

ASA/PIX: IPsec VPN Client Addressing Using DHCP Server with ASDM Configuration Example

Document ID: 109493

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

Configure

- Network Diagram
- Configure Remote Access VPN (IPSec)
- Configure the ASA/PIX using CLI
- Cisco VPN Client Configuration

Verify

- show Commands

Troubleshoot

- Clear Security Associations
- Troubleshooting Commands
- Sample debug Output

Related Information

Introduction

This document describes how to configure the Cisco 5500 Series Adaptive Security Appliance (ASA) to make the DHCP server provide the client IP address to all the VPN clients using the Adaptive Security Device Manager (ASDM) or CLI. The ASDM delivers world-class security management and monitoring through an intuitive, easy-to-use Web-based management interface. Once the Cisco ASA configuration is complete, it can be verified using the Cisco VPN Client.

Refer to PIX/ASA 7.x and Cisco VPN Client 4.x with Windows 2003 IAS RADIUS (Against Active Directory) Authentication Configuration Example in order to set up the remote access VPN connection between a Cisco VPN Client (4.x for Windows) and the PIX 500 Series Security Appliance 7.x. The remote VPN Client user authenticates against the Active Directory using a Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS server.

Refer to PIX/ASA 7.x and Cisco VPN Client 4.x for Cisco Secure ACS Authentication Configuration Example in order to set up a remote access VPN connection between a Cisco VPN Client (4.x for Windows) and the PIX 500 Series Security Appliance 7.x using a Cisco Secure Access Control Server (ACS version 3.2) for extended authentication (Xauth).

Prerequisites

Requirements

This document assumes that the ASA is fully operational and configured to allow the Cisco ASDM or CLI to make configuration changes.

Note: Refer to Allowing HTTPS Access for ASDM or PIX/ASA 7.x: SSH on the Inside and Outside Interface Configuration Example to allow the device to be remotely configured by the ASDM or Secure Shell (SSH).

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance Software Version 7.x and later
- Adaptive Security Device Manager Version 5.x and later
- Cisco VPN Client Version 4.x and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with Cisco PIX Security Appliance Version 7.x and later.

Conventions

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

Background Information

Remote access VPNs address the requirement of the mobile workforce to securely connect to the organization's network. Mobile users are able to set up a secure connection using the VPN Client software installed on their PCs. The VPN Client initiates a connection to a central site device configured to accept these requests. In this example, the central site device is an ASA 5500 Series Adaptive Security Appliance that uses dynamic crypto maps.

In security appliance address management we have to configure IP addresses that connect a client with a resource on the private network, through the tunnel, and let the client function as if it were directly connected to the private network. Furthermore, we are dealing only with the private IP addresses that get assigned to clients. The IP addresses assigned to other resources on your private network are part of your network administration responsibilities, not part of VPN management. Therefore, when IP addresses are discussed here, we mean those IP addresses available in your private network addressing scheme that let the client function as a tunnel endpoint.

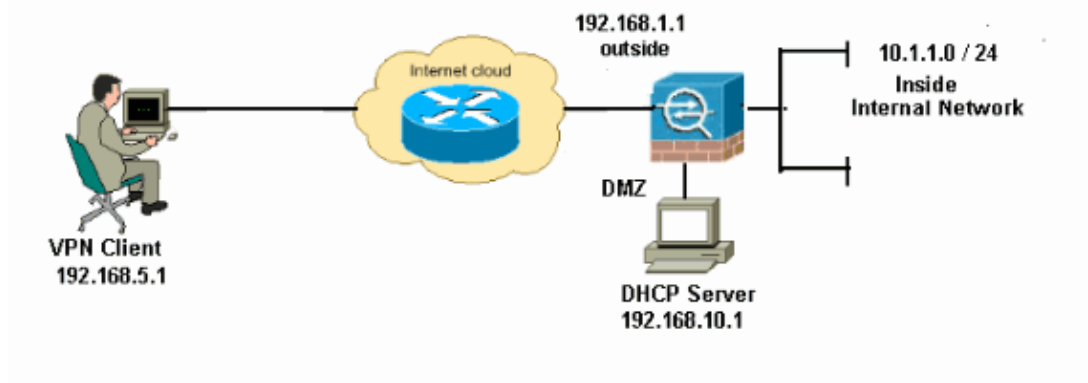
Configure

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

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



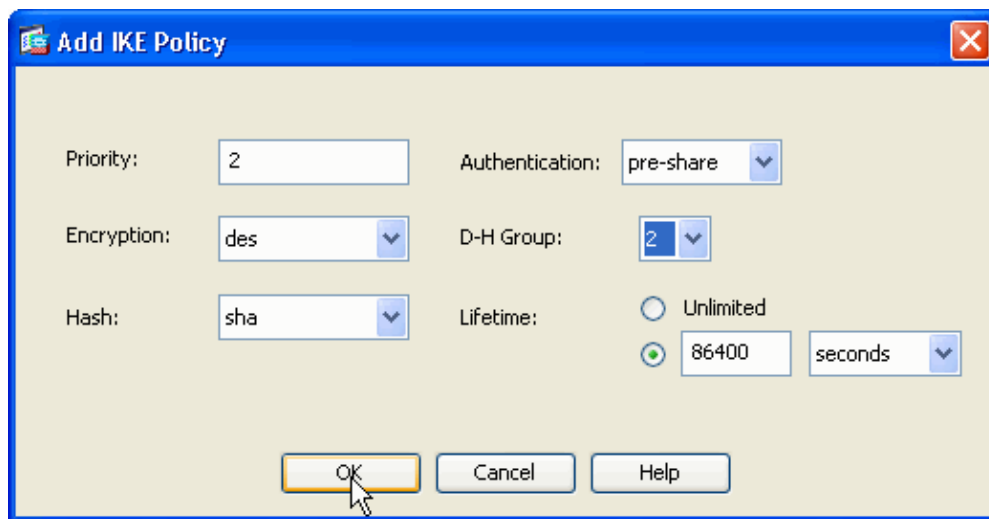
Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which were used in a lab environment.

Configure Remote Access VPN (IPSec)

ASDM Procedure

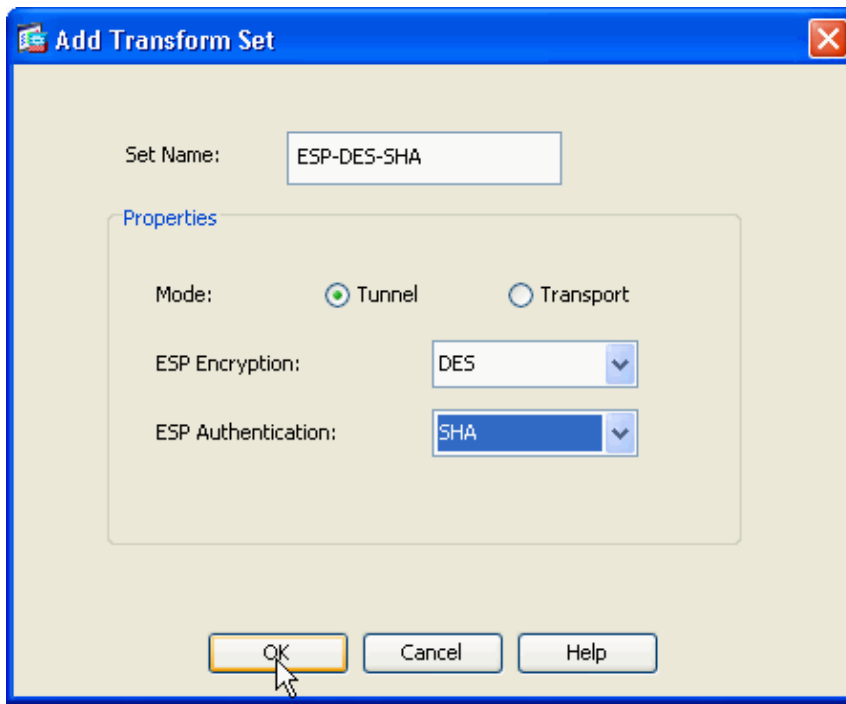
Complete these steps in order to configure the remote access VPN:

1. Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies > Add** in order to create a ISAKMP policy 2, as shown.



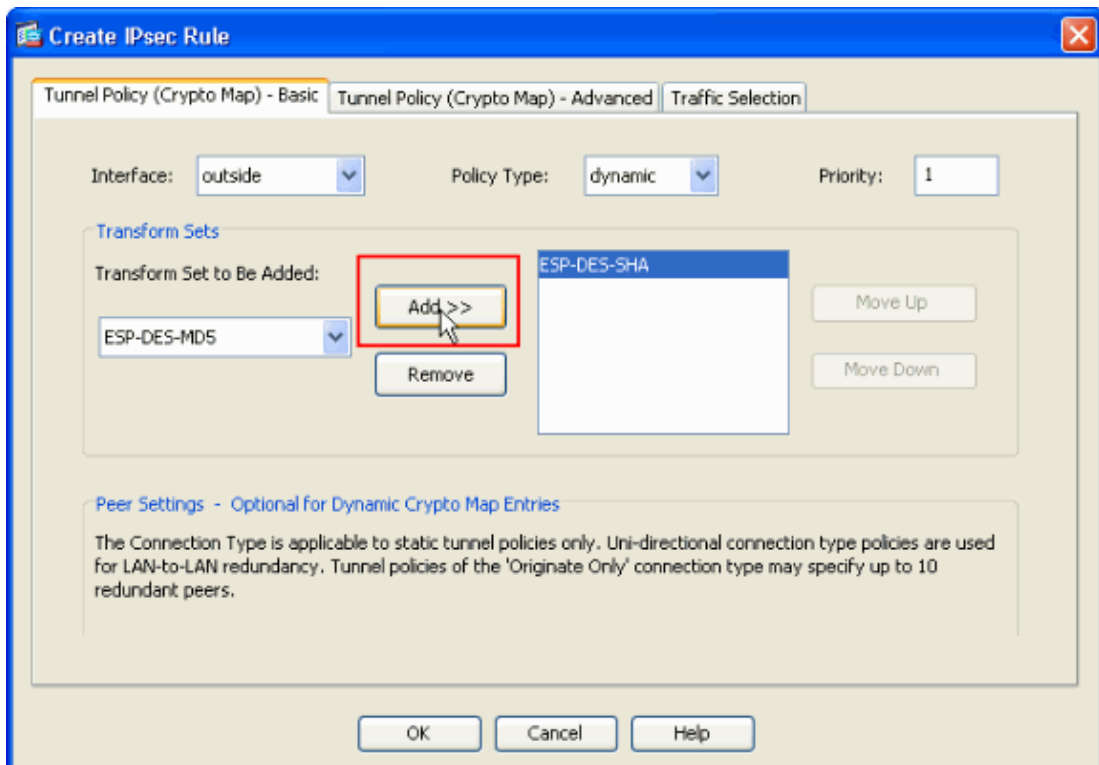
Click **OK** and **Apply**.

2. Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transform Sets > Add** in order to create the **ESP-DES-SHA** transform set, as shown.



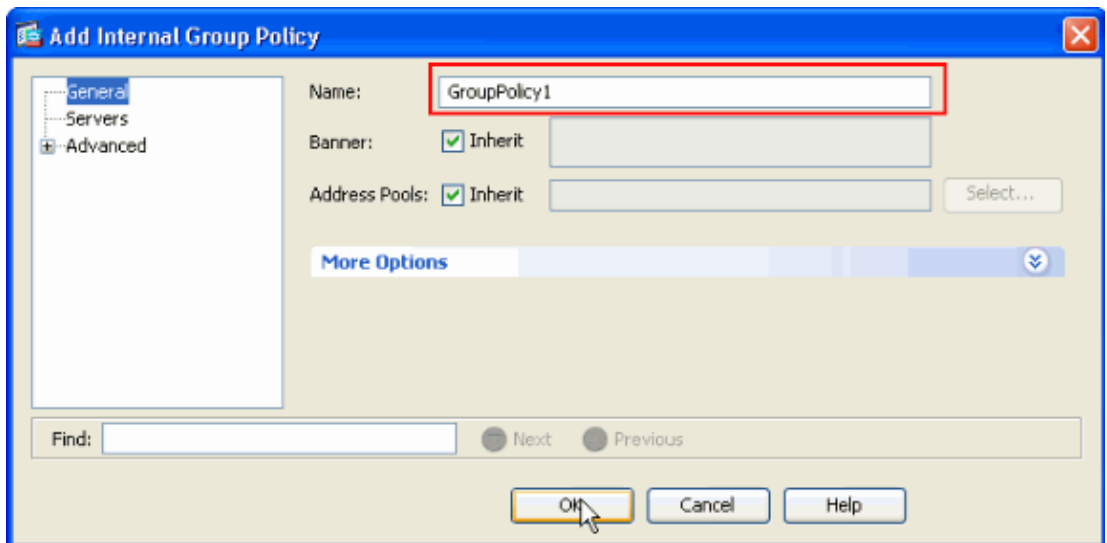
Click **OK** and **Apply**.

3. Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps > Add** in order to create a crypto map with dynamic policy of priority 1, as shown.



