Cisco Cloud Email Security CLI-toegang aanvragen

Inhoud

Inleiding

In dit document wordt beschreven hoe u toegang kunt aanvragen tot hun CLI voor Cloud Email Security (CES).

Achtergrondinformatie

Cisco CES-klanten hebben recht op toegang tot de CLI van hun ESA en SMA die worden geleverd via een SSH-proxy met behulp van sleutelverificatie. CLI-toegang tot uw gehoste apparaten moet worden beperkt tot belangrijke personen binnen uw organisatie.

Linux en Mac gebruikers

Voor Cisco CES-klanten:
Instructies voor een shell-script dat SSH gebruikt om CLI-toegang via CES-proxy te maken.

Voorwaarden

Als CES-klant moet u CES On-Boarding/Ops of Cisco TAC hebben ingeschakeld om SSH-sleutels te laten uitwisselen en plaatsen:

1. Genereer private/publieke RSA-sleutel(s).
2. Geef uw PublicRSA-sleutel aan Cisco.
3. Wacht tot Cisco uw sleutel(s) heeft opgeslagen in uw CES-klantaccount en laat u weten dat deze zijn opgeslagen.
4. Kopieer en wijzig het script connect2ces.sh.

Hoe maak ik private/publieke RSA-sleutels?

Cisco raadt het gebruik van 'ssh-keygen' aan op de terminal/CLI voor Unix/Linux/OS X. Gebruik de opdracht ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NAME>.

Opmerking: Ga voor meer informatie naar https://www.ssh.com/academy/ssh/keygen.
Zorg ervoor dat u te allen tijde de toegang tot uw RSA-privésleutels beveiligt.
Stuur uw privésleutel niet naar Cisco, alleen de openbare sleutel (.pub).
Wanneer u uw openbare sleutel bij Cisco indient, identificeert u het e-mailadres/de voornaam/achternaam waarvoor de sleutel is bedoeld.

Hoe open ik een ondersteuningsverzoek van Cisco om mijn publieke sleutel te verstrekken?

Navigeer naar deze link.

Zorg ervoor dat u de SR correct identificeert als 'Cisco CES Customer SSH / CLI Setup', enzovoort.

Configuratie

Om aan de slag te gaan, opent u het geleverde script en gebruikt u een van deze proxyhosts voor de hostnaam.

Zorg ervoor dat u de juiste proxy voor uw regio kiest (dat wil zeggen, als u een Amerikaanse CES-klant bent, om F4-datacenters en -apparaten te bereiken, gebruikt u de f4-ssh.iphmx.com. Als u een EU CES-klant bent met een toestel in Duits DC, gebruikt u 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)(Duits DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

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

Wat als ik verbinding wil maken met meer dan één e-mailbeveiligingsapparaat (ESA) of beveiligingsbeheerapparaat (SMA)?

Kopieer en bewaar een tweede kopie van connect2ces.sh, zoals connect2ces_2.sh.

Opmerking: U wilt de 'cloud_host' bewerken om het extra toestel te zijn dat u wilt openen. U wilt de 'local_port' wijzigen in iets ANDERS dan 2222. Als dit niet het geval is, ontvangt u een foutmelding: "WAARSCHUWING: IDENTIFICATIE VAN EXTERNE HOST IS GEWIJZIGD!"

Hoe kan ik mijn ESA of SMA configureren om in te loggen zonder om een wachtwoord te vragen?

Lees deze gids.

Hoe ziet dat eruit als ik de voorwaarden heb vervuld?

joe.user@my_local > ~ ./connect2ces
[-] Verbinding maken met uw proxyserver (f4-ssh.iphmx.com)...
[-] Proxyverbinding succesvol. Nu verbonden met f4-ssh.iphmx.com.
[-] proxy met PID: 31253
[-] Aansluiten op uw CES-toestel (esa1.rs1234-01.iphmx.com)...

Laatste aanmelding: ma apr 22 11:33:45 2019 van 10.123.123.123
AsyncOS 12.1.0 voor Cisco C100V build 071

Welkom bij de Cisco C100V Email Security Virtual Appliance

OPMERKING: Deze sessie verloopt als deze 1440 minuten niet wordt gebruikt. Alle niet-vastgelegde configuratiewijzigingen gaan verloren. Wijzig de configuratie zodra ze zijn gemaakt.

(Systeem: esa1.rs1234-01.iphmx.com)>
(Machine esa1.rs1234-01.iphmx.com)> afsluiten

Verbinding met 127.0.0.1 gesloten.
[-] Proxyverbinding wordt gesloten...
[-] Klaar.

