



# Deploying Cisco ASA Management Plane Security Controls

Network Infrastructure Protection Deployment

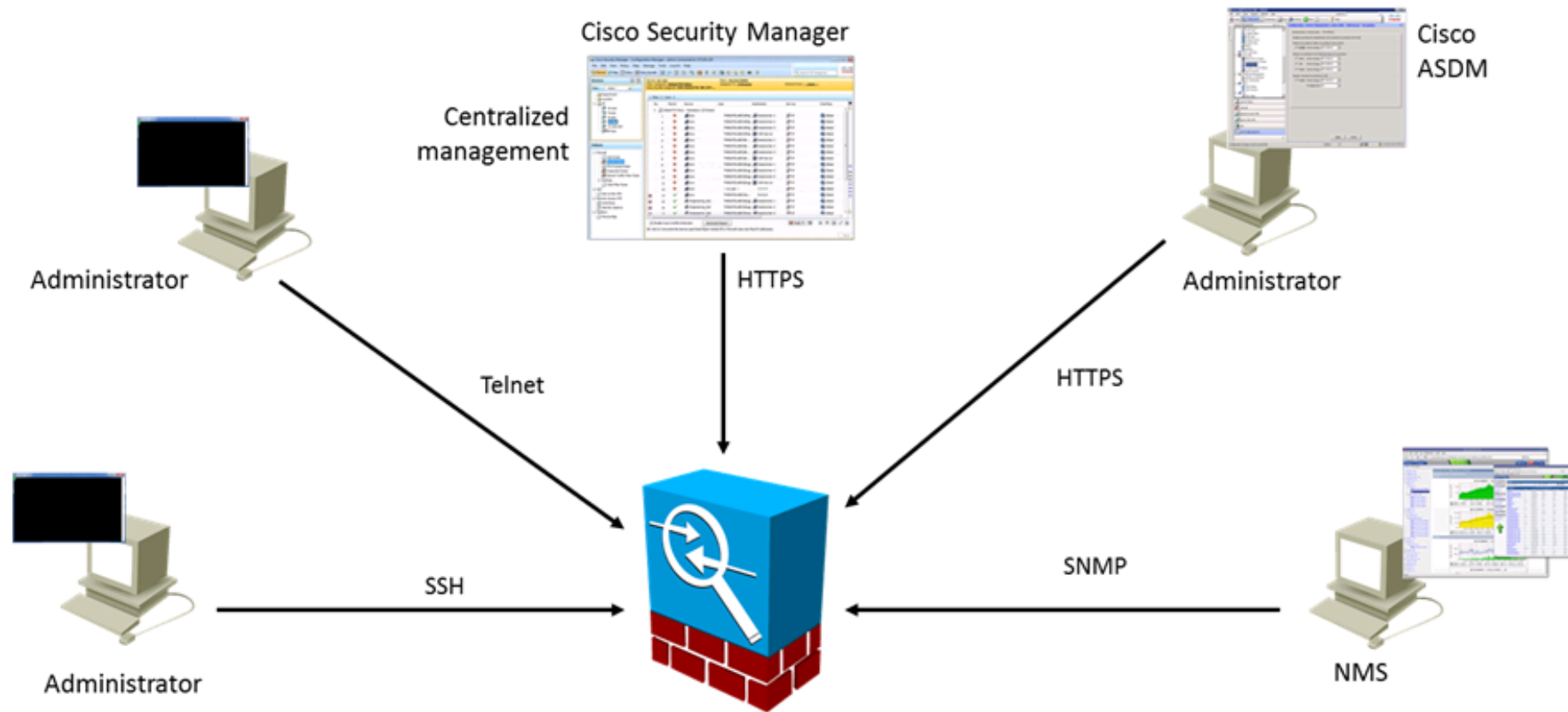
Ahmed Sultan  
Senior Network Security Engineer  
[ahmedsultan.me/about](http://ahmedsultan.me/about)

# Overview of Cisco ASA Management Plane Security Controls

Threat	Management Plane Countermeasure
Managment session spoofing	<p>Secure management access</p> <ul style="list-style-type: none"><li>• Out-of-band management path</li><li>• Use of cryptographically protected management protocols (SSH, HTTPS, SNMPv3)</li><li>• Use of cryptographic protection for management session</li><li>• Filtering of management access</li></ul>
Abuse of available management features	<p>Management access AAA</p> <ul style="list-style-type: none"><li>• Management access authentication</li><li>• Management access authorization/RBAC</li></ul>

