Cisco Secure ACS ：用户和用户组的有AAA客户端的网络访问限制

目录

简介

本文描述如何配置网络访问限制(NAR)在与AAA客户端的思科安全访问控制服务器(ACS) 4.x版本(包括路由器， PIX， ASA，无线控制器)用户和用户组的。

先决条件

要求

本文创建，假设Cisco Secure ACS和AAA客户端适当地配置并且工作。

使用的组件

本文档中的信息根据Cisco Secure ACS 3.0及以上版本。

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

此部分描述NARs，并且提供更多的指导信息配置与管理共享NARs。

此部分包括以下主题：

关于网络访问限制

NAR是定义，您在ACS做您必须符合的，另外的情况，在用户能访问网络前。ACS运用这些情况通过使用从您的AAA客户端发送的属性的信息。虽然您能设置NARs用几个方式，所有根据匹配AAA客户端发送的属性信息。所以，您必须了解属性的格式和内容您的AAA客户端发送，如果要使用有效NARs。

设置 NAR 时，可以选择过滤器是积极运行还是消极运行。即在NAR您是否指定根据从AAA客户端发送的信息允许或拒绝网络访问，当与在NAR存储的信息比较。不过，如果 NAR 没有充足的信息以运行，将会默认为拒绝访问。此表显示这些情况：

	基于IP的	**基于的非IP**	**不足的信息**
Permit	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NAR过滤器的两种类型：

- **基于IP的过滤器**—基于IP的NAR过滤根据最终用户客户端和AAA客户端的IP地址的限制访问。欲知更多信息，请参阅基于IP的NAR过滤器部分。
- **基于非IP的过滤器**—基于非IP的NAR过滤根据从AAA客户端发送的值的简单串比较的限制访问。值可以是主叫线路识别(CLI)编号、拨号号码识别服务(DNIS)编号、MAC地址，或者起源于客户端的另一个值。为了使运行此种的NAR，在NAR说明的值必须完全地匹配什么从客户端发送，包括使用任何格式。例如，电话号码(217) 555-4534不匹配217-555-4534。欲知更多信息，请参阅基于非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。欲知更多信息，请参阅集合网络访问限制关于用户或集合网络访问限制关于用户组部分。然而，在ACS的共享配置文件组件部分您能创建和命名共享NAR，无需直接援引任何用户或用户组。您给予共享NAR可以在ACS Web接口的其他部分中被参考的名称。然后，当您组成用户或用户组时，您什么都不能选择，一个或者多个共享的限制应用。当您指定多个共享的NARs的应用程序给用户或用户组时，您选择两个访问标准之一：

- 所有选定过滤器必须允许。
- 所有一个选择的过滤器必须允许。

您必须了解与不同种类的NARs涉及的优先级顺序。这是NAR过滤命令：

1. 在用户级的共享NAR
2. 在社团级别的共享NAR
3. 在用户级的非共享的NAR

4. 在社团级别的非共享的NAR

您应该也了解**访问否认在所有级别的优先于不拒绝访问的设置在另一个级别**。这是在ACS的一例外对裁决用户级设置改写组级设置。例如，特定用户不也许有应用的NAR限制在用户级。然而，如果该用户属于由共享或非共享的NAR限制的组，用户是拒绝访问。

共享NARs在ACS内部数据库被保留。您能使用ACS备份和恢复功能备份，并且恢复他们。您能与其他配置一起也复制共享NARs，到附属ACSs。

关于基于IP的NAR过滤器

对于基于IP的NAR过滤器， ACS使用属性如显示，依靠认证请求的AAA协议：

- **如果使用TACACS+** —使用从TACACS+启动数据包正文的`rem_addr`字段。**注意：** 当认证请求由ACS的时代理转发， TACACS+请求的所有NARs应用对转发AAA服务器的IP地址，不对产生AAA客户端的IP地址。
- **如果使用RADIUS IETF** —必须使用呼叫站点`id` (属性31)。**注意：** 基于IP的NAR过滤器工作，只有当ACS接收Radius呼叫站点Id (31个)属性。呼叫站点Id (31)必须包含有效IP地址。如果它不，将下跌对DNIS规则。

