

НАС (ССА): Настройка проверки подлинности Clean Access Manager (CAM) с помощью ACS

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Шаги для Настройки аутентификации на ССА с ACS](#)

[Конфигурация AcS](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как настроить аутентификацию на Clean Access Manager (CAM) с сервером Cisco Secure Access Control Server (ACS). Для подобной конфигурации с помощью ACS 5.x и позже, обратитесь к [НАС \(ССА\): Настройте Аутентификацию на Чистом Access Manager с ACS 5.x и Позже](#).

Предварительные условия

Требования

Эта конфигурация применима к версии 3.5 CAM и позже.

Используемые компоненты

Сведения в этом документе основываются на версии 4.1 CAM.

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.

Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

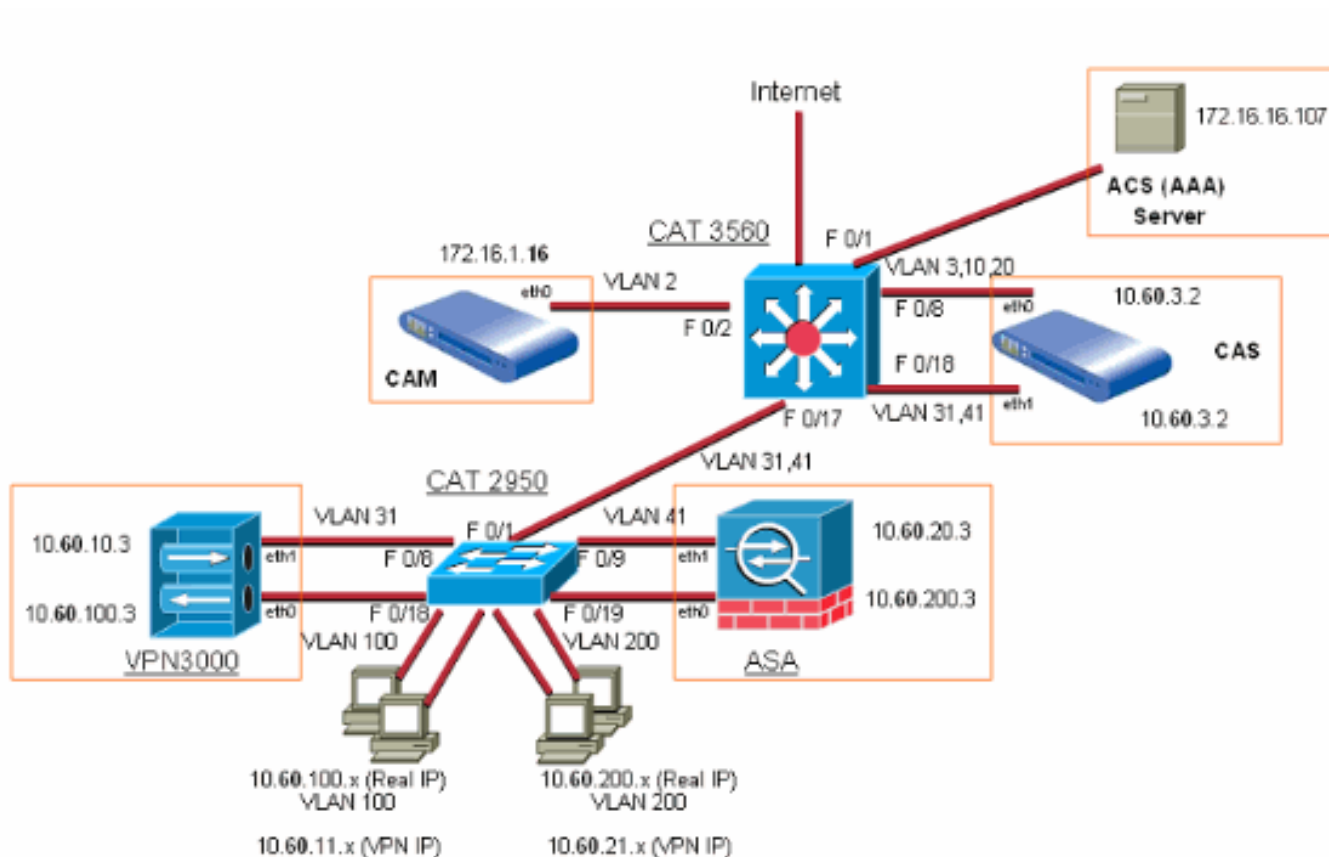
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Используйте инструмент Command Lookup \(только для зарегистрированных пользователей\)](#) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



Шаги для Настройки аутентификации на CCA с ACS

Выполните следующие действия:

1. **Добавьте новые роли** Создайте роль **AdminB** CAM выберите **User Management> User Roles> New Role**.