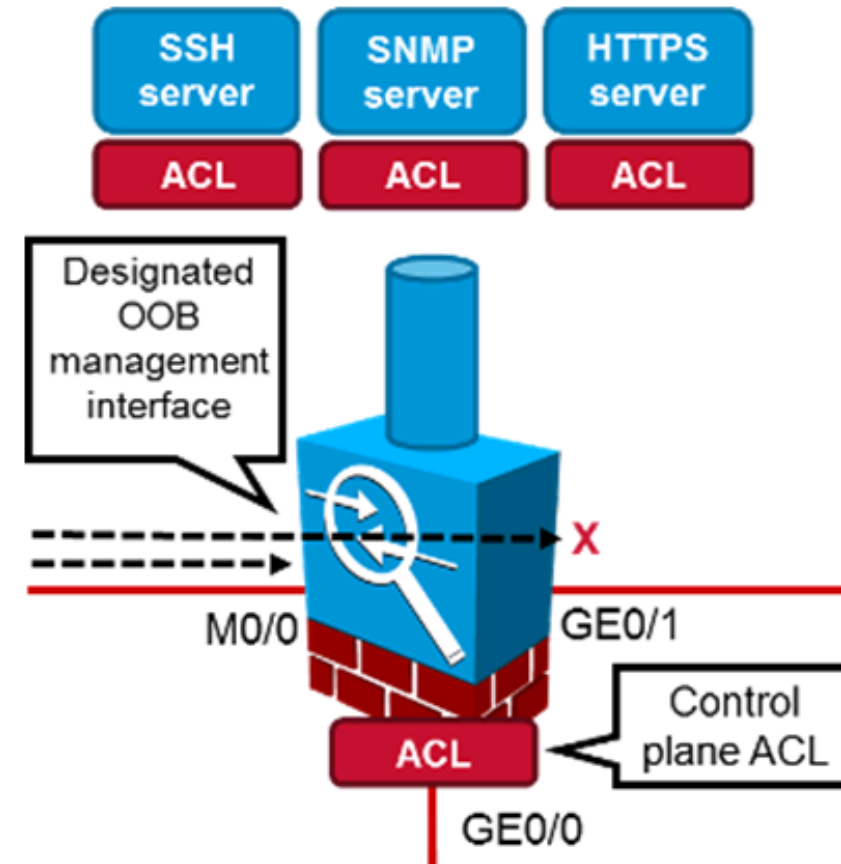
# Overview of Cisco ASA Management Plane Security Controls (Cont.)

## Remote Management Access Options



# Overview of Cisco ASA Secure Management Access

- The ASA allows management access only to the closest interface
- The ASA supports the following mechanisms to secure management access
  - OOB management interface
  - Secure management protocols (HTTPS, SSL, SNMPv3)
- The ASA does not allow management access unless specifically allowed using management rules
- The ASA also supports additional filtering of management access using control plane ACLs



