Cisco Secure ACS: Ограничения доступа к сети с клиентами AAA для пользователей и групп пользователей

Содержание

Введение

В этом документе описывается способ настройки ограничений доступа к сети (NAR) на защищенном сервере управления доступом Cisco ACS версии 4.x с клиентами AAA (включая маршрутизаторы, PIX, ASA, беспроводные контроллеры) для пользователей и групп пользователей.

Предварительные условия

Требования

Этот документ создан учитывая, что Cisco Secure ACS и клиенты AAA настроены и работают должным образом.

Используемые компоненты

Сведения в этом документе основываются на Cisco Secure ACS 3.0 и позже.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить

потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Ограничения доступа к сети

В этом разделе описываются NAR и предоставляет подробные инструкции, чтобы настроить и управлять разделенными NAR.

В этом разделе содержатся следующие темы:

- Об ограничениях доступа к сети
- Добавьте совместно используемый NAR
- Отредактируйте совместно используемый NAR
- Удалите совместно используемый NAR

Об ограничениях доступа к сети

NAR является определением, которое вы делаете в ACS дополнительных условий, которым необходимо удовлетворить, прежде чем пользователь может обратиться к сети. ACS применяет эти условия при помощи информации от атрибутов, которые передают ваши клиенты AAA. Несмотря на то, что можно установить NAR несколькими способами, все основываются на соответствующей информации об атрибутах, которую передает клиент AAA. Поэтому необходимо понять формат и содержание атрибутов, которые передают клиенты AAA, если вы хотите использовать эффективные NAR.

Когда вы устанавливаете NAR, можно выбрать, работает ли фильтр положительно или негативно. Т.е. в NAR вы задаете, permit ли or deny доступ к сети, на основе информации, передаваемой от клиентов AAA когда по сравнению с информацией, хранившей в NAR. Однако, если NAR не встречается с достаточными сведениями для работы, это принимает значение по умолчанию к запрещенному доступу. Эта таблица показывает эти условия:

	На основе IP	**Базирующийся не-IP**	**Недостаточная информация**
Разрешение	Доступ предоставлен	Access Denied	Access Denied
Deny	Access Denied	Доступ предоставлен	Access Denied

ACS поддерживает два типа фильтров NAR:

- **На основе IP фильтры** — на основе IP NAR фильтруют предельный доступ на основе IP-адресов клиента конечного пользователя и клиента AAA. Посмотрите О на основе IP

разделе Фильтров NAR для получения дополнительной информации.

- **Нена основе IP фильтры** — нена основе IP NAR фильтруют предельный доступ на основе сравнения простой строки значения, передаваемого от клиента AAA. Значение может быть номером Calling Line Identification (CLI), номером Сервиса идентификации набранного номера (DNIS), MAC-адресом или другим значением, которое происходит от клиента. Для этого типа NAR для работы значение в описании NAR должно точно совпасть с тем, что передается от клиента, который включает любой формат, используется. Например, номер телефона (217) 555-4534 не совпадает 217-555-4534. Посмотрите О нена основе IP разделе Фильтров NAR для получения дополнительной информации.

Можно определить NAR для и применить его к, определенный пользователь или группа пользователей. Посмотрите, что Ограничения доступа к сети Набора для Ограничений доступа к сети Пользователя или Набора для Группы пользователей разделяют для получения дополнительной информации. Однако в разделе Общих компонентов профиля ACS можно создать и назвать совместно используемый NAR, непосредственно не цитируя пользователя или группы пользователей. Вы даете совместно используемому NAR название, на которое можно сослаться в других частях веб-интерфейса ACS. Затем когда вы устанавливаете пользователей или группы пользователей, вы не можете выбрать ни один, один, или множественные совместно используемые ограничения, которые будут применены. При определении приложения множественных совместно используемых NAR пользователю или группе пользователей вы выбираете один из двух критериев доступа:

- Все выбранные фильтры должны разрешить.
- Любой выбранный фильтр должен разрешить.

Необходимо понять порядок очередности, который отнесен к различным типам NAR. Это - заказ фильтрации NAR:

1. Совместно используемый NAR в пользовательском уровне
2. Совместно используемый NAR на уровне группы
3. Несовместно используемый NAR в пользовательском уровне
4. Несовместно используемый NAR на уровне группы

Необходимо также понять, что **отказ доступа на любом уровне имеет приоритет по параметрам настройки на другом уровне, которые не запрещают доступ**. Это - одно исключение в ACS к правилу, что параметры настройки пользовательского уровня отвергают параметры настройки уровня группы. Например, у индивидуального пользователя не могло бы быть ограничений NAR в пользовательском уровне, которые применяются. Однако, если тот пользователь принадлежит группе, которая ограничена совместно используемым или несовместно используемым NAR, пользователю запрещают доступ.

Совместно используемые NAR сохранены во Внутренней базе данных ACS. Для их резервного копирования и восстановления можно использовать функции резервного копирования и восстановления сервера ACS. Можно также реплицировать совместно используемые NAR, наряду с другими конфигурациями, к вторичным ACS.

