

ASA/PIX 8.x : RADIUS授权(ACS 4.x) VPN访问的使用与CLI和ASDM配置示例的可下载的ACLs

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](#)

[为适用于个人用户的可下载 ACL 配置 ACS](#)

[为适用于组的可下载 ACL 配置 ACS](#)

[为用户组配置 IETF RADIUS 设置](#)

[验证](#)

[显示 Crypto 命令](#)

[适用于用户/组的可下载 ACL](#)

[Filter-Id ACL](#)

[故障排除](#)

[清除安全关联](#)

[故障排除命令](#)

[相关信息](#)

简介

本文档将说明如何配置安全设备针对网络访问对用户进行身份验证。因为 RADIUS 授权可以隐式启用，所以本部分未包含有关在安全设备上配置 RADIUS 授权的信息。本部分提供的是有关安全设备如何处理从 RADIUS 服务器接收的访问列表信息的信息。

可以将 RADIUS 服务器配置为下载访问列表到安全设备或在身份验证时下载访问列表名称。用户获得授权仅可执行用户特定访问列表中所允许的操作。

在使用 Cisco Secure ACS 为每位用户提供相应的访问列表时，可下载访问列表是最具扩展性的方法。有关可下载访问列表功能和 Cisco Secure ACS 的详细信息，请参阅[将 RADIUS 服务器配置为发送可下载访问控制列表](#)和[可下载 IP ACL](#)。

请参阅 [ASA 8.3及以上版本：RADIUS授权\(ACS 5.x\) VPN访问的使用与CLI和ASDM配置示例的可下载的ACLs](#)在Cisco ASA的相同配置的与版本8.3和以上。

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 [允许对 ASDM 进行 HTTPS 访问](#)或 [PIX/ASA 7.x：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
- Cisco 自适应安全设备管理器版本 5.x 及更高版本
- Cisco VPN 客户端 4.x 及更高版本
- Cisco 安全访问控制服务器 4.x

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

您可以使用可下载 IP ACL 创建能够应用于多个用户或用户组的 ACL 定义集。这些 ACL 定义集称为 ACL 内容。并且在整合 NAF 时，将对发送到 AAA 客户端（用户从中寻求访问）的 ACL 内容进行控制。也就是说，一个可下载 IP ACL 包含一个或多个 ACL 内容定义，每个内容定义又与一个 NAF 关联或（在默认情况下）与所有 AAA 客户端关联。NAF 根据 AAA 客户端的 IP 地址控制指定 ACL 内容的适用性。有关 NAF 及其如何调控可下载 IP ACL 的详细信息，请参阅[关于网络访问过滤器](#)。

可下载 IP ACL 的运行方式如下：

1. 当 ACS 授予用户访问网络的权限时，ACS 确定将可下载 IP ACL 分配给该用户还是该用户所在的组。
2. 如果找到某个已分配给用户或用户所在组的可下载 IP ACL，ACS 将确定 ACL 内容条目是否已与发送 RADIUS 身份验证请求的 AAA 客户端相关联。
3. 作为用户会话的一部分，ACS 将发送 RADIUS 访问接受数据包、指定已命名 ACL 的属性以及已命名 ACL 的版本。

4. 如果 AAA 客户端响应其缓存中没有当前版本的 ACL，即该 ACL 是新的或已发生更改，则 ACS 会将该 ACL（新的或已更新的）发送到设备。

可下载 IP ACL 是每个用户或用户组的 RADIUS Cisco cisco-av-pair 属性 [26/9/1] 中的替代 ACL 配置。您可以一次创建一个可下载 IP ACL 并为其指定名称，然后引用可下载 IP ACL 的名称以将其分配给每个适用的用户或用户组。相比于为每个用户或用户组配置 RADIUS Cisco cisco-av-pair 属性，该方法的效率更高。

而且在使用 NAF 时，您可以根据其所使用的 AAA 客户端将不同的 ACL 内容应用于相同的用户或包含多个用户的组。将 AAA 客户端配置为使用来自 ACS 的可下载 IP ACL 后，无需再对 AAA 客户端进行其他配置。可下载 ACL 受已建立的备份或复制方案保护。

在 ACS Web 界面中输入 ACL 定义时，请勿使用关键字或名称条目；在其他所有方面，请对计划应用可下载 IP ACL 的 AAA 客户端使用标准 ACL 命令语法和语义。输入 ACS 中的 ACL 定义包含一个或多个 ACL 命令。每个 ACL 命令必须独占一行。

您可以将一个或多个已命名 ACL 内容添加到可下载 IP ACL 中。默认情况下，每个 ACL 内容适用于所有 AAA 客户端，但如果定义了 NAF，则可以限制每个 ACL 内容应用于 NAF 中所列的与其相关联的 AAA 客户端。也就是说，在使用 NAF 时，可以根据网络安全策略，使单个可下载 IP ACL 中的每个 ACL 内容适用于多个不同的网络设备或网络设备组。

并且，您可以更改可下载 IP ACL 中 ACL 内容的顺序。ACS 将从表的顶端开始检查 ACL 内容，并会下载第一个 NAF 包含所用 AAA 客户端的 ACL 内容。在设置顺序时，如果将适用范围最广的 ACL 内容置于列表中的较高位置，则可以确保系统效率。您必须认识到，如果 NAF 中包括重叠的 AAA 客户端，则必须按照从更具体到更普遍的顺序进行操作。例如，ACS 将下载所有包含 All-AAA-Clients NAF 设置的 ACL 内容，而不会考虑任何处于列表中较低部分的内容。

要在特定的 AAA 客户端上使用可下载 IP ACL，AAA 客户端必须遵循以下说明：

- 使用 RADIUS 进行身份验证
- 支持可下载 IP ACL

以下是支持可下载 IP ACL 的 Cisco 设备示例：

- ASA 和 PIX 设备
- VPN 3000 系列集中器
- 运行 IOS 版本 12.3(8)T 或更高版本的 Cisco 设备

以下是在 ACL Definitions 框中输入 VPN 3000/ASA/PIX 7.x+ ACL 所必须使用的格式示例：

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

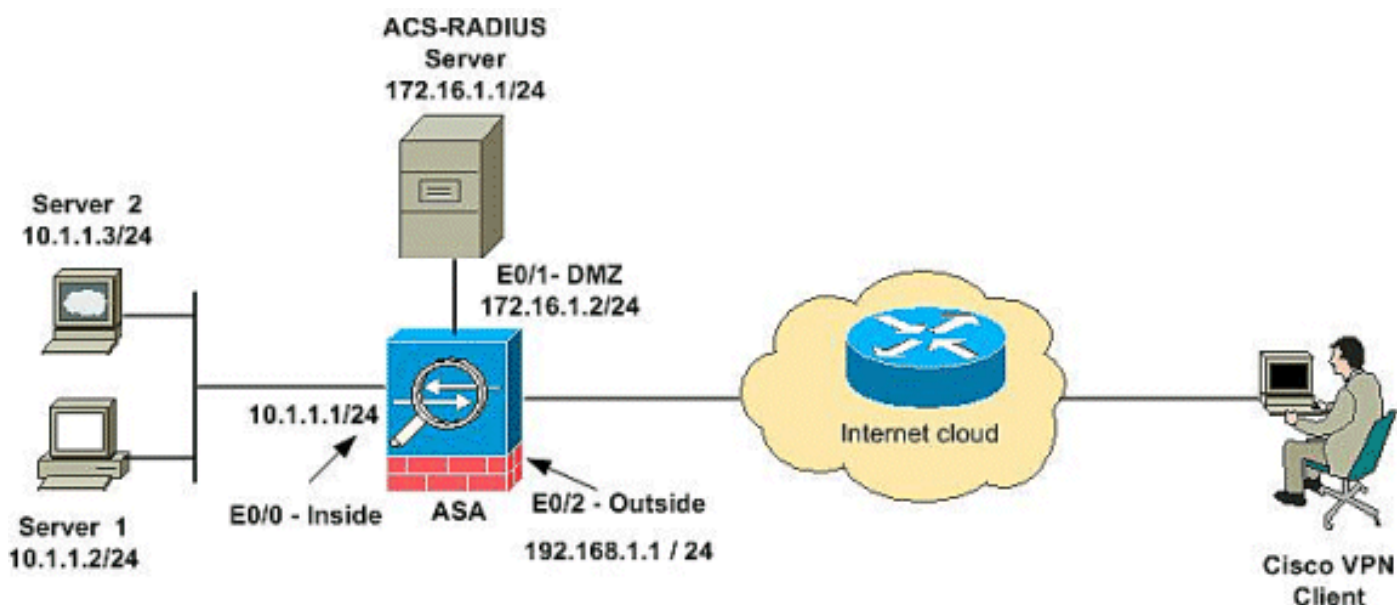
配置

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](#)（[仅限注册用户](#)）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