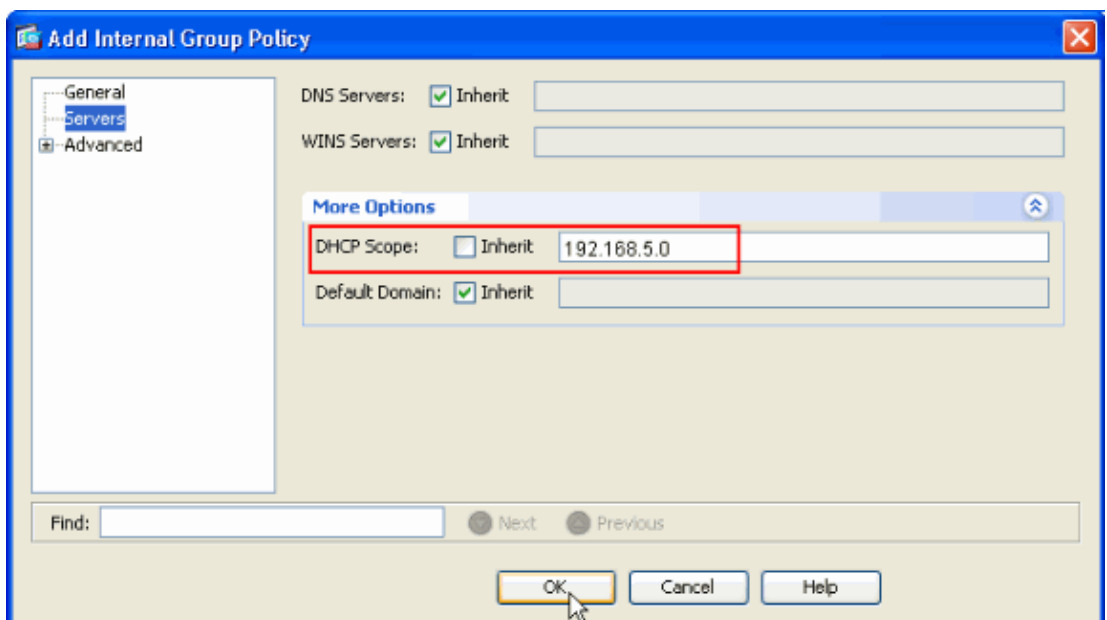
Click **OK** and **Apply**.

4. Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policies > Add>Internal Group Policies** in order to create a group policy (For example **GroupPolicy1**), as shown.



Click **OK** and **Apply**.

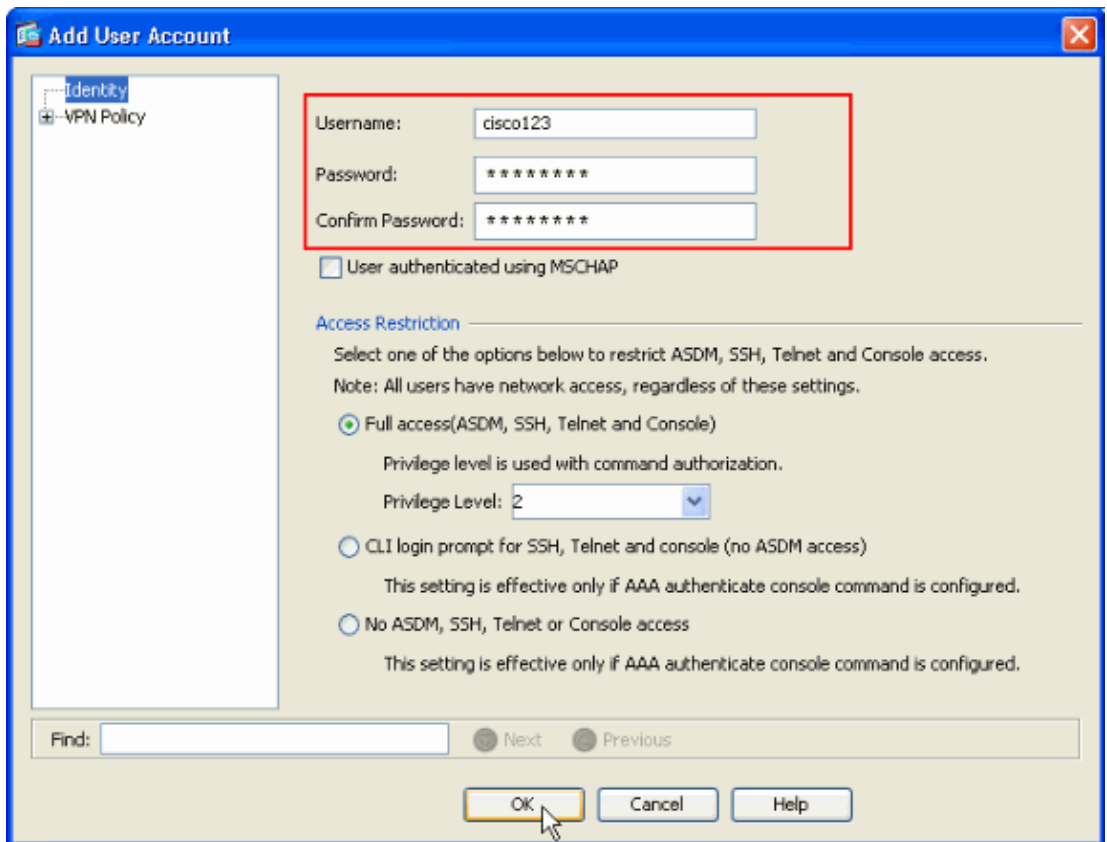
5. Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policies > Add>Internal Group Policies>Servers>>** in order to configure the **DHCP Scope** for the VPN client users to be assigned dynamically.



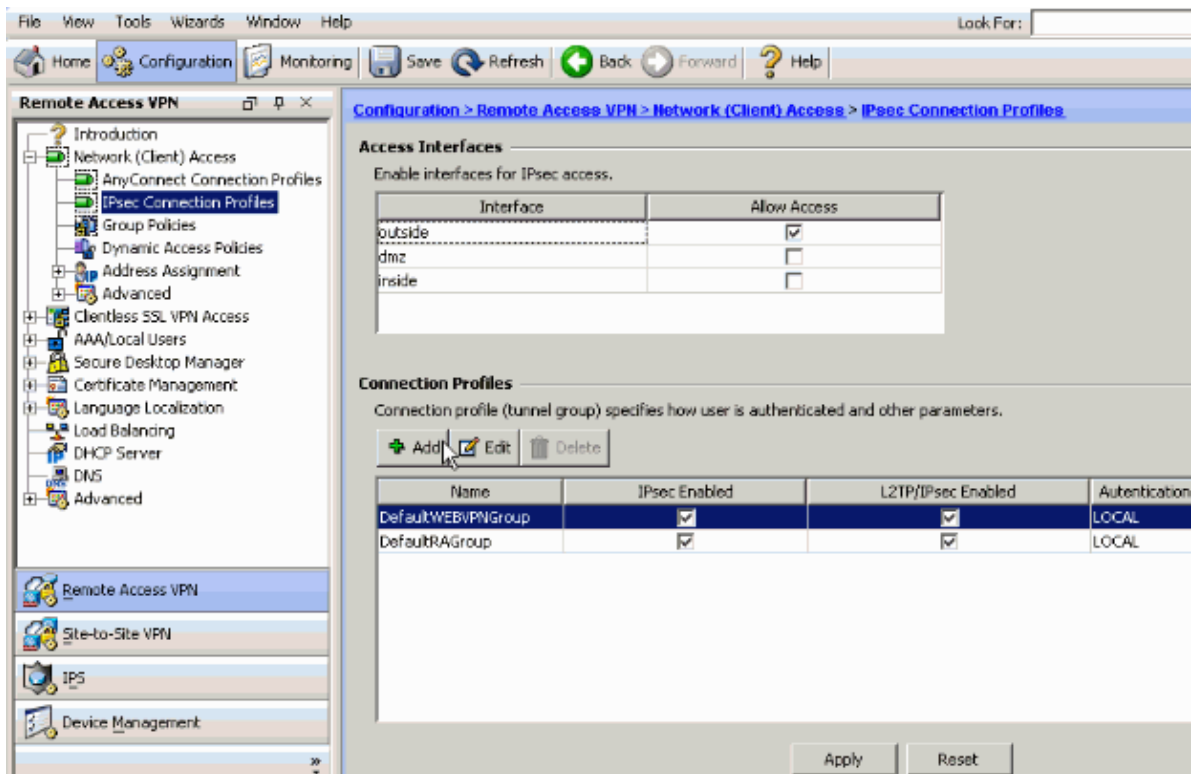
Click **OK** and **Apply**.