User Management > User Roles

List of Roles | **New Role** | Traffic Control | Bandwidth | Schedule

Disable this role

Role Name:

Role Description:

Role Type:

*VPN Policy:

*Dynamic IPsec Key: Enable Disable

*Max Sessions per User Account (Case-Insensitive): (1 - 255; 0 for unlimited)

Netag Trusted-side Egress Traffic with VLAN (In-Band): (0 - 4095, or leave it blank)

***Out-of-Band User Role VLAN:**

*After Successful Login Redirect to: previously requested URL
 this URL: (e.g. <http://www.cisco.com/>)

Redirect Blocked Requests to: default access blocked page
 this URL or HTML message:

*Roam Policy: Deny Allow

*Show Logged-on Users: IPsec info PPP info
 User info Logout button

B

введите уникальное имя, **admin**, для роли в поле Role Name. Введите **Роль пользователя Admin** как дополнительное Описание Роли. Выберите **Normal Login Role** в качестве типа роли. Настройте **Внеполосную (OOB) VLAN** роли пользователя с соответствующей VLAN. Например, выберите VLAN ID и задайте ID как 10. По окончании нажмите **Create Role**. Для восстановления свойств по умолчанию на форме нажмите **Reset**. Роль теперь появляется во вкладке List of Roles как показано в [VLAN Метки для Основанного на роли](#) раздела [сопоставлений OOB](#). **Создайте роль пользователя В CAM** выберите **User Management > User Roles > New Role**.

User Management > User Roles

List of Roles | **New Role** | Traffic Control | Bandwidth | Schedule

Disable this role

Role Name:

Role Description:

Role Type:

*VPN Policy:

*Dynamic IPsec Key: Enable Disable

*Max Sessions per User Account (Case-Insensitive): (1 - 255; 0 for unlimited)

Netag Trusted-side Egress Traffic with VLAN (In-Band): (0 - 4095, or leave it blank)

*Out-of-Band User Role VLAN:

*After Successful Login Redirect to: previously requested URL
 this URL: (e.g. <http://www.cisco.com/>)

Redirect Blocked Requests to: default access blocked page
 this URL or HTML message:

*Roam Policy: Deny Allow

*Show Logged-on Users: IPsec info PPP info
 User info Logout button

B

ведите уникальное имя, **пользователей**, для роли в поле Role Name. Введите **Роль Обычного пользователя** как дополнительное Описание Роли. Настройте **Внеполосную (OOB) VLAN** роли пользователя с соответствующей VLAN. Например, выберите VLAN ID и задайте ID как 20. По окончании нажмите **Create Role**. Для восстановления свойств по умолчанию на форме нажмите **Reset**. Роль теперь появляется во вкладке List of Roles как показано в [VLAN Метки для Основанного на роли](#) раздела [сопоставлений OOB](#).

2. **VLAN метки для Основанных на роли сопоставлений OOB** CAM выберите **User Management > User Roles > List of Roles** для наблюдения списка ролей до сих пор.

Role Name	IPsec	Roam	VLAN	Description	Policies	SW	Edit	Del
Unauthenticated Role	deny	deny		Role for unauthenticated users				
Temporary Role	deny	deny		Role for users to download requirements				
Quarantine Role	deny	deny		Role for quarantined users				
Allow_All	deny	deny						
admin	deny	deny	10	Admin User Role				
users	deny	deny	20	Normal User Role				

3. Добавьте сервер проверки подлинности RADIUS (ACS) Выберите User Management> Auth Servers> New.

User Management > Auth Servers

Auth Servers | Lookup Servers | Mapping Rules | Auth Test | Accounting

List · New

Authentication Type: Radius (dropdown) | Provider Name: ACS (text)

Server Name: auth.cisco.com (text) * | Server Port: 1812 (text) *

Radius Type: PAP (dropdown) | Timeout (sec): 5 (text) *

Default Role: Allow_All (dropdown) | Shared Secret: ***** (text) *
NOT SET

NAS-Identifier: (text) | NAS-IP-Address: 172.16.1.61 (text)

(Either a NAS-Identifier or NAS-IP-Address must be specified)

NAS-Port: (text) | NAS-Port-Type: (text)

Enable Failover | Failover Peer IP: (text)

Accept RADIUS packets with empty attributes from some old RADIUS servers

(* Asterisks indicate required fields.)