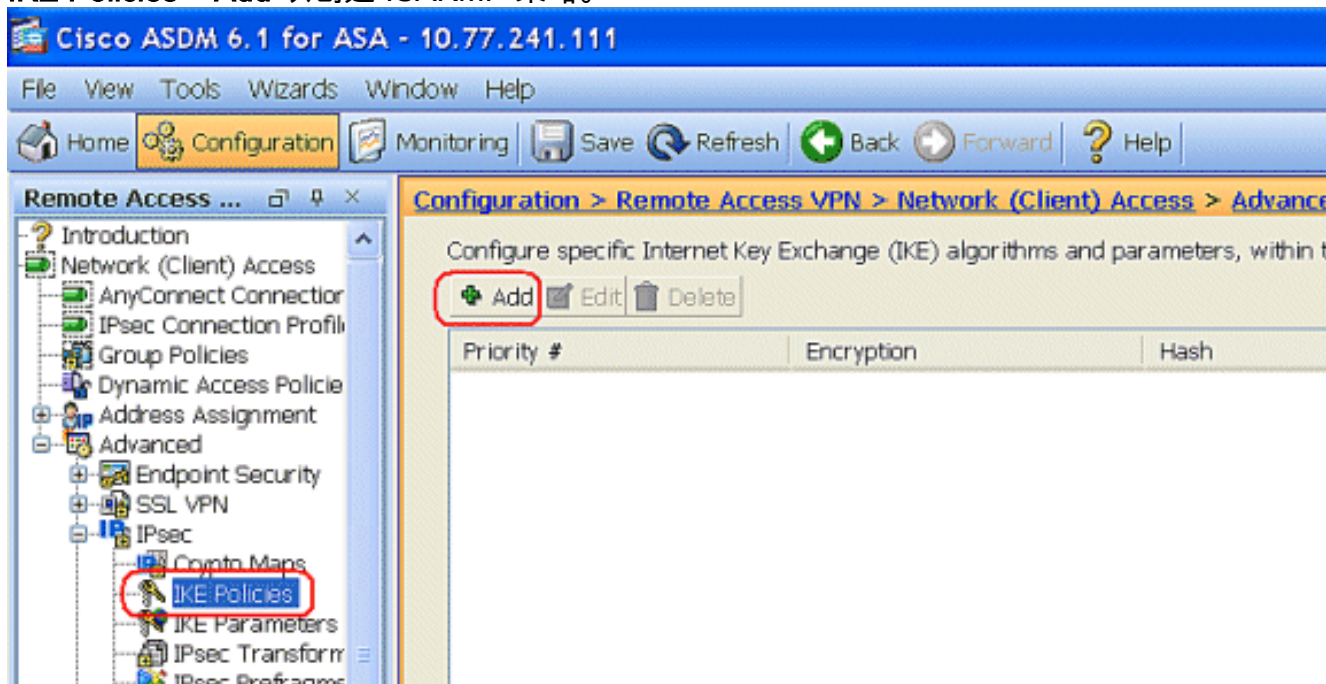
注意：此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

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. 提供 ISAKMP 策略详细信息，如下所示。

Add IKE Policy

Priority: Authentication:

Encryption: D-H Group:

Hash: Lifetime: Unlimited 86400

单击 OK，然后单击 Apply。

3. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters** 以启用外部接口上的 IKE。

Cisco ASDM 6.1 for ASA - 10.77.241.111

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access ...

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters

Interface	IKE Enabled
dmz	No
inside	No
outside	Yes

Enable IKE

Enable IPsec over NAT-T
NAT Keepalive: seconds

Enable IPsec over TCP
Enter up to 10 comma-separated TCP port values (1- 65535):

Identity to Be Sent to Peer

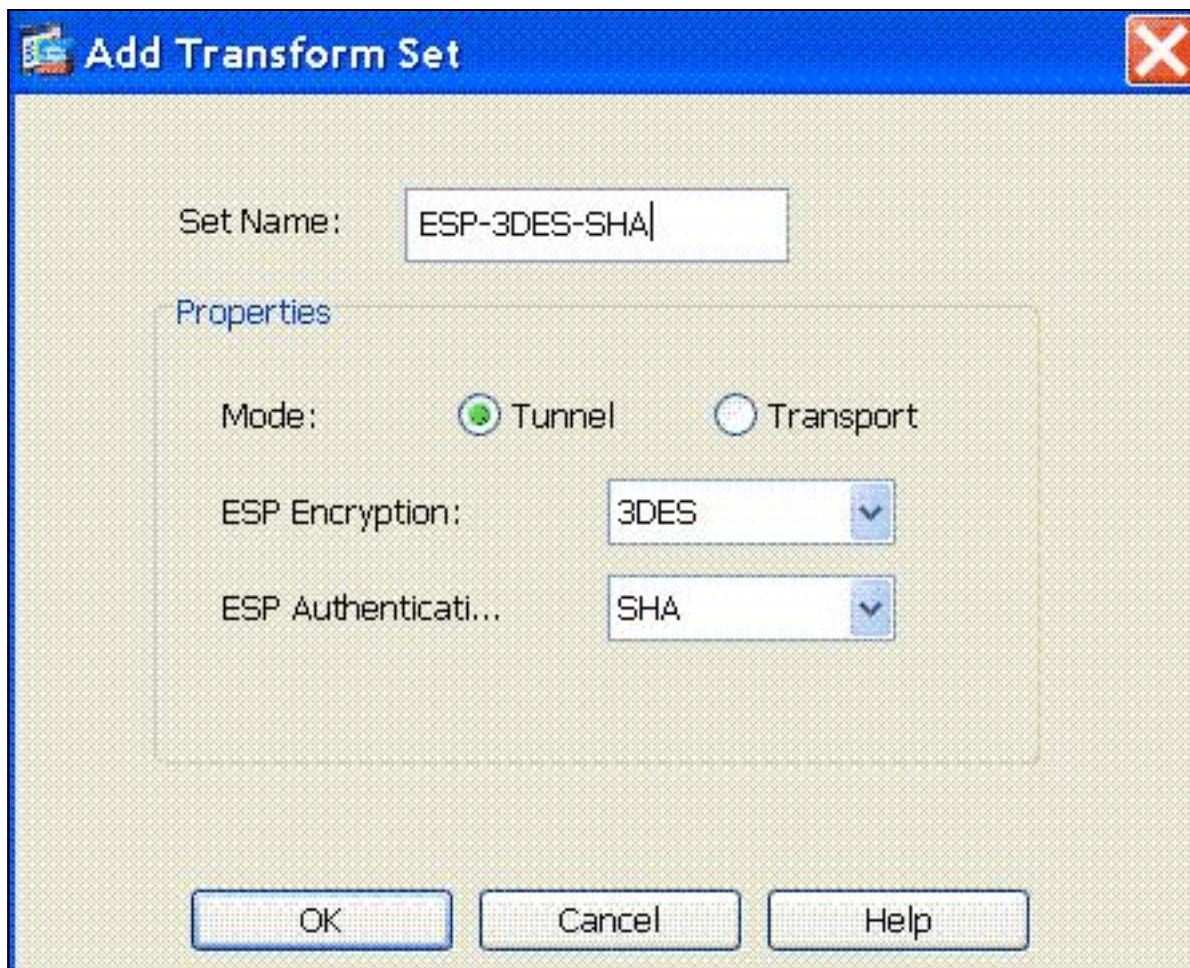
Identity: Key Id String:

Disable inbound aggressive mode connections

Alert peers before disconnecting

Wait for all active sessions to voluntarily terminate before rebooting

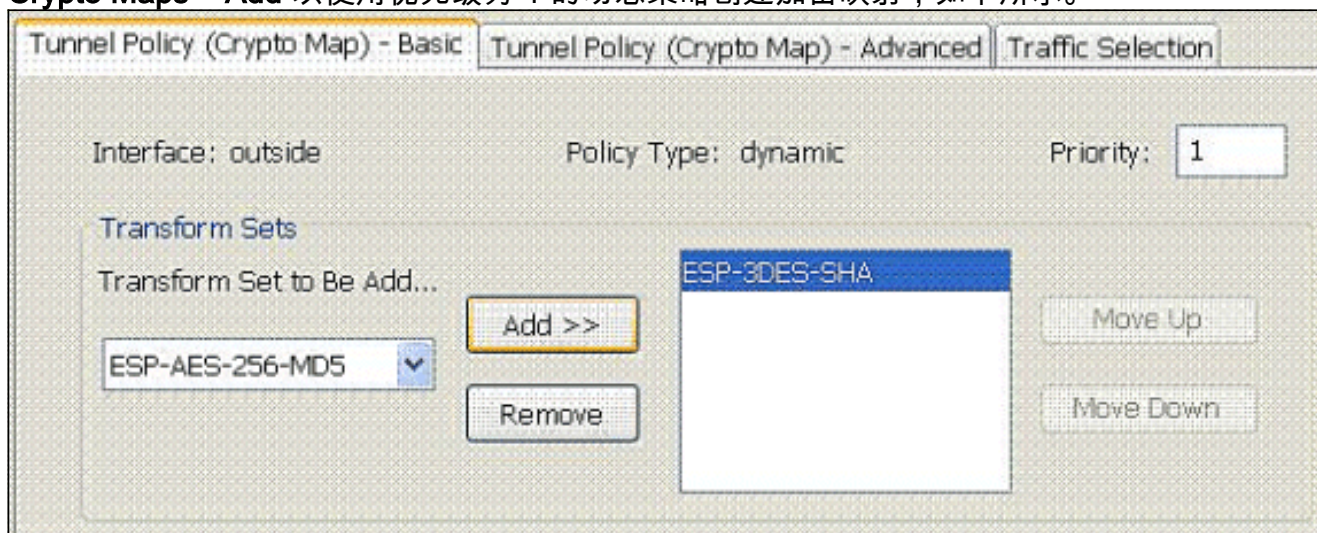
4. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IPsec Transform Sets > Add** 以创建 ESP-3DES-SHA 转换集，如下所示。