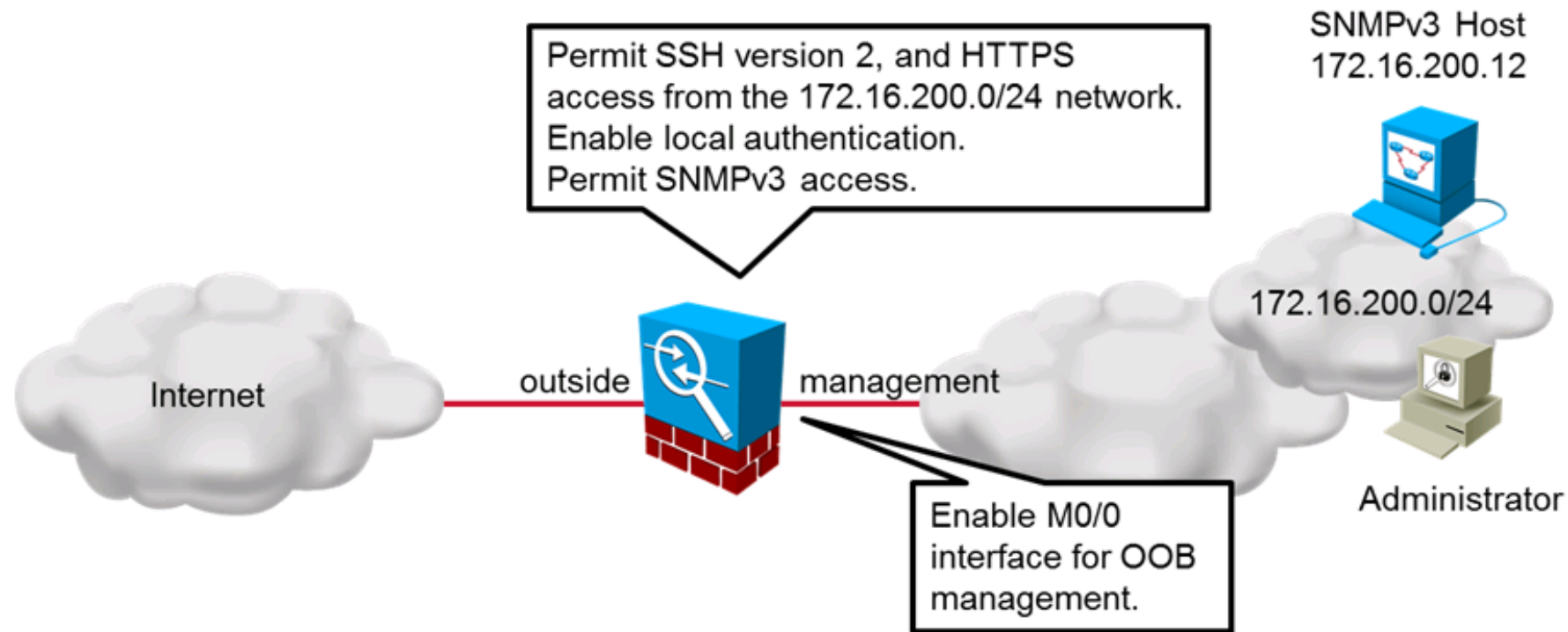
# Configure Cisco ASA Secure Management Access

To configure Cisco ASA secure management access, complete these tasks:

1. Configure OOB management interface
2. Enable HTTPS access
3. Enable SSH access
4. Create a user in the local user database
5. Enable local authentication for SSH and HTTPS
6. Enable SNMPv3 and configure credentials

# Configure Cisco ASA Secure Management Access (Cont.)

## Configuration Scenario



# Configure Cisco ASA Secure Management Access (Cont.)

Task 1: Configure OOB management interface

Task 2: Enable HTTPS access

```
interface Management0/0
 nameif management
 security-level 90
 ip address 10.10.2.1 255.255.255.0
 no shutdown
!
http server enable
http 172.16.200.0 255.255.255.0 management
```