不提供满足的IP地址信息例如的AAA客户端(防火墙一些类型)不支持全双工NAR功能。

基于IP的限制的其他属性，每份协议，包括NAR字段如显示：

- **如果使用TACACS+** — ACS的NAR字段使用这些值：**AAA客户端**— nas-ip-address从在socket的源地址被采取在ACS和TACACS+客户端之间。**端口**—端口字段从TACACS+启动数据包正文被采取。

关于基于非IP的NAR过滤器

一个基于非IP的NAR过滤器(即一个基于DNIS/CLI的NAR过滤器)是允许的或拒绝的呼叫或问题列表的访问位置您能使用限制AAA客户端，当您没有一已建立基于IP的连接时。非基于 IP 的 NAR 功能通常使用 CLI 编号和 DNIS 编号。

然而，当您在CLI位置时输入IP地址，您能使用基于非IP的过滤器;既使当AAA客户端不使用支持CLI或DNIS的一个Cisco IOS软件版本。在对输入CLI的另一例外，您能输入MAC地址允许或拒绝访问。例如，当您使用Cisco Aironet AAA客户端。同样，您可能在DNIS位置输入Cisco Aironet AP MAC地址。什么的格式您在CLI方框指定— CLI、IP地址或者MAC地址—必须匹配什么的格式您从您的AAA客户端接收。您能确定从您的RADIUS记帐日志的此格式。

基于DNIS/CLI的限制的属性，每份协议，包括NAR字段如显示：

- **如果使用TACACS+** —列出的NAR字段使用这些值：**AAA客户端**— `nas-ip-address`从在socket的源地址被采取在ACS和TACACS+客户端之间。**端口**—使用TACACS+启动数据包正文的。**CLI** —使用TACACS+启动数据包正文的`rem-addr`字段。**DNIS** —使用从TACACS+启动数据包正文采取的`rem-addr`字段。在rem-addr数据开始与斜线的案件中(/)， DNIS字段包含rem-addr数据，不用斜线(/)。**注意：** 当认证请求由ACS的时代理转发， TACACS+请求的所有NARs应用对转发AAA服务器的IP地址，不对产生AAA客户端的IP地址。
- **如果使用RADIUS** —列出的NAR字段使用这些值：**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`ID` (属

性31)。**DNIS** —使用ID (属性30)。

当您指定NAR时，您能使用星号(*)作为通配符所有值，或者作为任何值一部分设立范围。必须符合所有值或条件在NAR说明为了NAR能限制访问。这意味着值包含布尔和。

添加共享NAR

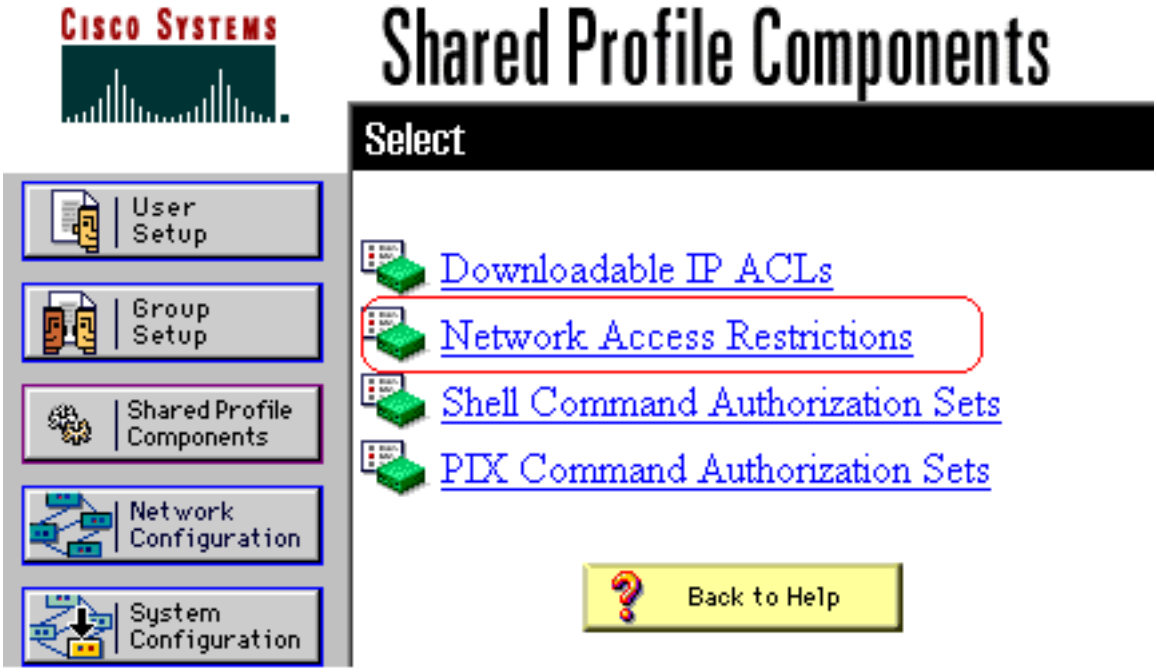
您能创建包含许多访问限制的共享NAR。虽然ACS Web接口不强制执行限额到访问限制数量在共享NAR的或对长度每个访问限制，您必须遵守这些限额：