单击

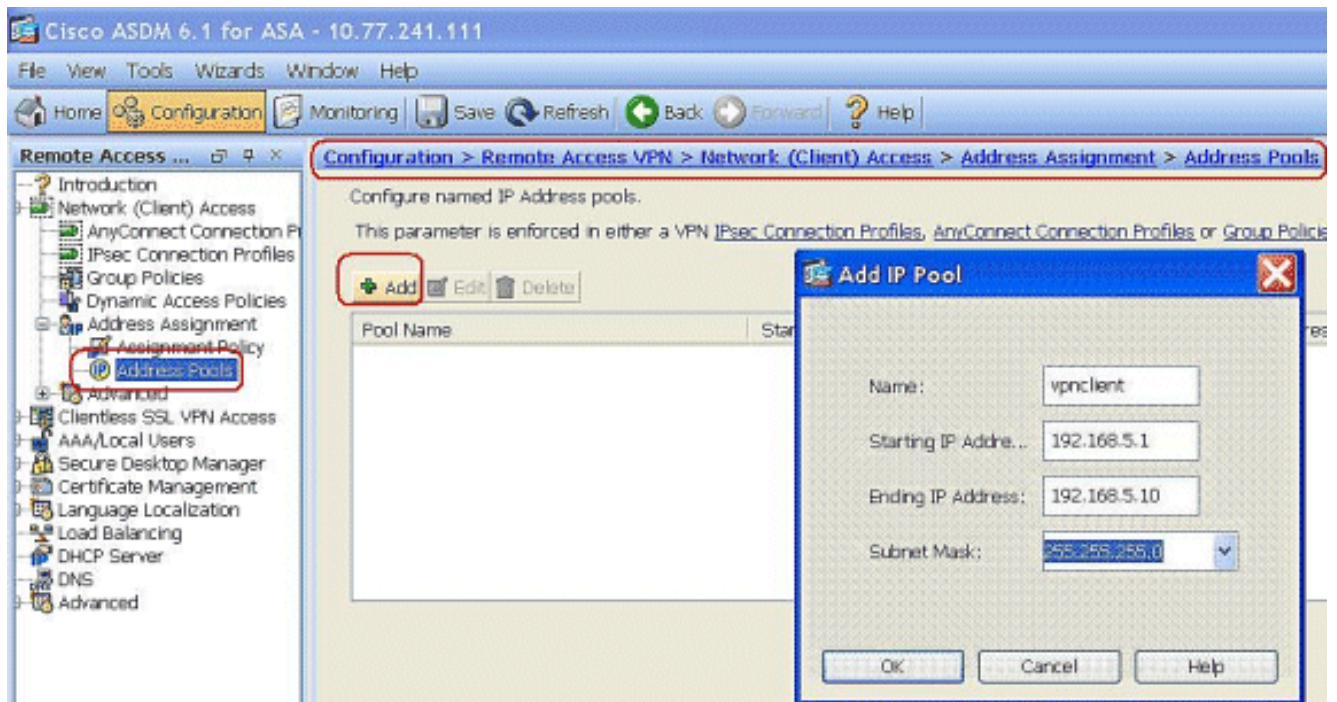
OK，然后单击 Apply。

5. 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。

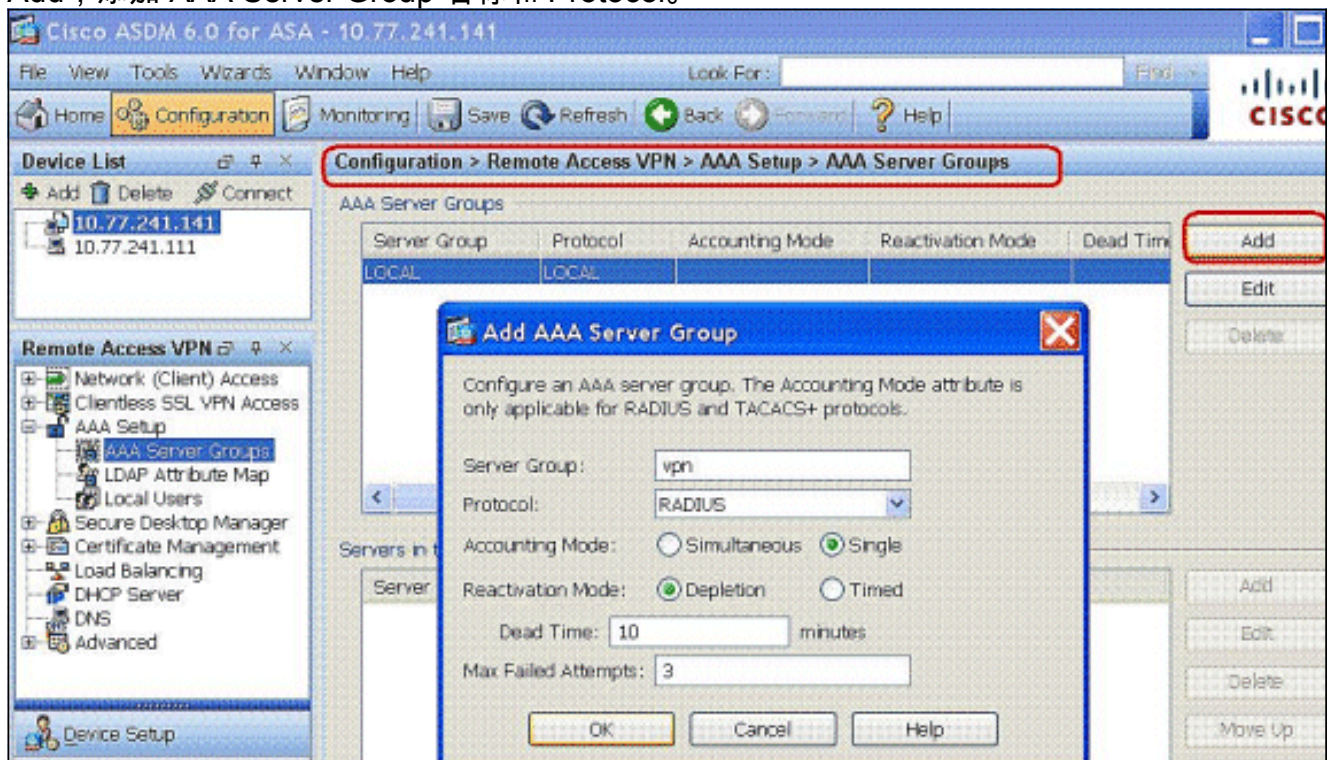


单击 OK，然后单击 Apply。

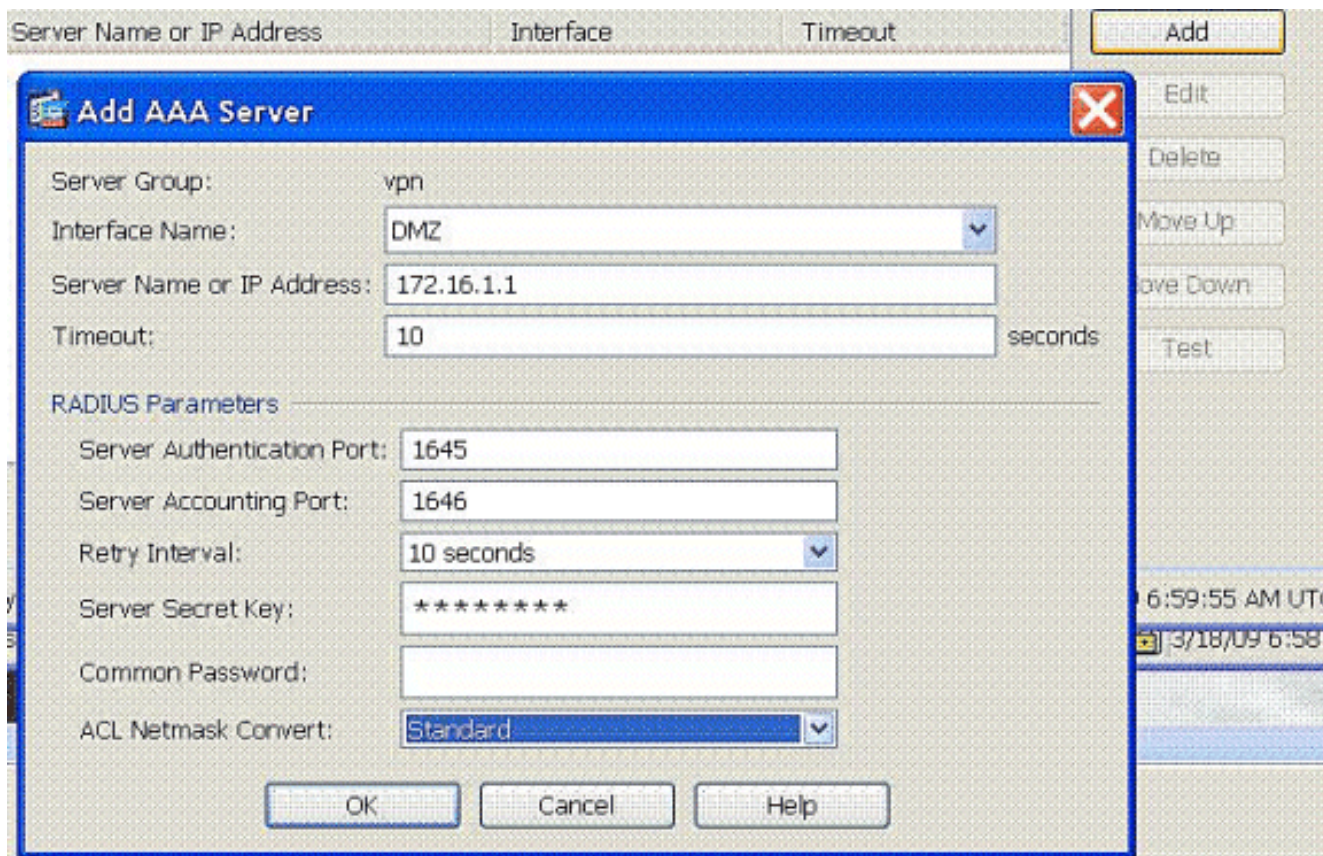
6. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools** 并单击 Add，为 VPN 客户端用户添加 VPN 客户端。



