请求思科云邮件安全CLI访问

目录

简介

本文档介绍如何请求访问其云邮件安全(CES)CLI。

背景信息

Cisco CES客户有权使用密钥身份验证通过SSH代理访问其ESA和SMA的CLI。对托管设备的CLI访问必须限于组织内的关键人员。

Linux和Mac用户

对于Cisco CES客户：
使用SSH通过CES代理进行CLI访问的外壳脚本的说明。

先决条件

作为CES客户，您必须参与CES自注册/运营或思科TAC，才能交换和放置SSH密钥：

1. 生成私有/公有RSA密钥。
2. 向思科提供您的PublicRSA密钥。

3. 等待思科保存并通知您您的密钥已保存到您的CES客户帐户。
4. 复制并修改connect2ces.sh脚本。

如何创建私有/公有RSA密钥？

Cisco建议在用于Unix/Linux/OS X的终端/CLI上使用“ssh-keygen”。请使用ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NAME> 命令。

注意：有关详细信息，请访问 https://www.ssh.com/academy/ssh/keygen。
确保始终保护对RSA私钥的访问。
不要将您的私钥发送到Cisco，只发送公钥(.pub)。
将您的公钥提交给思科时，请确定该密钥的电子邮件地址/名字/姓氏。

如何打开思科支持请求以提供我的公钥？

导航到此链接。

确保您正确将SR标识为“Cisco CES Customer SSH/CLI Setup”，以此类推。

配置

要开始使用，请使用opencopy提供的脚本，并将这些代理主机之一用于主机名。

确保您为所在区域选择正确的代理(即，如果您是美国CES客户，为了访问F4数据中心和设备，请使用f4-ssh.iphmx.com。如果您是欧洲CES客户，在德国DC拥有设备，请使用f17-ssh.eu.iphmx.com。)

无线接入点(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

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

欧盟(eu.iphmx.com)（德国DC）
f17-ssh.eu.ip hmx.com
f18-ssh.eu.ip hmx.com

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

如果要连接到多个邮件安全设备(ESA)或安全管理设备(SMA)，该怎么办？

复制并保存connect2ces.sh的第二个副本，例如connect2ces_2.sh。

注意：您需要将“cloud_host”编辑为您想要访问的附加设备。
您将要将“local_port”编辑为2222以外的内容。否则，您将收到错误消息“警告：远程主机标识已更改！”

如何配置ESA或SMA以在不提示输入密码的情况下登录？

请阅读本指南。

完成先决条件后，这会是什么样的？

joe.user@my_local > ~ ./connect2ces
[-]正在连接到您的代理服务器(f4-ssh.iphmx.com)。..
[-]代理连接成功。现在已连接到f4-ssh.iphmx.com。
[-]代理在PID上运行：31253
[-]正在连接到CES设备(esa1.rs1234-01.iphmx.com)。..

上次登录时间：2019年4月22日（星期一）：11:33:45（10.123.123.123起）
AsyncOS 12.1.0，适用于Cisco C100V版本071

欢迎使用思科C100V邮件安全虚拟设备

NOTE:如果闲置1440分钟，此会话将过期。所有未提交的配置更改都将丢失。更改配置后，请立即确认更改。

(机器esa1.rs1234-01.iphmx.com)>
(计算机esa1.rs1234-01.iphmx.com)>退出

到127.0.0.1的连接已关闭。
[-]正在关闭代理连接……
[-]完成。

connect2ces.sh

注意：确保您为所在区域选择正确的代理(即，如果您是美国CES客户，为了访问F4数据中心和设备，请使用f4-ssh.iphmx.com。如果您是欧洲CES客户，在德国DC拥有设备，请使用f17-ssh.eu.iphmx.com。)

#!/bin/bash

```
#--编辑以下值----------------------
#应已与CES建立以下值：
# cloud_user="username"
# cloud_host="esaX.CUSTOMER.iphmx.com"或"smaX.CUSTOMER.iphmx.com"
## [确保您具有适当的区域CES数据中心设置！]
# private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
# proxy_server="PROXY_SERVER" [仅选择一项！]
#
##对于“proxy_server”，以下是SSH代理：
##
##无线接入点(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
##
##欧盟(c3s2.iphmx.com)
## f10-ssh.c3s2.iphmx.com
## f11-ssh.c3s2.iphmx.com
##
##欧盟(eu.iphmx.com)（德国直流）
## f17-ssh.eu.iphmx.com
## f18-ssh.eu.iphmx.com
##
##美国(iphmx.com)
## f4-ssh.iphmx.com
## f5-ssh.iphmx.com

cloud_user="username"
cloud_host="esaX.CUSTOMER.iphmx.com"
private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
proxy_server="PROXY_SERVER"

#--保留这些值原样--------------------
# 'proxy_user'不应更改
# 'remote_port'保持22(SSH)
# “local_port”可根据需要设置为不同的值

proxy_user="dh-user"
remote_port=22
local_port=222

#--不要在此行下编辑----------------

proxycmd="ssh -f -L $local_port:$cloud_host:$remote_port -i $private_key -N
```

```
$proxy_user@$proxy_server"

printf "[-]正在连接到代理服务器($proxy_server)。..\n”
$proxycmd >/dev/null 2>&1
如果nc -z 127.0.0.1 $local_port >/dev/null 2>&1;然后
printf "[-]代理连接成功。现在已连接到$proxy_server。\n"
其他
printf "[-]代理连接失败。正在退出……\n”
退出
fi

#查找代理ssh进程
proxypid='ps -xo pid，命令 | grep "$cloud_host" | grep "$proxy_server" | head -n1 | sed "s/^[ \t]*/" | cut -d " " -f1'
printf "[-]代理在PID上运行：$proxypid\n"

printf "[-]正在连接到CES设备($cloud_host)。..\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

printf "[-]正在关闭代理连接……\n”
kill $proxypid

printf "[-]完成。\n"

#--想避免每次都键入密码？
#--请参阅：https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-technote-esa-00.html
#--需要访问多个ESA或SMA?复制相同的脚本并重命名为connect2ces_2.sh或类似名称。
```

原始文档:https://github.com/robsherw/connect2ces。

Windows用户

使用PuTTY和使用SSH以通过CES代理进行CLI访问的说明。

先决条件

作为CES客户，您必须参与CES自注册/运营，或思科TAC才能交换和放置SSH密钥：

1. 生成私有/公有RSA密钥。
2. 向思科提供公有RSA密钥。
3. 等待思科保存并通知您您的密钥已保存到CES客户帐户。
4. 按照以下说明中的详细信息设置PuTTY。

如何创建私有/公有RSA密钥？

Cisco建议对Windows使用PuTTYgen(https://www.puttygen.com/)。

有关详细信息，请访问https://www.ssh.com/ssh/putty/windows/puttygen。

注意：确保始终保护对RSA私钥的访问。
不要将您的私钥发送到Cisco，只发送公钥(.pub)。
将您的公钥提交给思科时，请确定该公钥的电子邮件地址/名字/姓氏。

如何打开思科支持请求以提供我的公钥？

导航到此链接。

确保您正确将SR标识为“Cisco CES Customer SSH/CLI Setup”，以此类推。

如何配置ESA或SMA以在不提示输入密码的情况下登录？

请阅读本指南。

PuTty配置

要开始使用，请打开PuTTY并将以下代理主机之一用于主机名:

确保您为所在区域选择正确的代理(即，如果您是美国CES客户，为了访问F4数据中心和设备，请使用f4-ssh.iphmx.com。如果您是欧洲CES客户，在德国DC拥有设备，请使用f17-ssh.eu.iphmx.com。)

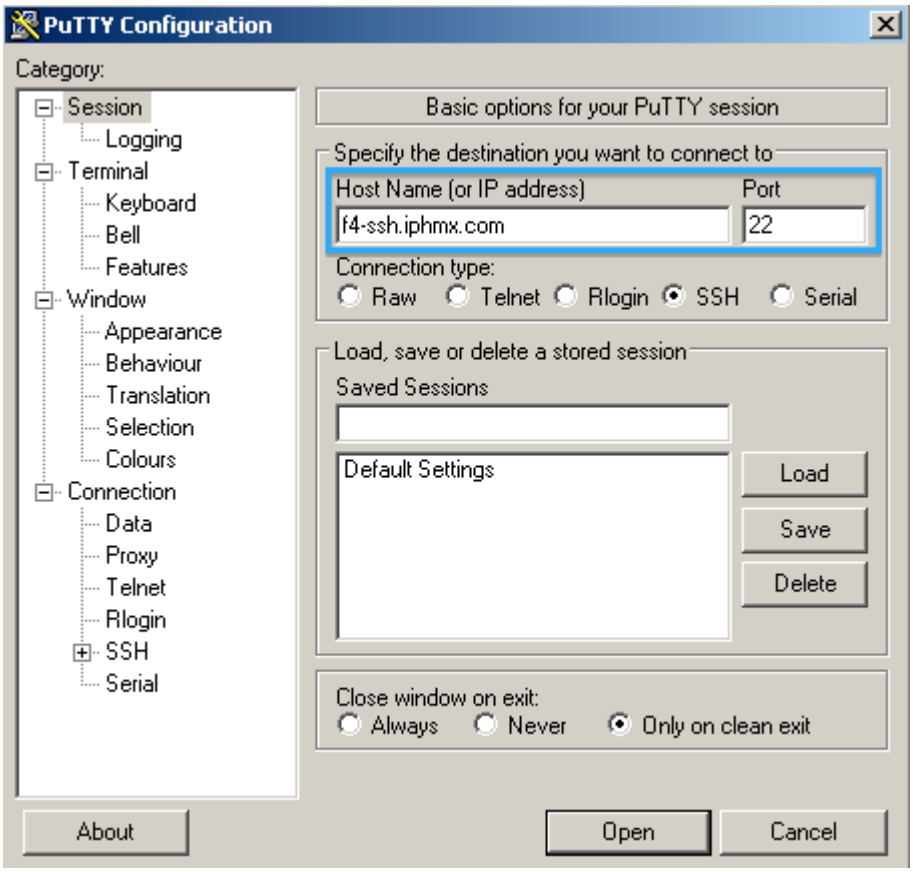
无线接入点(ap.iphmx.com)
f15-ssh.ap.ip hmx.com
f16-ssh.ap.ip hmx.com

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

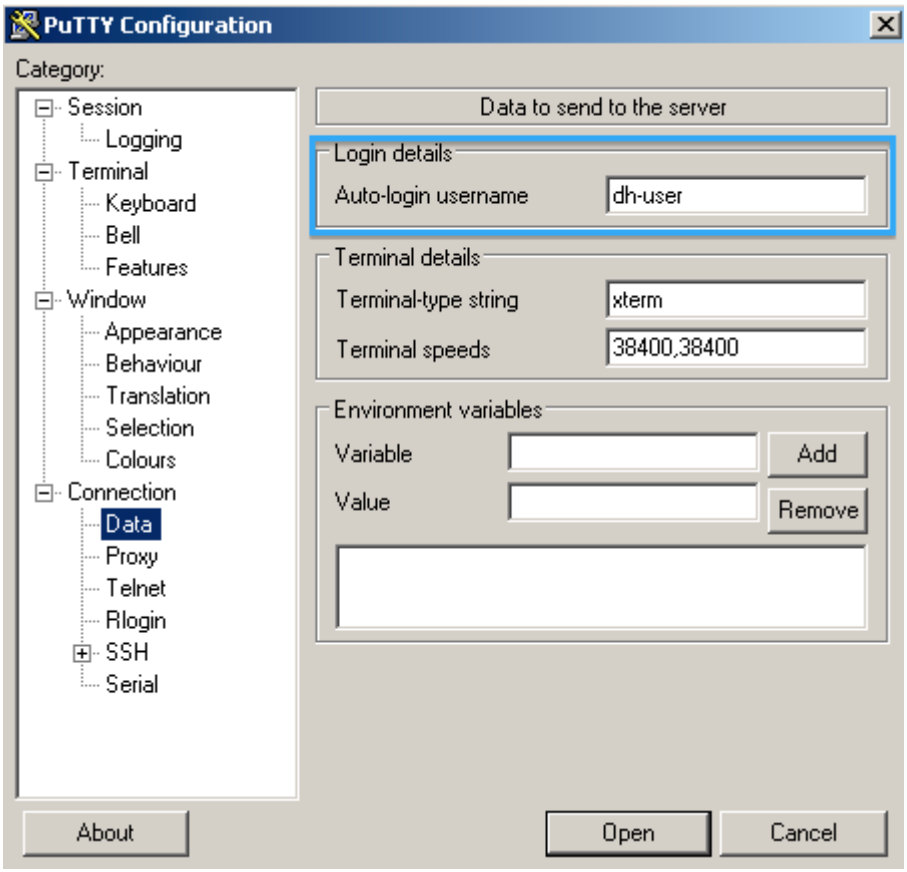
欧盟(c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

欧盟(eu.iphmx.com)（德国DC）
f17-ssh.eu.ip hmx.com
f18-ssh.eu.ip hmx.com

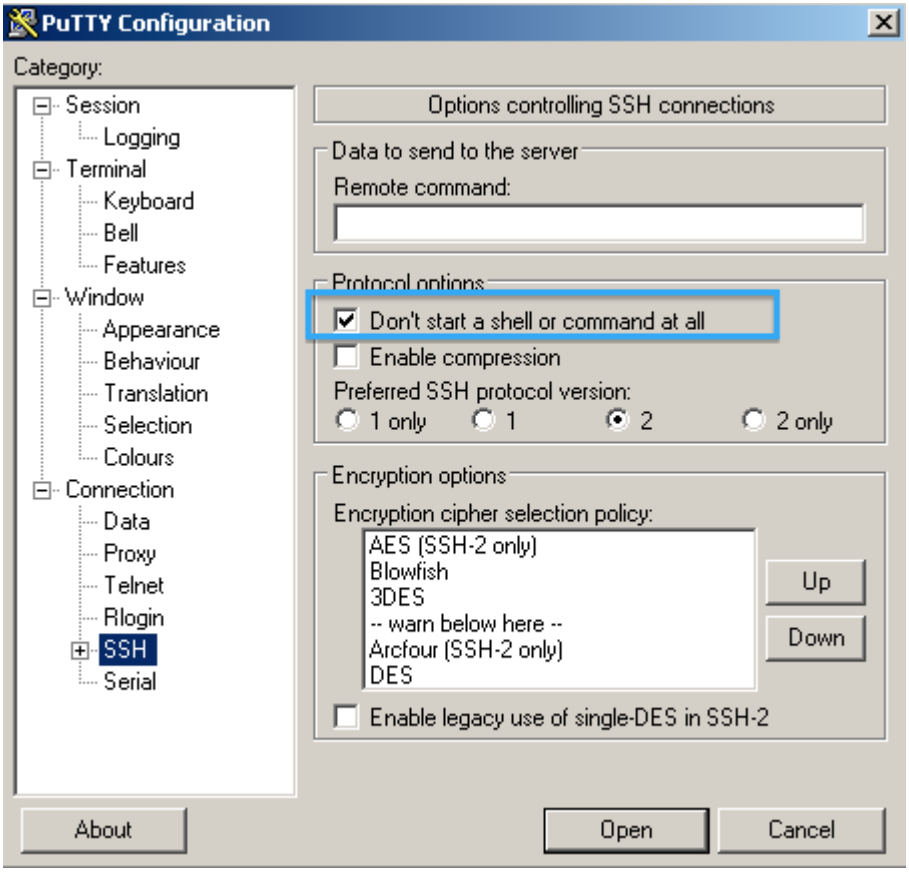
美国(iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



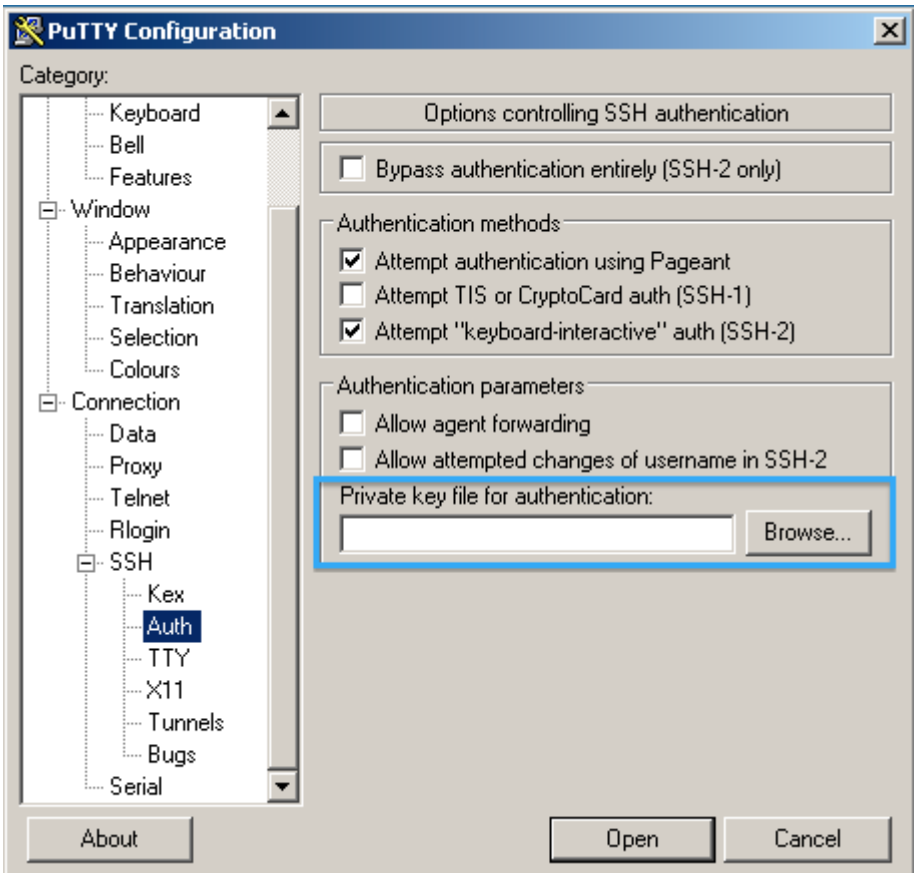
单击Dataand获取登录详细信息，使用自动登录用户名并输入dh-user。



选择SSH并选中Don't start a shell or command at all。

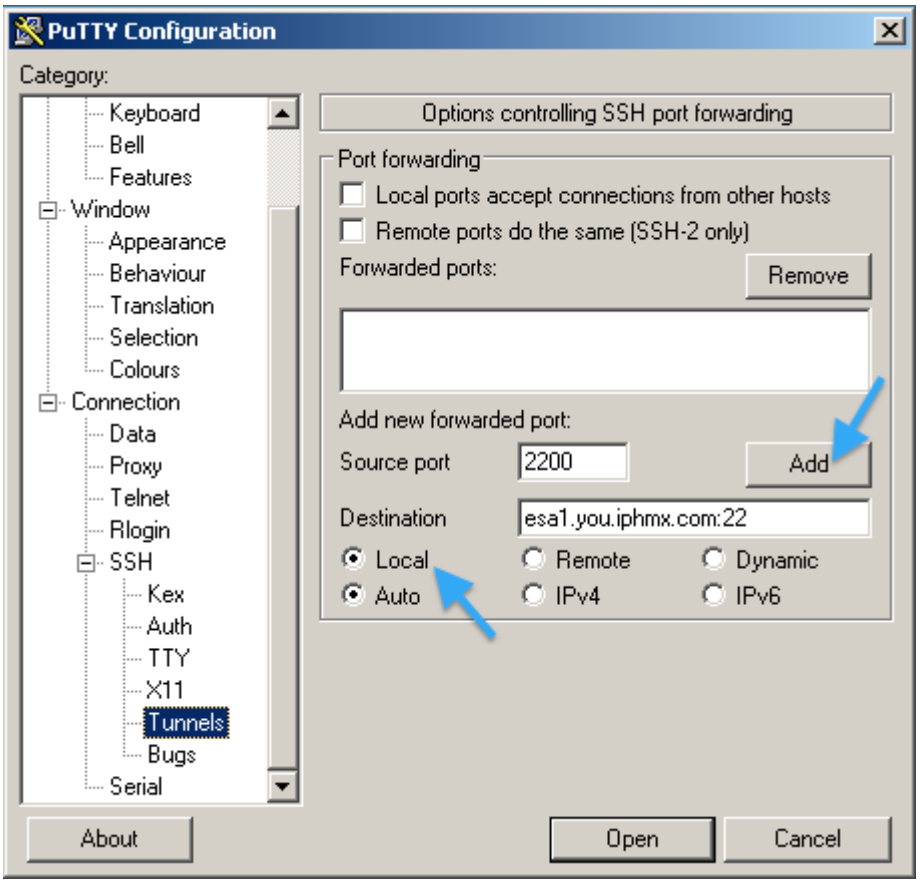


单击Authand for Private key file for authentication，浏览并选择您的私钥。

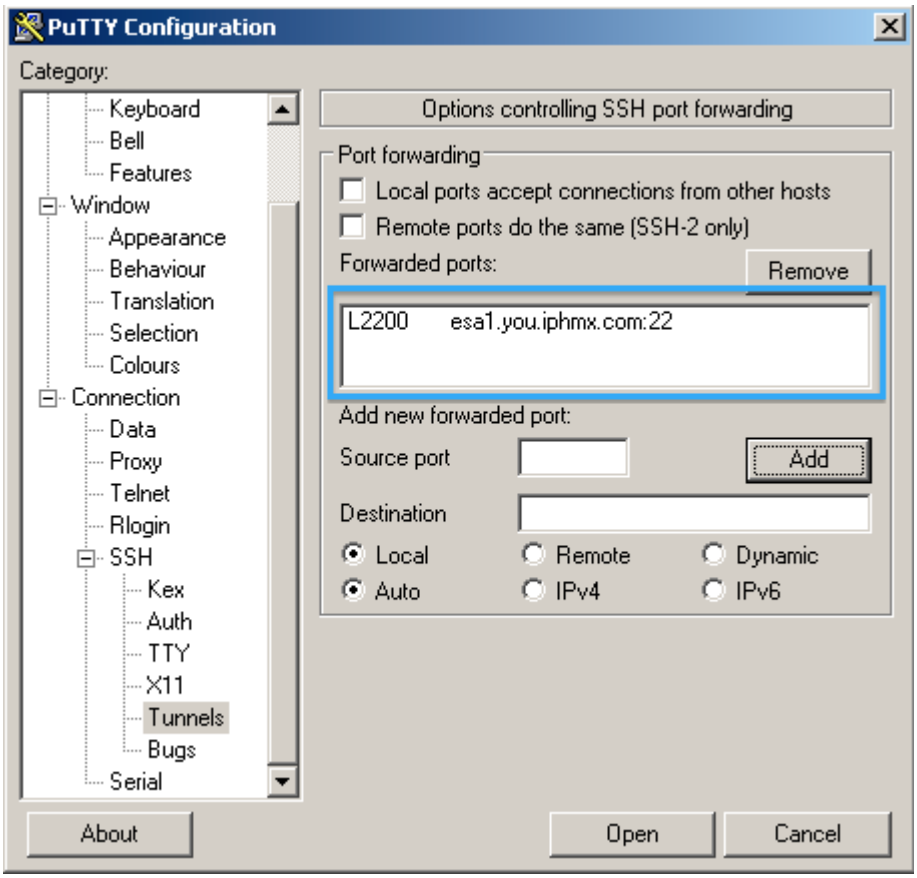


单击Tunnels。
输入源端口;这是您选择的任意端口（示例使用2200）。

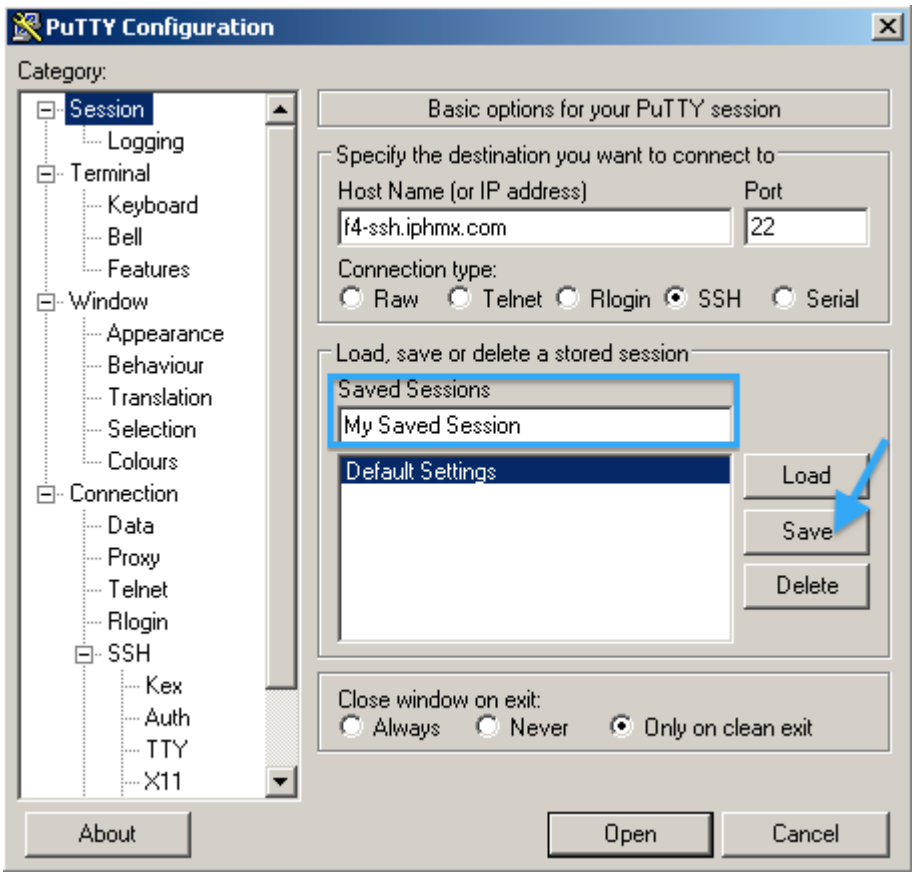
输入aDestination;这是您的ESA或SMA + 22（指定SSH连接）。



单击Add后，它必须如下所示。

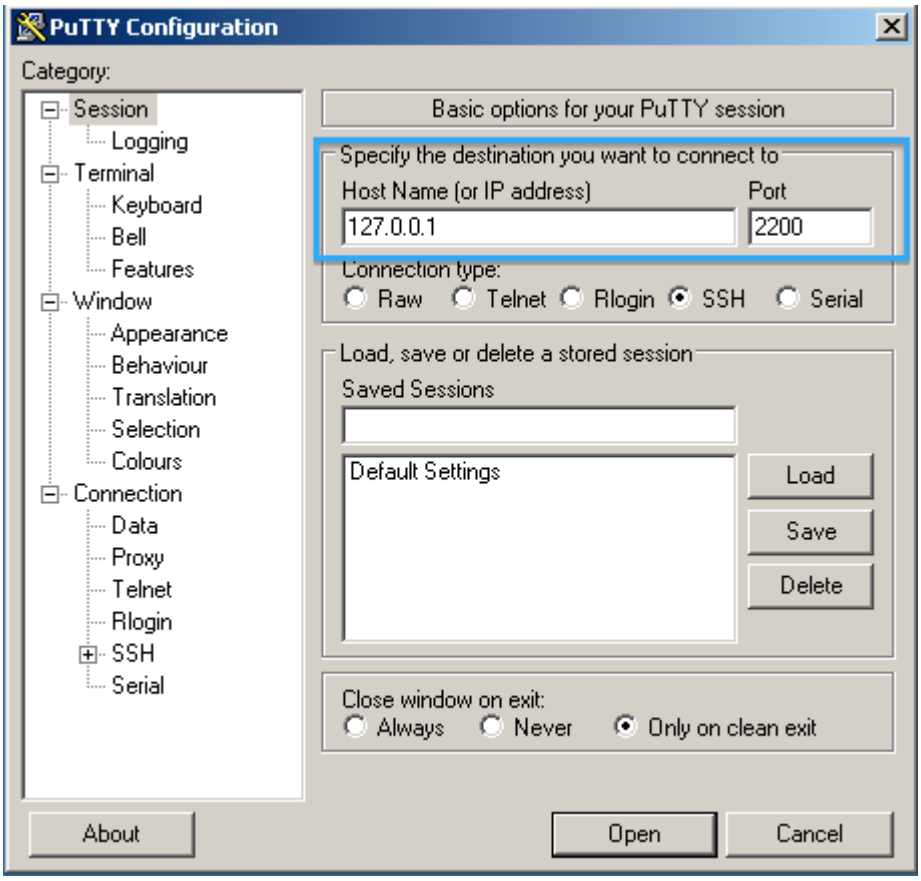


要保存会话以供将来使用，请单击Session。
输入“保存的会话”的名称，然后单击保存。



此时，您可以单击Open并启动代理会话。
不会出现任何登录提示或命令提示符。现在，您需要打开与您的ESA或SMA的第二个PuTTY会话。

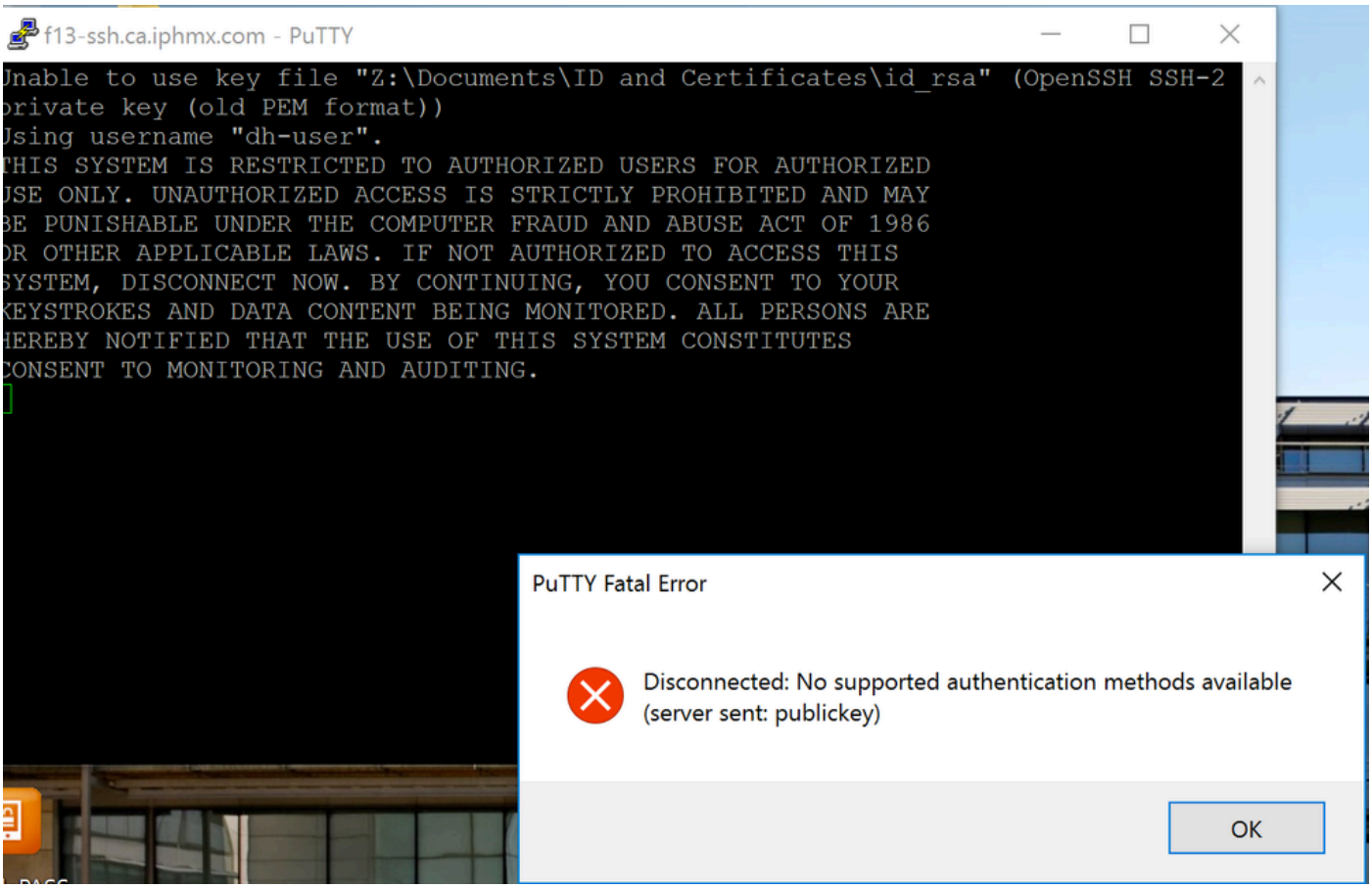
使用主机名127.0.0.1并在前面所示的隧道配置中使用源端口号。
在本例中，使用2200。
单击Open以连接到设备。



系统提示时，请使用设备用户名和密码，与具有UI访问权限时相同。

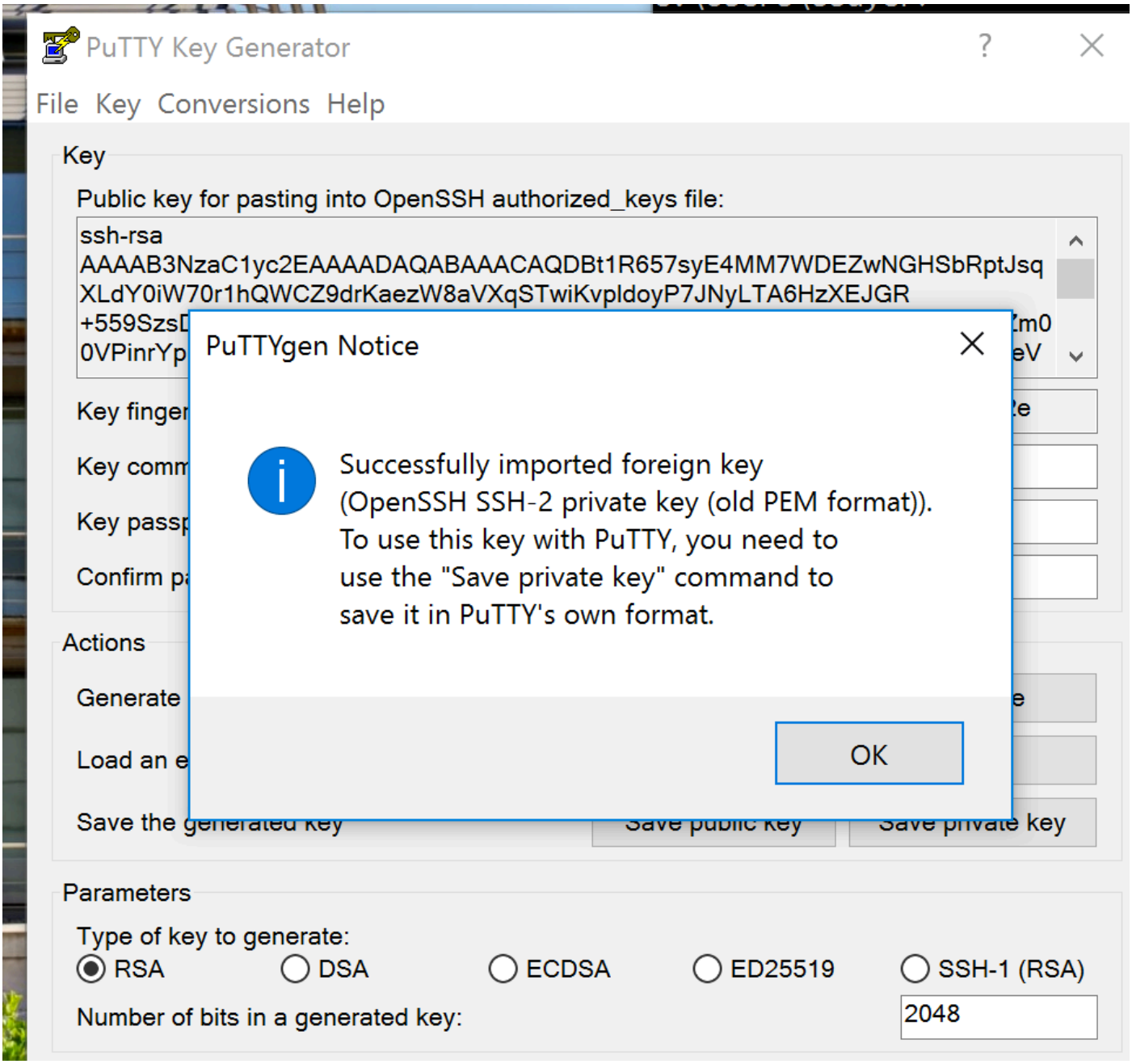
故障排除

如果您的SSH密钥对是使用OpenSSH（非PuTY）生成的，则您无法连接，并且会出现“旧PEM格式”错误。



可以使用PuTTY密钥生成器转换私钥。

- 打开PuTy密钥生成器。
- 点击Loadin以浏览和加载现有私钥。
- 您需要点击下拉列表并选择所有文件(.)，以便找到私钥。
- 找到私钥后，单击Opening。
- Puttygen将提供类似下图中的通知。



- 单击保存私钥。
- 从您的PuTTY会话中，使用此转换的私钥并保存会话。
- 尝试使用已转换的私钥重新连接。

确认您能够通过命令行访问设备。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。