ASA 8.3 及更高版本：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

目录

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。因为您能隐含地启用RADIUS授权，本文不包含关于RADIUS授权的配置的信息在安全工具的。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。

可下载的访问列表是最可扩展的平均值，当您使用思科安全访问控制服务器(ACS)时为每个用户提供适当的访问列表。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。

参考的ASA/PIX 8.x ：RADIUS授权(ACS)网络访问的使用与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8.2和以下。

先决条件

要求

本文假设，可适应安全工具(ASA)是完全能操作和已配置的允许Cisco Adaptive Security Device Manager (ASDM)或CLI做配置更改。

注意： 参考允许HTTPS访问ASDM为了允许ASDM或安全壳SSH远程配置的设备。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ASA软件版本8.3及以后
- Cisco ASDM版本6.3和以上
- Cisco VPN客户端软件版本5.x和以后
- Cisco Secure ACS 5.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。

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

您能使用可下载的IP ACL为了创建套您能应用对许多用户或用户组的ACL定义。这些 ACL 定义集称为 ACL 内容。

可下载 IP ACL 的运行方式如下：

1. 当ACS准许对网络时的一次用户访问， ACS确定可下载的IP ACL是否分配到在结果部分的授权配置文件。
2. 如果ACS找出分配到授权配置文件的可下载的IP ACL， ACS发送(的属性作为用户会话一部分， RADIUS访问接受信息包的)指定指定的ACL和指定的ACL的版本。
3. 如果AAA客户端响应它没在其缓存有ACL的当前版本(即ACL新建或更改)， ACS发送ACL (新建或更新)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。如果参考其名称，您能一次创建可下载的IP ACL，给予它名称，然后分配可下载的IP ACL到所有授权配置文件。如果配置授权配置文件的， RADIUS思科cisco-av-pair属性此方法是更有效的比。

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。

在ACS，您能定义多个可下载的IP ACL和使用他们用不同的授权配置文件。基于在访问服务授权规则的条件，您能发送包含可下载的IP ACL的不同的授权配置文件对不同的AAA客户端。

进一步，您能更改ACL内容的定货在可下载的IP ACL的。ACS从表的顶部开始检查ACL内容，并且下载第一个ACL满意查找。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。

为了使用在特定AAA客户端的可下载的IP ACL， AAA客户端必须遵守这些规则：

- 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
- 运行IOS版本12.3(8)T和以后的Cisco设备

这是您必须使用为了输入在ACL定义方框的ASA ACL格式的示例：

```
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。

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**向导> VPN向导> IPsec(IKEv1)**从家庭窗口的**远程访问VPN向导**。
2. 选择**VPN隧道接口**如所需求(**从外部**，在本例中)，并且确保在**Enable (event)绕过Inbound IPSec的会话旁边的**复选框**接口访问列表**被检查。
3. 选择VPN客户端类型作为**Cisco VPN Client，版本3.x或者更加高**。单击 **Next**。
4. 选择**认证方法**并且提供认证信息。使用的认证方法这里是**预先共享密钥**。并且，请提供在提供的空间的**隧道组**组名。使用的**预先共享密钥**这里是**cisco123，**并且使用的**隧道组组名**这里是思科**通道**。单击 **Next**。
5. 选择是希望使用本地用户数据库对远程用户进行身份验证，还是希望使用外部 AAA 服务器组对远程用户进行身份验证。这里，**使用AAA服务器组，**我们选择**验证**。单击**新**在AAA服务器组Name字段旁边为了创建新的AAA服务器组组名。
6. 提供服务器组组名、认证协议、服务器IP地址、接口名称和服务器秘密密钥在提供的各自空间，并且点击OK键。
7. 单击 **Next**。
8. 定义一个要在远程 VPN 客户端进行连接时动态分配给它们的本地地址池。单击**新**为了创建本地地址新池。
9. 在添加IP池窗口，请提供池名称，开始IP地址，结束IP地址和子网掩码。单击 **Ok**。
10. 选择从下拉列表的池名称，并且**其次**单击。池名称对于此示例是在步骤9.创建的示例**池**。
11. ***可选：***指定 DNS 和 WINS 服务器信息以及将被推送到远程 VPN 客户端的默认域名。
12. 指定哪些内部主机或网络（如果有）应向远程 VPN 用户公开。**其次**在提供在豁免网络字段和网络以后单击将豁免的接口名称。如果将此列表留空，则将允许远程 VPN 用户访问 ASA 的整个内部网络。您还可以在此窗口上启用分割隧道。分割隧道对发往本过程中前面所定义的资源的数据流进行加密，并通过不以隧道形式传输该数据流提供对整个 Internet 的未加密访问。如果*未* 启用分割隧道，则来自远程 VPN 用户的所有数据流将通过隧道传输到 ASA。这可能导致很高的带宽和处理器使用率，具体取决于您的配置。
13. 此窗口显示您已执行操作的汇总。如果对配置感到满意，请单击 **Finish**。

配置与CLI的ASA

这是CLI配置：

ASA 设备上的运行配置

