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

Contents

Introduction

本文描述如何用AAA客户端配置网络访问限制(NAR)在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。

Prerequisites

Requirements

本文被创建，假设适当配置Cisco Secure ACS和AAA客户端并且工作。

Components Used

本文的信息根据Cisco Secure ACS 3.0及以上版本。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

网络访问限制

此部分描述NARs，并且提供详细指令配置与管理共有的NARs。

此部分包含这些题目：

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适用这些情况通过使用信息从您的AAA客户端发送的属性。虽然您能设置NARs用几个方式，所有根据AAA客户端发送的配比的属性信息。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**
许可证	被准许的访问	拒绝访问	拒绝访问
拒绝	拒绝访问	被准许的访问	拒绝访问

ACS支持NAR过滤器的两种类型：

- **基于IP的过滤器**—基于IP的NAR过滤根据终端用户客户端和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的串比较的限制访问。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被发送，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。请参阅集网络访问限制关于用户或设置用户组部分的网络访问限制欲知更多信息。然而，在ACS的共享配置文件组件部分您能创建和命名共有的NAR，无需直接援引任何用户或用户组。您给予共有的NAR可以被参考ACS Web接口的其他部分的一个名字。然后，当您组成用户或用户组时，您什么都不能选择，一个或者多个共有的限制适用。当您指定多个共有的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：

- 所有所选的过滤器必须允许。
- 所有一台所选的过滤器必须允许。

您必须了解与不同种类的NARs有关的优先级顺序。这是NAR过滤命令：

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

4. 在社团级别的非共有的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，一个特定用户不也许有适用的NAR限制在用户级。然而，如果该用户属于由共有的或非共有的NAR限制的组，用户是拒绝访问。

共有的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有的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+启动信息包正文的`rem_addr`字段。**Note:** 当认证请求被对ACS时的代理转发， TACACS+请求的所有NARs适用于转发AAA服务器的IP地址，不于产生AAA客户端的IP地址。
- **如果使用RADIUS IETF** —必须使用呼叫位置`id` (属性31)。**Note:** 基于IP的NAR过滤器工作，只有当ACS接受Radius呼叫位置Id (31个)属性。呼叫位置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(防火墙的一些类型)不支持充分的NAR功能。

基于IP的限制的其他属性，每个协议，包括NAR字段如显示：

- **如果使用TACACS+** —在ACS的NAR字段使用这些值：**AAA客户端**— nas-ip-address从在插槽的源地址被采取在ACS和TACACS+客户端之间。**端口**— Port字段从TACACS+启动信息包正文被采取。

关于基于非IP的NAR过滤器

一台基于非IP的NAR过滤器(即一台基于DNIS/CLI的NAR过滤器)是允许的或被拒绝的呼叫或问题列表的您能使用限制AAA客户端的访问位置，当您没有被建立的基于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机箱指定— CLI、IP地址或者MAC地址—必须匹配什么的格式您从您的AAA客户端接受。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，每个协议，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`从在插槽的源地址被采取在ACS和TACACS+客户端之间。**端口**— TACACS+启动信息包正文的使用`Port`。**CLI** —使用在TACACS+启动信息包正文的`rem-addr`字段。**DNIS** —使用从TACACS+启动信息包正文采取的`rem-addr`字段。在rem-addr数据从斜线开始的案件(/)， DNIS字段包含rem-addr数据，不用斜线(/)。**Note:** 当认证请求被对ACS时的代理转发， TACACS+请求的所有NARs适用于转发AAA服务器的IP地址，不于产生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** —使用呼叫位

置ID (属性31)。**DNIS** —使用呼叫位置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。这意味着值包含一布尔型和。