Description: (text)

Add Server | Cancel

От раскрывающегося меню Типа проверки подлинности выберите **Radius**. Введите имя поставщика как **ACS**. Введите Имя сервера как **аутентификация. cisco . com**. Порт сервера — номер порта **1812**, на котором слушает сервер RADIUS. **RADIUS Type. Метод аутентификации RADIUS.** Поддерживаемые методы включают EAPMD5, PAP, CHAP, MSCHAP и MSCHAP2. **Роль по умолчанию** используется, если сопоставление с ACS не определено или установлено правильно, или если атрибут RADIUS не определен или установлен правильно на ACS. **Общий секретный ключ** — общий секретный ключ RADIUS, связанный с IP-адресом указанного клиента. **Nas-ip-address** — Это значение, которое будет передаваться со всеми пакетами Проверки подлинности RADIUS. **Нажмите Add сервер.**

Provider Name	Authentication Type	Description	Mapping	Edit	Delete
Local DB	local	Cisco local authentication			
ACS	radius	RADIUS Authentication			
Cisco VPN	vpn	Remote VPN Support			

4. Сопоставьте пользователей ACS с ролями пользователя ССА Выберите **User Management > Auth Servers > Mapping Rules > Add Mapping Link** для сопоставления пользователя с правами администратора в ACS к роли пользователя с правами администратора ССА.

User Management -> Auth Servers

List of Servers | New Server | **Mapping Rules** | Auth Test | Accounting

Provider Name: ACS | Priority: 1

Role Name: **admin** | Description:

Role Expression: (0,25,2 equals Admin)

Save Mapping

Condition Type: Attribute | Operator: equals

Vendor: Standard | Attribute Name: Class | Attribute Value: Admin

Data Type: String

Save Condition | Cancel

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,25,2	equals	Admin		

- Выберите **User Management > Auth Servers > Mapping Rules > Add Mapping Link** для сопоставления обычного пользователя в ACS к роли пользователя ССА.

User Management -> Auth Servers

List of Servers | New Server | **Mapping Rules** | Auth Test | Accounting

Provider Name: ACS | Priority: 2

Role Name: **users** | Description:

Role Expression: (-0,25,2 equals users)

Save Mapping

Condition Type: Attribute | Operator: equals

Vendor: Standard | Attribute Name: Class | Attribute Value: Users

Data Type: String

Save Condition | Cancel

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,25,2	equals	Users		

Вот сводка сопоставления роли пользователя:

ACS	Role	Expression	edit	delete	Priority
	admin	(0,25,2 equals Admin)			
	users	(0,25,2 equals Users)			

[Add Mapping Rule](#)

5. Включите альтернативным поставщикам на странице пользователя Выберите **Administration > User Pages > Login Page > Add > Content**, чтобы включить альтернативным поставщикам на странице регистрационной информации пользователя для входа.

Administration > User Pages

Login Page | File Upload

List · Add · Edit

General | **Content** | Style

Image: Title:

Username Label Password Label

Login Label Provider Label

Default Provider: Available Providers: Local DB ACS

Instructions:

Guest Label Root CA Label

Help Label Root CA File:

Help Contents:

Конфигурация AcS

1. Выберите **Interface Configuration**, чтобы удостовериться, что включен RADIUS (IETF) Атрибут Class

Interface Configuration

RADIUS (IETF)

User	Group
<input type="checkbox"/>	<input checked="" type="checkbox"/> [006] Service-Type
<input type="checkbox"/>	<input checked="" type="checkbox"/> [007] Framed-Protocol
<input type="checkbox"/>	<input checked="" type="checkbox"/> [009] Framed-IP-Netmask
<input type="checkbox"/>	<input checked="" type="checkbox"/> [010] Framed-Routing
	⋮
<input type="checkbox"/>	<input checked="" type="checkbox"/> [024] State
<input type="checkbox"/>	<input checked="" type="checkbox"/> [025] Class
<input type="checkbox"/>	<input checked="" type="checkbox"/> [027] Session-Timeout
<input type="checkbox"/>	<input checked="" type="checkbox"/> [028] Idle-Timeout

[025].

2. Добавьте КЛИЕНТА RADIUS к серверу ACS Выберите Network Configuration для добавления SAM клиента AAA как

Network Configuration

Edit

AAA Client Setup For CAM

AAA Client IP Address	<input type="text" value="172.16.1.16"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (IETF)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	
<input type="button" value="Submit"/> <input type="button" value="Submit + Restart"/> <input type="button" value="Delete"/> <input type="button" value="Delete + Restart"/> <input type="button" value="Cancel"/>	

показано:

Нажмите Submit + Restart.Примечание: Удостоверьтесь, что ключ RADIUS совпадает с клиентом AAA и RADIUS использования (IETF).Выберите **Network Configuration** для добавления CAS клиента AAA как

Network Configuration

Edit

AAA Client Setup For CAS

AAA Client IP Address	10.60.3.2
Key	cisco123
Authenticate Using	RADIUS (IETF)
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

показано:

Нажмите Submit + Restart.Примечание: Для учета RADIUS Шлюза VPN политика CCA должна позволить пакетам учета RADIUS (UDP 1646/1813) от IP-адреса CAS проходить не прошедший проверку подлинности к IP-адресу сервера ACS.Выберите **Network Configuration** для добавления ASA клиента AAA как

Network Configuration

Edit

AAA Client Setup For CCA_Lab_pix515

AAA Client IP Address	<input type="text" value="10.60.20.3"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco IOS/PIX)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	
<input type="button" value="Submit"/> <input type="button" value="Submit + Restart"/> <input type="button" value="Delete"/> <input type="button" value="Delete + Restart"/> <input type="button" value="Cancel"/>	

показано:

пользовательский PIX/ASA почти стороны взаимодействует адрес (как правило, внутренний интерфейс) Тип набора к RADIUS (Cisco IOS / PIX).

По

3. Добавьте, что / Настраивают Группы на Сервере ACS Создайте Административную

Group Settings : Admin

⋮

IETF RADIUS Attributes ?

[006] Service-Type Login

[007] Framed-Protocol PPP

[009] Framed-IP-Netmask 0.0.0.0

[010] Framed-Routing None

⋮

[025] Class Admin

группу

ставьте Атрибут Class РАДИУСА IETF [025] адаптировать групповое значение. Значение должно совпасть, который настроил на сопоставлении CAS. **Создайте Группу пользователей**

3а

Group Settings : Users



IETF RADIUS Attributes	
<input type="checkbox"/> [006] Service-Type	Login
<input type="checkbox"/> [007] Framed-Protocol	PPP
<input type="checkbox"/> [009] Framed-IP-Netmask	0.0.0.0
<input type="checkbox"/> [010] Framed-Routing	None
⋮	
<input checked="" type="checkbox"/> [025] Class	Users

Добавьт

е/настройте группу для каждой Чистой Роли Пользователя доступа, которая будет сопоставлена. **Добавьте/Настройте Пользователей на Сервере**

User Setup

Edit

User: chyps

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

ACS

Доба

вьте/настройте пользователя ACS для каждого Чистого Пользователя доступа, чтобы аутентифицироваться ACS. Состав группы ACS набора ACS также поддерживает проверку подлинности прокси-сервера к другим внешним серверам.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

В разделе мониторинга ACS вы видите информацию о переданных аутентификациях как показано:

Passed Authentications active.csv

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Application-Posture-Token	System-Posture-Token	Reason
08/02/2005	13:15:39	Authen OK	jsmith	Users	10.60.100.201	1039	10.60.10.3			

CAM (AAA client) IP address

Remote Authenticated User IP address

(address as seen by CAS—assigned by VPN gateway)

Точно так же вы видите снимок экрана для учета RADIUS:

RADIUS Accounting active.csv

Date ↓	Time	User-Name	Group-Name	Calling-Station-Id	Acct-Status-Type	Acct-Session-Id	Acct-Session-Time	Service-Type	Framed-Protocol	Acct-Input-Octets	Acct-Output-Octets	Acct-Input-Packets	Acct-Output-Packets	Framed-IP-Address	NAS-Port	NAS-IP-Address
08/02/2005	15:26:49	jsmith	Users	10.60.100.201	Stop	B2C00017	7869	Framed	PPP	350872	8528952	5993	8207	10.60.11.1	1039	10.60.10.3
08/02/2005	13:15:40	jsmith	Users	10.60.100.201	Start	B2C00017		Framed	PPP					10.60.11.1	1039	10.60.10.3

Real IP address of Remote Authenticated User

CAM (AAA client) IP address

Remote Authenticated User IP address

(address as seen by CAS—assigned by VPN gateway)

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- [Страница технической поддержки устройства Cisco NAC](#)
- [Cisco Systems – техническая поддержка и документация](#)