Присвоение группы политик для клиентов AnyConnect, которые используют LDAP на примере конфигурации головных станций Cisco IOS

Содержание

Введение

Этот документ описывает, как настроить карты атрибута Протокола LDAP для автоматического присвоения корректной политики VPN на пользователя на основе их учетных данных.

> **Примечание:** Поддержка проверки подлинности LDAP для VPN Уровня защищенных сокетов (VPN SSL) пользователи, которые соединяются с головным узлом Cisco IOS®, отслежена идентификатором ошибки Cisco CSCuj20940. Пока поддержка официально не добавлена, Поддержка LDAP является оптимальным уровнем.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- 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 сети Протокола IP. Сервисы каталогов играют важную роль в разработке интранет и интернет-приложений, поскольку они позволяют обмен информацией о пользователях, системах, сетях, сервисах и приложениях всюду по сети.

Часто у администраторов возникает необходимость предоставить пользователям сети VPN различные разрешения на доступ или различное содержание WebVPN. Это может быть завершено с конфигурацией другой политики VPN на сервере VPN и присвоении этих наборов политики к каждому зависиту от пользователя на их учетные данные. В то время как это может быть завершено 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, который понят под головной станцией VPN.

На Устройстве адаптивной защиты (ASA) это регулярно достигается через присвоение политики другой группы другим пользователям с Картой атрибутов LDAP как показано в Использовании ASA Примера конфигурации Карт атрибутов LDAP.

На Cisco IOS та же вещь может быть достигнута с конфигурацией других групп политик под контекстом WebVPN и использованием Карт атрибутов LDAP для определения, какая группа политик пользователю назначат. На головных станциях Cisco IOS атрибут "memberOf" AD сопоставлен с группой соискателя атрибута Аутентификации, авторизации и учета (AAA). Для получения дополнительной информации на сопоставлениях атрибута по умолчанию, посмотрите LDAP на Устройствах IOS Использование Динамического Примера конфигурации Карт Атрибута. Однако, для VPN SSL, существует два соответствующих сопоставления атрибута AAA:

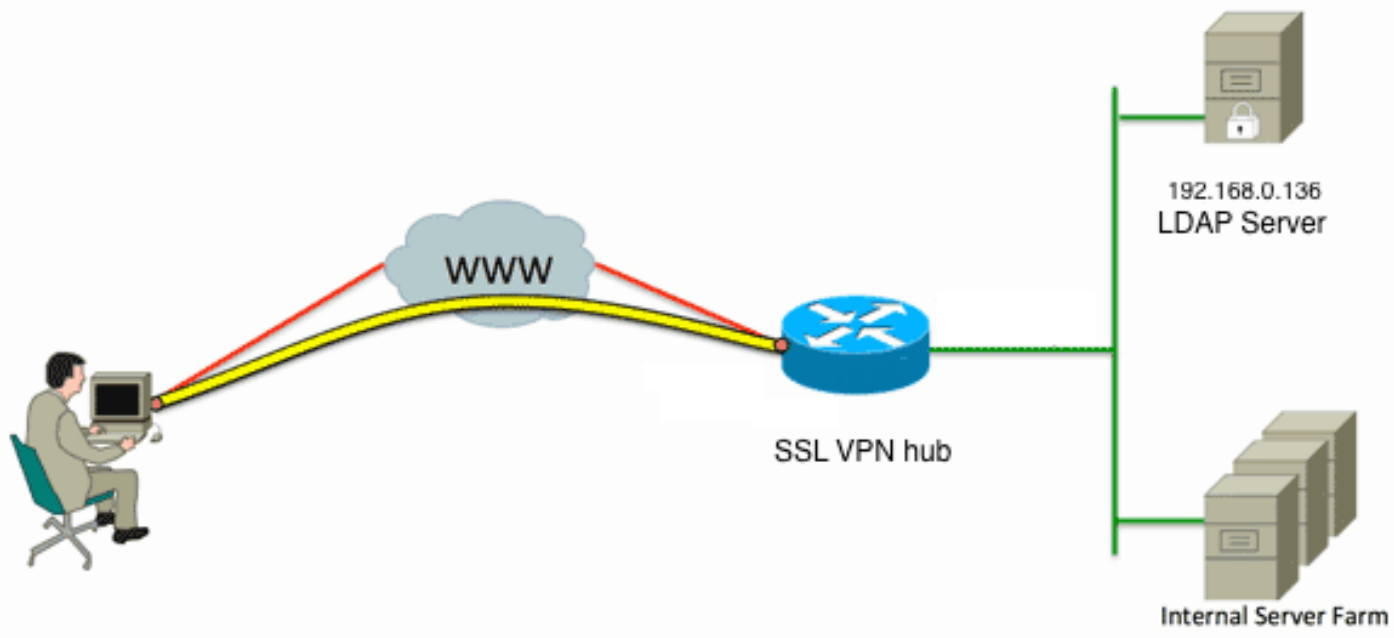
Название атрибута AAA	Уместность VPN SSL
пользовательская группа vpn	сопоставляет с группой политик, определенной под контекстом WebV
webvpn-context	сопоставляет с самим фактическим контекстом WebVPN

Поэтому Карта атрибутов LDAP должна сопоставить соответствующий атрибут LDAP с любым из этих двух атрибутов AAA.

Настройка

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети



Эта конфигурация использует Карту атрибутов LDAP для сопоставления атрибута "memberOf" LDAP с пользовательской группой vpn атрибута AAA.

1. Настройте метод аутентификации и группу AAA-серверов.

```
aaa new-model
!
!
aaa group server ldap AD
 server DC1
!
aaa authentication login default local
aaa authentication login vpn local
aaa authentication login AD group ldap local
aaa authorization exec default local
```

2. Настройте Карту атрибутов LDAP.

```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```

3. Настройте Сервер LDAP, который ссылается на предыдущую Карту атрибутов LDAP.

```
ldap server DC1
 ipv4 192.168.0.136
 attribute map ADMAP
 bind authenticate root-dn CN=Cisco Systems,OU=Service Accounts,DC=chillsthrills,
DC=local password 7 <removed>
 base-dn DC=chillsthrills,DC=local
```

4. Настройте маршрутизатор для действия как сервер WebVPN. В данном примере, так как атрибут "memberOf" будет сопоставлен с атрибутом "пользовательской группы vpn", одиночный контекст WebVPN настроен с группами несколька правил, которые включают политику "NOACCESS". Эта группа политик для пользователей, у которых нет соответствия "memberOf" значением.

```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
webvpn gateway gateway_1
 hostname vpn
 ip address 173.11.196.220 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
  hide-url-bar
  timeout idle 60
  timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
  functions svc-enabled
  banner "special access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

Предупреждения

1. Если пользователь является "memberOf" множителем группы, первое значение "memberOf" используется маршрутизатором.
2. То, что нечетно в этой конфигурации, - то, что название группы политик должно быть полным соответствием для **завершенной** строки, выдвинутой Сервером LDAP для "memberOf значение". Обычно администраторы используют короче и более

соответствующие названия для группы политик, такие как VPNACCESS, но кроме косметической проблемы это может привести к большей проблеме. Строке атрибута "memberOf" весьма свойственно быть значительно больше, чем, что использовалось в данном примере. Например, рассмотрите это сообщение отладки:

```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
webvpn gateway gateway_1
 hostname vpn
 ip address 173.11.196.220 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
  hide-url-bar
  timeout idle 60
  timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
  functions svc-enabled
  banner "special access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

Это ясно показывает, что строка, полученная от AD:

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

Однако с тех пор нет такой определенной группы политик, если администратор пытается настроить такую групповую политику, она приводит к ошибке, потому что Cisco IOS имеет предел на количестве символов на название группы политик:

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

В таких ситуациях существует два возможных обходной пути:

1. Используйте другой атрибут LDAP, такой как "отдел".Рассмотрите эту Карту атрибутов LDAP:

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

В этом случае значение атрибута отдела для пользователя может быть установлено в значение, такое как VPNACCESS, и конфигурация WebVPN немного более проста:

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

2. Используйте ключевое слово DN К СТРОКЕ в Карте атрибутов LDAP.Если предыдущий обходной путь не подходит тогда, администратор может использовать ключевое слово dn к строке в Карте атрибутов LDAP для извлечения просто значения Общего имени (CN) из строки "memberOf". В этом сценарии Карта атрибутов LDAP была бы:

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
```

```
end
```

И конфигурация WebVPN была бы:

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

Примечание: В отличие от этого, в ASA, где можно использовать команду **значения карты** в соответствии с картой атрибута для соответствия со значением, полученным от Сервера LDAP до некоторого другого локально значительного значения, головные станции Cisco IOS не имеют этой опции и поэтому не как гибкие. CSCts31840 идентификатора ошибки Cisco был подан для адресации к этому.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

- **атрибуты show ldap**
- **сервер show ldap все**

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с

документом "Важные сведения о командах отладки".

Для устранения проблем сопоставления атрибута LDAP включите эти отладки:

- ldap отладки все
- событие ldap отладки
- debug aaa authentication
- debug aaa authorization