インターフェイス内外での ASA バージョン 9.x SSH および Telnet の設定例

目次

概要
前提条件
要件
使用するコンポーネント
関連製品
表記法
設定
ネットワーク図
SSH の設定
セキュリティ アプライアンスへの SSH アクセス
ASA の設定
ASDM バージョン 7.2.1 の設定
Telnet の設定
Telnet のシナリオ例
確認
SSH のデバッグ
アクティブな SSH セッションの表示
公開 RSA キーの表示
トラブルシューティング
ASA から RSA キーを削除する
SSH 接続に失敗する

概要

このドキュメントでは、Cisco シリーズ セキュリティ アプライアンス バージョン 9.x 以降の内部および外部インターフェイスでセキュア シェル（SSH）を設定する方法について説明します。CLI で Cisco 適応型セキュリティ アプライアンス（ASA）をリモートに設定および監視する必要がある場合は、Telnet または SSH のいずれかの使用を必要とします。 Telnet 通信はパスワードを含むことができるクリア テキストで送信されるため、シスコでは SSH を強く推奨します。SSH トラフィックはトンネルで暗号化されるため、パスワードとその他の機密性の高い設定コマンドを傍受から保護するのに役立ちます。

ASA では、管理目的のためにセキュリティ アプライアンスへの SSH 接続を使用できます。 セキュリティ アプライアンスでは、利用可能であれば、セキュリティ コンテキストごとに最大で 5 つの同時 SSH 接続が使用でき、合計したすべてのコンテキストに関してグローバルで最大 100 個の接続が使用できます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco ASA ファイアウォール ソフトウェア バージョン 9.1.5 に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

> **注:** SSH バージョン 2（SSHv2）は ASA バージョン 7.x 以降でサポートされています。

関連製品

この設定は、ソフトウェア バージョン 9.x 以降で稼働する Cisco ASA 5500 シリーズ セキュリティ アプライアンスでも使用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

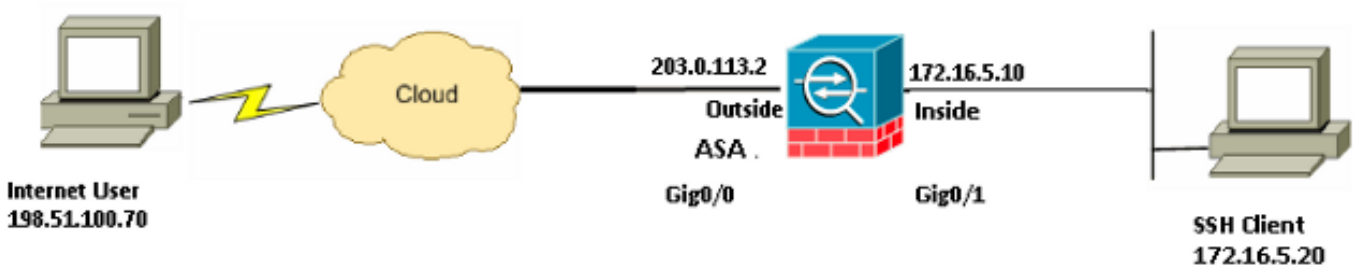
設定

このドキュメントで説明する機能を設定するには、このセクションに記載されている情報を使用します。

> **注:** 各設定手順の説明では、CLI または Adaptive Security Device Manager（ASDM）のいずれかを使用するために必要な情報を提供します。

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図



この設定例では、ASA は SSH サーバであると見なされます。 SSH クライアント（198.51.100.70/32 および 172.16.5.20/24）から SSH サーバへのトラフィックは暗号化されます。 セキュリティ アプライアンスでは、SSH バージョン 1 および 2 で提供されている SSH リモート シェル機能がサポートされ、さらにデータ暗号化規格（DES）と 3DES 暗号化がサポートされています。 SSH バージョン 1 と 2 は異なるため、相互運用性はありません。

SSH の設定

このドキュメントでは、次の設定を使用します。

- セキュリティ アプライアンスへの SSH アクセス
- SSH クライアントの使用方法
- ASA の設定

セキュリティ アプライアンスへの SSH アクセス

セキュリティ アプライアンスへの SSH アクセスを設定するには、次の手順を実行します。

1. SSH セッションは常に、ユーザ名やパスワードなどの認証方式を要求します。 この要件を満たすために、2 つの方法が使用できます。

   この要件を満たすための **1 つ目の方法**は、認証、許可、アカウンティング（AAA）を使用してユーザ名とパスワードを設定することです。

   ```
   ASA(config)#username username password password
   ASA(config)#aaa authentication {telnet | ssh | http | serial} console
   {LOCAL | server_group [LOCAL]}
   ```