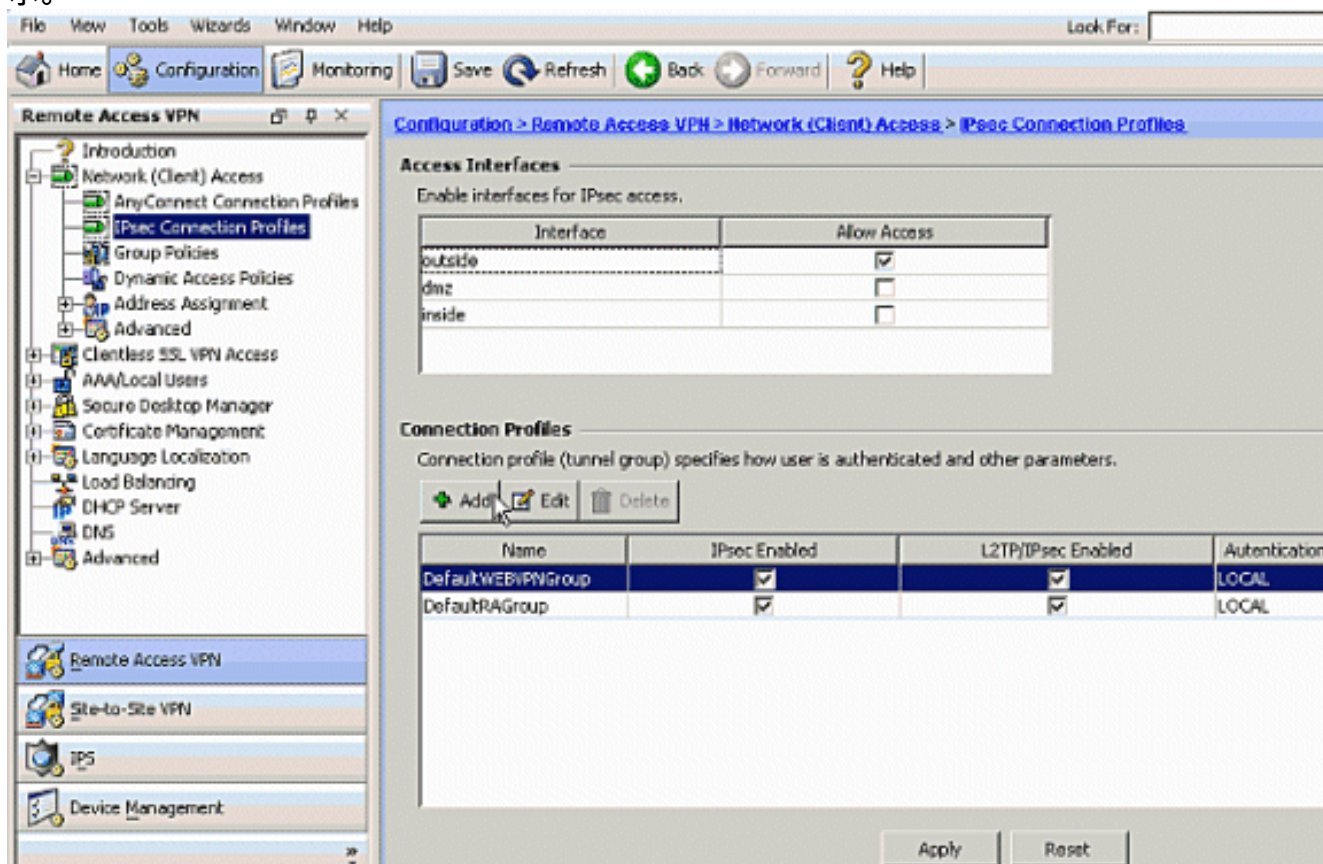
7. 选择 Configuration > Remote Access VPN > AAA Setup > AAA Server Groups 并单击 Add，添加 AAA Server Group 名称和 Protocol。



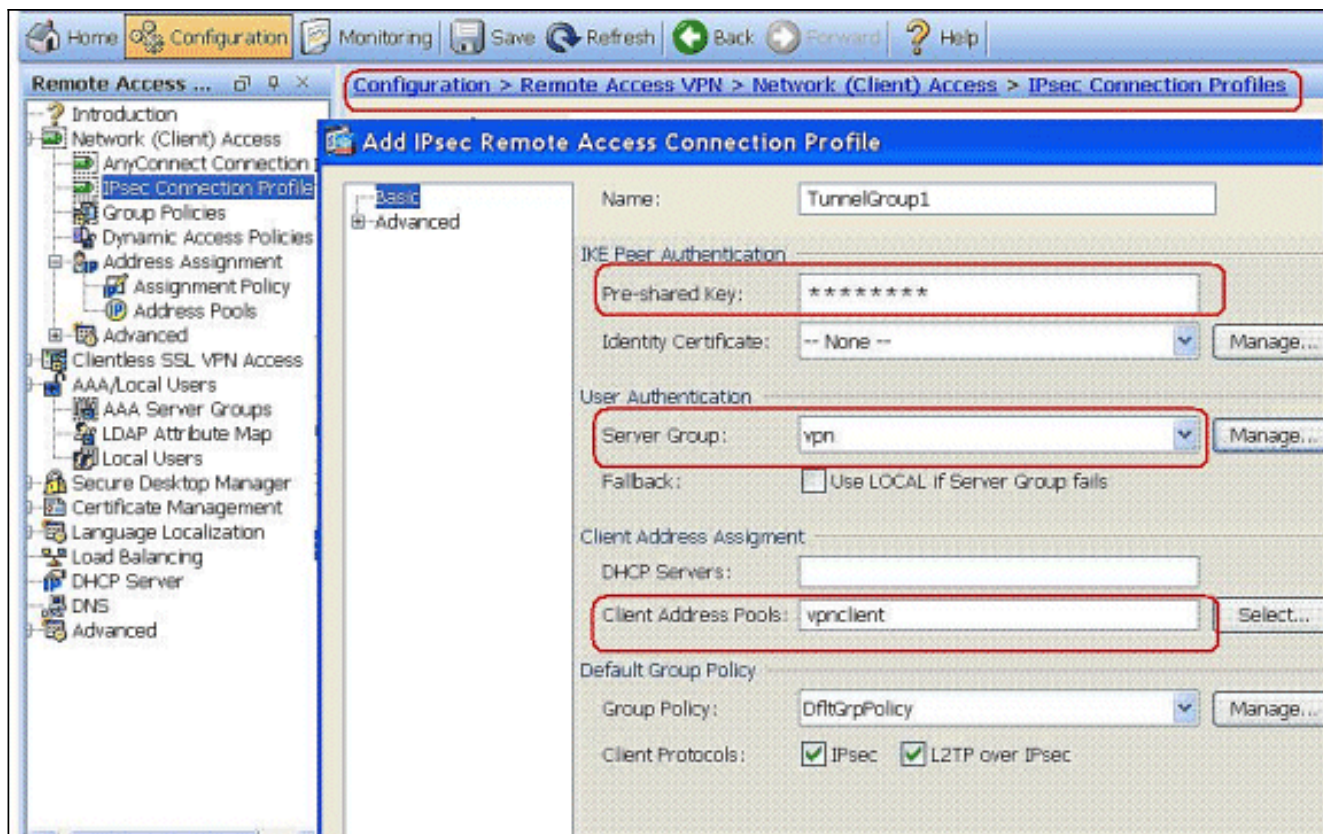
添加 AAA 服务器 IP 地址 (ACS) 及其连接的接口。并添加 RADIUS Parameters 区域中的 Server Secret Key。单击 Ok。



8. 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。

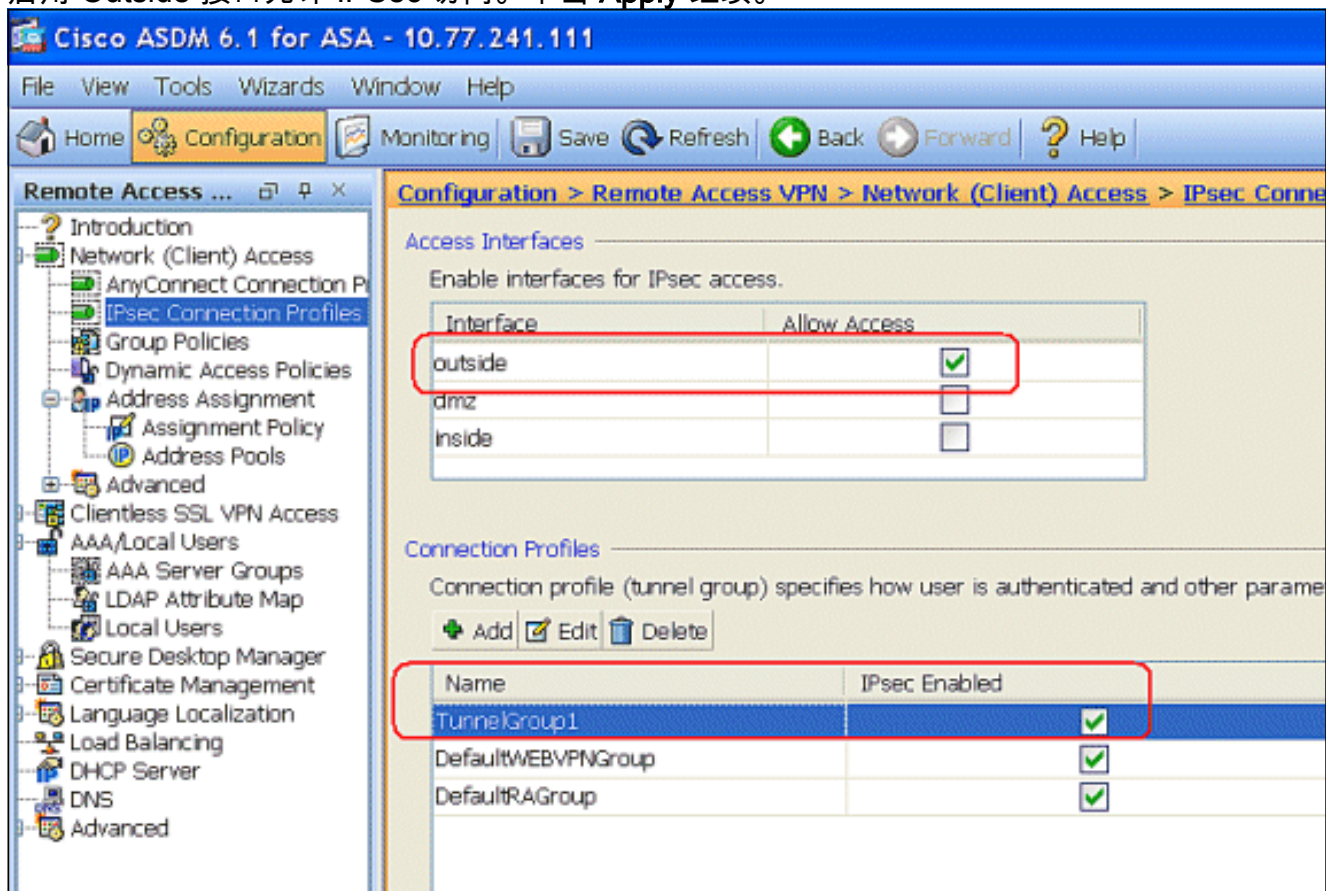


在 Basic 选项卡下，为 User Authentication 字段选择 **vpn** 作为 Server Group。为 VPN 客户端用户选择 **vpnclient** 作为 Client Address Pools。