О на основе IP фильтрах NAR

Для на основе IP фильтров NAR ACS использует атрибуты как показано, который зависит от протокола AAA (проверка подлинности, авторизация и учет) запроса аутентификации:

- **При использовании** поле **TACACS + — The** `rem_addr` от TACACS +, запускаются, тело пакета используется.**Примечание:** Когда запрос аутентификации передан по доверенности ACS, любым NAR для TACACS +, запросы применены к IP-адресу передающего AAA-сервера, не к IP-адресу инициирующего клиента AAA.
- **При использовании IETF RADIUS** — `calling-station-id` (припишите 31), должен использоваться.**Примечание:** На основе IP фильтры NAR работают, только если ACS получает Calling-Station-Id Радиуса (31) атрибут. Calling-Station-Id (31) должен содержать действительный IP - адрес. Если это не сделает, то это упадет к правилам DNIS.

Клиенты AAA, которые не предоставляют достаточную информацию о IP-адресе (например, некоторые типы межсетевого экрана) не поддерживают полную функциональность NAR.

Другие атрибуты для **на основе IP** ограничений, на протокол, включают поля NAR как показано:

- **При использовании** поля **TACACS + — The NAR** в использовании ACS эти значения:**Клиент AAA** — Nas-ip-address взят от адреса источника в сокете между ACS и TACACS + клиент.**Порт** — Поле порта взято от TACACS +, запускают тело пакета.

О нена основе IP фильтрах NAR

Нена основе IP фильтр NAR (т.е. фильтр NAR DNIS/CLI-based) являются списком разрешенного или запрещенного вызова или точкой местоположений доступа, которые можно использовать для ограничения клиента AAA, когда у вас нет установленного на основе IP соединением. Нена основе IP функция NAR обычно использует номер CLI и Набранный номер.

Однако при вводе IP-адреса вместо CLI можно использовать нена основе IP фильтр; даже когда клиент AAA не использует выпуск программного обеспечения Cisco IOS, который поддерживает CLI или DNIS. В другом исключении из ввода CLI можно ввести MAC-адрес для permit or deny доступа. Например, когда вы используете клиента AAA Cisco Aironet. Аналогично, вы могли ввести MAC-адрес точки доступа Cisco Aironet вместо DNIS. Формат того, что вы задаете в коробке CLI — CLI, IP-адресе, или MAC-адресе — должен совпасть с форматом того, что вы получаете от своего клиента AAA. Можно определить этот формат от Журнала RADIUS Accounting.

Атрибуты для ограничений DNIS/CLI-based, на протокол, включают поля NAR как показано:

- **При использовании** перечисленные поля **TACACS + — The NAR**, используют эти значения:**Клиент AAA** — `NAS-IP-address` взят от адреса источника в сокете между ACS и TACACS + клиент.Поле **Port — The** `port` в TACACS + запускается, тело пакета используется.Поле **CLI — The** `rem-addr` в TACACS + запускается, тело пакета используется.Поле **DNIS — The** `rem-addr`, взятое от TACACS +, запускается, тело пакета используется. В случаях, в которых данные адреса rem начинаются с наклонной черты (/), поле DNIS содержит данные адреса rem без наклонной черты (/).**Примечание:** Когда запрос аутентификации передан по доверенности ACS, любым NAR для TACACS +, запросы применены к IP-адресу передающего AAA-сервера, не к IP-адресу инициирующего клиента AAA.
- **При использовании** перечисленное использование полей **RADIUS — The NAR** эти значения:**Клиент AAA** — `NAS-IP-address` (приписывают 4) или, если Nas-ip-address не существует, `NAS-identifier` (атрибут RADIUS 32), используется.**Порт** — `NAS-port`

(приписывают 5) или, если порт NAS не существует, `NAS-port-ID` (приписывают 87) используется.**CLI** — `calling-station-ID` (приписывают 31) используется.**DNIS** — `called-station-ID` (приписывают 30) используется.

При определении NAR можно использовать звездочку (*) в качестве подстановочного знака для любого значения, или как часть любого значения для установления диапазона. Все значения или условия в описании NAR должны быть встречены для NAR для ограничения доступа. Это означает, что значения содержат булев AND.

