

安全ACS - NAR , 带用户和用户组的AAA客户端

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[网络访问限制](#)

[关于网络访问限制](#)

[添加共享NAR](#)

[编辑共享NAR](#)

[删除共享NAR](#)

[设置用户的网络访问限制](#)

[为用户组设置网络访问限制](#)

[相关信息](#)

简介

本文档介绍如何为用户和用户组配置Cisco安全访问控制服务器(ACS)4.x版本中的网络访问限制(NAR), 该版本包含AAA客户端(包括路由器、PIX、ASA、无线控制器)。

先决条件

要求

本文档的创建假设是思科安全ACS和AAA客户端已配置并正常运行。

使用的组件

本文档中的信息基于Cisco Secure ACS 3.0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。

规则

有关文档规则的详细信息, 请参阅 [Cisco 技术提示规则](#)。

网络访问限制

本节介绍NAR，并提供配置和管理共享NAR的详细说明。

此部分包括以下主题：

- [关于网络访问限制](#)
- [添加共享NAR](#)
- [编辑共享NAR](#)
- [删除共享NAR](#)

[关于网络访问限制](#)

NAR是您在ACS中定义的附加条件，用户必须满足这些条件才能访问网络。ACS使用AAA客户端发送的属性信息来应用这些条件。虽然可以通过多种方式设置NAR，但所有设置都基于AAA客户端发送的匹配属性信息。因此，如果要使用有效的NAR，您必须了解AAA客户端发送的属性的格式和内容。

设置NAR时，可以选择过滤器是积极运行还是消极运行。也就是说，在NAR中，根据与NAR中存储的信息相比从AAA客户端发送的信息指定是允许还是拒绝网络访问。不过，如果NAR没有充足的信息以运行，将会默认为拒绝访问。下表显示了以下条件：

	基于IP	非基于IP	信息不足
允许	授权访问	拒绝进入。	拒绝进入。
拒绝	拒绝进入。	授权访问	拒绝进入。

ACS支持两种类型的NAR过滤器：

- **基于IP的过滤器** — 基于IP的NAR过滤器根据最终用户客户端和AAA客户端的IP地址限制访问。有关详细信息，[请参阅关于基于IP的NAR过滤器部分](#)。
- **非基于IP的过滤器** — 非基于IP的NAR过滤器根据从AAA客户端发送的值的简单字符串比较限制访问。该值可以是主叫线路标识(CLI)号码、被叫号码标识服务(DNIS)号码、MAC地址或源自客户端的其他值。要运行此类NAR，NAR说明中的值必须与从客户端发送的内容完全匹配，包括使用的任何格式。例如，电话号码(217)555-4534与217-555-4534不匹配。有关详细信息，[请参阅关于非基于IP的NAR过滤器部分](#)。

可以针对某个特定用户或用户组定义一个NAR，然后将其应用到该用户或用户组。有关详细信息，[请参阅“为用户设置网络访问限制”或“为用户组设置网络访问限制”部分](#)。但是，在ACS的Shared Profile Components部分，您可以创建并命名共享NAR，而无需直接引用任何用户或用户组。您为共享NAR提供可在ACS Web界面的其他部分引用的名称。然后，在设置用户或用户组时，可以选择要应用的无、一个或多个共享限制。指定多个共享NAR对用户或用户组的应用时，可以选择以下两个访问标准之一：

- 所有选定的过滤器必须允许。
- 任何一个选定的过滤器都必须允许。

您必须了解与不同类型的NAR相关的优先顺序。以下是NAR过滤的顺序：

1. 用户级别的共享NAR
2. 在组级别共享NAR
3. 用户级别的非共享NAR
4. 组级别的非共享NAR

您还应了解，在**任何级别拒绝访问优先于在不拒绝访问的另一级别设置**。这是ACS中用户级别设置

覆盖组级别设置规则的唯一例外。例如，特定用户在所应用的用户级别可能没有NAR限制。但是，如果该用户属于受共享或非共享NAR限制的组，则拒绝该用户访问。

共享NAR保留在ACS内部数据库中。您可以使用ACS备份和恢复功能进行备份和恢复。您还可以将共享NAR及其他配置复制到辅助ACS。

[关于基于IP的NAR过滤器](#)

