Deploying Cisco ASA Management Plane Security Controls

Network Infrastructure Protection Deployment

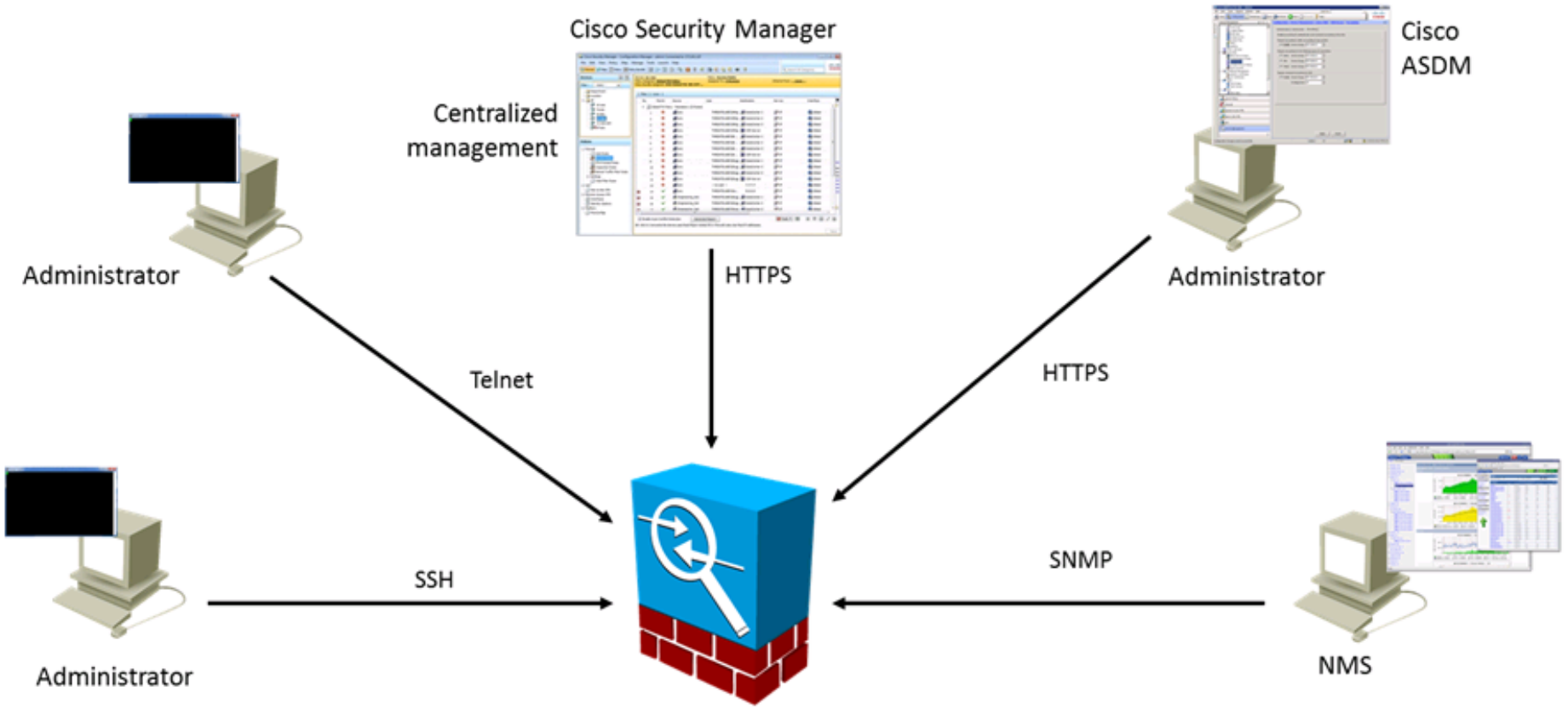
Ahmed Sultan
Senior Network Security Engineer
ahmedsultan.me/about

Overview of Cisco ASA Management Plane Security Controls

Threat	Management Plane Countermeasure
Managment session spoofing	Secure management access • Out-of-band management path • Use of cryptographically protected management protocols (SSH, HTTPS, SNMPv3) • Use of cryptographic protection for management session • Filtering of management access
Abuse of available management features	Management access AAA • Management access authentication • Management access authorization/RBAC

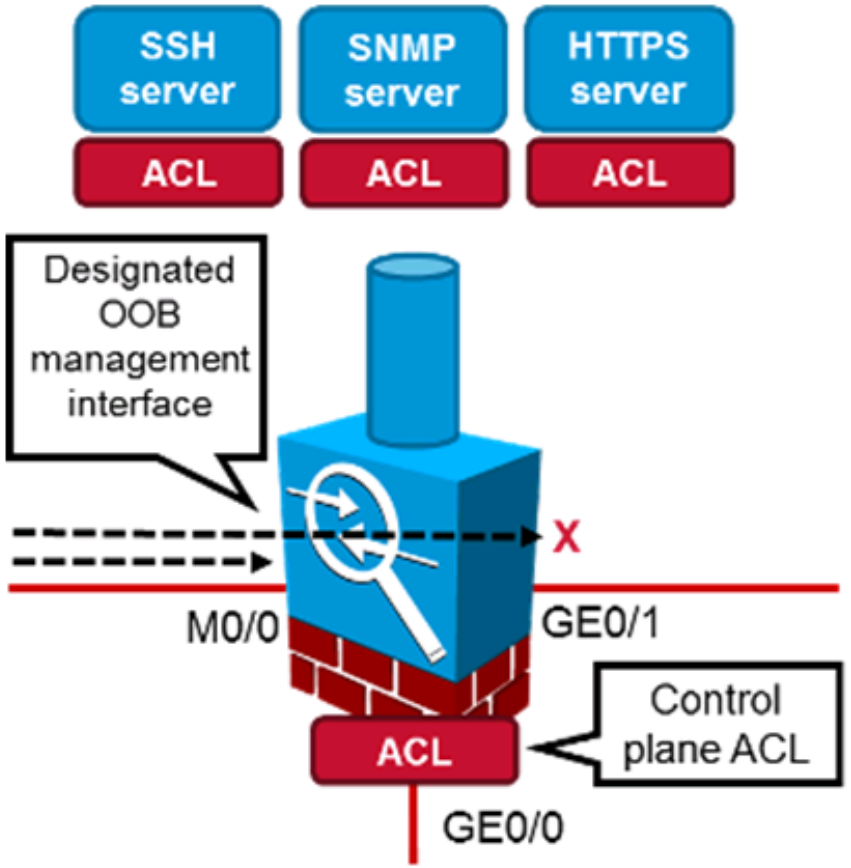
Overview of Cisco ASA Management Plane Security Controls (Cont.)