添加共有的NAR

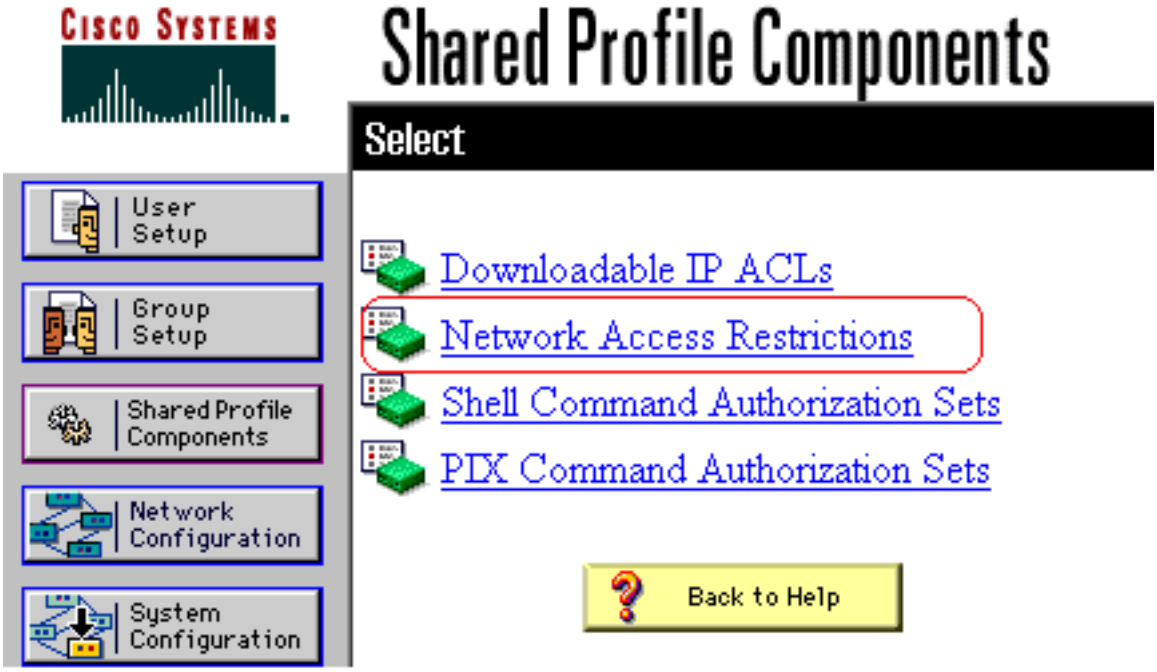
您能创建包含许多访问限制的共有的NAR。虽然ACS Web接口不强制执行限额对访问限制的数量在共有的NAR的或对每个访问限制的长度，您必须遵守这些限额：

- 字段的组合每行内容不可以超出1024个字符。
- 共有的NAR不能有超过字符16 KB。线路数支持的项目取决于每行内容的长度。例如，如果创建AAA客户端名是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行内容，在您达到16 KB限制前。

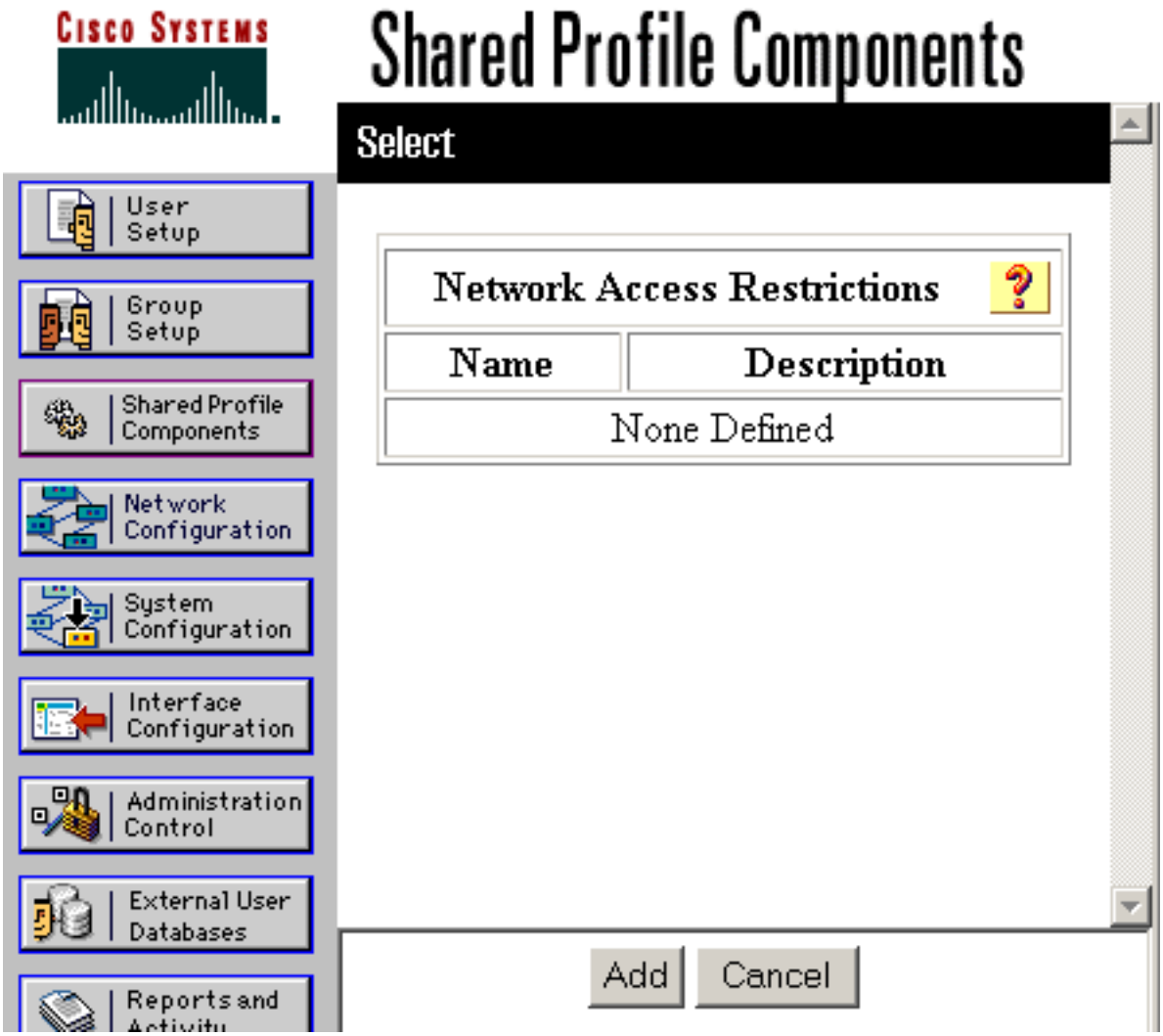
Note: 在您定义了NAR前，请确定您设立了您在该NAR打算使用的元素。所以，在您做他们一部分的NAR定义前，您一定指定了所有NAFs和NDGs和定义了所有相关AAA客户端。欲知更多信息，请参阅网络访问限制部分。

