Zugriff auf die Cisco Cloud Email Security CLI anfordern

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Zugriff auf die Cloud Email Security (CES)-CLI anfordern.

Hintergrundinformationen

Cisco CES-Kunden haben Anspruch auf den Zugriff auf die CLI ihrer ESA und SMA, die über einen SSH-Proxy bereitgestellt werden. Hierzu wird die Schlüsselauthentifizierung verwendet. Der CLI-Zugriff auf Ihre gehosteten Appliances muss auf die wichtigsten Personen in Ihrem Unternehmen beschränkt sein.

Linux- und Mac-Benutzer

Für Cisco CES-Kunden:
Anweisungen für ein Shell-Skript, das SSH verwendet, um CLI-Zugriff über den CES-Proxy zu

ermöglichen.

Voraussetzungen

Als CES-Kunde müssen Sie sich für CES On-Boarding/Ops oder Cisco TAC entschieden haben, damit die SSH-Schlüssel ausgetauscht und platziert werden können:

1. Generieren Sie privaten/öffentlichen RSA-Schlüssel.
2. Geben Sie Cisco Ihren PublicRSA-Schlüssel.
3. Warten Sie auf die Speicherung durch Cisco, und benachrichtigen Sie, dass Ihre Schlüssel in Ihrem CES-Kundenkonto gespeichert wurden.
4. Kopieren und ändern Sie das Skript connect2ces.sh.

Wie erstelle ich private/öffentliche RSA-Schlüssel?

Cisco empfiehlt die Verwendung von "ssh-keygen" auf dem Terminal/CLI für Unix/Linux/OS X. Verwenden Sie den Befehl ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NAME>.

Anmerkung: Weitere Informationen finden Sie unter https://www.ssh.com/academy/ssh/keygen.
Stellen Sie sicher, dass Sie jederzeit den Zugriff auf Ihre privaten RSA-Schlüssel schützen.
Senden Sie Ihren privaten Schlüssel nicht an Cisco, sondern nur an den öffentlichen Schlüssel (.pub).
Wenn Sie Ihren öffentlichen Schlüssel an Cisco übermitteln, geben Sie die E-Mail-Adresse, den Vor- und Nachnamen an, für die der Schlüssel bestimmt ist.

Wie öffne ich eine Cisco Support-Anfrage, um meinen öffentlichen Schlüssel bereitzustellen?

Navigieren Sie zu diesem Link.

Stellen Sie sicher, dass Sie den Serviceticket-Manager korrekt als "Cisco CES Customer SSH/CLI Setup" usw. identifizieren.

Konfiguration

Um zu beginnen, öffnen Sie das bereitgestellte Skript, und verwenden Sie einen dieser Proxyhosts für den Hostnamen.

Stellen Sie sicher, dass Sie den richtigen Proxy für Ihre Region wählen (d. h., wenn Sie ein Kunde von US CES sind, verwenden Sie die Adresse f4-ssh.iphmx.com, um das F4-Rechenzentrum und Appliances zu erreichen. Wenn Sie ein Kunde der EU-CES mit einer Appliance in deutschem Rechenzentrum sind, verwenden Sie f17-ssh.eu.iphmx.com.).

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) (Deutsches DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

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

Was ist, wenn ich mich mit mehr als einer E-Mail Security Appliance (ESA) oder Security Management Appliance (SMA) verbinden möchte?

Kopieren und speichern Sie eine zweite Kopie von connect2ces.sh, z. B. connect2ces_2.sh.

Anmerkung: Bearbeiten Sie "cloud_host" als zusätzliche Appliance, auf die Sie zugreifen möchten.
Sie möchten den 'local_port' so bearbeiten, dass er nicht 2222 ist. Andernfalls wird die folgende Fehlermeldung angezeigt: "WARNUNG: DIE REMOTE-HOST-IDENTIFIZIERUNG HAT SICH GEÄNDERT!"

Wie kann ich meine ESA oder SMA so konfigurieren, dass sie sich ohne Aufforderung zur Eingabe eines Kennworts anmelden?

Lesen Sie diesen Leitfaden.

Wie kann das aussehen, wenn die Voraussetzungen erfüllt sind?

joe.user@my_local > ~ ./connect2ces
[-] Verbindung mit dem Proxyserver wird hergestellt (f4-ssh.iphmx.com)...
[-] Proxy-Verbindung erfolgreich. Jetzt verbunden mit f4-ssh.iphmx.com.
[-] auf PID ausgeführter Proxy: 31253
[-] Verbindung mit der CES-Appliance herstellen (esa1.rs1234-01.iphmx.com)...

Letzte Anmeldung: Montag, 22. April 2019, 11:33:45 Uhr vom 10.123.123.123 Uhr
AsyncOS 12.1.0 für Cisco C100V, Build 071

Willkommen bei der Cisco Email Security Virtual Appliance C100V

HINWEIS: Diese Sitzung läuft ab, wenn sie 1440 Minuten lang nicht genutzt wird. Alle nicht bestätigten Konfigurationsänderungen gehen verloren. Bestätigen Sie die Konfigurationsänderungen, sobald sie vorgenommen wurden.

(Computer esa1.rs1234-01.iphmx.com)>
(Computer esa1.rs1234-01.iphmx.com)> exit

Verbindung zu 127.0.0.1 geschlossen.
[-] Proxy-Verbindung wird geschlossen...
[-] Fertig.

connect2ces.sh

Hinweis: Wählen Sie den richtigen Proxy für Ihre Region aus (d. h., wenn Sie ein Kunde der US-amerikanischen CES sind, verwenden Sie f4-ssh.iphmx.com, um das F4-Rechenzentrum und Appliances zu erreichen. Wenn Sie ein Kunde der EU-CES mit einer Appliance in deutschem Rechenzentrum sind, verwenden Sie f17-ssh.eu.iphmx.com.).

```
#!/bin/bash

#-- BEARBEITEN SIE DIE UNTEN STEHENDEN WERTE ----------------------
# Folgende Werte sollten mit CES bereits festgelegt werden:
# cloud_user="Benutzername"
# cloud_host="esaX.CUSTOMER.iphmx.com" oder "smaX.CUSTOMER.iphmx.com"
## [STELLEN SIE SICHER, DASS SIE ÜBER DAS RICHTIGE REGIONALE CES-
RECHENZENTRUM VERFÜGEN!]
# private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
# proxy_server="PROXY_SERVER" [NUR EINEN AUSWÄHLEN!]
Nr.
## Für 'proxy_server' sind dies SSH-Proxys:
##
## 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) (Deutsches Rechenzentrum)
## f17-ssh.eu.iphmx.com
## f18-ssh.eu.iphmx.com
##
## USA (iphmx.com)
## f4-ssh.iphmx.com
## f5-ssh.iphmx.com

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

#-- DIESE WERTE BLEIBEN WIE BESEHEN ----------
# 'proxy_user' darf nicht geändert werden.
# 'remote_port' bleibt 22 (SSH)
# 'local_port' kann bei Bedarf auf einen anderen Wert gesetzt werden

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

#-- UNTERHALB DIESER ZEILE NICHT BEARBEITEN ----------

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

printf "[-] Verbindung mit dem Proxyserver ($proxy_server) wird hergestellt...\n"
$proxycmd >/dev/null 2>&1
if nc -z 127.0.0.1 $local_port >/dev/null 2>&1; dann
printf "[-] Proxy-Verbindung erfolgreich. Jetzt mit $proxy_server verbunden.\n"
Sonst
printf "[-] Proxy-Verbindung fehlgeschlagen. Beenden...\n"
beenden
WiFi

# Proxy-SSH-Prozess suchen
proxypid=`ps -xo pid,Befehl | grep "$cloud_host" | grep "$proxy_server" | Überschrift -n1 | sed "s/^[
\t]*//" | cut -d " " -f1"
printf "[-] Proxy läuft auf PID: $proxypid\n"

printf "[-] Verbindung mit der CES-Appliance ($cloud_host)...\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

printf "[-] Proxy-Verbindung wird geschlossen...\n"
```

töten $proxypid

printf "[-] Fertig.\n"

#-- Sie möchten vermeiden, jedes Mal ein Kennwort eingeben zu müssen?
#-- Siehe: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-technote-esa-00.html
#-- Sie benötigen Zugriff auf mehr als eine ESA oder SMA? Kopieren Sie das gleiche Skript und benennen Sie es in connect2ces_2.sh oder ähnlich um.

Originaldokument:https://github.com/robsherw/connect2ces.

Windows-Benutzer

Anweisungen für die Verwendung von PuTTY und SSH, um CLI-Zugriff über den CES-Proxy zu ermöglichen.

Voraussetzungen

Als CES-Kunde müssen Sie sich für CES On-Boarding/Ops oder Cisco TAC entschieden haben, damit die SSH-Schlüssel ausgetauscht und platziert werden können:

1. Generieren Sie privaten/öffentlichen RSA-Schlüssel.
2. Übermitteln Sie Cisco Ihren öffentlichen RSA-Schlüssel.
3. Warten Sie zum Speichern auf Cisco, und benachrichtigen Sie, dass Ihre Schlüssel in Ihrem CES-Kundenkonto gespeichert wurden.
4. Richten Sie PuTTY wie hier in diesen Anweisungen beschrieben ein.

Wie erstelle ich private/öffentliche RSA-Schlüssel?

Cisco empfiehlt die Verwendung von PuTTYgen (https://www.puttygen.com/) für Windows.

Weitere Informationen finden Sie unter https://www.ssh.com/ssh/putty/windows/puttygen.

Anmerkung: Stellen Sie sicher, dass Sie jederzeit den Zugriff auf Ihre privaten RSA-Schlüssel schützen.
Senden Sie Ihren privaten Schlüssel nicht an Cisco, sondern nur an den öffentlichen Schlüssel (.pub).
Wenn Sie Ihren öffentlichen Schlüssel an Cisco übermitteln, geben Sie die E-Mail-Adresse, den Vor- und Nachnamen an, für die der Schlüssel bestimmt ist.

Wie öffne ich eine Cisco Support-Anfrage, um meinen öffentlichen Schlüssel bereitzustellen?

Navigieren Sie zu diesem Link.

Stellen Sie sicher, dass Sie den Serviceticket-Manager korrekt als "Cisco CES Customer SSH/CLI Setup" usw. identifizieren.

Wie kann ich meine ESA oder SMA so konfigurieren, dass sie sich ohne Aufforderung zur Eingabe eines Kennworts anmelden?

Lesen Sie diesen Leitfaden.

PuTy-Konfiguration

Um zu beginnen, öffnen Sie PuTTY, und verwenden Sie einen der folgenden Proxyhosts für die Hostnamen:

Stellen Sie sicher, dass Sie den richtigen Proxy für Ihre Region wählen (d. h., wenn Sie ein Kunde von US CES sind, verwenden Sie die Adresse f4-ssh.iphmx.com, um das F4-Rechenzentrum und Appliances zu erreichen. Wenn Sie ein Kunde der EU-CES mit einer Appliance in deutschem Rechenzentrum sind, verwenden Sie f17-ssh.eu.iphmx.com.).

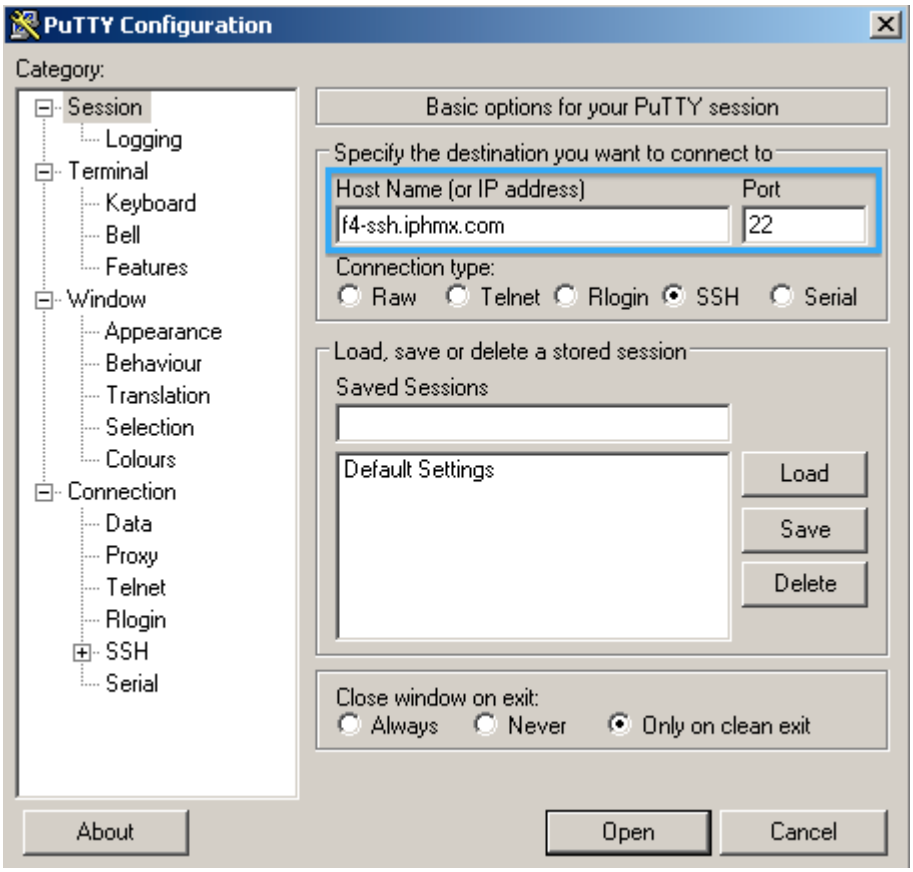
AP (ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

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

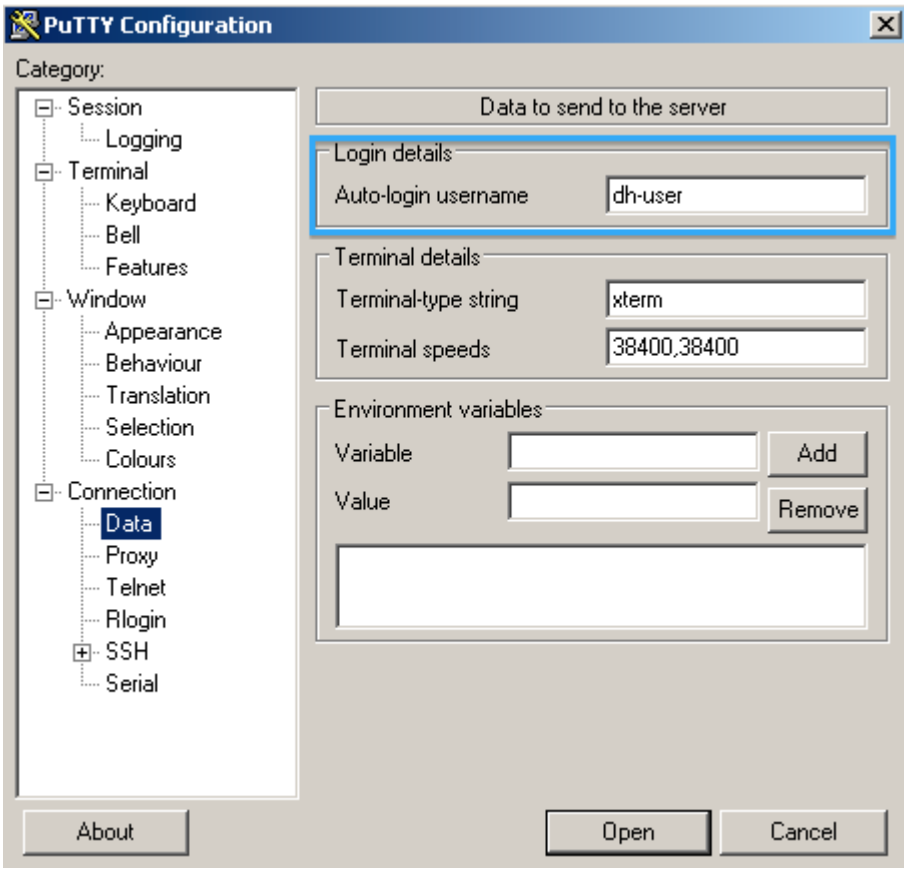
EU (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

EU (eu.iphmx.com) (Deutsches DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

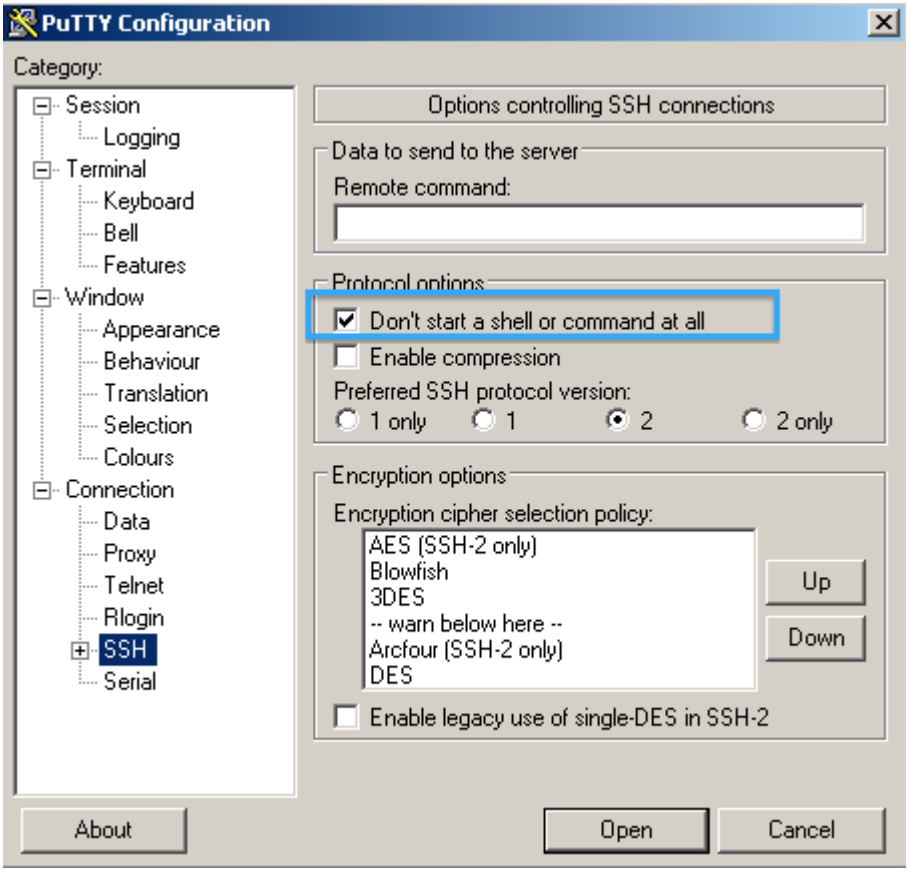
USA (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



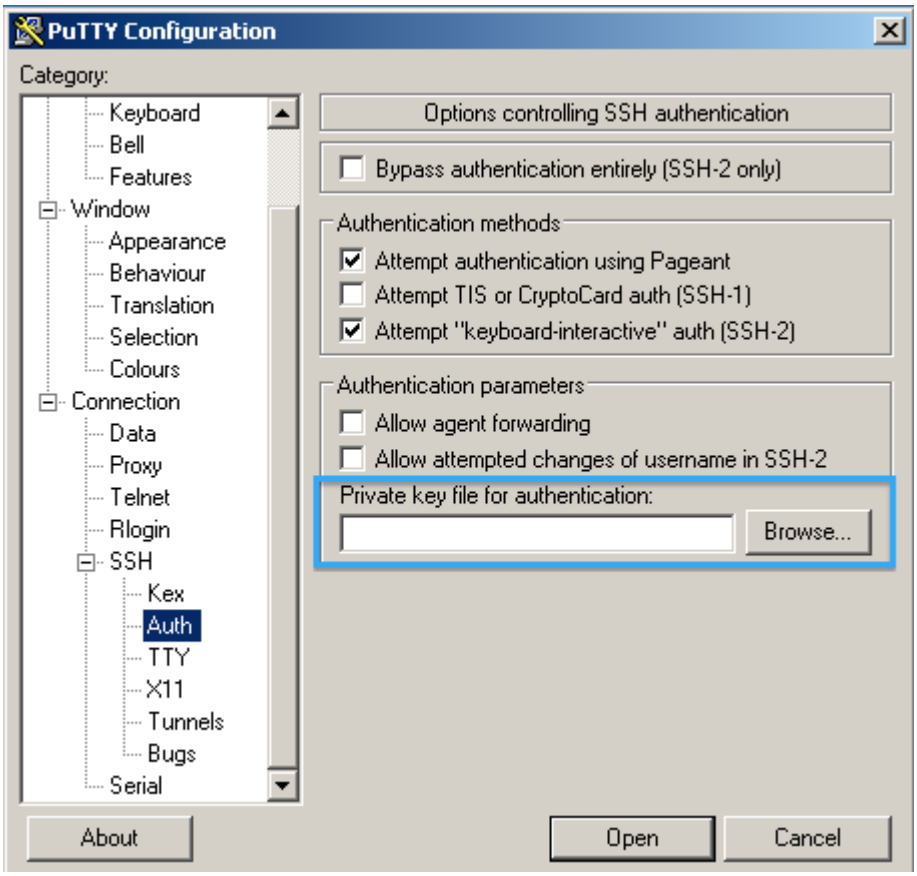
Klicken Sie aufDataAnd, und geben Sie den Benutzernamen für die automatische Anmeldung und den dh-user ein.



Wählen Sie SSH und aktivieren Sie Keine Shell oder keinen Befehl starten.

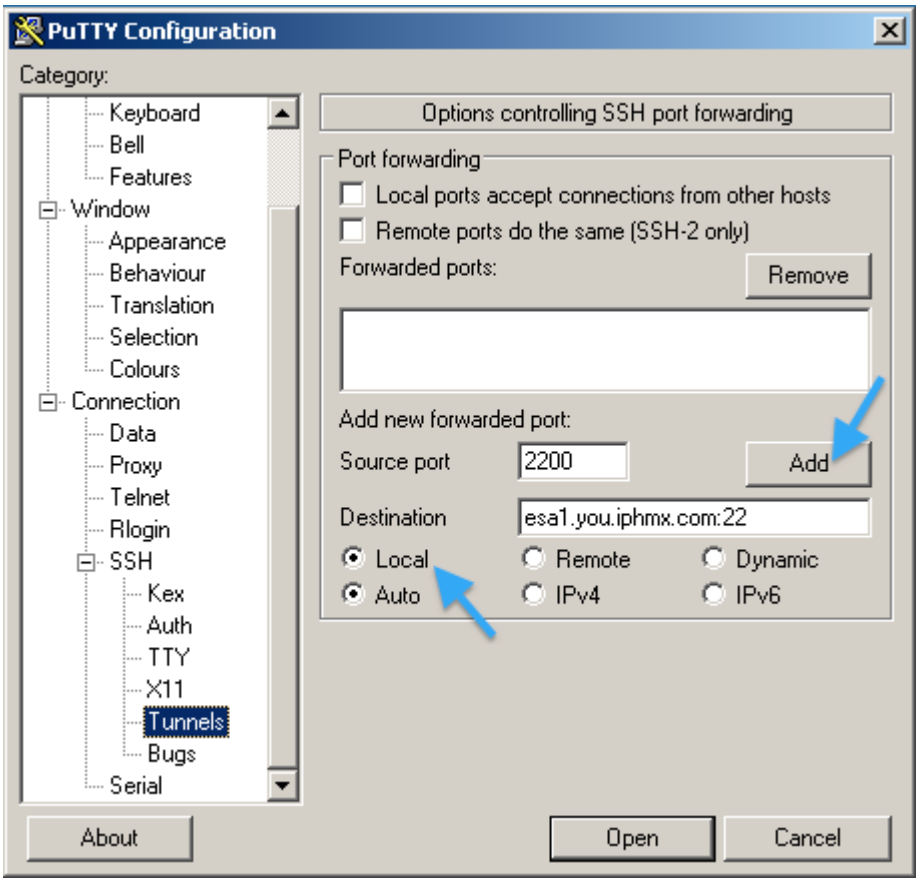


Klicken Sie auf Authand for Private key file (Authentifizierung für private Schlüsseldatei), suchen Sie nach dem privaten Schlüssel, und wählen Sie ihn aus.

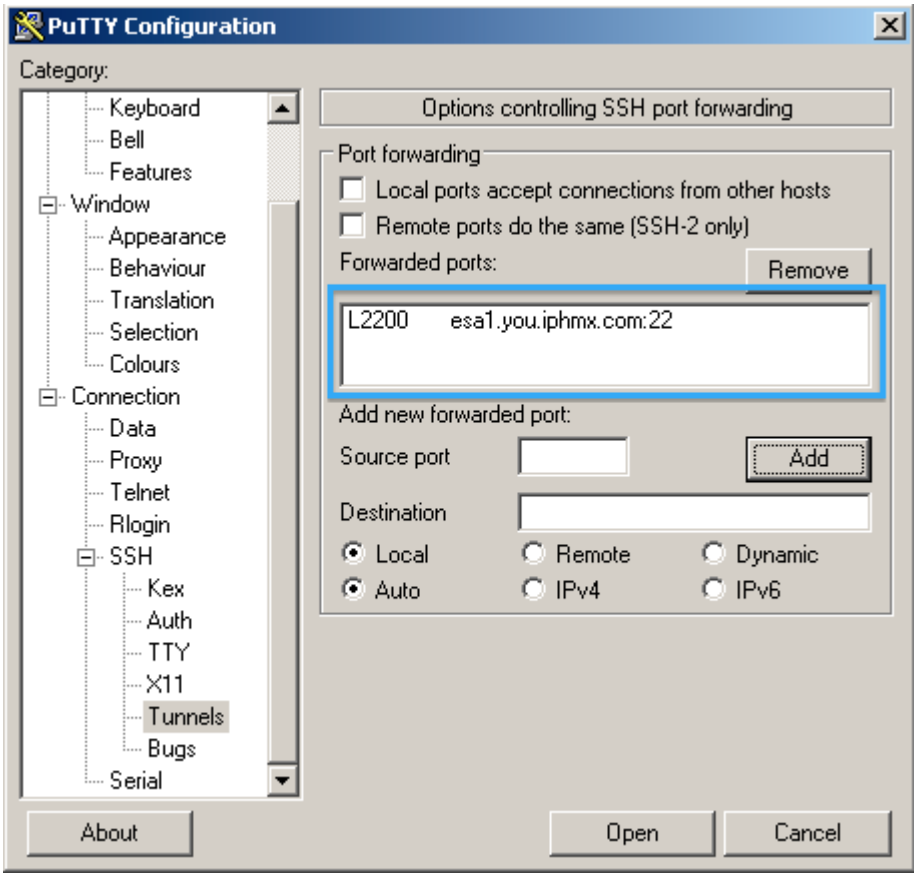


Klicken Sie auf Tunnel.

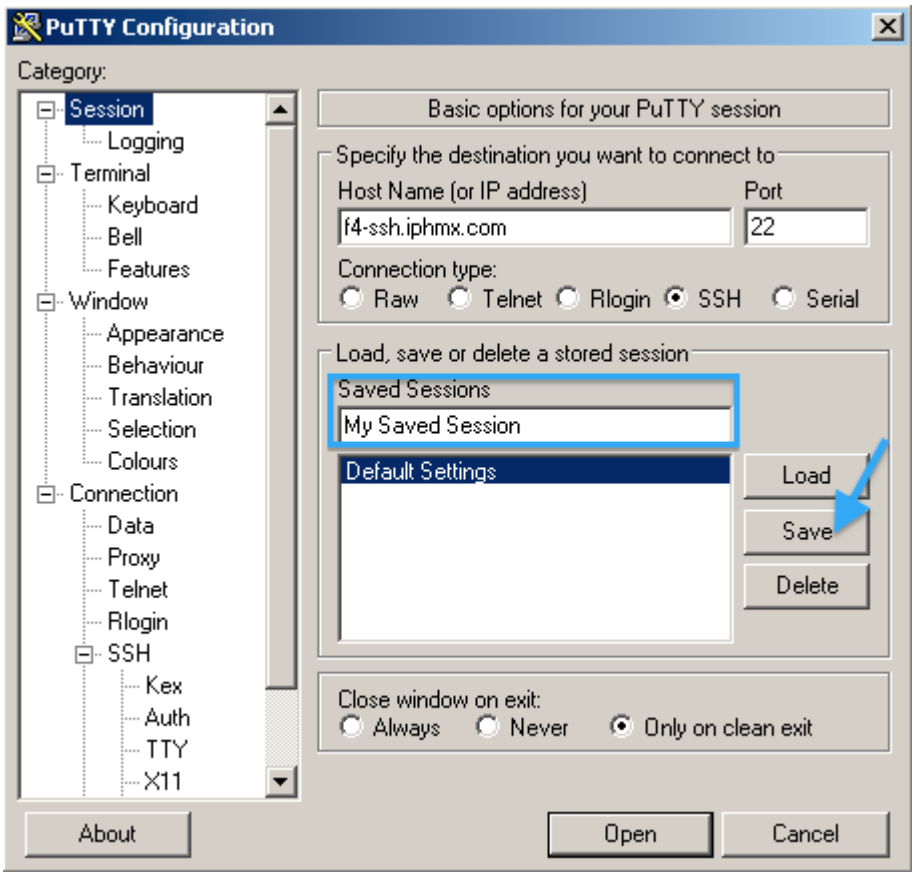
Geben Sie einen Quellport ein. Dies ist ein beliebiger Port Ihrer Wahl (Beispiel verwendet 2200).
Geben Sie ein Ziel ein. dies ist Ihre ESA oder SMA + 22 (Angabe der SSH-Verbindung).



Nachdem Sie auf Hinzufügen geklickt haben, muss es wie folgt aussehen.

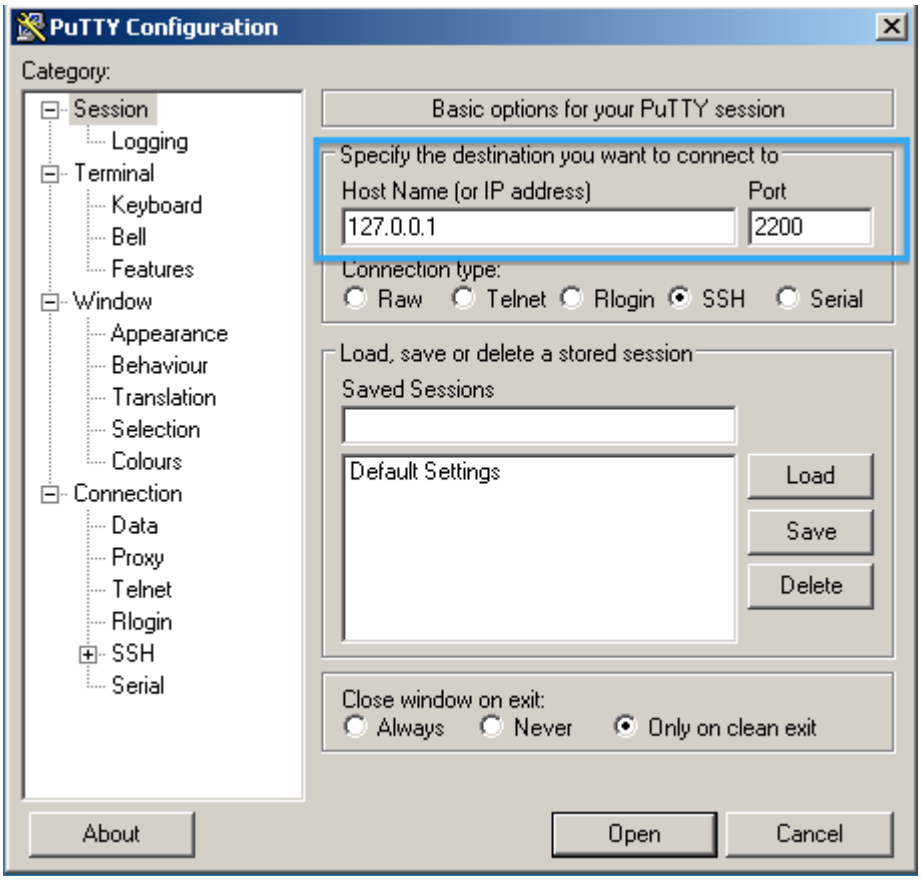


Um die Sitzung zur späteren Verwendung zu speichern, klicken Sie auf Sitzung.
Geben Sie einen Namen für Ihre "Gespeicherte Sitzung" ein, und klicken Sie auf Speichern.



Zu diesem Zeitpunkt können Sie auf Öffnen klicken und die Proxy-Sitzung starten.
Es gibt keine Anmelde- oder Eingabeaufforderung. Sie müssen nun eine zweite PuTTY-Sitzung für Ihre ESA oder SMA öffnen.

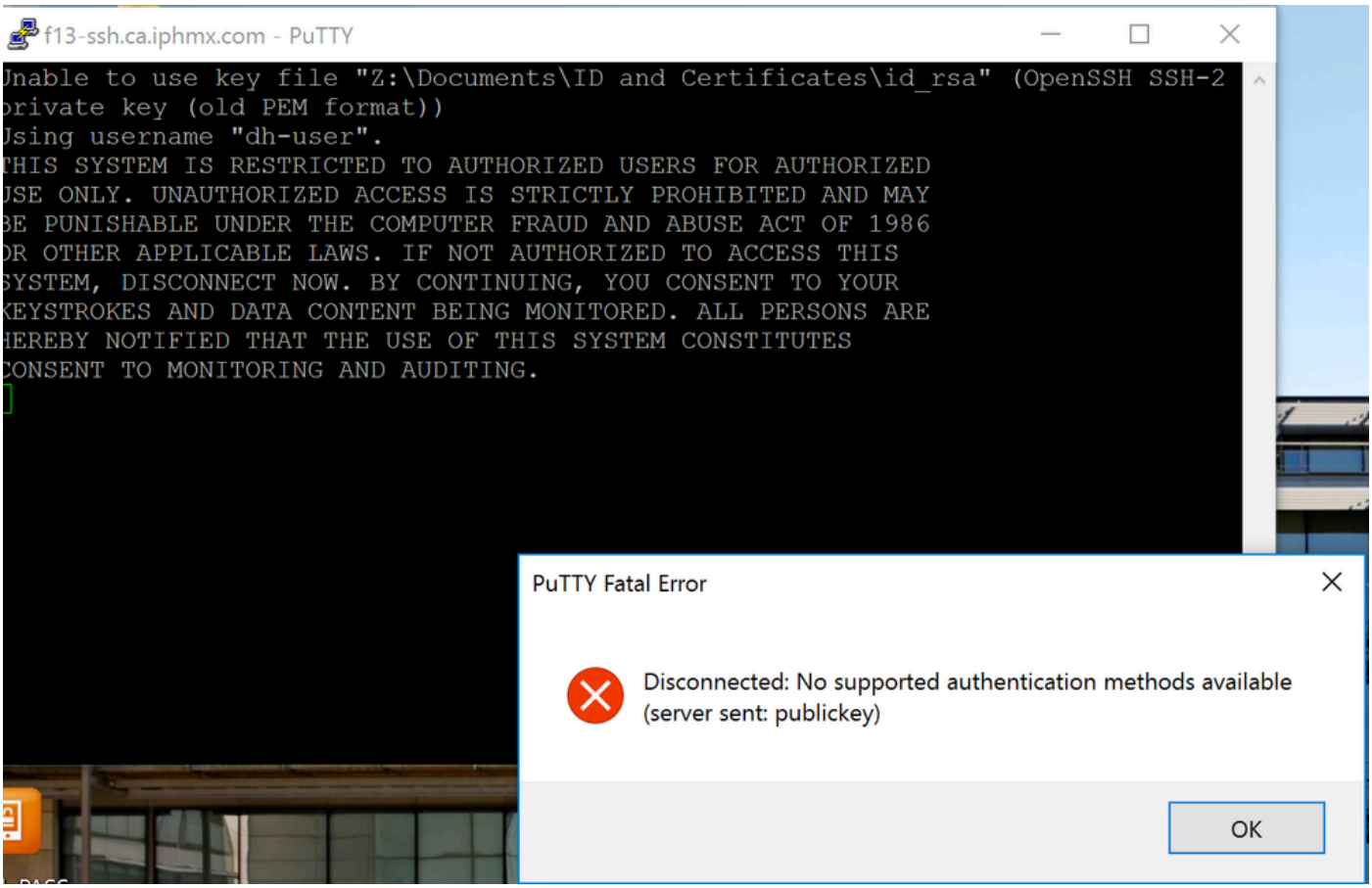
Verwenden Sie den Hostnamen 127.0.0.1 und die Quellportnummer in der zuvor gezeigten Tunnelkonfiguration.
Für dieses Beispiel wird 2200 verwendet.
Klicken Sie auf Öffnen, um eine Verbindung mit der Appliance herzustellen.



Wenn Sie dazu aufgefordert werden, geben Sie den Benutzernamen und das Kennwort der Appliance ein. Dies entspricht dem Benutzernamen und dem Kennwort für den Benutzeroberflächenzugriff.

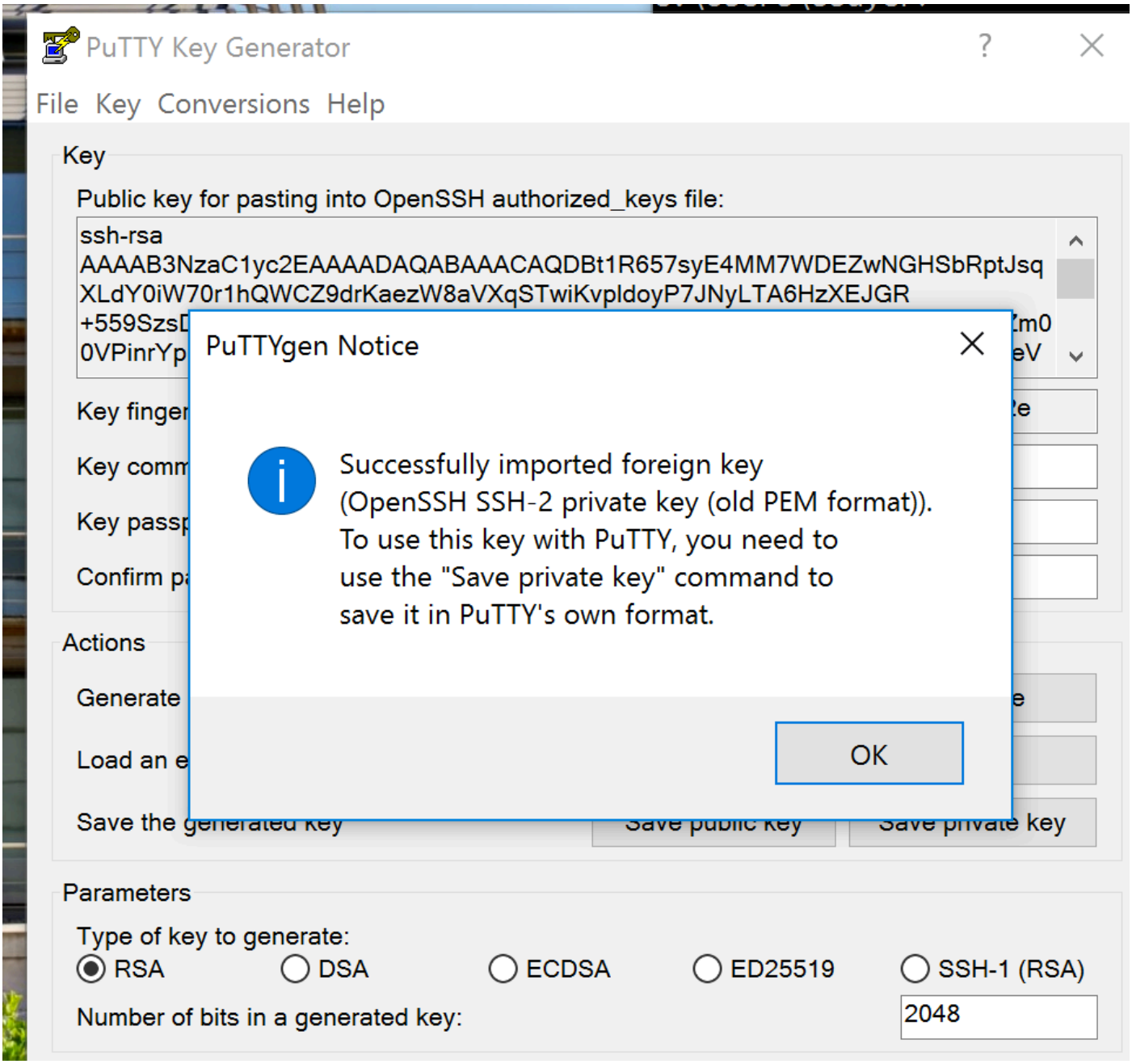
Fehlerbehebung

Wenn Ihr SSH-Schlüsselpaar mit OpenSSH (kein PuTy) generiert wurde, können Sie keine Verbindung herstellen und erhalten einen Fehler im "alten PEM-Format".



Der private Schlüssel kann [mit dem PuTTY Key Generator] konvertiert werden.

- Öffnen Sie PuTy Key Generator.
- Klicken Sie auf Bestellung laden, um den vorhandenen privaten Schlüssel zu durchsuchen und zu laden.
- Sie müssen auf das Dropdown-Menü klicken und Alle Dateien (.) auswählen, damit Sie den privaten Schlüssel suchen können.
- Klicken Sie auf Öffnen, sobald Sie den privaten Schlüssel gefunden haben.
- Puttygen wird einen Hinweis wie in diesem Bild.



- Klicken Sie auf Privaten Schlüssel speichern.
- Verwenden Sie in Ihrer PuTTY-Sitzung diesen konvertierten privaten Schlüssel, und speichern Sie die Sitzung.
- Versuchen Sie, erneut eine Verbindung mit dem konvertierten privaten Schlüssel herzustellen.

Bestätigen Sie, dass Sie über die Befehlszeile auf die Appliances zugreifen können.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.