Note: DHCP Scope configuration is optional. Refer to Configuring DHCP Addressing for more information.

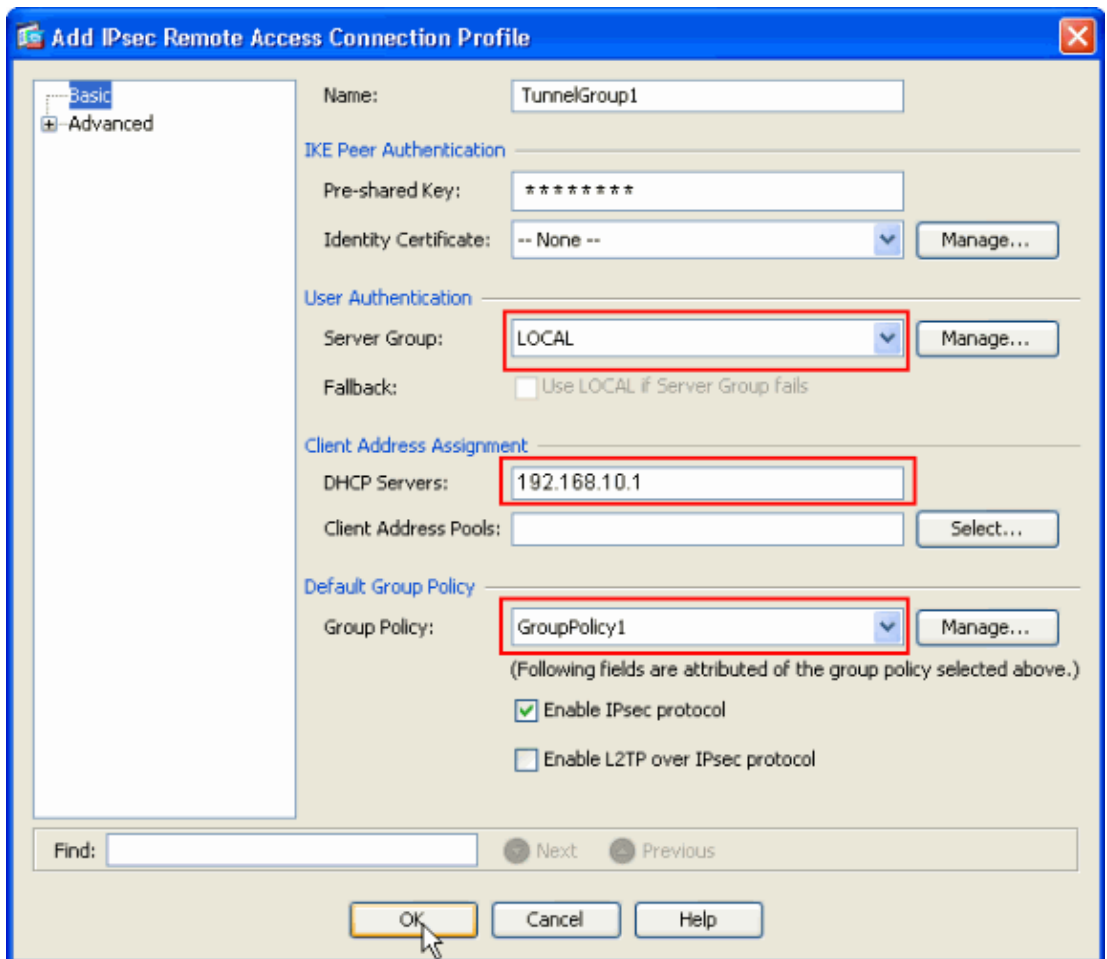
6. Choose **Configuration > Remote Access VPN > AAA Setup > Local Users > Add** in order to create the user account (for example, username – cisco123 and Password – cisco123) for VPN client access.



7. Choose **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles > Add** in order to add a tunnel group (for example, **TunnelGroup1** and the Preshared key as cisco123), as shown.



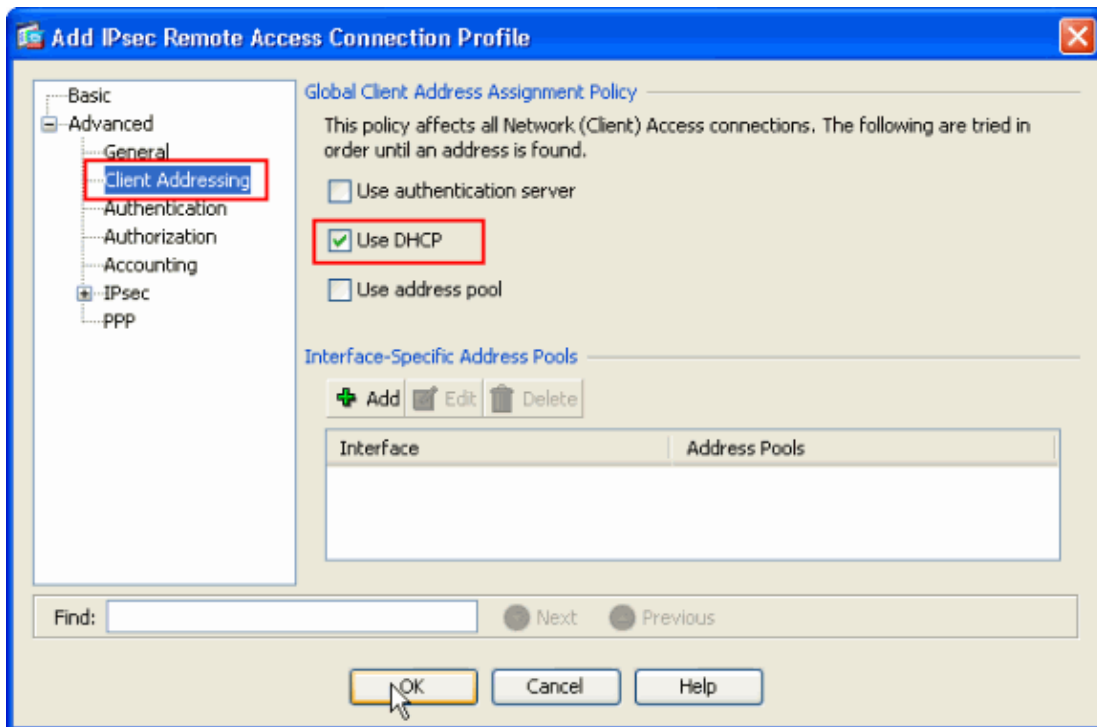
- ◆ Under the **Basic** tab choose the server group as **LOCAL** for the User Authentication field.
- ◆ Choose **Grouppolicy1** as the Group Policy for the Default Group Policy field.
- ◆ Provide the DHCP server IP address in the space provided for **DHCP Servers**.



