ASA/PIX：通过 ASDM 使用 DHCP 服务器实现 IPsec VPN 客户端寻址的配置示例

目录

简介
先决条件
要求
使用的组件
相关产品
规则
背景信息
配置
网络图
配置远程访问 VPN (IPSec)
使用 CLI 配置 ASA/PIX
Cisco VPN 客户端配置
验证
显示命令
故障排除
清除安全关联
故障排除命令
调试输出示例
相关信息

简介

本文档介绍如何使用自适应安全设备管理器 (ASDM) 或 CLI 配置 Cisco 5500 系列自适应安全设备 (ASA) 以使 DHCP 服务器向所有 VPN 客户端提供客户端 IP 地址。ASDM 通过一个直观且易于使用的基于 Web 的管理界面提供一流的安全管理和监控。完成 Cisco ASA 配置后，可以使用 Cisco VPN 客户端对其进行验证。

要在 Cisco VPN 客户端（适用于 Windows 的 4.x 版本）和 PIX 500 系列安全设备 7.x 之间设置远程访问 VPN 连接，请参阅使用 Windows 2003 IAS RADIUS（针对 Active Directory）进行身份验证的 PIX/ASA 7.x 和 Cisco VPN 客户端 4.x 配置示例。远程 VPN 客户端用户使用 Microsoft Windows 2003 Internet 身份验证服务 (IAS) RADIUS 服务器根据 Active Directory 进行身份验证。

要使用 Cisco 安全访问控制服务器 (ACS 版本 3.2) 进行扩展身份验证 (Xauth) 以在 Cisco VPN 客户端（适用于 Windows 的 4.x 版本）和 PIX 500 系列安全设备 7.x 之间设置远程访问 VPN 连接，请参阅使用 Cisco 安全 ACS 身份验证的 PIX/ASA 7.x 和 Cisco VPN 客户端 4.x 配置示例。

先决条件

要求

本文档假设 ASA 处于完全运行状态，并配置为允许 Cisco ASDM 或 CLI 进行配置更改。

注意：请参阅允许ASDM或PIX/ASA 7.x的HTTPS访问：内部和外部接口上的 SSH 配置示例以允许通过 ASDM 或Secure Shell (SSH) 远程对设备进行配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 自适应安全设备软件版本 7.x 及更高版本
- 自适应安全设备管理器5.x版及更高版本
- 思科VPN客户端版本4.x及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于Cisco PIX安全设备版本7.x及更高版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

远程访问 VPN 满足了移动工作者的安全连接组织网络的需要。移动用户可以使用安装在其 PC 机上的 VPN 客户端软件来建立安全连接。VPN 客户端将会向已配置为接受这些请求的中心站点设备发起连接。在本示例中，中心站点设备为使用动态加密映射的 ASA 5500 系列自适应安全设备。

在安全设备地址管理方面，我们必须通过隧道配置用于将客户端与专用网络上的资源连接起来的 IP 地址，使客户端运行起来似乎是直接连接到专用网络上。而且，我们仅配置分配给客户端的专用 IP 地址。分配给您的专用网络上其他资源的 IP 地址属于您的网络管理职责的一部分，不在 VPN 管理的范围内。因此，我们在此处讨论的 IP 地址指的是在您的专用网络编址方案中可将客户端作为隧道终点运行的 IP 地址。

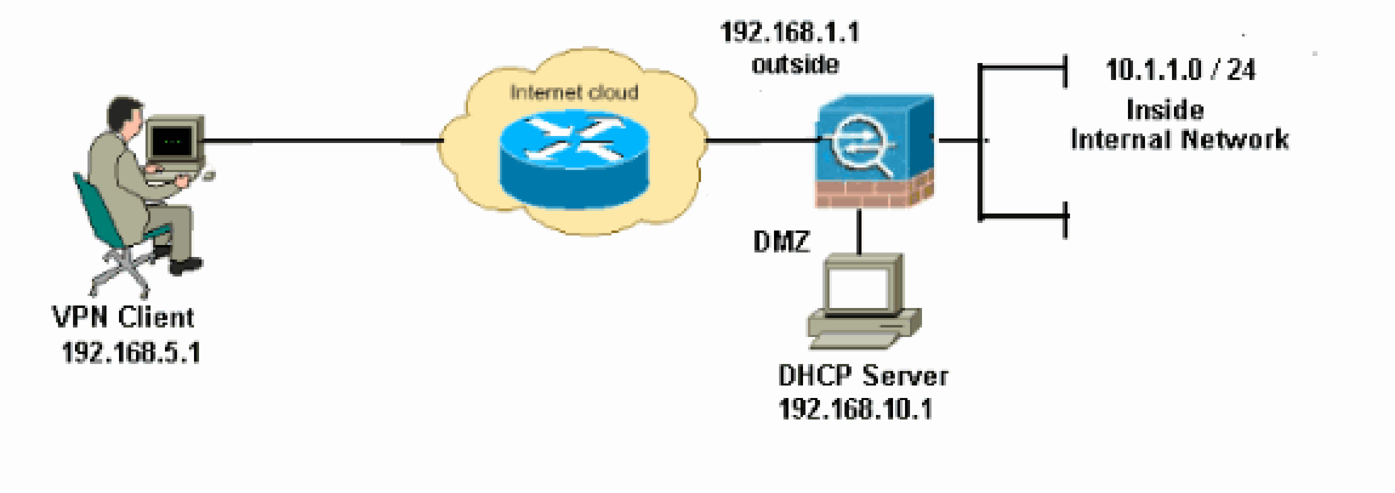
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



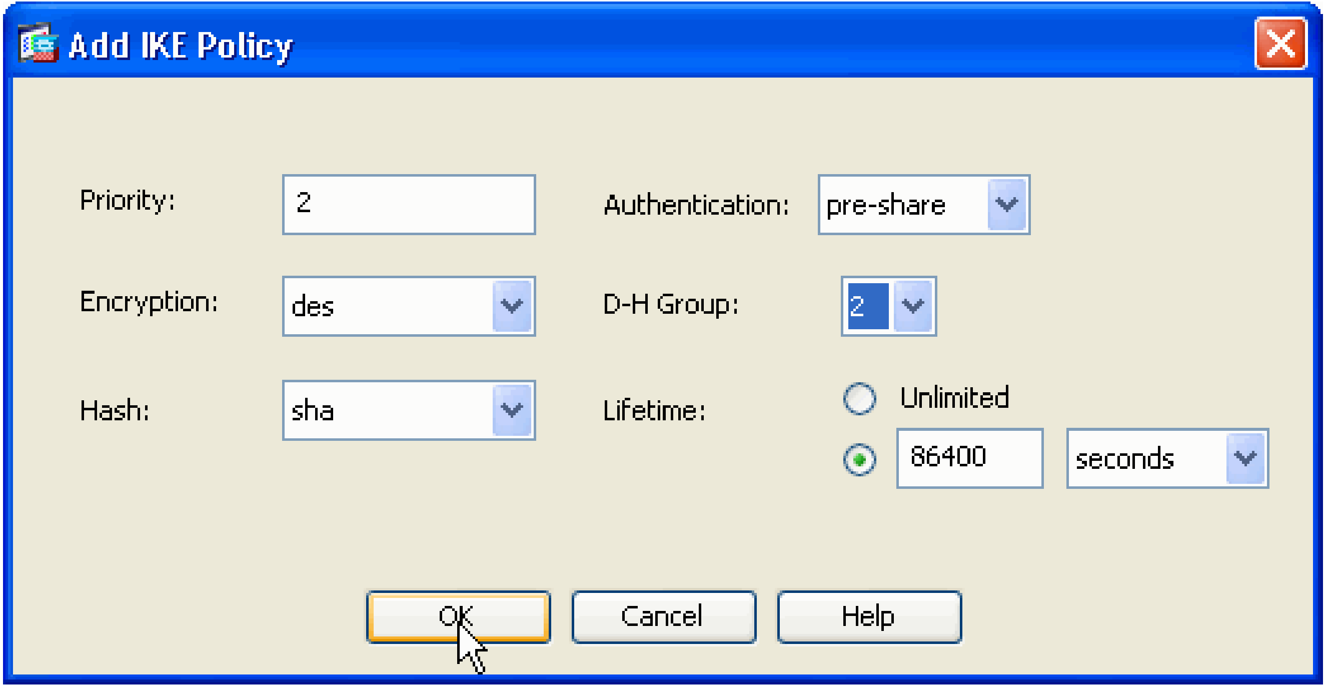
注意：此配置中使用的IP编址方案在Internet上无法合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

配置远程访问 VPN (IPSec)