   注: 認証に TACACS+ または RADIUS サーバ グループを使用する場合、AAA サーバが使用できないときには、フォールバック方式としてローカル データベースを使用するようにセキュリティ アプライアンスを設定できます。 サーバ グループ名を指定して、その後に **LOCAL** と続けます（**LOCAL** は大文字小文字が区別されます）。 セキュリティ アプライアンス プロンプトでは使用されている方式が表示されないため、ローカル データベースと AAA サーバで同じユーザ名とパスワードを使用することを推奨します。**TACACS+** の **LOCAL backup** を指定するには、次の設定を SSH 認証で使用します。

   ```
   ASA(config)#aaa authentication ssh console TACACS+ LOCAL
   ```

   または、フォールバックなしの認証のメイン方式としてローカル データベースを使用できます。 これを行うには、**LOCAL** だけを入力します。

   ```
   ASA(config)#aaa authentication ssh console LOCAL
   ```

   この要件を満たすための **2 つ目の方法**は、デフォルトのユーザ名に **ASA**、デフォルトの Telnet パスワードに **cisco** を使用することです。 次のコマンドを使用すると、Telnet パスワードを変更できます。

   ```
   ASA(config)#passwd password
   ```

   注: この場合、**password コマンド**を、両方のコマンド機能として同時に使用できます。

2. SSH に必要である ASA ファイアウォール用の RSA キー ペアを生成します。
   ASA(config)#**crypto key generate rsa modulus *modulus_size*注:** modulus_size（ビット単位）は 512、768、1024、または 2048 のいずれかになります。 指定する鍵モジュールのサイズが大きいほど、RSA 鍵ペアの生成に要する時間が長くなります。 値は 2048 を推奨します。 RSA キー ペアを生成するために使用するコマンドは、バージョン 7.x 以前の ASA ソフトウェア バージョンでは異なります。 前のバージョンでは、キーを作成する前にドメイン名を設定する必要があります。 マルチ コンテキスト モードでは、コンテキストごとに RSA キーを生成する必要があります。
3. セキュリティ アプライアンスへの接続が許可されているホストを指定します。 このコマンドでは、SSH を使用した接続が許可されているホストの発信元アドレス、ネットマスク、およびインターフェイスを指定します。 このコマンドは、複数のホスト、ネットワーク、またはインターフェイスに対して何度でも入力できます。 この例では、内部にある 1 つのホストと外部にある 1 つのホストが許可されています。
   ASA(config)#**ssh 172.16.5.20 255.255.255.255 inside**
   ASA(config)#**ssh 198.51.10.70 255.255.255.255 outside**
4. この手順はオプションです。 デフォルトでは、セキュリティ アプライアンスは SSH バージョン 1 とバージョン 2 の両方を許可します。接続を特定のバージョンに限定するには、次のコマンドを入力します。
   ASA(config)# **ssh version *<version_number>*注: version_number は 1 または 2 のいずれかです。**
5. この手順はオプションです。 デフォルトでは、非アクティブの状態が 5 分間続くと SSH セッションが終了します。 このタイムアウト時間は、1 分から最大 60 分まで設定できます。
   ASA(config)#**ssh timeout *minutes***

ASA の設定

ASA の設定には次の情報を使用します。

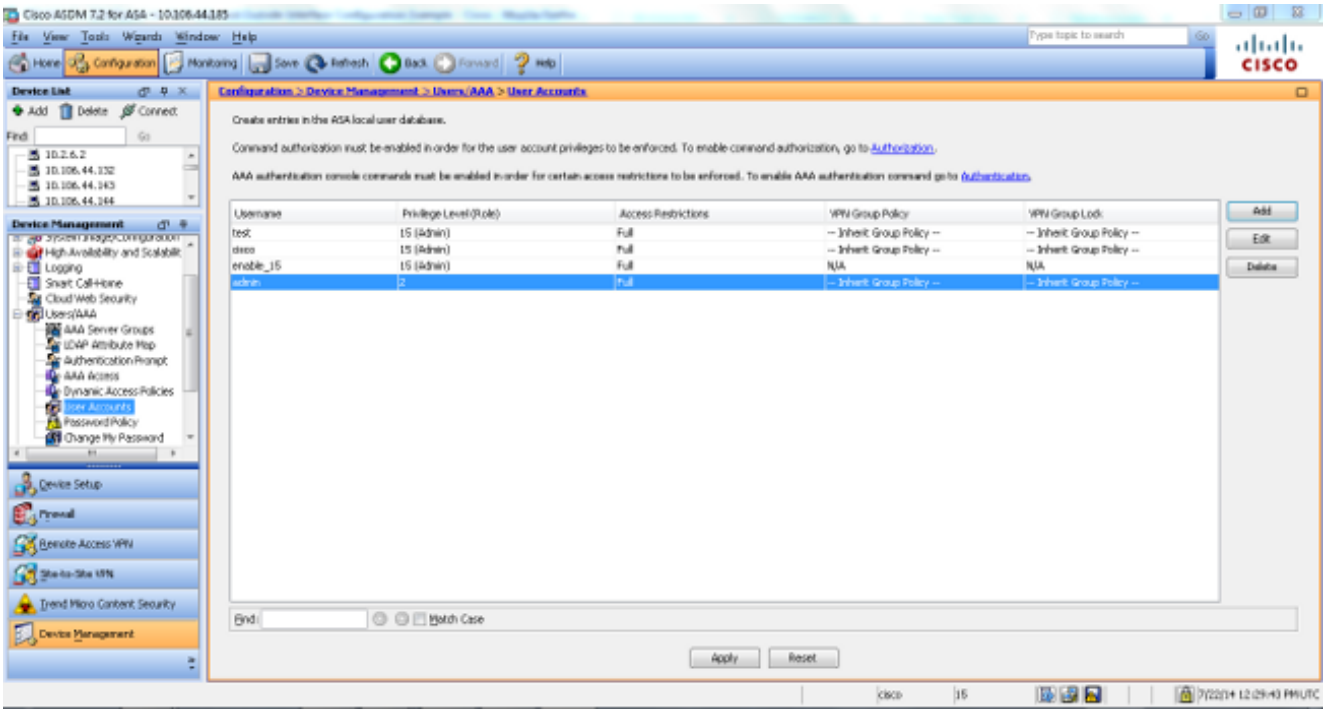
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 172.16.5.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.2 255.255.255.0