单击 Ok。

9. 启用 Outside 接口允许 IPsec 访问。单击 Apply 继续。



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](#)。

ASA 设备上的运行配置

```
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 DMZ security-level 100 ip
address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.1
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 !---
Radius Attribute Filter access-list new extended deny ip
any host 10.1.1.2 access-list new extended permit ip any
any pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.1-192.168.5.10
mask 255.255.255.0 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
(outside) 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 !---
Create the AAA server group "vpn" and specify the
protocol as RADIUS. !--- Specify the CSACS server as a
member of the "vpn" group and provide the !--- location
and key. aaa-server vpn protocol radius max-failed-
attempts 5 aaa-server vpn (DMZ) host 172.16.1.1 retry-
interval 1 timeout 30 key cisco123 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 !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. !--- A Triple DES encryption with !---
the sha hash algorithm is used. crypto ipsec transform-
set ESP-3DES-SHA esp-3des esp-sha-hmac !--- Defines a
dynamic crypto map with !--- the specified encryption
settings. crypto dynamic-map outside_dyn_map 1 set
transform-set ESP-3DES-SHA !--- Binds the dynamic map to
the IPsec/ISAKMP process. 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 3des hash sha group 2 lifetime 86400 no
crypto isakmp nat-traversal telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection basic-threat
```



```

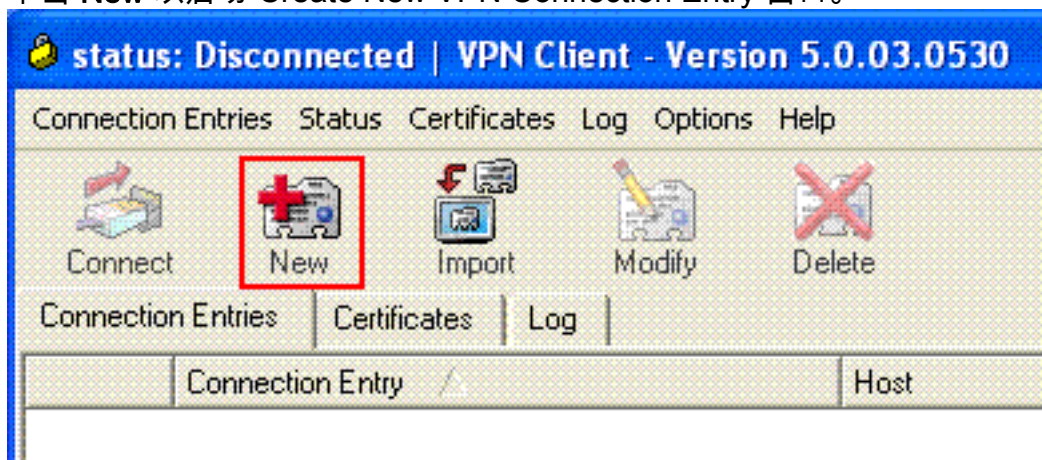
threat-detection statistics access-list ! class-map
inspection_default match default-inspection-traffic !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtip inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
! group-policy DfltGrpPolicy attributes vpn-tunnel-
protocol IPsec webvpn group-policy GroupPolicy1 internal
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (VPN) with the tunnel group. tunnel-group
TunnelGroup1 type remote-access tunnel-group
TunnelGroup1 general-attributes address-pool vpnclient
authentication-server-group vpn !--- 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#

```

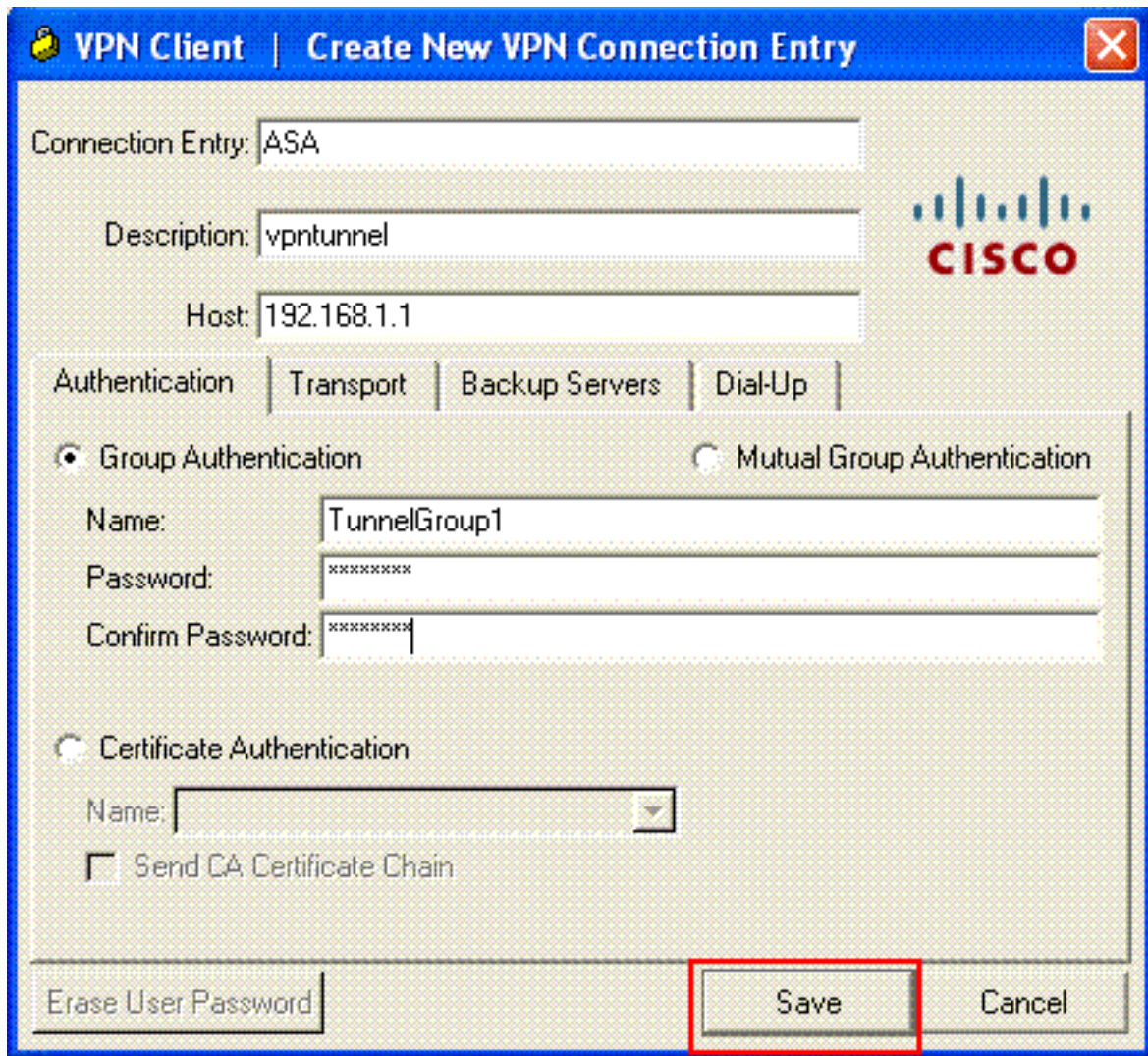
Cisco VPN 客户端配置

尝试使用 Cisco VPN 客户端连接到 Cisco ASA，以便验证是否已成功配置 ASA。

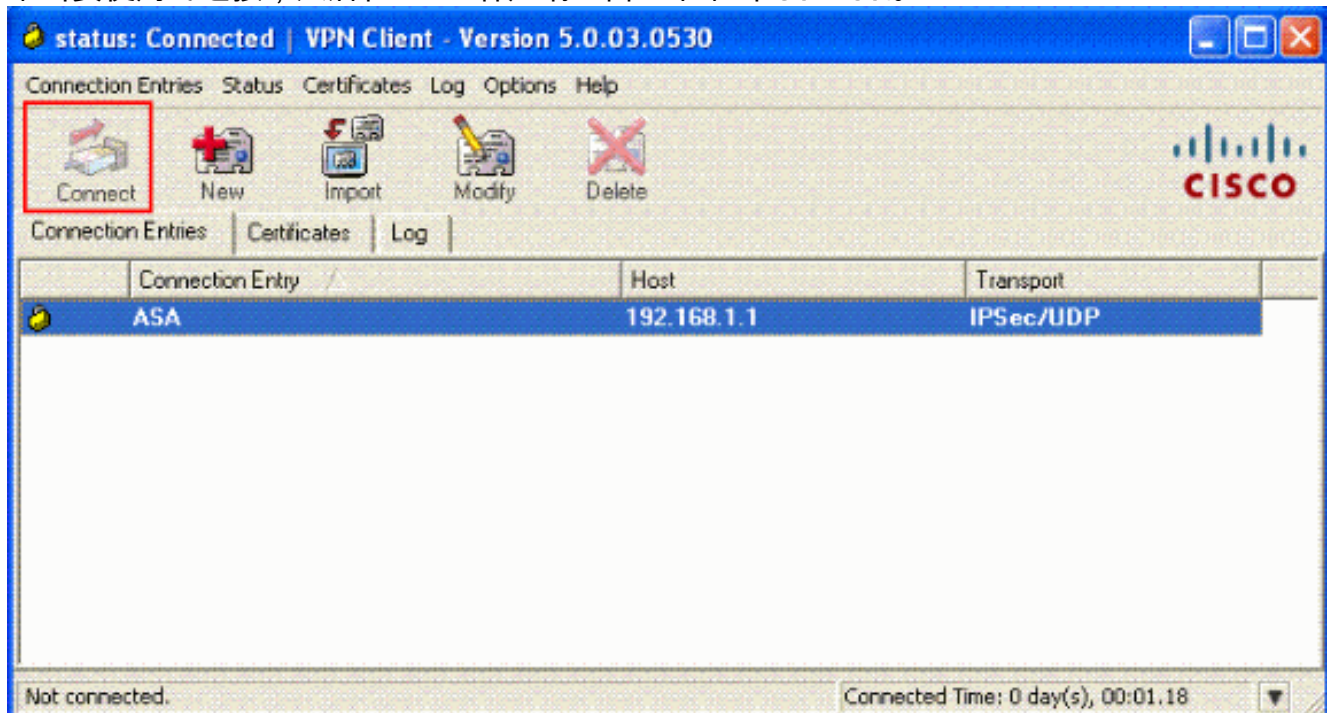
1. 选择开始 > 程序 > Cisco Systems VPN 客户端 > VPN 客户端。
2. 单击 **New** 以启动 Create New VPN Connection Entry 窗口。