Добавьте совместно используемый NAR

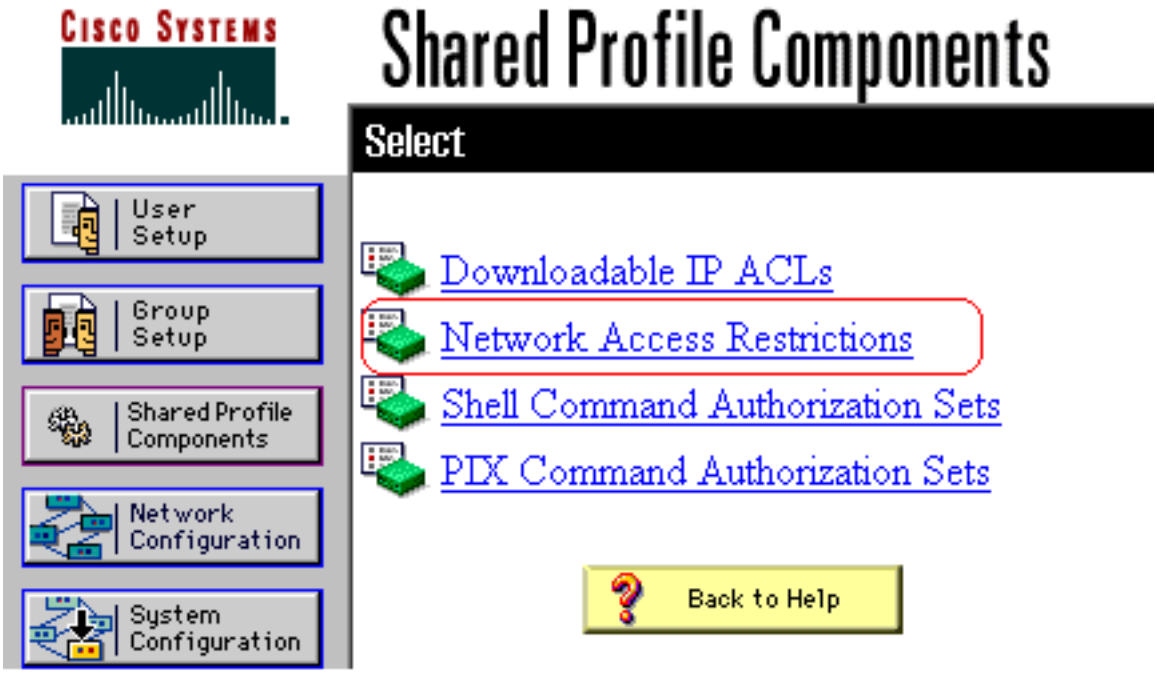
Можно создать совместно используемый NAR, который содержит много ограничений доступа. Несмотря на то, что веб-интерфейс ACS не принуждает пределы количеству ограничений доступа в совместно используемом NAR или к длине каждого ограничения доступа, необходимо придерживаться этих пределов:

- Комбинация полей для каждого элемента строки не может превысить 1024 символа.
- Совместно используемый NAR не может иметь больше чем 16 КБ символов. Поддерживаемые элементы числа линий зависят от длины каждого элемента строки. Например, при создании NAR CLI/на основе DNIS, где названия клиента AAA составляют 10 символов, номера портов составляют 5 символов, записи CLI составляют 15 символов, и записи DNIS составляют 20 символов, можно добавить 450 элементов строки перед достижением предела на 16 КБ.

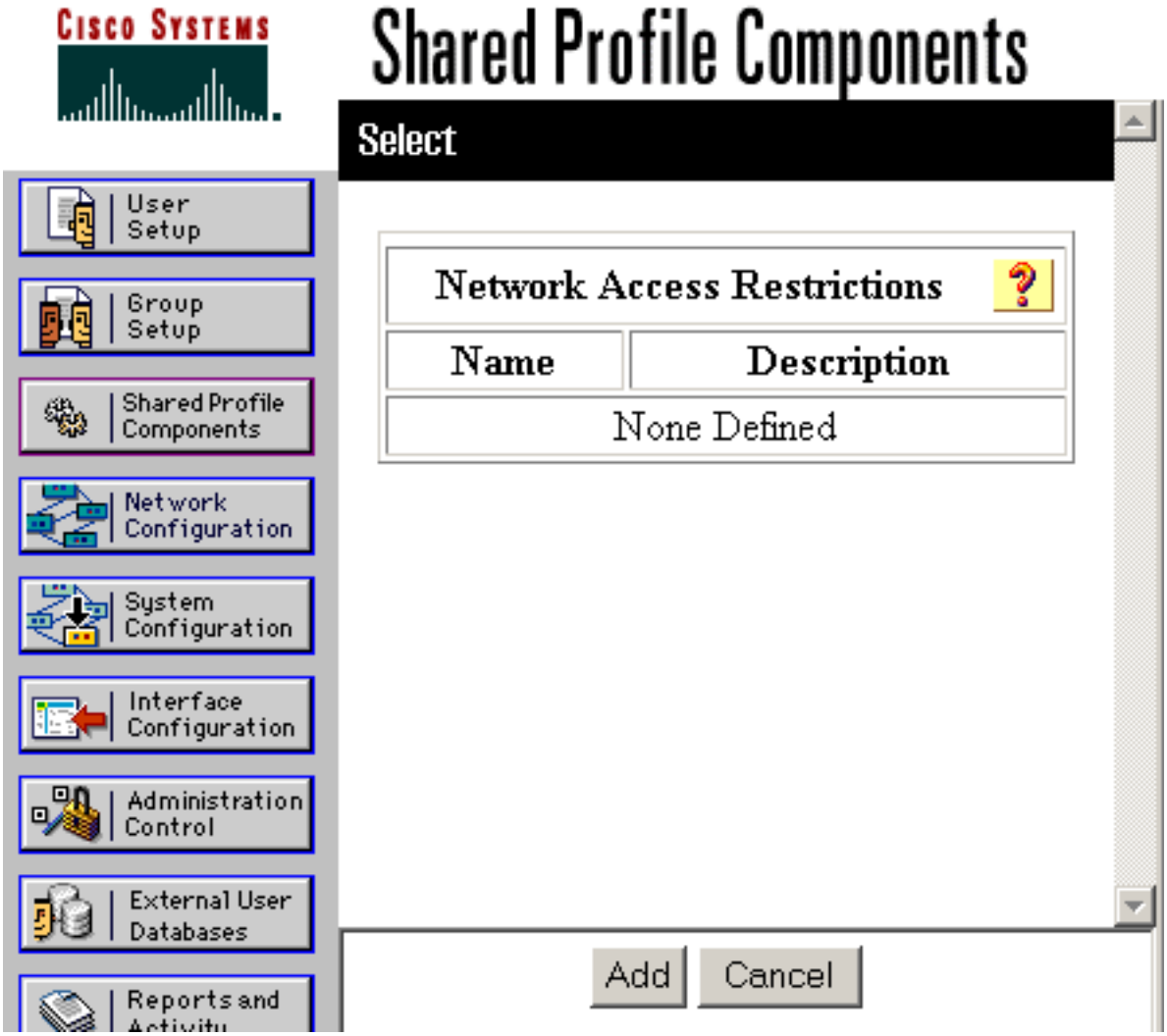
Примечание: Прежде чем вы определите NAR, удостоверитесь, что установили элементы, вы намереваетесь использовать в том NAR. Поэтому вы, должно быть, задали весь NAFs и NDGs, и определили всех соответствующих клиентов AAA перед созданием их частью определения NAR. Посмотрите О разделе Ограничений доступа к сети для получения дополнительной информации.