ASDM 步骤

执行下列步骤以配置远程访问 VPN：

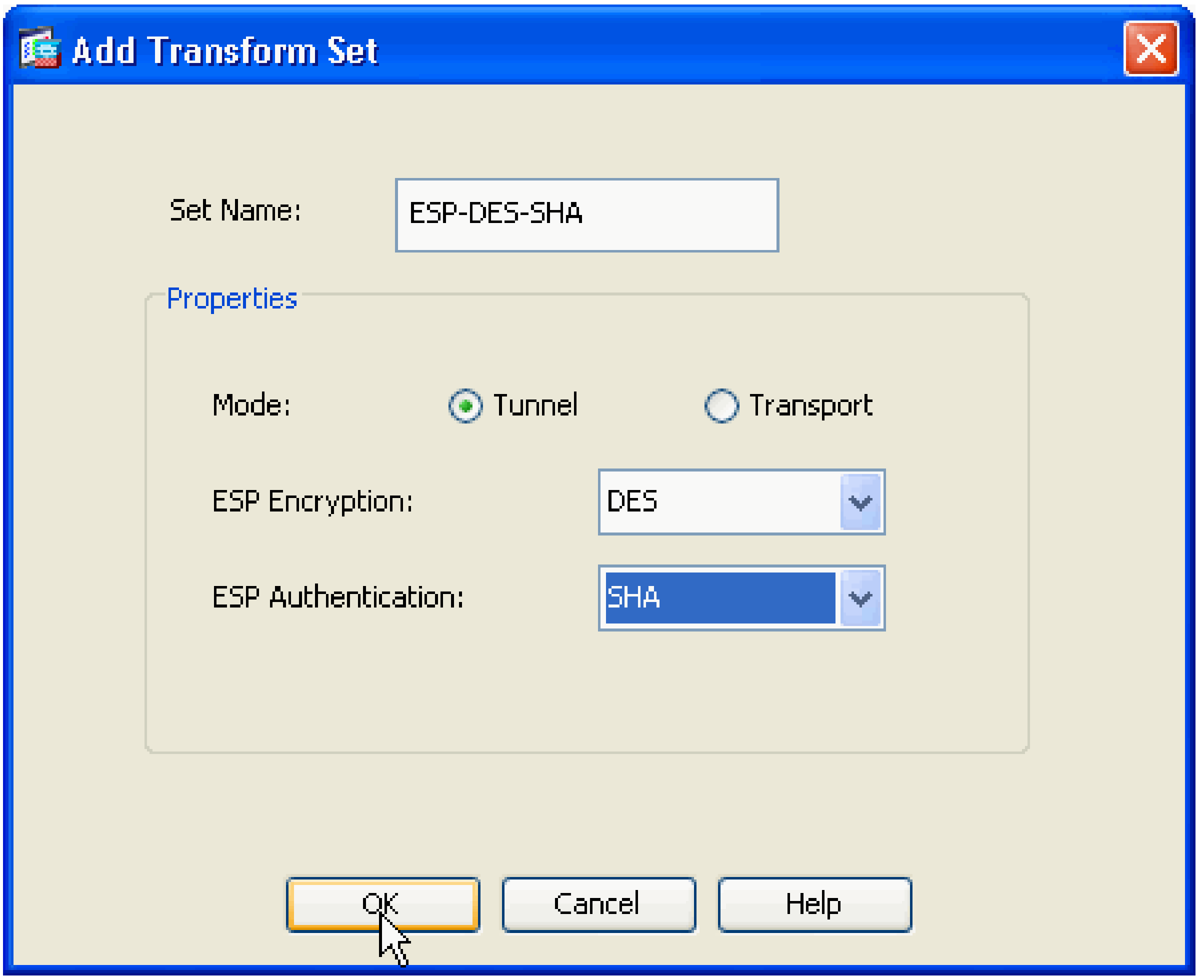
1. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies > Add 以创建 ISAKMP 策略 2，如下所示。**



Priority: 2
Authentication: pre-share
Encryption: des
D-H Group: 2
Hash: sha
Lifetime: ○ Unlimited
● 86400 seconds

单击 **OK，然后单击 Apply。**

2. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transform Sets > Add 以创建 ESP-DES-SHA 转换集，如下所示。**



Add Transform Set

Set Name: ESP-DES-SHA

Properties

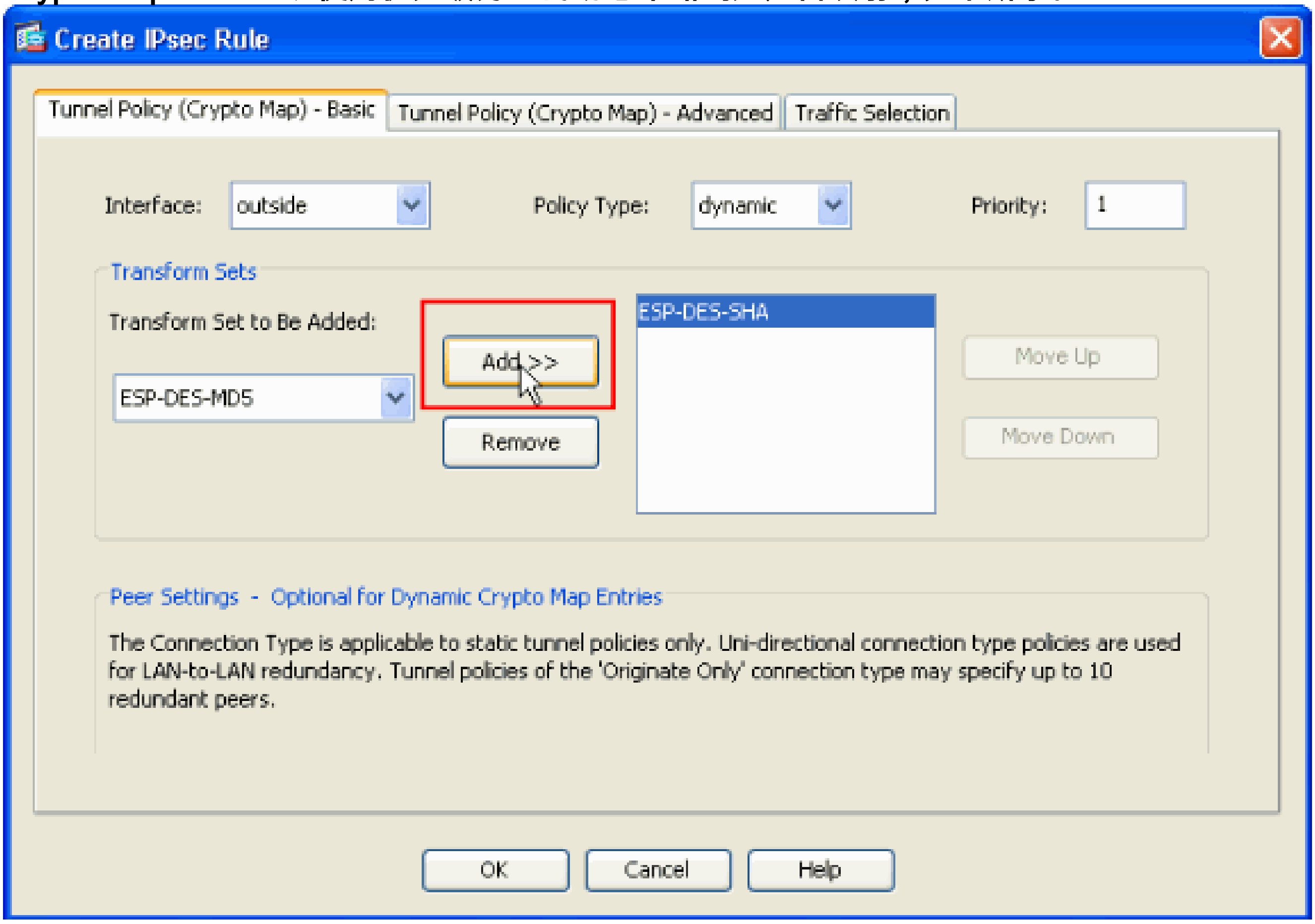
Mode: ● Tunnel ○ Transport

ESP Encryption: DES

ESP Authentication: SHA

单击 OK，然后单击 Apply。

3. 选择 Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add 以使用优先级为 1 的动态策略创建加密映射，如下所示。



Create IPsec Rule

Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection

Interface: outside

Policy Type: dynamic

Priority: 1

Transform Sets

Transform Set to Be Added: ESP-DES-MD5

ESP-DES-SHA

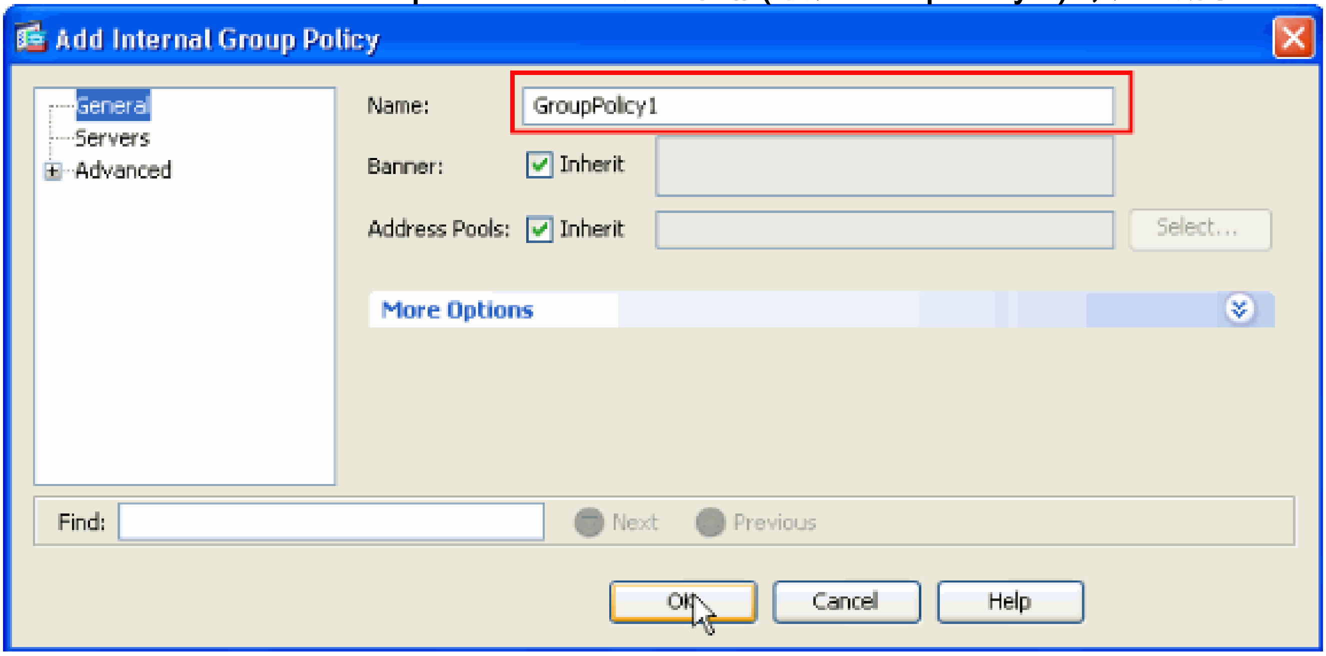
Add >>
Remove
Move Up
Move Down

Peer Settings - Optional for Dynamic Crypto Map Entries

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

单击 OK，然后单击 Apply。

4. 选择 Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policies > Add>Internal Group Policies 以创建组策略（例如 GroupPloicy1），如下所示。