对于基于IP的NAR过滤器，ACS使用如图所示的属性，这取决于身份验证请求的AAA协议：

- **如果使用TACACS+** — 使用`TACACS+`启动数据包正文中的`rem_addr`字段。**注意**：当代理将身份验证请求转发到ACS时，TACACS+请求的任何NAR都应用到转发AAA服务器的IP地址，而不是源AAA客户端的IP地址。
- **如果使用RADIUS IETF** — 必叫站ID (属性31)。**注意**：仅当ACS收到Radius Calling-Station-Id(31)属性时，基于IP的NAR过滤器才起作用。主叫站ID(31)必须包含有效的IP地址。否则，将由DNIS规则决定。

不提供足够IP地址信息 (例如，某些类型的防火墙) 的AAA客户端不支持完整的NAR功能。

基于IP的限制的其他属性 (按协议) 包括NAR字段，如下所示：

- **如果使用TACACS+** - ACS中的NAR字段使用以下值：**AAA client** - NAS-IP地址取自ACS和TACACS+客户端之间套接字中的源地址。**Port** — 端口字段取自TACACS+启动数据包正文。

[关于非基于IP的NAR过滤器](#)

非基于IP的NAR过滤器 (即基于DNIS/CLI的NAR过滤器) 是允许或拒绝的呼叫或接入点位置列表，当您没有建立的基于IP的连接时，您可以使用这些位置来限制AAA客户端。非基于IP的NAR功能通常使用CLI编号和DNIS编号。

但是，当您输入IP地址代替CLI时，可以使用非基于IP的过滤器；即使AAA客户端不使用支持CLI或DNIS的Cisco IOS®软件版本。在输入CLI的另一个例外中，可以输入MAC地址以允许或拒绝访问。例如，当您使用Cisco Aironet AAA客户端时。同样，您可以输入Cisco Aironet AP MAC地址代替DNIS。您在CLI框中指定的格式 (CLI、IP地址或MAC地址) 必须与您从AAA客户端接收的格式匹配。您可以从RADIUS记帐日志中确定此格式。

根据协议，基于DNIS/CLI的限制的属性包括NAR字段，如下所示：

- **如果使用TACACS+** — 列出的NAR字段使用以下值：**AAA client** - `NAS-IP-address`取自ACS和TACACS+客户端之间套接字中的源地址。**Port** — 使TACACS+启动数据包正文中的端口字段。**CLI** — 使`TACACS+`启动数据包正文中的`rem-addr`字段。**DNIS** — 使TACACS+启动数据包正文获取的`rem-addr`字段。在`rem-addr`数据以斜杠(/)开头的情况下，DNIS字段包含`rem-addr`数据，不带斜杠(/)。**注意**：当代理将身份验证请求转发到ACS时，TACACS+请求的任何NAR都应用到转发AAA服务器的IP地址，而不是源AAA客户端的IP地址。
- **如果使用RADIUS** — 列出的NAR字段使用以下值：**AAA client** — 使用 `NAS-IP-address` (属性 4) 或 (如果 `NAS-IP-address` 不存在) `NAS-identifier` (RADIUS 属性 32)。**端口** — 使用 `NAS-port` (属性 5) 或 (如果 `NAS-port` 不存在) `NAS-port-ID` (属性 87)。**CLI** — 使用 `calling-station-ID` (属性 31)。**DNIS** — 使用 `called-station-ID` (属性 30)。

指定NAR时，可以使用星号(*)作为任何值的通配符，或作为任何值的一部分来建立范围。NAR说明中的所有值或条件必须满足，NAR才能限制访问。这意味着这些值包含布尔值AND。

添加共享NAR

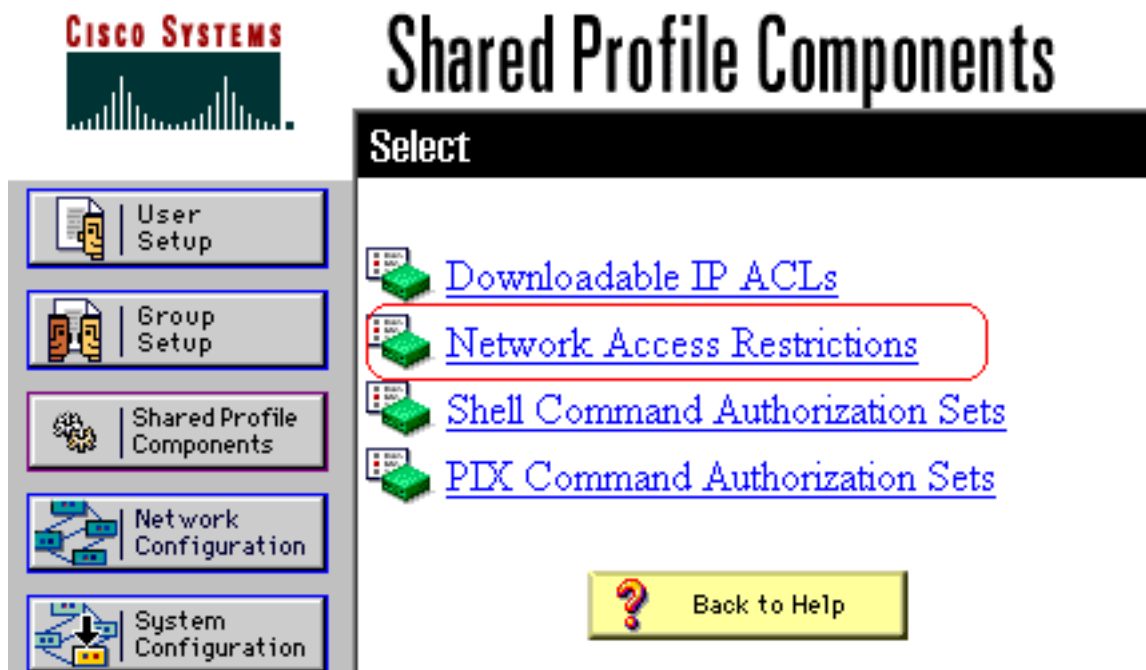
您可以创建包含许多访问限制的共享NAR。虽然ACS Web界面不对共享NAR中的访问限制数量或每个访问限制的长度实施限制，但必须遵守以下限制：

- 每个行项目的字段组合不能超过1024个字符。
- 共享NAR不能超过16 KB字符。支持的行项目数取决于每个行项目的长度。例如，如果创建基于CLI/DNIS的NAR，其中AAA客户端名称为10个字符，端口号为5个字符，CLI条目为15个字符，DNIS条目为20个字符，则可以在达到16 KB限制之前添加450行项目。

注：在定义NAR之前，请确保已建立要在该NAR中使用的要素。因此，您必须指定所有NAF和NDG，并定义所有相关AAA客户端，然后才能将它们作为NAR定义的一部分。有关详细信息，[请参阅关于网络访问限制部分](#)。

要添加共享NAR，请完成以下步骤：

1. 在导航栏中，单击“共享配置文件组件”。系统将显示Shared Profile Components窗口。




2. 单击Network Access Restrictions。



Shared Profile Components

Select

Network Access Restrictions 	
Name	Description
None Defined	

Add Cancel

3. 单击 **Add**。系统将显示Network Access Restriction窗口。

Shared Profile Components

Network Access Restriction

Name:

Description:

Define IP-based access restrictions

Table Defines:

AAA Client	Port	Src IP Address
<input type="text"/>		
<input type="button" value="remove"/>		
AAA Client	<input type="text" value="All AAA Clients"/>	<input type="text"/>
Port	<input type="text"/>	<input type="text"/>
Src IP Address	<input type="text"/>	<input type="text"/>
<input type="button" value="enter"/>		

Define CLI/DNIS-based access restrictions

Table Defines:

AAA Client	Port	CLI	DNIS
<input type="text"/>			

- 在“名称”框中，输入新共享NAR的名称。**注意：**名称最多可包含31个字符。不允许前导空格和尾随空格。名称不能包含以下字符：左括号(())、右括号(())、逗号(,)或斜杠(/)。
- 在“说明”框中，输入新共享NAR的说明。说明最多可以有 30,000 个字符。
- 如果要根据IP编址允许或拒绝访问：选中**定义基于IP的访问说明**复选框。要指定是否列出允许或拒绝的地址，请从表定义列表中选择适用的值。选择或在每个框中输入适用信息：**AAA Client** — 选择**All AAA clients**，或NDG的名称、NAF或允许或拒绝访问的单个AAA客户端。**Port** — 输入要允许或拒绝访问的端口的编号。您可以使用星号(*)作为通配符，允许或拒绝对所选AAA客户端上所有端口的访问。**Src IP Address** — 输入执行访问限制时要过滤的IP地址。您可以使用星号(*)作为通配符来指定所有IP地址。**注意：**AAA客户端列表以及端口和源IP地址框中的字符总数不得超过1024。虽然ACS在添加NAR时接受1024个以上字符，但您无法编辑NAR，并且ACS无法将其准确应用到用户。单击 Enter。AAA客户端、端口和地址信息在表中显示为行项。重复步骤c和d以输入其他基于IP的行项目。

7. 如果要根据呼叫位置或IP地址以外的值允许或拒绝访问：选中定义**基于CLI/DNIS的访问限制**复选框。要指定是否从“表定义”(Table Defines)列表中列出允许或拒绝的位置，请选择适用的值。要指定此NAR应用的客户端，请从AAA客户端列表中选择以下值之一：NDG的名称特定AAA客户端的名称所有AAA客户端**提示**：仅列出您已配置的NDG。要指定此NAR应过滤的信息，请在以下框中输入值（如适用）：**提示**：可以输入星号(*)作为通配符，以指定全部为值。**Port** — 输入要过滤的端口的编号。**CLI** — 输入要过滤的CLI编号。您还可以使用此框根据CLI以外的值（如IP地址或MAC地址）限制访问。有关详细信息，[请参阅关于网络访问限制部分](#)。**DNIS** — 输入要过滤的拨入号码。**注意**：AAA客户端列表和端口、CLI和DNIS框中的字符总数不得超过1024。虽然ACS在添加NAR时接受1024个以上字符，但您无法编辑NAR，并且ACS无法将其准确应用到用户。单击 Enter。指定NAR行项的信息将显示在表中。重复步骤c至e以输入其他非基于IP的NAR行项目。单击**Submit**以保存共享的NAR定义。ACS保存共享NAR并将其列在“网络访问限制”(Network Access Restrictions)表中。

[编辑共享NAR](#)

要编辑共享NAR，请完成以下步骤：

1. 在导航栏中，单击“共享配置文件组件”。系统将显示Shared Profile Components窗口。
2. 单击**Network Access Restrictions**。系统将显示Network Access Restrictions表。
3. 在“名称”列中，点击要编辑的共享NAR。系统将显示Network Access Restriction窗口，并显示所选NAR的信息。
4. 编辑NAR的名称或说明（如果适用）。说明最多可以有 30,000 个字符。
5. 要编辑基于IP的访问限制表中的行项目，请执行以下操作：双击要编辑的行项目。行项目的信息将从表中删除并写入表下的框。根据需要编辑信息。**注意**：AAA客户端列表以及端口和源IP地址框中的字符总数不得超过1024。虽然ACS在添加NAR时可以接受1024个以上的字符，但您无法编辑此NAR，并且ACS无法将其准确应用于用户。单击 Enter。此行项目的编辑信息将写入基于IP的访问限制表。
6. 要从基于IP的访问限制表中删除行项目，请执行以下操作：选择行项目。在表下，单击“**删除**”。行项目将从基于IP的访问限制表中删除。
7. 要编辑CLI/DNIS访问限制表中的行项目，请执行以下操作：双击要编辑的行项目。行项目的信息将从表中删除并写入表下的框。根据需要编辑信息。**注意**：AAA客户端列表和端口、CLI和DNIS框中的字符总数不得超过1024。虽然ACS在添加NAR时可以接受1024个以上的字符，但您无法编辑此NAR，并且ACS无法将其准确应用于用户。单击**Enter**此行项目的编辑信息将写入CLI/DNIS访问限制表。
8. 要从CLI/DNIS访问限制表中删除行项目：选择行项目。在表下，单击“**删除**”。行项目将从CLI/DNIS访问限制表中删除。
9. 单击**Submit**以保存您所做的更改。ACS使用新信息重新输入过滤器，该信息将立即生效。

[删除共享NAR](#)

注意：确保在删除共享NAR之前，删除该NAR与任何用户或组的关联。

要删除共享NAR，请完成以下步骤：

1. 在导航栏中，单击“共享配置文件组件”。系统将显示Shared Profile Components窗口。
2. 单击**Network Access Restrictions**。
3. 点击要删除的共享NAR的名称。系统将显示Network Access Restriction窗口，并显示所选NAR的信息。

4. 在窗口底部，单击“删除”。系统将显示一个对话框，警告您您将要删除共享NAR。
5. 单击OK以确认要删除共享NAR。所选共享NAR将被删除。

设置用户的网络访问限制

使用用户设置的“高级设置”(Advanced Settings)区域中的“网络访问限制”(Network Access Restrictions)表可以通过三种方式设置NAR:

- 按名称应用现有共享NAR。
- 定义基于IP的访问限制，以在IP连接建立后允许或拒绝用户访问指定AAA客户端或AAA客户端上的指定端口。
- 定义基于CLI/DNIS的访问限制，以根据所使用的CLI/DNIS允许或拒绝用户访问。**注意：**您还可以使用基于CLI/DNIS的访问限制区域指定其他值。有关详细信息，[请参阅“网络访问限制”部分](#)。

通常，您从“共享组件”部分定义（共享）NAR，以便您可以将这些限制应用于多个组或用户。有关详细信息，[请参阅“添加共享NAR”部分](#)。您必须已选中“接口配置”部分的“高级选项”页上的“用户级网络访问限制”复选框，才能在Web界面中显示此组选项。

但是，您也可以使用ACS在“用户设置”(User Setup)部分中为单个用户定义并应用NAR。必须已在“接口配置”部分的“高级选项”页面上为单个用户IP过滤选项和单个用户CLI/DNIS过滤选项启用用户级网络访问限制设置，以便在Web界面中显示。

注意：当代理将身份验证请求转发到ACS时，终端访问控制器访问控制系统(TACACS+)的任何NAR请求都应用到转发AAA服务器的IP地址，而不是源AAA客户端的IP地址。

当您按用户创建访问限制时，ACS不对访问限制的数量实施限制，也不对每个访问限制的长度实施限制。但是，有严格的限制：

- 每个行项目的字段组合长度不能超过1024个字符。
- 共享NAR不能超过16 KB字符。支持的行项目数取决于每个行项目的长度。例如，如果创建基于CLI/DNIS的NAR，其中AAA客户端名称为10个字符，端口号为5个字符，CLI条目为15个字符，DNIS条目为20个字符，则可以在达到16 KB限制之前添加450行项目。

要为用户设置NAR，请完成以下步骤：

1. 执行添加基本用户[帐户的步骤1至3](#)。“用户设置编辑”窗口打开。您添加或编辑的用户名显示在窗口顶部。

User Setup

Advanced Settings

Network Access Restrictions (NAR) ?

Shared Network Access Restrictions

Only Allow network access when

- All selected NARs result in permit
- Any one selected NAR results in permit

NARs
testnar

>><>

<<><

Selected NARs

View IP NARView CLI/DNIS NAR

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	Address

remove

AAA Client All AAA Clients

Port

Address

SubmitDeleteCancel

2. 要将之前配置的共享NAR应用于此用户：注：要应用共享NAR，必须在“共享配置文件组件”部分的“网络访问限制”下配置了共享NAR。有关详细信息，[请参阅“添加共享NAR”部分](#)。选中 **Only Allow network access when** 复选框。要指定是否必须应用一个或所有共享NAR才能允许用户访问，请选择一个（如果适用）：所有选定的NARS都会产生允许。任何一个选择的NAR都会导致允许。在NAR列表中选择共享NAR名称，然后点击 —>（右箭头按钮）将该名称移动到Selected NARs列表中。提示：要查看您选择应用的共享NAR的服务器详细信息，可

以点击视图IP NAR或查看CLID/DNIS NAR (如果适用)。

3. 要定义并应用NAR (针对此特定用户)，该NAR根据IP地址或IP地址和端口允许或拒绝此用户访问：**注：您应从“共享组件”部分定义大多数NAR，以便您可以将它们应用于多个组或用户。有关详细信息，请参阅“添加共享NAR”部分。**在Network Access Restrictions表中，在Per User Defined Network Access Restrictions下，选中**Define IP-based access restrictions**复选框。要指定后续列表是指定允许还是拒绝的IP地址，请从表定义列表选择一个：**允许的呼叫/接入点位置拒绝的呼叫/接入点位置**在以下框中选择或输入信息：**AAA Client** — 选择**All AAA Clients**，或网络设备组(NDG)的名称，或允许或拒绝访问的单个AAA客户端的名称。**Port** — 输入允许或拒绝访问的端口号。您可以使用星号(*)作为通配符，允许或拒绝对所选AAA客户端上所有端口的访问。**Address** — 输入执行访问限制时要使用的IP地址。您可以使用星号(*)作为通配符。**注意：AAA客户端列表中的字符总数，以及端口和源IP地址框的字符总数不得超过1024。虽然ACS在添加NAR时接受1024个以上字符，但您无法编辑NAR，并且ACS无法将其准确应用到用户。**单击 Enter。指定的AAA客户端、端口和地址信息显示在AAA客户端列表上方的表中。
4. 要根据呼叫位置或已建立的IP地址以外的值允许或拒绝此用户访问，请执行以下操作：选中**定义基于CLI/DNIS的访问限制**复选框。要指定后续列表是指定允许还是拒绝的值，请从表定义列表选择一个：**允许的呼叫/接入点位置拒绝的呼叫/接入点位置**按如下所示填写框：**注意：必须在每个框中输入。您可以使用星号(*)作为值全部或部分的通配符。您使用的格式必须与从AAA客户端接收的字符串的格式匹配。您可以从RADIUS记帐日志中确定此格式。****AAA Client** — 选择**All AAA Clients**，或NDG的名称，或允许或拒绝访问的单个AAA客户端的名称。**PORT** — 输入允许或拒绝访问的端口号。您可以使用星号(*)作为通配符来允许或拒绝访问所有端口。**CLI** — 输入允许或拒绝访问的CLI编号。您可以使用星号(*)作为通配符，根据部分号码允许或拒绝访问。**提示：如果要根据其他值 (如Cisco Aironet客户端MAC地址) 限制访问，请使用CLI条目。有关详细信息，请参阅关于网络访问限制部分。****DNIS** — 输入允许或拒绝访问的DNIS编号。使用此条目根据用户将拨打的号码限制访问。您可以使用星号(*)作为通配符，根据部分号码允许或拒绝访问。**提示：如果要根据其他值 (如Cisco Aironet AP MAC地址) 限制访问，请使用DNIS选择。有关详细信息，请参阅关于网络访问限制部分。****注意：AAA客户端列表和端口、CLI和DNIS框中的字符总数不得超过1024。虽然ACS在添加NAR时接受1024个以上字符，但您无法编辑NAR，并且ACS无法将其准确应用到用户。**单击 Enter。指定AAA客户端、端口、CLI和DNIS的信息显示在AAA客户端列表上方的表中。
5. 如果完成用户帐户选项的配置，请单击**Submit**以记录这些选项。

为用户组设置网络访问限制

使用组设置中的网络访问限制表以三种不同的方式应用NAR:

- 按名称应用现有共享NAR。
- 定义基于IP的组访问限制，以在IP连接建立后允许或拒绝对指定AAA客户端或AAA客户端上指定端口的访问。
- 定义基于CLI/DNIS的组NAR，以允许或拒绝对使用的CLI编号或DNIS编号的访问，或同时允许或拒绝访问两者。**注意：您还可以使用基于CLI/DNIS的访问限制区域指定其他值。有关详细信息，请参阅关于网络访问限制部分。**

通常，您从“共享组件”部分定义 (共享) NAR，以便这些限制可以应用于多个组或用户。有关详细信息，请参阅“添加共享NAR”部分。必须选中“接口配置”(Interface Configuration)部分的“高级选项”(Advanced Options)页面上的“组级共享网络访问限制”(Group-Level Shared Network Access Restriction)复选框，这些选项才会显示在ACS Web界面中。

但是，您也可以使用ACS在“组设置”(Group Setup)部分中为单个组定义并应用NAR。对于要在ACS

Web界面中显示的单组基于IP的过滤器选项和单组基于CLI/DNIS的过滤器选项，必须选中“接口配置”部分的“高级选项”页面下的“组级网络访问限制”设置。

注意：当代理将身份验证请求转发到ACS服务器时，RADIUS请求的任何NAR都应用到转发AAA服务器的IP地址，而不是源AAA客户端的IP地址。

要为用户组设置NAR，请完成以下步骤：

1. 在导航栏中，单击 **Group Setup**。“组设置选择”窗口打开。
2. 从“组”列表中选择一个组，然后单击“编辑设置”。组名称显示在“组设置”窗口的顶部。