- 字段的组合每行项目的不可以超出1024个字符。
- 共享NAR不能有超过字符16 KB。支持的线路数项目取决于长度每行项目。例如，如果创建AAA客户端名称是10个字符的基于CLI/DNIS的NAR，端口号是5个字符， CLI条目是15个字符，并且DNIS条目是20个字符，您能添加450行项目，在您达到16 KB限制前。

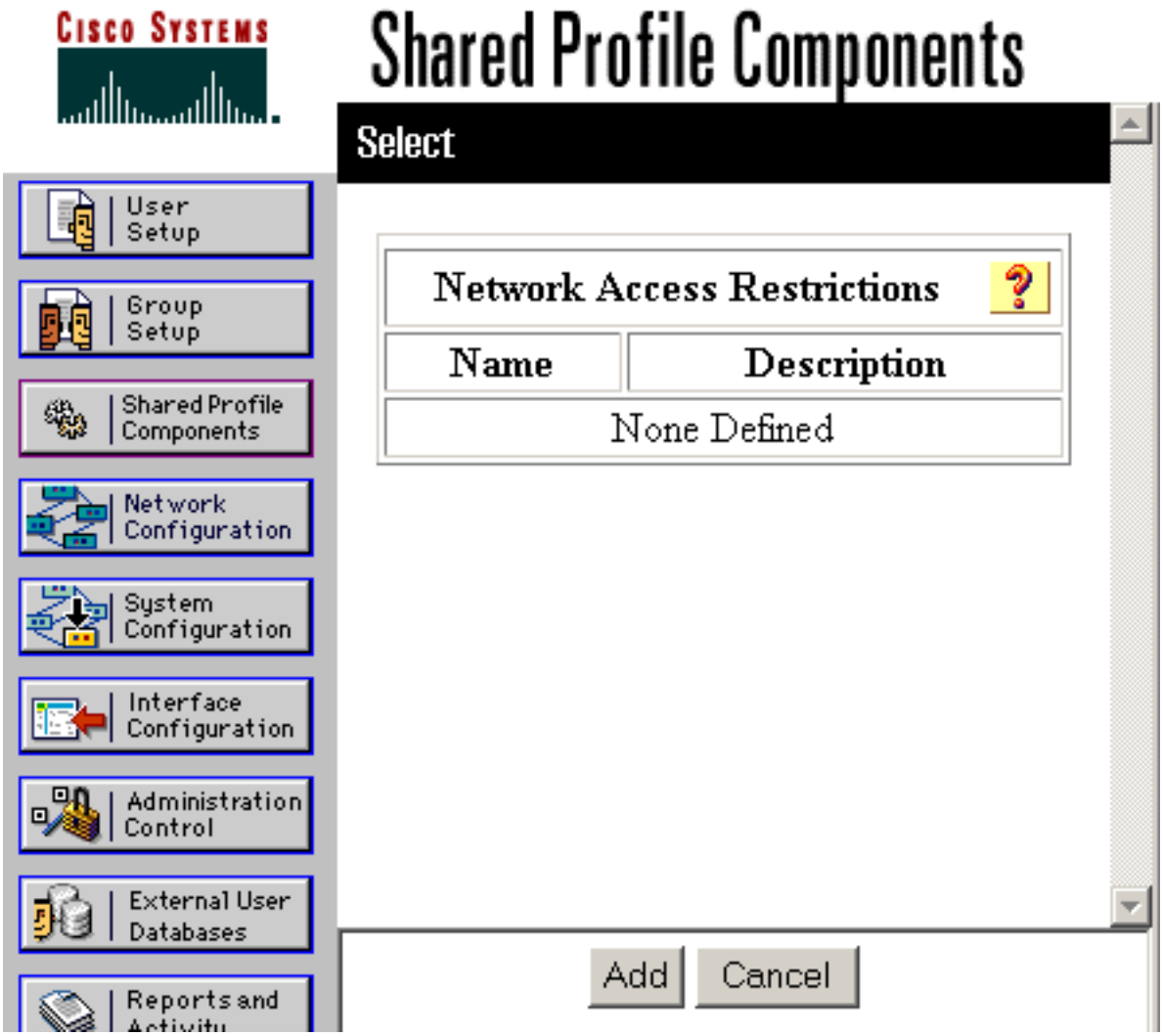
注意： 在您定义了NAR前，请确定您设立了您在该NAR打算使用的元素。所以，在您做他们一部分的NAR定义前，您一定指定所有NAFs和NDGs和定义所有相关AAA客户端。欲知更多信息，请参阅网络访问Restrictions部分。