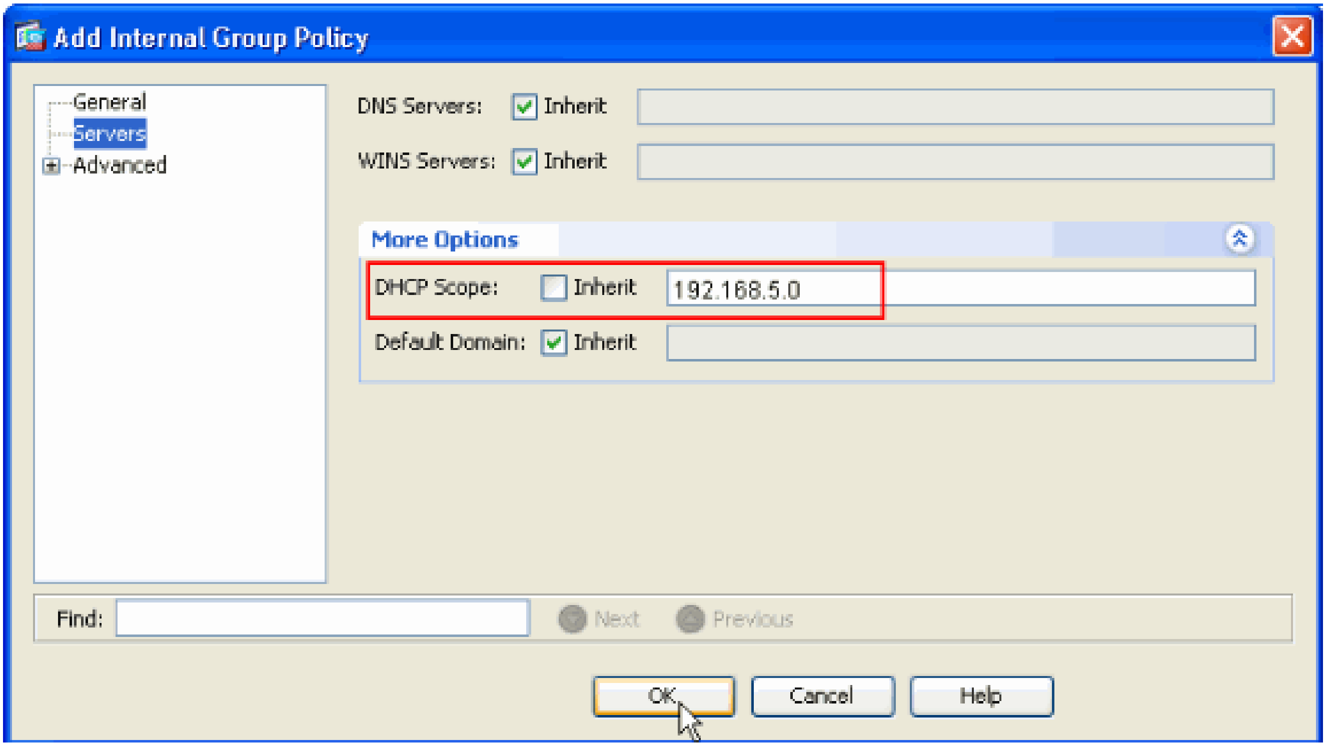
Name: GroupPolicy1

Banner: ☑ Inherit

Address Pools: ☑ Inherit

单击 OK，然后单击 Apply。

5. 选择 Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policies > Add>Internal Group Policies>Servers>> 以便将 VPN 客户端用户的 DHCP 作用域配置为动态分配。



DNS Servers: ☑ Inherit

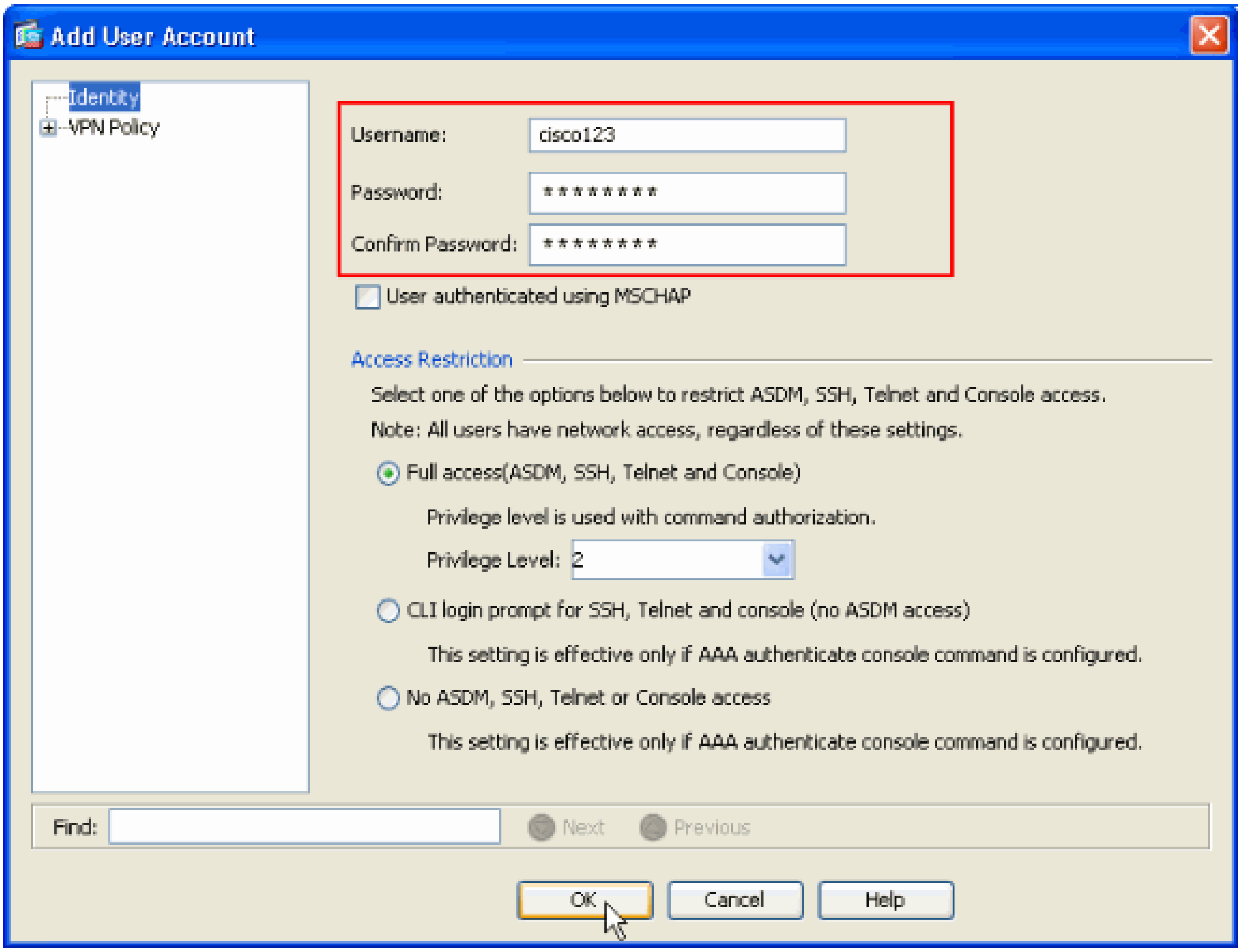
WINS Servers: ☑ Inherit

DHCP Scope: □ Inherit 192.168.5.0

Default Domain: ☑ Inherit

单击 OK，然后单击 Apply。注意：DHCP范围配置是可选的。有关详细信息，请参阅配置 DHCP 编址。

6. 选择 Configuration > Remote Access VPN > AAA Setup > Local Users > Add 以创建用于 VPN 客户端访问的用户帐户（例如，用户名 - cisco123，口令 - cisco123）。