```
ASA# sh run
ASA Version 8.4(3)
!
!--- Specify the hostname for the Security Appliance.
hostname ciscoasa enable password y.tvDXf6yFbMTAdD
encrypted passwd 2KFQnbNIdI.2KYOU encrypted names ! !---
Configure the outside and inside interfaces. interface
Ethernet0/0 nameif dmz security-level 50 ip address
192.168.26.13 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! interface Ethernet0/2 nameif outside
security-level 0 ip address 172.16.1.1 255.255.255.0 !
!--- Output is suppressed. boot system disk0:/asa843-
k8.bin ftp mode passive object network
NETWORK_OBJ_10.1.1.0_24 subnet 10.1.1.0 255.255.255.0
object network NETWORK_OBJ_10.2.2.0_24 subnet 10.2.2.0
255.255.255.0 access-list OUTIN extended permit icmp any
any !--- This is the Access-List whose name will be sent
by !--- RADIUS Server(ACS) in the Filter-ID attribute.
access-list new extended permit ip any host 10.1.1.2
```

```
access-list new extended deny ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500

ip local pool Sample-Pool 10.2.2.1-10.2.2.254 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-647.bin no asdm history enable arp timeout
14400 !--- Specify the NAT from internal network to the
Sample-Pool. nat (inside,outside) source static
NETWORK_OBJ_10.1.1.0_24 NETWORK_OBJ_10.1.1.0_24
destination static NETWORK_OBJ_10.2.2.0_24
NETWORK_OBJ_10.2.2.0_24 no-proxy-arp route-lookup
access-group OUTIN in interface outside !--- Create the
AAA server group "ACS5" and specify the protocol as
RADIUS. !--- Specify the ACS 5.x server as a member of
the "ACS5" group and provide the !--- location and key.
aaa-server ACS5 protocol radius
aaa-server ACS5 (dmz) host 192.168.26.51
timeout 5
key *****

aaa authentication http console LOCAL
http server enable 2003
http 0.0.0.0 0.0.0.0 inside


!--- PHASE 2 CONFIGURATION ---! !--- The encryption &
hashing types for Phase 2 are defined here. We are using
!--- all the permutations of the PHASE 2 parameters.
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-
aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-
aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-
aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-
aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes
esp-md5-hmac


!--- Defines a dynamic crypto map with !--- the
specified transform-sets created earlier. We are
specifying all the !--- transform-sets. crypto dynamic-
```

```
map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-
set
   ESP-AES-128-SHA ESP-AES-128-MD5
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-
256-MD5 ESP-3DES-SHA
   ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5

!--- Binds the dynamic map to the IPsec/ISAKMP process.
crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_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 policies defined with all the permutation !-
-- of the 5 ISAKMP parameters. The configuration
commands here define the !--- Phase 1 policy parameters
that are used. crypto ikev1 enable outside

crypto ikev1 policy 10
authentication crack
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 20
authentication rsa-sig
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 40
authentication crack
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 70
```

```
authentication crack
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 80
authentication rsa-sig
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 90
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 100
authentication crack
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 110
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 120
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 130
authentication crack
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 140
authentication rsa-sig
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 150
authentication pre-share
encryption des
hash sha
group 2
lifetime 86400


webvpn
```

```
group-policy Cisco-Tunnel internal
group-policy Cisco-Tunnel attributes
vpn-tunnel-protocol ikev1
default-domain value cisco.com
username admin password CdOTKv3uhDhHIw3A encrypted
privilege 15
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (ACS5) with the tunnel group. tunnel-group Cisco-
Tunnel type remote-access tunnel-group Cisco-Tunnel
general-attributes
address-pool Sample-Pool
authentication-server-group ACS5
default-group-policy Cisco-Tunnel