!--- AAA for the SSH configuration

username ciscouser password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL

http server enable
http 172.16.5.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstar
telnet timeout 5
```

```
!--- Enter this command for each address or subnet
!--- to identify the IP addresses from which
!--- the security appliance accepts connections.
!--- The security appliance accepts SSH connections from all interfaces.

ssh 172.16.5.20 255.255.255.255 inside
ssh 198.51.100.70 255.255.255.255 outside

!--- Allows the users on the host 172.16.5.20 on inside
!--- Allows SSH access to the user on internet 198.51.100.70 on outside
!--- to access the security appliance
!--- on the inside interface.

ssh 172.16.5.20 255.255.255.255 inside

!--- Sets the duration from 1 to 60 minutes
!--- (default 5 minutes) that the SSH session can be idle,
!--- before the security appliance disconnects the session.

ssh timeout 60

console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
```

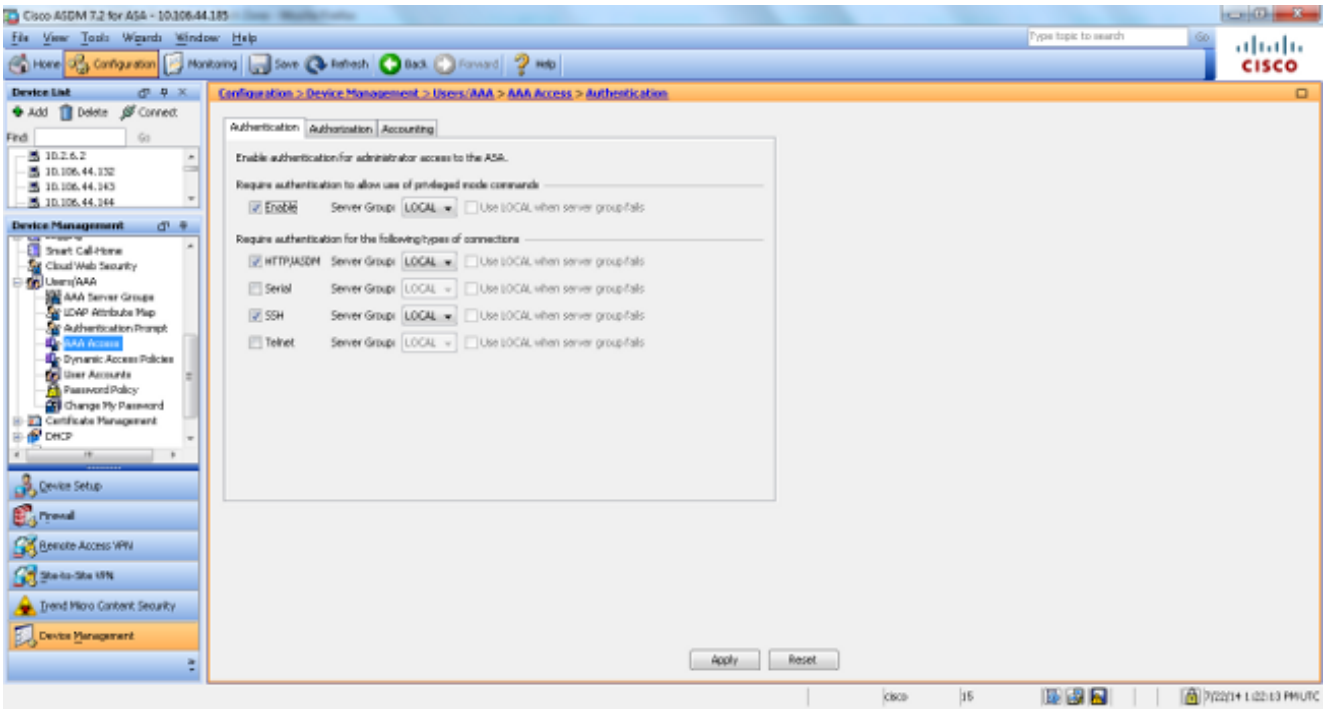
ASDM バージョン 7.2.1 の設定

ASDM バージョン 7.2.1 を設定するには、次の手順を実行します。

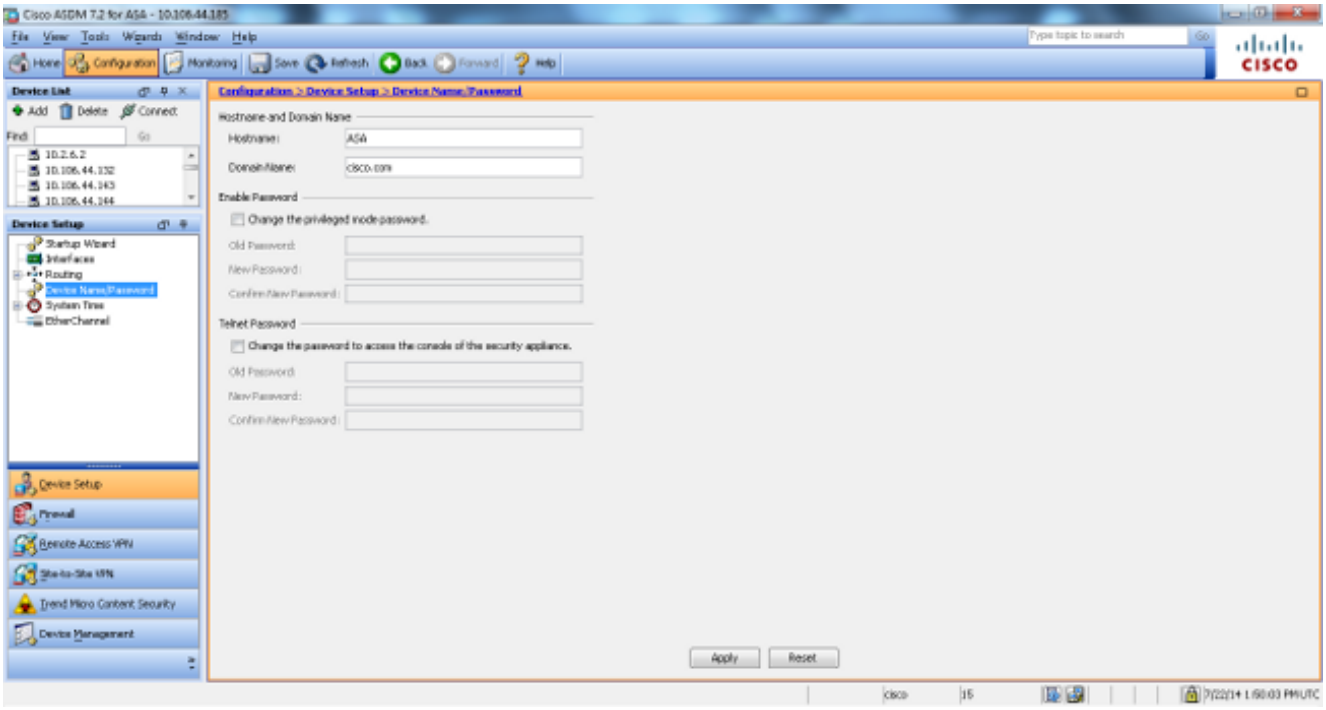
1. ASDM を使用してユーザを追加するには、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] に移動します。



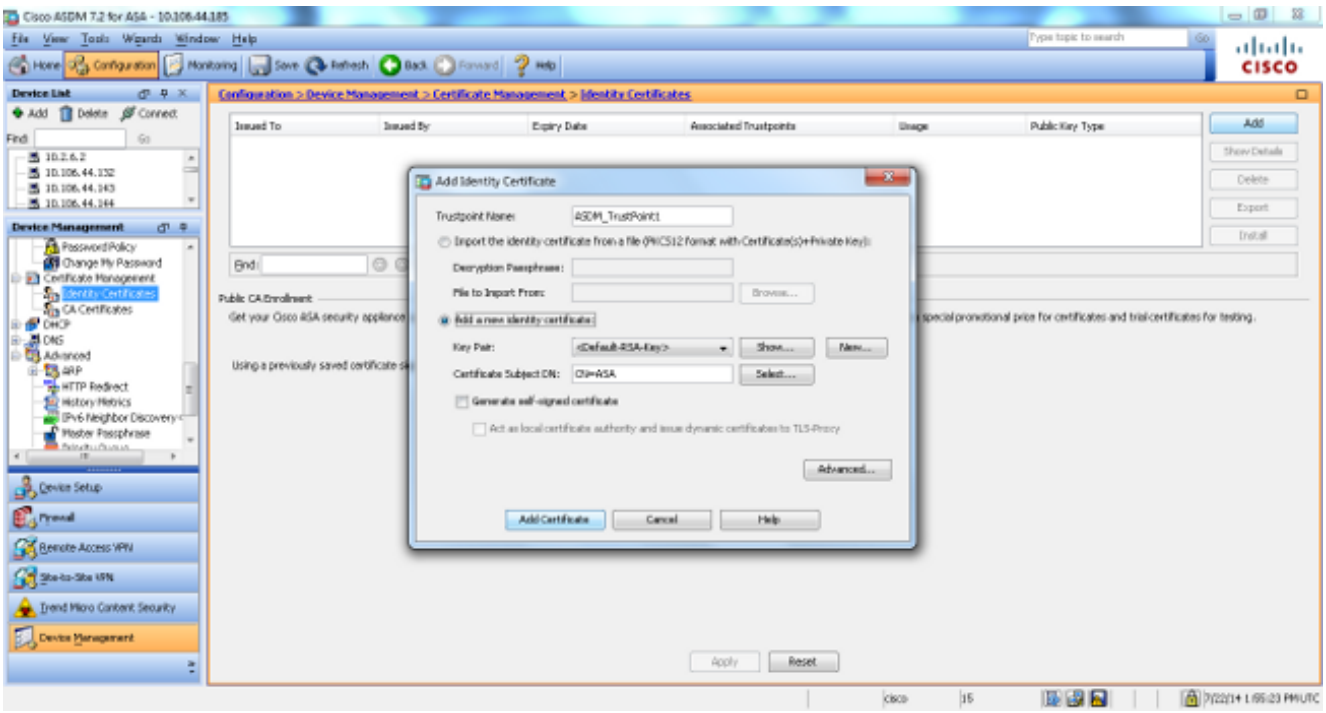
2. ASDM を使用して SSH 用の AAA 認証を設定するには、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] に移動します。



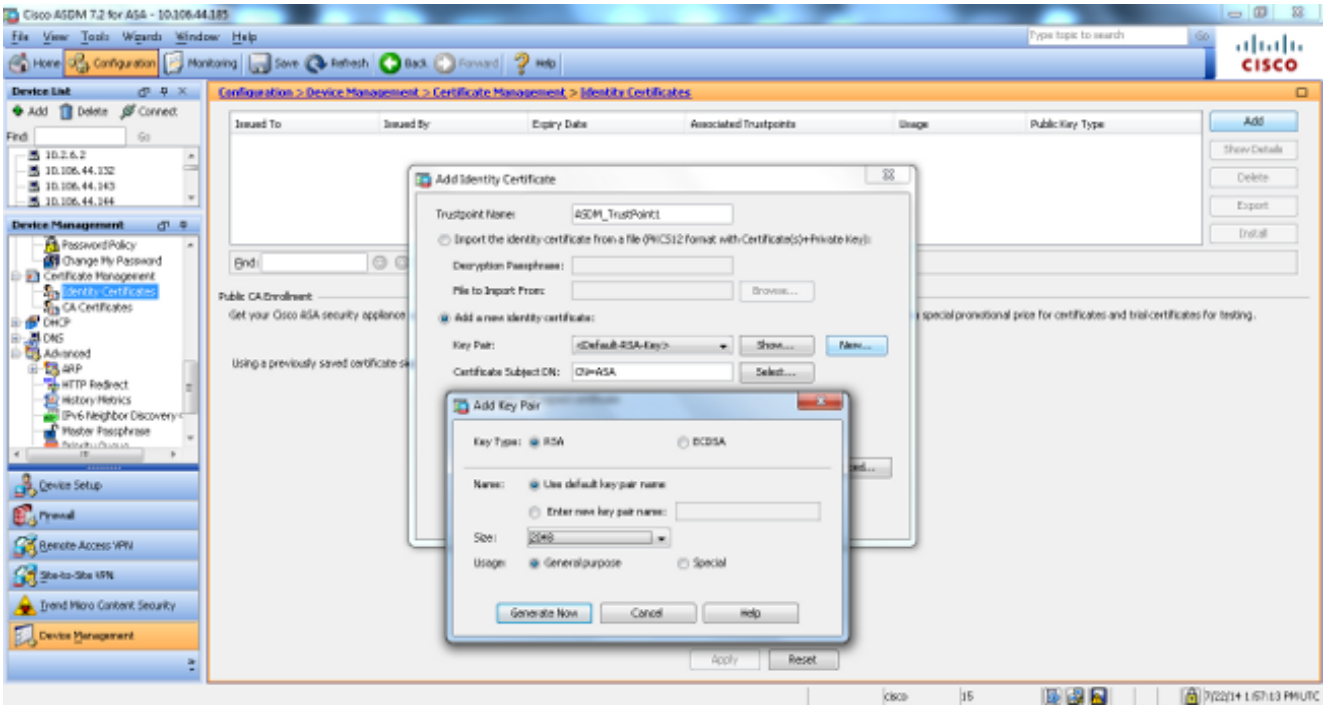
3. ASDM を使用して Telnet パスワードを変更するには、[Configuration] > [Device Setup] > [Device Name/Password] に移動します。



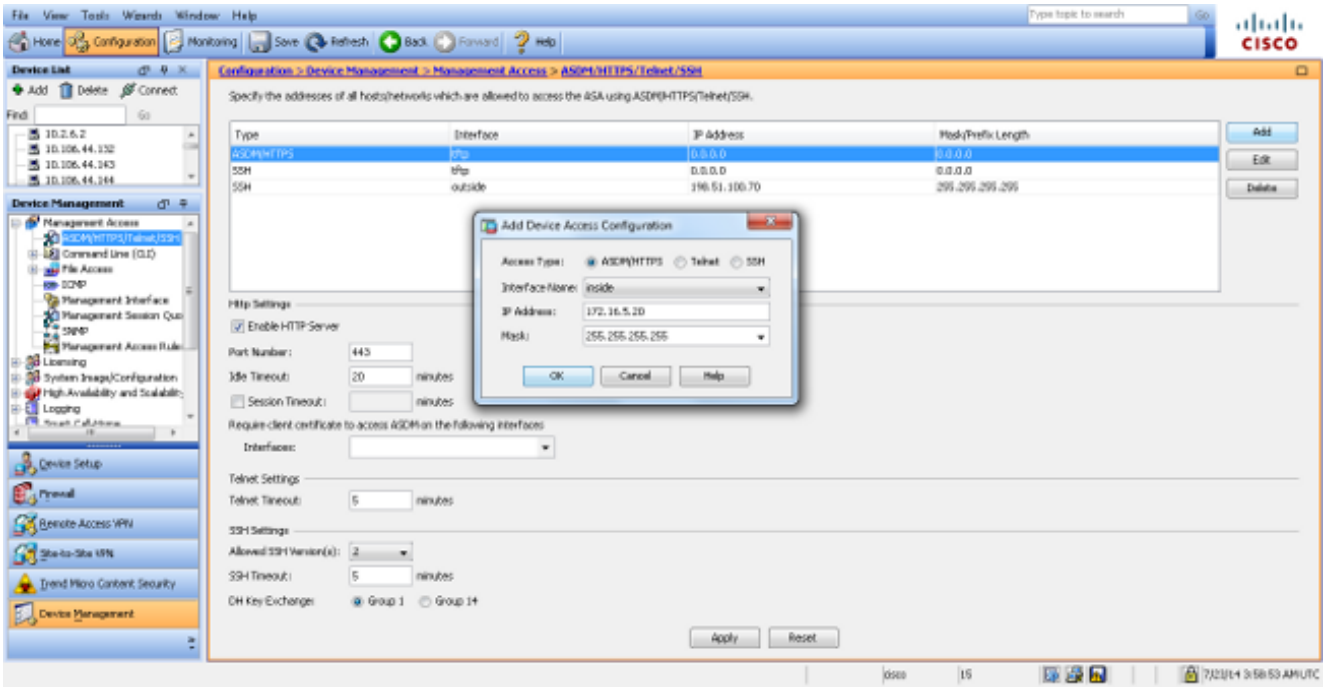