Username: cisco123

Password: ********

Confirm Password: ********

□ User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

● Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 2

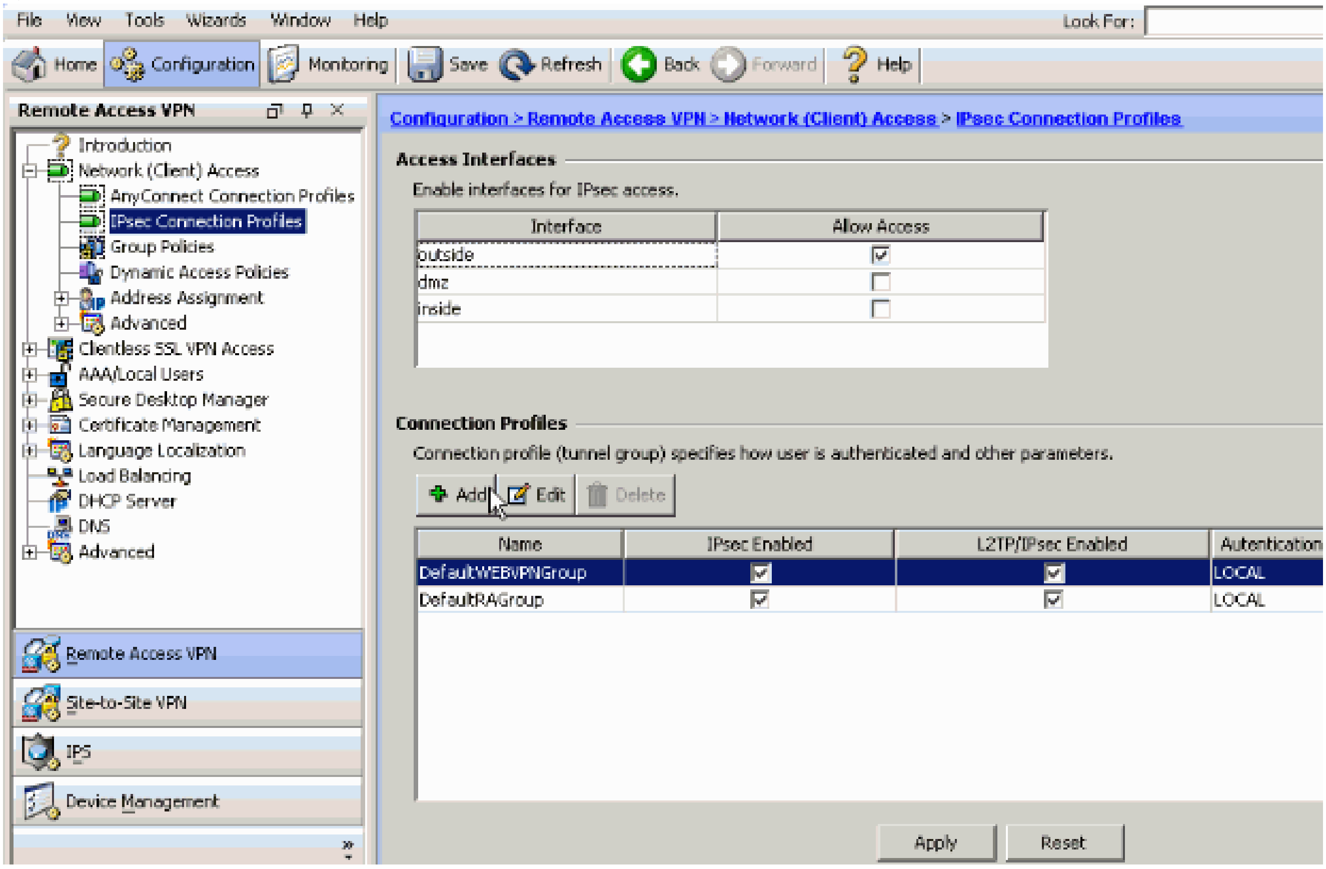
○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if AAA authenticate console command is configured.

○ No ASDM, SSH, Telnet or Console access

This setting is effective only if AAA authenticate console command is configured.

7. 选择 **Configuration > Remote Access VPN > Network (Client) Access > IPSec Connection Profiles > Add> 以添加隧道组（例如，TunnelGroup1，Preshared Key 为 cisco123），如下所示。**



Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	☑
dmz	□
inside	□

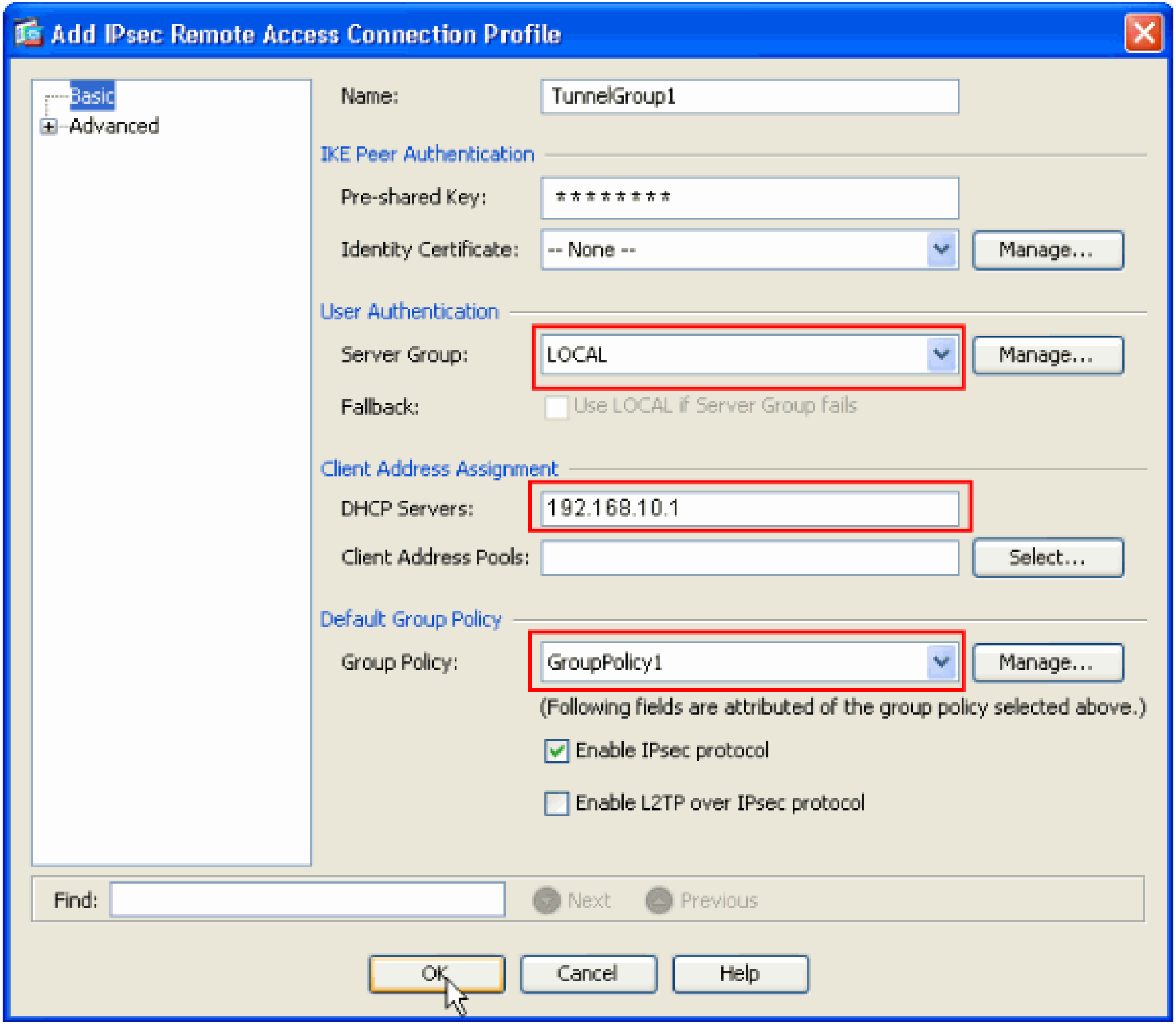
Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

Name	IPsec Enabled	L2TP/IPsec Enabled	Autentication
DefaultWEBVPNGroup	☑	☑	LOCAL
DefaultRAGroup	☑	☑	LOCAL

在 **Basic 选项卡中，为 User Authentication 字段选择 LOCAL 作为 Server Group。**为 Default

Group Policy 字段选择 **Grouppolicy1 作为 Group Policy。**在为 **DHCP Servers** 提供的空白处，输入 DHCP 服务器 IP 地址。



Add IPsec Remote Access Connection Profile

Name: TunnelGroup1

IKE Peer Authentication

Pre-shared Key: ********

Identity Certificate: -- None --

User Authentication

Server Group: LOCAL

Fallback: □ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers: 192.168.10.1

Client Address Pools:

Default Group Policy

Group Policy: GroupPolicy1

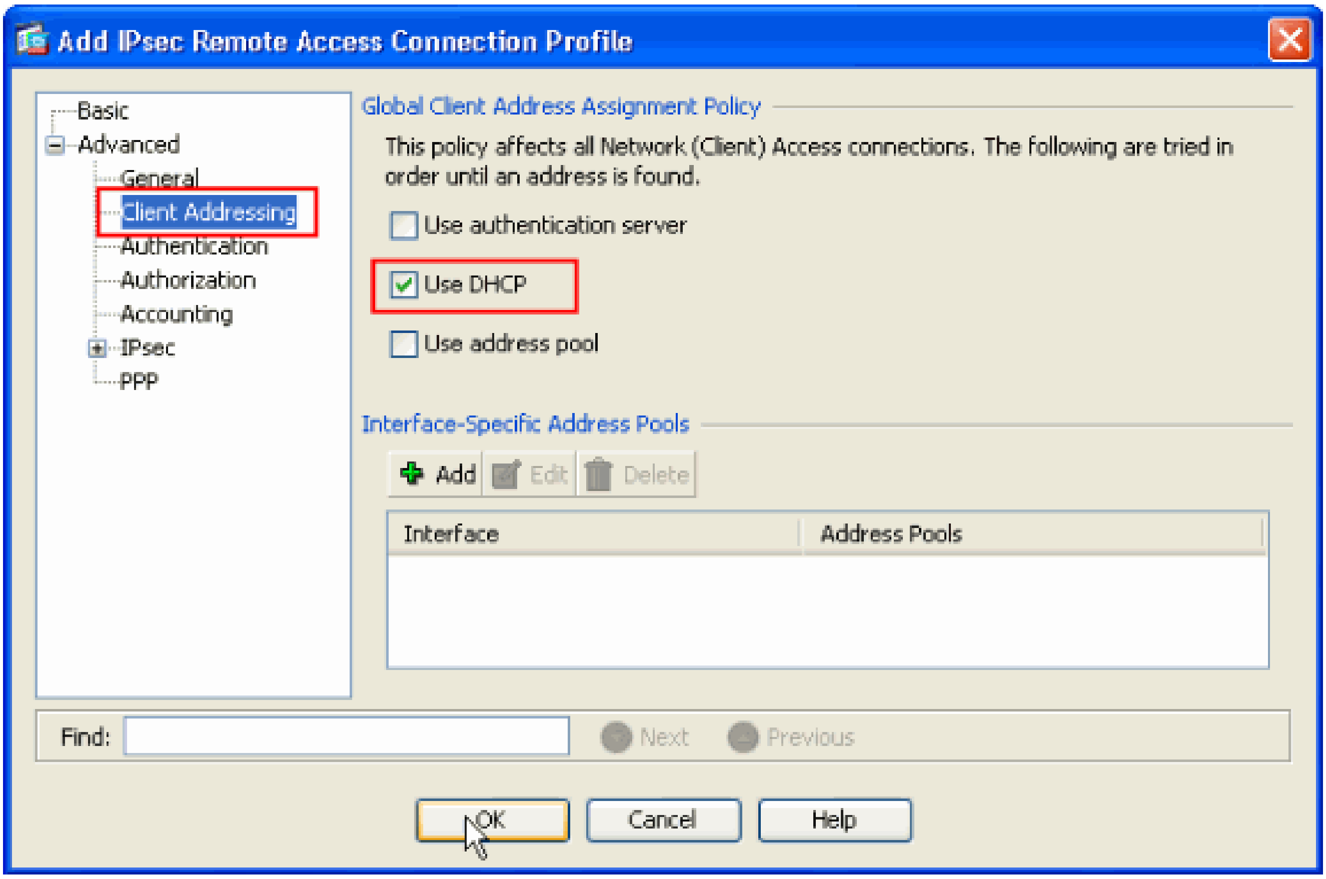
(Following fields are attributed of the group policy selected above.)

☑ Enable IPsec protocol

□ Enable L2TP over IPsec protocol

单击 OK。

8. 选择 **Advanced > Client Addressing > 并选中 Use DHCP 复选框，以使 DHCP 服务器向 VPN 客户端分配 IP 地址。注意：**确保取消选中“使用身份验证服务器”和“**使用地址**池”**复选框。**


Add IPsec Remote Access Connection Profile

Global Client Address Assignment Policy

This policy affects all Network (Client) Access connections. The following are tried in order until an address is found.

□ Use authentication server

☑ Use DHCP

□ Use address pool

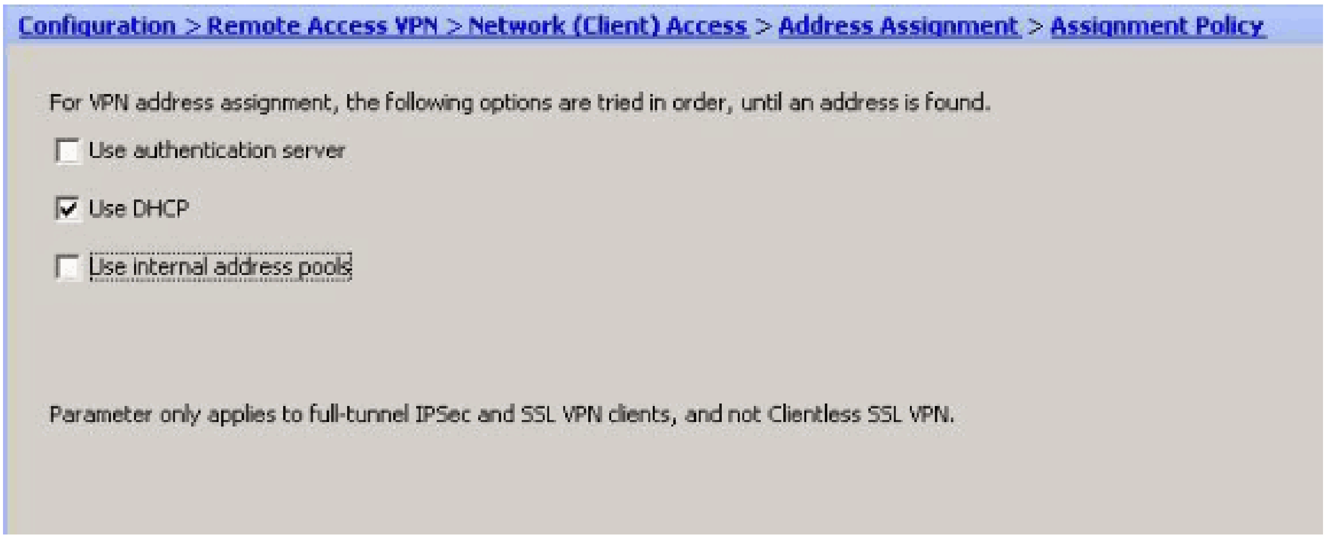
Interface-Specific Address Pools

Interface	Address Pools

ASDM 6.x配置

相同的ASDM配置与ASDM版本6.x配合使用，但ASDM路径的一些细微修改除外。ASDM路径到某些字段与ASDM 6.2版及更高版本有差异。修改和现有路径列于下面。在图形图像对于所有主要ASDM版本保持不变的情况下，图形图像不会附加。

1. Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IKE Policies > Add
2. Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IPSec Transform Sets > Add
3. Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > Crypto Maps > Add
4. 选择Configuration > Remote Access VPN > Network(Client)Access > Group Policies > Add > Internal Group Policies
5. 选择Configuration > Remote Access VPN > Network(Client)Access > Group Policies > Add > Internal Group Policies > Servers
6. 选择Configuration > Remote Access VPN > AAA Setup/Local Users > Local Users > Add
7. Configuration > Remote Access VPN > Network(Client)Access > IPSec Connection Profiles > Add
8. 选择Configuration > Remote Access VPN > Network(Client)Access > Address Assignment > Assignment
Policy



Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy

For VPN address assignment, the following options are tried in order, until an address is found.

□ Use authentication server

☑ Use DHCP

□ Use internal address pools

Parameter only applies to full-tunnel IPSec and SSL VPN clients, and not Clientless SSL VPN.

默认情况下，这三个选项均已启用。Cisco ASA按照相同的顺序为VPN客户端分配地址。取消选中其他两个选项时，Cisco ASA不会验证aaa服务器和本地池选项。默认启用的选项可通过show run **all验证 | in vpn-add命**令。以下是供您参考的输出示例：

```
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local reuse-delay 0
```

有关此命令的详细信息，请参阅vpn-addr-assign。

使用CLI配置ASA/PIX

完成以下步骤，以便通过命令行配置 DHCP 服务器向 VPN 客户端提供 IP 地址。有关所使用的每个命令的详细信息，请参阅配置远程接入 VPN 或 Cisco ASA 5500 系列自适应安全设备命令参考。

在 ASA 设备上运行配置

```
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 !--- 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
```

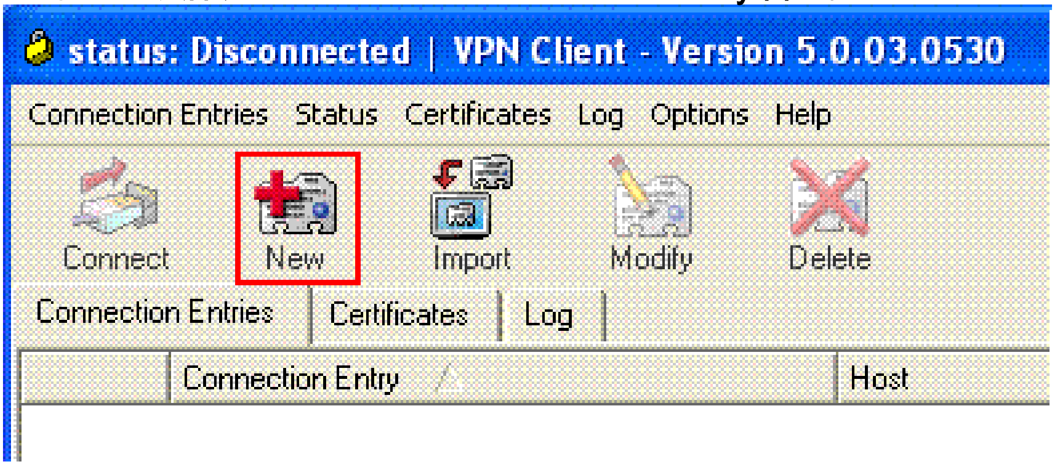
```
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown 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#
```

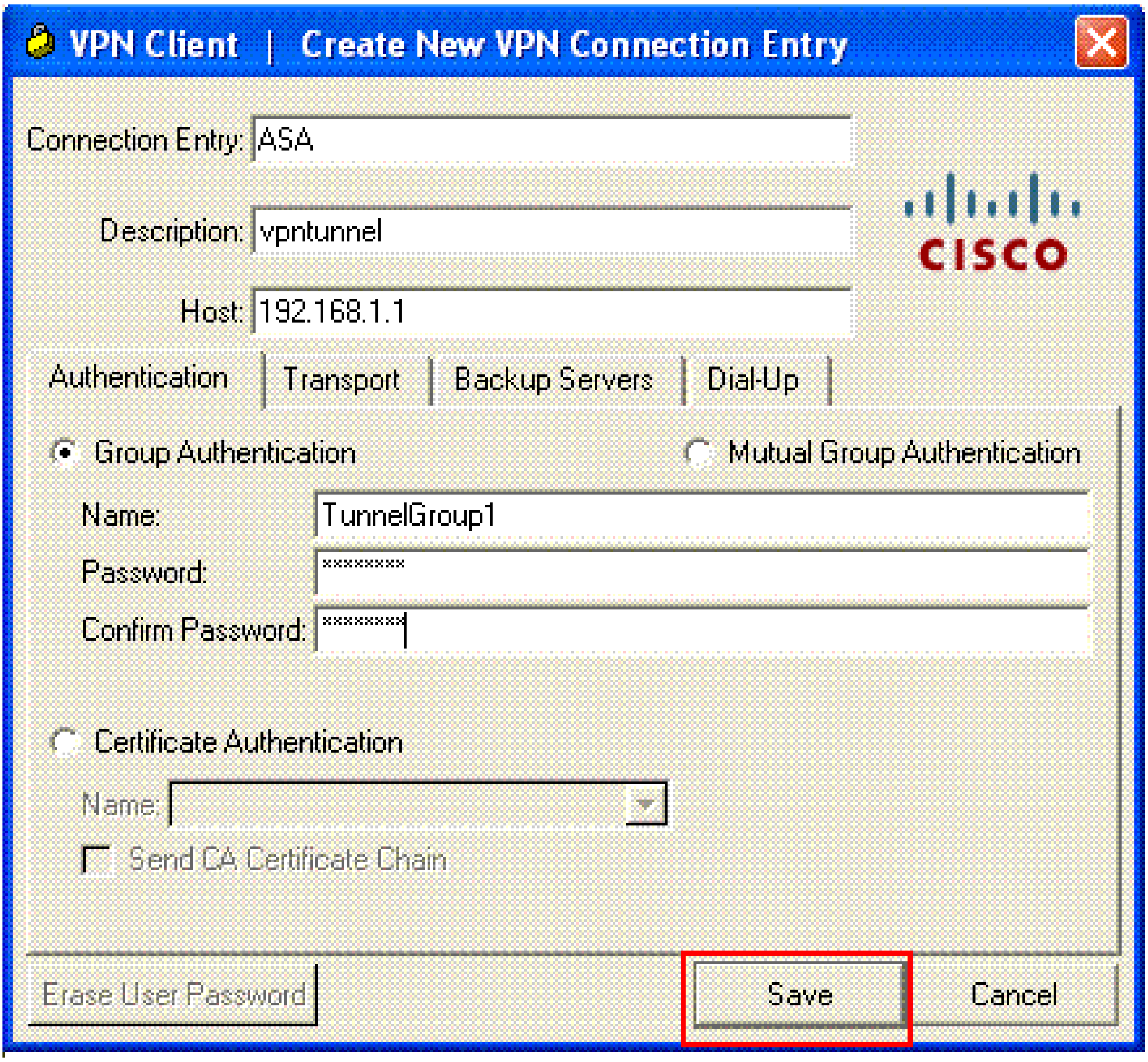
Cisco VPN 客户端配置

尝试使用 Cisco VPN 客户端连接到 Cisco ASA 以验证是否成功配置了 ASA。

1. 选择 **Start > Programs > Cisco Systems VPN Client > VPN Client**。
2. 单击 **New 以启动 Create New VPN Connection Entry 窗口。**



3. 填写新连接的详细信息。输入 Connection Entry 的名称与说明。在 Host 框中输入 **ASA 的外部 IP 地址。**然后输入ASA中配置的VPN隧道组名称(TunnelGroup1)和密码（预共享密钥 — cisco123）。Click



VPN Client | Create New VPN Connection Entry

Connection Entry: ASA

Description: vpntunnel

Host: 192.168.1.1

● Group Authentication ○ Mutual Group Authentication

Name: TunnelGroup1

Password: ********

Confirm Password: ********

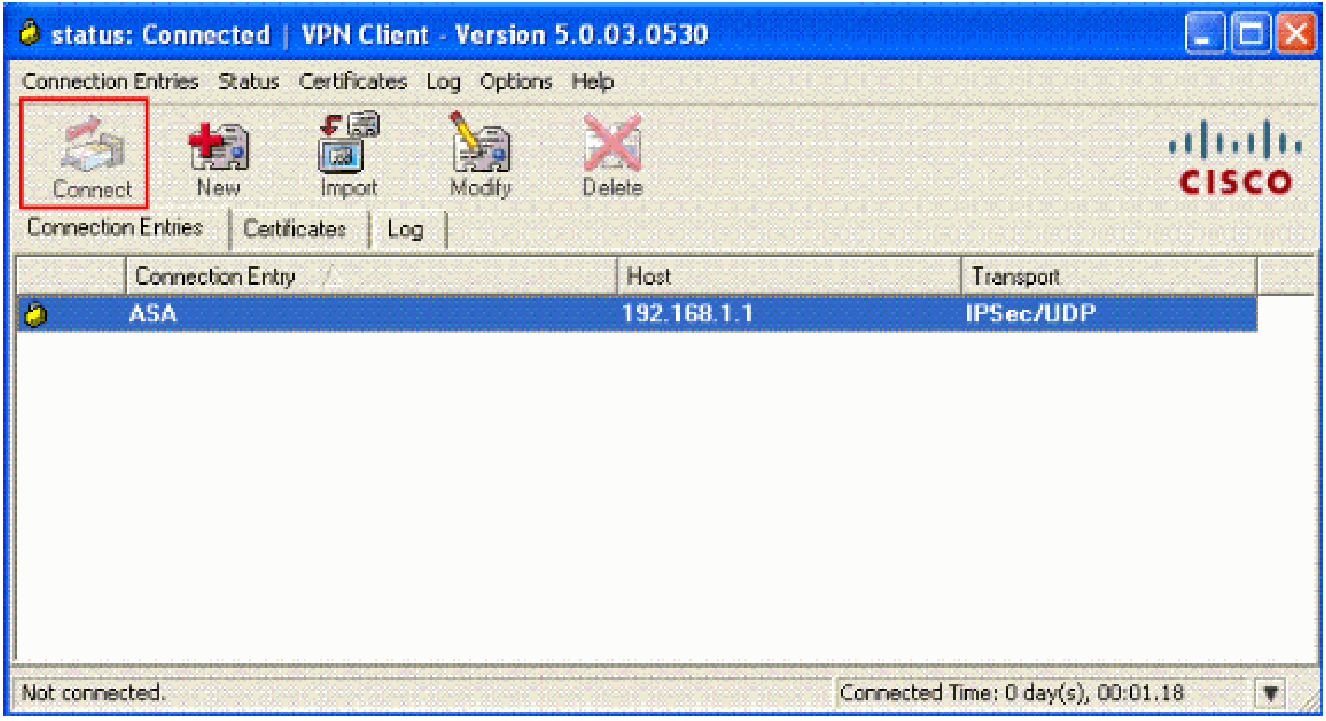
○ Certificate Authentication

Name:

□ Send CA Certificate Chain

Save.

4. 单击要使用的连接，然后在 VPN 客户端主窗口中单击 **Connect。**

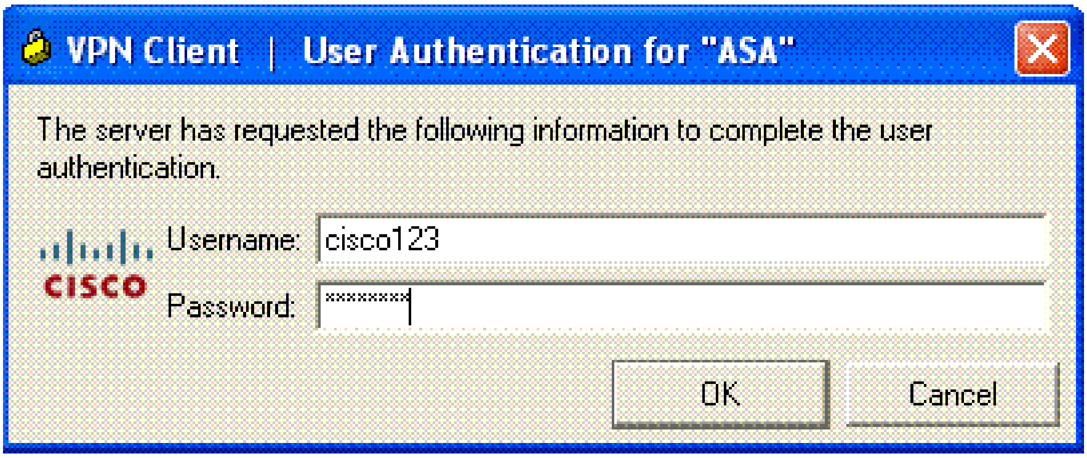


status: Connected | VPN Client - Version 5.0.03.0530

Connection Entry	Host	Transport
ASA	192.168.1.1	IPSec/UDP

Not connected. Connected Time: 0 day(s), 00:01.18

5. 出现提示时，输入 **Username:**cisco123 和 Password:cisco123（按照上面对 ASA 进行的扩展验证配置），然后单击 OK 以连接到远程网络。