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



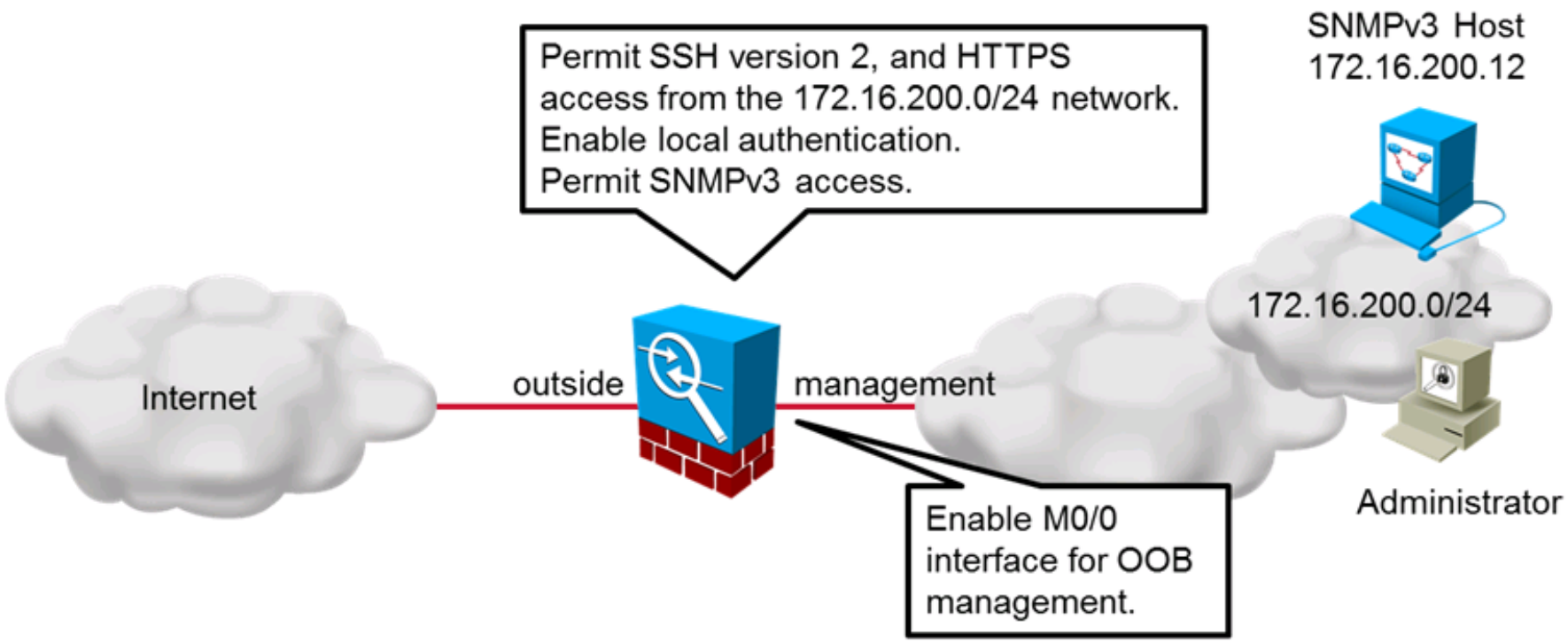
Configure Cisco ASA Secure Management Access

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

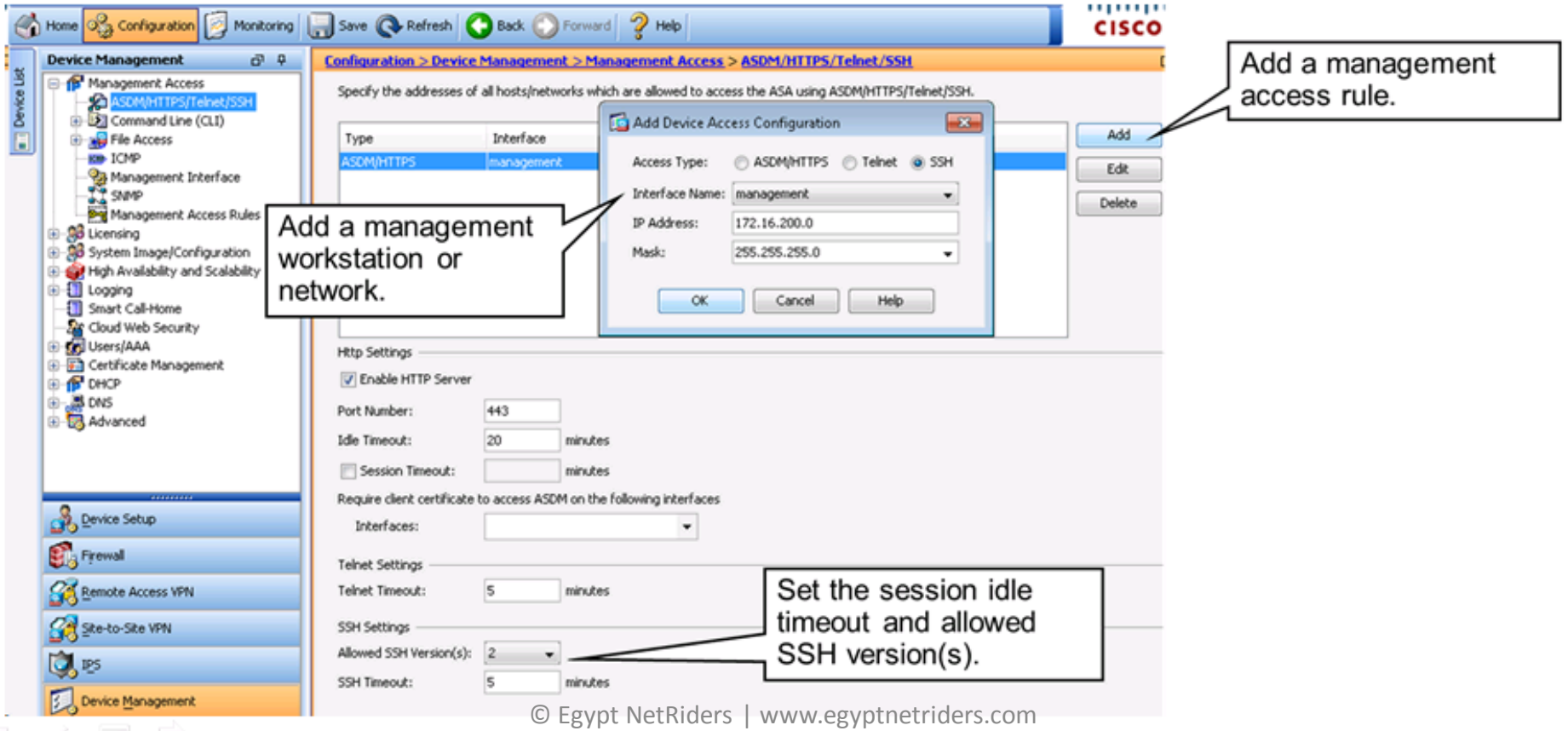
Task 2: Enable HTTPS access

```
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

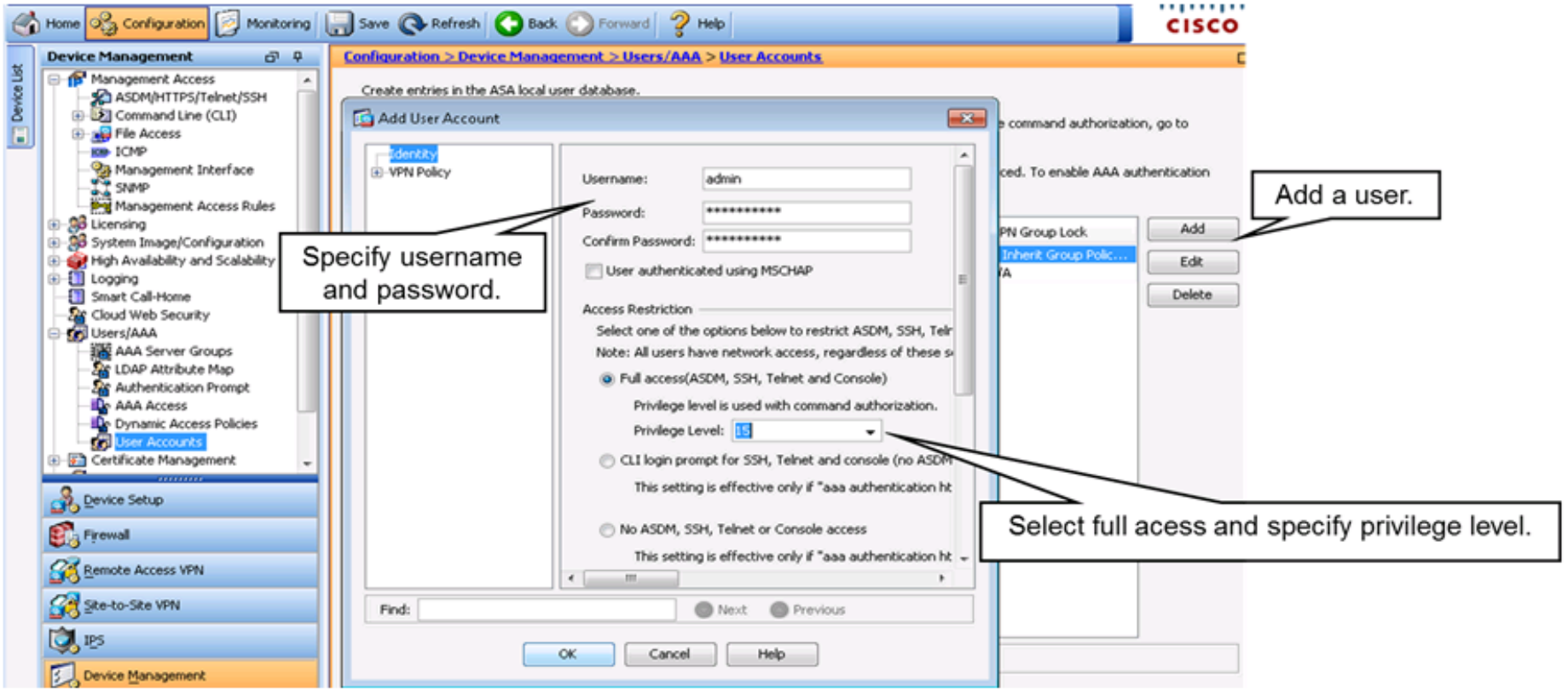
