ASA: удаленный доступ режима мультиконтекста (AnyConnect) VPN

Содержание

Введение

Этот документ описывает, как настроить Виртуальную частную сеть (VPN) Удаленного доступа (RA) на устройстве адаптивной защиты Cisco (ASA) межсетевой экран в режиме Составного контекста (MC). Это показывает Cisco ASA в поддерживаемом многоконтекстном режиме / неподдерживаемые характеристики и требование при лицензировании относительно VPN RA.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- SSL AnyConnect ASA Configuraiton
- Конфигурация составного контекста ASA

Используемые компоненты

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

- Два ASA 5585, работающие 9.5 (2) код
- Клиент AnyConnect 3.1.10010

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

Мультиконтекст является формой виртуализации, которая позволяет множественным независимым копиям приложения работать одновременно на тех же аппаратных средствах с каждой копией (или виртуальное устройство) появляющийся как разное физическое устройство пользователю. Это позволяет одиночному ASA появляться как множественные ASA множественным независимым пользователям. Семейство ASA поддержало действительные межсетевые экраны начиная со своего начального релиза; однако, не было никакой поддержки виртуализации Удаленного доступа в ASA. LAN2LAN VPN (L2L) поддержка мультиконтекста был добавлен для этих 9.0 выпусков. От 9.5.2 мультиконтекстов базировал поддержку виртуализации соединений Удаленного доступа (RA) VPN с ASA.

Поддерживаемые характеристики

- AnyConnect 3. X + подключение SSL (IPv4, IPv6)
- Централизованная конфигурация образа AnyConnect
- Обновление образа AnyConnect

Неподдерживаемые функции

- IKEv2, IKEv1
- Аварийное переключение с сохранением состояния
- Виртуализация Флэша
- Конфигурация образа AnyConnect на контекст
- WebLaunch
- Клиентская загрузка профиля
- DAP и CoA
- CSD/Hostscan
- Распределение нагрузки VPN
- Имя пользователя от сертификата и имя пользователя перед заливкой
- Кастомизация/Локализация

Лицензирование

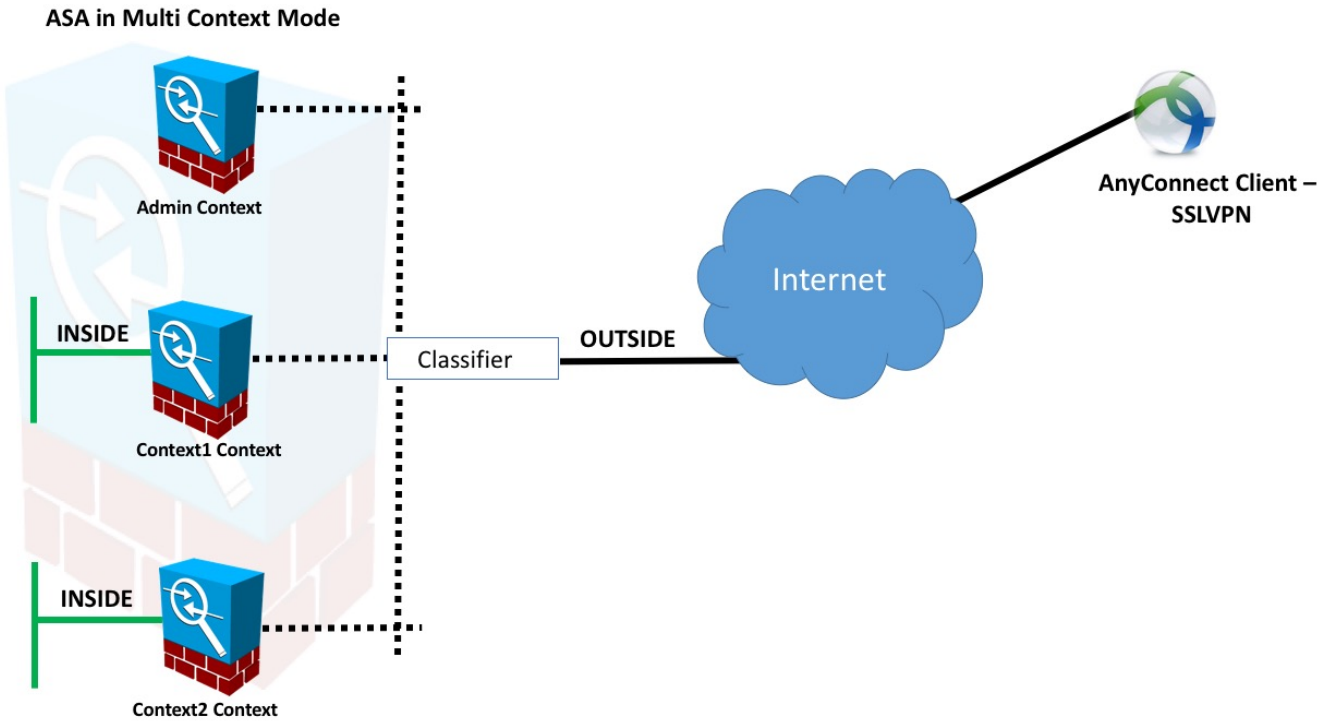
- Лицензия Вершины AnyConnect требуется
- Лицензии основ проигнорировали/не позволенный
- Конфигурируемость для управления максимальным использованием лицензии на контекст
- Конфигурируемость для разрешения разрыва лицензии на контекст