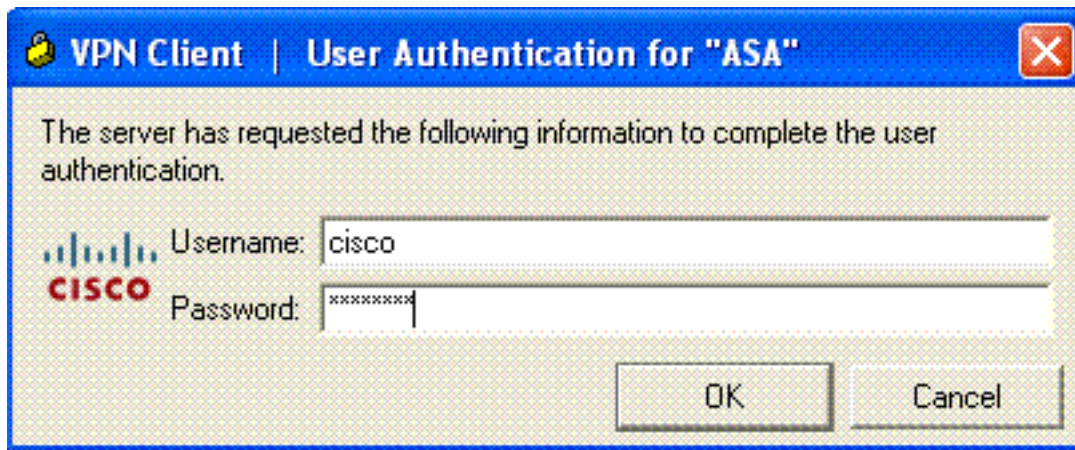
3. 填写新连接的详细信息。输入 Connection Entry 的名称与说明。在 Host 框中输入 **ASA 的外部 IP 地址**。然后按照 ASA 中的配置输入 VPN 隧道组名称 (TunnelGroup1) 和口令 (预共享密钥 - cisco123)。单击 **Save**。



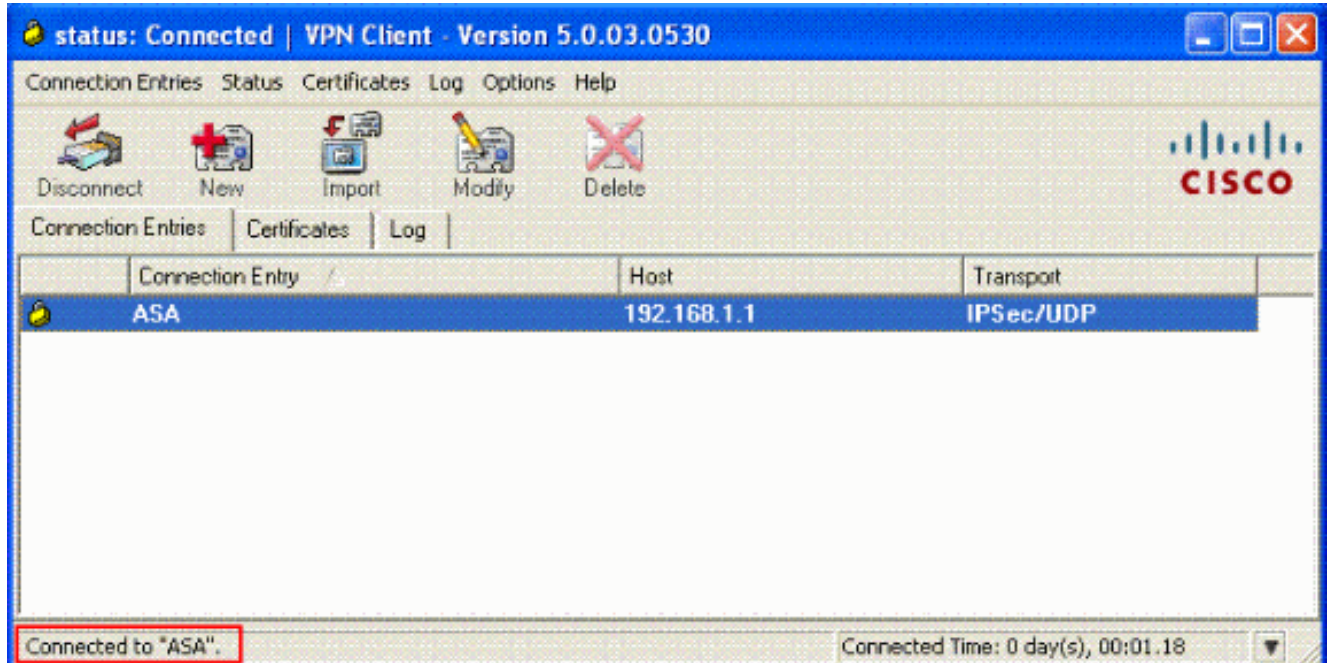
4. 单击要使用的连接，然后在 VPN 客户端主窗口中单击 **Connect**。



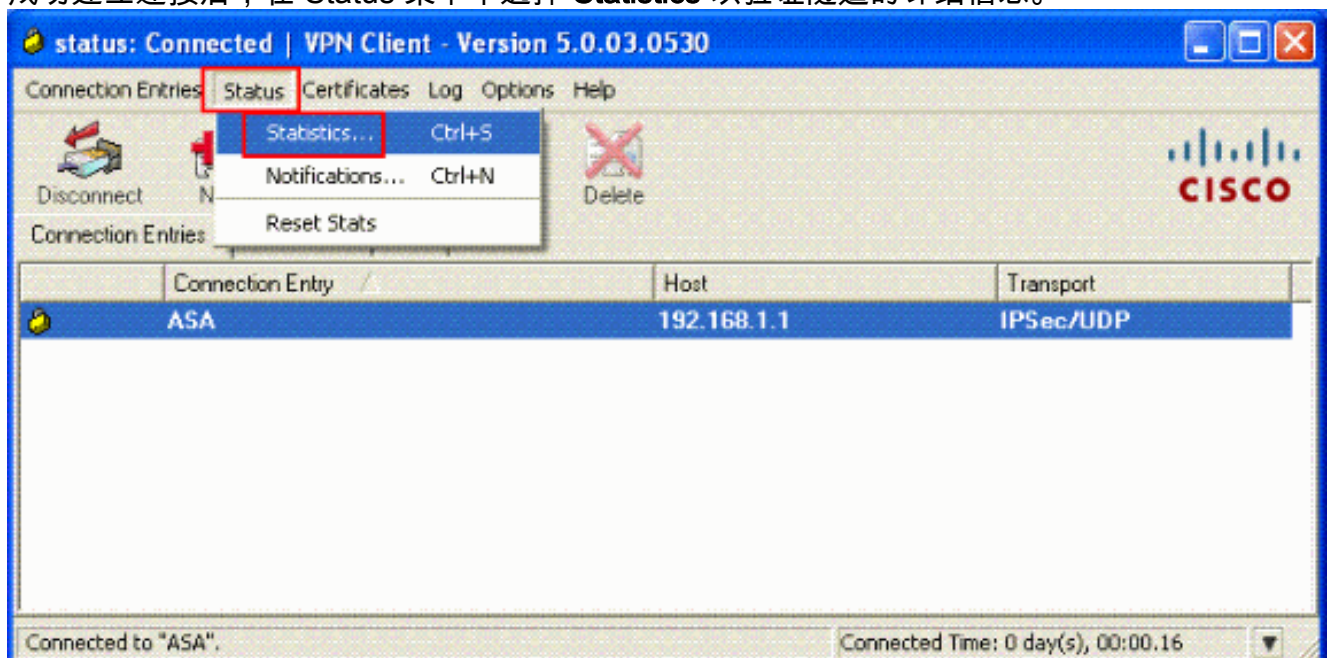
5. 出现提示时，输入 **Username:cisco** 和 **Password:password1**（如 ASA 中的扩展验证配置），然后单击 OK 以连接到远程网络。



6. 现在 VPN 客户端将与中心站点的 ASA 建立连接。



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。



[为适用于个人用户的可下载 ACL 配置 ACS](#)

您可以在 Cisco Secure ACS 上将可下载访问列表配置为共享配置文件组件，然后将访问列表分配

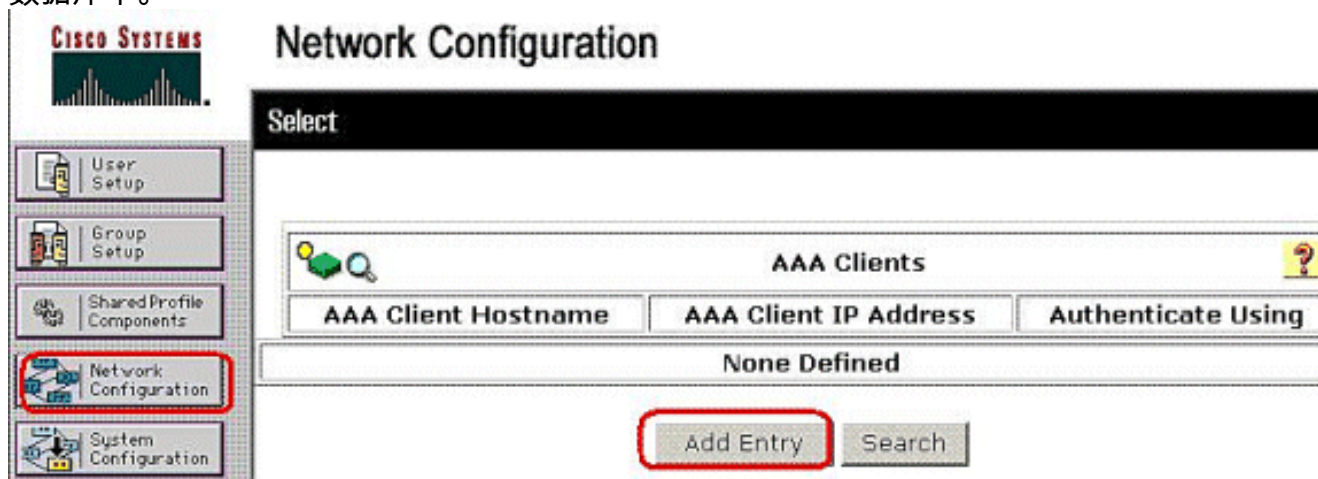
给某个组或单个用户。

要实施动态访问列表，您必须将 RADIUS 服务器配置为支持此操作。在用户进行身份验证时，RADIUS 服务器将向安全设备发送一份可下载访问列表或访问列表名称。该访问列表将允许或拒绝对指定服务的访问。身份验证会话过期后，安全设备将删除该访问列表。