# Configure Cisco ASA Secure Management Access (Cont.)

## Task 3: Enable SSH access

- **Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**

Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

Type	Interface
ASDM/HTTPS	management

**Add Device Access Configuration**

Access Type: ☐ ASDM/HTTPS ☐ Telnet ☒ SSH

Interface Name: management

IP Address: 172.16.200.0

Mask: 255.255.255.0

OK Cancel Help

Http Settings

☒ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

Allowed SSH Version(s): 2

SSH Timeout: 5 minutes

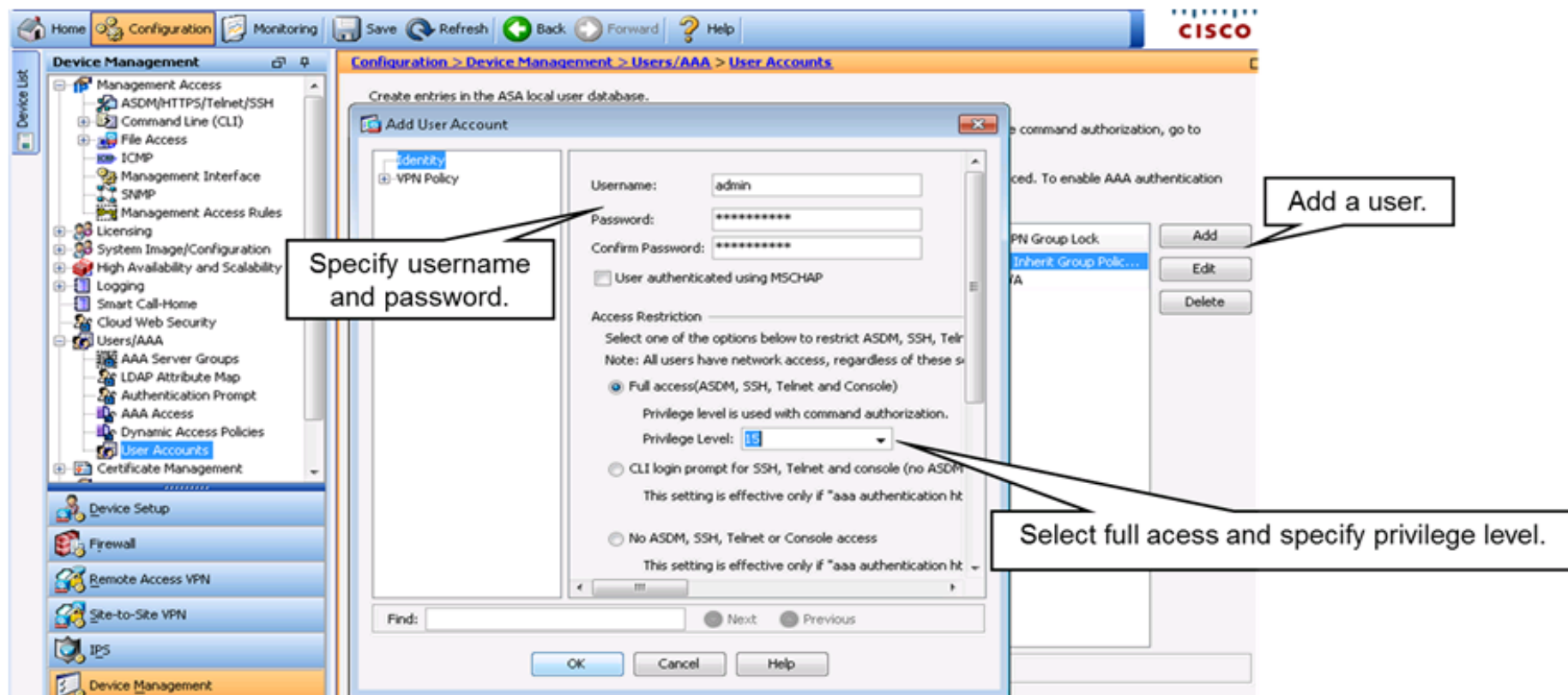
© Egypt NetRiders | www.egyptnetriders.com



# Configure Cisco ASA Secure Management Access (Cont.)

Task 4: Create a user in the local user database

- **Configuration > Device Management > Users/AAA > User Accounts**



# Configure Cisco ASA Secure Management Access (Cont.)

## Task 5: Enable local authentication for SSH and HTTPS

- **Configuration > Device Management > Users/AAA > AAA Access > Authentication**

The screenshot displays the Cisco ASA configuration web interface. The breadcrumb navigation at the top indicates the current path: **Configuration > Device Management > Users/AAA > AAA Access > Authentication**. The left sidebar shows the 'Device List' with 'Users/AAA' expanded, and 'AAA Access' selected. The main content area has three tabs: 'Authentication', 'Authorization', and 'Accounting'. The 'Authentication' tab is active, showing options to enable authentication for administrator access and for specific connection types. Under 'Require authentication for the following types of connections', the 'SSH' checkbox is checked, and its 'Server Group' is set to 'LOCAL'. A callout box points to the 'SSH' checkbox with the text: "Enable local authentication for required management access."

© Egypt NetRiders | www.egyptnetriders.com

# Configure Cisco ASA Secure Management Access (Cont.)

## Task 6: Enable SNMPv3 and configure credentials

- **Configuration > Device Management > Management Access > SNMP**

Configuration > Device Management > Management Access > SNMP

Configure SNMP parameters and management stations.

**Add SNMP User Entry**

Group Name: Authentication&Encryption

Username: admin

Password Type: ☐ Encrypted ☒ Clear Text

Authentication Algorithm: ☐ MD5 ☒ SHA

Authentication Password: .....

Retype Authentication Password: ..... (Only required for clear text password)

Encryption Algorithm: ☐ DES ☐ 3DES ☒ AES

Encryption Password: .....

Retype Encryption Password: ..... (Only required for clear text password)

AES Size: 256

OK Cancel Help

© Egypt NetRiders | www.egyptnetriders.com

UDP Port Add Edit Delete

AES Size Add Edit Delete

© 2014 Cisco Systems, Inc.

# Configure Cisco ASA Secure Management Access (Cont.)

## Task 6: Enable SNMPv3 and configure credentials (cont.)

- **Configuration > Device Management > Management Access > SNMP**

Configuration > Device Management > Management Access > SNMP

Configure SNMP parameters and management stations.

