Положение VPN версии ASA 9.2.1 с примером конфигурации ISE

Содержание

Введение

Этот документ описывает, как настроить устройство адаптивной защиты Cisco (ASA) Версия 9.2.1 чтобы пользователям VPN положения против платформы Cisco Identity Services Engine (ISE) без потребности в Промежуточном узле (IPN).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о конфигурации VPN Настройки интерфейса командной строки ASA и Протокола SSL
- Базовые знания о конфигурации VPN для удаленного доступа на ASA

- Базовые знания о ISE и сервисах положения

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Версии программного обеспечения Cisco ASA 9.2.1 и позже
- Версия 7 Microsoft Windows с версией 3.1 защищенного мобильного клиента Cisco AnyConnect Secure Mobility
- Версия 1.2 Cisco ISE с Исправлением 5 или позже

Общие сведения

Версия 9.2.1 Cisco ASA поддерживает изменение авторизации RADIUS (CoA) (RFC 5176). Это обеспечивает положение пользователей VPN против Cisco ISE без потребности в IPN. После того, как пользователь VPN входит, ASA перенаправляет веб - трафик к ISE, где пользователь настроен с Агентом Network Admission Control (NAC) или веб-Агентом. Агент выполняет определенные проверки на пользовательской машине для определения ее соответствия против настроенного набора правил положения, таких как Операционная система (OS), исправления, AntiVirus, Сервис, Приложение или правила Реестра.

Результаты подтверждения состояния тогда передаются ISE. Если машину считают жалобой, то ISE может передать RADIUS CoA к ASA с новым набором политики авторизации. После успешного подтверждения состояния и CoA, пользователь является предоставленным доступом к внутренним ресурсам.

Настройка

Диаграмма сети и поток трафика

Вот трафик, как проиллюстрировано в схеме сети:

1. Удаленный пользователь использует Cisco Anyconnect для доступа VPN к ASA.

2. ASA передает Access-Request RADIUS за тем пользователем к ISE.

3. Тот запрос поражает политику под названием **ASA92-положение** на ISE. В результате профиль авторизации **ASA92-положения** возвращен. ISE передает Access-Accept RADIUS с двумя Парами атрибут-значение Cisco:

   url-redirect-acl=redirect - это - название Списка контроля доступа (ACL), которое определено локально на ASA, который решает трафик, который должен быть перенаправлен.

url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway? sessionId=xx&action=cpp - это - URL, к которому должен быть перенаправлен удаленный пользователь.**Совет:** Серверы Системы доменных имен (DNS), которые назначены на клиенты VPN, должны быть в состоянии решить Полное доменное имя (FQDN), которое возвращено в URL перенаправления. Если фильтры VPN настроены, чтобы ограничить доступ на уровне туннельной группы, гарантировать, что клиентский пул в состоянии обратиться к серверу ISE на настраиваемом порте (**TCP 8443** в данном примере).

4. ASA передает Запрос RADIUS Accounting, запускают пакет, и получает ответ. Это необходимо для передачи всех подробных данных в отношении сеанса к ISE. Эти подробные данные включают session_id, внешний IP - адрес клиента VPN и IP-адрес ASA. ISE использует session_id для определения того сеанса. ASA также передает периодические промежуточные учетные данные, где большей частью Важного атрибута является Обрамленный IP-адрес с IP, который назначен на клиента ASA (**10.10.10.10** в данном примере).

5. Когда трафик от пользователя VPN совпадает с локально определенным ACL (перенаправление), это перенаправлено к **https://ise2.test-cisco.com:8443**. Зависящий от конфигурации, ISE настраивает Агента NAC или веб-Агента.

6. После того, как агент установлен на клиентском компьютере, он автоматически выполняет определенные проверки. В данном примере это ищет **c:\test.txt** файл. Это также передает отчёт о положении ISE, который может включать множественные обмены с использованием протокола SWISS и портов TCP/UDP 8905 для доступа к ISE.

7. Когда ISE получает отчёт о положении от агента, это обрабатывает правила авторизации еще раз. На этот раз результат положения известен, и другое правило поражено. Это передает пакет RADIUS CoA:

   Если пользователь совместим, то Загружаемый список ACL (DACL), который передается название, которое разрешает полный доступ (AuthZ управляют ASA92-совместимый).

   Если пользователь не соответствующ стандарту, то название DACL, которое разрешает ограниченный доступ, передается (AuthZ управляют ASA92-несовместимый).**Примечание:** RADIUS CoA всегда подтверждается; т.е. ASA передает ответ на ISE для подтверждения.

8. ASA удаляет перенаправление. Если этому не кэшировали DACLs, это должно передать Access-Request для загрузки их от ISE. Определенный DACL присоединен к сеансу VPN.

9. В следующий раз, когда пользователь VPN пытается обратиться к веб-странице, она может обратиться ко всем ресурсам, которые разрешены DACL, который установлен на ASA.
   Если пользователь несовместим, только ограниченный доступ предоставлен.
   Примечание: Эта модель потока отличается от большинства сценариев тот RADIUS CoA использования. Для проводных/беспроводных аутентификаций 802.1x RADIUS CoA не включает атрибутов. Это только инициирует вторую аутентификацию, на

которой подключены все атрибуты, такие как DACL. Для положения VPN ASA нет никакой второй аутентификации. Весь из атрибуты возвращен в RADIUS CoA. Сеанс VPN активен, и не возможно изменить большинство настроек пользователя VPN.

Конфигурации

Используйте этот раздел для настройки ASA и ISE.

ASA

Вот основная конфигурация ASA для доступа AnyConnect Cisco:

```
ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address xxxx 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.111.10 255.255.255.0

aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
 key cisco

webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable
```

Для интеграции ASA с положением ISE гарантируйте что вы:

- Настройте аутентификацию, авторизацию и учет (AAA) для динамической авторизации для принятия CoA.
- Настройте учет как туннельную группу для передачи подробных данных сеанса VPN к ISE.
- Настройте промежуточный учет, который передаст IP-адрес, назначенный на

пользователя, и периодически обновлять статус сеанса на ISE

- Настройте ACL перенаправления, который решает, позволены ли DNS и трафик ISE. Весь другой трафик HTTP перенаправлен к ISE для положения.

Вот пример конфигурации:

```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www

aaa-server ISE protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (inside) host 10.48.66.74
 key cisco

tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 accounting-server-group ISE
default-group-policy GP-SSL
```

ISE

Выполните эти шаги для настройки ISE:

1. Перейдите к **администрированию> Сетевые ресурсы> Сетевые устройства** и добавьте ASA как сетевое устройство:

2. Перейдите к **Политике> Результаты> Авторизация> Загружаемый список ACL** и настройте DACL так, чтобы это разрешило полный доступ. Конфигурация списка доступа по умолчанию разрешает весь IP - трафик на ISE:

3. Настройте подобный ACL, который предоставляет ограниченный доступ (для non совместимые пользователи).

4. Перейдите к **Политике> Результаты> Авторизация> Профили Авторизации** и настройте Профиль Авторизации под названием **ASA92-положение**, которое перенаправляет пользователей для положения. Проверьте **веб-**флажок **Redirection**, выберите **Client Provisioning** от выпадающего списка и гарантируйте, что **перенаправление** появляется в поле ACL (что ACL определен локально на ASA):

5. Настройте Профиль Авторизации под названием **ASA92-совместимый**, который должен только возвратить DACL под названием **PERMIT_ALL_TRAFFIC**, который

предоставляет полный доступ для совместимых пользователей:

6. Настройте подобный Профиль Авторизации под названием **ASA92-несовместимый**, который должен возвратить DACL с ограниченным доступом (для non совместимые пользователи).

7. Перейдите к **Политике> Авторизация** и настройте Правила авторизации:

   Создайте правило, которое позволяет полный доступ, если результаты положения совместимы. Результатом является **ASA92-совместимая** политика авторизации.

   Создайте правило, которое предоставляет ограниченный доступ, если результаты положения не соответствующи стандарту. Результатом является **ASA92-несовместимая** политика авторизации.

   Гарантируйте что, если ни одно из предыдущих двух правил не поражено, то стандартное правило возвращает **ASA92-положение**, которое вызывает перенаправление на ASA.

8. Правила проверки подлинности по умолчанию проверяют имя пользователя во внутреннем идентификационном хранилище. Если это должно быть изменено (зарегистрировался в Active Directory (AD), например), то перейдите к **Политике> Аутентификация** и внесите изменение:

9. Перейдите к **Политике> Клиентская Инициализация** и настройте правила инициализации. Это правила, которые решают тип Агента, который должен быть настроен. В данном примере существует только одно простое правило, и ISE выбирает NAC Agent для всех систем Microsoft Windows:

   Когда Агенты не находятся на ISE, возможно загрузить их:

10. Если необходимо, можно перейти к **администрированию> Система> Параметры настройки> Прокси** и настраивать прокси для ISE (для доступа к Интернету).

11. Настройте правила положения, которые проверяют конфигурацию клиента. Можно настроить правила, которые проверяют:

    файлы - существование, версия, дата

реестр - ключ, значение, существование

приложение - имя процесса, выполнение, не выполнение

сервис - имя сервиса, выполнение, не выполнение

когда определения обновлены, **антивирус** - больше чем 100 поставщиков поддержали, версия

когда определения обновлены, **антишпион** - больше чем 100 поставщиков поддержали, версия

составное условие - смесь всех

условия настраиваемого словаря - использование большинства словарей ISE

12. В данном примере выполнена только простая проверка существования файла. Если **c:\test.txt** файл присутствует на клиентском компьютере, это - совместимый и позволенный полный доступ. Перейдите к **Политике> Условия> Условия Файла** и настройте условие файла:

13. Перейдите к **Политике> Результаты> Положение> Требования** и создайте требование. Когда предыдущее условие удовлетворено, это требование должно быть удовлетворено. Если это не, то восстановительное мероприятие выполняется. Могло бы быть много типов доступных восстановительных мероприятий, но в данном примере, используется самый простой: отображено определенное сообщение.

Примечание: В обычном сценарии Восстановительное мероприятие Файла может использоваться (ISE предоставляет загружаемый файл).

14. Перейдите к **Политике> Положение** и используйте требование, чтобы вы создали в предыдущем шаге (названный **file_requirement**) в правилах положения. Единственное правило положения требует, чтобы все системы Microsoft Windows встретили **file_requirement**. Если это требование удовлетворено, то станция совместима; если это не встречено, то станция не соответствующа стандарту.

Периодическая переоценка

По умолчанию положение является одноразовым событием. Однако иногда существует потребность периодически проверить пользовательское соответствие и отрегулировать доступ к ресурсам на основе результатов. Эта информация выдвинута через протокол SWISS (Агент NAC) или закодирована в рамках приложения (веб-Агент).

Выполните эти шаги для проверения пользовательского соответствия:

1. Перейдите к **администрированию> Параметры настройки> Положение> Переоценки** и

включите переоценку глобально (на идентификационную конфигурацию группы):

2. Создайте условие положения, которое совпадает со всеми переоценками:

3. Создайте подобное условие, которое совпадает только с начальными оценками:

Оба из этих условий могут использоваться в правилах положения. Первое правило совпадает только с начальными оценками, и второй совпадает со всеми последующими оценками:

Проверка

Чтобы подтвердить, что ваша конфигурация работает правильно, гарантируйте, что эти шаги выполнены, как описано:

1. Пользователь VPN соединяется с ASA.

2. ASA передает RADIUS-Request и получает ответ с **перенаправлением URL** и атрибутами **acl перенаправления URL**:

3. Журналы ISE указывают, что авторизация совпадает с профилем положения (первая запись журнала):

4. ASA добавляет перенаправление к сеансу VPN:
```
aaa_url_redirect: Added url redirect:https://ise2.test-cisco.com:8443/
 guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
 acl:redirect for 10.10.10.10
```
5. Статус сеанса VPN на ASA показывает, что положение требуется и перенаправляет трафик HTTP:
```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username    : cisco                 Index       : 9
Assigned IP : 10.10.10.10           Public IP   : 10.147.24.61
Protocol    : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License     : AnyConnect Essentials
Encryption  : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing     : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx    : 16077                 Bytes Rx    : 19497
Pkts Tx     : 43                    Pkts Rx     : 225
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : GP-SSL                Tunnel Group : RA
```

```
Login Time  : 14:55:50 CET Mon Dec 23 2013
Duration    : 0h:01m:34s
Inactivity  : 0h:00m:00s
VLAN Mapping : N/A                    VLAN        : none
Audt Sess ID : c0a8700a0000900052b840e6
Security Grp : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
 Tunnel ID   : 9.1
 Public IP   : 10.147.24.61
 Encryption  : none                   Hashing     : none
 TCP Src Port : 50025                  TCP Dst Port : 443
 Auth Mode   : userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 28 Minutes
 Client OS   : win
 Client Type : AnyConnect
 Client Ver  : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx    : 5204                   Bytes Rx    : 779
 Pkts Tx     : 4                      Pkts Rx     : 1
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID   : 9.2
 Assigned IP : 10.10.10.10           Public IP   : 10.147.24.61
 Encryption  : RC4                    Hashing     : SHA1
 Encapsulation: TLSv1.0                TCP Src Port : 50044
 TCP Dst Port : 443                    Auth Mode   : userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 28 Minutes
 Client OS   : Windows
 Client Type : SSL VPN Client
 Client Ver  : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx    : 5204                   Bytes Rx    : 172
 Pkts Tx     : 4                      Pkts Rx     : 2
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0

DTLS-Tunnel:
 Tunnel ID   : 9.3
 Assigned IP : 10.10.10.10            Public IP   : 10.147.24.61
 Encryption  : AES128                 Hashing     : SHA1
 Encapsulation: DTLSv1.0               UDP Src Port : 63296
 UDP Dst Port : 443                    Auth Mode   : userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Client OS   : Windows
 Client Type : DTLS VPN Client
 Client Ver  : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx    : 5669                   Bytes Rx    : 18546
 Pkts Tx     : 35                     Pkts Rx     : 222
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0

ISE Posture:
 Redirect URL : https://ise2.test-cisco.com:8443/guestportal/gateway?
   sessionId=c0a8700a0000900052b840e6&action=cpp
 Redirect ACL : redirect
```

6. Клиент, который инициирует трафик HTTP, который совпадает с ACL перенаправления, перенаправлен к ISE:

```
aaa_url_redirect: Created proxy for 10.10.10.10
aaa_url_redirect: Sending url redirect:https://ise2.test-cisco.com:8443/
 guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
 for 10.10.10.10
```

7. Клиент перенаправлен к ISE для положения:

8. Агент NAC установлен. После того, как Агент NAC установлен, это загружает правила положения через протокол SWISS и выполняет проверки для определения соответствия. Отчёт о положении тогда передается ISE.

9. ISE получает отчёт о положении, переоценивает правила авторизации, и (в случае необходимости) изменяет статус авторизации и передает CoA. Это может быть проверено в ise-psc.log:

```
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8700a0000900052b840e6
 :::- Decrypting report
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
 :::- User cisco belongs to groups NAC Group:NAC:IdentityGroups:User Identity
 Groups:Employee,NAC Group:NAC:IdentityGroups:An
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
 :::- Posture report token for endpoint mac 08-00-27-CD-E8-A2 is Healthy
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
 :::- Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2
cisco.cpm.posture.runtime.PostureCoA -:cisco:c0a8700a0000900052b840e6
 :::- Posture CoA is triggered for endpoint [null] with session
 [c0a8700a0000900052b840e6]
```

10. ISE передает RADIUS CoA, который включает session_id и название DACL, которое разрешает полный доступ:

    Это отражено в журналах ISE:

    Первая запись журнала для начальной аутентификации, которая возвращает профиль положения (с перенаправлением).

    Вторая запись журнала заполнена после того, как совместимый отчёт SWISS получен.

    Когда CoA передается, наряду с подтверждением (описанный как Динамическая Следовавшая Авторизация), третья запись журнала заполнена.

    Когда ASA загружает DACL, заключительная запись журнала создана.

11. Отладки на ASA показывают, что CoA получен, и перенаправление удалено. ASA загружает DACLs в случае необходимости:

```
ASA# Received RAD_COA_REQUEST

RADIUS packet decode (CoA-Request)

Radius: Value (String) =
41 43 53 3a 43 69 73 63 6f 53 65 63 75 72 65 2d   | ACS:CiscoSecure-
44 65 66 69 6e 65 64 2d 41 43 4c 3d 23 41 43 53   | Defined-ACL=#ACS
41 43 4c 23 2d 49 50 2d 50 45 52 4d 49 54 5f 41   | ACL#-IP-PERMIT_A
```

```
4c 4c 5f 54 52 41 46 46 49 43 2d 35 31 65 66 37   | LL_TRAFFIC-51ef7
64 62 31                                          | db1

Got AV-Pair with value audit-session-id=c0a8700a0000900052b840e6
Got AV-Pair with value ACS:CiscoSecure-Defined-ACL=
 #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1

aaa_url_redirect: Deleted url redirect for 10.10.10.10
```

12. После сеанса VPN Cisco имеет DACL, примененный (полный доступ) для пользователя:

```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username    : cisco                 Index       : 9
Assigned IP : 10.10.10.10           Public IP   : 10.147.24.61
Protocol    : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License     : AnyConnect Essentials
Encryption  : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing     : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx    : 94042                 Bytes Rx    : 37079
Pkts Tx     : 169                   Pkts Rx     : 382
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : GP-SSL                Tunnel Group : RA
Login Time  : 14:55:50 CET Mon Dec 23 2013
Duration    : 0h:05m:30s
Inactivity  : 0h:00m:00s
VLAN Mapping : N/A                   VLAN        : none
Audt Sess ID : c0a8700a0000900052b840e6
Security Grp : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
 Tunnel ID   : 9.1
 Public IP   : 10.147.24.61
 Encryption  : none                  Hashing     : none
 TCP Src Port : 50025                 TCP Dst Port : 443
 Auth Mode   : userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 24 Minutes
 Client OS   : win
 Client Type : AnyConnect
 Client Ver  : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx    : 5204                  Bytes Rx    : 779
 Pkts Tx     : 4                     Pkts Rx     : 1
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID   : 9.2
 Assigned IP : 10.10.10.10           Public IP   : 10.147.24.61
 Encryption  : RC4                   Hashing     : SHA1
 Encapsulation: TLSv1.0               TCP Src Port : 50044
 TCP Dst Port : 443                   Auth Mode   : userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 24 Minutes
 Client OS   : Windows
 Client Type : SSL VPN Client
 Client Ver  : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx    : 5204                  Bytes Rx    : 172
 Pkts Tx     : 4                     Pkts Rx     : 2
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0
 Filter Name : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

```
DTLS-Tunnel:
 Tunnel ID   : 9.3
 Assigned IP : 10.10.10.10          Public IP   : 10.147.24.61
 Encryption  : AES128               Hashing     : SHA1
 Encapsulation: DTLSv1.0             UDP Src Port : 63296
 UDP Dst Port : 443                  Auth Mode   : userPassword
 Idle Time Out: 30 Minutes           Idle TO Left : 29 Minutes
 Client OS   : Windows
 Client Type : DTLS VPN Client
 Client Ver  : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx    : 83634                Bytes Rx    : 36128
 Pkts Tx     : 161                  Pkts Rx     : 379
 Pkts Tx Drop : 0                    Pkts Rx Drop : 0
 Filter Name : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

Примечание: ASA всегда удаляет правила перенаправления, даже когда CoA не имеет никакого DACL подключенным.

Устранение неполадок

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

Отладки на ISE

Перейдите к **администрированию> Регистрация> Конфигурация Журнала Отладки** для включения отладок. Cisco рекомендует включить временные отладки для:

- ШВЕЙЦАРЕЦ
- Без остановок передача (NSF)
- Сеанс NSF
- Условие
- Положение

Введите эту команду в CLI для просмотра отладок:

```
ise2/admin# show logging application ise-psc.log tail count 100
```

Перейдите к **Операциям> Отчёты> Отчёты о ISE> Оконечные точки и Пользователи> Подробная Оценка Положения** для просматривания отчетов о положении:

На странице Posture More Detail Assessment существует название политики с названием требования, которое отображено, наряду с результатами:

Отладки на ASA

Можно включить эти отладки на ASA:

- **перенаправление URL debug aaa**
- **debug aaa authorization**
- **динамическая авторизация debug radius**

- **debug radius декодирует**
- **пользовательский Cisco debug radius**

Отладки для агента

Для Агента NAC возможно собрать отладки с Поставщиком программного блока Журнала Cisco, который инициируется от GUI или с CLI: **CCAAgentLogPackager.app**.

> **Совет:** Можно декодировать результаты с программным средством Центра технической поддержки (TAC).

Для получения журналов для веб-Агента перейдите к этим местоположениям:

- **C :> Документ и Параметры настройки> <*user*>> Местные настройки> Температура> webagent.log** (декодируемый с Инструментом TAC)
- **C :> Документ и Параметры настройки> <*user*>> Местные настройки> Температура> webagentsetup.log**

> **Примечание:** Если журналы не находятся в этих местоположениях, то проверяют **Переменную среды TEMP**.

Сбой Положения Агента NAC

Если положение отказывает, пользователю предоставляют причину:

Пользователю тогда разрешают восстановительные мероприятия, если они настроены:

Дополнительные сведения

- Настройка внешний сервер для авторизации пользователя на устройстве безопасности
- Руководство конфигурации интерфейса командой строки VPN серии Cisco ASA, 9.1
- Руководство пользователя платформы Cisco Identity Services Engine, выпуск 1.2
- Cisco Systems – техническая поддержка и документация