Настройка

В этом разделе описывается настроить Cisco ASA как Локальный сервер CA.

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

Схема сети



> **Примечание:** Составные контексты в данном примере совместно используют интерфейс (СНАРУЖИ), тогда классификатор использует уникальный интерфейс (автоматический или ручной) MAC-адреса к передачам пакетов. Для получения дополнительной информации о том, как устройство безопасности классифицирует пакеты на составной контекст, относятся, Как ASA Классифицирует Пакеты

Конфигурации

Системный контекст

Шаг 1. Конфигурация аварийного переключения.

```
 !! Active Firewall

failover
failover lan unit primary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2

 !! Secondary Firewall

failover
failover lan unit secondary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

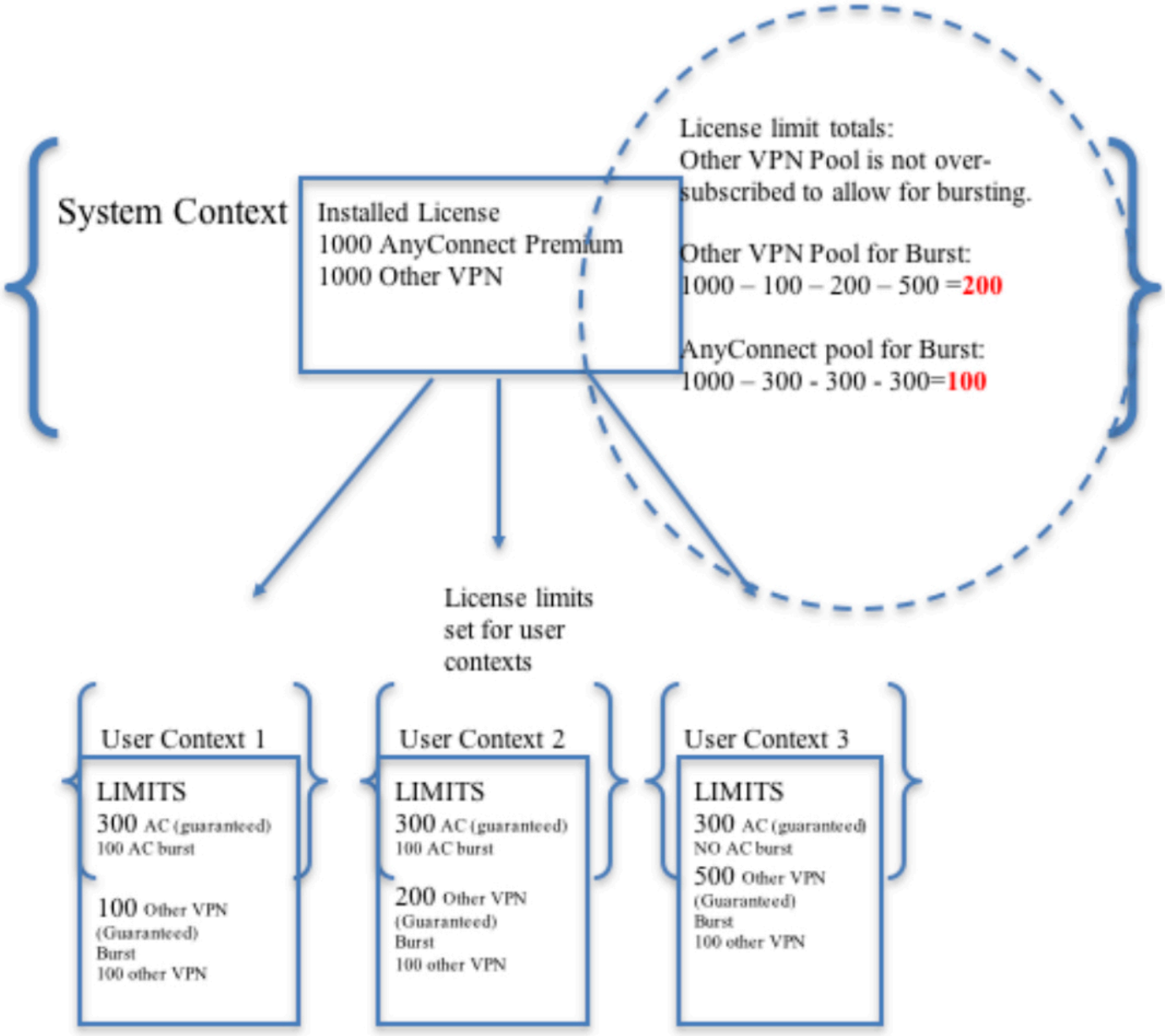
Шаг 2. Выделите VPN Resouce.

Настроенный через существующий класс … конфигурация. Лицензии позволены количеством лицензий или % общего количества на контекст

Новые типы ресурсов представили для MC RAVPN:

- AnyConnect VPN: Гарантируемый контексту и не может быть превышен
- Пакетный AnyConnect VPN: Позвольте дополнительные лицензии контекста вне гарантируемого предела. Пакетный пул состоит из любых лицензий, не гарантируемых контексту, и позволен разрывному контексту на first-come-first-serve основе

Лицензия VPN, Настраивающая модель:



Примечание: ASA5585 предлагает 10,000 максимальных пользовательских сеансов AnyConnect Cisco, и в данном примере 4000 пользовательских сеансов AnyConnect Cisco выделены на контекст.