Community String (default):  (optional)

Contact:  Administrator

ASA Location:

Listening Port:

SNMP Host Access

Interface	IP Address	UDP Port	SNMP Version	Username	Poll	Trap
management	172.16.200.12	162	3	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Interface Name:  management

IP Address:  172.16.200.12

UDP Port:  162

SNMP Version:  3

Username:  admin

Server Poll/Trap Specification

Select a specified function of the SNMP Host.

☒ Poll

☒ Trap

OK Cancel Help

Version Poll/Trap UDP Port

Add Edit Delete

according to the group to which they belong.

Group Name	Encryption Algorithm	AES Size
admin	AES	256

Add Edit Delete

Toggle SNMP poll and trap functionalities.

Select interface and specify SNMP NMS IP address.

Add SNMP host entry.

Select SNMP version and select user in case of SNMPv3.



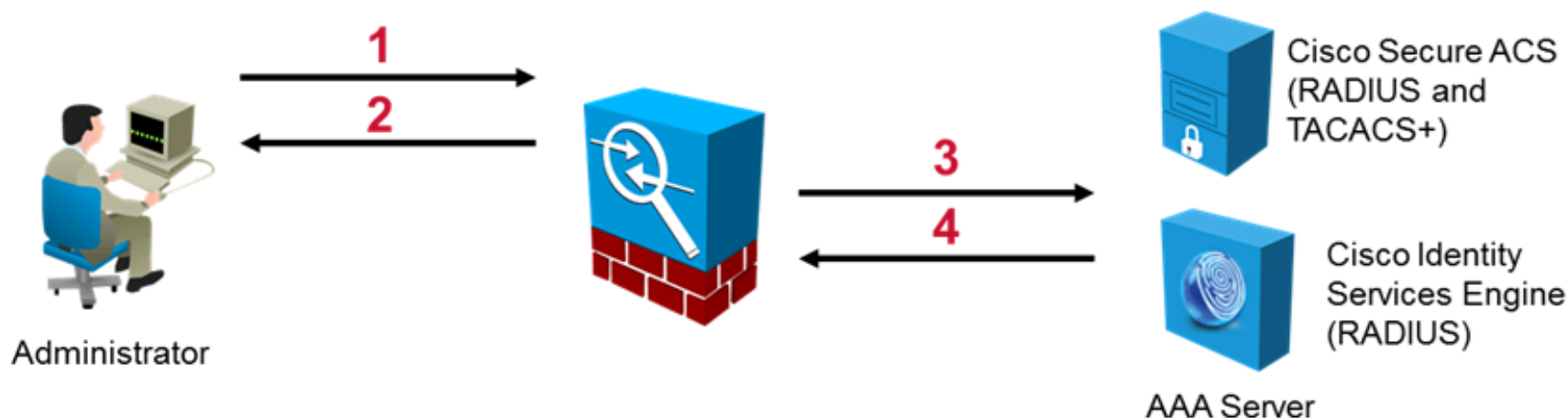
# Configure Cisco ASA Secure Management Access (Cont.)

## CLI Configuration

```
ssh 172.16.200.0 255.255.255.0 inside
ssh timeout 5
ssh version 2
!
username admin password Ci5coAdmin privilege 15
!
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
!
snmp-server group Authentication&Encryption v3 priv
snmp-server user admin Authentication&Encryption v3 auth SHA Ci5coAdminAuth
priv AES 256 Ci5coAdminPriv
snmp-server host management 172.16.200.12 version 3 admin
```

# Overview of Cisco ASA Management Access AAA

- Administrator access AAA specifies who can access the ASA, what a user can perform on the ASA, and what user did on the ASA.
- You can perform the AAA authentication and authorization process using these database options:
  - Local database on a device
  - External AAA server



