Объединение пользователей в группу концентратора VPN 3000 с помощью сервера RADIUS

Содержание

Введение

Cisco VPN 3000 Concentrator имеет способность блокировать пользователей в Группу концентраторов, которая отвергает группу, которую пользователь настроил в Cisco VPN 3000 Client. Таким образом ограничения доступа могут быть применены к различным группам, настроенным на Концентраторе VPN с обеспечением, что пользователи блокированы в ту группу с сервером RADIUS.

Этот документ детализирует, как установить эту функцию на Cisco Secure ACS для Windows и Cisco Secure для UNIX (CSUnix).

Конфигурация на Концентраторе VPN подобна стандартной конфигурации. Способность блокировать пользователей в группу, определенную на Концентраторе VPN, включена путем определения атрибута return в Профиле пользователя RADIUS. Этот атрибут содержит имя группы Концентратора VPN, в которое администратор хочет, чтобы пользователь был блокирован. Этот атрибут является Атрибутом Class (атрибут RADIUS IETF номер 25) и должен быть возвращен к Концентратору VPN в этом формате:

```
OU=groupname;
```

где *имя группы* является названием группы на Концентраторе VPN, в который блокирует пользователь. *OU* должен быть в прописных буквах, и должна быть точка с запятой в конце.

В данном примере ПО Cisco VPN Client распределен всем пользователям с профилем существующего соединения с помощью *имени группы* "Всех" и пароля "Что-либо". У каждого

пользователя есть отдельное имя пользователя / пароль (в данном примере, имя пользователя/пароль является TEST/TEST). Когда название пользователя передается серверу RADIUS, сервер RADIUS передает вниз информацию о *реальной группе*, в которой должен быть пользователь. В примере это - "группа фильтра".

Путем выполнения этого можно полностью управлять присвоением группы на сервере RADIUS, очевидном для пользователей. Если сервер RADIUS не назначает группу на пользователя, пользователь остается во "Всех" группой. Начиная со "Всех" у группы есть очень ограничительные фильтры, пользователь не может передать трафик. Если сервер RADIUS действительно назначает группу на пользователя, пользователь наследовал атрибуты, включая меньшее-количество-ограничительный-фильтр, определенное группе. В данном примере вы применяете фильтр к группе "группа фильтра" на Концентраторе VPN для разрешения всего трафика.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

Примечание: Это было также успешно протестировано с ACS 3.3, Концентратор VPN 4.1.7 и Клиент VPN 4.0.5.

- Рэл версии 4.0 (1) Концентратора серии Cisco VPN 3000
- Рэл Версии клиентской части Cisco VPN 4.0 (1)
- Cisco Secure ACS для Версий Windows 2.4 до 3.2
- Cisco Secure для Версий UNIX 2.3, 2.5, и 2.6

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 в документах см. Cisco Technical Tips Conventions.

Настройте Cisco VPN 3000 Concentrator

Примечание: Эта конфигурация предполагает, что Концентратор VPN уже установлен с IP-адресами, шлюзом по умолчанию, пулами адресов, и так далее. Пользователь должен быть в состоянии аутентифицироваться локально перед продолжением. Если это не будет работать, то эти изменения не будут работать.

1. При **Configuration> System> Servers> Authentication** добавьте IP-адрес сервера RADIUS.
2. Как только вы добавили сервер, используйте **кнопку Test**, чтобы проверить, что можно аутентифицировать пользователя успешно.Если это не работает, блокировка группы не работает.
3. Определите фильтр, который отбрасывает доступ ко всему во внутренней сети.Это применено для группировки "Всех" так, чтобы, даже если пользователи могут аутентифицироваться в эту группу и остаться в ней, они все еще не были в состоянии обратиться к чему-либо.
4. В соответствии с **Configuration> Policy Management> Traffic Management> Rules**, добавьте правило под названием **Отбрасывание Все** и оставьте все в настройках по умолчанию.
5. Под **Configuration> Policy Management> Traffic Management> Filters** создайте фильтр под названием **Отбрасывание Все**, оставьте все в настройках по умолчанию и добавьте Отбрасывание Все правило к нему.
6. Под **Configuration> User Management> Groups** добавляют группу под названием **Все**.Это - группа, которую все пользователи предварительно сконфигурировали в Клиенте VPN. Они аутентифицируются в эту группу первоначально, и затем блокированы в другую группу после проверки подлинности пользователя. Определяйте группу обычно. Удостоверьтесь, что вы добавляете Отбрасывание Весь фильтр (что вы просто создали) под Вкладкой Общие. Для использования Проверки подлинности RADIUS для пользователей в этой группе заставьте Тип группы (под вкладкой Identity) быть **Внутренним** и Опознавательным (под вкладкой IPSec) к **RADIUS**. Удостоверьтесь, что Функция Блокировка группы не проверена для этой группы.**Примечание:** Даже если вы не определяете Отбрасывание Весь фильтр, удостоверьтесь, что существует по крайней мере один фильтр, определенный здесь.
7. Определите группу конечного пункта назначения пользователя (примером является "группа фильтра"), применяя фильтр.**Примечание:** Необходимо определить фильтр здесь. Если вы не хотите блокировать какой-либо трафик для этих пользователей, создавать, "Позволяют Весь" фильтр и применяют "Любого В" и "Любого" правила к нему. Необходимо определить фильтр некоторого вида для передачи трафика. Для использования Проверки подлинности RADIUS для пользователей в этой группе заставьте Тип группы (под вкладкой Identity) быть **Внутренним** и Опознавательным (под вкладкой IPSec) к **RADIUS**. Удостоверьтесь, что Функция Блокировка группы не проверена для этой группы.

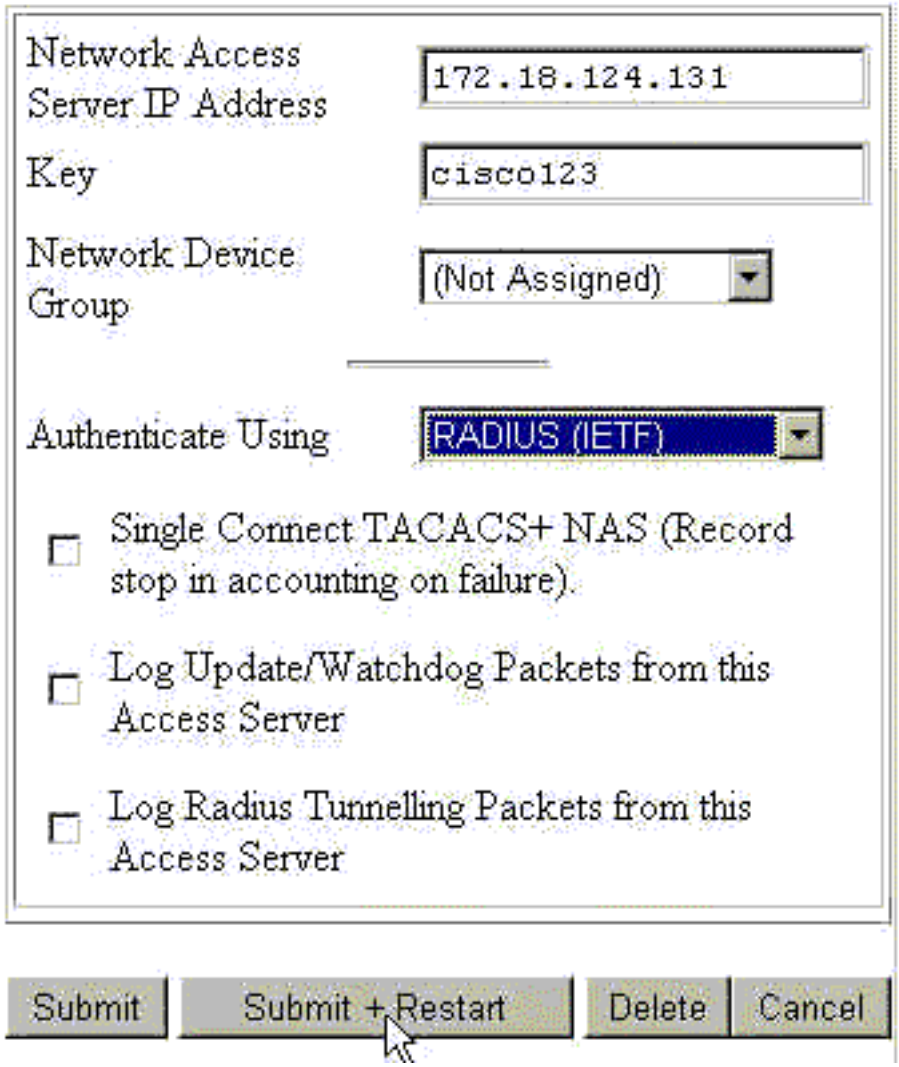
Настройка RADIUS-сервера

Cisco Secure ACS для Windows

Эти шаги устанавливают ваш Cisco Secure ACS для Сервера Windows Radius для блокировки пользователя в конкретную группу, настроенную на Концентраторе VPN. Следует иметь в виду, что группы, определенные на сервере RADIUS, не имеют никакого отношения к группам, определенным на Концентраторе VPN. Можно использовать группы на сервере RADIUS для создания администрирования пользователей легче. Названия не должны совпадать с тем, что настроено на Концентраторе VPN.

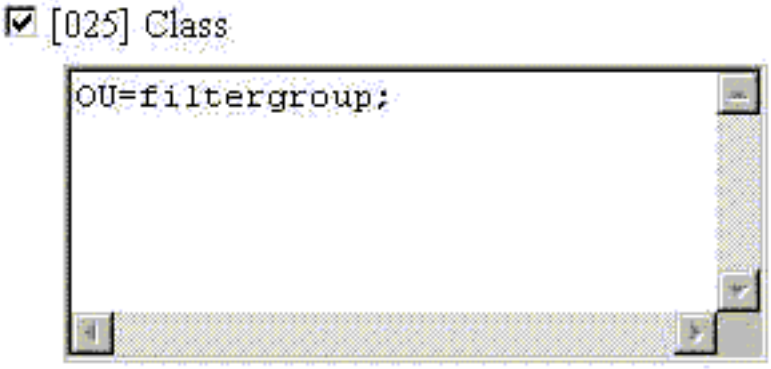
1. Добавьте Концентратор VPN как Сервер доступа к сети (NAS) на сервере RADIUS под Разделом конфигурации сети.Добавьте IP-адрес Концентратора VPN в Блоке IP-

адресов NAS.Добавьте тот же ключ, вы определили раньше Концентратор VPN в Поле Ключ.От раскрывающегося меню Используемой аутентификации выберите **RADIUS (IETF).Нажмите Submit +**



Restart.

2. Под Конфигурацией интерфейса выберите **RADIUS (IETF)** и удостоверьтесь, приписывают **25 (Класс)**, проверен.Это позволяет вам изменять его в Группе/Пользовательской конфигурации.
3. Добавьте пользователя.В данном примере пользователя называют "TECTOM". Этот пользователь может быть в любом Cisco Secure ACS для группы Windows. Кроме передачи атрибута 25 для сообщения Концентратора VPN, что группу использовать для пользователя нет никакой корреляции между Cisco Secure ACS для групп Windows и группами Концентратора VPN. Этот пользователь размещен в "Group_1".
4. При Настройке групп отредактируйте параметры настройки на группе (в нашем примере, это - "Group_1").
5. Нажмите зеленую кнопку **IETF RADIUS** для взятия вас к соответствующим атрибутам.
6. Прокрутите вниз и модифицируйте атрибут 25.
7. Добавьте атрибут как показано здесь. Замените именем группы, в которое вы хотите блокировать пользователей для группы фильтра.Удостоверьтесь, что OU находится в прописных буквах и что существует точка с запятой после имени



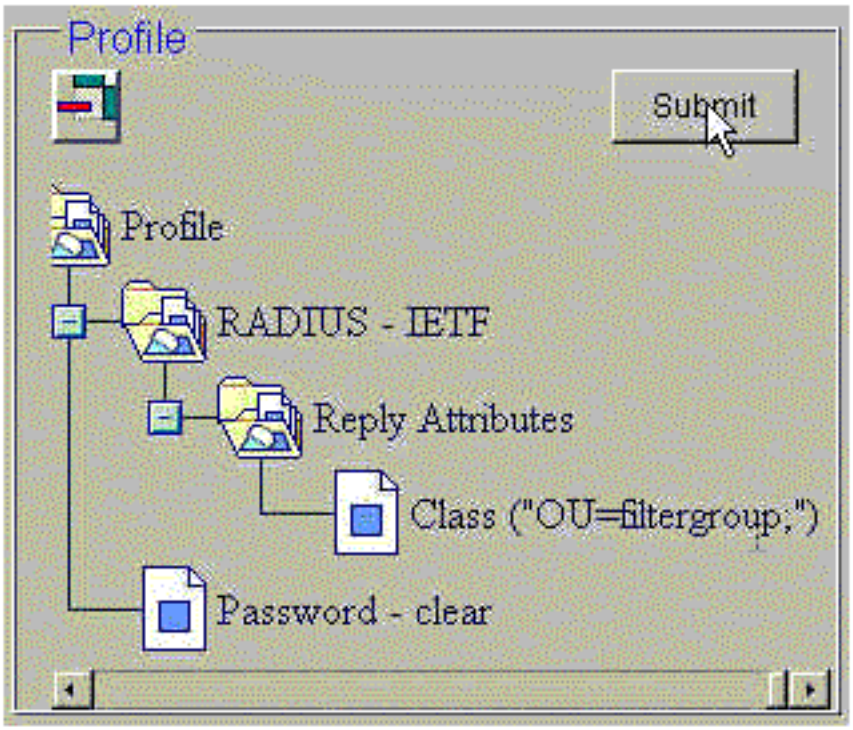
группы.

8. **Нажмите Submit + Restart.**

CiscoSecure для UNIX

Эти шаги устанавливают ваш сервер RADIUS Cisco Secure UNIX для блокировки пользователя в конкретную группу, настроенную на Концентраторе VPN. Следует иметь в виду, что группы, определенные на сервере RADIUS, не имеют никакого отношения к группам, определенным на Концентраторе VPN. Можно использовать группы на сервере RADIUS для создания администрирования пользователей легче. Названия не должны совпадать с тем, что настроено на Концентраторе VPN.

1. Включите Концентратор VPN как NAS на сервере RADIUS под Усовершенствованным разделом.Выберите словарь, который позволяет атрибуту 25 передаваться как атрибут ответа. Например, IETF или Возрастание.
2. Добавьте пользователя.В данном примере пользователь является "ТЕСТОМ". Этот пользователь может быть в любой группе Cisco Secure UNIX или никакой группе. Кроме передачи атрибута 25 для сообщения Концентратора VPN, что группу использовать для пользователя нет никакой корреляции между группами Cisco Secure UNIX и группами Концентратора VPN.
3. При пользователе/профиле группы определите RADIUS (IETF), возвращают атрибут.
4. Добавьте Атрибут Class, номер атрибута **25**, и сделайте его значение **OU=filtergroup;**. замените группой, определенной на Концентраторе VPN для группы фильтра.**Примечание:** В Cisco Secure UNIX определите атрибут, окруженный кавычками. Когда атрибут передается Концентратору VPN, они являются неизолированными. Пользователь/профиль группы должен выглядеть подобным



этому.

5. Нажмите **Submit** для сохранения каждой записи.Законченные записи Cisco Secure UNIX кажутся подобными этим выходным данным:

```
# ./ViewProfile -p 9900 -u
NAS.172.18.124.132
User Profile Information
user = NAS.172.18.124.132{
profile_id = 68
profile_cycle = 1
NASNAME="172.18.124.132"
SharedSecret="cisco"
RadiusVendor="IETF"
Dictionary="DICTIONARY.IETF"

}

# ./ViewProfile -p 9900 -u TEST
User Profile Information
user = TEST{
profile_id = 70
set server current-failed-logins = 0
profile_cycle = 3
password = clear "********"
radius=IETF {
check_items= {
2="TEST"
}
reply_attributes= {
25="OU=filtergroup"
 !--- The semi-colon does NOT appear !--- after the group name, even though it has to be
included !--- when it defines the attribute via the GUI. } } } # ./ViewProfile -p 9900 -u
filtergroup User Profile Information user = filtergroup{ profile_id = 80 profile_cycle = 1
radius=IETF { check_items= { 2="filtergroup" } } } # ./ViewProfile -p 9900 -u Everyone User
Profile Information user = Everyone{ profile_id = 67 profile_cycle = 1 radius=IETF {
check_items= { 2="Anything" } } }
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Обработка атрибута пользователя и группы Cisco VPN 3000 Client на VPN 3000 Concentrator
- Страница поддержки технологии RADIUS (Служба Проверки Подлинности Удаленного Наборного Телефонного Доступа Пользователя)
- Страницы технической поддержки концентраторов Cisco VPN серии 3000
- Страницы поддержки Cisco VPN 3000 Client
- Протокол IP-безопасности (IPSec) страницы технической поддержки продукта
- Запросы комментариев (RFC)
- Страница поддержки продукта CiscoSecure ACS для Windows
- Уведомления о дефектах продуктов безопасности
- Cisco Secure ACS для страницы поддержки продуктов UNIX
- Техническая поддержка - Cisco Systems