!--- Enter the pre-shared-key to configure the
authentication method. tunnel-group Cisco-Tunnel ipsec-
attributes
ikev1 pre-shared-key *****

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

为适用于个人用户的可下载 ACL 配置 ACS

您能配置在Cisco Secure ACS 5.x的可下载的访问列表，因为已命名Permissions Object然后分配它到在规则结果部分在访问服务中将选择的授权配置文件。

在本例中， IPSec VPN用户**cisco**成功验证，并且RADIUS服务器发送一可下载的访问列表到安全工具。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。

完成这些步骤为了配置Cisco Secure ACS的5.x RADIUS客户端：

1. 选择**网络资源>网络设备和AAA客户端**，并且单击**创建**为了添加ASA的一个条目在RADIUS服务器数据库。
2. 输入一局部重要的名称对于ASA (示例**ASA**，在本例中)，然后进入在IP地址字段的**192.168.26.13**。通过检查**RADIUS**复选框选择在认证选项部分的**RADIUS**并且进入共享秘密字段的**cisco123**。单击 **submit**。
3. ASA成功地添加到RADIUS服务器(ACS)数据库。
4. 选择**用户，并且标识存储>内部标识存储>** Users，并且单击**创建**为了创建ACS的本地数据库的一个用户VPN验证的。
5. 输入用户名**cisco**。选择密码类型作为**内部用户**，并且输入密码(**cisco123**，在本例中)。证实密码，并且单击**提交**。
6. 用户**cisco**顺利地创建。
7. 为了创建可下载的ACLs，选择**策略元素>授权和权限>命名了Permission Objects >可下载的ACLs**，并且单击**创建**。
8. 为可下载的ACLs提供**名称**，以及**ACL内容**。单击 **submit**。
9. 可下载的ACLs**示例DACL**顺利地创建。
10. 为了配置VPN验证的访问策略，请选择**访问策略**>Access **Services>服务选择规则**，并且确定哪服务迎合RADIUS协议。在本例中，**规则1**匹配**RADIUS**，并且默认网络网络访问将迎合RADIUS请求。

11. 从步骤10.选择确定的**访问服务**。在本例中，使用**默认网络网络访问**。选择**允许Protocols选项**，并且确保请**允许PAP/ASCII**并且**允许MS-CHAPv2**选择。单击 **submit**。
12. 点击**访问服务的Identity部分**，并且确保**内部用户**选择作为标识来源。在本例中，我们采取了默认网络网络访问。
13. 选择**访问策略**>Access **Services>默认网络网络访问>授权**，并且点击**自定义**。
14. 移动**System:** 从**可用的**列的**用户名**到**选定**列，和点击OK键。
15. 单击**创建**为了创建新规则。
16. 在**System:旁边**确保复选框**用户名**选择，从下拉列表选择**等于**，并且输入用户名**cisco**。
17. 单击**选择**。
18. 单击**创建**为了创建一新的授权配置文件。
19. 为**授权配置文件**提供一名称。**示例配置文件**用于此示例。
20. 选择**普通的任务**选项卡，并且选择从下拉列表的**静态可下载的ACLs名称的**。选择新建立的**DACL (示例- DACL)**从值下拉式列表。
21. 单击 **submit**。
22. 确保在**示例配置文件**(新建立的授权配置文件)旁边的复选框被检查，并且点击OK键。
23. 一旦验证新建立的**示例配置文件**在**授权配置文件**字段选择，请点击OK键。
24. 验证新规则(**Rule-2**)创建与System: 用户名**等于cisco**情况和**示例配置文件**作为结果。点击**Save Changes**。规则2顺利地创建。