# Configure Cisco ASA Management Access AAA

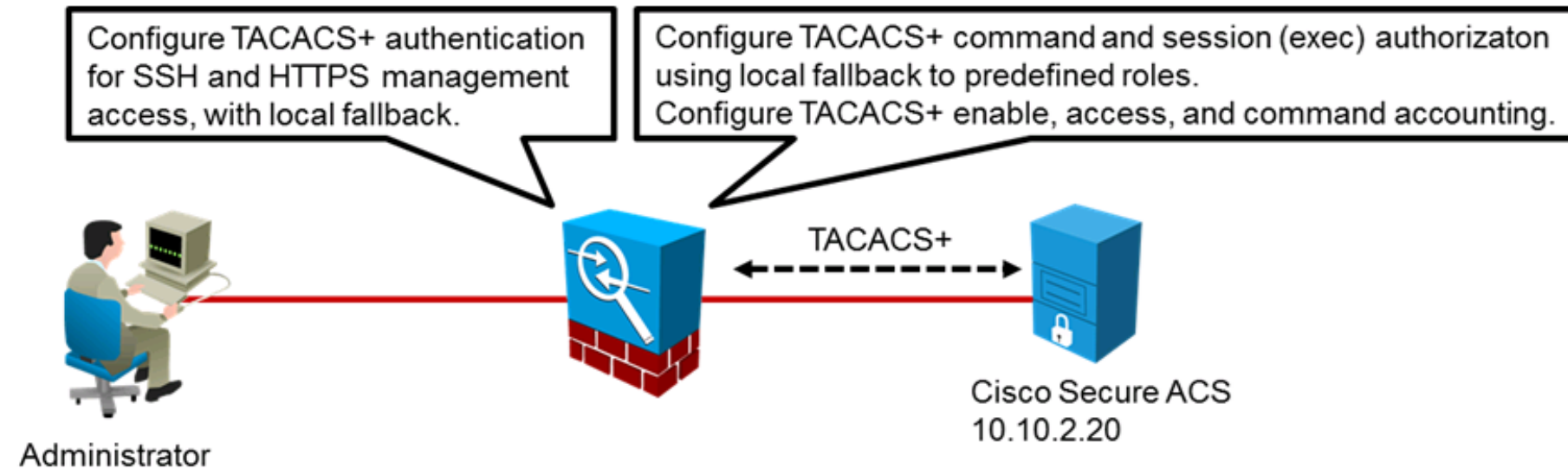
To configure Cisco ASA management access AAA, complete these tasks:

1. Configure external AAA servers
2. Create local user accounts with required privilege levels
3. Configure external authentication for management access
4. Configure external TACACS+ command and/or exec authorization, or change privilege level of command to implement local command authorization.
5. Configure enable and access event and command accounting for management access



# Configure Cisco ASA Management Access AAA (Cont.)

## Configuration Scenario



# Configure Cisco ASA Management Access AAA (Cont.)

## Task 1: Configure external AAA servers

- **Configuration > Device Management > Users/AAA > AAA Server Groups**

The screenshot displays the Cisco ASA Management Access configuration interface. The left sidebar shows the navigation tree with 'Users/AAA' expanded and 'AAA Server Groups' selected. The main content area shows the 'AAA Server Groups' configuration page with a table listing existing groups (LOCAL). An 'Add AAA Server Group' dialog box is open in the foreground, prompting for the following information:

- AAA Server Group: MY-TACACS
- Protocol: TACACS+ (selected from a dropdown)
- Accounting Mode: ☐ Simultaneous ☒ Single
- Reactivation Mode: ☒ Depletion ☐ Timed
- Dead Time: 10 minutes
- Max Failed Attempts: 3

Buttons at the bottom of the dialog are OK, Cancel, and Help. Callout boxes provide instructions: 'Add a server group.' points to the 'Add' button in the background; 'Assign a name to the server group.' points to the 'AAA Server Group' text field; and 'Choose an authentication protocol.' points to the 'Protocol' dropdown.

# Configure Cisco ASA Management Access AAA (Cont.)

## Task 1: Configure external AAA servers (cont.)

- **Configuration > Device Management > Users/AAA > AAA Server Groups**

The screenshot shows the Cisco ASA Configuration Assistant interface. The left pane displays the 'Device Management' tree with 'Users/AAA' expanded. The right pane shows the 'AAA Server Groups' configuration page. A table lists the server groups:

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
MY-TACACS	TACACS+	Single	Depletion	10	3

An 'Add AAA Server' dialog box is open, showing the configuration for the 'MY-TACACS' group. The fields are:

- Server Group: MY-TACACS
- Interface Name: inside (dropdown menu)
- Server Name or IP Address: 10.10.2.20
- Timeout: 10 seconds
- TACACS+ Parameters: Server Port: 49, Server Secret Key: [masked]

Callouts provide instructions for the fields:

- 'Specify the server location.' points to the Interface Name dropdown.
- 'With multiple servers, specify a timeout.' points to the Timeout field.
- 'Specify the server session key.' points to the Server Secret Key field.
- 'Add servers to the selected server group.' points to the Add button.