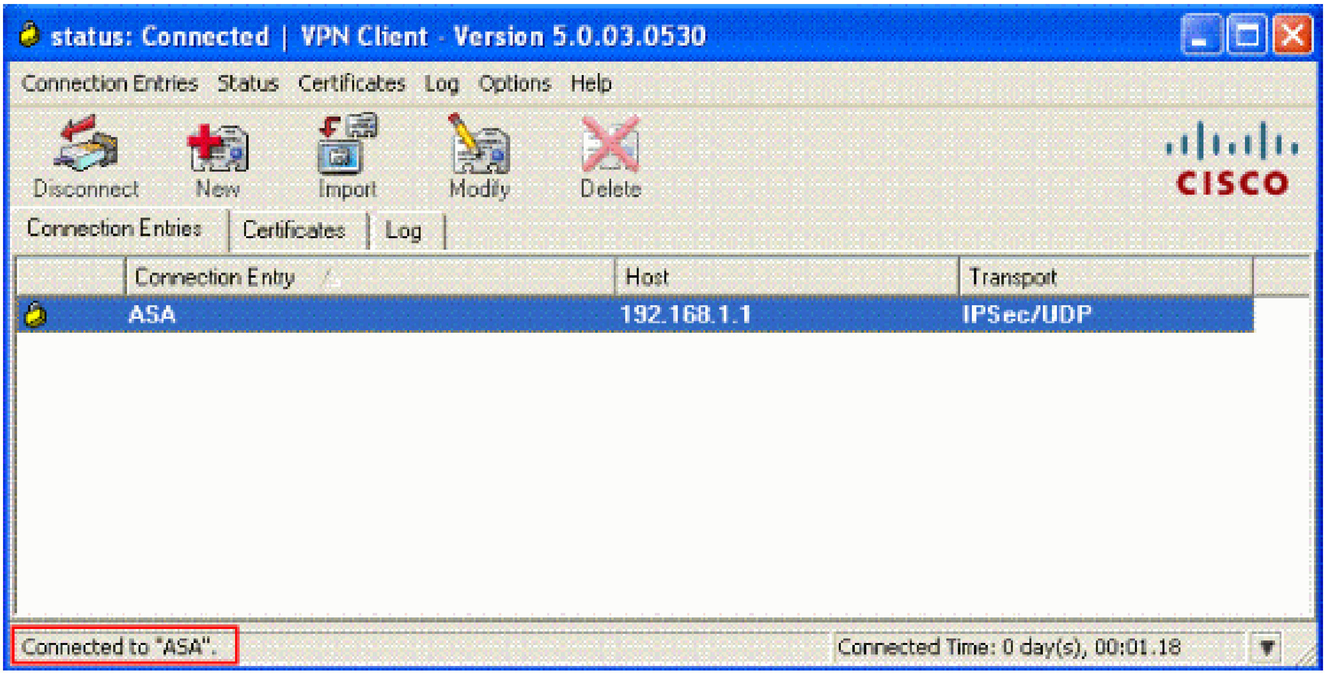
VPN Client | User Authentication for "ASA"

The server has requested the following information to complete the user authentication.

Username: cisco123

Password: ********

6. 现在 VPN 客户端将与中心站点的 ASA 建立连接。



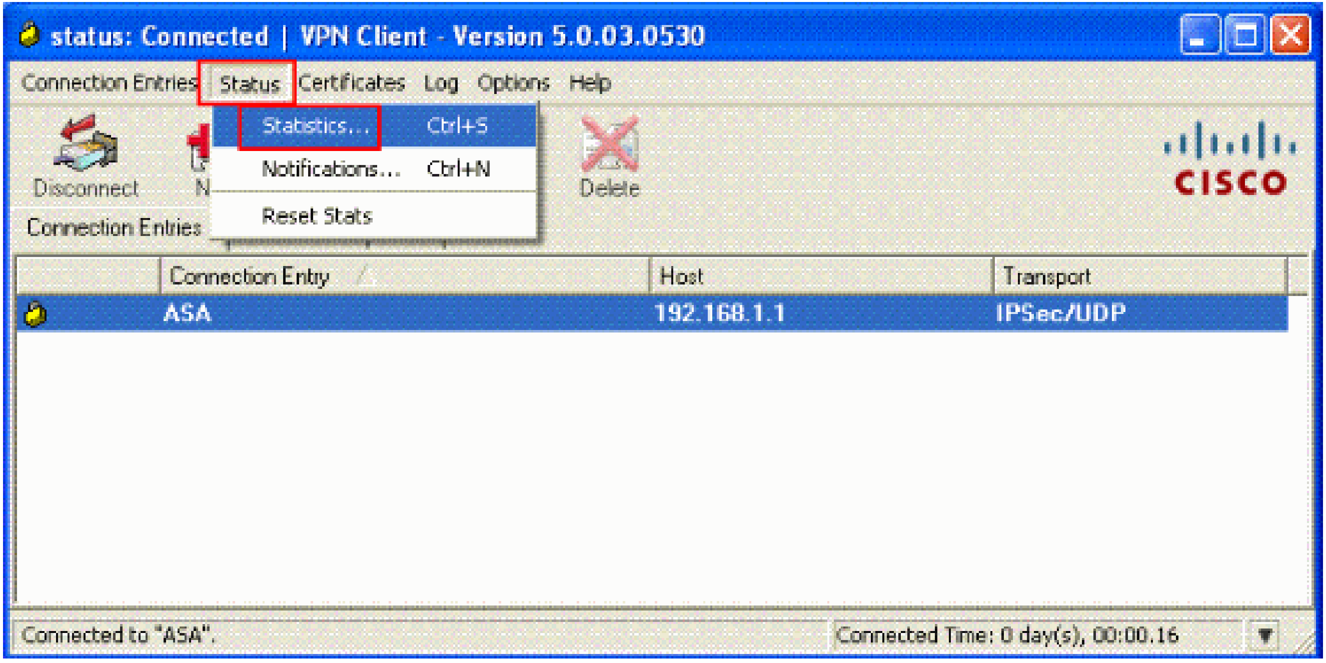
status: Connected | VPN Client - Version 5.0.03.0530

Connection Entry	Host	Transport
ASA	192.168.1.1	IPSec/UDP

Connected to "ASA".

Connected Time: 0 day(s), 00:01.18

7. 成功建立连接后，在 Status 菜单中选择 **Statistics 以验证隧道的详细信息。**



status: Connected | VPN Client - Version 5.0.03.0530

Connection Entry	Host	Transport
ASA	192.168.1.1	IPSec/UDP

Connected to "ASA".

Connected Time: 0 day(s), 00:00.16

验证

显示命令

使用本部分可确定配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto isakmp sa — 显示对等体上的所有当前 IKE 安全关联 (SA)。**
- **show crypto ipsec sa — 显示当前 SA 使用的设置。**

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。此外本部分还提供了 debug 输出示例。

注意：有关排除远程访问IPsec VPN故障的详细信息，请参阅最常见的L2L和远程访问IPSec VPN故障排除解决方案

清除安全关联

进行故障排除时，请务必在做出更改后清除现有的安全关联。在 PIX 的特权模式下，使用以下命令：

- **clear [crypto] ipsec sa - 删除活动 IPsec SA。**关键字 crypto 是可选的。
- **clear [crypto] isakmp sa - 删除活动 IKE SA。**关键字 crypto 是可选的。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关**debug命**令的重要信息。

- **debug crypto ipsec 7 - 显示阶段 2 的 IPsec 协商。**
- **debug crypto isakmp 7 - 显示第 1 阶段的 ISAKMP 协商。**

调试输出示例

- ASA 8.0
- 适用于 Windows 的 VPN 客户端 5.0

ASA 8.0

```
ASA#debug crypto isakmp 7
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message
 (msgid=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, construct
ing xauth V6 VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing dpd vid payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing Fragmentation VID + extended capabilities payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Alti
ga/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 le
ngth : 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, processin
g 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, processin
g notify payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
g 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, processin
g 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, construct
ing blank hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing qm hash payload
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a
1816d) 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=e8
a1816d) 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_a
ttr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
```

```
g MODE_CFG Reply attributes.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: primary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: secondary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: primary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: secondary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: IP Compression = disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, 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 = 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, 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
63a1dd) 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
```