Click **OK**.

8. Choose **Advanced > Client Addressing >** and check the **Use DHCP** checkbox for the DHCP server to assign IP Address to the VPN clients.

Note: Make sure to uncheck the check boxes for **Use authentication server** and **Use address pool**.



Configure the ASA/PIX using CLI

Complete these steps in order to configure the DHCP server to provide IP address to the VPN clients from the command line. Refer to *Configuring Remote Access VPNs* or *Cisco ASA 5500 Series Adaptive Security Appliances—Command References* for more information on each command that is used.

| Running Config on the ASA Device |
|---|
| <pre> ASA# sh run ASA Version 8.0(2) ! !--- Specify the hostname for the Security Appliance. hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted names ! !--- Configure the outside and inside interfaces. interface Ethernet0/0 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0 ! interface Ethernet0/1 nameif outside security-level 0 ip address 192.168.1.1 255.255.255.0 ! interface Ethernet0/2 nameif DMZ security-level 50 ip address 192.168.10.2 255.255.255.0 </pre> |

!--- Output is suppressed.

```
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
```

```
access-list 101 extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
```

!--- Specify the location of the ASDM image for ASA to fetch the image for ASDM access.

```
asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400
```

```
global (outside) 1 192.168.1.5
nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set ESP-DES-SHA
crypto map outside_map 1 ipsec-isakmp dynamic outside_dyn_map
```

*!--- Specifies the interface to be used with
!--- the settings defined in this configuration.*

```
crypto map outside_map interface outside
```

!--- PHASE 1 CONFIGURATION ---!

*!--- This configuration uses ISAKMP policy 2.
!--- The configuration commands here define the Phase
!--- 1 policy parameters that are used.*

```
crypto isakmp enable outside
```

```
crypto isakmp policy 2
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
```

```
no crypto isakmp nat-traversal

!--- Specifies that the IP address to the vpn clients are assigned
by the DHCP Server and now by AAA or the Local pool.The CLI vpn-addr-assign dhcp
for VPN address assignment through DHCP Server is hidden in the CLI provided by
show run command.

no vpn-addr-assign aaa
no vpn-addr-assign local

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
!
group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes

!--- define the DHCP network scope
in the group policy.This configuration is Optional

dhcp-network-scope 192.168.5.0

!--- In order to identify remote access users to the Security Appliance,
!--- you can also configure usernames and passwords on the device.

username cisco123 password ffIRPGpDSOJh9YLq encrypted

!--- Create a new tunnel group and set the connection
!--- type to remote-access.

tunnel-group TunnelGroup1 type remote-access

!--- Define the DHCP server address to the tunnel group.
```

```
tunnel-group TunnelGroup1 general-attributes
default-group-policy GroupPolicy1
dhcp-server 192.168.10.1
```

!--- Enter the pre-shared-key to configure the authentication method.

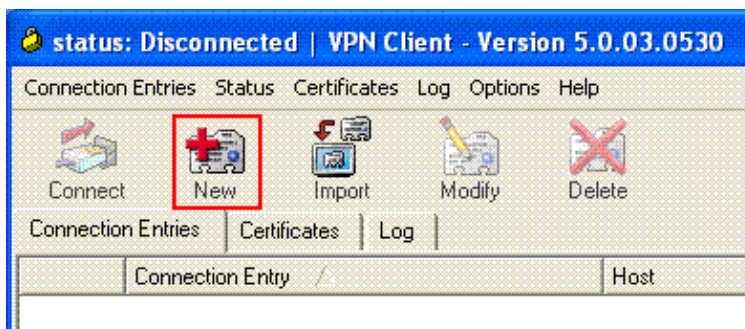
```
tunnel-group TunnelGroup1 ipsec-attributes
pre-shared-key *

prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d
: end
ASA#
```

Cisco VPN Client Configuration

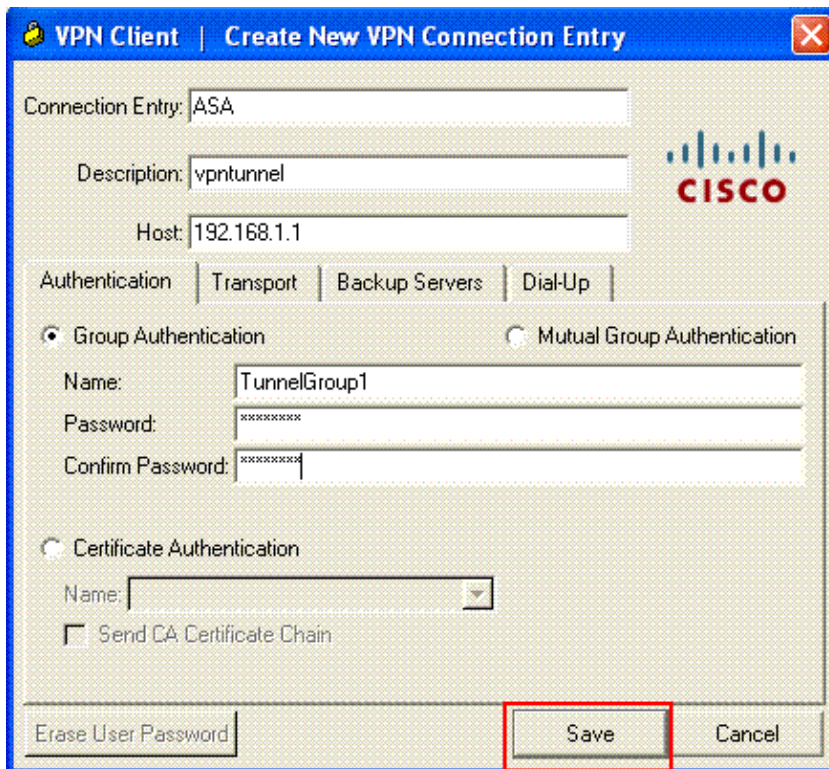
Attempt to connect to the Cisco ASA using the Cisco VPN Client in order to verify that the ASA is successfully configured.

1. Select **Start > Programs > Cisco Systems VPN Client > VPN Client**.
2. Click **New** to launch the Create New VPN Connection Entry window.

