PIX/ASA 7.x： Inside および Outside インターフェイスでの SSH/Telnet の設定例

目次

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 7.x 以降の Inside と Outside のインターフェイスでの Secure Shell (SSH; セキュア シェル) の設定例を紹介しています。 リモートでコマンドラインを使用するこのシリーズのセキュリティ アプライアンスの設定では、Telnet または SSH のいずれかを使用します。 パスワードを含む Telnet 通信はクリア テキストで送信されるため、SSH を強く推奨いたします。 SSH トラフィックはトンネルで暗号化されるため、パスワードなどの設定コマンドを傍受から保護するのに役立ちます。

セキュリティ アプライアンスでは、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。

この設定例では、PIX セキュリティ アプライアンスは SSH サーバであると見なされます。 SSH クライアント（10.1.1.2/24 および 172.16.1.1/16）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 Data Encryption Standard（DES; データ暗号規格）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。

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 PIX Firewall ソフトウェア バージョン 7.1 および 8.0 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: SSHv2 は、PIX/ASA バージョン 7.x 以降でサポートされており、7.x よりも前のバージョンではサポートされません。

関連製品

この設定は、ソフトウェア バージョン 7.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

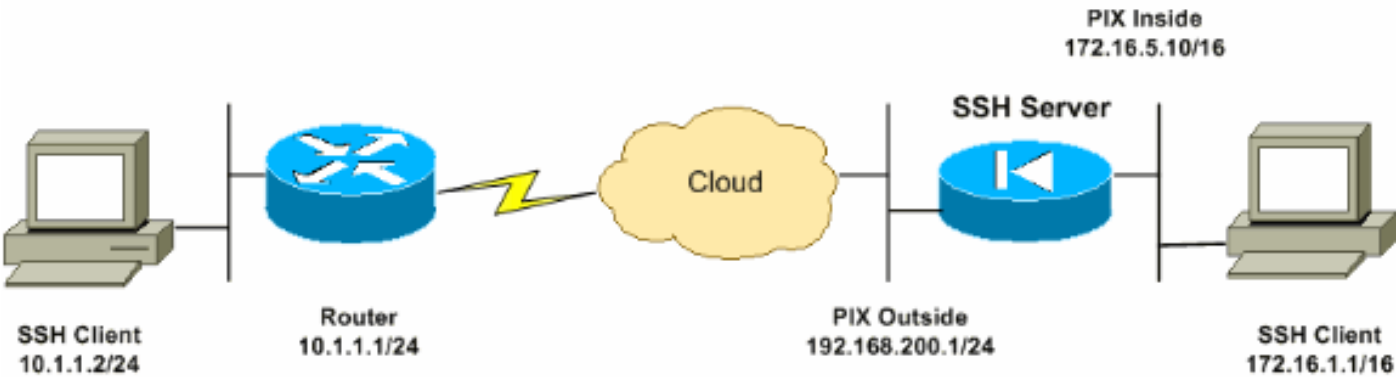
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: 各設定手順では、コマンドラインまたは Adaptive Security Device Manager（ASDM）を使用するのに必要な情報を示しています。

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

このドキュメントでは、次のネットワーク構成を使用しています。



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
- PIX 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 セッションでは常に認証用のユーザ名とパスワードが必要です。 この要件を満たすには次の 2 つの方法があります。ユーザ名とパスワードを設定し、AAA を使用します。構文：`pix(config)#username username password password` `pix(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group [LOCAL]}` **注:** TACACS+ RADIUS AAA 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 データベース内では AAA サーバと同じユーザ名とパスワードを使用することを推奨いたします。**注:** 例：`pix(config)#aaa authentication ssh console TACACS+ LOCAL` **注:** 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。例：`pix(config)#aaa authentication ssh console LOCAL` **または**デフォルトのユーザ名 **pix** およびデフォルトの Telnet パスワード **cisco** を使用します。 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。`pix(config)#passwd password` **注:** ここで **password** コマンドを使用することもできます。 両方のコマンドは同じことを実行します。
2. SSH に必要である PIX Firewall 用の RSA 鍵ペアを生成します。`pix(config)#crypto key generate rsa modulus modulus_size` **注:** modulus_size（ビット単位）は 512、768、1024、または 2048 のいずれかを指定します。 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 1024 が推奨されます。**注:** RSA 鍵ペアの生成に使用するコマンドは、7.x よりも前の PIX 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、鍵を作成する前にドメイン名を設定する必要があります。**注:** マルチ コンテキスト モードでは、各コンテキストの RSA キーを生成する必要があります。 また、システム コンテキスト モードでは crypto コマンドはサポートされていません。
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、Inside にある 1 つ

のホストと Outside にある 1 つのホストが許可されています。pix(config)#**ssh 172.16.1.1 255.255.255.255 inside** pix(config)#**ssh 10.1.1.2 255.255.255.255 outside**

4. **オプション：** デフォルトで、セキュリティ アプライアンス モデルは SSH バージョン 1 を可能にし、バージョン 2.は特定のバージョンへの接続を制限するためにこのコマンドを入力します:pix(config)# **ssh version** *<version_number>* **注:** version_number は 1 または 2 です。
5. **オプション：** デフォルトでは、5 分間無活動になった後 SSH セッションは終了されます。このタイムアウトは、1 ~ 60 分間継続するように設定できます。pix(config)#**ssh timeout** *minutes*

SSH クライアントの使用方法

SSH セッションを開いている間に、PIX 500 シリーズ セキュリティ アプライアンスのユーザ名とログイン パスワードを入力します。 SSH セッションを開始すると、SSH ユーザ認証プロンプトが表示される前に、セキュリティ アプライアンス コンソールではドット (.) が表示されます。

```
hostname(config)# .
```

ドットが表示されていても SSH の機能には影響しません。 ドットがコンソールに表示されるのは、ユーザ認証が行われる前、SSH 鍵交換中にサーバ鍵が生成されるか、メッセージが秘密鍵で復号化される時点です。 これらのタスクは、最長で 2 分間以上を要する場合があります。 ドットは進行状況のインジケータで、セキュリティ アプライアンスがビシー状態でありハングしていないことを確認するものです。

SSH バージョン 1.x と 2 はまったく異なるプロトコルであるため、互換性はありません。 互換性のあるクライアントをダウンロードします。 詳細は、『拡張設定』の「SSH クライアントの入手」セクションを参照してください。

PIX の設定

このドキュメントでは次の設定を使用しています。

PIX の設定

```
PIX Version 7.1(1)
!
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.16.5.10 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp permit any outside
```