4. ASDM を使用して同じ RSA キーを生成するには、[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] に移動し、[Add] をクリックして、使用可能なデフォルトのオプションを使用します。



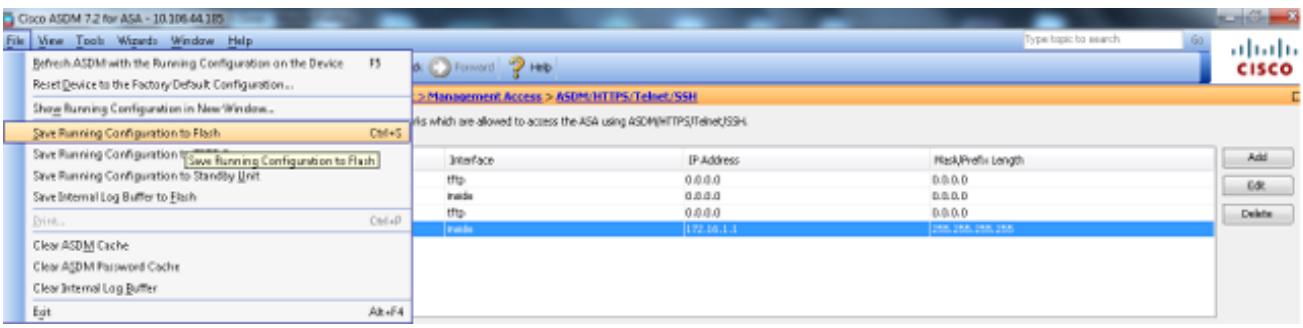
5. キーが存在しない場合は、[Add a new Identity certificate] オプション ボタンをクリックし、[New] をクリックしてデフォルトのキー ペアを追加します。 完了したら、[Generate Now] をクリックします。



6. ASDM を使用して、SSH との接続が許可されるホストを指定できるようにし、バージョンとタイムアウトのオプションを指定するには、[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Secure Shell (SSH)] に移動します。



7. ポップアップ ウィンドウで [Save] をクリックして設定を保存します。



8. フラッシュ上で設定を保存するかどうかを確認するプロンプトが表示されたら、[Apply] を選択して設定を保存します。

Telnet の設定

コンソールに Telnet アクセスを追加し、アイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **telnet コマンド**を入力します。 デフォルトでは、5 分間アイドル状態に放置された Telnet セッションは、セキュリティ アプライアンスにより終了されます。 以前に設定した IP アドレスから Telnet アクセスを削除するには、このコマンドの **no 形式**を使用します。