```
class resource02
 limit-resource VPN AnyConnect  4000
 limit-resource VPN Burst AnyConnect  2000

class resource01
 limit-resource VPN AnyConnect 4 000
 limit-resource VPN Burst AnyConnect  2000
```

Шаг 3. Настройте контексты и назначьте ресурсы.

Примечание: В данном примере GigabitEthernet0/0 разделен среди всего контекста.

```
admin-context admin
context admin
  allocate-interface GigabitEthernet0/0
  config-url disk0:/admin
```

```
context context1
  member resource01
  allocate-interfaceGigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context1
  join-failover-group 1

context context2
  member resource02
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/2
  config-url disk0:/context2
  join-failover-group 2
```

Шаг 4. . Установите Лицензию Вершины на межсетевом экране.

[Активация или деактивация ключей активации]

Контекст администратора

Шаг 1. Установите пакет клиента AnyConnect.

> **Примечание: 1**. Флэш-диск не виртуализирован, и это только доступно от системного контекста.
> 2. Файлы копии к флэш-памяти в системном контексте т.е. образе AnyConnect.
> 3. Образ AnyConnect является совместно используемой конфигурацией.
> 4. Настроенный в контексте администратора только. Не доступный в других контекстах.
> 5. Все контексты автоматически обращаются к этой глобальной конфигурации образа AnyConnect.

```
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
 anyconnect enable
```

Пользовательский контекст 1

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.106.44.38  255.255.255.0 standby 10.106.44.39

!! Enable WebVPN on respective interfaces

webvpn
 enable OUTSIDE
 anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_1 internal
```

```
group-policy GroupPolicy_MC_RAVPN_1 attributes
 banner value "Welcome to Context1 SSLVPN"
 wins-server none
 dns-server value 192.168.20.10
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
 address-pool mypool
 default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
 group-alias MC_RAVPN_1 enable
 group-url https://10.106.44.38/context1  enable
```

Пользовательский контекст 2

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.106.44.36  255.255.255.0 standby 10.106.44.37

!! Enable WebVPN on respective interface

webvpn
 enable OUTSIDE
 anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
 banner value "Welcome to Context2 SSLVPN"
 wins-server none
 dns-server value 192.168.60.10
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com

tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
 address-pool mypool
 default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
 group-alias MC_RAVPN_2 enable
 group-url https://10.106.44.36/context2 enable
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

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

Проверьте, Установлена ли Лицензия Вершины

ASA в частности не распознает лицензию Вершины AnyConnect, но он принуждает характеристики лицензии лицензии Вершины, которые включают:

- AnyConnect, Premium лицензируемый для предела платформы
- AnyConnect для мобильного
- AnyConnect для телефона VPN Cisco
- Advanced Endpoint Assessment

Проверьте, Установлен ли Пакет AnyConnect в Контексте администратора и доступен в пользовательских контекстах

```
 !! AnyConnect package is installed in Admin Context

ciscoasa/pri/ admin/act# show run webvpn
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
 anyconnect enable

ciscoasa/pri/admin/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,1,10010
  Hostscan Version 3.1.10010
  Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed

!! AnyConnect package is available in context1
ciscoasa/pri/admin/act# changeto context context1

ciscoasa/pri/context1/act# show run webvpn
webvpn
 enable OUTSIDE
 anyconnect enable
 tunnel-group-list enable

ciscoasa/pri/context1/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,1,10010
  Hostscan Version 3.1.10010
  Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed
```