connect2ces.sh

Opmerking: Zorg ervoor dat u de juiste proxy voor uw regio kiest (dat wil zeggen, als u een Amerikaanse CES-klant bent, om F4-datacenters en -apparaten te bereiken, gebruikt u de f4-ssh.iphmx.com. Als u een EU CES-klant bent met een toestel in Duits DC, gebruikt u f17-ssh.eu.iphmx.com.).

```
#!/bin/bash

#-- BEWERK DE ONDERSTAANDE WAARDEN ------------------------
# De volgende waarden moeten al worden vastgesteld met CES:
# cloud_user="gebruikersnaam"
# cloud_host="esaX.CUSTOMER.iphmx.com" of "smaX.CUSTOMER.iphmx.com"
## [ZORG ERVOOR DAT U DE JUISTE REGIONALE CES-DATACENTERSET HEBT!]
# private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
# proxy_server="PROXY_SERVER" [SELECTEER ER MAAR ÉÉN!]
#
## Voor 'proxy_server' zijn dit SSH-proxies:
##
## 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)(Duits DC)
## f17-ssh.eu.iphmx.com
## f18-ssh.eu.iphmx.com
##
## VS (iphmx.com)
## f4-ssh.iphmx.com
## f5-ssh.iphmx.com
```

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

#-- LAAT DEZE WAARDEN ONGEWIJZIGD --------------------
# 'proxy_user' mag niet worden gewijzigd
# 'remote_port' blijft 22 (SSH)
# 'local_port' kan worden ingesteld op verschillende waarden, indien nodig

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

#-- BEWERK NIET ONDER DEZE REGEL ------------------

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

print "[-] Verbinding maken met uw proxyserver ($proxy_server)...\n"
$proxycmd >/dev/null 2>&1
Als nc -z 127.0.0.1 $local_port >/dev/null 2>&1; dan
afdrukken "[-] Proxyverbinding gelukt. Nu verbonden met $proxy_server.\n"
anders
afdrukken "[-] Proxyverbinding mislukt. Bezig met stoppen...\n"
uitgang
fi

# Proxyssh-proces zoeken
proxypid=`ps -xo PID, opdracht | grep "$cloud_host" | grep "$proxy_server" | head -n1 | SED "S/^[
\t]*//" | cut -d " " -f1"
print "[-] proxy uitgevoerd op PID: $proxypid\n"

print "[-] Verbinding maken met uw CES-toestel ($cloud_host)...\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

print "[-] Proxyverbinding sluiten...\n"
$proxypid doden

print "[-] Done.\n"