完成这些步骤为了添加共享NAR ：

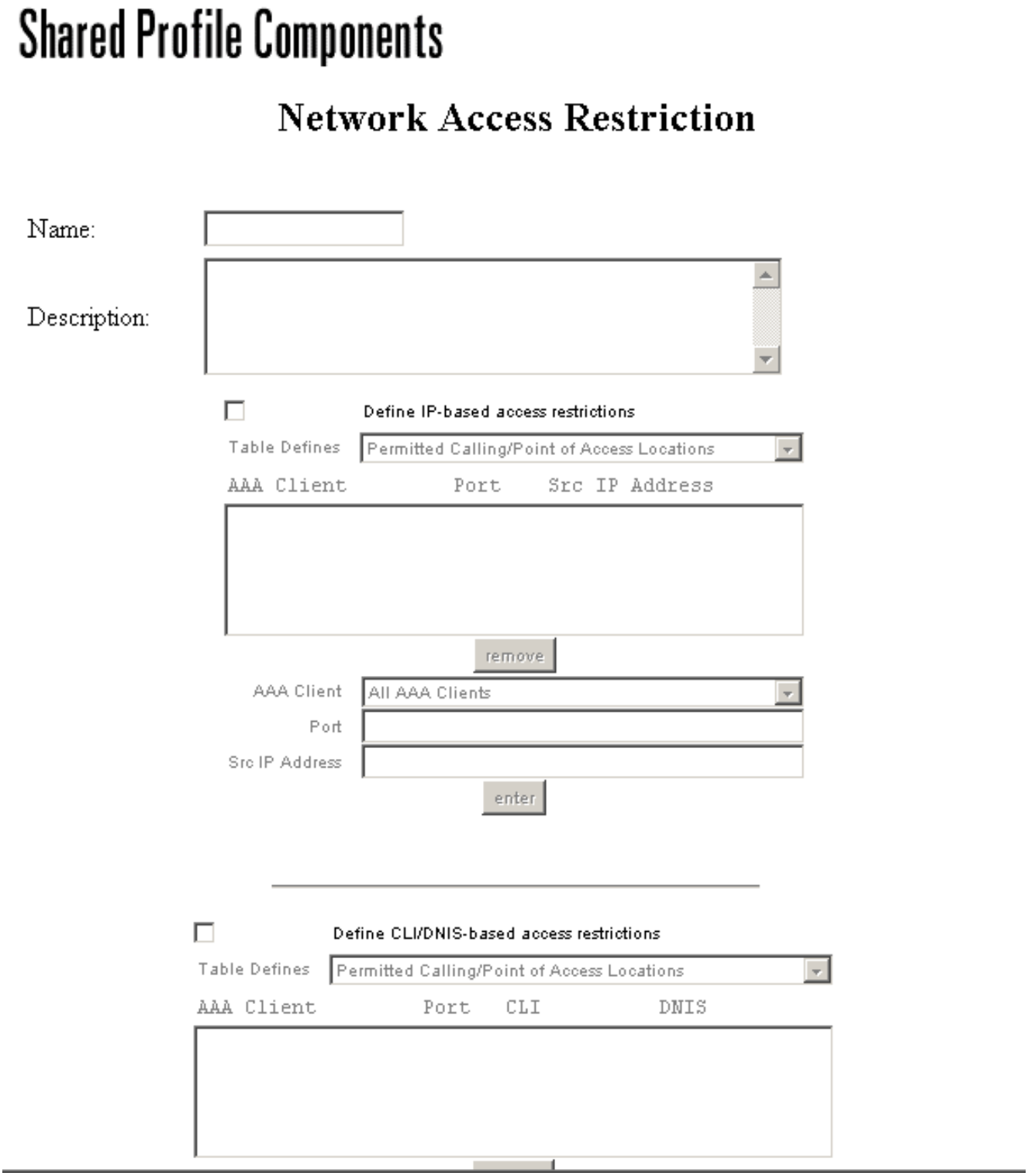
1. 在导航条，请点击**共享配置文件组件**。共享配置文件组件窗口出现。



2. 点击**网络访问限制**。



3. 单击 **Add**。网络访问限制窗口出现。



4. 在名称框中，请输入一名称对于新建的共享NAR。**注意：** 名称能包含31个字符。导致和句尾空格没有允许。名称不能包含这些字符：左侧托架([)， right bracket (])，逗号()，或者斜线(/)。
5. 在说明方框中，请输入新建的共享NAR的说明。说明可以是30,000个字符。
6. 如果要允许或拒绝根据IP寻址的访问：检查**定义基于IP的访问说明**复选框。为了从表指定您是否列出允许或拒绝的地址，定义了列表，选择可适用的值。选择或输入在这些方框中的每一个的可适用的信息：**AAA客户端**—选择**所有AAA客户端**或者NDG或者氟化钠或者个人AAA客户端的名称，访问允许或拒绝。**波尔特**—输入您要允许或拒绝访问端口的编号。您能使用星号(*)作为通配符允许或拒绝对所有端口的访问选定AAA客户端的。**Src IP地址**—输入IP地址过滤在，当执行的访问限制。您能使用星号(*)作为通配符指定所有IP地址。**注意：** 字符总数在AAA客户端列表的和波尔特和Src IP地址框，不能超过1024。虽然ACS接受超过1024个字符，当您添加NAR时，您不能编辑NAR和ACS不能准确地应用它对用户。单击 Enter。AAA客户