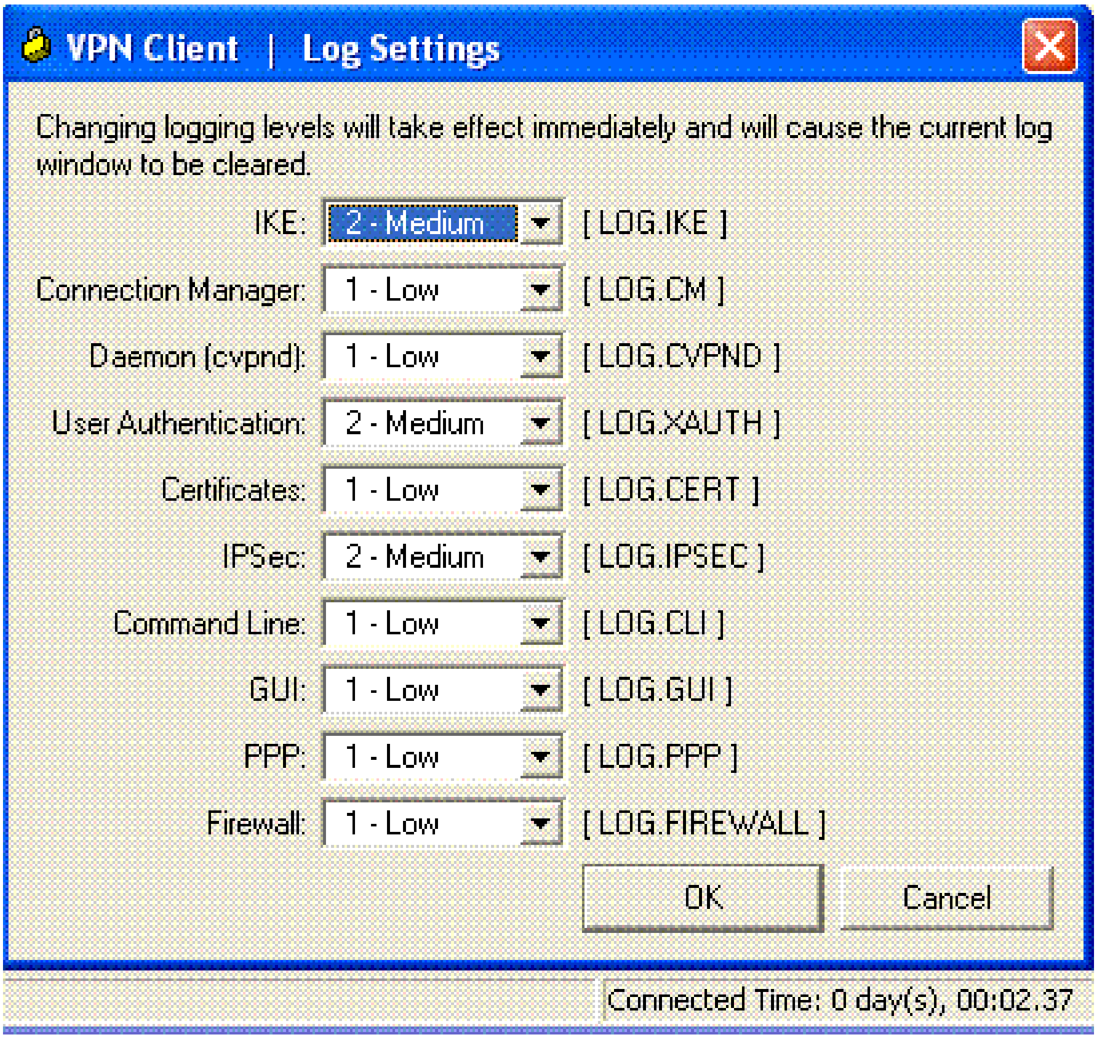
```
.1.2, Received unknown transaction mode attribute: 28684
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Application Version!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Client Type: 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=266
3a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, 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 = 1
92.168.1.2, Starting P1 rekey timer: 950 seconds.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, sending notify message
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, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f44
35669) 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=54
1f8e43) 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 = 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, processing SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, 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, Proto
col 0, Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, 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 = 1
92.168.1.2, processing IPSec SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IPSec SA Proposal # 14, Transform # 1 acceptable  Matches global IPS
ec 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 = 1
92.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, oakley constucting quick mode
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, 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 secon
ds
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing IPSec nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, 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
```

适用于 Windows 的 VPN 客户端 5.0

选择 Log > Log settings 以便在 VPN 客户端中启用日志级别。



Changing logging levels will take effect immediately and will cause the current log window to be cleared.

IKE: 2 - Medium [LOG.IKE]

Connection Manager: 1 - Low [LOG.CM]

Daemon (cvpnd): 1 - Low [LOG.CVPND]

User Authentication: 2 - Medium [LOG.XAUTH]

Certificates: 1 - Low [LOG.CERT]

IPSec: 2 - Medium [LOG.IPSEC]

Command Line: 1 - Low [LOG.CLI]

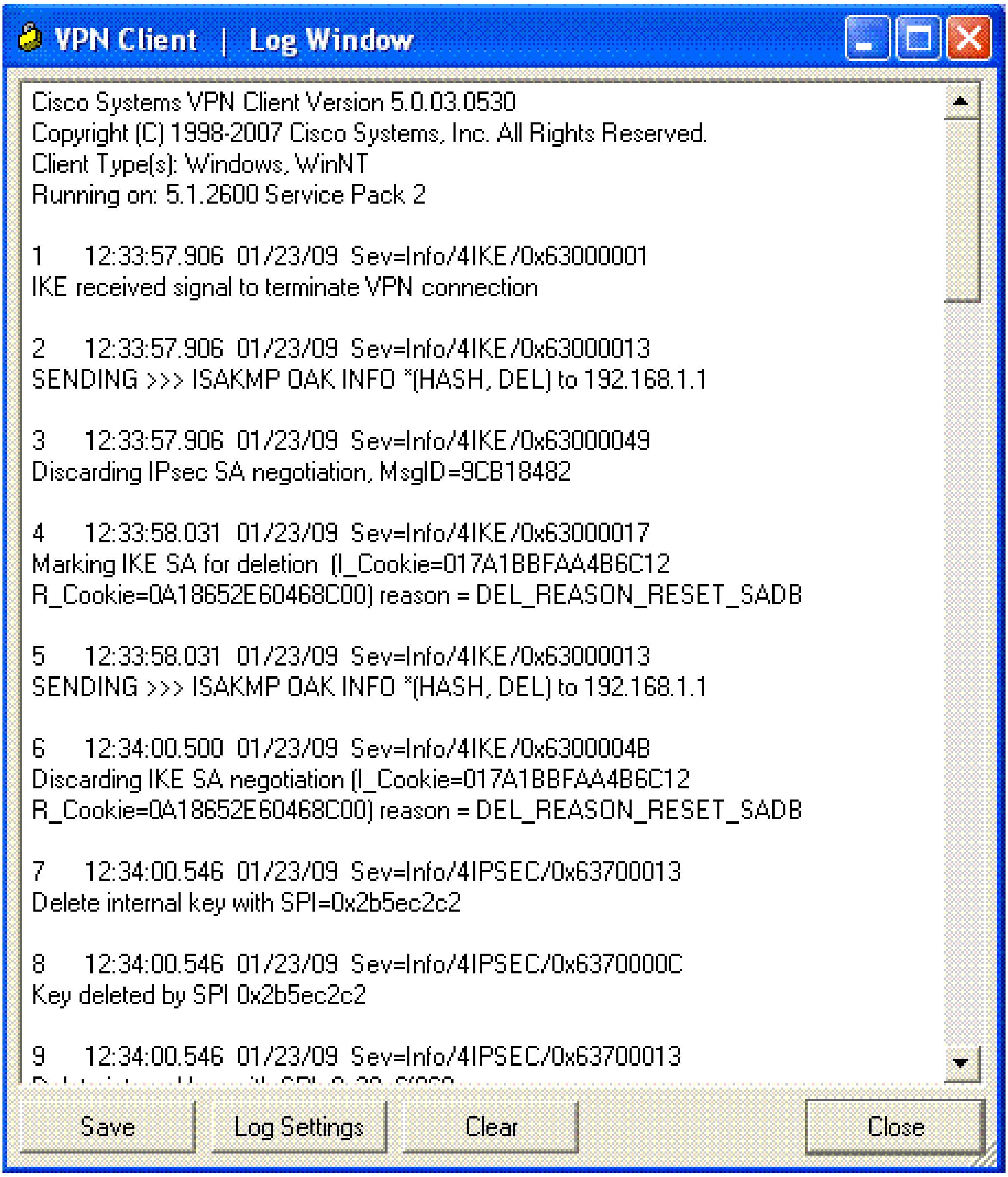
GUI: 1 - Low [LOG.GUI]

PPP: 1 - Low [LOG.PPP]

Firewall: 1 - Low [LOG.FIREWALL]

Connected Time: 0 day(s), 00:02.37

选择 **Log > Log Window 以查看 VPN 客户端中的日志项。**



```
Cisco Systems VPN Client Version 5.0.03.0530
Copyright (C) 1998-2007 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      12:33:57.906  01/23/09  Sev=Info/4IKE/0x63000001
IKE received signal to terminate VPN connection

2      12:33:57.906  01/23/09  Sev=Info/4IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 192.168.1.1

3      12:33:57.906  01/23/09  Sev=Info/4IKE/0x63000049
Discarding IPsec SA negotiation, MsgID=9CB18482

4      12:33:58.031  01/23/09  Sev=Info/4IKE/0x63000017
Marking IKE SA for deletion  (I_Cookie=017A1BBFAA4B6C12
R_Cookie=0A18652E60468C00) reason = DEL_REASON_RESET_SADB

5      12:33:58.031  01/23/09  Sev=Info/4IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 192.168.1.1

6      12:34:00.500  01/23/09  Sev=Info/4IKE/0x6300004B
Discarding IKE SA negotiation (I_Cookie=017A1BBFAA4B6C12
R_Cookie=0A18652E60468C00) reason = DEL_REASON_RESET_SADB

7      12:34:00.546  01/23/09  Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2b5ec2c2

8      12:34:00.546  01/23/09  Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2b5ec2c2

9      12:34:00.546  01/23/09  Sev=Info/4IPSEC/0x63700013
```

相关信息

- Cisco ASA 5500 系列自适应安全设备支持页
- Cisco ASA 5500 系列自适应安全设备命令参考
- Cisco PIX 500 系列安全设备支持页
- Cisco PIX 500 系列安全设备命令参考
- Cisco 自适应安全设备管理器
- IPsec协商/IKE协议支持页