为适用于组的可下载 ACL 配置 ACS

完成步骤1至12可下载的ACLs的配置ACS个人用户的并且执行这些步骤为了配置组的可下载的ACLs Cisco Secure ACS的。

在本例中， IPSec VPN用户“cisco”属于示例**组**。

示例组用户**cisco**成功验证，并且RADIUS服务器发送一可下载的访问列表到安全工具。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. 在导航条，请点击**用户，并且标识存储>标识组**，并且单击**创建**为了创建一新的组。
2. 提供一个组名(示例**组**)，并且单击**提交**。
3. 选择**用户标识存储>内部标识存储>** Users，并且选择用户**cisco**。单击**编辑**为了更改此用户的组成员。
4. 在标识组旁边单击**精选**。
5. 选择新建立的组(即示例**组**)，并且点击OK键。
6. 单击 **submit**。
7. 选择**访问策略**>Access **Services>默认网络网络访问>授权**，并且单击**创建**为了创建新规则。
8. 确保在**标识组旁边的**复选框被检查，并且点击**精选**。
9. 选择示例**组**，并且点击OK键。
10. 点击**精选**，在授权配置文件部分。
11. 单击**创建**为了创建一新的授权配置文件。
12. 为**授权配置文件**提供一名称。**示例配置文件**是用于此示例的名称。
13. 选择**普通的任务**选项卡，并且选择从下拉列表的**静态可下载的ACLs名称的**。选择新建立的**DACL (示例- DACL)**从值下拉式列表。
14. 单击 **submit**。
15. 选择创建的授权配置文件**示例配置文件**前，并且点击OK键。
16. 单击 **Ok**。

17. 验证**Rule-1**创建与标识组示例**组**作为情况和**示例配置文件**作为结果。点击**Save Changes**。

配置可下载的ACLs的ACS网络设备组的

完成步骤1至12可下载的ACLs的配置ACS个人用户的并且执行这些步骤为了配置一个网络设备组的可下载的ACLs Cisco Secure ACS的。

在本例中， RADIUS客户端(ASA)属于网络设备组来自用户的“cisco” ASA的VPNGateways.The认证请求成功验证的VPN，并且RADIUS服务器发送一可下载的访问列表到安全工具。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. 选择**网络资源>网络设备组>设备类型**，并且单击**创建**为了创建一个新的网络设备组。
2. 提供**网络设备组**组名(在本例中的**VPN网关**)，并且单击**提交**。
3. 选择**网络资源>网络设备和AAA客户端**，并且选择创建的**RADIUS客户端示例ASA**前。单击**编辑**为了更改**网络设备组**会员此RADIUS客户端(asa)。
4. 在设备类型旁边单击**精选**。
5. 选择是**VPN网关**)的新建立的网络设备组(并且点击OK键。
6. 单击 **submit**。
7. 选择**访问策略**>Access **Services>默认网络网络访问>授权**，并且点击**自定义**。
8. 移动**NDG ：从可用的**部分的**设备类型**到**所选的部分**，和点击OK键。
9. 单击**创建**为了创建新规则。
10. 确保在**NDG旁边的**复选框：**设备类型**选择并且从下拉列表选择。单击**选择**。
11. 选择创建的网络设备组**VPN网关**前，并且点击OK键。
12. 单击**选择**。
13. 单击**创建**为了创建一新的授权配置文件。
14. 为**授权配置文件**提供一名称。**示例配置文件**是用于此示例的名称。
15. 选择**普通的任务**选项卡，并且选择从下拉列表的**静态**可下载的ACLs名称的。从值下拉式列表选择新建立的**DACL (示例DACL)**。
16. 单击 **submit**。
17. 选择创建的**示例配置文件**前，并且点击OK键。
18. 单击 **Ok**。
19. 验证**Rule-1**用**VPN网关**创建作为NDG ：设备类型作为情况和**示例配置文件**结果。点击**Save Changes**。

为用户组配置 IETF RADIUS 设置

为了下载一名称对于您在从RADIUS服务器的安全工具已经创建的访问列表，当用户验证时，请配置IETF RADIUS过滤器ID属性(属性编号11) ：

```
filter-id=acl_name
```

示例组usercisco成功验证，并且RADIUS服务器下载一ACL名称(新建)您在安全工具已经创建的访问列表的。用户“cisco”能访问是在ASA网络里面**除了**10.1.1.2服务器的所有设备。为了验证ACL，请参阅过滤器ID ACL部分。