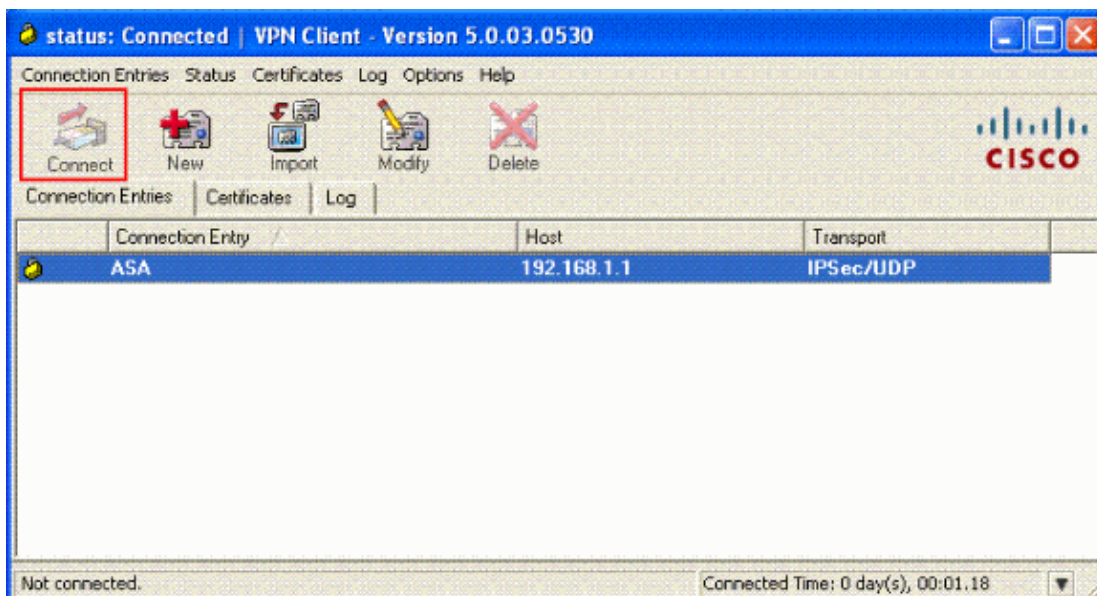


3. Fill in the details of your new connection.

Enter the name of the Connection Entry along with a description. Enter the **outside IP address of the ASA** in the Host box. Then enter the VPN Tunnel Group name(TunnelGroup1) and password (Pre-shared Key – cisco123) as configured in ASA. Click **Save**.



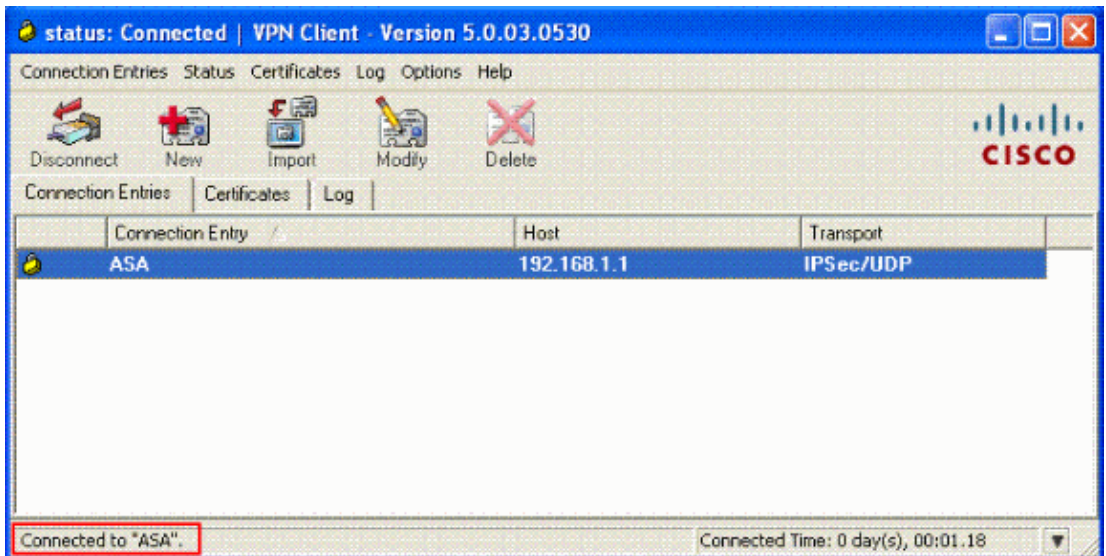
4. Click on the connection you want to use and click **Connect** from the VPN Client main window.



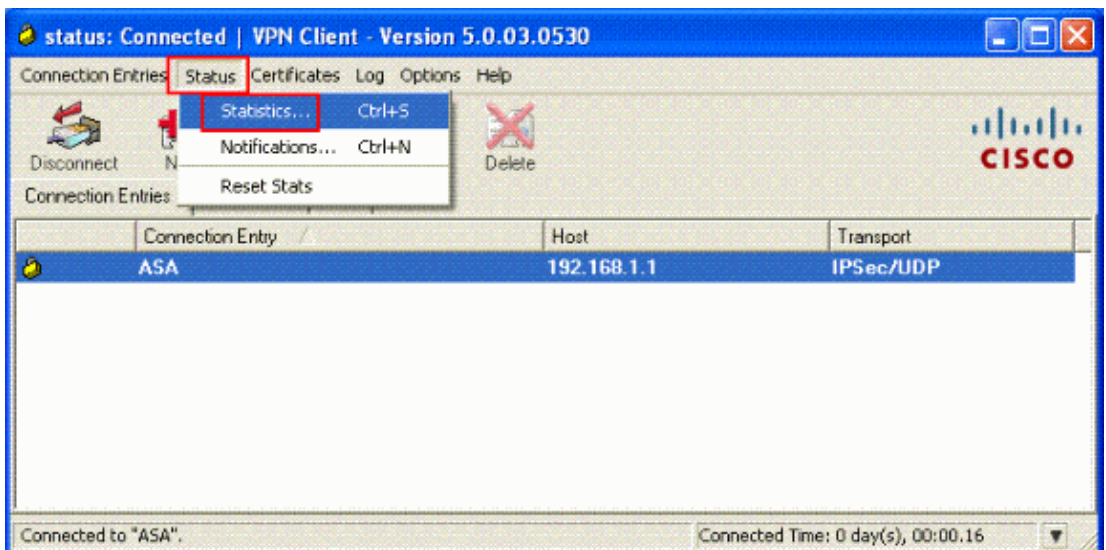
5. When prompted, enter the **Username : cisco123** and **Password : cisco123** as configured in the ASA above for xauth, and click **OK** to connect to the remote network.



6. The VPN Client is connected with the ASA at the central site.



- Once the connection is successfully established, select **Statistics** from the Status menu to verify the details of the tunnel.



Verify

show Commands

Use this section to confirm your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto isakmp sa** Shows all current IKE Security Associations (SAs) at a peer.
- **show crypto ipsec sa** Shows the settings used by current SAs.

```
ASA #show crypto ipsec sa
      interface: outside
Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.1

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0)
current_peer: 192.168.1.2, username: cisco123
dynamic allocated peer ip: 192.168.5.1
```

```

#pkts encaps: 55, #pkts encrypt: 55, #pkts digest: 55
#pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.1.2

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: C2C25E2B

inbound esp sas:
spi: 0x69F8C639 (1777911353)
  transform: esp-des esp-md5-hmac none
  in use settings = {RA, Tunnel, }
  slot: 0, conn_id: 40960, crypto-map: dynmap
  sa timing: remaining key lifetime (sec): 28337
  IV size: 8 bytes
  replay detection support: Y
outbound esp sas:
spi: 0xC2C25E2B (3267517995)
  transform: esp-des esp-md5-hmac none
  in use settings = {RA, Tunnel, }
  slot: 0, conn_id: 40960, crypto-map: dynmap
  sa timing: remaining key lifetime (sec): 28337
  IV size: 8 bytes
  replay detection support: Y

```

ASA #show crypto isakmp sa

```

Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 192.168.1.2
   Type    : user           Role     : responder
   Rekey   : no           State    : AM_ACTIVE

```

Troubleshoot

This section provides information you can use to troubleshoot your configuration. Sample debug output is also shown.