Выполните эти шаги для добавления совместно используемого NAR:

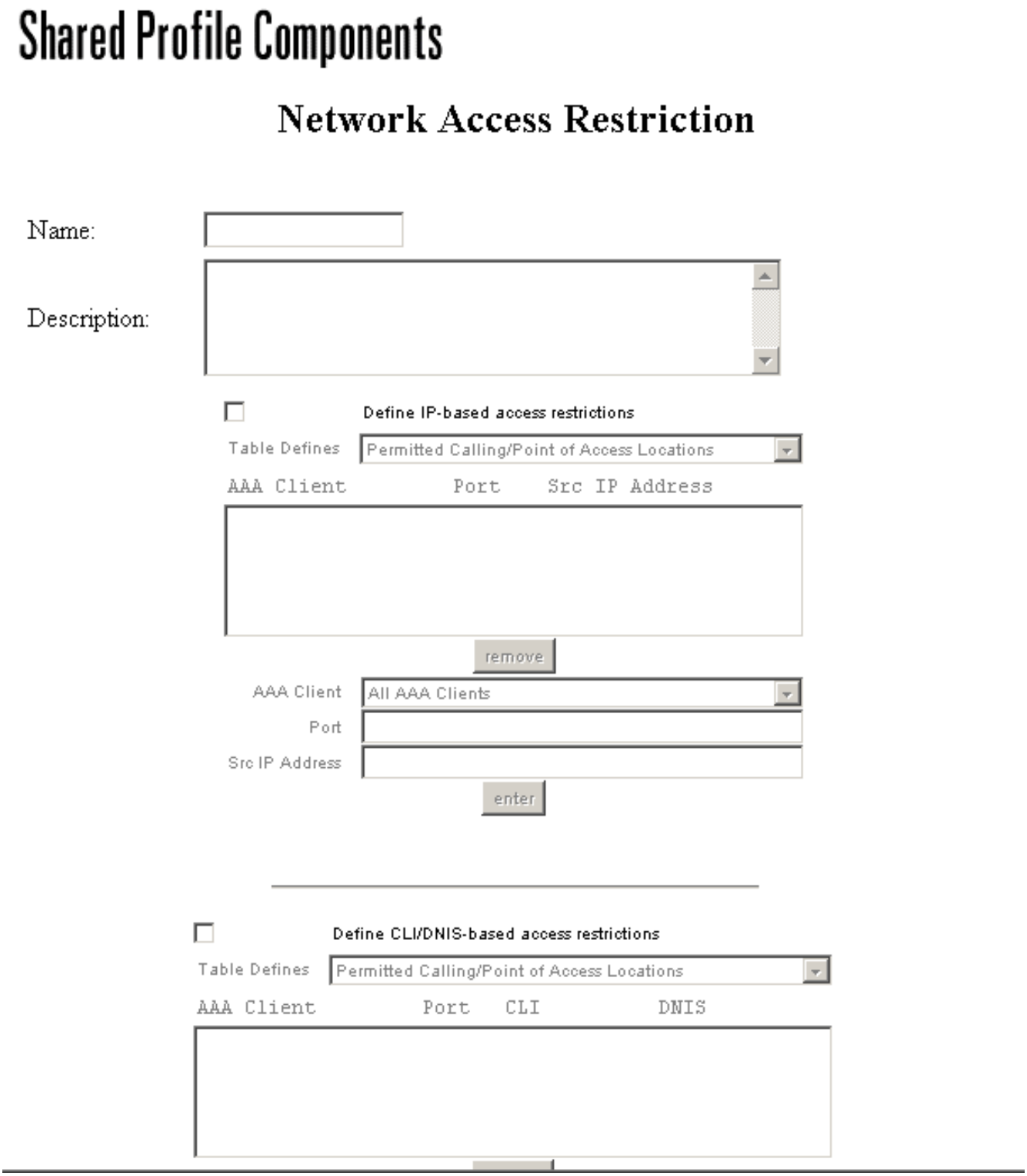
1. В Панели навигации нажмите **Shared Profile Components**.Окно Shared Profile Components появляется.