端、端口和地址信息在表里出现作为一行项目。重复步骤c和d为了输入另外的基于IP的行项目。

7. 如果要允许或拒绝根据呼叫位置或值的访问除IP地址之外：检查**定义CLI/DNIS基于访问限制**复选框。为了指定您是否列出允许或拒绝从表定义了列表的位置，请选择可适用的值。为了指定此NAR适用的客户端，请选择从AAA客户端列表的这些值之一：NDG的名称特定AAA客户端的名称所有AAA客户端**提示**： 您已经配置仅的NDGs是列出的。为了指定此NAR应该过滤的信息，回车在这些方框重视，如可适用：**提示**： 您能输入星号(*)作为通配符指定**所有**作为值。**波尔特**—输入过滤端口的编号。**CLI** —输入过滤的CLI编号。您能也使用此方框限制根据值的访问除CLIs之外，例如IP地址或MAC地址。欲知更多信息，请参阅网络访问Restrictions部分。**DNIS** —输入拨号对在哪些的编号过滤。**注意**： 字符总数在AAA客户端列表和波尔特、CLI和DNIS方框的不能超过1024。虽然ACS接受超过1024个字符，当您添加NAR时，您不能编辑NAR和ACS不能准确地应用它对用户。单击 Enter。指定NAR行项目的信息在表里出现。重复步骤c至e为了输入另外的基于非IP的NAR行项目。单击**提交**为了保存共享NAR定义。ACS在**网络访问**限制表里保存共享NAR并且列出它。