Note: For more information on troubleshooting Remote Access IPsec VPN refer Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions

Clear Security Associations

When you troubleshoot, make sure to clear existing Security Associations after you make a change. In the privileged mode of the PIX, use these commands:

- **clear [crypto] ipsec sa** Deletes the active IPsec SAs. The keyword crypto is optional.
- **clear [crypto] isakmp sa** Deletes the active IKE SAs. The keyword crypto is optional.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec 7** Displays the IPsec negotiations of Phase 2.
- **debug crypto isakmp 7** Displays the ISAKMP negotiations of Phase 1.

Sample debug Output

- ASA 8.0
- VPN Client 5.0 for Windows

ASA 8.0

```
ASA#debug crypto isakmp 7
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message
(msgsid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le
ngth : 856
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ISA_KE payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received xauth V6 VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Fragmentation VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, IKE Peer included IKE fragmenta
tion capability flags: Main Mode: True Aggressive Mode: False
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received NAT-Traversal ver 02 V
ID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity client VID
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group Tun
nelGroup1
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g IKE SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, IKE SA Pr
oposal # 1, Transform # 13 acceptable Matches global IKE entry # 2
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ISAKMP SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Generatin
g keys for Responder...
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing
hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing Cisco Unity VID payload
```

Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, constructing xauth V6 VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, constructing dpd vid payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, constructing Fragmentation VID + extended capabilities payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, constructing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 368
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 116
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processing hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processing notify payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processing IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408)
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Received Cisco Unity client VID
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, constructing blank hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, constructing qm hash payload
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=e8a1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 84
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, process_attr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processing MODE_CFG Reply attributes.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: primary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: secondary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: primary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: secondary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: IP Compression = disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKEGetUserAttributes: Browser Proxy Bypass Local = disable
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, User (cisco123) authenticated.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=143

60de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=14
360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, process_attr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Processing cfg ACK attributes
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=26
63aldd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, process_attr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Processing cfg Request attributes
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for IPV4 address!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for IPV4 net mask!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for DNS server address!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for WINS server address!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received unsupported transaction mode attribute: 5
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Banner!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Save PW setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Default Domain Name!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Split Tunnel List!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Split DNS!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for PFS setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Client Browser Proxy Setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for backup ip-sec peer list!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received unknown transaction mode attribute: 28684
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Application Version!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Client Type: WinNT Client Application Version: 5.0.03.0530
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for FWTYPE!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for DHCP hostname for DDNS is: Wireless12
3!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for UDP Port!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth e
nabled)
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Assigned private IP address 192.168.5.1 to remote user
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Send Client Browser Proxy Attributes!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Browser Proxy set to No-Modify. Browser Proxy data will NOT be inclu
ded in the mode-cfg reply
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload

Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=2663aldd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, **PHASE 1 COMPLETED**
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection: DPD
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Starting P1 rekey timer: 950 seconds.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, sending notify message
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f4435669) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 84
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=541f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 1022
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing ID payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Received remote Proxy Host data in ID Payload: Address 192.168.5.1, Protocol 0, Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing ID payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Received local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, QM IsRekeyed old sa not found by addr
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKE Remote Peer configured for crypto map: dynmap
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, processing IPsec SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IPsec SA Proposal # 14, Transform # 1 acceptable Matches global IPsec SA entry # 10
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKE: requesting SPI!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, oakley constructing quick mode
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing IPsec SA payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing IPsec nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 192.168.1.2, constructing proxy ID
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1

```
92.168.1.2, Transmitting Proxy Id:
  Remote host: 192.168.5.1 Protocol 0 Port 0
  Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Sending RESPONDER LIFETIME notification to Initiator
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=541
f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NOTIFY (11) + NONE (0) total length : 176
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54
1f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, loading all IPSEC SAs
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Generating Quick Mode Key!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Generating Quick Mode Key!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Security negotiation complete for User (cisco123) Responder, Inbound SPI
= 0x31de01d8, Outbound SPI = 0x8b7597a9
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKE got a KEY_ADD msg for SA: SPI = 0x8b7597a9
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Pitcher: received KEY_UPDATE, spi 0x31de01d8
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Starting P2 rekey timer: 27360 seconds.
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Adding static route for client address: 192.168.5.1
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, PHASE 2 COMPLETED (msgid=541f8e43)
Jan 22 22:21:41 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=78
f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 8
0
```

```
ASA#debug crypto ipsec 7
```

```
!--- Deletes the old SAs.
```

```
ASA# IPSEC: Deleted inbound decrypt rule, SPI 0x7F3C985A
  Rule ID: 0xD5567DB0
IPSEC: Deleted inbound permit rule, SPI 0x7F3C985A
  Rule ID: 0xD4EF1DF0
IPSEC: Deleted inbound tunnel flow rule, SPI 0x7F3C985A
  Rule ID: 0xD556AF60
IPSEC: Deleted inbound VPN context, SPI 0x7F3C985A
  VPN handle: 0x0004678C
IPSEC: Deleted outbound encrypt rule, SPI 0xC921E280
  Rule ID: 0xD517EE30
IPSEC: Deleted outbound permit rule, SPI 0xC921E280
  Rule ID: 0xD5123250
IPSEC: Deleted outbound VPN context, SPI 0xC921E280
  VPN handle: 0x00040AB4
```

```
!--- Creates new SAs.
```

```
ASA# IPSEC: New embryonic SA created @ 0xD4EF2390,
  SCB: 0xD4EF22C0,
  Direction: inbound
  SPI      : 0x7F3C985A
```