完成这些步骤为了添加共有的NAR ：

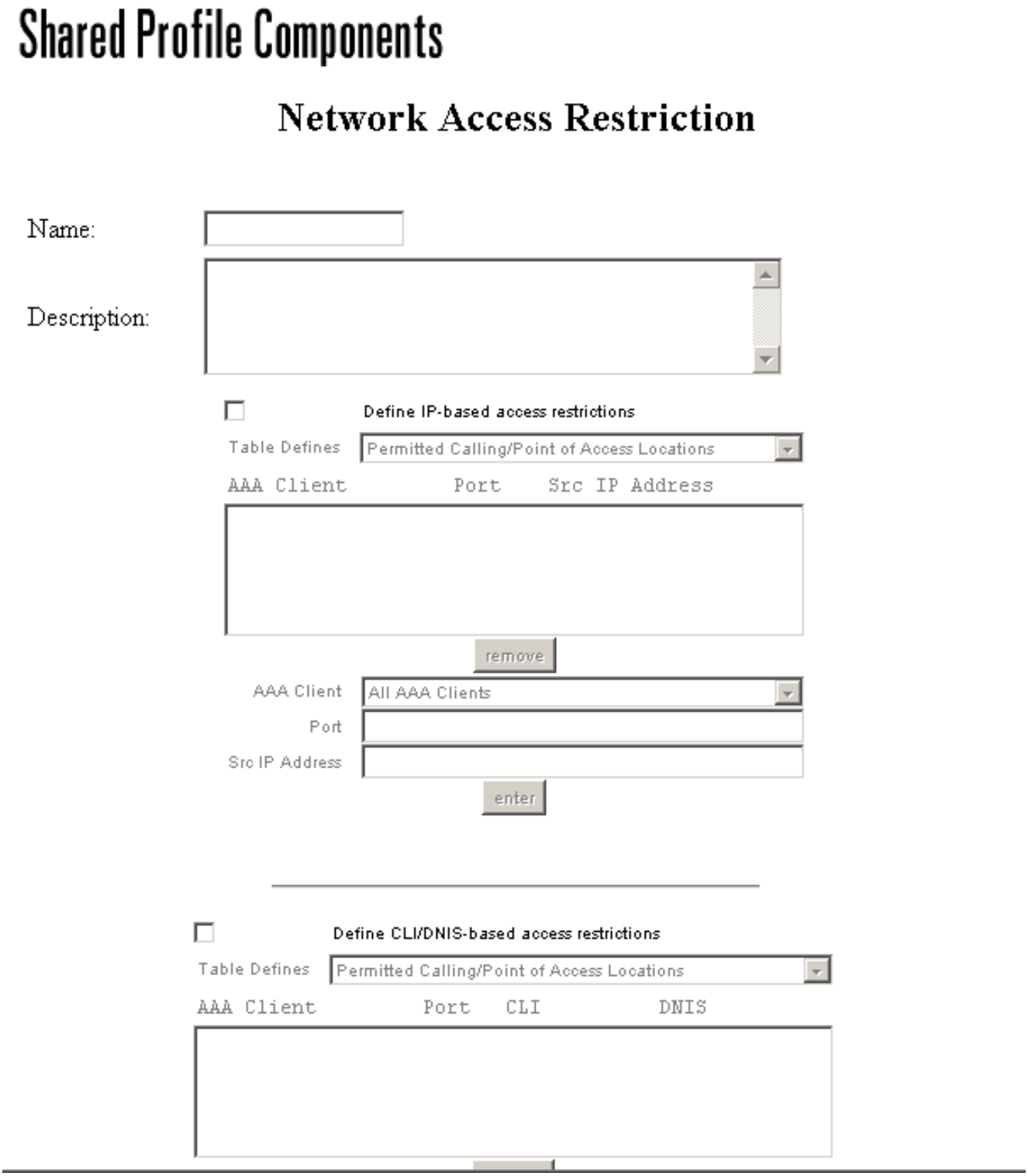
1. 在导航条，请点击**共享配置文件组件**。共享配置文件组件窗口出现。



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，请输入一个名字对于新的共有的NAR。**Note:** 名字能包含31个字符。导致和句尾空格不允许。名字不能包含这些字符：左托架([)， right bracket (])，逗号()，或者斜线(/)。
5. 在说明机箱中，请输入新的共有的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编址的访问：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被拒绝的地址，定义了列表，选择可适用的值。选择或输入可适用的信息在这些机箱中的每一个：**AAA客户端**—选择**所有AAA客户端**或者NDG或者氟化钠或者单个AAA客户端的名字，访问允许或被拒绝。**端口**—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在所选的AAA客户端。**Src IP地址**—输入IP地址过滤在，当执行访问限制时。您能使用星号(*)作为通配符指定所有IP地址。**Note:** 字符总数在AAA客户端列表的和端口和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不能准确地适用它于用户。单击 Enter。AAA客户端、端口和地址信息在表里出现作为行内容。重复步骤c和d为了输入另外的基于IP的行内容。

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，请选择这些值之一从AAA客户端列表：NDG的名字特定AAA客户端的名字所有AAA客户端**提示**： 您已经配置了仅的NDGs是列出的。为了指定此NAR应该过滤的信息，请输入值在这些机箱，如可适用：**提示**： 您能输入星号(*)作为通配符指定**所有**作为值。**端口**—输入过滤端口的编号。**CLI** —输入过滤的CLI编号。