Использование ASA примера конфигурации карт атрибутов LDAP

Содержание

Введение

Этот документ описывает, как использовать Карты Атрибута Протокола LDAP для настройки гранулированной Динамической Политики Accesss по Устройству адаптивной защиты (ASA).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- VPN уровня защищенных сокетов (VPN SSL) на Cisco IOS®
- Проверка подлинности LDAP на Cisco IOS
- Службы каталога

Используемые компоненты

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

- CISCO881-SEC-K9
- Программное обеспечение Cisco IOS, программное обеспечение C880 (C880DATA-UNIVERSALK9-M), версия 15.1 (4) M, РЕЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (fc1)

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.

Общие сведения

LDAP является открытым, нейтральным поставщиком прикладным протоколом промышленного стандарта, чтобы обратиться и поддержать информационные сервисы распределенного справочника по IP - сети. Сервисы каталогов играют важную роль в разработке интранет и интернет-приложений, потому что они позволяют информации о пользователях, системах, сетях, сервисах и приложениях быть разделенной всюду по сети.

Часто у администраторов возникает необходимость предоставить пользователям сети VPN различные разрешения на доступ или различное содержание WebVPN. Если вы настраиваете другую политику VPN на сервере VPN и назначаете эти наборы политики на каждого пользователя на основе их учетных данных, это может быть сделано. В то время как это может быть сделано вручную, это более эффективно для автоматизации процесса с Сервисами каталогов. Для использования LDAP для присвоения групповой политики на пользователя, необходимо настроить карту, которая сопоставляет атрибут LDAP, такой как атрибут Active Directory (AD) **memberOf**, к атрибуту **Класса радиуса IETF**, который понят под головной станцией VPN.

На Cisco IOS может быть достигнута та же вещь, если вы настраиваете другие группы политик под контекстом WebVPN и используете Карты атрибутов LDAP для определения, какая группа политик пользователю назначат, как описано в документе.

Посмотрите Присвоение Группы политик для Клиентов AnyConnect Что LDAP Использования на Примере конфигурации головных станций Cisco IOS.

Устройство ASA штатным образом реализует такую возможность путем назначения различных групповых политик разным пользователям. В случае использования аутентификации посредством LDAP это может быть выполнено автоматически путем привязки атрибутов LDAP. Для использования LDAP для присвоения групповой политики на пользователя, необходимо сопоставить атрибут LDAP, такой как AD атрибут **memberOf** к атрибуту **Групповой политики**, который понят под ASA. После установления карты атрибутов необходимо привязать значение атрибута, настроенное на сервере LDAP, к имени групповой политики в устройстве ASA.

> **Примечание:** Атрибут **memberOf** соответствует группе, что пользователь является частью в Active Directory. Пользователь может быть членом сразу нескольких групп в Active Directory. **В этом случае сервер отправляет несколько атрибутов memberOf, но устройство ASA может связать с одной политикой группы только один атрибут.**

Часто задаваемые вопросы

Вопрос. . Существует ли предел конфигурации на количестве карт атрибутов LDAP для ASA?

O. Нет, нет никаких пределов. карты атрибутов LDAP динамично выделены во время сеанса удаленного доступа VPN, который использует проверку подлинности LDAP / авторизация.

Вопрос. . Существует ли предел на количестве атрибутов, которые могут быть сопоставлены на карту атрибутов LDAP?

O. Никакие пределы configuraiton.

Вопрос. . Существует ли ограничение на то, сколько серверов LDAP, к которым может быть применена определенная карта атрибутов LDAP?

O. Никакое ограничение. Код LDAP только проверяет, что название карты атрибутов LDAP допустимо.

Вопрос. . Есть ли ограничения с картами атрибутов LDAP и muti-ценными атрибутами как AD memberOf?

O. Да. Здесь, только AD объяснен, но он применяется к любому Серверу LDAP, который использует атрибуты мультизначения для решений о применении политики. Карта атрибутов LDAP имеет ограничение с многозначными атрибутами как AD memberOf. Если пользователь будет memberOf нескольких AD групп (который распространен), и карта атрибутов LDAP совпадает с несколькими из них, то сопоставленное значение будет

выбрано на основе расположения в алфавитном порядке записей, с которыми совпадают. Так как это поведение не очевидно или интуитивно, важно иметь ясное знание о том, как это работает.

Сводка: Если результаты сопоставления LDAP во множественных значениях для атрибута, заключительное значение атрибута будет выбрано следующим образом:

- Во-первых, выберите значение (значения) самым маленьким количеством символов.
- Если это приводит к нескольким значениям, выберите значение, которое является самым низким в алфавитном порядке.

Примеры варианта использования

LDAP Active Directory возвращает эти четыре memberOf экземпляра для проверки подлинности пользователя или запроса авторизации:

```
memberOf: value = CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Cisco-Eng,CN=Users,DC=stbu,OU=cisco,DC=com
memberOf: value = CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com
```

MAP LDAP #1: Предположите, что эта карта атрибутов LDAP настроена для сопоставления других групповых политик ASA на основе значения memberOf:

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup4
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

В этом случае соответствия произойдут на всех четырех значениях групповой политики (ASAGroup1 - ASAGroup4). Однако соединение будет назначено на групповую политику ASAGroup1, потому что это происходит сначала в алфавитном порядке.

MAP LDAP #2: Эта карта атрибутов LDAP является тем же, кроме первого memberOf не имеет явного значения карты назначенным (№ ASAGroup4). Обратите внимание на то, что, когда нет никакого явного определенного значения карты, текст атрибута, полученный от LDAP, используется.

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

Как в предыдущем случае, соответствия происходят на всех четырех записях. В этом случае, так как никакое сопоставленное значение не предоставлено для записи VPN SSL APP, сопоставленное значение примет значение по умолчанию CN=APP-SSL-VPN Менеджерам, Cn=Users, OU=stbu, DC=cisco, DC=com. С тех пор CN=APP-SSL-VPN кажется первым в заказе aphabetical, VPN SSL APP будет выбрана как значение политики.

См. идентификатор ошибки Cisco CSCub64284 для получения дополнительной информации. См. PIX/ASA 8.0: Используйте Проверку подлинности LDAP для Присвоения Групповой политики при Входе в систему, который показывает простой случай LDAP с memberOf, который мог бы работать в определенных развертываниях.

Опции Обходного пути/Оптимального метода

1. Используйте политику динамического доступа (DAP) - DAP не имеет этого ограничения парсинга многозначных атрибутов (как memberOf); но DAP в настоящее время не может устанавливать групповую политику из себя. Это означает, что сеанс должен был бы быть должным образом сегментирован с помощью методов ассоциации туннельной группы/групповой политики. В будущем DAP будет иметь возможность установить любой атрибут authorizaiton, включая групповую политику, (идентификатор ошибки Cisco CSCsi54718), таким образом, для этой цели не будет в конечном счете требоваться потребность в карте атрибутов LDAP.

2. Как возможная альтернатива и если сценарий развертывания позволяет его, каждый раз, когда необходимо использовать карту атрибутов LDAP для установки атрибута Class, вы могли также использовать однозначный атрибут (как Отдел), который представляет ваше дифференцирование группы на AD.

   Примечание: В memberOf DN, таком как "CN=Engineering, OU=Office1, DC=cisco, DC=com", можно только принять решение о первом DN, который является CN=Engineering, не Подразделением (OU). Существует усовершенствование, чтобы быть в состоянии способное фильтровать на любом поле DN.

Настройка- Пример использования

Примечание: Каждый пример, описанный в этом разделе, является автономной конфигурацией, но может быть смешан и совпасться друг с другом для создания желаемой Политики доступа.

Совет: Имена и значения атрибутов воспринимаются с учетом регистра. Если сопоставление не происходит должным образом, уверены, что корректное написание и капитализация использовались в Карте атрибутов LDAP и для Cisco и для названий атрибута LDAP и значений.

1. Принудительная политика атрибутов на основе пользователя

Любой стандартный атрибут LDAP может быть сопоставлен с известным Определяемым поставщиком атрибутом (VSA) устройства. Один или более атрибутов (атрибутов) LDAP могут быть сопоставлены с одним или более атрибутами LDAP Cisco. Для полного списка VSA LDAP Cisco обратитесь Поддерживаемые Атрибуты Cisco для Авторизации LDAP. Данный пример показывает, как принудить баннер для user1 LDAP. User1 может быть любым типом Удаленного доступа VPN: IPsec, SVC или Безклиентый WebVPN. Данный пример использует Свойства/Общий/Офис, attribute/field для осуществления Banner1.

Примечание: Вы могли использовать AD атрибут/поле Отдела для сопоставления с VSA Класса радиуса IETF Cisco для осуществления политики от групповой политики

ASA/PIX. Существуют примеры этого позже в документе.

LDAP (для Microsoft AD и Sun) сопоставление атрибута поддерживается с Версии 7.1 PIX/ASA. x. Любой атрибут Microsoft/AD может быть сопоставлен с атрибутом Cisco. Вот процедура для выполнения этого:

1. На AD/сервере LDAP:Выберите user1.Щелкните правой кнопкой мыши> **Свойства**.Выберите вкладку, которая будет использоваться, для установки атрибута (Пример. Вкладка Общие).Выберите поле/атрибут, например поле "Office", чтобы использоваться, чтобы принудить time-range и ввести текст заголовка (пример, Добро пожаловать в LDAP !!!!). Конфигурация "офиса" на GUI сохранена в "physicalDeliveryOfficeName" атрибута AD/LDAP.

2. На ASA, для создания таблицы соответствий атрибута LDAP, сопоставляют атрибут AD/LDAP "physicalDeliveryOfficeName" с "Banner1" атрибута ASA:
```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. Привяжите Карту атрибутов LDAP к записи aaa-server:
```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. Установите Удаленный доступ, открывают сеанс и проверяют что Баннер, "Добро пожаловать в LDAP !!!!" представлен пользователю VPN.

2. Разместите пользователей LDAP в определенную групповую политику - Общий пример

Данный пример демонстрирует аутентификацию user1 на AD Сервере LDAP и получает значение поля отдела, таким образом, это может быть сопоставлено с групповой политикой ASA/PIX, от которой будет принуждена политика.

1. На AD/сервере LDAP:Выберите user1.Щелкните правой кнопкой мыши> **Свойства**.Выберите вкладку, которая будет использоваться, для установки атрибута (Пример. Вкладка Organization).Выберите поле/атрибут, например "Отдел", чтобы использоваться, чтобы принудить групповую политику и ввести значение групповой политики (Группа-Policy1) на ASA/PIX. Конфигурация "Отдела" на GUI сохранена в "отделе" атрибута AD/LDAP.

2. Определите таблицу карты атрибутов LDAP.
```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

Примечание: В результате реализации идентификатора ошибки Cisco CSCsv43552, новый атрибут карты атрибутов LDAP, Групповая политика, был представлен для замены Класса радиуса IETF. CLI на Версии ASA 8.2 поддерживает ключевое слово Класса радиуса IETF как допустимый выбор в map-name и команды значения карты для чтения 8.0 файлов config (сценарий обновления программного обеспечения). Код Менеджера устройств адаптивной безопасности (ASDM) (ASDM) был уже обновлен, чтобы больше не отобразить Класс радиуса IETF как выбор при настройке элемента схемы атрибута. Кроме того, ASDM выпишет атрибут Класса радиуса IETF (если считано в от 8.0 config) как атрибут Групповой политики.

3. Определите групповую политику Group_policy1 на устройстве и требуемых атрибутах политики.

4. Установите удаленный доступ VPN, туннелируют и проверяют, что сеанс наследовал атрибуты от Группы-Policy1 (и любые другие применимые атрибуты от групповой политики по умолчанию).

   Примечание: Добавьте большие атрибуты к карте как требуется. Данный пример показывает только минимум для управления этой определенной функцией (разместите пользователя в определенный ASA/PIX 7.1.x групповая политика). Третий пример показывает этот тип карты.

Настройте групповую политику NOACCESS

Когда пользователь не является частью ни одной из групп LDAP, можно создать групповую политику NOACCESS для запрета VPN-подключения. Этот фрагмент конфигурации показывают для вашей ссылки:

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

Необходимо применить эту групповую политику как политику группы по умолчанию к туннельной группе. Это позволяет пользователям, которые получают сопоставление от Карты атрибутов LDAP, например те, кто принадлежит желаемой группе LDAP, для получения их желаемых групповых политик и пользователей, которые не получают сопоставления, например те, кто не принадлежит ни одной из желаемых групп LDAP, для получения групповой политики NOACCESS от туннельной группы, которая блокирует доступ для них.

Совет: Так как атрибут vpn-simultaneous-logins установлен в 0 здесь, это должно быть явно определенный во всех других групповых политиках также; иначе, это будет наследовано от групповой политики по умолчанию для той туннельной группы, которая в этом случае является политикой NOACCESS.

3. Основанная на группе принудительная политика атрибутов - пример

Примечание: Реализация/исправлять идентификатора ошибки Cisco, CSCse08736 требуется, таким образом, ASA должен выполнить, по крайней мере, Версию 7.2.2.

1. На AD Сервере LDAP, Пользователях и компьютерах Active Directory, устанавливает запись пользователя (VPNUserGroup), который представляет группу, где настроены атрибуты виртуальной частной сети VPN.

2. На AD Сервере LDAP, Пользователях и компьютерах Active Directory, определяют поле Department каждой записи пользователя для обращения к групповой записи (VPNUserGroup) в Шаге 1. Имя пользователя в данном примере является **web1**.

   Примечание: Атрибут AD Отдела использовался только потому, что логически "отдел" обращается к групповой политике. В действительности любое поле могло использоваться. Требование - то, что это поле должно сопоставить с Групповой политикой атрибута виртуальной частной сети VPN Cisco как показано в данном примере.

3. Определите таблицу карты атрибутов LDAP:

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department IETF-Radius-Class
map-name description\Banner1
map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
5520-1(config)#
```

   Два Описания атрибутов AD LDAP и офис (представленный AD описанием названий и PhysicalDeliveryOfficeName) являются атрибутами групповой записи (для VPNUSerGroup), который сопоставляет с атрибутами виртуальной частной сети VPN Cisco Banner1 и IETF-Radius-Session-Timeout.

   Атрибут отдела для записи пользователя для сопоставления с названием внешней групповой политики на ASA (VPNUSer), который тогда сопоставляет назад с записью VPNuserGroup на AD Сервере LDAP, где определены атрибуты.

   Примечание: Атрибут Cisco (Групповая политика) должен быть определен в карте атрибутов LDAP. Его сопоставленный AD атрибут может быть любым устанавливаемым AD атрибутом. Данный пример использует отдел, потому что это - наиболее логическое имя, которое обращается к групповой политике.

4. Настройте aaa-server с названием карты атрибутов LDAP, которое будет использоваться для Проверки подлинности LDAP, Авторизации, и Бухгалтерские (AAA) операции:

```
5520-1(config)# show runn aaa-server LDAP-AD11
aaa-server LDAP-AD11 protocol ldap
aaa-server LDAP-AD11 host 90.148.1.11
ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
ldap-scope onelevel
ldap-naming-attribute sAMAccountName
ldap-login-password altiga
ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
```

```
ldap-attribute-map Our-AD-Map
5520-1(config)#
```

5. Определите туннельную группу с или с Проверкой подлинности LDAP или с Авторизацией LDAP.

   Пример с Проверкой подлинности LDAP. Если атрибуты определены, выполняет аутентификацию + (авторизация) принудительная политика атрибута.

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group LDAP-AD11
accounting-server-group RadiusACS28
```

   5520-1(config)#Пример с Авторизацией LDAP. Конфигурация используется для использования Цифровых сертификатов.

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group none
authorization-server-group LDAP-AD11
accounting-server-group RadiusACS28
authorization-required
authorization-dn-attributes ea
5520-1(config)#
```

6. Определите внешнюю групповую политику. Название групповой политики является значением записи AD Пользователя LDAP, которая представляет группу (VPNUserGroup).

```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```

7. Установите туннель и проверьте, что принуждены атрибуты. В этом случае Баннер и Session-Timeout принуждены от записи VPNuserGroup на AD.

4. Реализация Active Directory "Назначает статический IP - адрес" для туннелей SVC и IPsec

AD атрибут является msRADIUSFramedIPAddress. Атрибут настроен в AD Свойствах пользователя, Вкладке наборный (телефонный) доступ, "Назначьте Статический IP - адрес".

Далее перечислены действия:

1. На AD сервере, под свойствами пользователя, Вкладкой наборный (телефонный) доступ, "Назначают Статический IP - адрес", вводят значение IP-адреса для присвоения на сеанс IPsec/SVC (10.20.30.6).

2. На ASA создают карту атрибутов LDAP с этим сопоставлением:

```
5540-1# show running-config ldap
```

```
ldap attribute-map Assign-IP
map-name msRADIUSFrameIPAdddress IETF-Radius-Framed-IP-Address
5540-1#
```

3. На ASA проверьте, что vpn-address-assigment настроен для включения "vpn-addr-assign-aaa":

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

4. Установите сеансы Удаленных полномочий (RA) IPsec/SVC и проверьте с "покажите vpn-sessiondb remote|svc", что поле "Assigned IP" корректно (10.20.30.6).

5. Реализация Active Directory "коммутации разрешений удаленного доступа, разрешите/Запретите доступ"

Поддерживает всю VPN Удаленные сеансы Acccess: IPSec, WebVPN и SVC. Предоставьте Доступ, имеет значение ИСТИННЫХ. Запретите Acccess, имеет значение ЛЖИ. AD название атрибута является msNPAllowDialin.

Данный пример демонстрирует создание карты атрибутов LDAP, которая использует Протоколы туннелирования Cisco для создания, Предоставляют (ИСТИННЫЙ) Доступ и Запрещают (ЛОЖНЫЕ) условия. Например, если вы сопоставляете tunnel-protocol=L2TPover IPsec (8), можно создать ЛОЖНОЕ условие, при попытке принудить доступ для WebVPN и IPsec. Обратная логика применяется также.

Далее перечислены действия:

1. На AD Свойствах user1 сервера, Наборном (телефонный) доступе, выбирают соответствующее, предоставляют Доступ или Запрещают доступ для каждого пользователя.

   Примечание: При выборе третьей опции "Control access through the Remote Access Policy" никакое значение не возвращено из AD сервера, таким образом, разрешения, которые принуждены, основываются на значении внутренней групповой политики ASA/PIX.

2. На ASA создайте карту атрибутов LDAP с этим сопоставлением:

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

   Примечание: Добавьте большие атрибуты к карте как требуется. Данный пример показывает только минимум для управления этой определенной функцией (Позвольте или Запретите Доступ на основе значения Наборного (телефонный) доступа).

Что карта атрибутов LDAP означает или принуждает?

значение карты msNPAllowDialin ЛОЖЬ 8

Запретите Доступ для user1. ЛОЖНОЕ условие значения сопоставляет с протоколом туннелирования L2TPoverIPsec, (оцените 8).

Предоставьте Доступ для user2. Условие Истинного значения сопоставляет с протоколом туннелирования WebVPN + IPsec, (оцените 20).

WEBVPN/ПОЛЬЗОВАТЕЛЬ IPSEC, authenticaticated как user1 на AD, отказал бы из-за несоответствия протокола туннелирования.

L2TPoverIPsec, authenticaticated как user1 на AD, отказал бы из-за Запрещать правила.

WEBVPN/ПОЛЬЗОВАТЕЛЬ IPSEC, authenticaticated как user2 на AD, успешно выполнился бы (Позвольте правило + протокол туннелирования, с которым совпадают).

L2TPoverIPsec, authenticaticated как user2 на AD, отказал бы из-за несоответствия протокола туннелирования.
Поддержка Протокола туннелирования, как определено в RFC 2867 и 2868.

6. Реализация Active Directory "Участника" / Состав группы, чтобы Позволить или Запретить Доступ

Этот случай тесно связан для Преобразования регистра 5, обеспечивает более логический поток и является рекомендуемым методом, так как это устанавливает проверку состава группы как условие.

1. Настройте AD пользователя, чтобы быть "Участником" определенной группы. Используйте название, которое размещает его наверху иерархии группы (КОНСУЛЬТАНТЫ VPN ASA). В AD LDAP Состав группы определен AD атрибутом "memberOf".

   Важно, чтобы группа была наверху списка, так как можно в настоящее время только применить правила к первой группе / "memberOf" строка. В Выпуске 7.3 вы будете в состоянии выполнить несколько групп фильтрацию и осуществление.
2. На ASA создайте карту атрибутов LDAP с минимальное сопоставление:

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

Примечание: Добавьте большие атрибуты к карте как требуется. Данные примеры показывают только минимум для управления этой определенной функцией (Позвольте или Запретите Доступ на основе Состава группы).

Что карта атрибутов LDAP означает или принуждает?

User=joe_consultant, часть AD, который является участником AD группы "КОНСУЛЬТАНТЫ VPN ASA", будет предоставленным доступом, только если пользователь использует IPsec (tunnel-protocol=4=IPSec).

User=joe_consultant, часть AD, откажет доступ VPN во время любого другого клиента удаленного доступа (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC, и так далее).

User=bill_the_hacker не позволят войти, так как у пользователя нет AD членства.

7. Реализация Active Directory "Правил Часов/Времени дня Входа в систему"

Этот вариант использования описывает, как установить и принудить правила Времени дня о AD/LDAP.

Вот процедура, чтобы сделать это:

1. На AD/сервере LDAP:Выберите пользователя.Щелкните правой кнопкой мыши> **Свойства**.Выберите вкладку, которая будет использоваться, для установки атрибута (Пример. Вкладка Общие).Выберите поле/атрибут, например поле "Office", чтобы использоваться, чтобы принудить time-range и ввести имя time-range (например, Бостон). Конфигурация "офиса" на GUI сохранена в "physicalDeliveryOfficeName" атрибута AD/LDAP.

2. На ASA

   Создайте таблицу соответствий атрибута LDAP.Сопоставьте атрибут AD/LDAP "physicalDeliveryOfficeName" с "Пунктами меню Access Hours (Часы доступа)" атрибута ASA.

   Пример:

   ```
   B200-54(config-time-range)# show run ldap
   ldap attribute-map TimeOfDay
   map-name physicalDeliveryOfficeName Access-Hours
   ```

3. На ASA привяжите Карту атрибутов LDAP к записи aaa-server:

   ```
   B200-54(config-time-range)# show runn aaa-server microsoft
   aaa-server microsoft protocol ldap
   aaa-server microsoft host audi-qa.frdevtestad.local
   ldap-base-dn dc=frdevtestad,dc=local
   ldap-scope subtree
   ldap-naming-attribute sAMAccountName
   ldap-login-password hello
   ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
   ldap-attribute-map TimeOfDay
   ```

4. На ASA создайте объект time-range, который имеет значение названия, которое

назначено на пользователя (значение офиса в шаге 1): `B200-54(config-time-range)# show runn time-range`

```
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```

5. Установите сеанс удаленного доступа VPN:

   Сеанс должен успешно выполниться если в time-range.Сеанс должен отказать если вне time-range.

8. Используйте конфигурацию карты ldap для Сопоставления Пользователя в Определенную Групповую политику и Использование Команда группы серверов авторизации, в случае Двойной аутентификации

1. В этом сценарии, двойная аутентификация используется. Первый используемый сервер проверки подлинности является RADIUS, и вторая аутентификация разъединяют используемый, Сервер LDAP.

   Настройте Сервер LDAP, а также сервер RADIUS. Например:

```
ASA5585-S10-K9# show runn aaa-server
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

   Definine Карта атрибутов LDAP. Например:

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

   Определите туннельную группу и привяжите RADIUS и Сервер LDAP для аутентификации. Например:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

   Просмотрите групповую политику, которая используется в конфигурации туннельной

группы:

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

С этой конфигурацией пользователи AnyConnect, которые были сопоставлены правильно с использованием атрибутов LDAP, не были размещены в групповую политику, Тестовый Safenet Политики. Вместо этого они были все еще размещены в групповую политику по умолчанию, в этом случае NoAccess.

Посмотрите фрагмент отладок (ldap 255 отладки) и системные журналы на информационном уровне:

```
----------------------------------------------------------------------------

memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                        mapped to IETF-Radius-Class: value = Test-Policy-Safenet

[47]                        mapped to LDAP-Class: value = Test-Policy-Safenet

----------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
test123

%ASA-6-113003: AAA group policy for user test123 is being set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123

%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

Эти системные журналы показывают сбой, поскольку пользователю давали групповую политику NoAccess, которой установили одновременный вход в систему в 0 даже при

том, что системные журналы говорят, что это получило пользователя определенная групповая политика.

Для назначения пользователя в групповой политике, на основе карты LDAP, у вас должна быть эта команда: **тестовый ldap группы серверов авторизации** (в этом случае, **тестовый ldap** является названием Сервера LDAP). Например:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. Теперь, если первый сервер проверки подлинности (RADIUS, в данном примере) действительно передавал определяемые пользователем атрибуты, например IEFT-атрибут-Class, в этом случае, пользователь будет сопоставлен с групповой политикой, передаваемой RADIUS. Таким образом даже при том, что дополнительному серверу настроили карту LDAP, и атрибуты LDAP пользователя действительно сопоставляют пользователя с другой групповой политикой, групповая политика, передаваемая первым сервером проверки подлинности, будет принуждена.

   Чтобы сделать, чтобы пользователь разместил в групповую политику на основе атрибута карты LDAP, необходимо задать эту команду под туннельной группой: **тестовый ldap группы серверов авторизации**.

3. Если первый сервер проверки подлинности является SDI или OTP, который не может передать определяемый пользователем атрибут, то пользователь попал бы в групповую политику по умолчанию туннельной группы. В этом случае, NoAccess даже при том, что сопоставление LDAP корректно.

   В этом случае вам также были бы нужны команда, **тестовый ldap группы серверов авторизации**, под туннельной группой для пользователя, чтобы быть размещенными в корректную групповую политику.

4. Если оба из серверов являются тем же RADIUS или Серверами LDAP, то вам не нужна команда **группы серверов авторизации** для блокировки групповой политики для работы.

Проверка

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username    : test123                Index       : 2
Assigned IP : 10.34.63.1           Public IP   : 10.116.122.154
```

```
Protocol    : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License     : AnyConnect Essentials
Encryption  : 3DES 3DES 3DES        Hashing     : SHA1 SHA1 SHA1
Bytes Tx    : 14042                 Bytes Rx    : 8872
Group Policy : Test-Policy-Safenet   Tunnel Group : Test_Safenet
Login Time  : 10:45:28 UTC Fri Sep 12 2014
Duration    : 0h:01m:12s
Inactivity  : 0h:00m:00s
NAC Result  : Unknown
VLAN Mapping : N/A                   VLAN        : none
```

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Отладка транзакции LDAP

Эти отладки могут использоваться, чтобы помочь изолировать проблемы с DAP configuraiton:

- **debug ldap 255**
- **отладьте трассировку dap**
- **debug aaa authentication**

ASA не в состоянии Аутентифицировать Пользователей от Сервера LDAP

В случае, если ASA не в состоянии аутентифицировать пользователей от подачи LDAP, вот некоторые примеры отладки:

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username    : test123                 Index       : 2
Assigned IP : 10.34.63.1            Public IP   : 10.116.122.154
Protocol    : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License     : AnyConnect Essentials
Encryption  : 3DES 3DES 3DES        Hashing     : SHA1 SHA1 SHA1
Bytes Tx    : 14042                 Bytes Rx    : 8872
Group Policy : Test-Policy-Safenet   Tunnel Group : Test_Safenet
Login Time  : 10:45:28 UTC Fri Sep 12 2014
Duration    : 0h:01m:12s
Inactivity  : 0h:00m:00s
NAC Result  : Unknown
VLAN Mapping : N/A                   VLAN        : none
```

От этих отладок или формат DN Входа в систему LDAP является неправильным или пароль, является неправильным, так проверьте обоих для решения вопроса.