- **Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**



Configure Cisco ASA Secure Management Access (Cont.)

Task 4: Create a user in the local user database

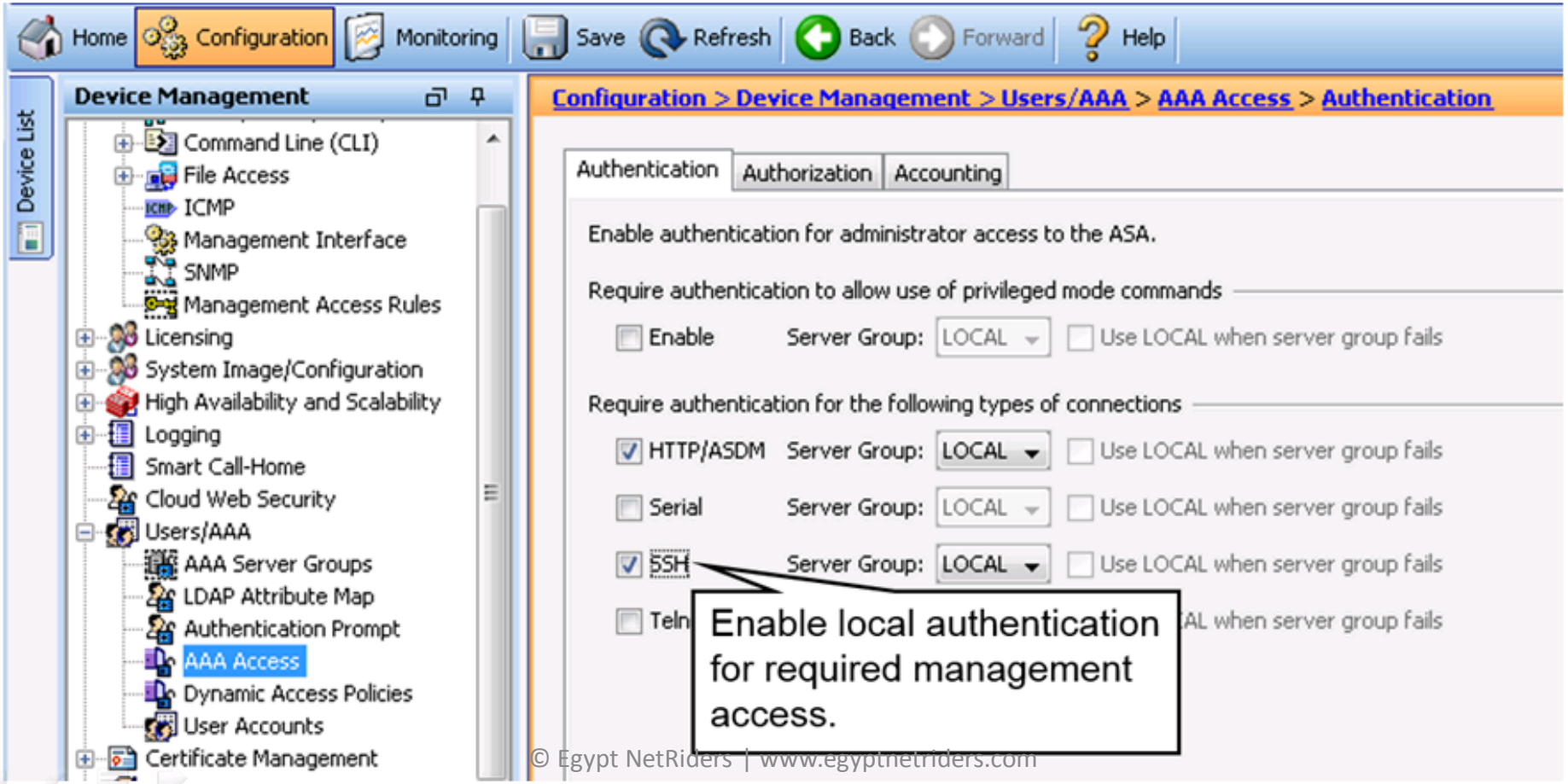
- **Configuration > Device Management > Users/AAA > User Accounts**



Configure Cisco ASA Secure Management Access (Cont.)

Task 5: Enable local authentication for SSH and HTTPS

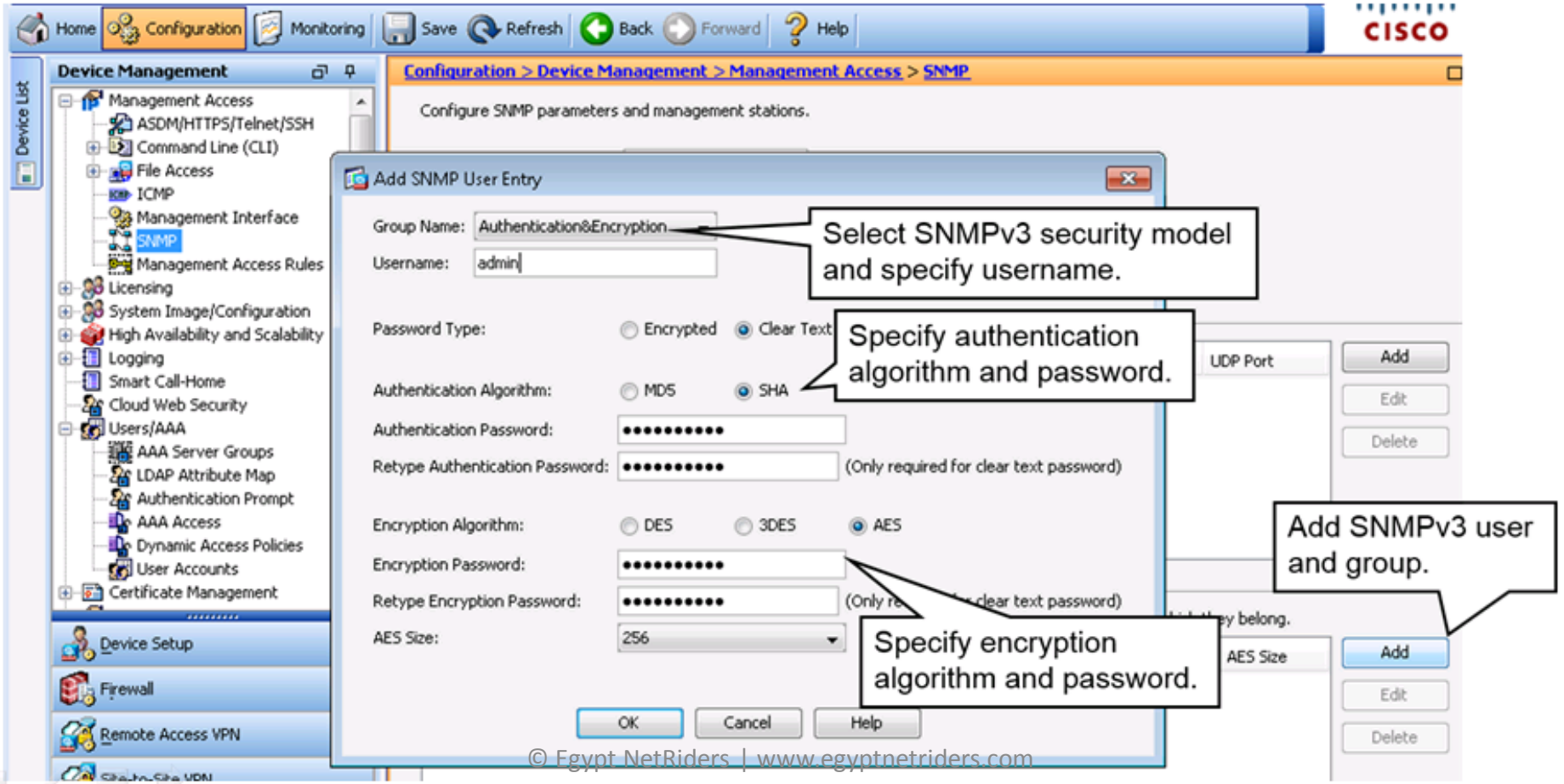
- **Configuration > Device Management > Users/AAA > AAA Access > Authentication**



Configure Cisco ASA Secure Management Access (Cont.)

Task 6: Enable SNMPv3 and configure credentials

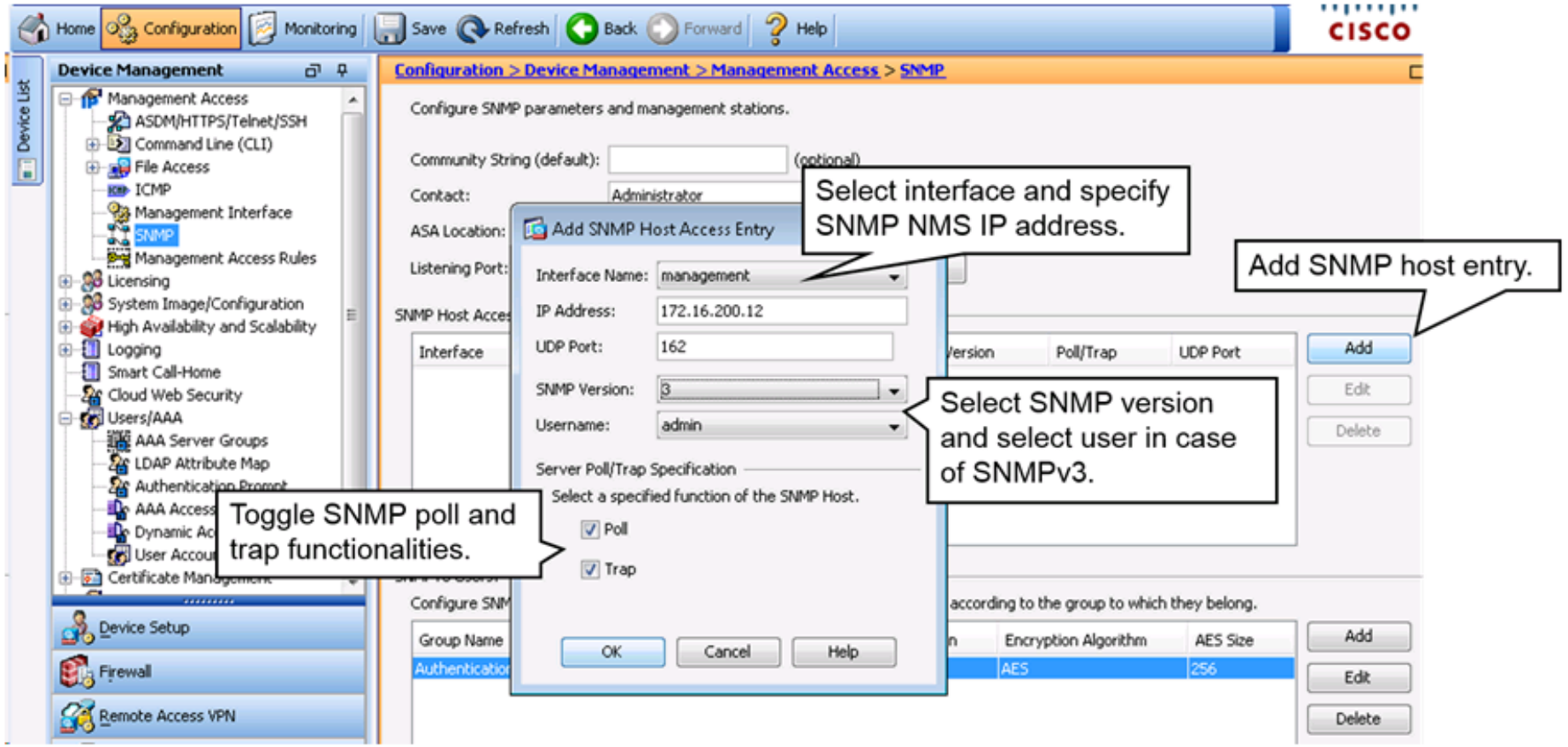
- **Configuration > Device Management > Management Access > SNMP**



Configure Cisco ASA Secure Management Access (Cont.)

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

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



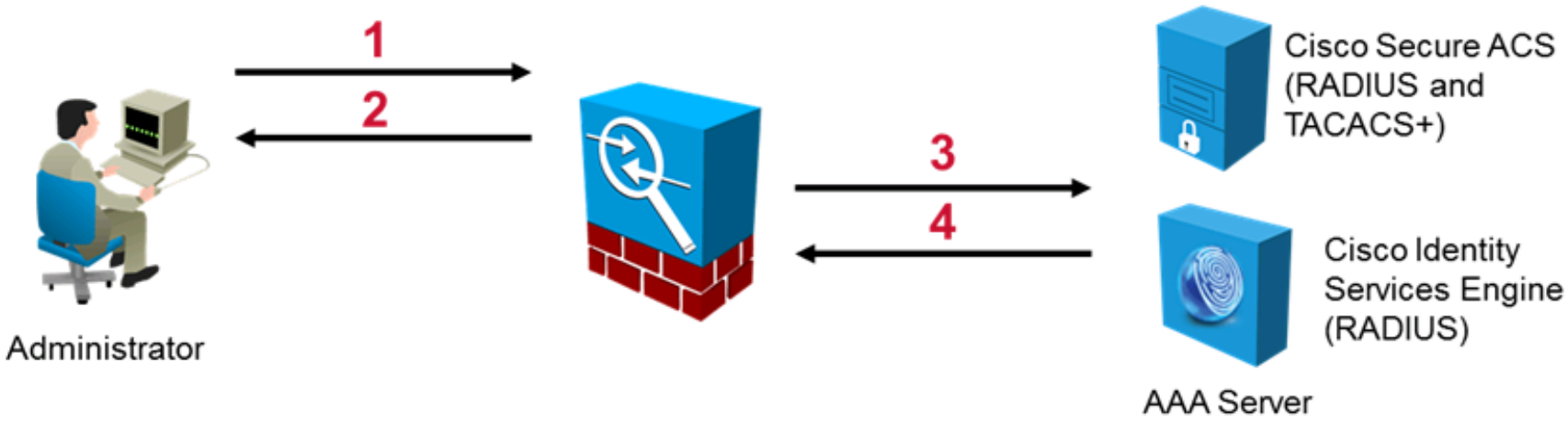
Configure Cisco ASA Secure Management Access (Cont.)

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



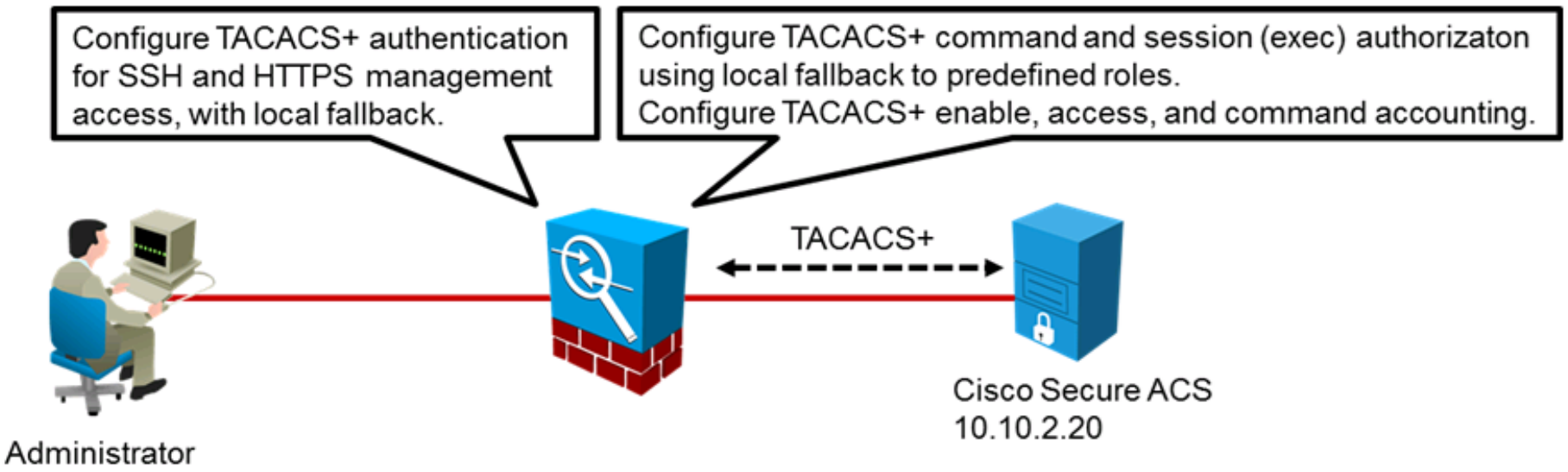
Configure Cisco ASA Management Access AAA

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.)

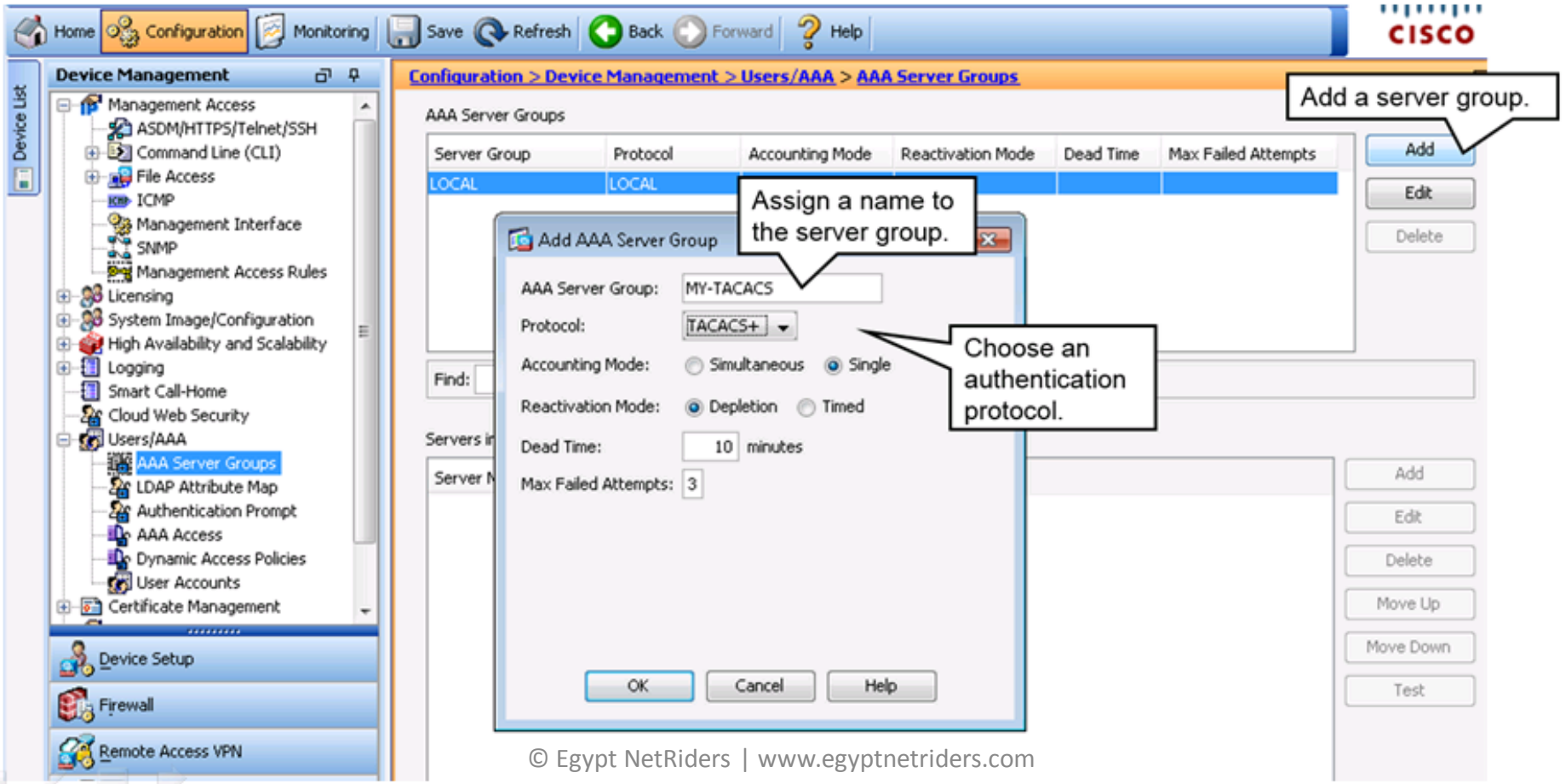
Configuration Scenario



Configure Cisco ASA Management Access AAA (Cont.)

Task 1: Configure external AAA servers

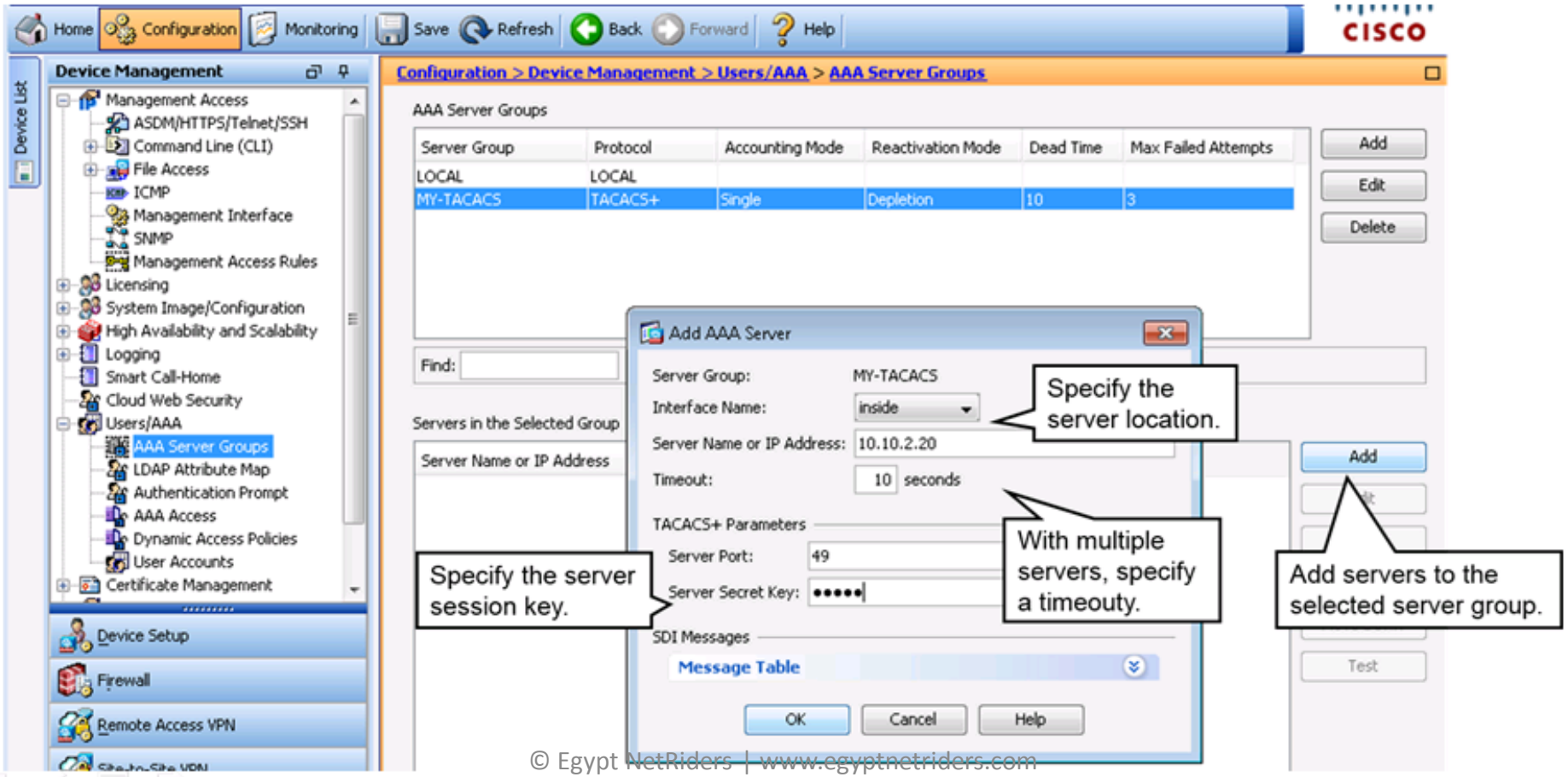
- **Configuration > Device Management > Users/AAA > AAA Server Groups**



Configure Cisco ASA Management Access AAA (Cont.)

Task 1: Configure external AAA servers (cont.)

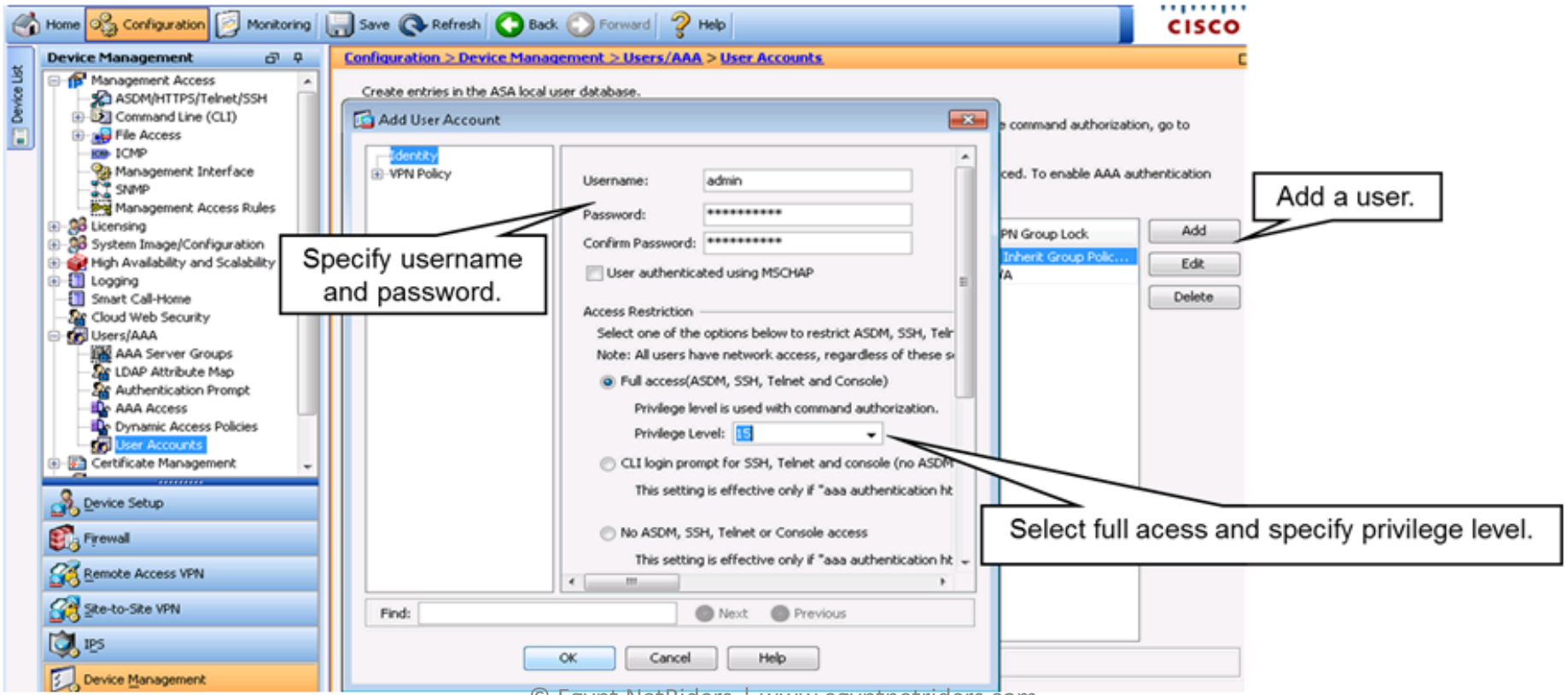
- **Configuration > Device Management > Users/AAA > AAA Server Groups**



Configure Cisco ASA Management Access AAA (Cont.)

Task 2: Create local user accounts with required privilege levels

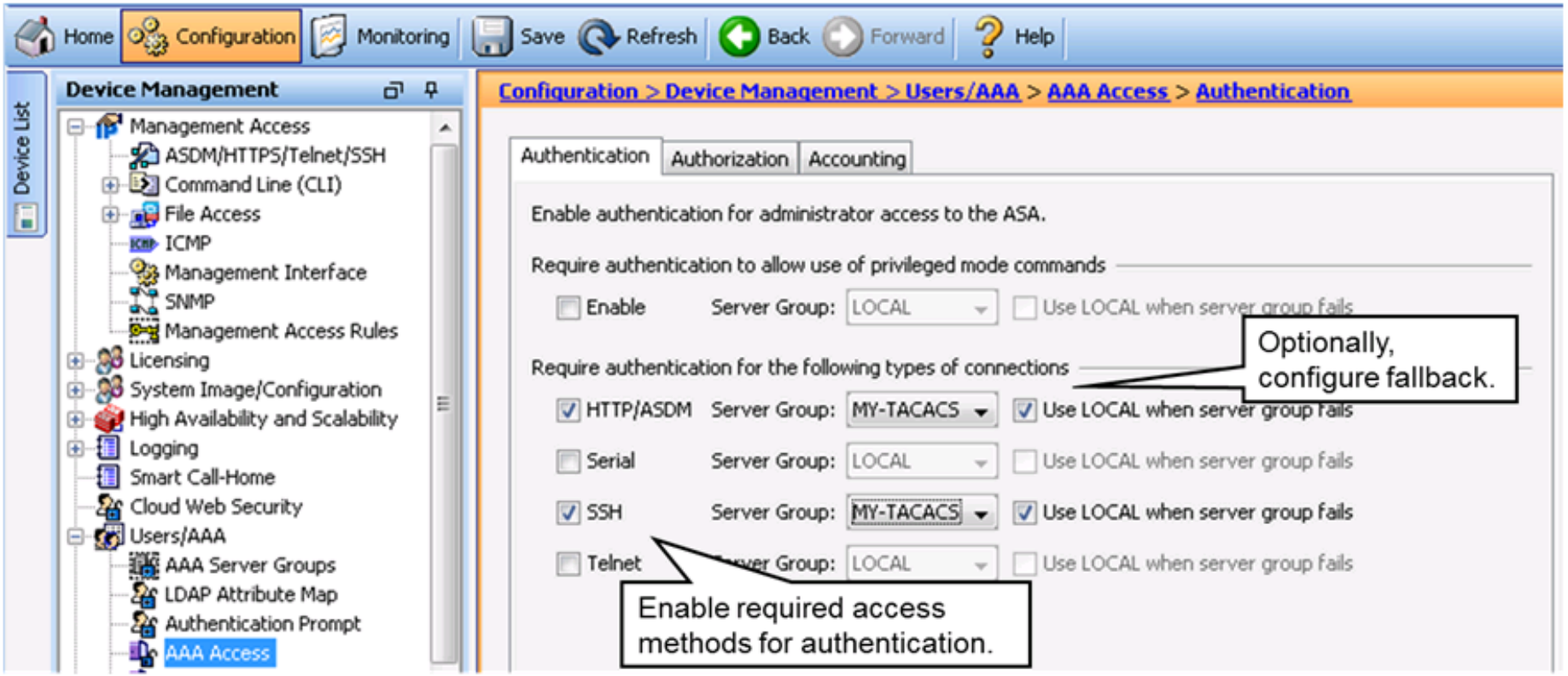
- **Configuration > Device Management > Users/AAA > AAA Server Groups**



Configure Cisco ASA Management Access AAA (Cont.)

Task 3: Configure external authentication for management access

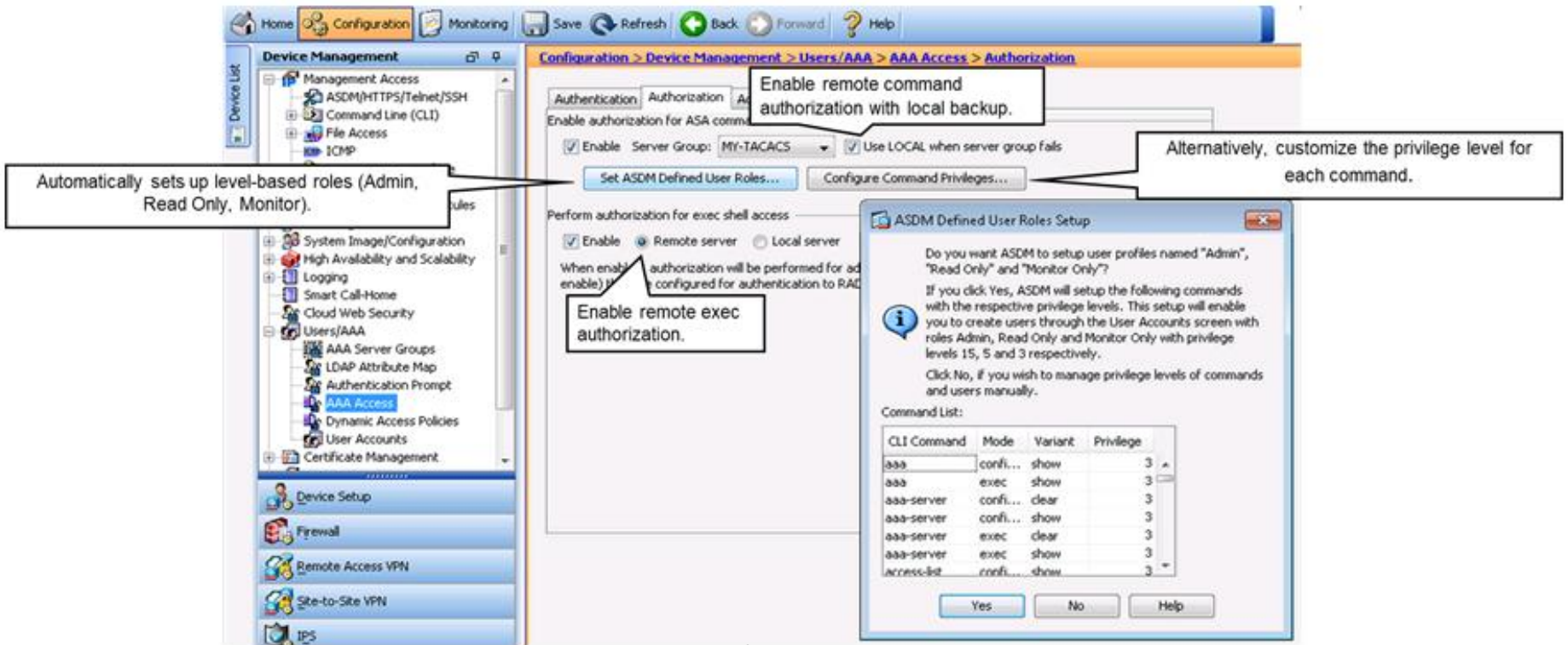
- **Configuration > Device Management > Users/AAA > AAA Access > Authentication**



Configure Cisco ASA Management Access AAA (Cont.)

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

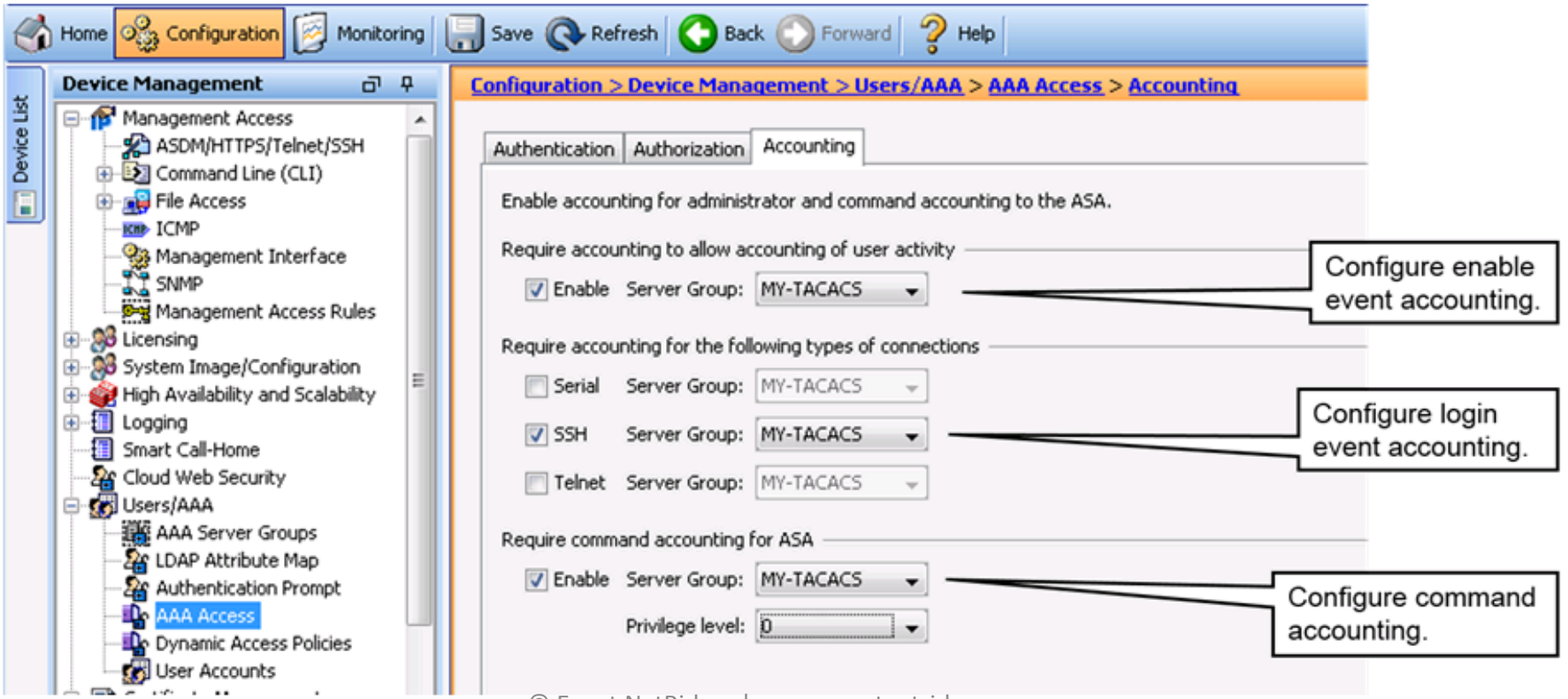
- **Configuration > Device Management > Users/AAA > AAA Access > Authorization**



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**



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
show aaa-server	Displays AAA server statistics for AAA servers.
test aaa-server	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.