根据示例，名为**新建的**ACL为过滤配置在ASA ：

```
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。您配置：

- 在 Network Configuration 中将 AAA 客户端配置为使用其中一个 RADIUS 协议
- 与RADIUS (IETF)过滤器ID的一授权配置文件在访问服务中选择在规则的结果部分下。

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。

完整步骤1至6和10至12可下载的ACLs的配置ACS个人用户的，跟随由步骤1至6可下载的ACLs的配置ACS组的，和在此部分执行这些步骤为了配置在Cisco Secure ACS的过滤器ID。

为了配置**IETF RADIUS属性**设置应用正如在授权配置文件，请执行这些步骤：

1. 选择**策略元素>授权和权限>网络访问>授权配置文件**，并且单击**创建**为了创建一新的授权配置文件。
2. 为**授权配置文件**提供一名称。**过滤器ID**是在本例中选择的授权配置文件名称为了简化。
3. 点击**普通的任务**选项卡，并且从**过滤器ID ACL的**下拉列表选择**静态**。输入访问列表名称如**新建**在Value字段，并且单击**提交**。
4. 选择**访问策略**>Access **Services>默认网络网络访问>授权**，并且单击**创建**为了创建新规则。
5. 确保在**标识组旁边的**复选框被检查，并且点击**精选**。
6. 选择示例**组**，并且点击OK键。
7. 点击**精选**在授权配置文件部分。
8. 选择创建的授权配置文件**过滤器ID**前，并且点击OK键。
9. 单击 **Ok**。
10. 验证**Rule-1**创建与标识组示例**组**作为情况和**过滤器ID**结果。点击**Save Changes**。

Cisco VPN 客户端配置

连接对思科ASA以Cisco VPN Client为了验证ASA顺利地配置。

完成这些步骤：

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. 填写您的新连接详细信息：输入 Connection Entry 的名称与说明。在 Host 框中输入 **ASA 的外部 IP 地址**。输入VPN隧道组组名(思科**通道**)和密码(预先共享密钥- **cisco123**)如ASA所配置的一样。Click **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. 当提示，请进入用户名**cisco**和Password Cisco123如验证的ASA所配置的一样，并且点击OK键为了连接到远程网络。
6. 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。

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

IKEv1 SAs:

   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: 172.16.1.50
    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: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr:
       172.16.1.1

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
      current_peer: 172.16.1.50, username: cisco
      dynamic allocated peer ip: 10.2.2.1

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
      #pkts decaps: 333, #pkts decrypt: 333, #pkts verify: 333
      #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.: 172.16.1.1/0, remote crypto endpt.: 172.16.1.50/0
      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 9A06E834
      current inbound spi : FA372121

    inbound esp sas:
      spi: 0xFA372121 (4197916961)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 28678
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x9A06E834 (2584143924)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 28678
         IV size: 16 bytes
         replay detection support: Y
```

```
            Anti replay bitmap:
             0x00000000 0x00000001
```

适用于用户/组的可下载 ACL

验证用户 Cisco 的可下载 ACL。ACL从CSACS下载。

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list #ACSACL#-IP-Sample-DACL-4f3b9117; 2 elements; name hash: 0x3c878038
   (dynamic)
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 1 extended permit ip any host
   10.1.1.2 (hitcnt=0) 0x5e896ac3
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 2 extended deny ip any any
   (hitcnt=130) 0x19b3b8f5
```

Filter-Id ACL

[011]过滤器ID为组应用-组的示例组和用户根据ACL被过滤(新建)定义在ASA。

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list new; 2 elements; name hash: 0xa39433d3
access-list new line 1 extended permit ip any host 10.1.1.2 (hitcnt=4)
   0x58a3ea12
access-list new line 2 extended deny ip any any (hitcnt=27) 0x61f918cd
```

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

当您排除故障时，请确保清除现存SAS，在您做一个变动后。在 PIX 的特权模式下，使用以下命令：

- **clear [crypto] ipsec sa** -删除活动IPSec SAS。关键字 crypto 是可选的。
- **clear [crypto] isakmp sa** -删除活动IKE SAS。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 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
- 思科安全访问控制系统
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems