CiscoクラウドEメールセキュリティCLIアクセスのリクエスト

内容

はじめに

このドキュメントでは、クラウドEメールセキュリティ(CES)CLIへのアクセスを要求する方法について説明します。

背景説明

Cisco CESをご利用のお客様は、SSHプロキシを通じて提供されるESAとSMAのCLIに、キー認証を使用してアクセスできます。ホステッドアプライアンスへのCLIアクセスは、組織内の主要な個人に制限する必要があります。

LinuxおよびMacユーザ

Cisco CESのお客様：
CESプロキシ経由でCLIアクセスを行うための、SSHを利用したシェルスクリプトの手順。

前提条件

CESカスタマーとして、SSHキーの交換と配置を行うには、CESオンボーディング/運用部門、またはCisco TACと契約する必要があります。

1. プライベート/パブリックRSAキーを生成します。
2. CiscoにyourPublicRSAキーを提供します。
3. シスコがキーを保存し、CESカスタマーアカウントにキーが保存されたことを通知するまで待ちます。
4. connect2ces.shスクリプトをコピーして変更します。

プライベート/パブリックRSAキーの作成方法

Unix/Linux/OS Xのターミナル/CLIで「ssh-keygen」を使用することをお勧めします。ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NAME>コマンドを使用します。

注：詳細については、https://www.ssh.com/academy/ssh/keygenを参照してください。
RSA秘密鍵へのアクセスを常に保護するようにしてください。
秘密キーはシスコに送信しないでください。公開キー(.pub)のみを送信してください。
公開キーをシスコに送信する際には、キーの送信先の電子メールアドレス、名、姓を特定してください。

公開キーを提供するためにシスコサポートリクエストをオープンするにはどうしたらよいですか。

このリンクに移動します。

SRが「Cisco CES Customer SSH/CLI Setup」などのように正しく識別されていることを確認します。

コンフィギュレーション

開始するには、opencopy the scriptによって提供され、ホスト名にこれらのプロキシホストのいずれかを使用します。

各地域に適したプロキシを選択していることを確認してください(つまり、US CESをご利用の場合、F4データセンターおよびアプライアンスにアクセスするには、f4-ssh.iphmx.comを使用します。EU CESをご利用で、ドイツのDCにあるアプライアンスを使用している場合は、f17-ssh.eu.iphmx.comを使用してください)。

アクセスポイント(ap.iphmx.com)
f15-ssh.ap.ip hmx.com
f16-ssh.ap.ip hmx.com

CA(ca.iphmx.com)

f13-ssh.ca.ip hmx.com
f14-ssh.ca.ip hmx.com

EU(c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

EU(eu.iphmx.com)（ドイツのDC）
f17-ssh.eu.ip hmx.com
f18-ssh.eu.ip hmx.com

米国(iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com

複数のEメールセキュリティアプライアンス(ESA)またはセキュリティ管理アプライアンス(SMA)に接続する場合はどうすればよいですか。

connect2ces.shの2番目のコピー(connect2ces_2.shなど)をコピーして保存します。

注:「cloud_host」を、アクセスする追加アプライアンスとして編集します。「local_port」を2222以外に編集する必要があります。そうでない場合は、「WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!」というエラーが表示されます。

パスワードの入力を求めるプロンプトを表示せずにログインするようにESAまたはSMAを設定するにはどうすればよいですか。

このガイドをお読みください。

前提条件を満たしたら、どのようになりますか。

joe.user@my_local > ~ ./connect2ces
[-]プロキシサーバー(f4-ssh.iphmx.com)に接続しています…
[-]プロキシ接続に成功しました。これでf4-ssh.iphmx.comに接続されました。
[-] PID 31253で実行されているプロキシ
[-] CESアプライアンス(esa1.rs1234-01.iphmx.com)に接続しています…

最終ログイン：2019年4月22日（月）10.123.123.123から11:33:45
AsyncOS 12.1.0 for Cisco C100Vビルド071

Cisco C100V Eメールセキュリティ仮想アプライアンスへようこそ

注：このセッションは、アイドル状態が1440分間続くと期限切れになります。コミットされていない設定変更はすべて失われます。設定の変更を行ったらすぐにコミットします。

(マシンesa1.rs1234-01.iphmx.com)>
(マシンesa1.rs1234-01.iphmx.com)>終了

127.0.0.1への接続が閉じられました。
[-]プロキシ接続を閉じています…
[-]完了。

connect2ces.sh（接続2ces.sh）

注：各地域に適したプロキシを選択していることを確認してください(つまり、US CESの顧客は、F4データセンターおよびアプライアンスにアクセスするために、f4-ssh.iphmx.comを使用します。EU CESをご利用で、ドイツのDCにあるアプライアンスを使用している場合は、f17-ssh.eu.iphmx.comを使用してください)。