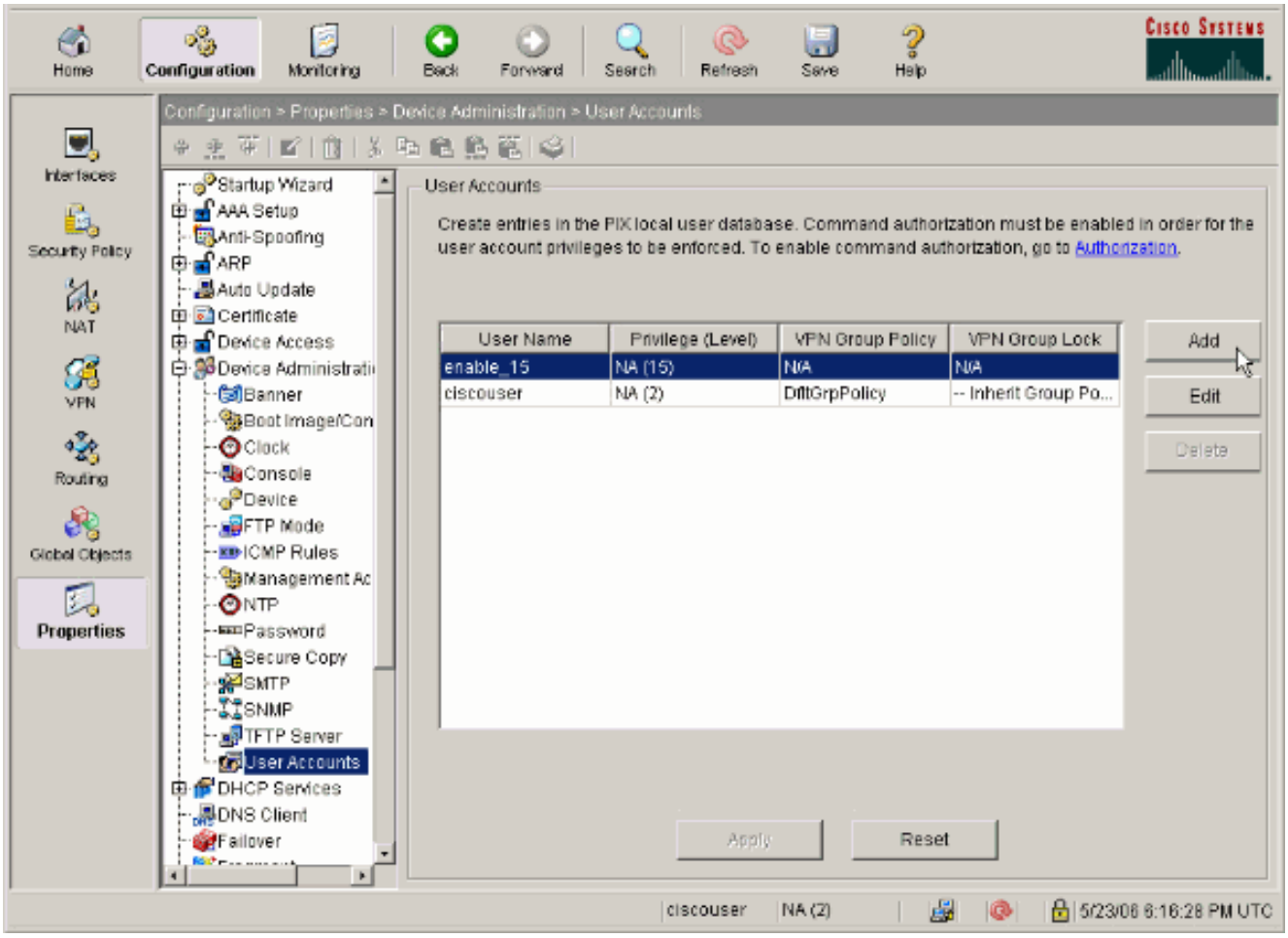
```
no asdm history enable
arp timeout 14400
route outside 10.1.1.0 255.255.255.0 192.168.200.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- AAA for the SSH configuration username ciscouser
password 3USUcOPFUiMCO4Jk encrypted aaa authentication
ssh console LOCAL http server enable http 172.16.0.0
255.255.0.0 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 10.1.1.2 255.255.255.255 outside !---
Allows the users on the host 172.161.1.1 !--- to access
the security appliance !--- on the inside interface. ssh
172.16.1.1 255.255.255.255 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
Cryptochecksum:a6b05fd04f9fbd0a39f1ca7328de91f7 : end
```

注: SSH を使用して ASA/PIX の管理インターフェイスにアクセスするには、次のコマンドを発行します。 `ssh 172.16.16.160 255.255.255.255 Management`

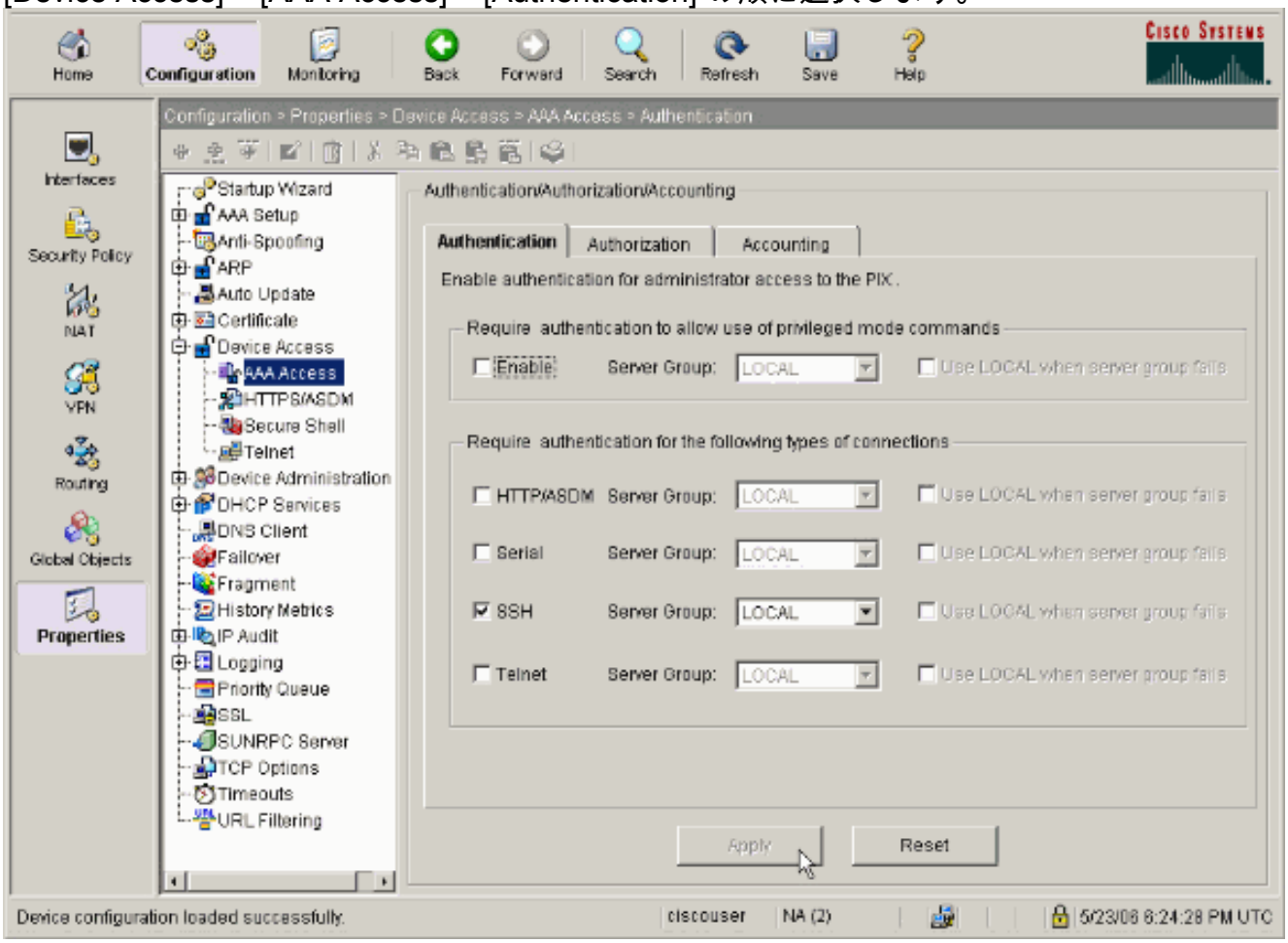
ASDM 5.x を使用した設定

ASDM を使用して SSH 向けにデバイスを設定するには、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] > [Properties] > [Device Administration] > [User Accounts] の順に選択します。