# Configure Cisco ASA Management Access AAA (Cont.)

Task 2: Create local user accounts with required privilege levels

- **Configuration > Device Management > Users/AAA > AAA Server Groups**

Configuration > Device Management > Users/AAA > User Accounts

Create entries in the ASA local user database.

**Add User Account**

**Identity**

Username: admin

Password: [masked]

Confirm Password: [masked]

☐ User authenticated using MSCHAP

**Access Restriction**

Select one of the options below to restrict ASDM, SSH, Telnet, and Console access. Note: All users have network access, regardless of these settings.

☒ Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 15

☐ CLI login prompt for SSH, Telnet and console (no ASDM)

This setting is effective only if "aaa authentication http" is configured.

☐ No ASDM, SSH, Telnet or Console access

This setting is effective only if "aaa authentication http" is configured.

Find: [text box] [Next] [Previous]

OK Cancel Help

© 2014 Cisco Systems, Inc.



# Configure Cisco ASA Management Access AAA (Cont.)

Task 3: Configure external authentication for management access

- **Configuration > Device Management > Users/AAA > AAA Access > Authentication**

The screenshot displays the Cisco ASA Configuration Assistant interface. The left pane shows the 'Device List' with a tree view where 'AAA Access' is selected under 'Users/AAA'. The main pane shows the 'Authentication' configuration page for 'AAA Access'. The breadcrumb path at the top is 'Configuration > Device Management > Users/AAA > AAA Access > Authentication'. The 'Authentication' tab is active, showing options to enable authentication for administrator access and for specific connection types. A callout box points to the 'Require authentication for the following types of connections' section, stating 'Optionally, configure fallback.' Another callout box points to the 'HTTP/ASDM' and 'SSH' entries, stating 'Enable required access methods for authentication.'

Configuration > Device Management > Users/AAA > AAA Access > Authentication

Authentication Authorization Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

☐ Enable Server Group: LOCAL ☐ Use LOCAL when server group fails

Require authentication for the following types of connections

☒ HTTP/ASDM Server Group: MY-TACACS ☒ Use LOCAL when server group fails

☐ Serial Server Group: LOCAL ☐ Use LOCAL when server group fails

☒ SSH Server Group: MY-TACACS ☒ Use LOCAL when server group fails

☐ Telnet Server Group: LOCAL ☐ Use LOCAL when server group fails

Optionally, configure fallback.

Enable required access methods for authentication.

# Configure Cisco ASA Management Access AAA (Cont.)

Task 4: Configure external TACACS+ command and/or exec authorization

- **Configuration > Device Management > Users/AAA > AAA Access > Authorization**

The screenshot shows the Cisco ASDM (Adaptive Security Desktop Manager) interface. The left sidebar contains a tree view of configuration options, including 'System Image/Configuration', 'High Availability and Scalability', 'Logging', 'Smart Call-Home', 'Cloud Web Security', 'Users/AAA', 'AAA Server Groups', 'LDAP Attribute Map', 'Authentication Prompt', 'Dynamic Access Policies', 'User Accounts', and 'Certificate Management'. The main configuration area is titled 'Configuration > Device Management > Users/AAA > AAA Access > Authorization'. It contains several sections: 'Authentication', 'Authorization', and 'Access'. The 'Authorization' section is currently selected and shows options to 'Enable authorization for ASA commands' and 'Perform authorization for exec shell access'. The 'Enable authorization for ASA commands' section has a checkbox for 'Enable' (checked), a dropdown for 'Server Group' (set to 'MY-TACACS'), and a checkbox for 'Use LOCAL when server group fails' (checked). Below this are buttons for 'Set ASDM Defined User Roles...' and 'Configure Command Privileges...'. The 'Perform authorization for exec shell access' section has a checkbox for 'Enable' (checked), radio buttons for 'Remote server' (selected) and 'Local server', and a text box for 'When enabled, authorization will be performed for all commands configured for authentication to RADIUS server'. A callout box points to the 'Set ASDM Defined User Roles...' button, stating: 'Automatically sets up level-based roles (Admin, Read Only, Monitor)'. Another callout box points to the 'Enable' checkbox in the 'Perform authorization for exec shell access' section, stating: 'Enable remote exec authorization.'. A third callout box points to the 'Configure Command Privileges...' button, stating: 'Alternatively, customize the privilege level for each command.'. A fourth callout box points to the 'Enable' checkbox in the 'Enable authorization for ASA commands' section, stating: 'Enable remote command authorization with local backup.'. The 'Set ASDM Defined User Roles' dialog box is open, showing a message: 'Do you want ASDM to setup user profiles named "Admin", "Read Only" and "Monitor Only"? If you click Yes, ASDM will setup the following commands with the respective privilege levels. This setup will enable you to create users through the User Accounts screen with roles Admin, Read Only and Monitor Only with privilege levels 15, 5 and 3 respectively. Click No, if you wish to manage privilege levels of commands and users manually.' Below the message is a 'Command List' table with columns 'CLI Command', 'Mode', 'Variant', and 'Privilege'. The table contains the following data:

CLI Command	Mode	Variant	Privilege
aaa	confi...	show	3
aaa	exec	show	3
aaa-server	confi...	clear	3
aaa-server	confi...	show	3
aaa-server	exec	clear	3
aaa-server	exec	show	3
access-list	confi...	show	3

At the bottom of the dialog box are buttons for 'Yes', 'No', and 'Help'.

# Configure Cisco ASA Management Access AAA (Cont.)

Task 5: Configure enable and access event and command accounting

- **Configuration > Device Management > Users/AAA > AAA Access > Accounting**

Configuration > Device Management > Users/AAA > AAA Access > Accounting

Authentication Authorization Accounting

Enable accounting for administrator and command accounting to the ASA.

Require accounting to allow accounting of user activity

☒ Enable Server Group: MY-TACACS

Require accounting for the following types of connections

☐ Serial Server Group: MY-TACACS

☒ SSH Server Group: MY-TACACS

☐ Telnet Server Group: MY-TACACS

Require command accounting for ASA

☒ Enable Server Group: MY-TACACS

Privilege level: 0

Configure enable event accounting.

Configure login event accounting.

Configure command accounting.



# Configure Cisco ASA Secure Management Access (Cont.)

## CLI Configuration

```
aaa-server MY-TACACS protocol tacacs+
aaa-server MY-TACACS (inside) host 10.10.2.20
  key *****
!
username admin password Ci5coAdmin privilege 15
username monitor password Ci5coAdmin privilege 3
!
aaa authentication http console MY-TACACS LOCAL
aaa authentication ssh console MY-TACACS LOCAL
!
aaa authorization command MY-TACACS LOCAL
aaa authorization exec authentication-server
!
privilege show level 3 mode configure command aaa
privilege show level 3 mode exec command aaa
privilege clear level 3 mode configure command aaa-server
<output omitted>
!
aaa accounting enable console MY-TACACS
aaa accounting ssh console MY-TACACS
aaa accounting command MY-TACACS
```

# Verify Cisco ASA Management Access AAA

Verification Commands	Description
<b>show aaa-server</b>	Displays AAA server statistics for AAA servers.
<b>test aaa-server</b>	Verifies connectivity from the ASA to the AAA server.

# Verify Cisco ASA Management Access AAA (Cont.)

```
ASA# show aaa-server
```

```
Server Group:      MY-TACACS
Server Protocol:   tacacs+
Server Address:    172.16.1.17
Server port:       49
Server status:     ACTIVE, Last transaction at 08:24:27 UTC Thu Apr 15 2010
Number of pending requests          0
Average round trip time             36ms
Number of authentication requests    10
Number of authorization requests     0
Number of accounting requests       0
Number of retransmissions            0
Number of accepts                   5
Number of rejects                   4
Number of challenges                 0
Number of malformed responses        0
Number of bad authenticators         0
Number of timeouts                  1
Number of unrecognized responses     0
```

# Verify Cisco ASA Management Access AAA (Cont.)

```
ASA# test aaa-server authentication MY-TACACS username admin password  
Ci5coAdmin  
Server IP Address or name: 10.10.2.20  
INFO: Attempting Authentication test to IP address < 10.10.2.20 > (timeout:  
12 seconds)  
INFO: Authentication Successful
```

# Summary

- Cisco ASA supports many remote management access methods.
- Cisco ASA does not allow management access by default and has to be enabled using management rules.
- To enable secure management access to the Cisco ASA, use the OOB management interface or use secure management protocols.
- Cisco ASA management access AAA can be performed against local user database or against external AAA server.
- Cisco ASA remote command authorization and accounting can be configured only with the TACACS+ server.