#!/bin/bash

次#--値を編集してください----------
#次の値はCESですでに設定されています。
cloud_user="username"
cloud_host="esaX.CUSTOMER.iphmx.com"または"smaX.CUSTOMER.iphmx.com"
[各地域のCESデータセンターが正しく設定されていることを確認します。]
private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
proxy_server="PROXY_SERVER" [1つだけ選択してください！]
#
'proxy_server'の場合、SSHプロキシは次のようになります。
##
AP(ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com
##
CA (ca.iphmx.com)
f13-ssh.ca.iphmx.com
f14-ssh.ca.iphmx.com
##
EU (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com
##
EU (eu.iphmx.com)（ドイツのDC）
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com
##
##米国(iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com

```
cloud_user="ユーザ名"
cloud_host="esaX.CUSTOMER.iphmx.com"
private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
proxy_server="PROXY_SERVER"

こ#--らの値は----------のまま
# 'proxy_user'は変更できません
# 'remote_port'は22のまま(SSH)
# 'local_port'は、必要に応じて異なる値に設定できます

proxy_user="dh-user"
remote_port=22
local_port=2222

#--この行の下では編集しないでください----------

proxycmd="ssh -f -L $local_port:$cloud_host:$remote_port -i $private_key -N
$proxy_user@$proxy_server"

printf "[-]プロキシサーバー($proxy_server)に接続しています…\n"
$proxycmd >/dev/null 2>&1
nc -z 127.0.0.1 $local_port >/dev/null 2>&1の場合、
printf "[-]プロキシ接続に成功しました。$proxy_server.\nに接続されました。
else
printf "[-]プロキシ接続に失敗しました。終了しています…\n"
exit
fi

#プロキシSSHプロセスの検索
proxypid='ps -xo pid,command | grep "$cloud_host" | grep "$proxy_server" | head -n1 | sed "s/^[
\t]*//" | cut -d " " " -f1'
printf "[-] proxy running on PID: $proxypid\n"

printf "[-] CESアプライアンス($cloud_host)に接続しています…\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

printf "[-]プロキシ接続を閉じています…\n"
kill $proxypid

printf "[-]完了。\n"

#--毎回パスワードを入力する必要がないようにしますか？
#--覧：https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-
technote-esa-00.html
#--複数のESAまたはSMAへのアクセスが必要ですか。同じスクリプトをコピーして、名前を
connect2ces_2.shまたは同様の名前に変更します。
```

元のドキュメント：https://github.com/robsherw/connect2ces。

Windowsユーザー

CESプロキシ経由でCLIアクセスを行うためにPuTTYを使用し、SSHを使用する手順。

前提条件

CESカスタマーとして、CESオンボーディング/運用部門、またはCisco TACにSSHキーの交換と配置を依頼する必要があります。

1. プライベート/パブリックRSAキーを生成します。
2. 公開 RSAキーをCiscoに提供します。
3. シスコがキーを保存し、CESカスタマーアカウントにキーが保存されたことを通知するまで待ちます。
4. 次の手順に従ってPuTTYをセットアップします。

プライベート/パブリックRSAキーの作成方法

WindowsではPuTTYgen(https://www.puttygen.com/)を使用することを推奨します。

詳細については、https://www.ssh.com/ssh/putty/windows/puttygenを参照してください。

注:RSA秘密鍵へのアクセスが常に保護されていることを確認してください。
秘密キーはシスコに送信しないでください。公開キー(.pub)のみを送信してください。
公開キーをシスコに提出する際には、公開キーの対象となる電子メールアドレス、名、姓を特定してください。

公開キーを提供するためにシスコサポートリクエストをオープンするにはどうしたらよいですか。

このリンクに移動します。

SRが「Cisco CES Customer SSH/CLI Setup」などのように正しく識別されていることを確認します。

パスワードの入力を求めるプロンプトを表示せずにログインするようにESAまたはSMAを設定するにはどうすればよいですか。

このガイドをお読みください。

PuTTyの設定

開始するには、PuTTYを開いて、ホスト名に次のプロキシホストのいずれかを使用します。

各地域に適したプロキシを選択していることを確認してください(つまり、US CESをご利用の場

合、F4データセンターおよびアプライアンスにアクセスするには、f4-ssh.iphmx.comを使用します。EU CESをご利用で、ドイツのDCにあるアプライアンスを使用している場合は、f17-ssh.eu.iphmx.comを使用してください)。

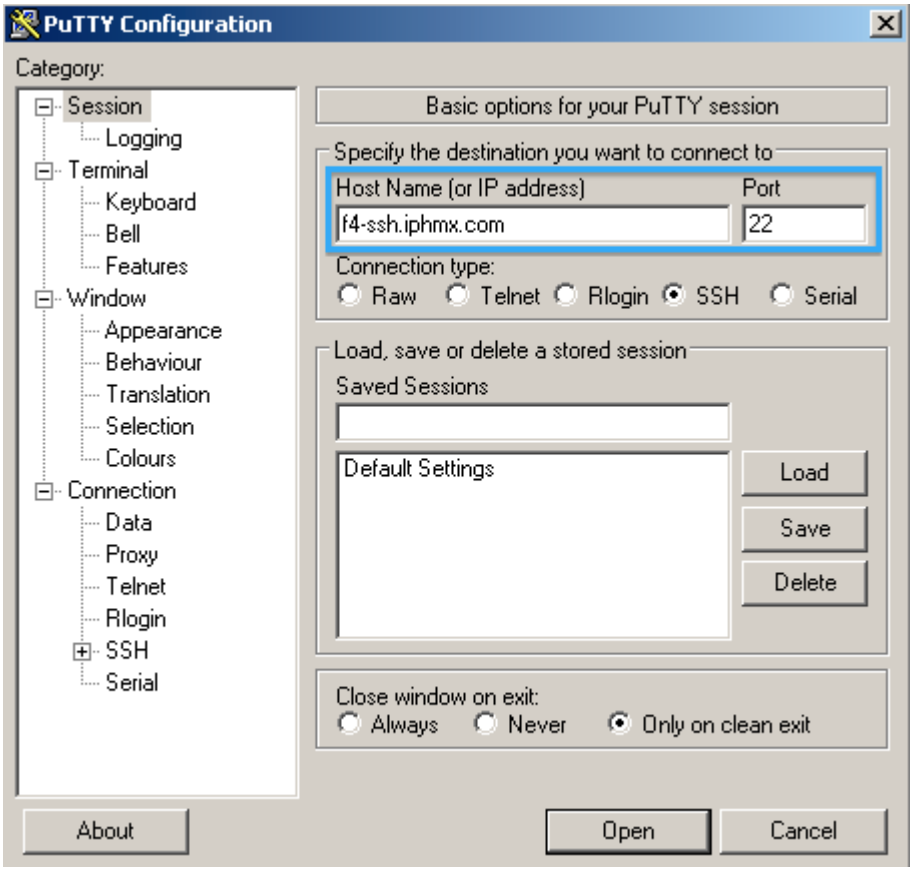
アクセスポイント(ap.iphmx.com)
f15-ssh.ap.ip hmx.com
f16-ssh.ap.ip hmx.com

CA(ca.iphmx.com)
f13-ssh.ca.ip hmx.com
f14-ssh.ca.ip hmx.com

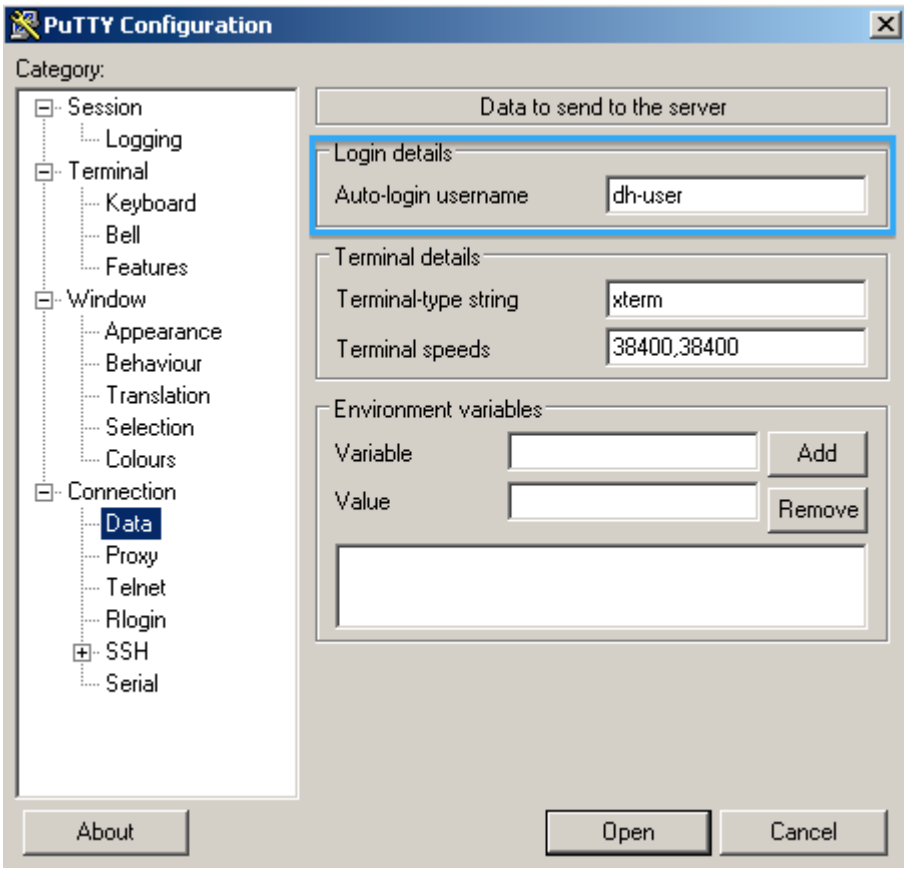
EU(c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

EU(eu.iphmx.com) (ドイツのDC)
f17-ssh.eu.ip hmx.com
f18-ssh.eu.ip hmx.com

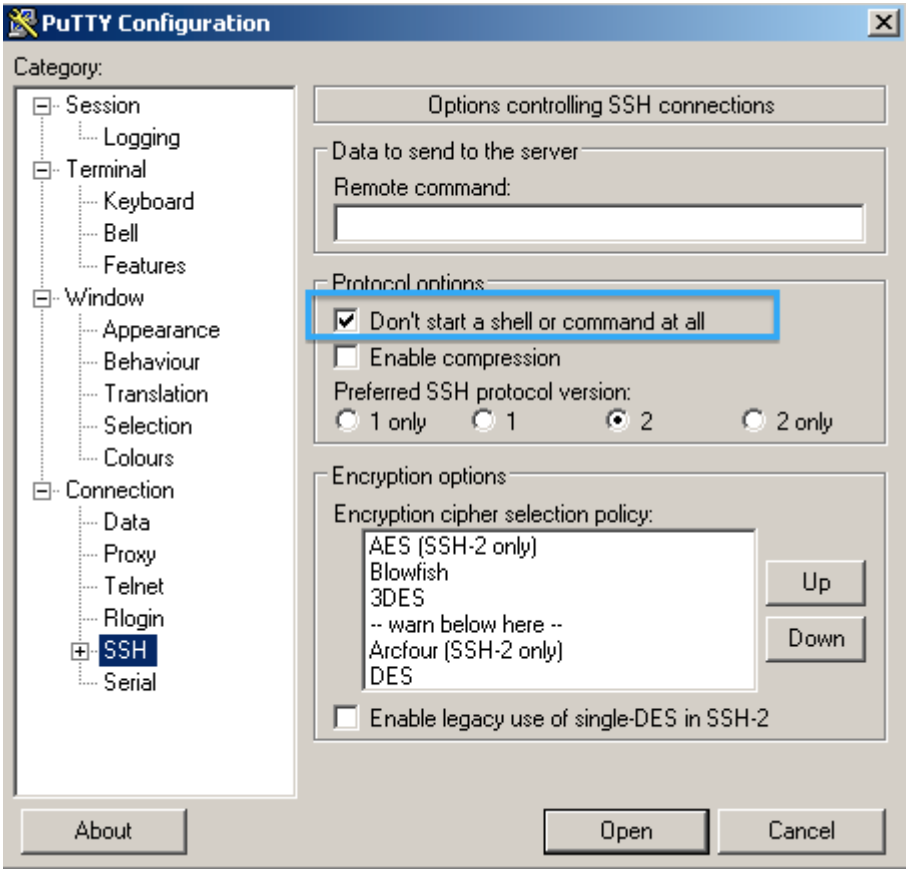
米国(iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



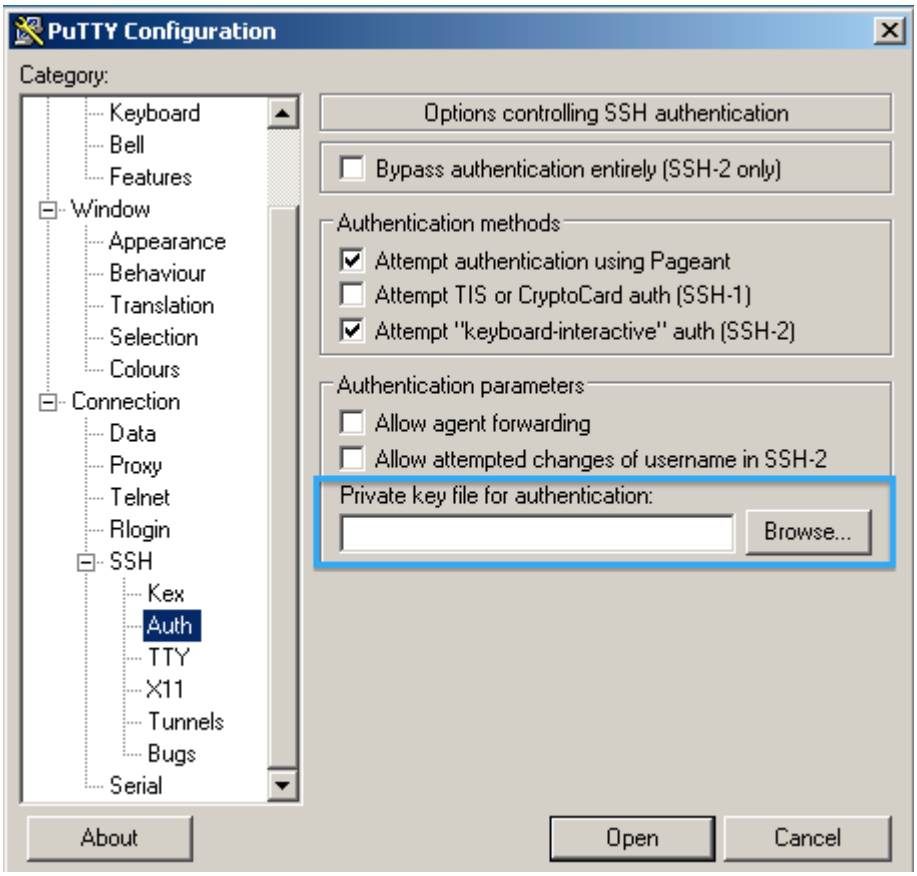
Dataandをクリックし、ログインの詳細を確認するには、自動ログインユーザ名を使用し、dh-userと入力します。



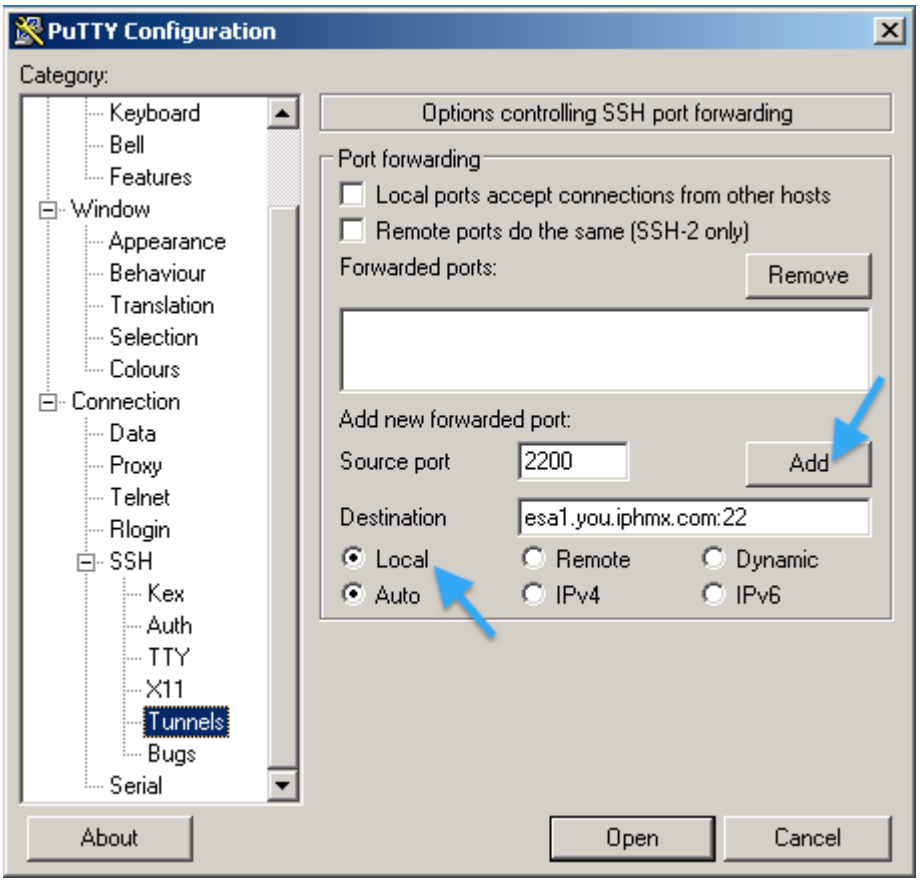
SSHを選択し、Don't start a shell or command at allにチェックマークを入れます。



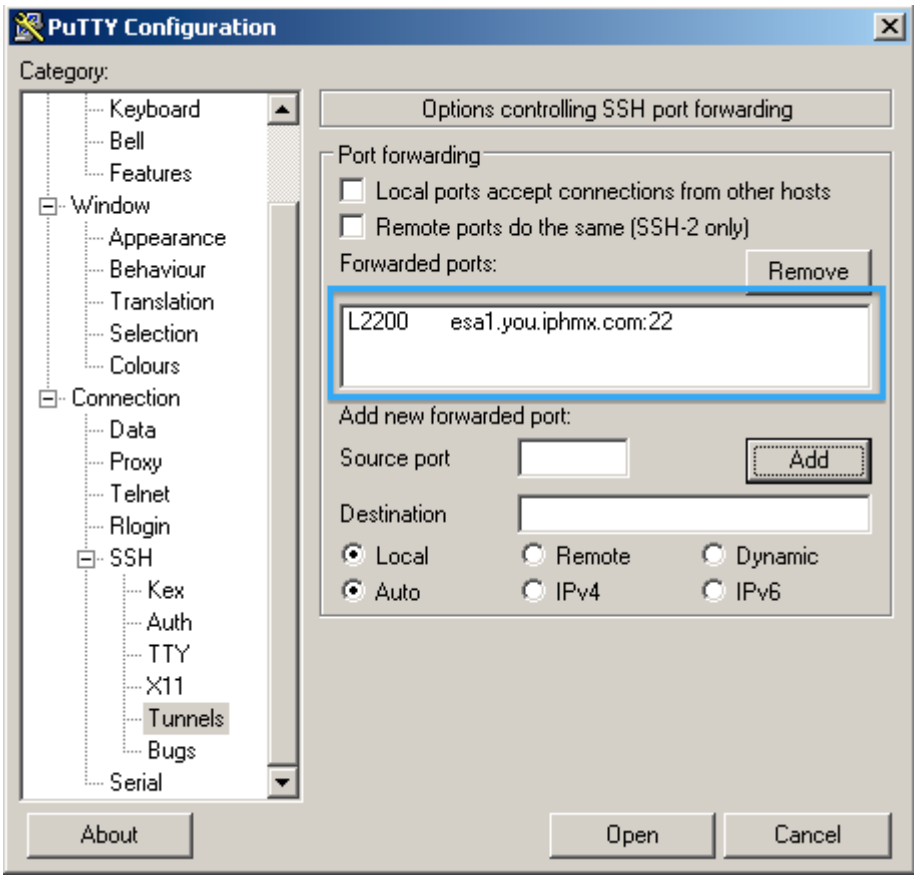
Authand for Private key file for authenticationをクリックし、秘密鍵を参照して選択します。



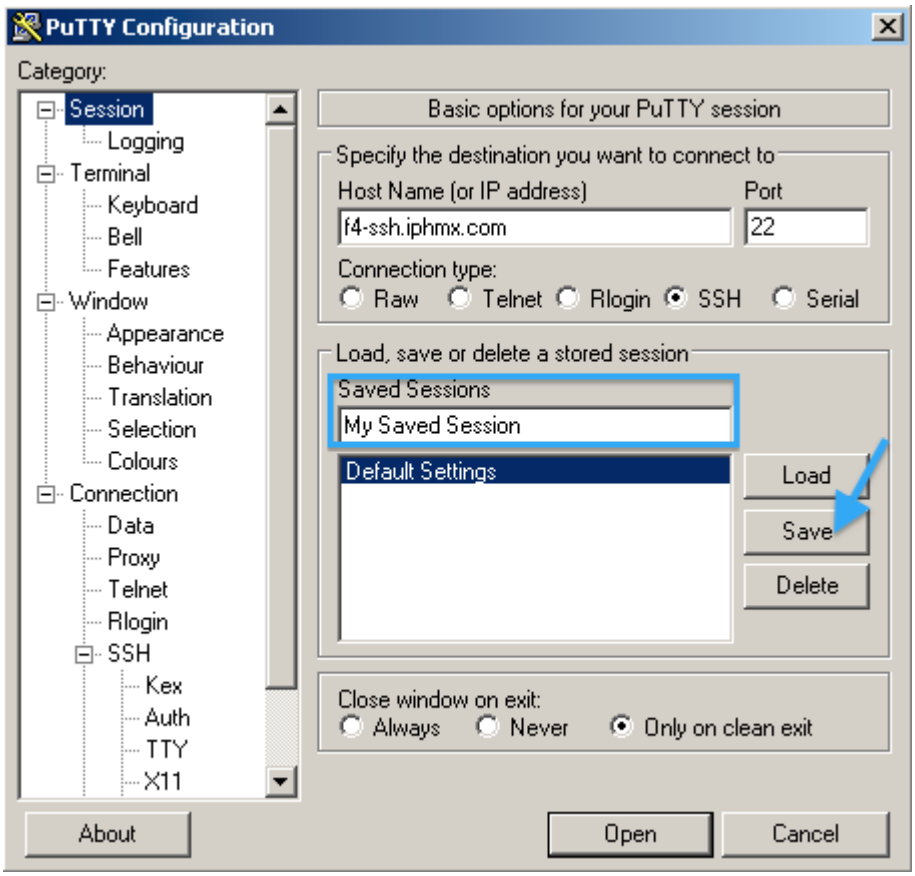
Tunnelsをクリックします。
Source portに任意のポートを入力します（例：2200）。
aDestinationに入力します。これは、使用するESAまたはSMA + 22（SSH接続を指定）です。



Addをクリックすると、次のように表示されます。

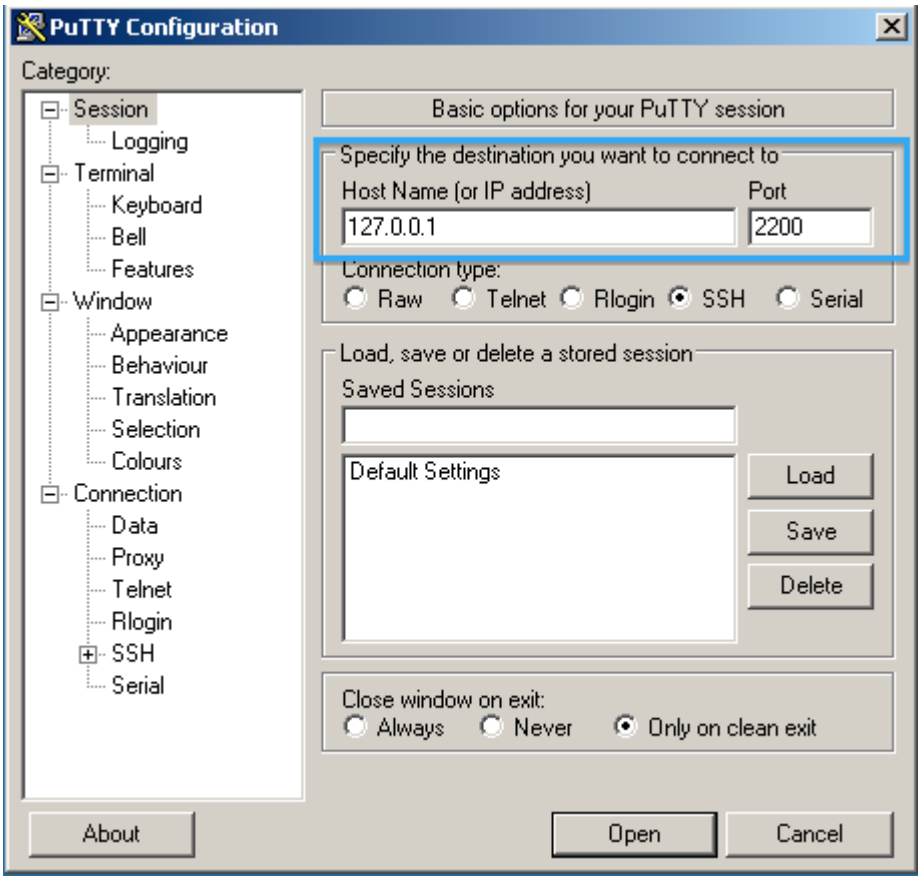


今後の使用のためにセッションを保存する場合は、Sessionをクリックします。
「Saved Session」の名前を入力し、Saveをクリックします。



この時点で、Openをクリックしてプロキシセッションを開始できます。
ログインやコマンドプロンプトはありません。次に、ESAまたはSMAへの2つ目のPuTTYセッションを開く必要があります。

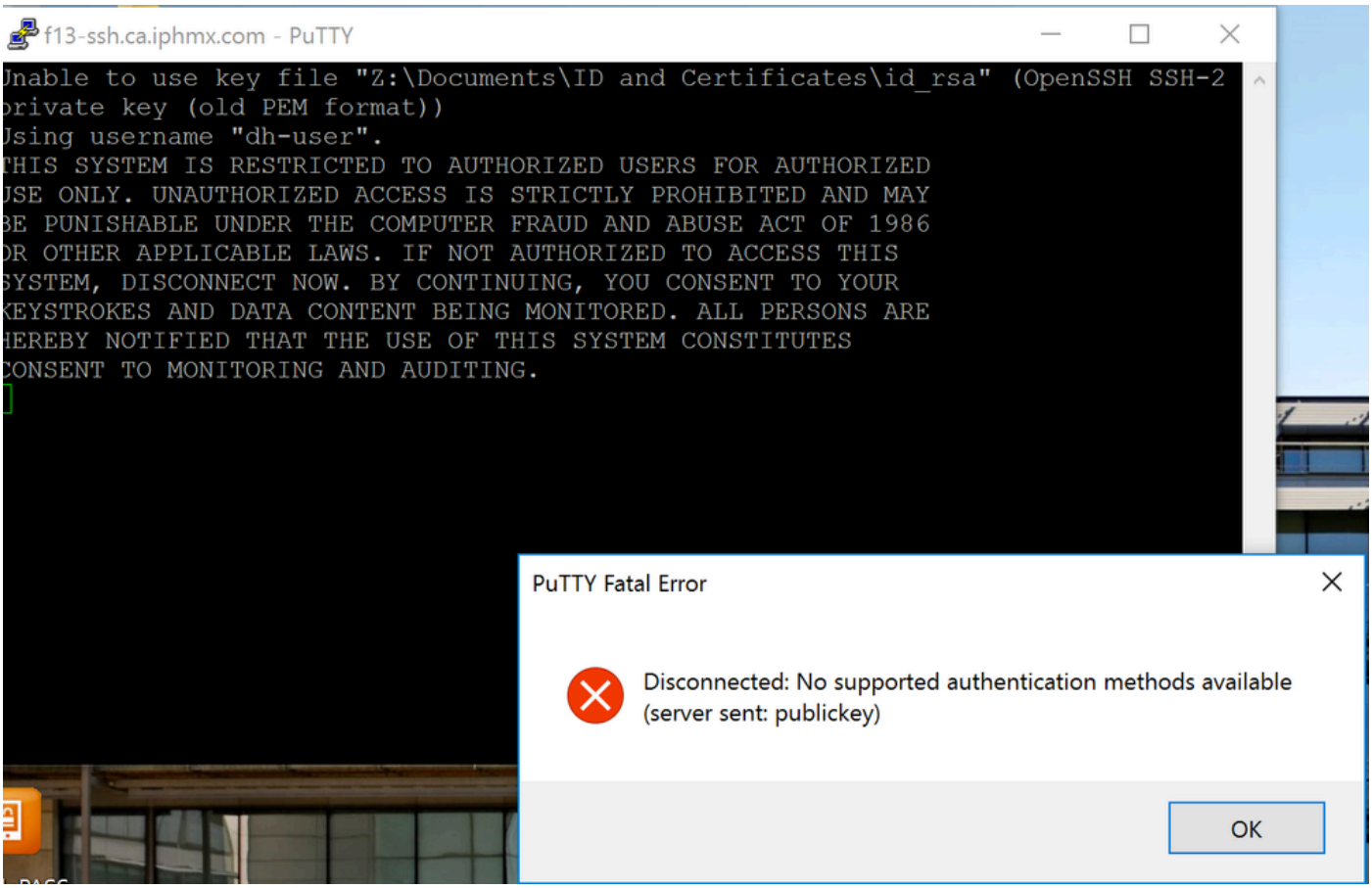
ホスト名127.0.0.1を使用し、前述のトンネル設定の送信元ポート番号を使用します。
この例では、2200が使用されています。
Openをクリックしてアプライアンスに接続します。



プロンプトが表示されたら、UIアクセスの場合と同じように、アプライアンスのユーザ名とパスワードを使用します。

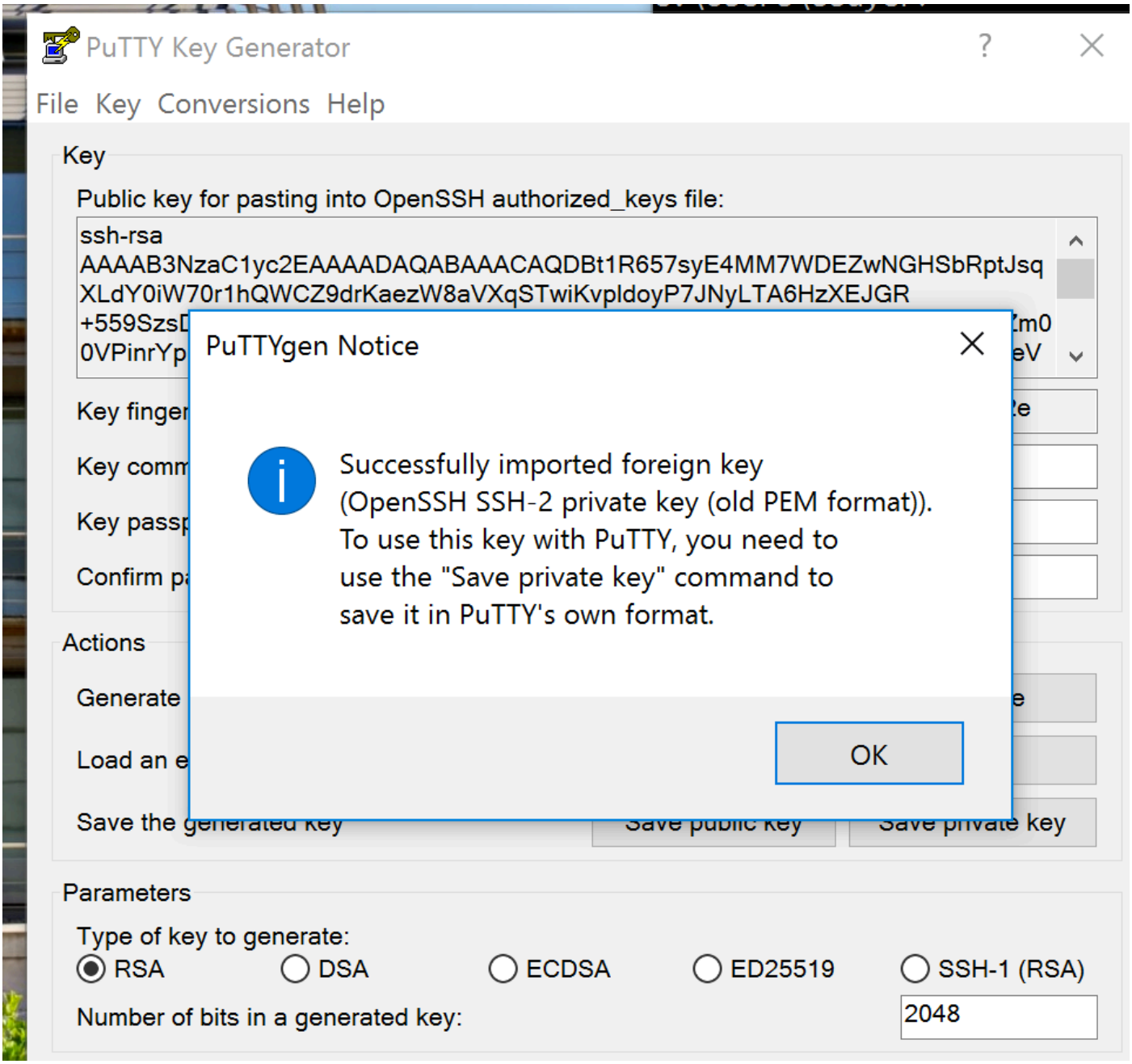
トラブルシューティング

SSHキーペアがOpenSSH（非PuTTy）を使用して生成された場合、接続できず、「古いPEM形式」のエラーが表示されます。



秘密鍵は、PuTTY Key Generatorを使用して変換できます。

- PuTTy Key Generatorを開きます。
- 既存の秘密キーを参照してロードするには、Loadをクリックします。
- 秘密キーを見つけるには、ドロップダウンをクリックしてAll Files (.)を選択する必要があります。
- 秘密キーが見つかったら、[開く]をクリックします。
- Puttygenは、次の図のような通知を提供します。



- [秘密キーの保存]をクリックします。
- PuTTYセッションから、この変換された秘密キーを使用してセッションを保存します。
- 変換された秘密キーで再接続を試みます。

コマンドラインからアプライアンスにアクセスできることを確認します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。