您能也使用此机箱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，请参阅网络访问限制部分。**DNIS** —输入拨号对在哪些的编号过滤。**Note:** 字符总数在AAA客户端列表和端口、CLI和DNIS机箱的不能超过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不能准确地适用它于用户。单击 Enter。指定NAR行内容的信息在表里出现。重复步骤c至e为了输入另外的基于非IP的NAR行内容。点击**提交**为了保存共有的NAR定义。ACS在**网络访问限制**表里保存共有的NAR并且列出它。

编辑共有的NAR

完成这些步骤为了编辑共有的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有的NAR。网络访问限制窗口出现并且显示所选的NAR信息。
4. 编辑NAR的名字或说明，如可适用。说明可以是30,000个字符。
5. 为了编辑行内容在基于IP的限制表里：双击您要编辑的行内容。行内容信息从表被取消并且被写到在表下的机箱。编辑信息，如所需要。**Note:** 字符和Src IP地址框总数在AAA客户端列表和端口的不能超过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不能准确地适用它于用户。单击 Enter。此行内容编辑的信息给基于IP的限制表被写。
6. 为了从基于IP的限制表删除行内容：选择行内容。在表下，请点击**去除**。行内容从基于IP的限制表被删除。
7. 为了编辑行内容在CLI/DNIS访问限制表里：双击您要编辑的行内容。行内容信息从表被取消并且被写到在表下的机箱。编辑信息，如所需要。**Note:** 字符总数在AAA客户端列表和端口、CLI和DNIS机箱的不能超过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不能准确地适用它于用户。点击**进入**此行内容编辑的信息给CLI/DNIS访问限制表被写。
8. 为了从CLI/DNIS访问限制表删除行内容：选择行内容。在表下，请点击**去除**。行内容从CLI/DNIS访问限制表被删除。
9. 点击**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。