2. Нажмите **Network Access Restrictions**.



3. **Нажмите Add.**Окно Network Access Restriction появляется.



4. В Поле имени введите имя для нового совместно используемого NAR.**Примечание:** Название может содержать до 31 символа. Продвижение и замыкающие пробел не позволено. Названия не могут содержать эти символы: левая скобка ([), правая скобка (]), запятая (), или наклонная черта (/).
5. В коробке Описания введите описание нового совместно используемого NAR. Описание может составить до 30,000 символов.
6. Если вы хотите permit or deny доступ на основе IP-адресации:Проверьте**, что Определение на основе IP обращается** к флажку **описаний**.Чтобы задать, перечисляете ли вы адреса, которые разрешены или запрещены, от Таблицы Определяет список, выберите применимое значение.Выберите или введите применимые данные в каждую из этих коробок:**Клиент AAA** — Выбирает **All AAA clients**, или название NDG, или NAF или отдельного клиента AAA, к которому доступ разрешен

или запрещен.**Порт** — Введите номер порта, к которому вы хотите permit or deny доступ. Можно использовать звездочку (*) в качестве подстановочного знака для permit or deny доступа ко всем портам на выбранном клиенте AAA.**IP-адрес src** — Вводит IP-адрес для фильтрации на при выполнении ограничений доступа. Можно использовать звездочку (*) в качестве подстановочного знака для определения всех IP-адресов.**Примечание:** Общее число символов в списке Клиента AAA, и порт и Блоки IP-адресов Src, не должно превышать 1024. Несмотря на то, что ACS принимает больше чем 1024 символа, когда вы добавляете NAR, вы не можете отредактировать NAR, и ACS не может точно применить его к пользователям.Нажмите **Enter**.Клиент AAA, порт и адресная информация появляются как элемент строки в таблице.Повторите шаги c и d для ввода дополнительный на основе IP элементы строки.

7. Если вы хотите permit or deny доступ на основе вызова местоположения или значений кроме IP-адресов:Проверьте**, что Определить CLI/DNIS базировал** флажок **ограничений доступа**.Чтобы задать, перечисляете ли вы местоположения, которые разрешены или запрещены от Таблицы, Определяет список, выберите применимое значение.Для определения клиентов, к которым этот NAR применяется, выберите одно из этих значений из списка Клиента AAA:Название NDGИмя определенного клиента AAAВсе клиенты AAA**Совет:** Только NDGs, которые вы уже настроили, перечислены.Для определения информации, на которой этот NAR должен фильтровать, ввести значения в эти коробки, как применимые:**Совет:** Можно ввести звездочку (*) как подстановочный знак для определения **всех** как значения.**Порт** — Введите номер порта, на котором можно фильтровать.**CLI** — Вводит номер CLI, на котором можно фильтровать. Можно также использовать эту коробку для ограничения доступа на основе значений кроме CLI, таких как IP-адрес или MAC-адрес. Посмотрите О разделе Ограничений доступа к сети для получения дополнительной информации.**DNIS** — Вводит номер, набираемый в к, на котором можно фильтровать.**Примечание:** Общее число символов в списке Клиента AAA и порту, CLI и коробках DNIS не должно превышать 1024. Несмотря на то, что ACS принимает больше чем 1024 символа, когда вы добавляете NAR, вы не можете отредактировать NAR, и ACS не может точно применить его к пользователям.Нажмите **Enter**.Информация, которая задает элемент строки NAR, появляется в таблице.Повторите шаги c через e для ввода дополнительный нена основе IP элементы строки NAR.Нажмите **Submit** для сохранения совместно используемого определения NAR.ACS сохраняет совместно используемый NAR и перечисляет его в таблице **Ограничений доступа к сети**.

Отредактируйте совместно используемый NAR

Выполните эти шаги для редактирования совместно используемого NAR:

1. В Панели навигации нажмите **Shared Profile Components**.Окно Shared Profile Components появляется.
2. Нажмите **Network Access Restrictions**.Таблица Ограничений доступа к сети появляется.
3. В столбце Name нажмите совместно используемый NAR, который вы хотите отредактировать.Окно Network Access Restriction появляется и отображает информацию для выбранного NAR.
4. Отредактируйте Название или Описание NAR, как применимые. Описание может составить до 30,000 символов.

5. Для редактирования элемента строки в на основе IP таблица ограничений доступа:Дважды нажмите элемент строки, который вы хотите отредактировать.Информация для элемента строки удалена из таблицы и записана в коробки под таблицей.Отредактируйте информацию по мере необходимости.**Примечание:** Общее число символов в списке Клиента AAA и порту и Блоках IP-адресов Src не должно превышать 1024. Несмотря на то, что ACS может принять больше чем 1024 символа, когда вы добавляете NAR, вы не можете отредактировать такой NAR, и ACS не может точно применить его к пользователям.Нажмите **Enter**.Отредактированная информация для этого элемента строки записана в на основе IP таблица ограничений доступа.
6. Для удаления элемента строки из на основе IP таблица ограничений доступа:Выберите элемент строки.Под таблицей нажмите **Remove**.Элемент строки удален из на основе IP таблица ограничений доступа.
7. Для редактирования элемента строки в таблице ограничений доступа CLI/DNIS:Дважды нажмите элемент строки, который вы хотите отредактировать.Информация для элемента строки удалена из таблицы и записана в коробки под таблицей.Отредактируйте информацию по мере необходимости.**Примечание:** Общее число символов в списке Клиента AAA и порту, CLI и коробках DNIS не должно превышать 1024. Несмотря на то, что ACS может принять больше чем 1024 символа, когда вы добавляете NAR, вы не можете отредактировать такой NAR, и ACS не может точно применить его к пользователям.Нажмите **Enter**Отредактированная информация для этого элемента строки записана в таблицу ограничений доступа CLI/DNIS.
8. Для удаления элемента строки из таблицы ограничений доступа CLI/DNIS:Выберите элемент строки.Под таблицей нажмите **Remove**.Элемент строки удален из таблицы ограничений доступа CLI/DNIS.
9. Нажмите **Submit** для сохранения изменений, которые вы сделали.ACS повторно входит в фильтр с новой информацией, которая сразу вступает в силу.

Удалите совместно используемый NAR

Примечание: Гарантируйте удаление ассоциации совместно используемого NAR любому пользователю или группе перед удалением того NAR.

Выполните эти шаги для удаления совместно используемого NAR:

1. В Панели навигации нажмите **Shared Profile Components**.Окно Shared Profile Components появляется.
2. Нажмите **Network Access Restrictions**.
3. Нажмите название совместно используемого NAR, который вы хотите удалить.Окно Network Access Restriction появляется и отображает информацию для выбранного NAR.
4. У основания окна нажмите **Delete**.Диалоговое окно предупреждает вас, что вы собираетесь удалить совместно используемый NAR.
5. Нажмите **OK**, чтобы подтвердить, что вы хотите удалить совместно используемый NAR.Выбранный совместно используемый NAR удален.

Ограничения доступа к сети набора для пользователя

Вы используете таблицу Ограничений доступа к сети в области Advanced Settings Настройки пользователя для установки NAR тремя способами:

- Примените существующие совместно используемые NAR по имени.
- Определите на основе IP ограничения доступа, чтобы permit or deny пользовательский доступ указанному клиенту AAA или указанным портам на клиенте AAA, когда будет установлен IP - подключение.
- Определите ограничения доступа CLI/на основе DNIS для permit or deny пользовательского доступа на основе CLI/DNIS, который используется.**Примечание:** Можно также использовать область ограничений доступа CLI/на основе DNIS для определения других значений. Посмотрите раздел Ограничений доступа к сети для получения дополнительной информации.

Как правило, вы определяете (разделенные) NAR из раздела Совместно используемых компонентов так, чтобы можно было ввести эти ограничения на несколько групп или пользователя. Посмотрите Добавление Совместно используемого раздела NAR для получения дополнительной информации. Вы, должно быть, установили флажок **User-Level Network Access Restrictions** на странице Advanced Options раздела Конфигурации интерфейса для этого набора опций для появления в веб-интерфейсе.

Однако можно также использовать ACS, чтобы определить и применить NAR для одиночного пользователя из Раздела настройки пользователя. Вы, должно быть, позволили значению **Ограничений доступа к сети Пользовательского уровня** на странице Advanced Options раздела Конфигурации интерфейса для одиночного пользователя на основе IP параметры фильтрации и параметры фильтрации CLI/на основе DNIS одиночного пользователя появиться в веб-интерфейсе.

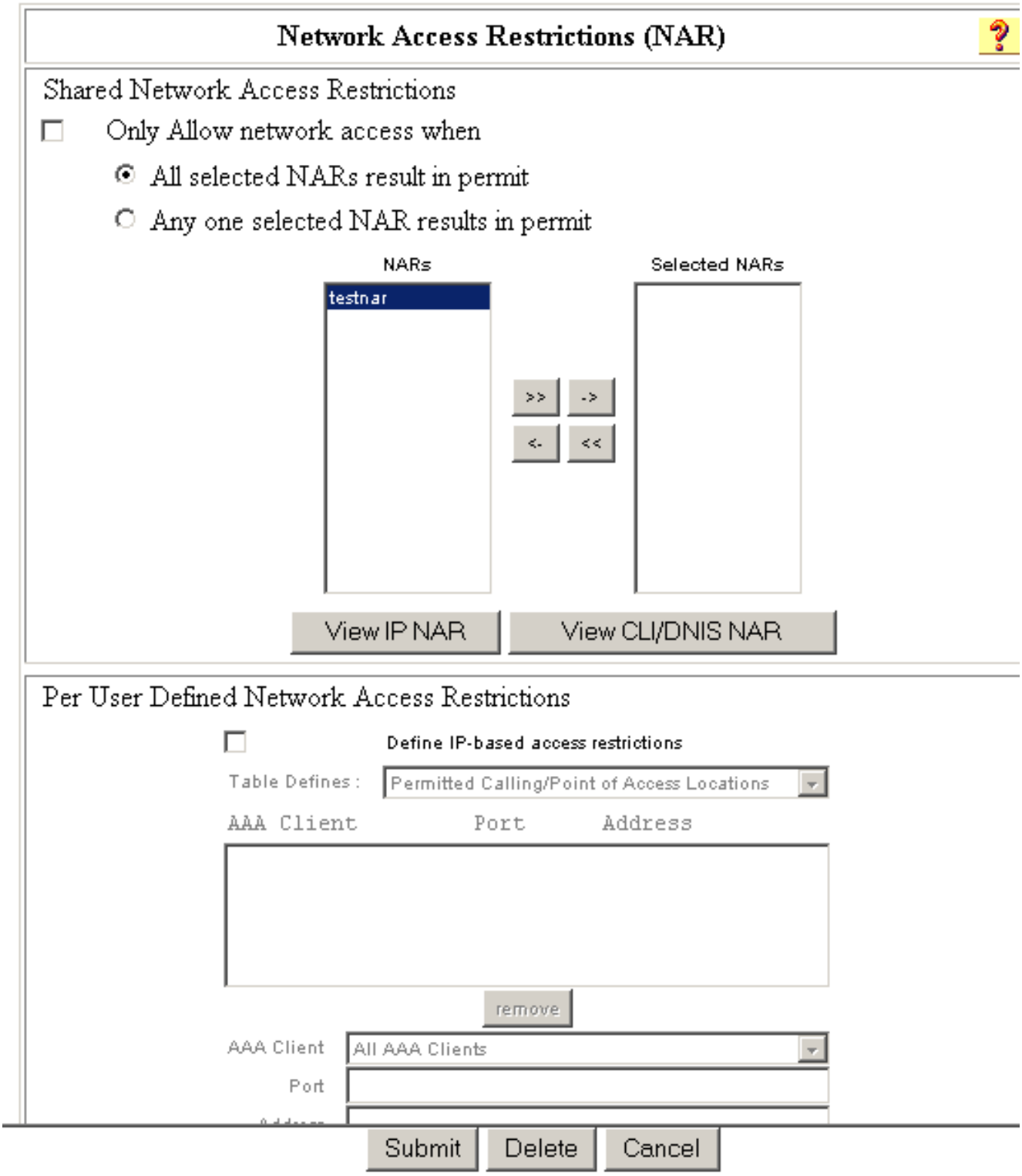
Примечание: Когда запрос аутентификации передан по доверенности ACS, любым NAR для Terminal Access Controller Access Control System (TACACS) (TACACS +), запросы применены к IP-адресу передающего AAA-сервера, не к IP-адресу инициирующего клиента AAA.

При создании ограничений доступа на основе для каждого пользователя ACS не принуждает пределы количеству ограничений доступа и не принуждает предел длине каждого ограничения доступа. Однако существуют строгие пределы:

- Комбинация полей для каждого элемента строки не может превысить 1024 символа в длине.
- Совместно используемый NAR не может иметь больше чем 16 КБ символов. Поддерживаемые элементы числа линий зависят от длины каждого элемента строки. Например, при создании NAR CLI/на основе DNIS, где названия клиента AAA составляют 10 символов, номера портов составляют 5 символов, записи CLI составляют 15 символов, и записи DNIS составляют 20 символов, можно добавить 450 элементов строки перед достижением предела на 16 КБ.

Выполните эти шаги для установки NAR для пользователя:

1. Выполните шаги 1 - 3 Добавления Учетной записи Рядового пользователя.Окно редактирования Настройки пользователя открывается. Имя пользователя, которое вы добавляете или редактируете, появляется наверху
   окна.



2. Для применения ранее настроенного совместно используемого NAR к этому пользователю:**Примечание:** Для применения совместно используемого NAR вы, должно быть, настроили его под Ограничениями доступа к сети в разделе Общих компонентов профиля. Посмотрите Добавление Совместно используемого раздела NAR для получения дополнительной информации.Проверьте**, что Единственные Позволяют доступ к сети когда** флажок.Для определения или один, или все совместно

используемые NAR должны просить пользователя, чтобы быть доступом разрешен, выбрать один, как применимые:Все выбрали результат NARS в разрешении.Любой выбрал результаты NAR в разрешении.Выберите совместно используемое название NAR в списке NAR, и затем нажмите-> (кнопка правой стрелки) для перемещения названия в Выбранный список NAR.**Совет:** Чтобы посмотреть детали сервера совместно используемых NAR, которые вы выбрали для применения, можно нажать **View IP NAR** или **View CLID/DNIS NAR**, как применимые.

3. Чтобы определить и применить NAR для этого индивидуального пользователя, который разрешает или запрещает этот пользовательский доступ на основе IP-адреса, или IP-адреса и порта:**Примечание:** Необходимо определить большинство NAR из раздела Совместно используемых компонентов так, чтобы можно было применить их к нескольким группам или пользователю. Посмотрите Добавление Совместно используемого раздела NAR для получения дополнительной информации.В таблице Ограничений доступа к сети, под На Определяемые пользователем Ограничения доступа к сети, проверяют **Определение на основе IP** флажка **ограничений доступа**.Чтобы задать, задает ли последующая распечатка разрешенный или запрещенные IP-адреса, от Таблицы Определяет список, выберите тот:**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**Выберите или введите информацию в эти коробки:**Клиент AAA** — Выбирает **All AAA Clients**, или название группы сетевых устройств (NDG) или имя отдельного клиента AAA, к которому можно permit or deny доступ.**Порт** — Введите номер порта, к которому можно permit or deny доступ. Можно использовать звездочку (*) в качестве подстановочного знака для permit or deny доступа ко всем портам на выбранном клиенте AAA.**Адрес** — Вводит IP-адрес или адреса для использования при выполнении ограничений доступа. Можно использовать звездочку (*) в качестве подстановочного знака.**Примечание:** Общее число символов в списке Клиента AAA, и порт и Блоки IP-адресов Src не должны превышать 1024. Несмотря на то, что ACS принимает больше чем 1024 символа, когда вы добавляете NAR, вы не можете отредактировать NAR, и ACS не может точно применить его к пользователям.Нажмите **Enter**.Указанный клиент AAA, порт и адресная информация появляются в таблице выше списка Клиента AAA.
4. Чтобы permit or deny, чтобы этот пользователь обратился на основе вызова местоположения или значений кроме установленного IP-адреса:Проверьте**, что Определить CLI/DNIS базировал** флажок **ограничений доступа**.Чтобы задать, задает ли последующая распечатка разрешенный или запрещенные значения, от Таблицы Определяет список, выберите тот:**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**Завершите коробки как показано:**Примечание:** Необходимо сделать запись в каждой коробке. Можно использовать звездочку (*) в качестве подстановочного знака для всех или части значения. Формат, который вы используете, должен совпасть с форматом строки, которую вы получаете от своего клиента AAA. Можно определить этот формат от Журнала RADIUS Accounting.**Клиент AAA** — Выбирает **All AAA Clients**, или название NDG или имя отдельного клиента AAA, к которому можно permit or deny доступ.**ПОРТ** — Введите номер порта, к которому можно permit or deny доступ. Можно использовать звездочку (*) в качестве подстановочного знака для permit or deny доступа ко всем портам.**CLI** — Вводит номер CLI, к которому можно permit or deny доступ. Можно использовать звездочку (*) в качестве подстановочного знака для permit or deny доступа, основанного со стороны номера.**Совет:** Используйте запись CLI, если вы хотите ограничить доступ на основе других значений, таких как MAC - адрес клиента

Cisco Aironet. Посмотрите О разделе Ограничений доступа к сети для получения дополнительной информации.**DNIS** — Вводит Набранный номер, к которому можно permit or deny доступ. Используйте эту запись для ограничения доступа на основе номера, в который пользователь наберет. Можно использовать звездочку (*) в качестве подстановочного знака для permit or deny доступа, основанного со стороны номера.**Совет:** Используйте выбор DNIS, если вы хотите ограничить доступ на основе других значений, таких как MAC-адрес точки доступа Cisco Aironet. Посмотрите О разделе Ограничений доступа к сети для получения дополнительной информации.**Примечание:** Общее число символов в списке Клиента AAA и **порту**, **CLI** и коробках **DNIS** не должно превышать 1024. Несмотря на то, что ACS принимает больше чем 1024 символа, когда вы добавляете NAR, вы не можете отредактировать NAR, и ACS не может точно применить его к пользователям.Нажмите **Enter**.Информация, которая задает клиента AAA, порт, CLI и DNIS, появляется в таблице выше списка Клиента AAA.

5. Если вы закончены, настроив опции учетной записи пользователя, нажмите **Submit** для записи опций.

Ограничения доступа к сети набора для группы пользователей

Вы используете таблицу Ограничений доступа к сети в Настройке групп для применения NAR тремя отдельными способами:

- Примените существующие совместно используемые NAR по имени.
- Определите на основе IP ограничения группового доступа, чтобы permit or deny доступ указанному клиенту AAA или указанным портам на клиенте AAA, когда будет установлен IP - подключение.
- Определите NAR группы CLI/на основе DNIS для permit or deny доступа или к, или к оба, номер CLI или используемый Набранный номер.**Примечание:** Можно также использовать область ограничений доступа CLI/на основе DNIS для определения других значений. Посмотрите О разделе Ограничений доступа к сети для получения дополнительной информации.

Как правило, вы определяете (разделенные) NAR из раздела Совместно используемых компонентов так, чтобы эти ограничения могли примениться к нескольким группам или пользователю. Посмотрите Добавление Совместно используемого раздела NAR для получения дополнительной информации. Необходимо проверить флажок **Group-Level Shared Network Access Restriction** на странице **Advanced Options** раздела Конфигурации интерфейса для этих опций для появления в веб-интерфейсе ACS.

Однако можно также использовать ACS, чтобы определить и применить NAR для одиночной группы из **Раздела Настройка группы**. Необходимо проверить значение **Ограничения доступа к сети Уровня Группы** под страницей Advanced Options раздела Конфигурации интерфейса для одиночной группы на основе IP параметры фильтрации и одиночные параметры фильтрации CLI/на основе DNIS группы для появления в веб-интерфейсе ACS.

Примечание: Когда запрос аутентификации передан по доверенности серверу ACS, любые NAR для Запросов RADIUS применены к IP-адресу передающего AAA-сервера, не к IP-адресу инициирующего клиента AAA.

Выполните эти шаги для установки NAR для группы пользователей:

1. **На панели навигации выберите Group Setup (Настройка групп).**Окно Group Setup Select открывается.
2. Из списка Группы выберите группу, и затем нажмите **Edit Settings**.Название группы появляется наверху окна Group
   Settings.