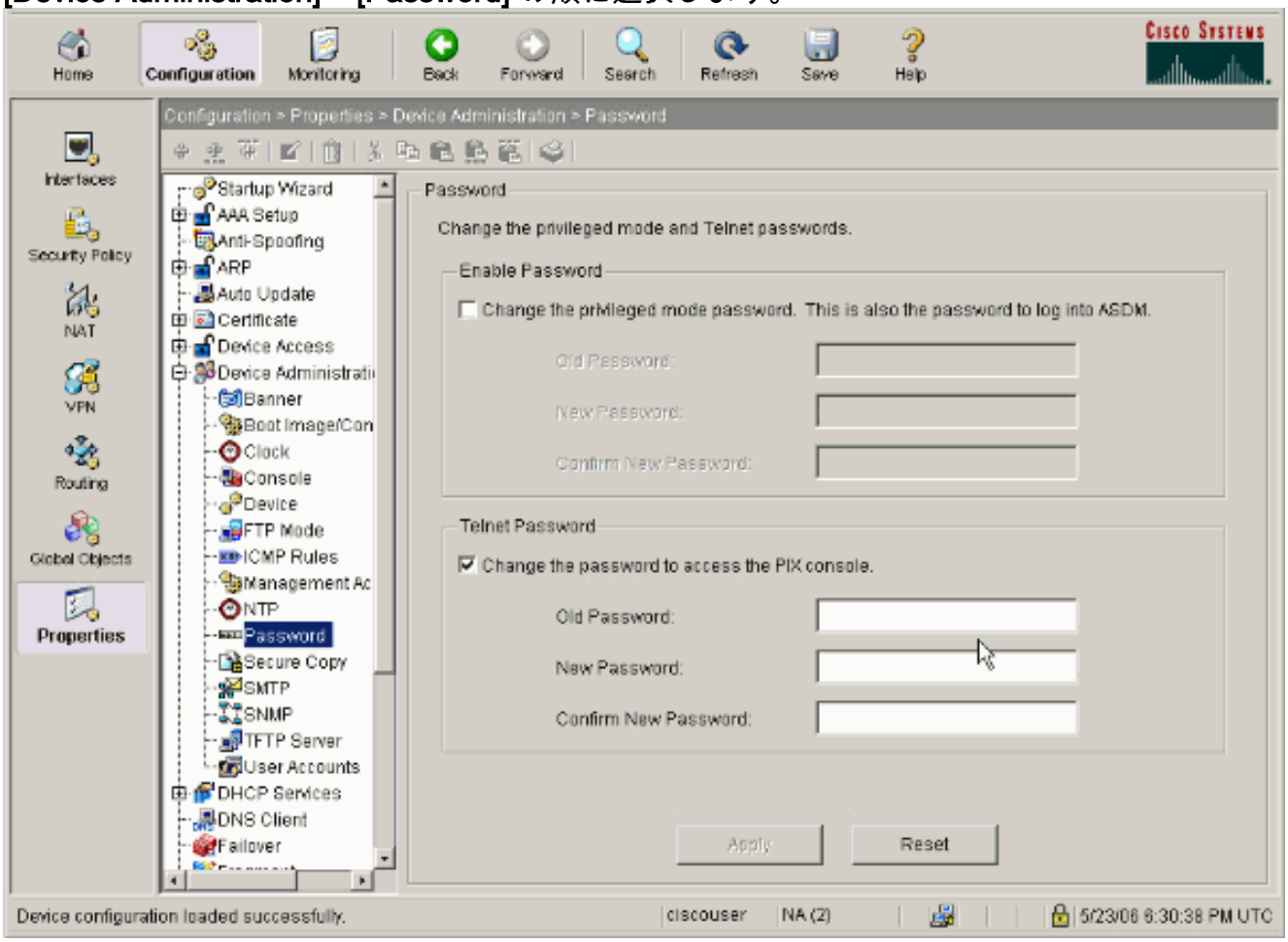


2. ASDM を使用して SSH 用の AAA 認証を設定するには、[Configuration] > [Properties] > [Device Access] > [AAA Access] > [Authentication] の順に選択します。