```
telnet {{hostname | IP_address mask interface_name} | {IPv6_address
interface_name} | {timeout number}}
no telnet {{hostname | IP_address mask interface_name} | {IPv6_address
interface_name} | {timeout number}}
```

telnet コマンドは、Telnet 経由でセキュリティ アプライアンス コンソールにアクセスできるホストを指定します。

> **注:** すべてのインターフェイス上でセキュリティ アプライアンスへの Telnet を有効にすることができます。 ただし、セキュリティ アプライアンスは、外部インターフェイスへのすべての Telnet トラフィックが IPSec で保護される必要があります。 外部インターフェイスへの Telnet セッションを有効にするには、セキュリティ アプライアンスにより生成される IP トラフィックを含むように外部インターフェイス上で IPSec を設定し、外部インターフェイス上で Telnet を有効にします。

> **注:** 通常、セキュリティ レベルが 0 であるか、他のインターフェイスよりも低い場合、ASA はそのインターフェイスへの Telnet を許可しません。

> **注:** Telnet セッションを通じてセキュリティ アプライアンスへアクセスすることは推奨されません。 パスワードなど、認証のためのクレデンシャル情報はクリア テキストで送信されます。 SSH を使用して、よりセキュリティ保護されたデータ通信を行うことが推奨されます。

コンソールへの Telnet アクセス用のパスワードを設定するには、**password コマンド**を入力します。 デフォルトのパスワードは **cisco** です。 現在セキュリティ アプライアンス コンソールにアクセスしている IP アドレスを表示するには、**who コマンド**を入力します。 アクティブな Telnet コンソール セッションを終了するには、**kill コマンド**を入力します。

Telnet のシナリオ例

内部インターフェイスへの Telnet セッションを有効にするには、このセクションの例を参照します。

例 1

この例では、ホスト **172.16.5.20** のみが、Telnet 経由でのセキュリティ アプライアンス コンソールへのアクセスを許可されています。

```
ASA(config)#telnet 172.16.5.20 255.255.255.255 inside
```

例 2

この例では、ネットワーク 172.16.5.0/24 のみが、Telnet 経由でのセキュリティ アプライアンス コンソールへのアクセスを許可されています。

```
ASA(config)#telnet 172.16.5.0 255.255.255.0 inside
```

例 3

この例では、すべてのネットワークが、Telnet 経由でのセキュリティ アプライアンス コンソールへのアクセスを許可されています。

```
ASA(config)#telnet 0.0.0.0 0.0.0.0 inside
```

コンソール キーワードとともに aaa コマンドを使用する場合、認証サーバを使用して Telnet コンソール アクセスを認証する必要があります。

> **注:** ユーザが **aaa コマンド**を設定してセキュリティ アプライアンスと Telnet コンソール アクセスの認証を要求し、コンソール ログイン要求がタイムアウトした場合、シリアル コンソールからセキュリティ アプライアンスにアクセスできます。 これを行うには、**enable password** コマンドで設定されたセキュリティ アプライアンスのユーザ名とパスワードを入力します。

セキュリティ アプライアンスにより ログオフされる前に、コンソール Telnet セッションがアイドル状態を維持する最大時間を設定するには、**telnet timeout** コマンドを発行します。 **no telnet** コマンドと **telnet timeout** コマンドを組み合わせて使用することはできません。

次の例に、最大セッション アイドル時間の変更方法を示します。

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

確認

このセクションでは、設定が正常に機能していることを確認します。

> **注:** Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

SSH のデバッグ

SSH のデバッグを有効にするには、**debug ssh コマンド**を入力します。