Проверьте, Могут ли Пользователи соединиться через AnyConnect на пользовательских контекстах

Совет: Поскольку лучший показ смотрит ниже видео в полном экране.

```
 !! One Active Connection on Context1

ciscoasa/pri/context1/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username    : cisco                 Index       : 5
Assigned IP : 192.168.1.1           Public IP   : 10.142.168.102
Protocol    : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License     : AnyConnect Premium, AnyConnect for Mobile
Encryption  : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing     : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx    : 3186                  Bytes Rx    : 426
Group Policy : GroupPolicy_MC_RAVPN_1 Tunnel Group : MC_RAVPN_1
Login Time  : 15:33:25 UTC Thu Dec 3 2015
Duration    : 0h:00m:05s
Inactivity  : 0h:00m:00s
VLAN Mapping : N/A                   VLAN        : none
Audt Sess ID : 0a6a2c2600005000566060c5
Security Grp : none

!! Changing Context to Context2

ciscoasa/pri/context1/act# changeto context context2

!! One Active Connection on Context2

ciscoasa/pri/context2/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username    : cisco                 Index       : 1
Assigned IP : 192.168.51.1          Public IP   : 10.142.168.94
Protocol    : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License     : AnyConnect Premium
Encryption  : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing     : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx    : 10550                 Bytes Rx    : 1836
Group Policy : GroupPolicy_MC_RAVPN_2 Tunnel Group : MC_RAVPN_2
Login Time  : 15:34:16 UTC Thu Dec 3 2015
Duration    : 0h:00m:17s
Inactivity  : 0h:00m:00s
VLAN Mapping : N/A                   VLAN        : none
Audt Sess ID : 0a6a2c2400001000566060f8
Security Grp : none

!! Changing Context to System

ciscoasa/pri/context2/act# changeto system

!! Notice total number of connections are two (for the device)

ciscoasa/pri/act# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                   Status : Capacity : Installed : Limit
                                 ----------------------------------------
AnyConnect Premium               : ENABLED :   10000 :    10000 :  NONE
Other VPN (Available by Default) : ENABLED :   10000 :    10000 :  NONE
AnyConnect for Mobile            : ENABLED(Requires Premium or Essentials)
```

```
Advanced Endpoint Assessment    : ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone  : ENABLED
VPN-3DES-AES                    : ENABLED
VPN-DES                         : ENABLED
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
VPN Licenses Usage Summary
-------------------------------------------------------------------------------
                        Local : Shared :  All :  Peak : Eff. :
                       In Use : In Use : In Use : In Use : Limit : Usage
                      ------------------------------------------------
AnyConnect Premium    :      2 :      0 :      2 :      2 : 10000 :   0%
 AnyConnect Client    :                :      2 :      2         :   0%
   AnyConnect Mobile  :                :      2 :      2         :   0%
Other VPN             :                :      0 :      0 : 10000 :   0%
 Site-to-Site VPN     :                :      0 :      0         :   0%
-------------------------------------------------------------------------------

!! Notice the resource usage per Context

ciscoasa/pri/act# show resource usage all resource VPN AnyConnect
Resource                Current       Peak     Limit       Denied Context
AnyConnect                    1          1      4000            0 context1
AnyConnect                    1          1      4000            0 context2
```

Устранение неполадок

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

Устранение проблем AnyConnect

> **Совет:** В случае, если ASA не установили Лицензию Вершины, сеанс AnyConnect был бы завершен с ниже системного журнала:
>
> %ASA-6-725002: Устройство завершило подтверждение связи SSL с клиентским OUTSIDE:10.142.168.86/51577 к 10.106.44.38/443 для сеанса TLSv1
> %ASA-6-113012: Успешная проверка подлинности пользователя AAA: локальная база данных: Cisco user =
> %ASA-6-113009: AAA получил политику группы по умолчанию (GroupPolicy_MC_RAVPN_1) для Cisco user =
> %ASA-6-113008: статус транзакции AAA ACCEPT: Cisco user =
> %ASA-3-716057: IP Группового пользователя <10.142.168.86> Сеанс завершился, никакая доступная лицензия Вершины AnyConnect
> %ASA-4-113038: IP Группового пользователя <10.142.168.86> Неспособный создать AnyConnect порождает сеанс.

Ссылки

Комментарии к релизу: 9.5 (2)

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Руководство по поиску и устранению проблем клиента AnyConnect VPN Client - типичные проблемы
- Управление, контролируя и устраняя неполадки сеансов AnyConnect
- Cisco Systems – техническая поддержка и документация