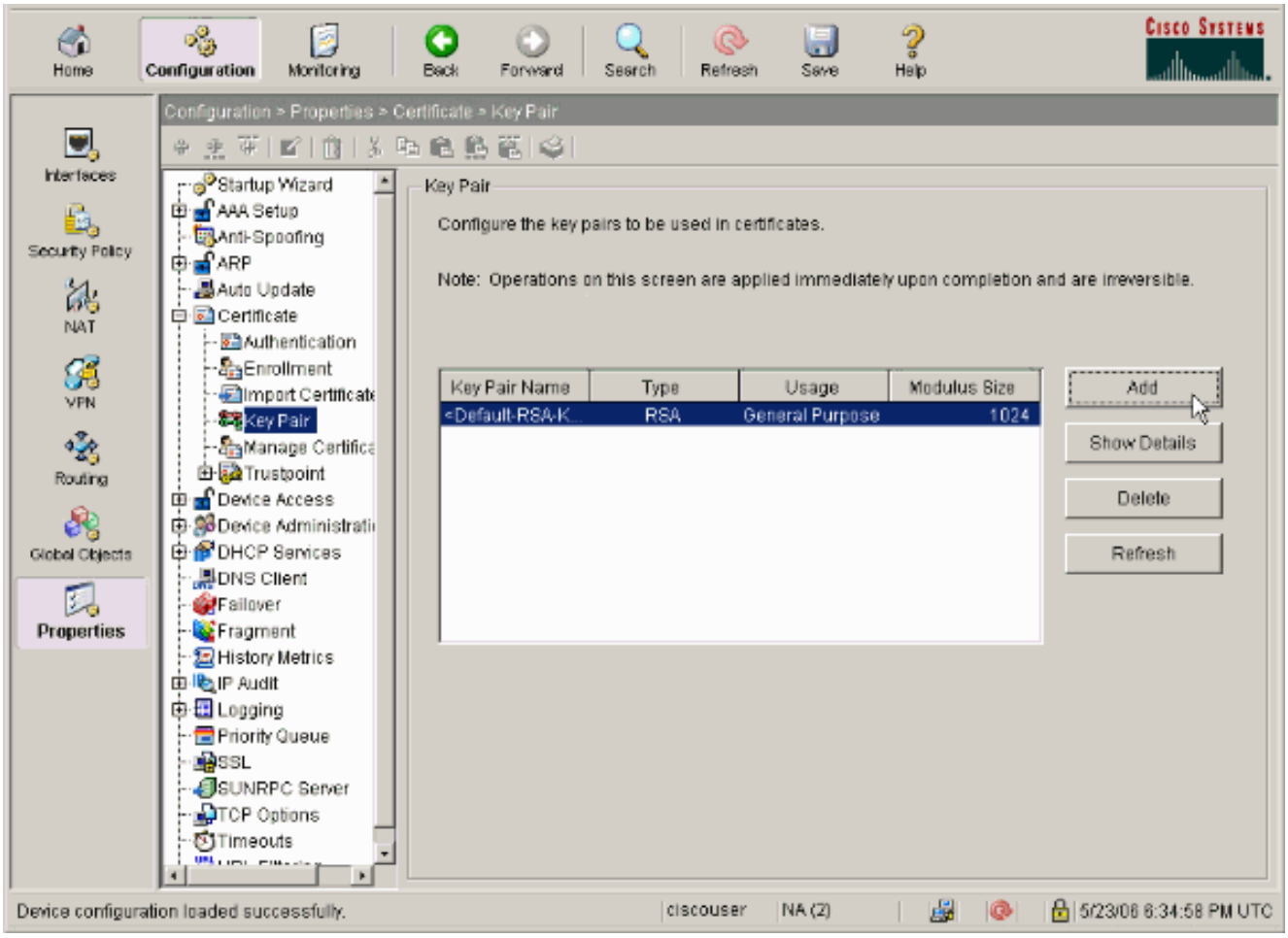


3. ASDM を使用して Telnet パスワードを変更するには、**[Configuration] > [Properties] >**

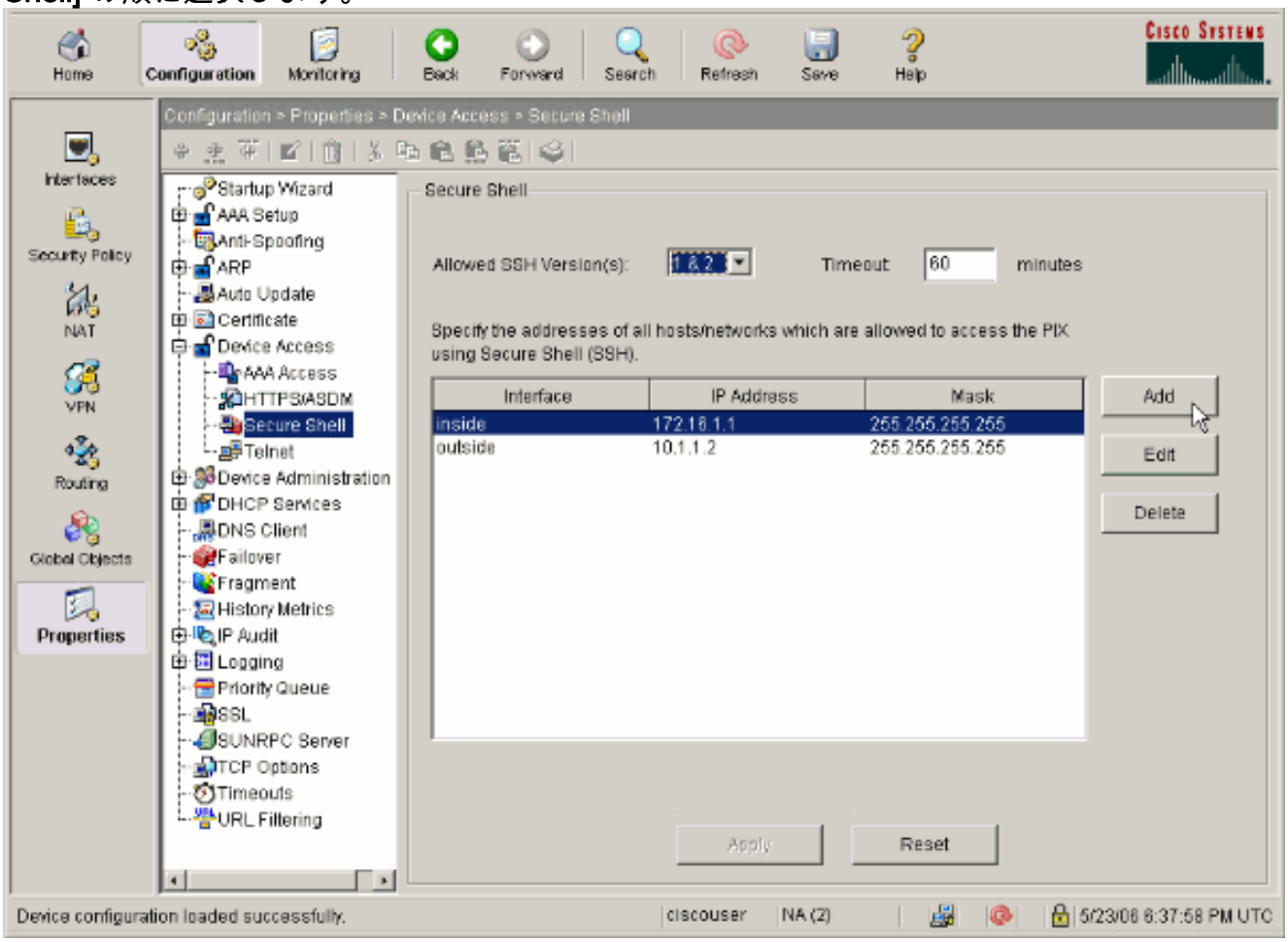
[Device Administration] > [Password] の順に選択します。



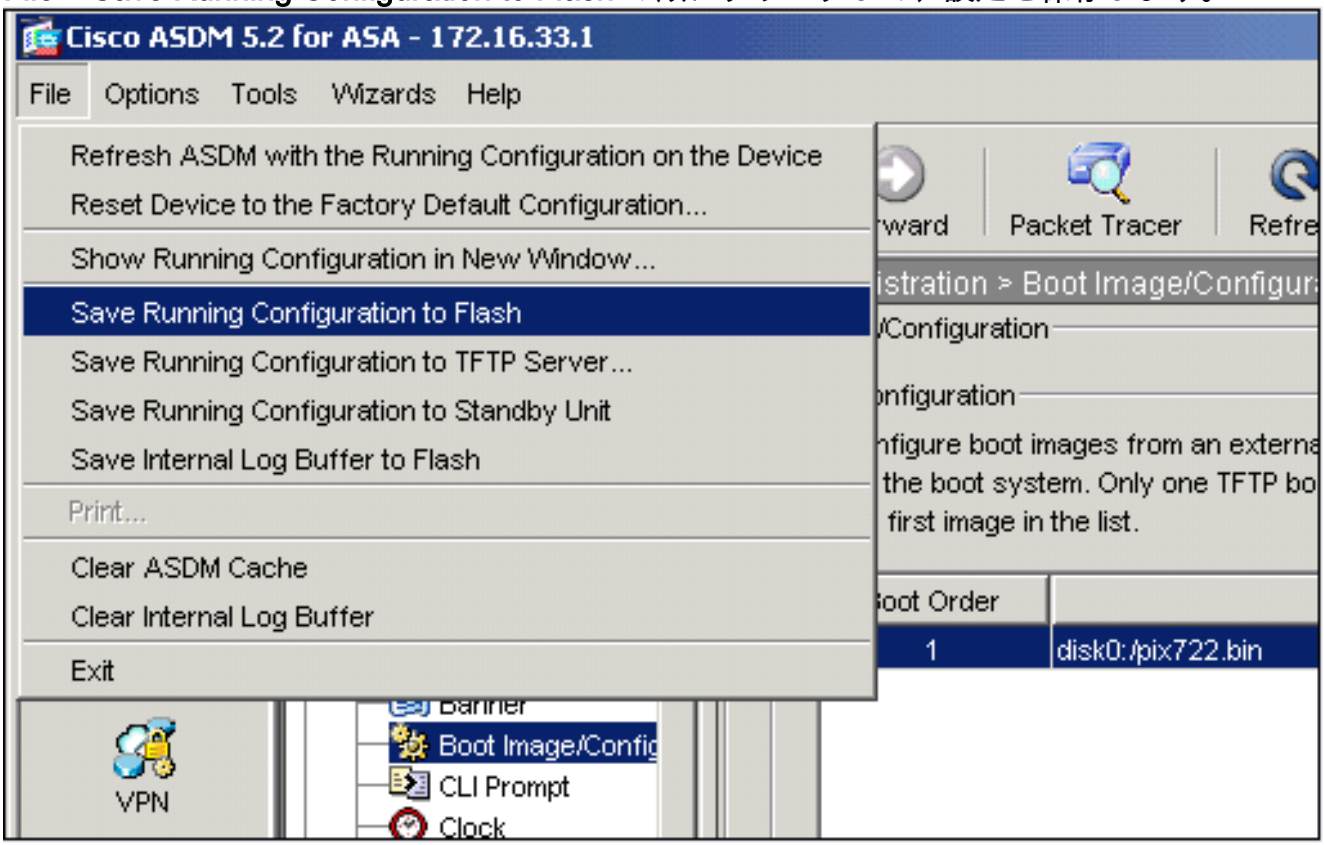
4. ASDM を使用して同じ RSA 鍵を生成するには、[Configuration] > [Properties] > [Certificate] > [Key Pair] の順に選択し、[Add] をクリックして、表示されるデフォルトのオプションを使用します。



5. ASDM を使用して SSH による接続を許可するホストを指定し、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] > [Properties] > [Device Access] > [Secure Shell]** の順に選択します。



