

# ASA 8.0: Настройка проверки подлинности RADIUS для пользователей WebVPN

## Содержание

[Введение](#)

[Предварительные условия](#)

[Настройка сервера ACS](#)

[Настройка устройства защиты](#)

[ASDM](#)

[Интерфейс командной строки](#)

[Проверка](#)

[Проверка с помощью ASDM](#)

[Проверка в интерфейсе командной строки](#)

[Поиск и устранение неполадок](#)

[Дополнительные сведения](#)

## Введение

В этом документе демонстрируется настройка устройства адаптивной защиты Cisco (ASA) для использования сервера RADIUS при аутентификации пользователей WebVPN.

Сервером RADIUS в этом примере является Cisco Access Control Server (ACS) версии 4.1. Настройка выполняется посредством Менеджера устройств адаптивной защиты (ASDM) 6.0(2) на устройстве ASA, работающем под управлением версии ПО 8.0(2).

**Примечание.** В этом примере аутентификация RADIUS настраивается для пользователей WebVPN, но эта конфигурация может использоваться и для других типов сетей VPN удаленного доступа. Достаточно назначить группу сервера AAA требуемому профилю подключения (группе туннелей), как это будет продемонстрировано.

## Предварительные условия

Требуется базовая конфигурация WebVPN.

Для аутентификации пользователей на сервере Cisco ACS должны быть настроены пользователи. Дополнительные сведения см. в разделе [Добавление базовой учетной записи пользователя](#) документа [Управление пользователями](#).

## Настройка сервера ACS

В этом разделе представлены сведения о настройке аутентификации RADIUS на сервере ACS и устройстве ASA.

Для настройки взаимодействия сервера ACS с устройством ASA выполните следующие шаги:

В меню в левой части экрана ACS выберите **Network Configuration** (Конфигурация сети).

В разделе **AAA Clients** (Клиенты AAA) выберите **Add Entry** (Добавить запись).

Укажите сведения о клиенте.

**AAA Client Hostname** (Имя хоста клиента AAA) — выбранное вами имя.

**AAA Client IP Address** (IP-адрес клиента AAA) — адрес, с которого устройство защиты обращается к серверу ACS.

**Shared Secret** (Общий Секретный ключ) — секретный ключ, настроенный на сервере ACS и на устройстве защиты.

В раскрывающемся списке **Authenticate Using** (Средство аутентификации) выберите **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**.

Нажмите кнопку **Submit+Apply** (Отправить и применить).

Пример конфигурации клиента AAA

## [Настройка устройства защиты](#)

### [ASDM](#)

Чтобы настроить устройство ASA для взаимодействия с сервером ACS и аутентификации клиентов WebVPN, выполните следующие шаги в ASDM:

Выберите **Configuration > Remote Access VPN > AAA Setup > AAA Server Groups** (Конфигурация > VPN для удаленного доступа > Настройка AAA > Группы серверов AAA).

Рядом со списком AAA Server Groups (Группы серверов AAA) выберите **Add** (Добавить).

В появившемся окне определите имя новой группы серверов AAA и в качестве протокола выберите **RADIUS**. По окончании нажмите **OK**.

Убедитесь, что новая группа выбрана в верхней области, и нажмите кнопку **Add** (Добавить) справа от нижней области.

Укажите сведения о сервере.

**Interface Name** (Имя интерфейса) — интерфейс, который устройство ASA должно использовать для обращения к серверу ACS.

**Server Name or IP address** (Имя или IP-адрес сервера) — адрес, который устройство ASA должно использовать для обращения к серверу ACS.

**Server Secret Key** (Секретный ключ сервера) — общий секретный ключ, настроенный для устройства ASA на сервере ACS.

### Пример конфигурации сервера AAA на устройстве ASA

После настройки группы серверов и сервера AAA перейдите в раздел Configuration (Конфигурация) > Remote Access VPN (VPN для удаленного доступа) > Clientless SSL VPN Access (Бесклиентский доступ по VPN на основе SSL) > Connection Profiles (Профили подключений), чтобы ввести в действие новую конфигурацию AAA.

**Примечание.** Несмотря на то, что в этом примере используется WebVPN, для использования этой конфигурации AAA возможно настроить любой профиль подключения удаленного доступа (группу туннелей).

Выберите профиль, для которого необходимо настроить AAA, и нажмите **Edit** (Изменить).

В разделе **Authentication** (Аутентификация) выберите группу серверов RADIUS, созданную ранее. По окончании нажмите **OK**.