```
ASA(config)#debug ssh
SSH debugging on
```

次の出力は、内部 IP アドレス（172.16.5.20）から ASA の内部インターフェイスへの SSH の試行を示します。 次のデバッグは、正常な接続と認証を示しています。

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication successful for cisco

!--- Authentication for the ASA was successful.

SSH2 0: channel open request
SSH2 0: pty-req request
SSH2 0: requested tty: vt100, height 25, width 80
SSH2 0: shell request
SSH2 0: shell message received
```

cisco と入力すべきところを cisco1 と入力するなど、誤ったユーザ名を入力してしまった場合、ASA ファイアウォールでは認証が拒否されます。 次のデバッグ出力は、失敗した認証を示しています。

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
```

```
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA1 was not successful due to the wrong username.
```

同様に、誤ったパスワードが入力された場合、認証は失敗します。 次のデバッグ出力は、失敗した認証を示しています。

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA was not successful due to the wrong password.
```

アクティブな SSH セッションの表示

ASA に接続されている（接続状態の）SSH セッションの数を確認するには、次のコマンドを入力します。

```
ASA(config)# show ssh sessions

SID Client IP    Version Mode Encryption Hmac State           Username
0   172.16.5.20 2.0     IN   aes256-cbc sha1 SessionStarted  cisco
                        OUT  aes256-cbc sha1 SessionStarted  cisco
```

ASDM を使用してセッションを表示するには、[Monitoring] > [Properties] > [Device Access] > [Secure Shell Sessions] に移動します。

TCP セッションが確立しているかどうかを確認するには、**show asp table socket** コマンドを入力します。

```
ASA(config)# show asp table socket

Protocol Socket State Local Address Foreign Address
```

```
SSL 02444758 LISTEN 203.0.113.2:443 0.0.0.0:*
TCP 02448708 LISTEN 203.0.113.2:22 0.0.0.0:*
SSL 02c75298 LISTEN 172.16.5.10:443 0.0.0.0:*
TCP 02c77c88 LISTEN 172.16.5.10:22 0.0.0.0:*
TCP 02d032d8 ESTAB 172.16.5.10:22 172.16.5.20:52234
```

公開 RSA キーの表示

セキュリティ アプライアンス上の RSA キーの公開部分を表示するには、次のコマンドを入力します。

```
ASA(config)#show crypto key mypubkey rsa
Key pair was generated at: 23:23:59 UTC Jul 22 2014
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Key:

 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
 00aa82d1 f61df1a4 7cd1ae05 c92322c1 1ce490e3 c9db00fd d75afe77 1ea0b2c2
 3325576f a7dc5ffe a6166bf5 7f0f2551 25b8cb23 a8908b49 81c42618 c98e3aea
 ce6f9e42 367974d1 5c2ea6b1 e7aac40b 44a6c0a5 23c4d845 a57d4c04 6de49dbb
 2c6f074e 25e3b19e 7c5da809 ac7d775c 0c01bb9d 211b7078 741094b4 94056e75
 72d5e938 c59baaec 12285005 ee6abf81 90822610 cf7ee4c1 ae8093d9 6943bde3
 16d8748c d86b5f66 1a6ccf33 9cde0432 b3cabab5 938b1874 c3d7c13e 43a95a8f
 ed36db2e f9ca5d2c 0c65858e 3e513723 2d362b47 7984d845 faf22579 654113d1
 24d59f27 55d2ddf3 20af3b65 62f039cb a3aafc31 d92a3d9b 14966eb3 cb6ca249
 55020301 0001
```

ASDM を使用して RSA キーを表示するには、[Configuration] > [Properties] > [Certificate] > [Key Pair] に移動し、[Show Details] をクリックします。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

ASA から RSA キーを削除する

ASA ソフトウェアをアップグレードするか、ASA の SSH バージョンを変更する際は、RSA キーを削除して再作成する必要がある場合があります。 ASA から RSA キー ペアを削除するには、次のコマンドを入力します。

```
ASA(config)#crypto key zeroize rsa
```

ASDM を使用して RSA キーを削除するには、[Configuration] > [Properties] > [Certificate] > [Key Pair] に移動し、[Delete] をクリックします。

SSH 接続に失敗する

ASA では次のエラー メッセージが表示される場合があります。

```
%ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
```

これは SSH クライアント マシンに表示されるエラー メッセージです:

Selected cipher type <unknown> not supported by server.

この問題を解決するには、RSA キーを削除し、再作成します。 ASA から RSA キー ペアを削除するには、次のコマンドを入力します。

```
ASA(config)#crypto key zeroize rsa
```

新しいキーを生成するには、次のコマンドを入力します。

```
ASA(config)# crypto key generate rsa modulus 2048
```