删除共有的NAR

Note: 保证您去除共有的NAR的关联给所有用户或组队，在您删除该NAR前。

完成这些步骤为了删除共有的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. 点击您要删除共有的NAR的名字。网络访问限制窗口出现并且显示所选的NAR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有的NAR。
5. 点击OK键为了确认您要删除共有的NAR。所选的共有的NAR被删除。

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：

- 名义上适用现有的共有的NARs。
- 当IP连接建立时，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。**Note:** 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，请参阅网络访问限制部分。

一般，您定义了(共有的) NARs从共有的组件部分的内部，以便您能运用这些限制于超过一个组或用户。欲知更多信息，请参阅添加一个共有的NAR部分。您一定为此一套选项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**复选框出现于Web接口。

然而，您能也使用ACS定义和适用单个用户的NAR从User Setup部分的内部。您一定启用了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于Web接口。

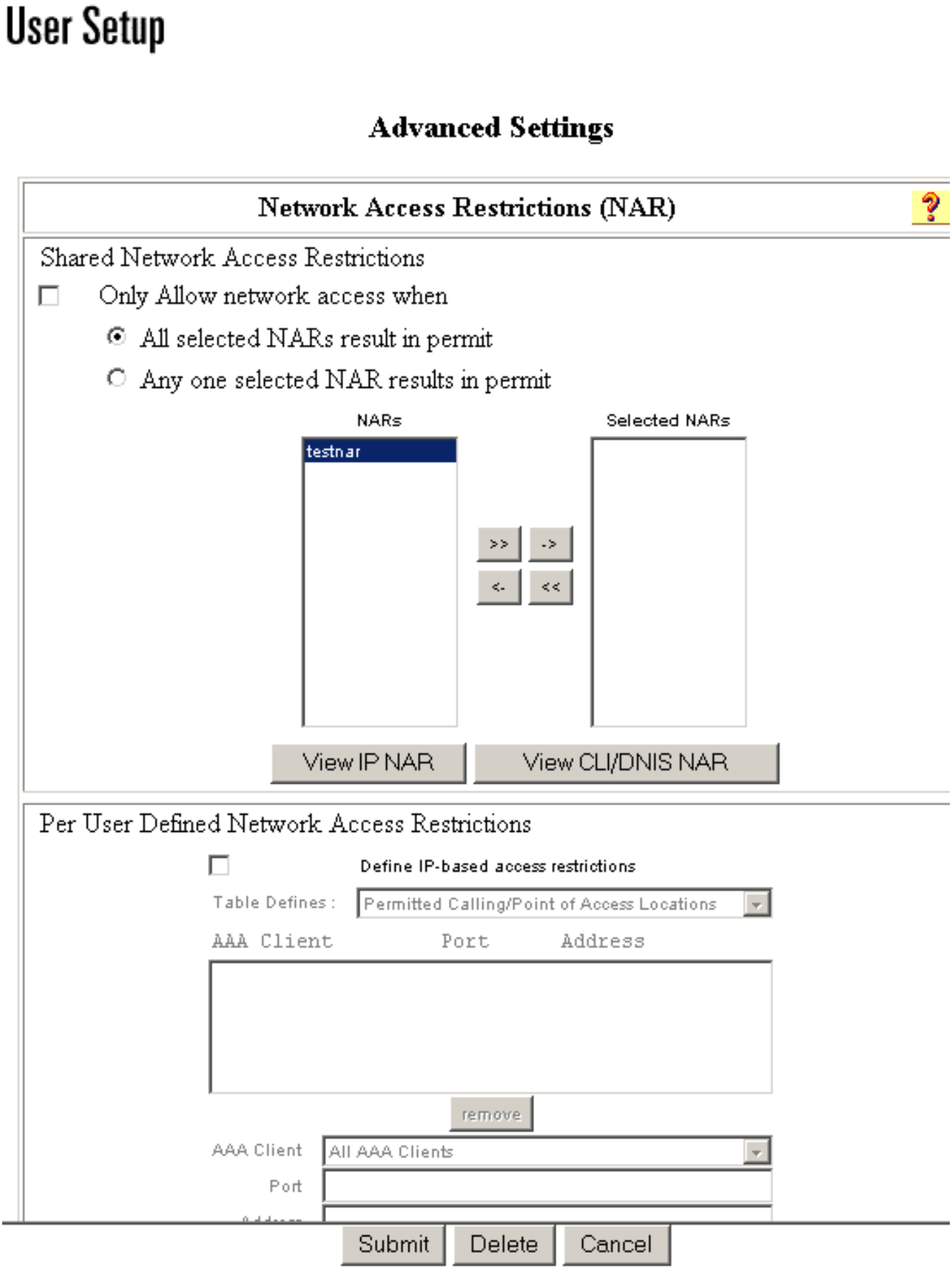
Note: 当认证请求被对ACS时的代理转发，终端访问控制器访问控制系统(TACACS+)请求的所有NARs适用于转发AAA服务器的IP地址，不于产生AAA客户端的IP地址。