## Интерфейс командной строки

Чтобы настроить устройство ASA для взаимодействия с сервером ACS и выполнения аутентификации клиентов WebVPN, выполните следующие шаги в интерфейсе командной строки.

```
ciscoasa#configure terminal

!--- Configure the AAA Server group. ciscoasa(config)# aaa-server RAD_SRV_GRP
protocol RADIUS ciscoasa(config-aaa-server-group)# exit !--- Configure the AAA
Server. ciscoasa(config)# aaa-server RAD_SRV_GRP (inside) host 192.168.1.2
ciscoasa(config-aaa-server-host)# key secretkey ciscoasa(config-aaa-server-host)#
exit !--- Configure the tunnel group to use the new AAA setup. ciscoasa(config)#
tunnel-group ExampleGroup1 general-attributes ciscoasa(config-tunnel-general)#
authentication-server-group RAD_SRV_GRP
```

## Проверка

Этот раздел служит для проверки работоспособности вашей конфигурации.

### Проверка в ASDM

Проверьте конфигурацию RADIUS кнопкой **Test** (Проверка) на экране настройки групп

серверов AAA. Эта кнопка позволяет после указания имени пользователя и пароля отправить проверочный запрос аутентификации на сервер ACS.

Выберите **Configuration > Remote Access VPN > AAA Setup > AAA Server Groups** (Конфигурация > VPN для удаленного доступа > Настройка AAA > Группы серверов AAA).

Выберите требуемую группу серверов AAA в верхней области.

В нижней области выберите сервер AAA, который необходимо проверить.

Справа от нее нажмите кнопку **Test** (Проверить).

В появившемся окне выберите переключатель **Authentication** (Аутентификация) и укажите реквизиты аутентификации, которые необходимо проверить. По окончании нажмите **OK**.

После того, как устройство ASA обратится к серверу AAA, появится сообщение об успешном выполнении операции или ошибке.

## [Проверка в интерфейсе командной строки](#)

Для проверки настроек AAA можно использовать команду **test** в интерфейсе командной строки. На сервер AAA направляется проверочный запрос, а результат появляется в командной строке.

```
ciscoasa#test aaa-server authentication RAD_SVR_GRP host 192.168.1.2 username kate
password cisco123
INFO: Attempting Authentication test to IP address <192.168.1.2> (timeout: 12
seconds)
INFO: Authentication Successful
```

## [Поиск и устранение неполадок](#)

Команда **debug radius** помогает диагностировать проблемы аутентификации в этом сценарии. Эта команда позволяет отлаживать сеансы RADIUS, а также декодировать пакеты RADIUS. В каждом из приведенных фрагментов выходных данных отладки первый декодированный пакет — это пакет, отправленный с устройства ASA на сервер ACS. Второй пакет представляет собой отклик от сервера ACS.

**Примечание.** Перед использованием команд **debug** ознакомьтесь с документом [Важные сведения о командах debug](#).

После успешного прохождения аутентификации сервер RADIUS отправляет сообщение **access-accept**.

```
ciscoasa#debug radius
```

```

!--- First Packet. Authentication Request. ciscoassa#radius mkreq: 0x88 alloc_rip
0xd5627ae4 new request 0x88 --> 52 (0xd5627ae4) got user '' got password add_req
0xd5627ae4 session 0x88 id 52 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode
(authentication request) ----- Raw packet data
(length = 62)..... 01 34 00 3e 18 71 56 d7 c4 ad e2 73 30 a9 2e cf | .4.>.qV....s0...
5c 65 3a eb 01 06 6b 61 74 65 02 12 0e c1 28 b7 | \e:...kate....(. 87 26 ed be 7b 2c
7a 06 7c a3 73 19 04 06 c0 a8 | .&..{,z.|.s..... 01 01 05 06 00 00 00 34 3d 06 00 00
00 05 | .....4=..... Parsed packet data..... Radius: Code = 1 (0x01) Radius:
Identifier = 52 (0x34) Radius: Length = 62 (0x003E) Radius: Vector:
187156D7C4ADE27330A92ECF5C653AEB Radius: Type = 1 (0x01) User-Name Radius: Length = 6
(0x06) Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-
Password Radius: Length = 18 (0x12) Radius: Value (String) = 0e c1 28 b7 87 26 ed be
7b 2c 7a 06 7c a3 73 19 | ..(&..{,z.|.s. Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06) Radius: Value (IP Address) = 192.168.1.1 (0xC0A80101)
Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6 (0x06) Radius: Value (Hex) = 0x34
Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6 (0x06) Radius: Value (Hex)
= 0x5 send_pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id 52 rad_vrfy() : response
message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer 0x0 : reqauth:
18 71 56 d7 c4 ad e2 73 30 a9 2e cf 5c 65 3a eb : info 0x88 session_id 0x88
request_id 0x34 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip
192.168.1.2 type 1 !--- Second Packet. Authentication Response. RADIUS packet decode
(response) ----- Raw packet data (length = 50).....
02 34 00 32 35 a1 88 2f 8a bf 2a 14 c5 31 78 59 | .4.25.../*..1xY 60 31 35 89 08 06
ff ff ff ff 19 18 43 41 43 53 | `15.....CACS 3a 30 2f 32 61 36 2f 63 30 61 38 30
31 30 31 2f | :0/2a6/c0a80101/ 35 32 | 52 Parsed packet data..... Radius: Code = 2
(0x02) Radius: Identifier = 52 (0x34) Radius: Length = 50 (0x0032) Radius: Vector:
35A1882F8ABF2A14C531785960313589 Radius: Type = 8 (0x08) Framed-IP-Address Radius:
Length = 6 (0x06) Radius: Value (IP Address) = 255.255.255.255 (0xFFFFFFFF) Radius:
Type = 25 (0x19) Class Radius: Length = 24 (0x18) Radius: Value (String) = 43 41 43
53 3a 30 2f 32 61 36 2f 63 30 61 38 30 | CACS:0/2a6/c0a80 31 30 31 2f 35 32 | 101/52
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0xd5627ae4 session 0x88 id 52
free_rip 0xd5627ae4
radius: send queue empty

```

В случае ошибки аутентификации сервер ACS отправляет сообщение **access-reject**.

```
ciscoasa#debug radius
```

```

!--- First Packet. Authentication Request. ciscoasa# radius mkreq: 0x85 alloc_rip
0xd5627ae4 new request 0x85 --> 49 (0xd5627ae4) got user '' got password add_req
0xd5627ae4 session 0x85 id 49 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode
(authentication request) ----- Raw packet data
(length = 62)..... 01 31 00 3e 88 21 46 07 34 5d d2 a3 a0 59 1e ff | .1.>.!F.4]...Y..
cc 15 2a 1b 01 06 6b 61 74 65 02 12 60 eb 05 32 | ..*...kate..`.2 87 69 78 a3 ce d3
80 d8 4b 0d c3 37 04 06 c0 a8 | .ix.....K..7.... 01 01 05 06 00 00 00 31 3d 06 00 00
00 05 | .....1=..... Parsed packet data..... Radius: Code = 1 (0x01) Radius:
Identifier = 49 (0x31) Radius: Length = 62 (0x003E) Radius: Vector:
88214607345DD2A3A0591EFFCC152A1B Radius: Type = 1 (0x01) User-Name Radius: Length = 6
(0x06) Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-
Password Radius: Length = 18 (0x12) Radius: Value (String) = 60 eb 05 32 87 69 78 a3

```

```

ce d3 80 d8 4b 0d c3 37 | `..2.ix.....K..7 Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06) Radius: Value (IP Address) = 192.168.1.1 (0xC0A80101)
Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6 (0x06) Radius: Value (Hex) = 0x31
Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6 (0x06) Radius: Value (Hex)
= 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id 49 rad_vrfy() : response
message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer 0x0 : reqauth:
88 21 46 07 34 5d d2 a3 a0 59 1e ff cc 15 2a 1b : info 0x85 session_id 0x85
request_id 0x31 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip
192.168.1.2 type 1 !--- Second packet. Authentication Response. RADIUS packet decode
(response) ----- Raw packet data (length = 32).....
03 31 00 20 70 98 50 af 39 cc b9 ba df a7 bd ff | .1. p.P.9..... 06 af fb 02 12 0c
52 65 6a 65 63 74 65 64 0a 0d | .....Rejected.. Parsed packet data..... Radius: Code
= 3 (0x03) Radius: Identifier = 49 (0x31) Radius: Length = 32 (0x0020) Radius:
Vector: 709850AF39CCB9BADFA7BDFF06AFFB02 Radius: Type = 18 (0x12) Reply-Message
Radius: Length = 12 (0x0C) Radius: Value (String) =
52 65 6a 65 63 74 65 64 0a 0d | Rejected..
rad_procpkt: REJECT
RADIUS_DELETE
remove_req 0xd5627ae4 session 0x85 id 49
free_rip 0xd5627ae4
radius: send queue empty

```

## [Дополнительные сведения](#)

- [Служба удаленной аутентификации пользователей коммутируемого доступа \(RADIUS\)](#)
- [Документы RFC](#)
- [Cisco Systems — техническая поддержка и документация](#)