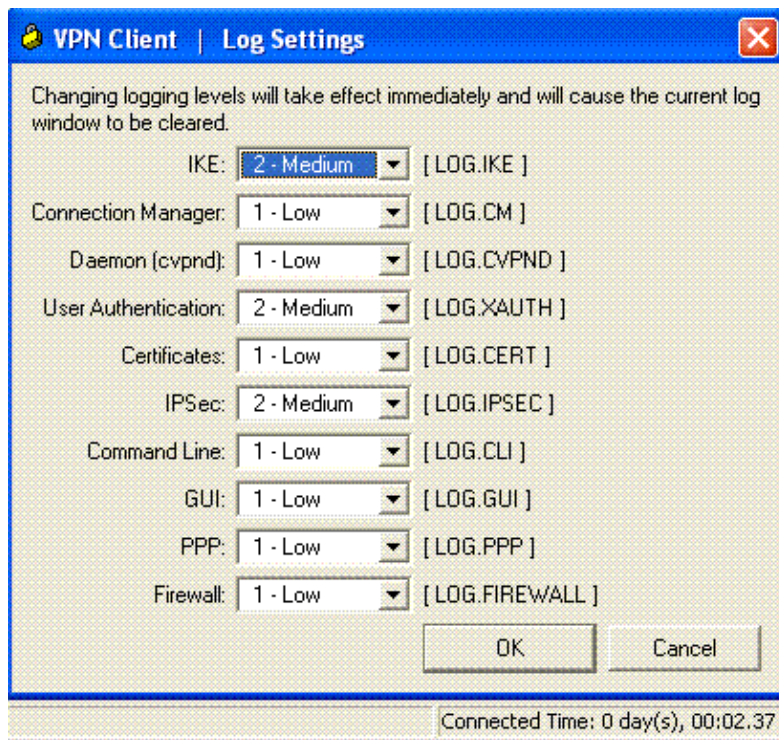
Session ID: 0x0000F000
VPIF num : 0x00000002
Tunnel type: ra
Protocol : esp
Lifetime : 240 seconds
IPSEC: New embryonic SA created @ 0xD556B118,
SCB: 0xD556B048,
Direction: outbound
SPI : 0xC921E280
Session ID: 0x0000F000
VPIF num : 0x00000002
Tunnel type: ra
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0xC921E280
IPSEC: Creating outbound VPN context, SPI 0xC921E280
Flags: 0x00000005
SA : 0xD556B118
SPI : 0xC921E280
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x0133B741
Channel: 0xD4160FA8
IPSEC: Completed outbound VPN context, SPI 0xC921E280
VPN handle: 0x00040AB4
IPSEC: New outbound encrypt rule, SPI 0xC921E280
Src addr: 0.0.0.0
Src mask: 0.0.0.0
Dst addr: 192.168.5.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0xC921E280
Rule ID: 0xD517EE30
IPSEC: New outbound permit rule, SPI 0xC921E280
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.2
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0xC921E280
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xC921E280
Rule ID: 0xD5123250
IPSEC: Completed host IBSA update, SPI 0x7F3C985A
IPSEC: Creating inbound VPN context, SPI 0x7F3C985A

```
Flags: 0x00000006
SA : 0xD4EF2390
SPI : 0x7F3C985A
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x00040AB4
SCB : 0x0132B2C3
Channel: 0xD4160FA8
IPSEC: Completed inbound VPN context, SPI 0x7F3C985A
VPN handle: 0x0004678C
IPSEC: Updating outbound VPN context 0x00040AB4, SPI 0xC921E280
Flags: 0x00000005
SA : 0xD556B118
SPI : 0xC921E280
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x0004678C
SCB : 0x0133B741
Channel: 0xD4160FA8
IPSEC: Completed outbound VPN context, SPI 0xC921E280
VPN handle: 0x00040AB4
IPSEC: Completed outbound inner rule, SPI 0xC921E280
Rule ID: 0xD517EE30
IPSEC: Completed outbound outer SPD rule, SPI 0xC921E280
Rule ID: 0xD5123250
IPSEC: New inbound tunnel flow rule, SPI 0x7F3C985A
Src addr: 192.168.5.1
Src mask: 255.255.255.255
Dst addr: 0.0.0.0
Dst mask: 0.0.0.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7F3C985A
Rule ID: 0xD556AF60
IPSEC: New inbound decrypt rule, SPI 0x7F3C985A
Src addr: 192.168.1.2
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x7F3C985A
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7F3C985A
Rule ID: 0xD5567DB0
IPSEC: New inbound permit rule, SPI 0x7F3C985A
Src addr: 192.168.1.2
Src mask: 255.255.255.255
```

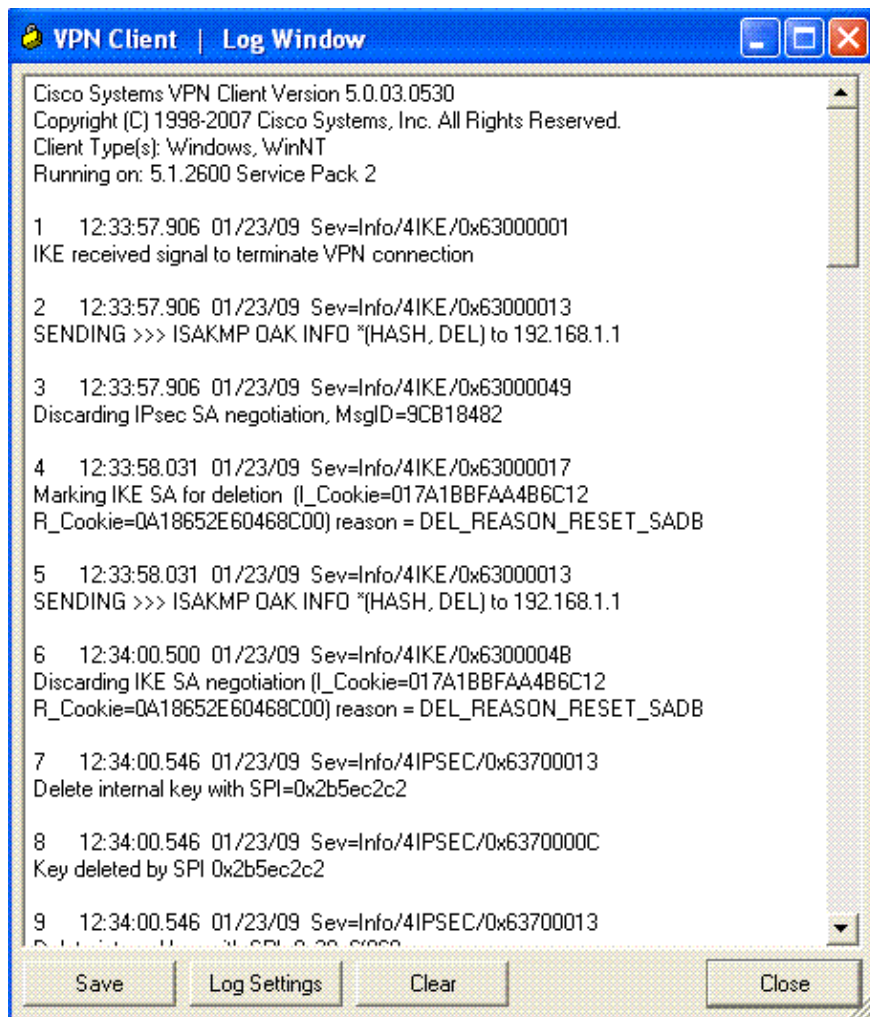
```
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
  Upper: 0
  Lower: 0
  Op   : ignore
Dst ports
  Upper: 0
  Lower: 0
  Op   : ignore
Protocol: 50
Use protocol: true
SPI: 0x7F3C985A
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7F3C985A
Rule ID: 0xD4EF1DF0
```

VPN Client 5.0 for Windows

Select **Log > Log settings** to enable the log levels in the VPN Client.



Select **Log > Log Window** to view the log entries in the VPN Client.



Related Information

- [Cisco ASA 5500 Series Adaptive Security Appliances Support Page](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances Command References](#)
- [Cisco PIX 500 Series Security Appliances Support Page](#)
- [Cisco PIX 500 Series Security Appliances Command Reference](#)
- [Cisco Adaptive Security Device Manager](#)
- [IPsec Negotiation/IKE Protocols Support Page](#)
- [Cisco VPN Client Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 27, 2009

Document ID: 109493