#-- Wil je voorkomen dat je elke keer een wachtwoord moet typen?
#-- Zie: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-
technote-esa-00.html
#-- Toegang nodig tot meer dan één ESA of SMA? Kopieer hetzelfde script en hernoem naar
connect2ces_2.sh, of vergelijkbaar.
```

Originele document: https://github.com/robsherw/connect2ces.

Windows-gebruikers

Instructies voor het gebruik van PuTTY en het gebruik van SSH om CLI-toegang via CES-proxy te maken.

Voorwaarden

Als CES-klant moet u CES On-Boarding/Ops of Cisco TAC hebben ingeschakeld om SSH-sleutels te laten uitwisselen en plaatsen:

1. Genereer private/publieke RSA-sleutel(s).
2. Geef Cisco uw openbare RSA-sleutel.
3. Wacht op Cisco om uw sleutel(s) op te slaan en u te laten weten dat deze zijn opgeslagen in uw CES-klantenaccount.
4. Stel PuTTY in zoals hier in deze instructies wordt beschreven.

Hoe maak ik private/publieke RSA-sleutels?

Cisco raadt het gebruik van PuTTYgen (https://www.puttygen.com/) voor Windows.

Voor meer informatie: https://www.ssh.com/ssh/putty/windows/puttygen.

Opmerking: Zorg ervoor dat u te allen tijde de toegang tot uw RSA-privésleutels beveiligt. Stuur uw privésleutel niet naar Cisco, alleen de openbare sleutel (.pub). Wanneer u uw openbare sleutel bij Cisco indient, identificeert u het e-mailadres/de voornaam/achternaam waarvoor deze sleutel is.

Hoe open ik een ondersteuningsverzoek van Cisco om mijn publieke sleutel te verstrekken?

Navigeer naar deze link.

Zorg ervoor dat u de SR correct identificeert als 'Cisco CES Customer SSH / CLI Setup', enzovoort.

Hoe kan ik mijn ESA of SMA configureren om in te loggen zonder om een wachtwoord te vragen?

Lees deze gids.

PuTTy-configuratie

Om aan de slag te gaan, opent u PuTTY en gebruikt u een van deze proxyhosts voor de hostnamen:

Zorg ervoor dat u de juiste proxy voor uw regio kiest (dat wil zeggen, als u een Amerikaanse CES-klant bent, om F4-datacenters en -apparaten te bereiken, gebruikt u de f4-ssh.iphmx.com. Als u een EU CES-klant bent met een toestel in Duits DC, gebruikt u f17-ssh.eu.iphmx.com.).

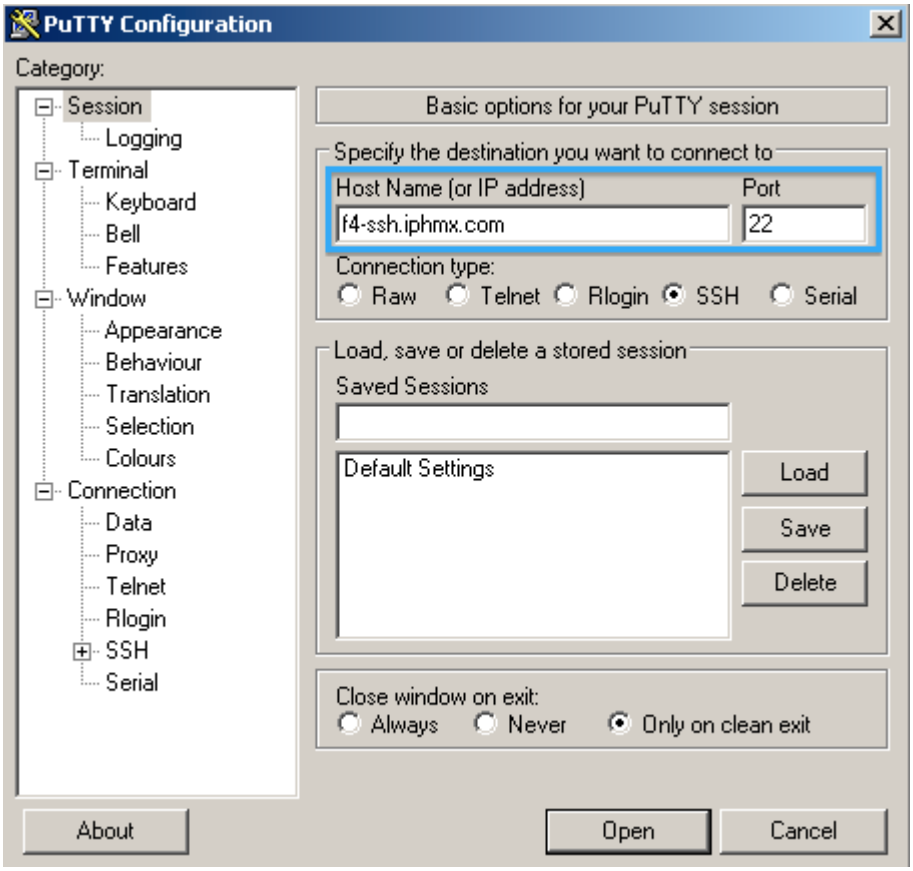
AP (ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

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

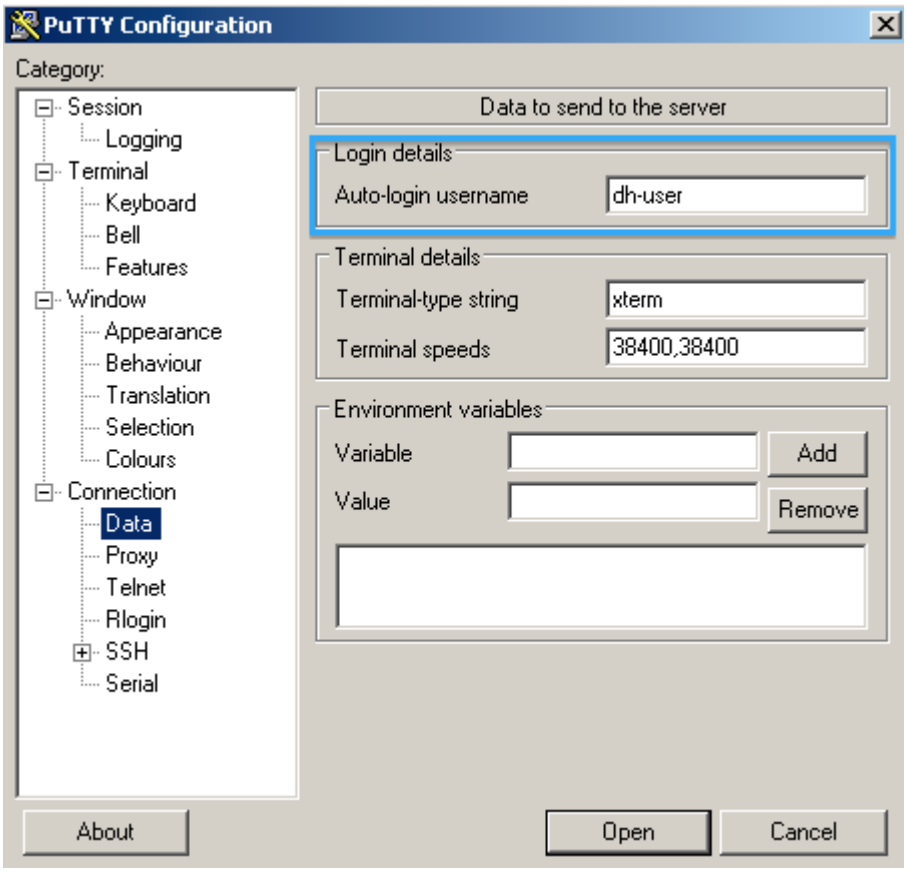
EU (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

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

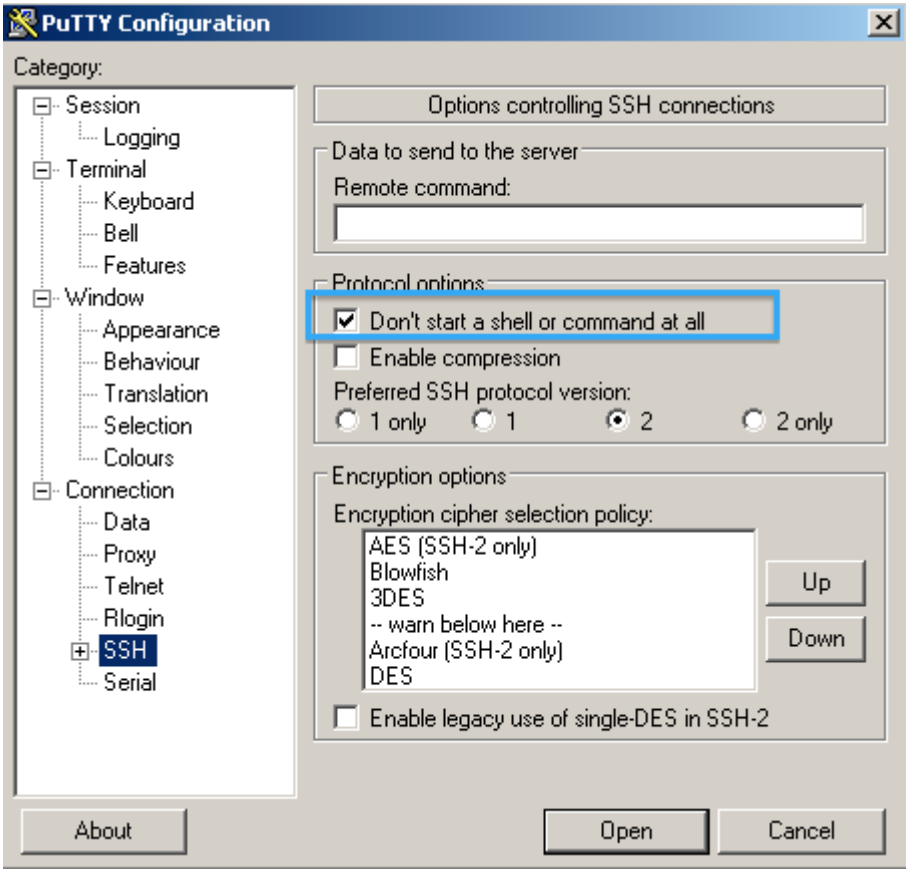
VS (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



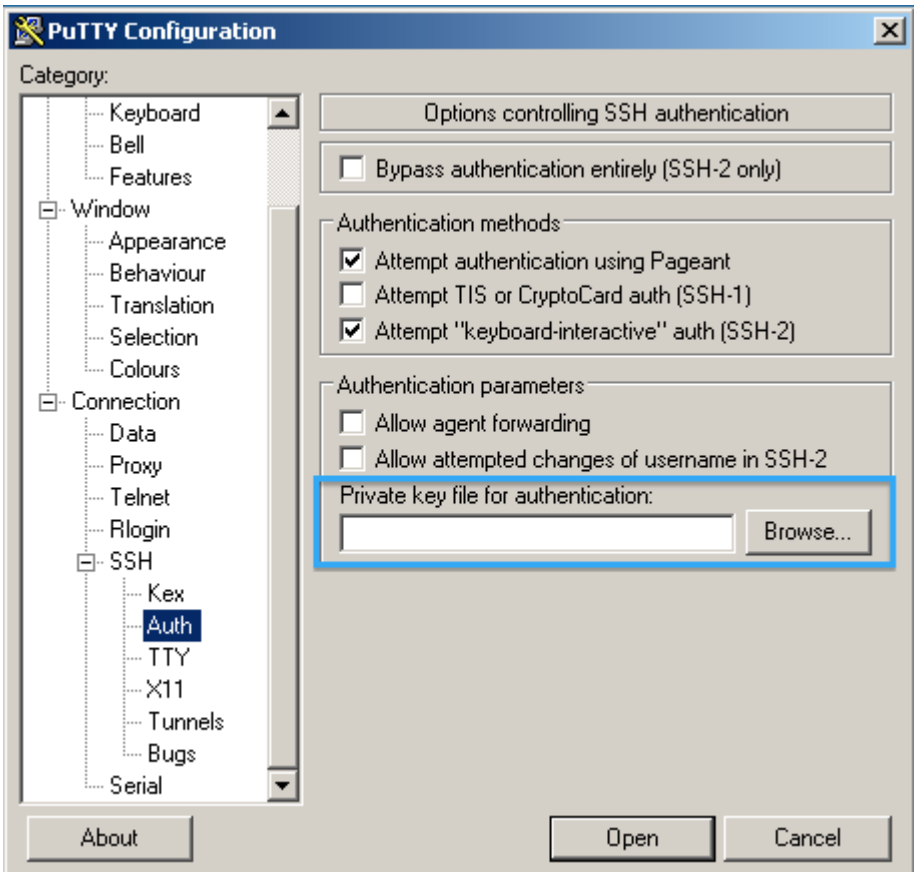
Klik opData en voor inloggegevens gebruikt u de gebruikersnaam voor automatische aanmelding en voert u dh-user in.



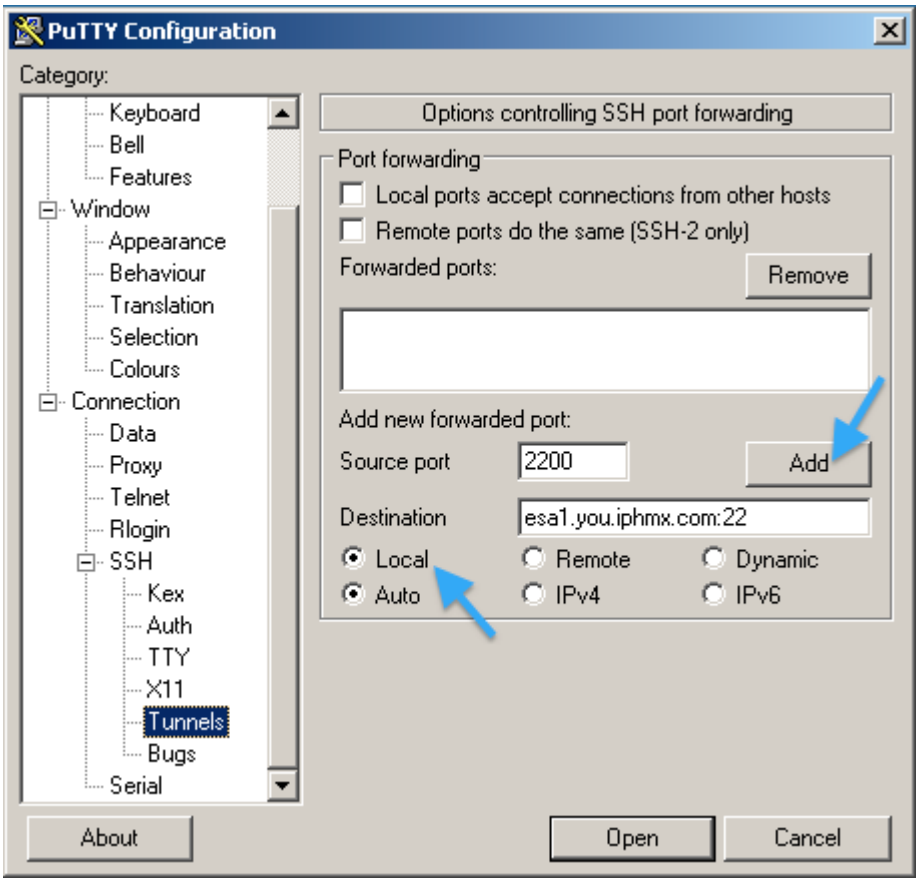
Kies SSH en controleer of u helemaal geen shell of opdracht start.



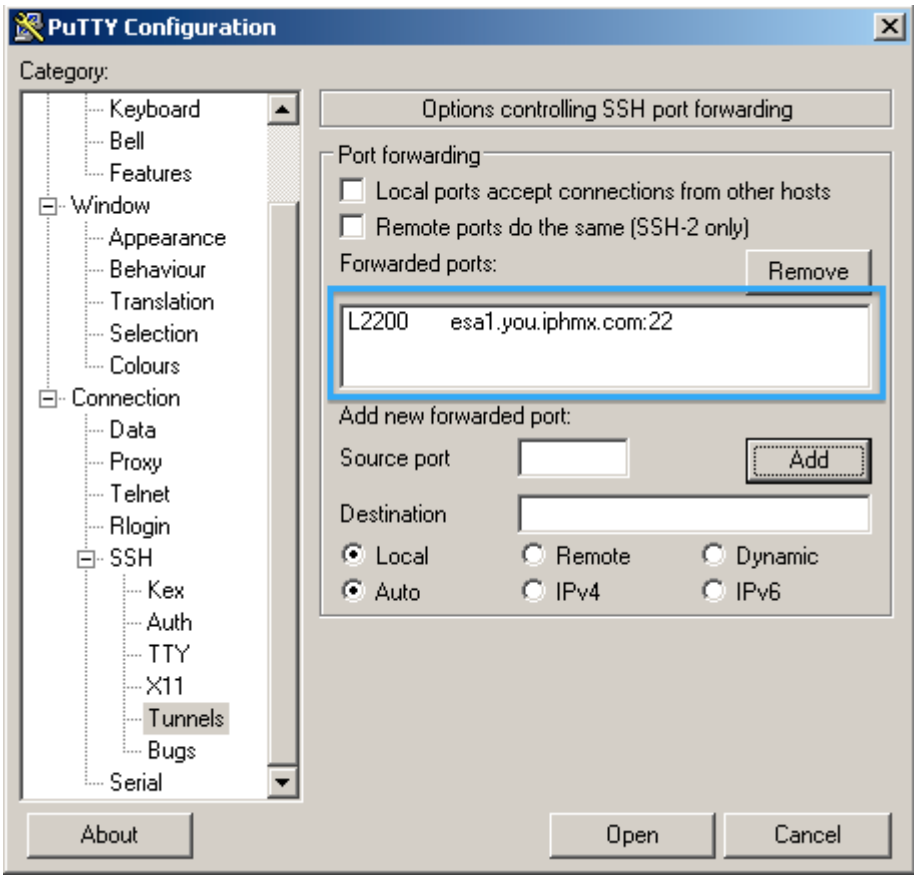
Klik op Auteur voor privésleutelbestand voor verificatie, blader en kies uw privésleutel.



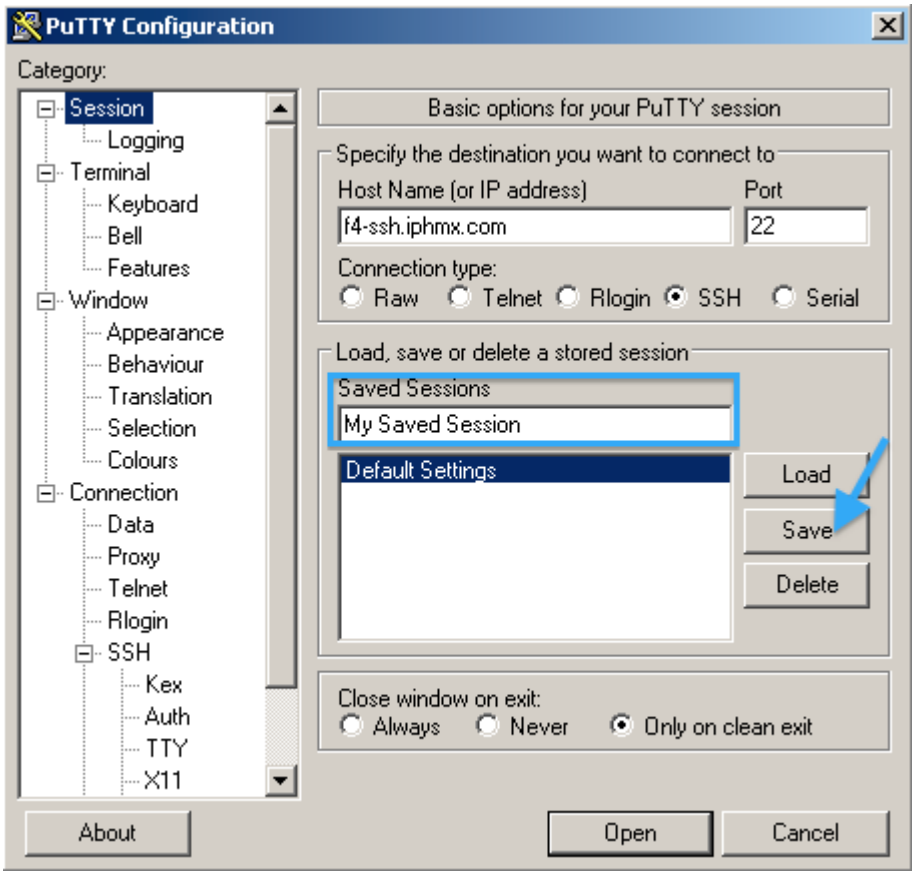
Klik op Tunnels.
Voer een bronpoort in; dit is een willekeurige poort naar keuze (voorbeeld gebruikt 2200).
Voer aDestination in; dit is uw ESA of SMA + 22 (met vermelding van SSH-verbinding).



Nadat u op Toevoegen klikt, moet het er zo uitzien.

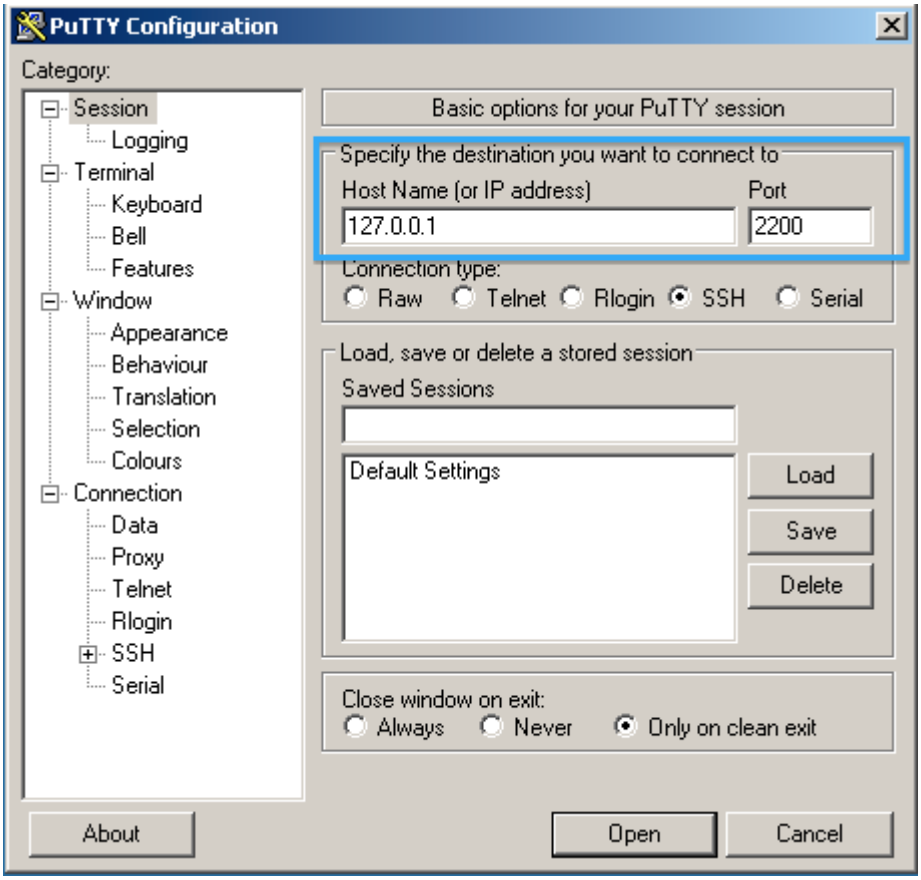


Om de sessie op te slaan voor toekomstig gebruik, klikt u op Sessie.
Voer een naam in voor de 'Opgeslagen sessie' en klik op Opslaan.



U kunt nu op Openen klikken en de proxysessie starten.
Er zal geen login of opdrachtprompt zijn. U moet nu een tweede PuTTY-sessie openen voor uw ESA of SMA.

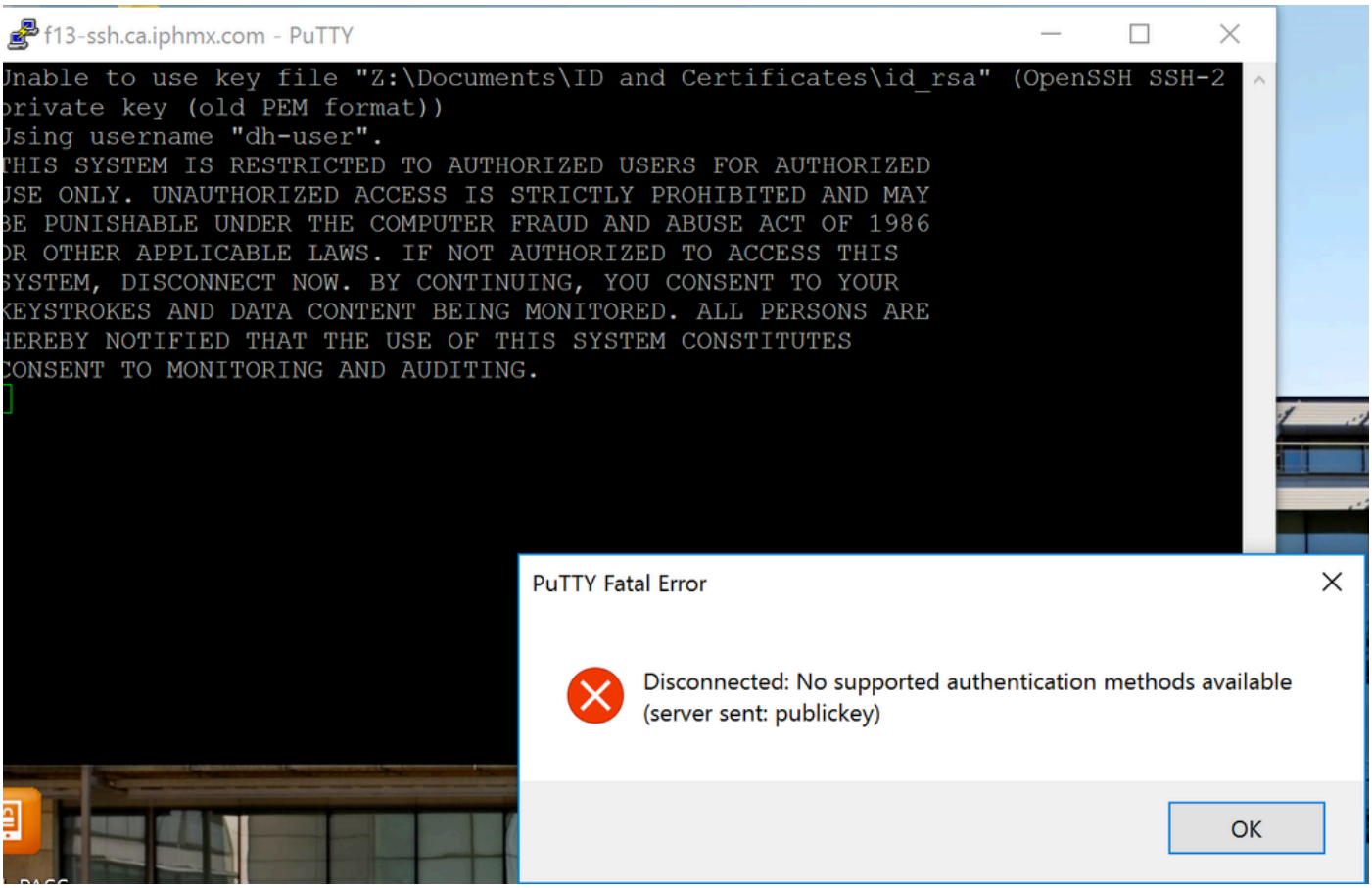
Gebruik de hostnaam 127.0.0.1 en gebruik het bronpoortnummer in de tunnelconfiguratie die eerder is weergegeven.
Voor dit voorbeeld wordt 2200 gebruikt.
Klik op Openen om verbinding te maken met uw toestel.



Wanneer u wordt gevraagd om uw toestelgebruikersnaam en wachtwoord te gebruiken, hetzelfde als bij UI-toegang.

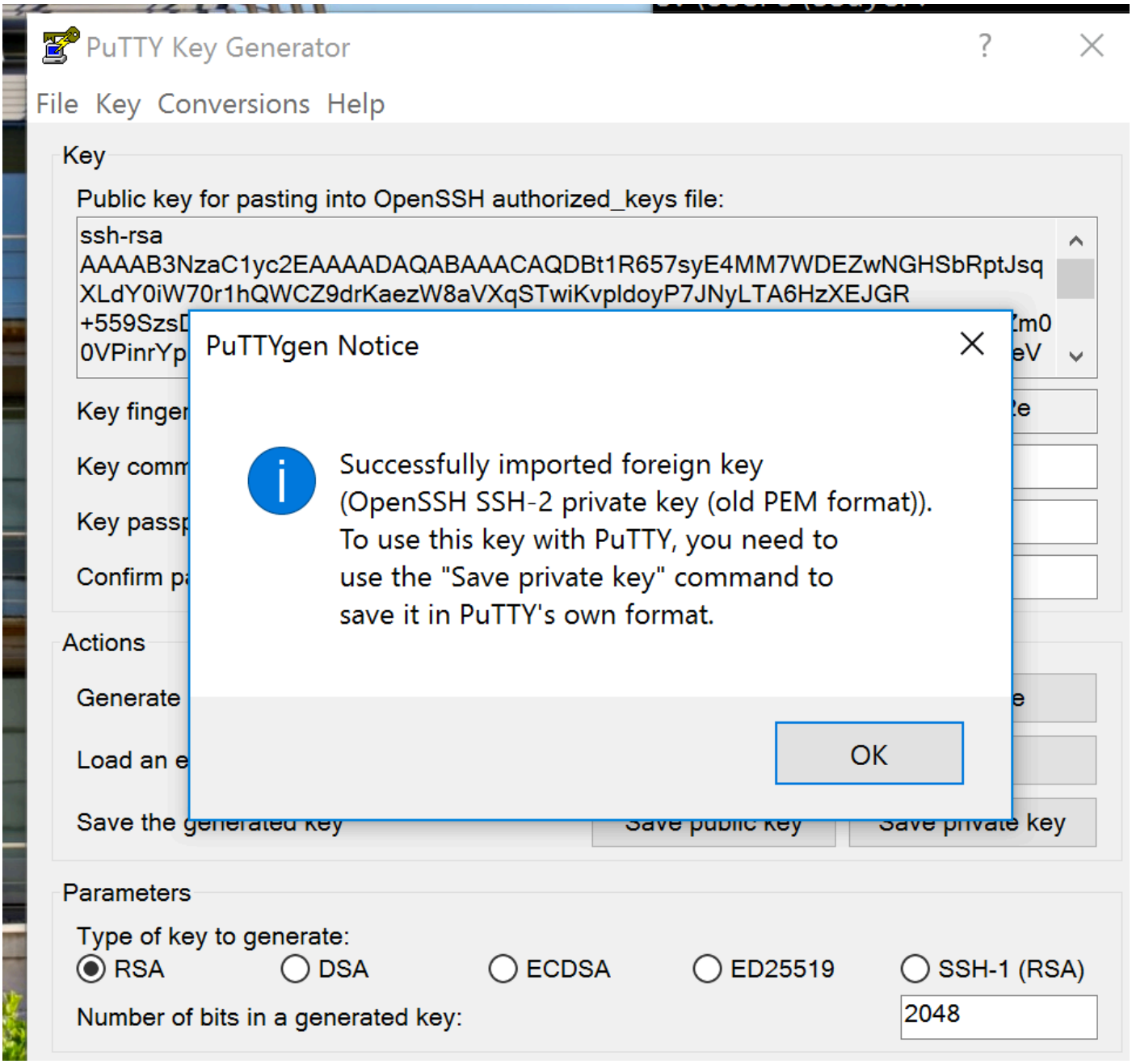
Probleemoplossing

Als uw SSH-sleutelpaar is gegenereerd met behulp van OpenSSH (niet-PuTTy), kunt u geen verbinding maken en krijgt u een "oude PEM-indeling" -fout te zien.



De privésleutel kan worden geconverteerd met PuTTY Key Generator.

- Open de PuTTy-sleutelgenerator.
- Klik op Laden om door uw bestaande privésleutel te bladeren en deze te laden.
- U moet op de vervolgkeuzelijst klikken en Alle bestanden (.) kiezen, zodat u de privésleutel kunt vinden.
- Klik op Openen zodra u uw privésleutel hebt gevonden.
- Puttygen zal een melding als in deze afbeelding geven.



- Klik op Privésleutel opslaan.
- Gebruik vanaf uw PuTTY-sessie deze geconverteerde privésleutel en sla de sessie op.
- Probeer opnieuw verbinding te maken met de geconverteerde privésleutel.

Bevestig dat u toegang hebt tot uw apparaten via de opdrachtregel.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.