编辑共享NAR

完成这些步骤为了编辑共享NAR ：

1. 在导航条，请点击**共享配置文件组件**。共享配置文件组件窗口出现。
2. 点击**网络访问限制**。网络访问限制表出现。
3. 在命名列，请点击您要编辑的共享NAR。网络访问限制窗口出现并且显示选定NAR的信息。
4. 编辑NAR的名称或说明，如可适用。说明可以是30,000个字符。
5. 为了编辑一行项目在基于IP的限制表里：双击您要编辑的行项目。行项目的信息从表删除并且写入到在表下的方框。编辑信息，如所需要。**注意**： 字符和波尔特和Src IP地址框总数AAA客户端列表的不能超过1024。虽然ACS能接受超过1024个字符，当您添加NAR时，您不能编辑这样NAR和ACS不能准确地应用它对用户。单击 Enter。此行项目的编辑的信息写入对基于IP的限制表。
6. 为了从基于IP的限制表删除行项目：选择行项目。在表下，请点击**删除**。行项目从基于IP的限制表删除。
7. 为了编辑一行项目在CLI/DNIS访问限制表里：双击您要编辑的行项目。行项目的信息从表删除并且写入到在表下的方框。编辑信息，如所需要。**注意**： 字符总数在AAA客户端列表和波尔特、CLI和DNIS方框的不能超过1024。虽然ACS能接受超过1024个字符，当您添加NAR时，您不能编辑这样NAR和ACS不能准确地应用它对用户。按回车此行项目的编辑的信息写入对CLI/DNIS访问限制表。
8. 为了从CLI/DNIS访问限制表删除行项目：选择行项目。在表下，请点击**删除**。行项目从CLI/DNIS访问限制表删除。
9. 单击**提交**为了保存您做了的变动。ACS重新输入有最新信息的过滤器，立即生效。

删除共享NAR

注意： 保证您取消共享NAR的关联给所有用户或组，在您删除该NAR前。

完成这些步骤为了删除共享NAR ：

1. 在导航条，请点击**共享配置文件组件**。共享配置文件组件窗口出现。
2. 点击**网络访问限制**。
3. 点击您要删除共享NAR的名称。网络访问限制窗口出现并且显示选定NAR的信息。

4. 在窗口的底部，请点击**删除**。对话框警告您您将删除共享NAR。
5. 点击OK键为了确认您要删除共享NAR。选定共享NAR删除。

设置用户的网络访问限制

您在用户设置先进的设置地区使用网络访问限制表设置NARs用三种方式：

- 应用名义上存在共享NARs。
- 当IP连接设立了时，请定义基于IP的访问限制允许或拒绝用户访问对一个指定的AAA客户端或对AAA客户端的指定的端口。
- 定义基于CLI/DNIS的访问限制允许或拒绝使用根据CLI/DNIS的用户访问。**注意：** 您能也使用基于CLI/DNIS的访问限制区域指定其他值。欲知更多信息，请参阅网络访问Restrictions部分。

一般，您定义了(共享) NARs从共享组件部分的内部，以便您能运用这些限制对超过一个组或用户。欲知更多信息，请参阅添加一个共享NAR部分。您在Web接口一定选择在接口配置部分的高级选项页的**用户级网络访问限制**复选框此一组选项的能出现。

然而，您能也使用ACS定义和申请NAR单个用户从User Setup部分的内部。您在Web接口一定启用设置在接口配置部分的高级选项页的**用户级网络访问限制**单个用户基于IP的过滤器选项和单个用户基于CLI/DNIS的过滤器选项的能出现。