当您逐个用户时创建访问限制， ACS不强制执行限额对访问限制的数量，并且不强制执行限制对每个访问限制的长度。然而，有严格的限额：

- 字段的组合每行内容不可以超出长度1024个字符。
- 共有的NAR不能有超过字符16 KB。线路数支持的项目取决于每行内容的长度。例如，如果创建AAA客户端名是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行内容，在您达到16 KB限制前。

完成这些步骤为了设置用户的NARs ：

1. 执行第1步至第3步添加一个基本的用户帐户。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. 为了适用早先配置的共有的NAR于此用户：**Note:** 为了适用共有的NAR，您一定配置了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，请参阅添加一个共有的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有的NARs是否必须申请用户是允许的访问，请选择一，如可适用：所有所选的NARS导致许可证。所有一个所选的NAR导致许可证。选择在NARs列表的一个共有的NAR名字，然后点击--> (右箭头按钮)搬入名字所选的NARs列表。**提示**： 为了查看您选择适用共有的NARs的服务器详细资料，您能点击**视图IP**

NAR或**视图CLID/DNIS NAR**，如可适用。

3. 为了定义和适用NAR，此特定用户的，允许或拒绝根据IP地址的此用户访问，或者IP地址和端口：**Note:** 您应该定义多数NARs从共有的组件部分的内部，以便您能应用他们于超过一个组或用户。欲知更多信息，请参阅添加一个共有的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被拒绝的IP地址，定义了列表，选择一：**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**选择或输入信息在这些机箱：**AAA客户端**—选择**所有AAA客户端**或者网络设备组(NDG)的名字，或者单个AAA客户端的名字，允许或拒绝访问。**端口**—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在所选的AAA客户端。**地址**—，当执行访问限制时，请输入IP地址或地址使用。您能使用星号(*)作为通配符。**Note:** 字符总数在AAA客户端列表的和端口和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不能准确地适用它于用户。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设立的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被拒绝的值，定义了列表，选择一：**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**完成机箱如显示：**Note:** 您必须做在每个机箱的一个条目。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客户端接受字符串的格式。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的名字或者单个AAA客户端的名字，允许或拒绝访问。**端口**—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，请参阅网络访问限制部分。**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，请参阅网络访问限制部分。**Note:** 字符总数在AAA客户端列表和**端口**、**CLI**和**DNIS**机箱的不能超过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不能准确地适用它于用户。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，请点击**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适用NARs用三种明显的方式：

- 名义上适用现有的共有的NARs。
- 当IP连接建立时，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， CLI编号或者使用的DNIS编号。**Note:** 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，请参阅网络访问限制部分。

一般，您定义了(共有的) NARs从共有的组件部分的内部，以便这些限制能适用于超过一个组或用户。欲知更多信息，请参阅添加一个共有的NAR部分。您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于ACS Web接口。

然而，您能也使用ACS定义和适用一个组的NAR从**Group Setup部分的内部**。您必须检查**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

项出现于ACS Web接口。

Note: 当认证请求被对ACS服务器时的代理转发， RADIUS请求的所有NARs适用于转发AAA服务器的IP地址，不于产生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，请选择一个组，然后点击**编辑设置**。组的名字出现在Settings窗口的组顶部。