在本示例中，IPSec VPN 用户“cisco”成功进行了身份验证，RADIUS 服务器向安全设备发送了一份可下载访问列表。用户“cisco”只能访问 10.1.1.2 服务器，拒绝其他所有访问。为了验证ACL，请参阅[可下载的ACLs关于用户/组](#)部分。

完成以下步骤，以便在 Cisco Secure ACS 中配置 RADIUS。

1. 在左侧选择 **Network Configuration**，单击 Add Entry 以便为 ASA 添加条目到 RADIUS 服务器数据库中。



2. 在 Client IP Address 字段中输入 **172.16.1.2**，在 Shared Secret Key 字段中输入“cisco123”。在 *Authenticate Using* 下拉框中，选择 **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**。单击 **Submit**。

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Add AAA Client

AAA Client Hostname

AAA Client IP Address

Shared Secret

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format ASCII Hexadecimal

Authenticate Using

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

- 在 User 字段中，输入 Cisco 安全数据库中的用户名，然后单击 **Add/Edit**。在本示例中，用户名为 **cisco**。

User Setup

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture

User:

Find

Add/Edit

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

List all users

Remove Dynamic Users

4. 在下一个窗口中，输入“cisco”的口令。在本示例中，口令也是 password1。完成时，请单击 Submit。

CISCO SYSTEMS

User Setup

User: cisco

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

ACS Internal Database


CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password









Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

5. 使用 Advanced Options 页以确定 ACS 将显示的高级选项。如果隐藏不使用的高级选项，则可以简化在 ACS Web 界面的其他区域显示的页面。单击 **Interface Configuration**，然后单击 **Advanced Options** 以打开 **Advanced Options** 页。



Interface Configuration

-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration
-  System Configuration
-  Interface Configuration
-  Administration Control
-  External User Databases


Advanced Options ?

Note: Only the selected options will appear in the user interface.





- Per-user TACACS+/RADIUS Attributes
- User-Level Shared Network Access Restrictions
- User-Level Network Access Restrictions
- User-Level Downloadable ACLs
- Default Time-of-Day / Day-of-Week Specification
- Group-Level Shared Network Access Restrictions
- Group-Level Network Access Restrictions
- Group-Level Downloadable ACLs
- Group-Level Password Aging

选中 **User-Level Downloadable ACLs** 和 **Group-Level Downloadable ACLs** 复选框。**User-Level Downloadable ACLs** - 选中该选项后，User Setup 页上将显示 Downloadable ACLs (访问控制列表) 部分。**Group-Level Downloadable ACLs** - 选中该选项后，Group Setup 页上将显示 Downloadable ACLs 部分。






- 在导航栏中，依次单击 **Shared Profile Components** 和 **Downloadable IP ACLs**。注意：如果 **Downloadable IP ACLs** 未显示在 **Shared Profile Components** 页上，则必须在 **Interface Configuration** 部分的 **Advanced Options** 页中启用 **User-Level Downloadable ACLs**、**Group-Level Downloadable ACLs** 选项，或者同时启用这两个选项。



Shared Profile Components

-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration

Select

-  [Downloadable IP ACLs](#)
-  [Network Access Filtering](#)
-  [RADIUS Authorization Components](#)
-  [Shell Command Authorization Sets](#)
-  [PIX/ASA Command Authorization Sets](#)

- 单击 **Add**。此时将出现 **Downloadable IP ACLs** 页。

Shared Profile Components

Select

Downloadable IP ACLs	
Name	Description
None Defined	

Add

Cancel

- 在 Name 框中，键入新 IP ACL 的名称。**注意：**IP ACL 的名称最多可以包含 27 个字符。名称中不得包含空格或以下字符之一：连字符 (-)、左方括号 ([)、右方括号 (])、斜线 (/)、反斜线 (\)、引号 (")、左尖括号 (<)、右尖括号 (>) 或破折号 (-)。在 Description 框中，键入新 IP ACL 的说明。说明最多可以有 1,000 个字符。

Shared Profile Components

Edit


Downloadable IP ACLs

Name:
Description:

ACL Contents

Network Access Filtering

No ACLs

 Back to Help

要向新 IP

ACL 添加 ACL 内容，请单击 **Add**。

9. 在 Name 框中，键入新 ACL 内容的名称。**注意**：ACL 内容的名称最多可以包含 27 个字符。名称中不得包含空格或以下字符之一：连字符 (-)、左方括号 ([)、右方括号 (])、斜线 (/)、反斜线 (\)、引号 (")、左尖括号 (<)、右尖括号 (>) 或破折号 (-)。在 ACL Definition 框中，键入新的 ACL 定义。**注意**：在 ACS Web 界面中输入 ACL 定义时，请勿使用关键字或名称条目；而应以 permit 或 deny 关键字开始。要保存 ACL 内容，请单击 **Submit**。

Shared Profile Components

Edit

Downloadable IP ACL Content

Name:

VPN_Client

ACL Definitions

```
permit ip any host 10.1.1.2  
deny ip any any
```



Back to Help

Submit

Cancel

10. 此时将出现 Downloadable IP ACLs 页，其中在 ACL Contents 列中列出了新 ACL 内容的名称。要将 NAF 与 ACL 内容关联，请从新 ACL 内容右边的 Network Access Filtering 框中选择一个 NAF。默认情况下，NAF 为 (All-AAA-Clients)。如果不分配 NAF，ACS 会默认将 ACL 内容与所有网络设备相关联。

Shared Profile Components


Edit

Downloadable IP ACLs

Name:

Description:

	ACL Contents	Network Access Filtering
<input checked="" type="radio"/>	VPN_Client	(All-AAA-Clients) ▼



要设置

ACL 内容的顺序，请单击 ACL 定义所对应的单选按钮，再单击 **Up** 或 **Down** 以改变其在列表中的顺序位置。要保存 IP ACL，请单击 **Submit**。**注意**：ACL 内容的顺序非常重要。从顶部到底部，ACS 只会下载第一个包含适用 NAF 设置的 ACL 定义，该适用 NAF 设置应包含 All-AAA-Clients 默认设置（如果使用）。通常，ACL 内容的列表会按照从最具体（范围最窄）的 NAF 到最普遍 (All-AAA-Clients) NAF 的顺序排列。**注意**：ACS 输入的新 IP ACL 将立即生效。例如，如果 IP ACL 可与 PIX 防火墙一起使用，则其可发送到任何尝试对用户（他或她将该可下载 IP ACL 分配到用户或组配置文件）进行身份验证的 PIX 防火墙。

11. 转到 User Setup 页并编辑 User 页。在 Downloadable ACLs 部分下，单击 **Assign IP ACL:** 复选框。从列表选择一个 IP ACL。如果已完成用户帐户选项的配置，请单击 **Submit** 以记录这些选项。

User Setup

Account Disable

Never

Disable account if:

Date exceeds:

Failed attempts exceed:

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

Downloadable ACLs

Assign IP ACL:

[为适用于组的可下载 ACL 配置 ACS](#)

完成[为适用于个人用户的可下载 ACL 配置 ACS](#)中的步骤 1 到 9，然后执行以下步骤，在 Cisco Secure ACS 中为组配置可下载 ACL。

在本示例中，IPSec VPN 用户“cisco”属于 VPN 组。VPN 组策略适用于该组中的所有用户。

VPN 组用户“cisco”已成功进行身份验证，RADIUS 服务器将向安全设备发送一份可下载访问列表。用户“cisco”只能访问 10.1.1.2 服务器，拒绝其他所有访问。要验证 ACL，请参阅[适用于用户/组的可下载 ACL](#)部分。

1. 在导航栏中，单击 **Group Setup**。将打开 Group Setup Select 页。



Group Setup



Select

Group : 1: Group 1

Users in Group Edit Settings

Rename Group

2. 将 Group 1 重命名为 VPN，然后单击 Submit。



Group Setup



Select

Renaming Group: Group 1

Group VPN

Submit Cancel

3. 从 Group 列表选择一个组，然后单击 Edit Settings。

Group Setup

Select

Group 1: VPN (1 user)

Users in Group Edit Settings

Rename Group

4. 在 Downloadable ACLs 部分下，单击 Assign IP ACL 复选框。从列表选择一个 IP ACL。

Group Setup

Jump To Access Restrictions

Sessions available to users of this group

Unlimited

IP Assignment ?