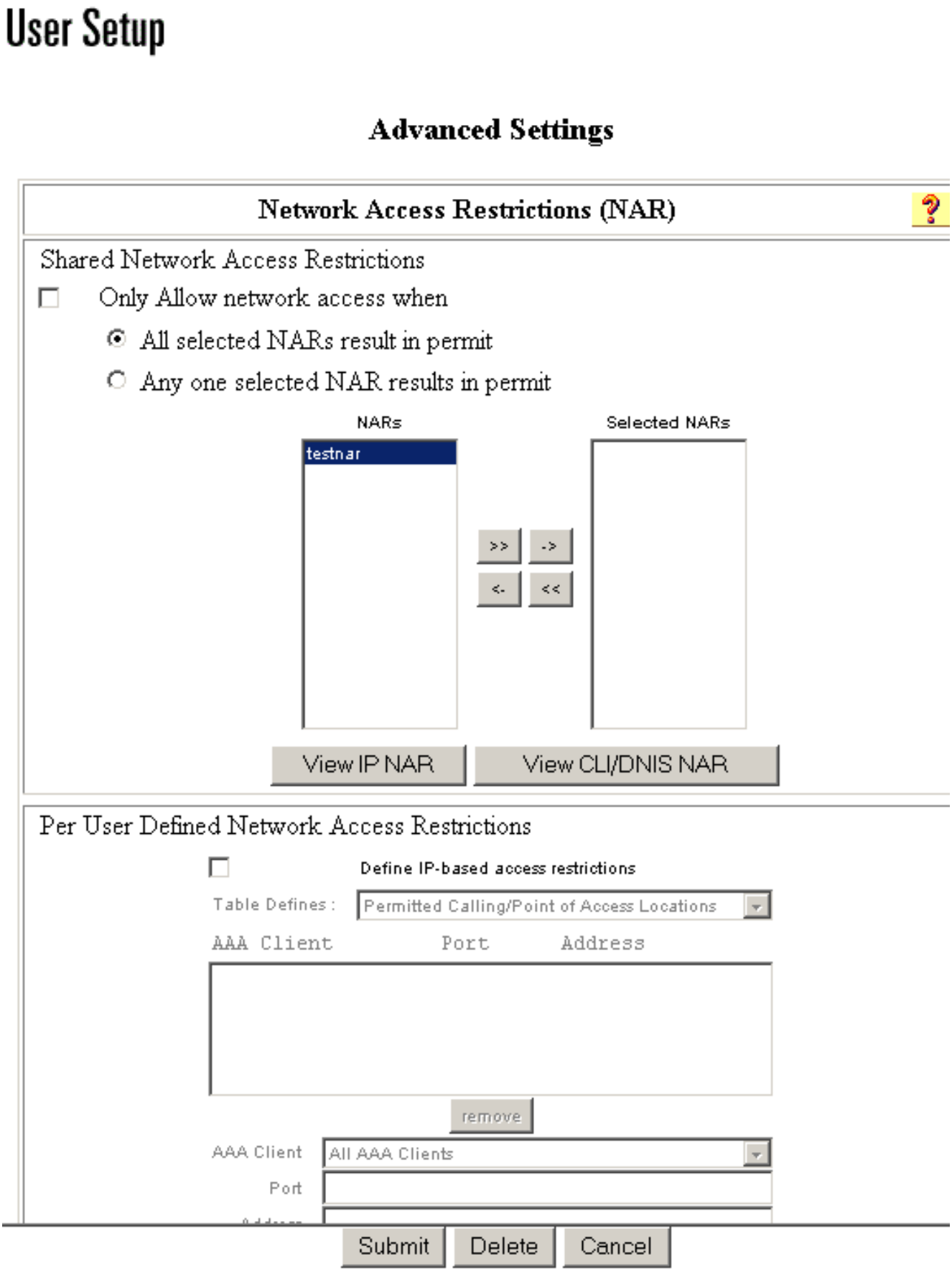
注意： 当认证请求由ACS的时代理转发，终端访问控制器访问控制系统(TACACS+)请求的所有NARs应用对转发AAA服务器的IP地址，不对产生AAA客户端的IP地址。

当您逐个用户时创建访问限制， ACS不强制执行限额到访问限制数量，并且不强制执行限制对长度每个访问限制。然而，有严格限额：

- 字段的组合每行项目的不可以超出长度1024个字符。
- 共享NAR不能有超过字符16 KB。支持的线路数项目取决于长度每行项目。例如，如果创建AAA客户端名称是10个字符的基于CLI/DNIS的NAR，端口号是5个字符， CLI条目是15个字符，并且DNIS条目是20个字符，您能添加450行项目，在您达到16 KB限制前。

完成这些步骤为了设置用户的NARs ：

1. 执行步骤1至3添加一个基本用户帐户。Edit窗口的用户设置打开。您添加或编辑的用户名出现在窗口顶部。



2. 为了应用以前已配置的共享NAR对此用户：**注意：** 为了应用共享NAR，您一定配置它在共享配置文件组件部分的网络访问限制下。欲知更多信息，请参阅添加一个共享NAR部分。检查**唯一允许网络访问，当**复选框。为了指定一或所有共享NARs是否必须申请用户是允许的访问，请选择一，如可适用：所有选定NARS导致permit。所有一个选择的NAR导致permit。选择在NARs列表的一共享NAR名称，然后单击--> (右箭头按钮)搬入名称选定NARs列表。**提示**：为了查看您选择应用共享NARs的服务器详细信息，您能点击**视图IP NAR**或**观看CLID/DNIS**

NAR，如可适用。

3. 为了定义和申请NAR，此特定用户，允许或拒绝根据IP地址的此用户访问，或者IP地址和端口：**注意：** 您应该定义多数NARs从共享组件部分的内部，以便您能应用他们对超过一个组或用户。欲知更多信息，请参阅添加一个共享NAR部分。在网络访问限制表里，下每用户定义的网络访问限制，请检查**定义基于IP的访问限制**复选框。为了从表指定随后的列表是否指定允许的或拒绝的IP地址，定义了列表，选择一：**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**选择或输入在这些方框的信息：**AAA客户端**—选择**所有AAA客户端**或者网络设备组(NDG)的名称，或者个人AAA客户端的名称，允许或拒绝访问。**波尔特**—输入允许或拒绝访问端口的编号。您能使用星号(*)作为通配符允许或拒绝对所有端口的访问选定AAA客户端的。**地址**—输入IP地址或地址使用，当执行的访问限制。您能使用星号(*)作为通配符。**注意：** 字符总数在AAA客户端列表的和波尔特和Src IP地址框不能超过1024。虽然ACS接受超过1024个字符，当您添加NAR时，您不能编辑NAR和ACS不能准确地应用它对用户。单击 Enter。指定的AAA客户端、端口和地址信息在上表出现AAA客户端列表。
4. 为了允许或拒绝根据呼叫位置或值的此用户访问除一个已建立IP地址之外：检查**定义CLI/DNIS基于访问限制**复选框。为了从表指定随后的列表是否指定允许的或拒绝的值，定义了列表，选择一：**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**完成方框如显示：**注意：** 您必须做在每个方框的一个条目。您能使用星号(*)作为通配符值的所有或部分。您使用的格式必须匹配您从您的AAA客户端接收字符串的格式。您能确定从您的RADIUS记帐日志的此格式。**AAA客户端**—选择**所有AAA客户端**或者NDG的名称或者个人AAA客户端的名称，允许或拒绝访问。**波尔特**—输入允许或拒绝访问端口的编号。您能使用星号(*)作为通配符允许或拒绝对所有端口的访问。**CLI** —输入允许或拒绝访问的CLI编号。您能使用星号(*)作为通配符允许或拒绝根据一部分的访问的编号。**提示：** 如果要限制根据其他值的访问例如Cisco Aironet客户端MAC地址，请使用CLI条目。欲知更多信息，请参阅网络访问Restrictions部分。**DNIS** —输入允许或拒绝访问的DNIS编号。请使用此条目限制根据用户将拨号的编号的访问。您能使用星号(*)作为通配符允许或拒绝根据一部分的访问的编号。**提示：** 如果要限制根据其他值的访问例如Cisco Aironet AP MAC地址，请使用DNIS选择。欲知更多信息，请参阅网络访问Restrictions部分。**注意：** 字符总数在AAA客户端列表和**波尔特**、**CLI**和**DNIS**方框的不能超过1024。虽然ACS接受超过1024个字符，当您添加NAR时，您不能编辑NAR和ACS不能准确地应用它对用户。单击 Enter。指定AAA客户端的信息，端口、CLI和DNIS在上表出现AAA客户端列表。
5. 如果完成配置用户帐户选项的，请单击**提交**为了记录选项。

设置用户组的网络访问限制

您在组建立使用网络访问限制表应用NARs用三种明显的方式：

- 应用名义上存在共享NARs。
- 当IP连接设立了时，请定义基于IP的组访问限制允许或拒绝访问对一个指定的AAA客户端或对AAA客户端的指定的端口。
- 定义基本组NARs允许或拒绝访问对或者两个，使用的CLI编号或者DNIS编号。**注意：** 您能也使用基于CLI/DNIS的访问限制区域指定其他值。欲知更多信息，请参阅网络访问Restrictions部分。

一般，您定义了(共享) NARs从共享组件部分的内部，以便这些限制能适用对超过一个组或用户。欲知更多信息，请参阅添加一个共享NAR部分。您在ACS Web接口必须检查在接口配置部分的**高级选项**页的**组级共享网络访问限制**复选框这些选项出现。

然而，您能也使用ACS定义和申请NAR一组从**Group Setup部分的内部**。您在ACS Web接口必须检

查**组级网络访问限制**设置在接口配置部分的高级选项页下组基于IP的过滤器选项和组基于CLI/DNIS的过滤器选项出现。

注意： 当认证请求由ACS服务器的时代理转发， RADIUS请求的所有NARs应用对转发AAA服务器的IP地址，不对产生AAA客户端的IP地址。

完成这些步骤为了设置用户组的NARs ：

1. 在导航栏中，单击 **Group Setup**。Select窗口的组建立打开。
2. 从组列表，请选择组，然后单击**编辑设置**。组的名称出现在组设置窗口顶部。