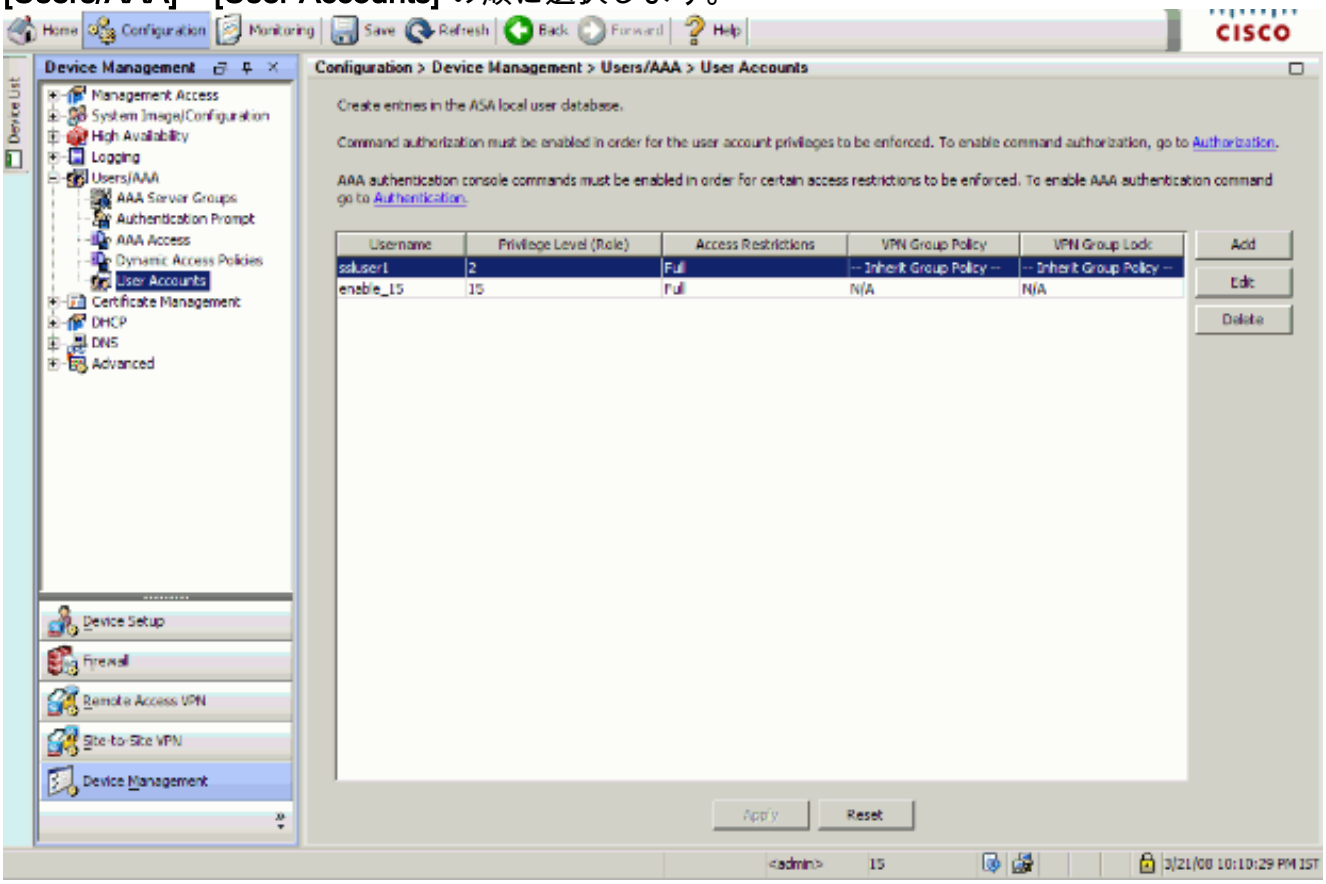
6. File > Save Running Configuration to Flash の順にクリックして、設定を保存します。