No IP address assignment

Assigned by dialup client

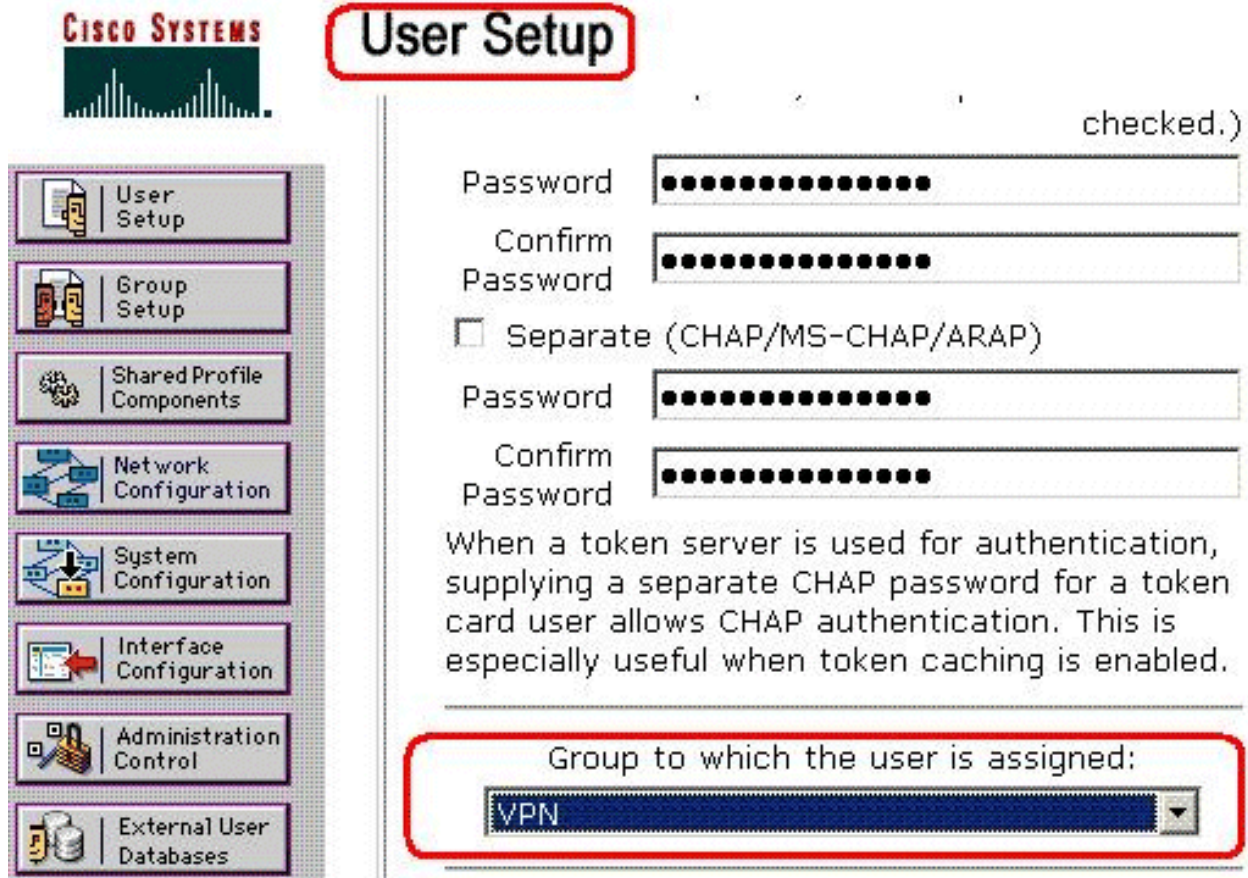
Assigned from AAA Client pool

Downloadable ACLs ?

Assign IP ACL:

5. 要保存刚才所作的组设置，请单击 **Submit**。

6. 转到 User Setup 并编辑要添加到组：VPN.完成时，请单击 **Submit**。



现在，为 VPN 组配置的可下载 ACL 已应用于该用户。

7. 要继续指定其他组设置，请执行本章中的其他步骤（如适用）

为用户组配置 IETF RADIUS 设置

要在用户进行身份验证时从 RADIUS 服务器为已在安全设备上创建的某个访问列表下载名称，请按如下方法配置 IETF RADIUS filter-id 属性（属性编号 11）：

```
filter-id=acl_name
```

VPN 组用户“cisco”已成功进行身份验证，RADIUS 服务器将为已在安全设备上创建的访问列表下载 ACL 名称 (new)。用户“cisco”可以访问 ASA 内部网络的所有设备，除了 10.1.1.2 服务器。为了验证 ACL，请参阅[过滤器 ID ACL 部分](#)。

根据本示例，名为 new 的 ACL 配置为在 ASA 中过滤。

```
access-list new extended deny ip any host 10.1.1.2 access-list new extended permit ip any any
```

这些参数只有在以下条件成立时才会显示。您已进行以下配置

- 在 Network Configuration 中将 AAA 客户端配置为使用其中一个 RADIUS 协议
- 在 Web 界面的 Interface Configuration 部分中，在 RADIUS (IETF) 页上配置组级别的 RADIUS 属性

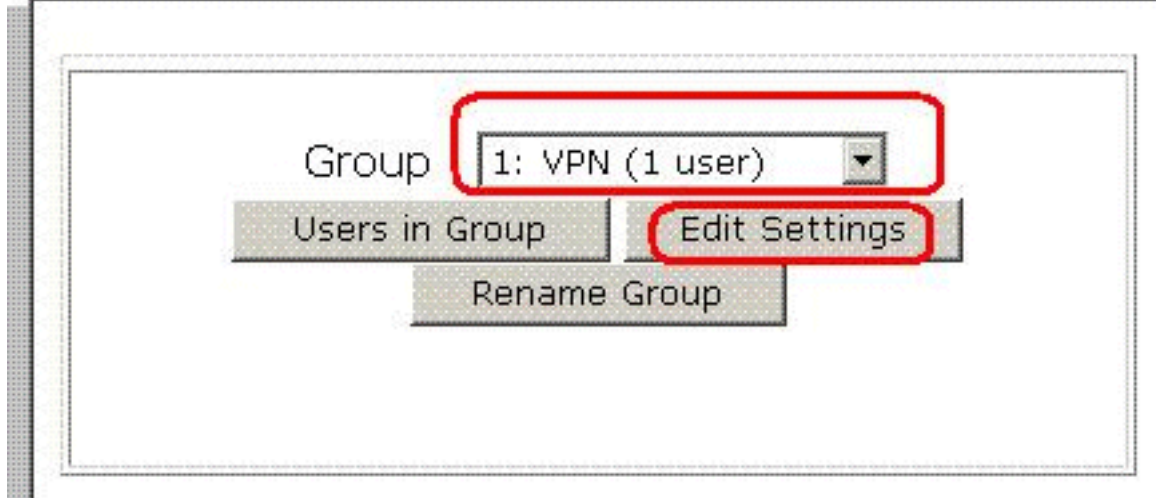
RADIUS 属性会作为每个用户的配置文件从 ACS 发送到请求的 AAA 客户端。

要配置 IETF RADIUS 属性设置以应用为当前组中每个用户的授权，请执行以下操作：

1. 在导航栏中，单击 **Group Setup**。将打开 Group Setup Select 页。
2. 从 Group 列表选择一个组，然后单击 **Edit Settings**。

Group Setup

Select



该组的名称

将出现在 Group Settings 页的顶部。

3. 滚动到 IETF RADIUS Attributes。对于每个 IETF RADIUS 属性，必须授权当前组。选中 [011] Filter-Id 属性的复选框，然后在字段中添加 ASA 在为属性授权时定义的 ACL 名称 (new)。请参阅 ASA *show running configuration* 输出。

Group Setup

Jump To Access Restrictions

IETF RADIUS Attributes

[006] Service-Type

Authenticate only

[007] Framed-Protocol

Ascend MPP

[009] Framed-IP-Netmask

0.0.0.0

[010] Framed-Routing

None

[011] Filter-Id

new

[012] Framed-MTU (64..65535)

4. 要保存刚才所作的组设置并立即应用，请依次单击 **Submit** 和 **Apply**。注意：要保存组设置且以后应用，请单击 **Submit**。当准备好实施更改时，请选择 **System Configuration > Service Control**。然后选择 **Restart**。

验证

使用本部分可确认配置能否正常运行。

[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。

显示 Crypto 命令

- **show crypto isakmp sa** — 显示对等体上的所有当前 IKE 安全关联 (SA)。`ciscoasa# sh 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: 192.168.10.2 Type : user Role : responder Rekey : no State : AM_ACTIVE ciscoasa#
```

- **show crypto ipsec sa** — 显示当前 SA 使用的设置。ciscoasa# **sh crypto ipsec sa interface:**
outside Crypto map tag: outside_dyn_map, seq num: 1, 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: 192.168.10.2, username: cisco dynamic allocated peer ip: 192.168.5.1 #pkts encaps: 65, #pkts encrypt: 65, #pkts digest: 65 #pkts decaps: 65, #pkts decrypt: 65, #pkts verify: 65 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 4, #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.: 192.168.10.2 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: EEF0EC32 inbound esp sas: spi: 0xA6F92298 (2801345176) transform: esp-3des esp-sha-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 86016, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 28647 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xEEF0EC32 (4008766514) transform: esp-3des esp-sha-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 86016, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 28647 IV size: 8 bytes replay detection support: Y

[适用于用户/组的可下载 ACL](#)

验证用户 Cisco 的可下载 ACL。ACL 从 CSACS 进行下载。

```
ciscoasa(config)# sh access-list access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300 access-list 101; 1 elements access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411 access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic) access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit ip any host 10.1.1.2 (hitcnt=2) 0x334915fe access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny ip any any (hitcnt=40) 0x7c718bd1
```

[Filter-Id ACL](#)

[011] Filter-Id 已应用于 VPN 组，该组的用户按 ASA 中定义的 ACL (new) 进行过滤。

```
ciscoasa# sh access-list  
access-list cached ACL log flows: total 0,  
  denied 0 (deny-flow-max 4096)  
  alert-interval 300  
access-list 101; 1 elements  
access-list 101 line 1 extended permit ip 10.1.1.0  
  255.255.255.0 192.168.5.0 255.255.255.0  
  (hitcnt=0) 0x8719a411  
access-list new; 2 elements  
access-list new line 1 extended deny ip any host 10.1.1.2 (hitcnt=4) 0xb247fec8 access-list new  
line 2 extended permit ip any any (hitcnt=39) 0x40e5d57c
```

[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：关于故障排除远程访问IPSec VPN的更多信息，参考[最普通的L2L和排除故障解决方案的远程访问IPSec VPN](#)。

[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： 使用 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

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

[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 自适应安全设备管理器](#)
- [IPsec 协商/IKE 协议支持页](#)
- [Cisco VPN 客户端支持页](#)
- [用于 Windows 的 Cisco 安全访问控制服务器](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)