.41
ISAKMP Tx Encrypted
ISAKMP Network Tx:
     localPort=4500 remotePort=58248
     00 00 00 00 a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b
     08 10 20 01 66 e9 36 20 00 00 00 b4 e5 be 2c dc 7b 6b ba df
     03 6d 87 e5 ec 6e a5 a0 bb 6b 8e 07 93 f6 58 67 f1 33 39 56
     22 b6 8d 3b c4 7a 7c e8 9d 37 75 8d 4e 71 df ce 84 06 c4 e3
     d7 ee 54 62 ba a9 fa 7b 00 52 fe 90 a5 58 2f 73 c1 f2 21 0a
     98 e1 cd 94 37 e7 48 d9 03 20 6c e3 bf bb 82 57 3e f4 37 7d
     07 4d d4 79 5e b4 7e ea 89 aa 7b de 95 8d cc db 43 b1 15 63
     98 be 20 8c 40 01 a3 96 ab 60 57 1a 65 fd 34 69 e5 24 09 95
     cc 13 b8 04 07 8a c1 07 68 30 85 21 fd 78 d4 a9 f3 aa f1 66
     cb 6a f6 77
ISAKMP Network Rx:
     remotePort=58248 localPort=4500
     00 00 00 00 a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b
     08 10 20 01 66 e9 36 20 00 00 00 34 5f 4d f0 24 ff 80 8e 9e
     74 46 b2 37 89 ac fa 7d 23 5c 69 90 5c db b6 37
ISAKMP Network Rx: Removed Non-ESP Marker.
ISAKMP Rx (decrypted)<---
a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 08 10 20 01
```

```
66 e9 36 20 00 00 00 34 00 00 00 18 39 4b d7 b9 17 61 ff a4
6c 2c 12 93 74 57 5c 44 95 95 ae 95
ISAKMP Rx Message (decrypted)
     Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
     Xchg Type:  QUICK(32)  Ver: 10  Flags: 01
     MessageID:  66e93620   Total Length: 52
     Payload #:  0  Length: 24  Type: Hash (HASH)
       39 4b d7 b9 17 61 ff a4 6c 2c 12 93 74 57 5c 44 95 95 ae 95

ISAKMP QUICK: RESP: xchg 24: rx msg 1: start
ISAKMP QUICK exchange 24: New State: RECEIVING_MESSAGE
ISAKMP QUICK: RESP: xchg 24: rx msg 2: payloads good:
ISAKMP QUICK: RESP: xchg 24: rx msg 2: good

ISAKMP QR 24: HASH3: 01465434 45
0066e93620404db6b70b41e3a57c624ad1b130939660fb823859c56af9ea23b5
82b53959f8eabe471d397e1b19

ISAKMP QR 24: HASH3: result 394bd7b91761ffa46c2c129374575c449595ae95
ISAKMP CORE: Exchange 24 done

ISAKMP QUICK exchange 24: New State: DONE
```

IPSec and ISAKMP SAs on the head office router

This section shows the output of the commands **show ipsec sa** and **show isakmp sa** on the head office router. For each command, specifying the SA number gives much more detail.

show ipsec sa

```
SA Id  Policy                Bundle  State     Protocol    OutSPI       InSPI
-------------------------------------------------------------------------------
    5  office                   10  Valid     ESP     3793464965  2968634655
    6  windows_warriors          1  Valid     ESP     4219699788  3020707765
    7  windows_warriors          1  Valid     ESP     1950591120  4032628863
```

show ipsec sa=7

```
SA Id ................................ 7
  Policy ............................. windows_warriors
  Bundle ............................. 1
  SA Specification Used ............... 1
  State .............................. Valid
  Protocol ........................... ESP
  Role ............................... RESPONDER
  Mode ............................... UDP_ENCAP_TRANSPORT
  Outbound SPI ....................... 1950591120
  Inbound SPI ........................ 4032628863
  Encryption algorithm ............... 3DESOUTER
  Encryption ENCO channel............. 5
  Hash algorithm ..................... SHA
  Hash ENCO channel................... 6
  NAT-Traversal NAT-OA
    Peer original source IP address ..... 172.16.2.67
    Peer original destination IP address  -
  Filters
    Local IP address ................... 172.28.40.41
    Local IP address mask .............. 255.255.255.255
    Remote IP address .................. 172.28.40.80
    Remote IP address mask ............. 255.255.255.255
    Local port number .................. 1701
    Remote port number ................. 1701
    NAPT remote port number ............ 7
    Transport protocol ................. UDP
    Local Name ......................... ANY
    Remote Name ........................ slimy
  DF Bit ............................. CLEAR
  Last sent sequence number ........... 43
  Anti-replay checking enabled ........ FALSE
  Debug device ....................... 16
  Filter debug flags ................. 00000000
  Packet debug flags ................. 00000000
  Trace debug flags .................. 00000000
  Packet debug length ................ 72
```

show isakmp sa

```
                                    Expiry Limits - hard/soft/used
SA Id PeerAddress     EncA.  HashA. Bytes                Seconds
-----------------------------------------------------------------------
1     172.28.40.80    DES    SHA    -/-/-               86400/75593/23763
2     172.28.40.80    3DES   SHA    -/-/-               28800/25188/75
3     172.28.40.80    DES    SHA    -/-/-               28800/25186/18
```

show isakmp sa=3

```
SA Id ............................... 3
  Initiator Cookie .................. a9185aba7f5c8599
  Responder Cookie .................. 7d74dae5cbf5eb8b
  DOI ............................... IPSEC
  Policy name ....................... office
  State ............................. ACTIVE
  Local address ..................... 172.28.40.41
  Remote Address .................... 172.28.40.80
  Remote Port ....................... 58248
  Time of establishment ............. 18-May-2007:14:51:24
  Commit bit set .................... FALSE
  Send notifies ..................... FALSE
  Send deletes ...................... FALSE
  Always send ID .................... FALSE
  Message Retry Limit ............... 8
  Initial Message Retry Timeout (s) ... 4
  Message Back-off .................. Incremental
  Exchange Delete Delay (s) ......... 30
  Do Xauth .......................... FALSE
    Xauth Finished .................. TRUE
  Expiry Limit (bytes) .............. -
  Soft Expiry Limit (bytes) ......... -
  Bytes seen ........................ -
  Expiry Limit (seconds) ............ 28800
  Soft Expiry Limit (seconds) ....... 25186
  Seconds since creation ............ 20
  Number of Phase 2 exchanges allowed . 4294967294
  Number of acquires queued ......... 0
```

continued on next page

continued from previous page

```
Sa Definition Information:
  Authentication Type ................. PRESHARED
  Encryption Algorithm ................ DES - 56 bit
  Hash Algorithm ...................... SHA
  group Type .......................... MODP
  group Description ................... MODP768
  DH Private Exponent Bits ............ 160
  expiry seconds ...................... 28800
  expiry kilobytes .................... -

XAuth Information:
  Id .................................. 0
  Next Message ........................ UNKNOWN
  Status .............................. FAIL
  Type ................................ Generic
  Max Failed Attempts.................. 0
  Failed Attempts...................... 0

NAT-Traversal Information:
  NAT-T enabled ....................... YES
  Peer NAT-T capable .................. YES (v2)
  NAT discovered ...................... REMOTE

Heartbeat Information:
  Send Heartbeats ..................... NO
  Next sequence number tx ............. 1
  Receive Heartbeats .................. NO
  Last sequence number rx ............. 0
```

An XP client is disconnected

ISAKMP SA status and debug output on the head office router

show isakmp sa output before disconnection

```
                                    Expiry Limits - hard/soft/used
SA Id PeerAddress     EncA.  HashA. Bytes                Seconds
-------------------------------------------------------------------------
1     172.28.40.80    DES    SHA    -/-/-               86400/75593/23763
2     172.28.40.80    3DES   SHA    -/-/-               28800/25188/75
3     172.28.40.80    DES    SHA    -/-/-               28800/25186/18
```

show isakmp debug output after disconnection

```
SecOff Head Office> ISAKMP Network Rx:
     remotePort=58248 localPort=4500
     00 00 00 00 a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b
     08 10 05 01 99 4c 55 7d 00 00 00 44 85 ca 0c b8 21 81 58 fc
     57 cd ff 1b 2c 56 2b a7 f1 ac a5 b6 65 1b 46 04 14 4c 9e be
     7b 9c 08 d5 24 d1 cc b7 6b 81 b2 ce
ISAKMP Network Rx: Removed Non-ESP Marker.
ISAKMP Rx (decrypted)<---
a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 08 10 05 01
99 4c 55 7d 00 00 00 44 0c 00 00 18 4d dd dd 88 3d 4b 3f 2e
4f 6a 29 ac 02 65 1f 56 7e fc 23 6f 00 00 00 10 00 00 00 01
03 04 00 01 74 43 a8 90
ISAKMP Rx Message (decrypted)
     Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
     Xchg Type:  INFORMATIONAL(5)  Ver: 10  Flags: 01
     MessageID:  994c557d   Total Length: 68
     Payload #:  0  Length: 24  Type: Hash (HASH)
       4d dd dd 88 3d 4b 3f 2e 4f 6a 29 ac 02 65 1f 56 7e fc 23 6f
     Payload #:  1  Length: 16  Type: Delete (D)
       00 00 00 01 03 04 00 01 74 43 a8 90
ISAKMP CORE: Exchange 25 done

ISAKMP Network Rx:
     remotePort=58248 localPort=4500
     00 00 00 00 a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b
     08 10 05 01 58 6e ff d1 00 00 00 54 c0 48 80 2a ff 94 1d a2
     d4 80 6a 2b 75 3c 67 81 1f 9c b7 3d e2 ab 4a df 59 d7 0d bd
     87 3c 39 12 8b e8 00 1e 52 14 ef 3e 71 dd ec 71 53 fd 17 b0
     64 76 d5 0f f1 17 79 b2
ISAKMP Network Rx: Removed Non-ESP Marker.
```

```
ISAKMP Rx (decrypted)<---
a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b 08 10 05 01
58 6e ff d1 00 00 00 54 0c 00 00 18 43 93 8e 6d fd c3 61 cf
f5 57 53 c2 08 f9 de ec 4c 03 75 fa 00 00 00 1c 00 00 00 01
01 10 00 01 a9 18 5a ba 7f 5c 85 99 7d 74 da e5 cb f5 eb 8b
00 00 00 00
ISAKMP Rx Message (decrypted)
     Cookies:   a9185aba7f5c8599:7d74dae5cbf5eb8b
     Xchg Type:  INFORMATIONAL(5)  Ver: 10  Flags: 01
     MessageID:  586effd1   Total Length: 80
     Payload #:  0  Length: 24  Type: Hash (HASH)
       43 93 8e 6d fd c3 61 cf f5 57 53 c2 08 f9 de ec 4c 03 75 fa
     Payload #:  1  Length: 28  Type: Delete (D)
       00 00 00 01 01 10 00 01 a9 18 5a ba 7f 5c 85 99 7d 74 da e5
       cb f5 eb 8b
ISAKMP CORE: Exchange 26 done

ISAKMP CORE: Info: No active isakmp SA with D/N enabled found for 172.28.40.80
```

show isakmp sa output after disconnection

```
                                    Expiry Limits - hard/soft/used
SA Id PeerAddress     EncA.  HashA. Bytes                Seconds
-------------------------------------------------------------------------
1     172.28.40.80    DES    SHA    -/-/-               86400/75593/23792
2     172.28.40.80    3DES   SHA    -/-/-               28800/25188/104
```

A Vista client is disconnected

ISAKMP SA status and debug output on the head office router

show isakmp sa output before disconnection

```
                                    Expiry Limits - hard/soft/used
SA Id PeerAddress      EncA.  HashA. Bytes                 Seconds
-------------------------------------------------------------------------
1     172.28.40.80     DES    SHA    -/-/-                86400/75593/23792
2     172.28.40.80     3DES   SHA    -/-/-                28800/25188/104
```

show isakmp debug output after disconnection

```
SecOff Head Office> ISAKMP Network Rx:
     remotePort=48348 localPort=4500
     00 00 00 00 db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39
     08 10 05 01 76 36 d4 8f 00 00 00 4c 91 61 50 44 bd a6 dc 23
     1d be 62 fb fd f7 75 cf 80 f0 3e b1 39 74 b2 fb ca 18 51 8c
     89 55 2a e9 5f cb 29 ad 9b 4b 3a da a7 dc 3b 32 a3 e7 10 29

ISAKMP Network Rx: Removed Non-ESP Marker.
ISAKMP Rx (decrypted)<---
db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 08 10 05 01
76 36 d4 8f 00 00 00 4c 0c 00 00 18 99 6d b0 ab 7b 07 08 9e
b4 01 3d 5c 75 fc 2d d0 dc 02 b9 0c 00 00 00 10 00 00 00 01
03 04 00 01 fb 83 82 4c 00 00 00 00 00 00 00 00
ISAKMP Rx Message (decrypted)
     Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
     Xchg Type:  INFORMATIONAL(5)  Ver: 10  Flags: 01
     MessageID:  7636d48f   Total Length: 68
     Payload #:  0  Length: 24  Type: Hash (HASH)
       99 6d b0 ab 7b 07 08 9e b4 01 3d 5c 75 fc 2d d0 dc 02 b9 0c
     Payload #:  1  Length: 16  Type: Delete (D)
       00 00 00 01 03 04 00 01 fb 83 82 4c
ISAKMP CORE: Exchange 27 done

ISAKMP Network Rx:
     remotePort=48348 localPort=4500
     00 00 00 00 db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39
     08 10 05 01 2e 8f ec b3 00 00 00 54 7f 18 92 f1 2c 1c 0d d2
     32 98 0e 39 5f 95 da 6f dc 16 3c 8f 4b 9b 32 81 f8 66 9b 4b
     42 40 fb 82 f5 f6 4b ed b6 8b c3 8f 1a 21 81 8e 74 01 3a a4
     b7 ed 84 b9 f0 8c af 4a
ISAKMP Network Rx: Removed Non-ESP Marker.
```

```
ISAKMP Rx (decrypted)<---
db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39 08 10 05 01
2e 8f ec b3 00 00 00 54 0c 00 00 18 b5 35 50 37 69 65 75 04
f1 ec 60 5d 5d e0 81 1c 94 97 a0 8a 00 00 00 1c 00 00 00 01
01 10 00 01 db b8 0f 0a a0 ab df a1 3e 39 eb d4 72 4d b8 39
00 00 00 00
ISAKMP Rx Message (decrypted)
     Cookies:   dbb80f0aa0abdfa1:3e39ebd4724db839
     Xchg Type:  INFORMATIONAL(5)  Ver: 10  Flags: 01
     MessageID:  2e8fecb3   Total Length: 80
     Payload #:  0  Length: 24  Type: Hash (HASH)
       b5 35 50 37 69 65 75 04 f1 ec 60 5d 5d e0 81 1c 94 97 a0 8a
     Payload #:  1  Length: 28  Type: Delete (D)
       00 00 00 01 01 10 00 01 db b8 0f 0a a0 ab df a1 3e 39 eb d4
       72 4d b8 39
ISAKMP CORE: Exchange 28 done

ISAKMP CORE: Info: No active isakmp SA with D/N enabled found for 172.28.40.80
```

show isakmp sa output after disconnection

```
                                    Expiry Limits - hard/soft/used
SA Id PeerAddress     EncA.  HashA. Bytes                Seconds
-----------------------------------------------------------------------------
1     172.28.40.80    DES    SHA    -/-/-               86400/75593/23816
```

The remaining SA is for the VPN to the remote office router. This VPN is still up.

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16115-00 REV A