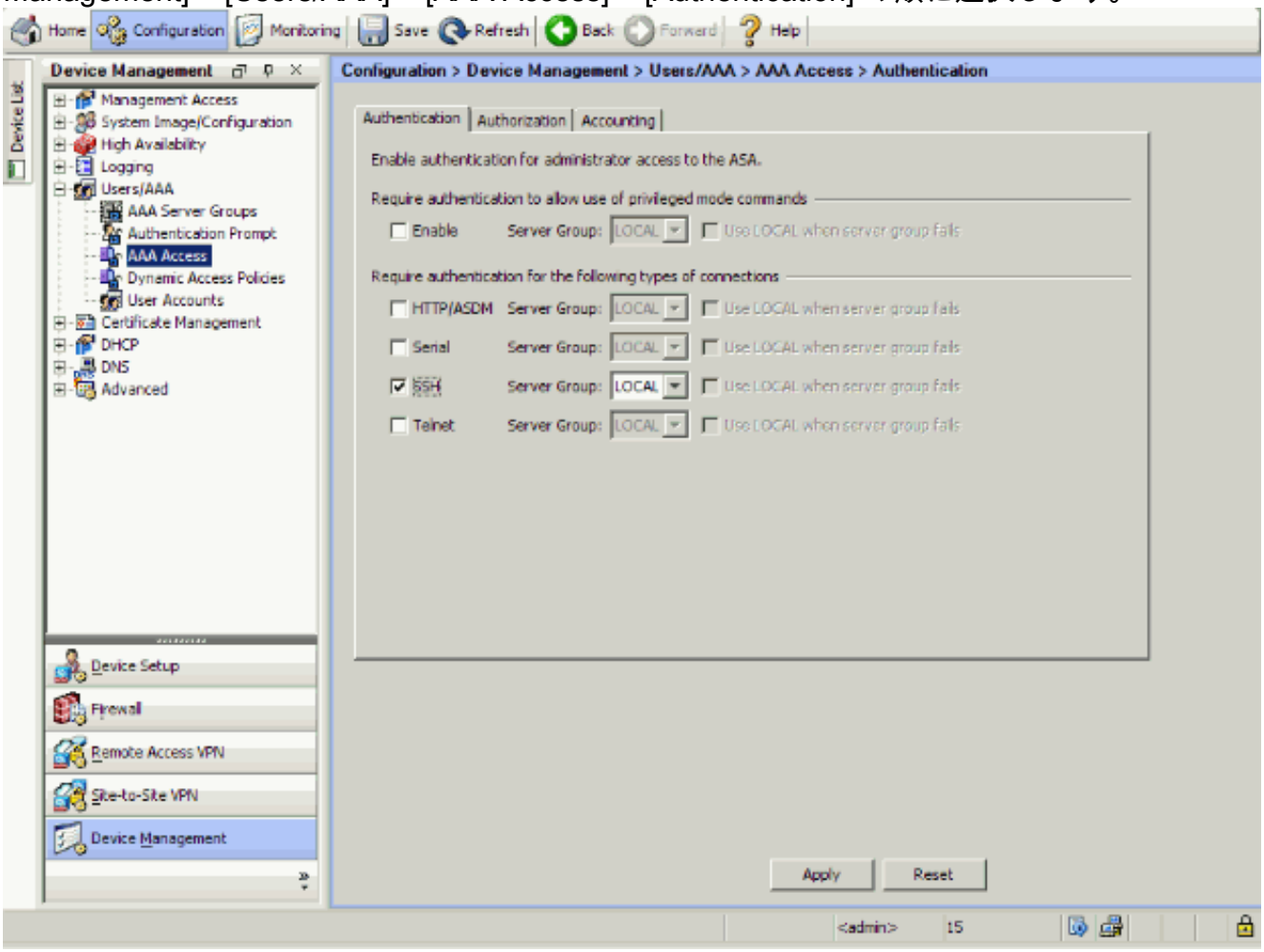
ASDM 6.x を使用した設定

次の手順を実行します。

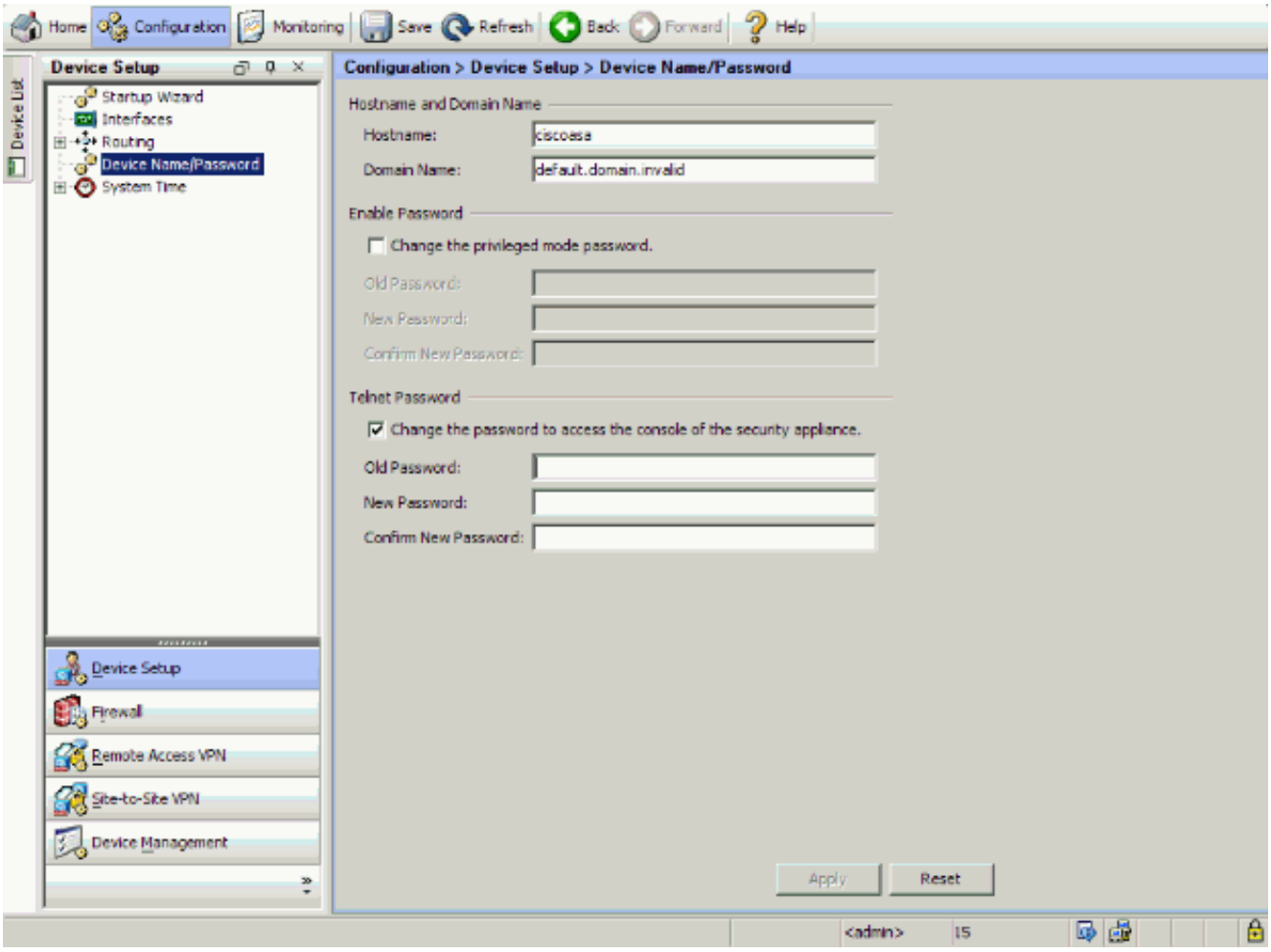
1. ASDM を使用してユーザを追加するには、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] の順に選択します。



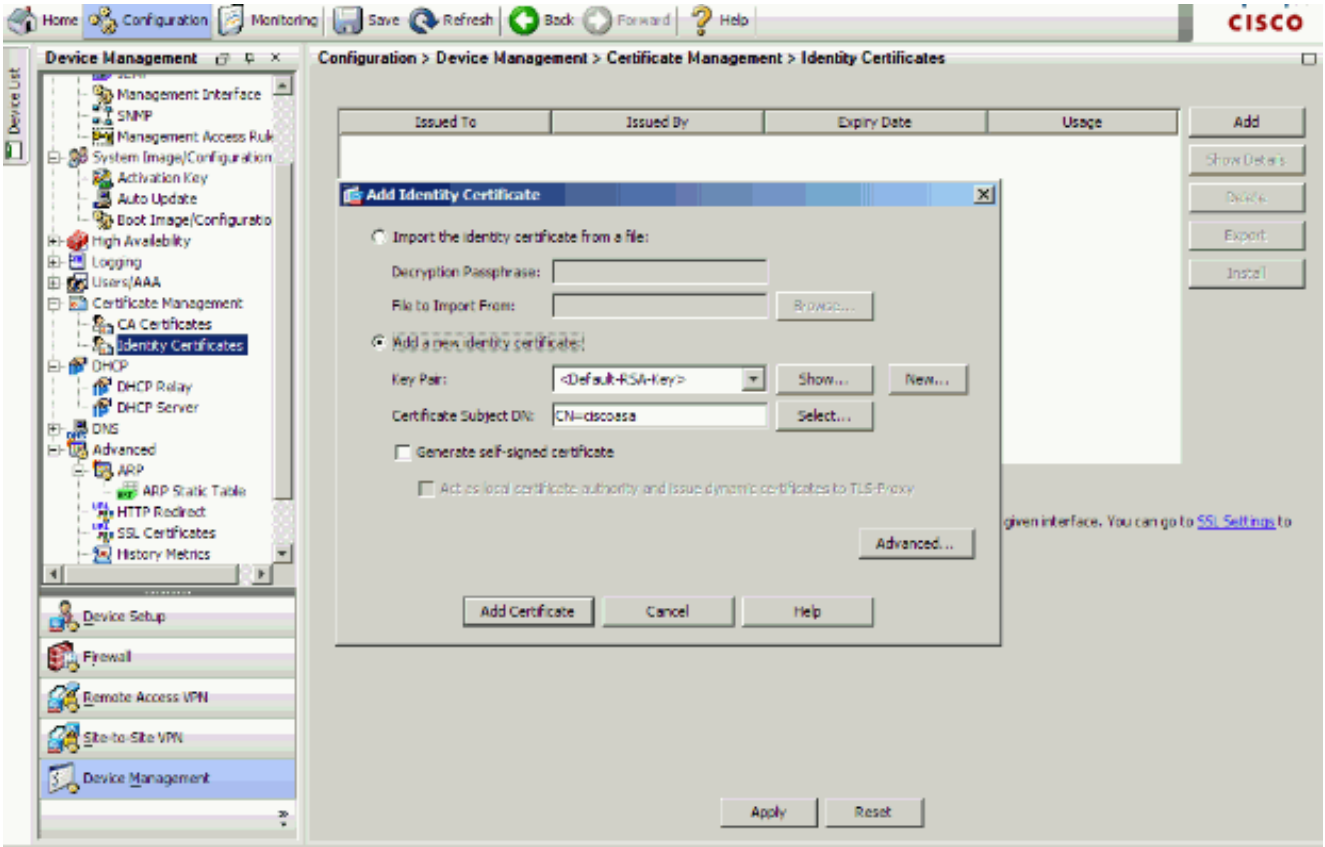
2. ASDM を使用して SSH 用の AAA 認証を設定するには、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] の順に選択します。



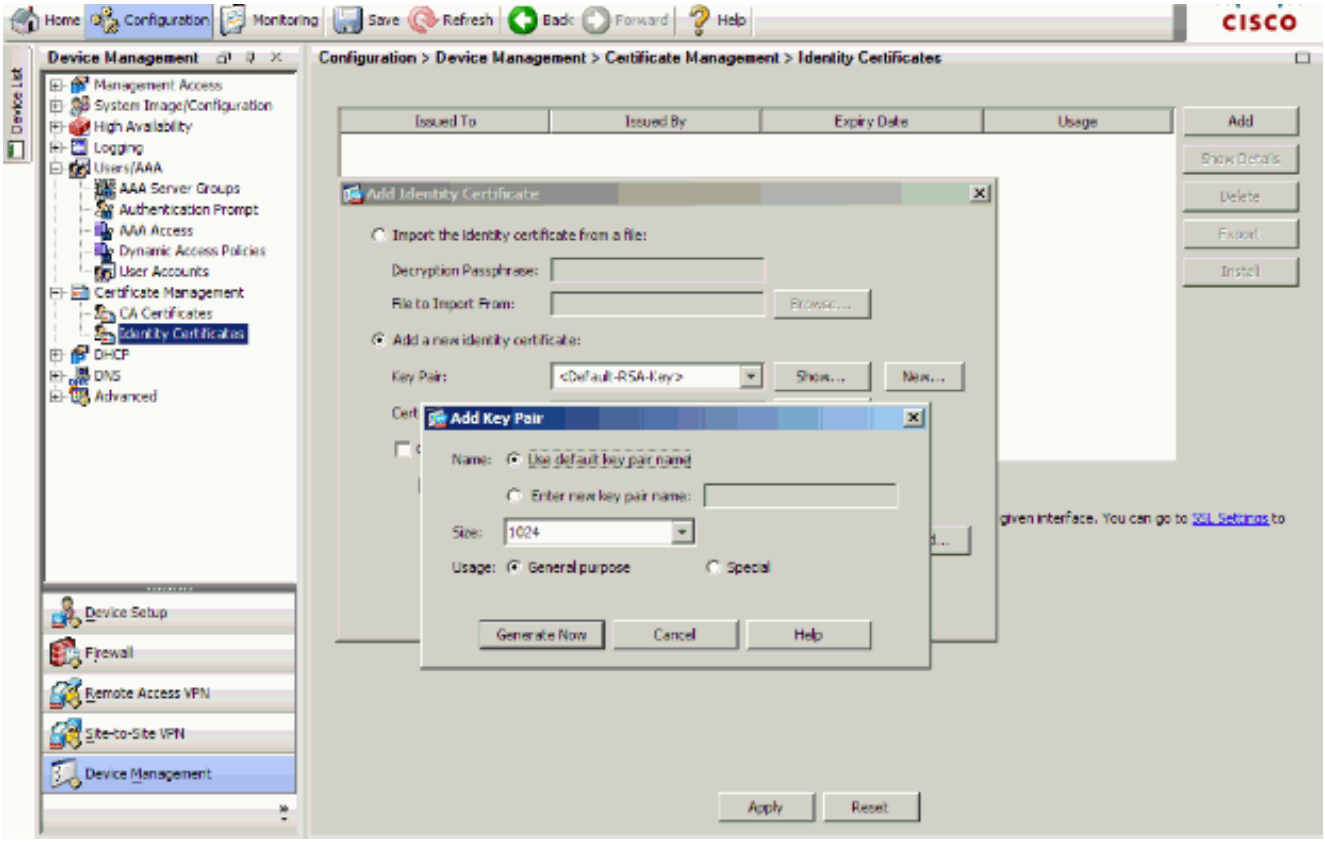
3. ASDM を使用して Telnet パスワードを変更するには、[Configuration] > [Device Setup] > [Device Name/Password] の順に選択します。



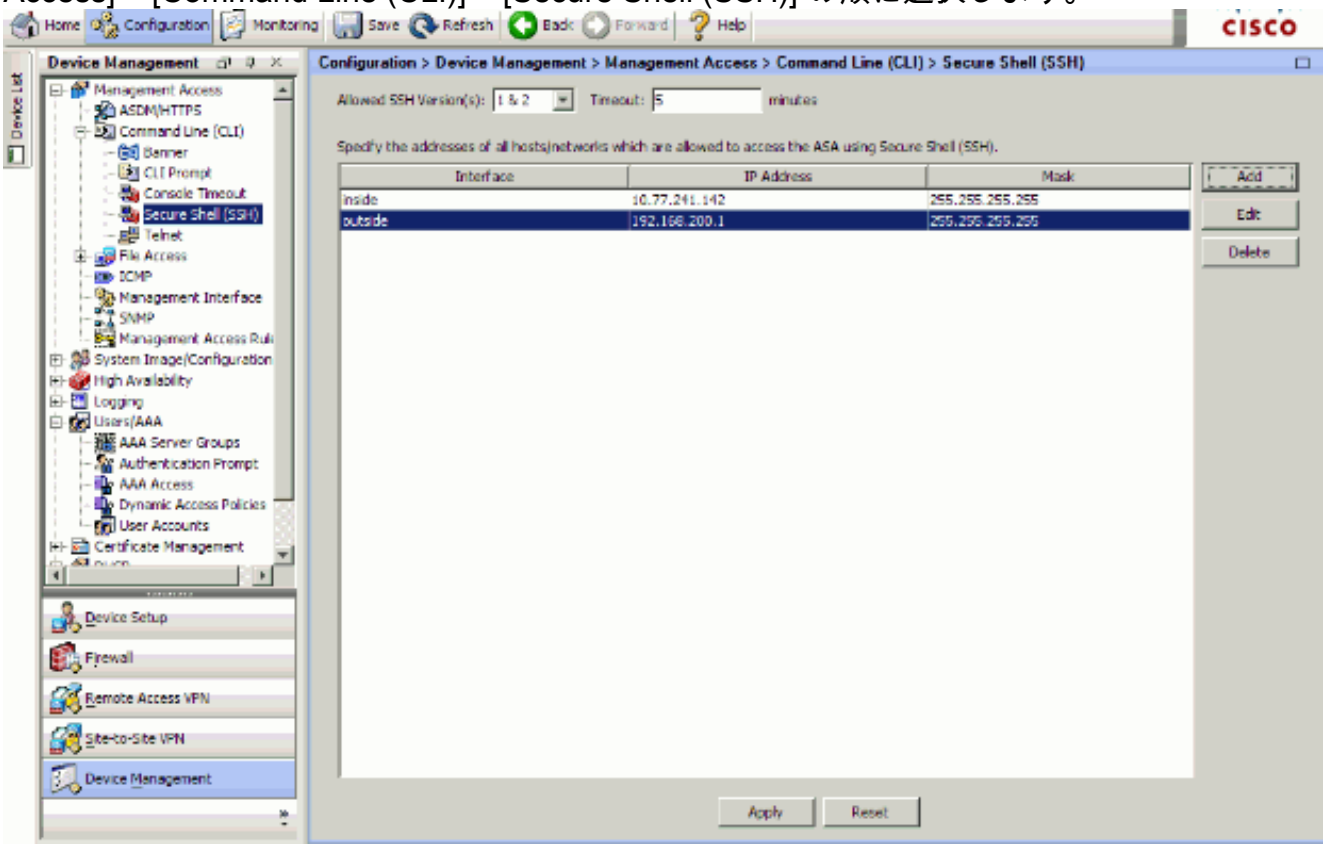
4. ASDM を使用して同じ RSA 鍵を生成するには、[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] の順に選択し、[Add] をクリックして、表示されるデフォルトのオプションを使用します。



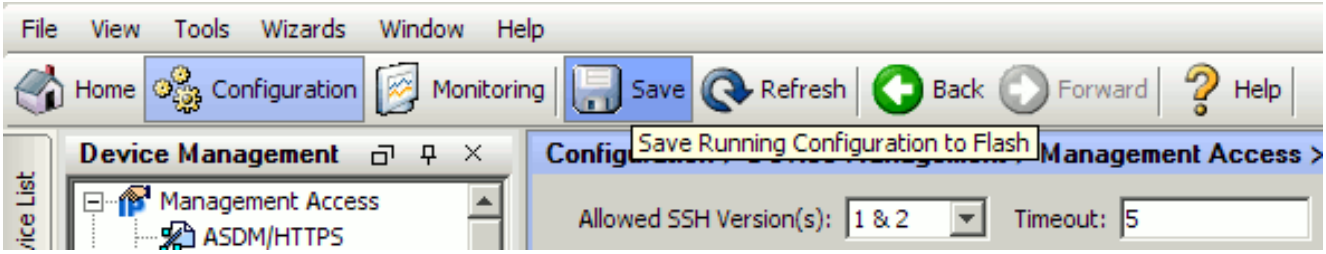
5. デフォルトの鍵ペアが存在しない場合にこれを追加するには、[**Add a new Identity certificate**] の下で [**New**] をクリックします。 次に、[Generate Now] をクリックします。



6. ASDM を使用して SSH による接続を許可するホストを指定し、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)] の順に選択します。



7. ウィンドウの上部にある **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** コマンドを発行します。 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 コマンドを使用すると、Telnet を使用してセキュリティ 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できます。

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 アプライアンスにより、Outside インターフェイスへのすべての Telnet トラフィックが IPSec で保護されます。 Outside 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 Outside インターフェイス上で IPSec を設定し、Outside 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インターフェイスの場合、PIX/ASA ではそのインターフェイスへの Telnet が許可されません。

注: Telnet セッションを通じてセキュリティ アプライアンスに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。 Telnet のサーバ/クライアント通信はクリア テキストのみで行われます。 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。

IP アドレスを入力する場合は、ネットマスクも入力する必要があります。 デフォルトのネットマスクはありません。 内部ネットワークのサブネットワーク マスクは使用しないでください。 ネットマスクは IP アドレスのビット マスクにすぎません。 アクセスを 1 つの IP アドレスに制限するには、各オクテットで 255 を使用します（255.255.255.255 など）。

IPSec が稼働している場合、セキュリティで保護されていないインターフェイス名（通常は Outside インターフェイス）を指定できます。 少なくとも、**crypto map** コマンドを設定すると、**telnet** コマンドを使用してインターフェイス名を指定できます。

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** コマンドを発行します。 デフォルトは cisco です。 どの IP アドレスが現時点でセキュリティ アプライアンス コンソールにアクセスしているかを表示するには、**who** コマンドを発行します。 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** コマンドを発行します。

Inside インターフェイスへの Telnet セッションを有効にするには、次の例を参照してください。

例 1

この例では、ホスト 10.1.1.1 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。

```
pix(config)#telnet 10.1.1.1 255.255.255.255 inside
```

例 2

この例では、ネットワーク 10.0.0.0/8 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。

```
pix(config)#telnet 10.0.0.0 255.0.0.0 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。

```
pix(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 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
```

ACS 4.x での SSH/Telnet のサポート

RADIUS の機能について見ると、SSH 機能向けに RADIUS が使用できます。

Telnet、SSH、HTTP、またはシリアル コンソール接続を使用してセキュリティ アプライアンスにアクセスしようとして、トラフィックが認証設定に一致すると、セキュリティ アプライアンスからユーザ名とパスワードが要求されます。 続いてセキュリティ アプライアンスは RADIUS (ACS) サーバにこれらのクレデンシャルを送信し、サーバからの応答に基づいて CLI アクセスを許可または拒否します。

詳細は、『AAA サーバとローカル データベースの設定』の「AAA サーバとローカル データベースのサポート」を参照してください。

たとえば、次のように、ASA セキュリティ アプライアンス 7.0 には、セキュリティ アプライアンスが接続を受け入れる IP アドレスが必要です。

```
hostname(config)#ssh source_IP_address mask source_interface
```
詳細は、『AAA サーバとローカル データベースの設定』の「SSH アクセスの許可」を参照してください。

Cisco ASA をバージョン 8.2 以前と同じ構成にする場合は、『PIX/ASA： TACACS+ および RADIUS サーバを使用したネットワーク アクセスのカットスルー プロキシの設定例』を参照してください。

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。

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 のデバッグをオンにするには、**debug ssh** コマンドを発行します。

```
pix(config)#debug ssh SSH debugging on
```
次の出力は、ホスト 10.1.1.2（PIX の Outside）から pix への認証要求が成功したことを示しています。

```
pix#
Device ssh opened successfully.
   SSH0: SSH client: IP = '10.1.1.2' interface # = 1
   SSH: host key initialised
   SSH0: starting SSH control process
   SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
   SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows
client version string:SSH-1.99-3.2.0 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 receivedSSH(pix): user authen method is
'no AAA', aaa server group ID = 0
   SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication successful for pix !--- Authentication for the PIX 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
```
pix ではなく pix1 のように、ユーザが正しくないユーザ名を入力した場合、PIX Firewall 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。

```
pix#
```

```
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows client version
    string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1960 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 receivedSSH(pix1): user authen method is
'no AAA', aaa server group ID = 0
SSH(pix1): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix1 !--- Authentication for pix1 was not successful due to
the wrong username.
```

同様に、ユーザが正しくないパスワードを入力した場合、デバッグ出力では認証に失敗したことが示されます。

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2'  interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL server version string:
SSH-1.99-Cisco-1.25SSH0: receive      SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for
Windows client version string:SSH-1.99-3.2.0
SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1920 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 receivedSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
     SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pixSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix !--- Authentication for PIX was not successful due to the
wrong password.
```

アクティブな SSH セッションの表示

接続されている SSH セッションの数、および PIX に対する接続状態を確認するには、次のコマンドを発行します。

```
pix#show ssh session SID Client IP Version Mode Encryption Hmac State Username 0 10.1.1.2 1.99
IN aes128-cbc md5 SessionStarted pix OUT aes128-cbc md5 SessionStarted pix
```

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] の順に選択します。

公開 RSA 鍵の表示

セキュリティ アプライアンス上の RSA 鍵の公開部分を表示するには、次のコマンドを発行します。

```
pix#show crypto key mypubkey rsa Key pair was generated at: 19:36:28 UTC May 19 2006 Key name:
<Default-RSA-Key> Usage: General Purpose Key Modulus Size (bits): 1024 Key Data: 30819f30
0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c172f4 95f66c34 2c2ced37 aa3442d8
12158c93 131480dd 967985ab 1d7b92d9 5290f695 8e9b5b0d d88c0439 6169184c d8fb951c 19023347
d6b3f939 99ac2814 950f4422 69b67328 f64916b1 82e15341 07590da2 390fbefd 38758888 7319196c
de61aef1 165c4bab 03d081d5 ddaf15cc c9ddb204 c2b451e0 f19ce0f3 485b1d69 8b020301 0001
```

Configuration > Properties > Certificate > Key Pair の順に選択 し、ASDM の RSA キーを表示するために『Show Details』 をクリック して下さい。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

PIX から RSA 鍵を削除する方法

PIX ソフトウェアをアップグレードしたり、PIX の SSH バージョンを変更する場合など、状況によっては RSA キーを削除して再作成することが必要になる場合があります。 PIX から RSA 鍵ペアを削除するには、次のコマンドを発行します。

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

Configuration > Properties > Certificate > Key Pair の順に選択 し、ASDM と RSA キーを削除するために『Delete』 をクリック して下さい。

SSH 接続に失敗する

PIX/ASA で次のエラー メッセージが表示されます。

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

それに対応して、SSH クライアント マシンには、次のエラー メッセージが表示されます。

```
Selected cipher type <unknown> not supported by server.
```

この問題を解決するには、RSA 鍵を削除し、再作成します。 ASA から RSA 鍵ペアを削除するには、次のコマンドを発行します。

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

新しい鍵を生成するには、次のコマンドを発行します。

```
ASA(config)# crypto key generate rsa modulus 1024
```

SSH を使用して ASA にアクセスできない

エラー メッセージ：

```
ssh_exchange_identification: read: Connection reset by peer
```

この問題を解決するには、次の手順を実行します。

1. ASA をリロードするか、または SSH に関連したすべての設定および RSA 鍵を削除します。
2. SSH コマンドを再構成して、RSA 鍵を再生成します。

SSH を使用してセカンダリ ASA にアクセスすることが不可能

ASA はフェールオーバー モードにあるとき、VPN トンネルによってスタンバイ ASA に SSH に可能性のあるではないです。 これは SSH のための応答トラフィックがスタンバイ ASA の outside インターフェイスを戻すという理由によります。

関連情報

- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- SSH 接続の設定：Cisco ルータおよび Cisco コンセントレータ
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems