Richiesta di accesso Cisco Cloud Email Security CLI

Sommario

Introduzione

Questo documento descrive come richiedere l'accesso alla CLI di Cloud Email Security (CES).

Premesse

I clienti Cisco CES hanno diritto ad accedere alla CLI dell'ESA e dell'SMA forniti tramite un proxy SSH utilizzando l'autenticazione a chiave. L'accesso CLI alle appliance ospitate deve essere limitato ai principali utenti dell'organizzazione.

Utenti Linux e Mac

Per i clienti Cisco CES:
Istruzioni per uno script shell che utilizza SSH per consentire l'accesso CLI tramite il proxy CES.

Prerequisiti

In qualità di cliente CES, per poter scambiare e posizionare le chiavi SSH, è necessario aver

contattato il servizio CES di onboarding/assistenza o Cisco TAC:

1. Generare una o più chiavi RSA pubbliche/private.
2. Fornire a Cisco la chiave PublicRSA.
3. Attendere che Cisco salvi e informarvi che le vostre chiavi sono state salvate nel vostro account cliente CES.
4. Copiare e modificare lo script connect2ces.sh.

Come creare le chiavi RSA private/pubbliche?

Cisco consiglia di utilizzare 'ssh-keygen' sul terminale/CLI per Unix/Linux/OS X. Usare il comando ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NOME>.

Nota: Per ulteriori informazioni, visitare il sito https://www.ssh.com/academy/ssh/keygen.
Garantire sempre l'accesso sicuro alle chiavi private RSA.
Non inviare la chiave privata a Cisco, ma solo la chiave pubblica (.pub).
Quando invii la chiave pubblica a Cisco, identifica l'indirizzo e-mail/nome/cognome a cui la chiave è destinata.

Come aprire una richiesta di supporto Cisco per fornire la chiave pubblica?

Passare a questo collegamento.

Accertarsi di aver identificato correttamente la SR come "Cisco CES Customer SSH/CLI Setup", ecc.

Configurazione

Per iniziare, aprire la copia dello script fornito e usare uno di questi host proxy per il nome host.

Assicurarsi di scegliere il proxy corretto per la propria area geografica (se si è un cliente US CES, per raggiungere il centro dati e le appliance F4, utilizzare il sito f4-ssh.iphmx.com). Se si è un cliente CES dell'UE con un'appliance nella Repubblica democratica tedesca, utilizzare 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

UE (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com

f11-ssh.c3s2.iphmx.com

EU (eu.iphmx.com) (Repubblica democratica tedesca)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

STATI UNITI (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com

Cosa succede se si desidera connettersi a più appliance Email Security Appliance (ESA) o Security Management Appliance (SMA)?

Copiare e salvare una seconda copia di connect2ces.sh, ad esempio connect2ces_2.sh.

Nota: Modificare 'cloud_host' in modo che diventi l'appliance aggiuntiva a cui si desidera accedere.
Modificare 'local_port' in modo che sia diverso da 2222. In caso contrario, si riceverà un messaggio di errore, "WARNING: L'IDENTIFICAZIONE DELL'HOST REMOTO È CAMBIATA!"

Come configurare l'ESA o l'SMA per l'accesso senza richiedere una password?

Leggere questa guida.

Che aspetto può avere una volta completati i prerequisiti?

joe.user@my_local > ~ ./connect2ces
[-] Connessione al server proxy (f4-ssh.iphmx.com) in corso...
[-] Connessione proxy riuscita. Ora connesso a f4-ssh.iphmx.com.
[-] proxy in esecuzione sul PID: 31253
[-] Connessione all'accessorio CES (esa1.rs1234-01.iphmx.com) in corso...

Ultimo accesso: lun apr 22 11:33:45 2019 da 10.123.123.123
AsyncOS 12.1.0 per Cisco C100V build 071

Benvenuti in Cisco C100V Email Security Virtual Appliance

NOTA: Questa sessione scadrà se viene lasciata inattiva per 1440 minuti. Tutte le modifiche di configurazione di cui non è stato eseguito il commit verranno perse. Eseguire il commit delle modifiche di configurazione non appena vengono apportate.

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

Connessione a 127.0.0.1 chiusa.
[-] Chiusura della connessione proxy in corso...
[-] Fine.

connect2ces.sh

Nota: assicurarsi di scegliere il proxy corretto per la propria area (se si è un cliente US CES, per raggiungere il centro dati e gli accessori F4, utilizzare il sito f4-ssh.iphmx.com. Se si è un cliente CES dell'UE con un'appliance nella Repubblica democratica tedesca, utilizzare f17-ssh.eu.iphmx.com.).

```
#!/bin/bash

#— MODIFICA I SEGUENTI VALORI —
# I seguenti valori devono essere già stabiliti con CES:
# cloud_user="nomeutente"
# cloud_host="esaX.CUSTOMER.iphmx.com" o "smaX.CUSTOMER.iphmx.com"
## [ASSICURARSI DI DISPORRE DEL SET DI CENTRI DATI CES APPROPRIATO A LIVELLO REGIONALE!]
# private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
# proxy_server="SERVER_PROXY" [SELEZIONARE UNA SOLA OPZIONE]
N.
## Per 'proxy_server', si tratta dei proxy SSH:
##
## punto di accesso (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
##
## UE (c3s2.iphmx.com)
## f10-ssh.c3s2.iphmx.com
## f11-ssh.c3s2.iphmx.com
##
## UE (eu.iphmx.com)(DC tedesco)
## f17-ssh.eu.iphmx.com
## f18-ssh.eu.iphmx.com
##
## STATI UNITI (iphmx.com)
## f4-ssh.iphmx.com
## f5-ssh.iphmx.com

cloud_user="nomeutente"
```

```
cloud_host="esaX.CUSTOMER.iphmx.com"
private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
proxy_server="SERVER_PROXY"

#— NON MODIFICATE QUESTI VALORI —
# 'proxy_user' non deve essere modificato
# 'porta_remota' rimane 22 (SSH)
# 'local_port' può essere impostato su un valore diverso, se necessario

proxy_user="utente-dh"
porta_remota=22
local_port=2222

#— NON MODIFICARE SOTTO QUESTA RIGA —

proxycmd="ssh -f -L $porta_locale:$cloud_host:$porta_remota -i $chiave_privata -N
$utente_proxy@$server_proxy"

printf "[-] Connessione al server proxy ($proxy_server)...\n"
$proxycmd >/dev/null 2>&1
if nc -z 127.0.0.1 $local_port >/dev/null 2>&1; quindi
printf "[-] Connessione proxy riuscita. Ora connesso a $proxy_server.\n"
Altrimenti
printf "[-] Connessione proxy non riuscita. Chiusura in corso...\n"
exit
fi

# Ricerca processo ssh proxy
proxypid=`ps -xo pid,comando | grep "$cloud_host" | grep "$proxy_server" | testa -n1 | sed "s/^[
\t]*//" | cut -d " " -f1"
printf "[-] proxy in esecuzione su PID: $proxypid\n"

printf "[-] Connessione all'appliance CES ($cloud_host) in corso...\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

printf "[-] Chiusura della connessione proxy in corso...\n"
uccidere $proxypid

printf "[-] Fine.\n"

#— Desiderate evitare di dover digitare la password ogni volta?
#— Vedere: https://www.cisco.com/c/en/us/support/docs/security/email-security-
appliance/118305-technote-esa-00.html
#— È necessario accedere a più ESA o SMA? Copiare lo stesso script e rinominarlo in
connect2ces_2.sh o in un file simile.
```

Documento originale:https://github.com/robsherw/connect2ces.

Utenti di Windows

Istruzioni per l'uso di PuTTy e dell'uso di SSH per effettuare l'accesso CLI tramite il proxy CES.

Prerequisiti

In qualità di cliente CES, è necessario aver contattato CES On-Boarding/Ops o Cisco TAC per scambiare e posizionare le chiavi SSH:

1. Generare una o più chiavi RSA pubbliche/private.
2. Fornire a Cisco la chiave RSA pubblica.
3. Attendere che Cisco salvi e informarvi che le vostre chiavi sono state salvate nel vostro account cliente CES.
4. Configurare PuTTY come descritto in queste istruzioni.

Come creare le chiavi RSA private/pubbliche?

Cisco consiglia di utilizzare PuTTYgen (https://www.puttygen.com/) per Windows.

Per ulteriori informazioni:https://www.ssh.com/ssh/putty/windows/puttygen.

Nota: Garantire sempre l'accesso sicuro alle chiavi private RSA.
Non inviare la chiave privata a Cisco, ma solo la chiave pubblica (.pub).
Quando invii la chiave pubblica a Cisco, identifica l'indirizzo e-mail/nome/cognome a cui si riferisce la chiave.

Come aprire una richiesta di supporto Cisco per fornire la chiave pubblica?

Passare a questo collegamento.

Accertarsi di aver identificato correttamente la SR come "Cisco CES Customer SSH/CLI Setup", ecc.

Come configurare l'ESA o l'SMA per l'accesso senza richiedere una password?

Leggere questa guida.

Configurazione PuTTy

Per iniziare, aprire PuTTY e usare uno dei seguenti host proxy per i nomi host:

Assicurarsi di scegliere il proxy corretto per la propria area geografica (se si è un cliente US CES, per raggiungere il centro dati e le appliance F4, utilizzare il sito f4-ssh.iphmx.com). Se si è un cliente CES dell'UE con un'appliance nella Repubblica democratica tedesca, utilizzare f17-

ssh.eu.iphmx.com.).

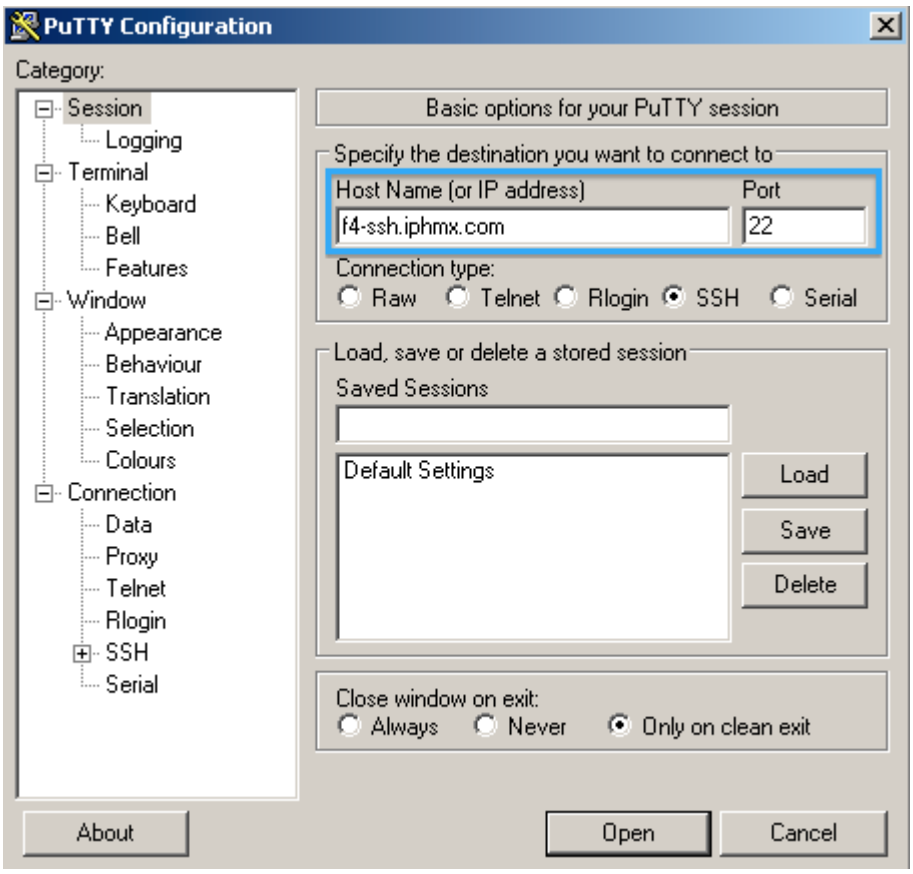
AP (ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

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

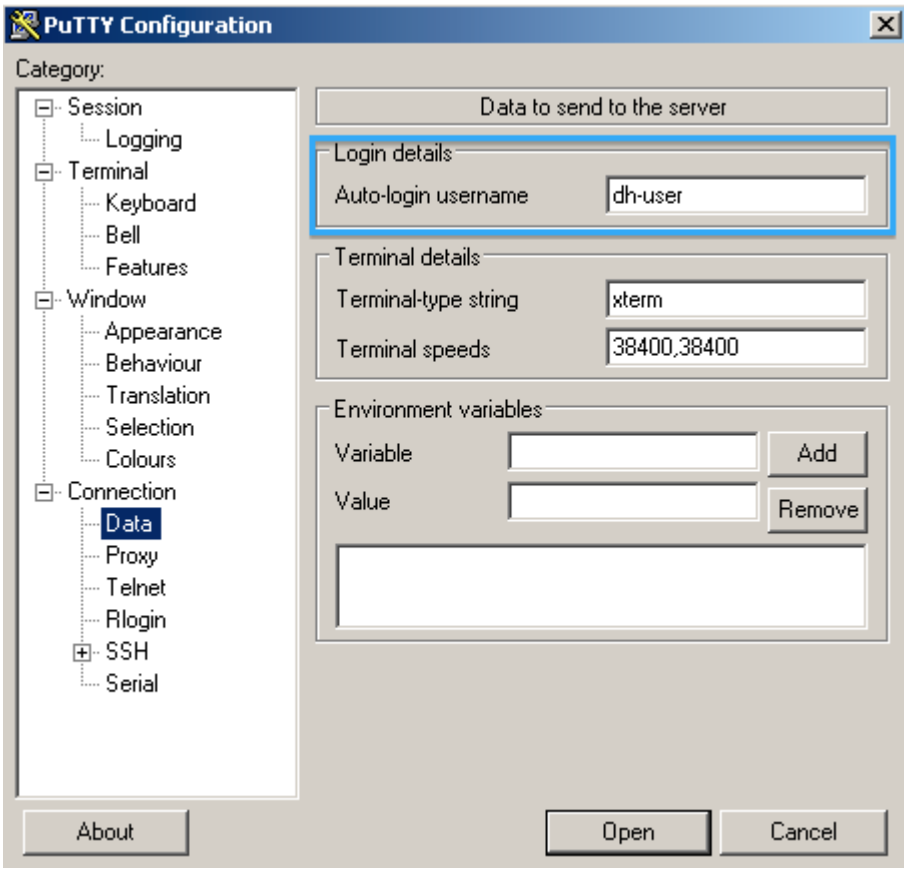
UE (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

EU (eu.iphmx.com) (Repubblica democratica tedesca)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

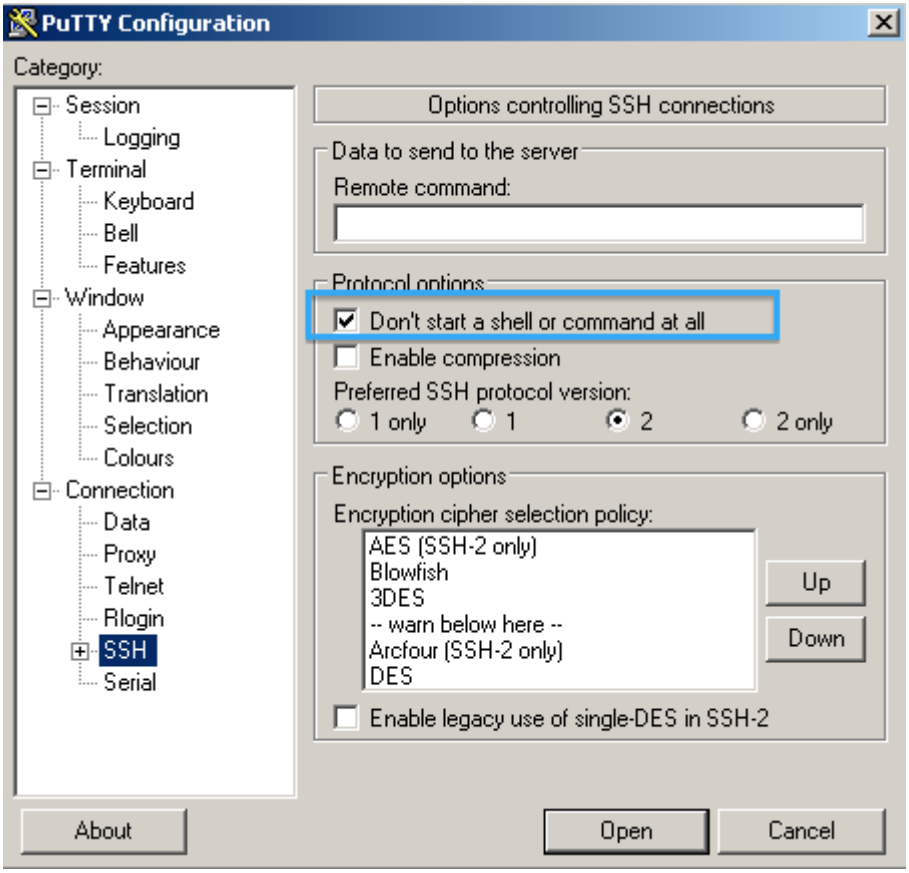
STATI UNITI (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



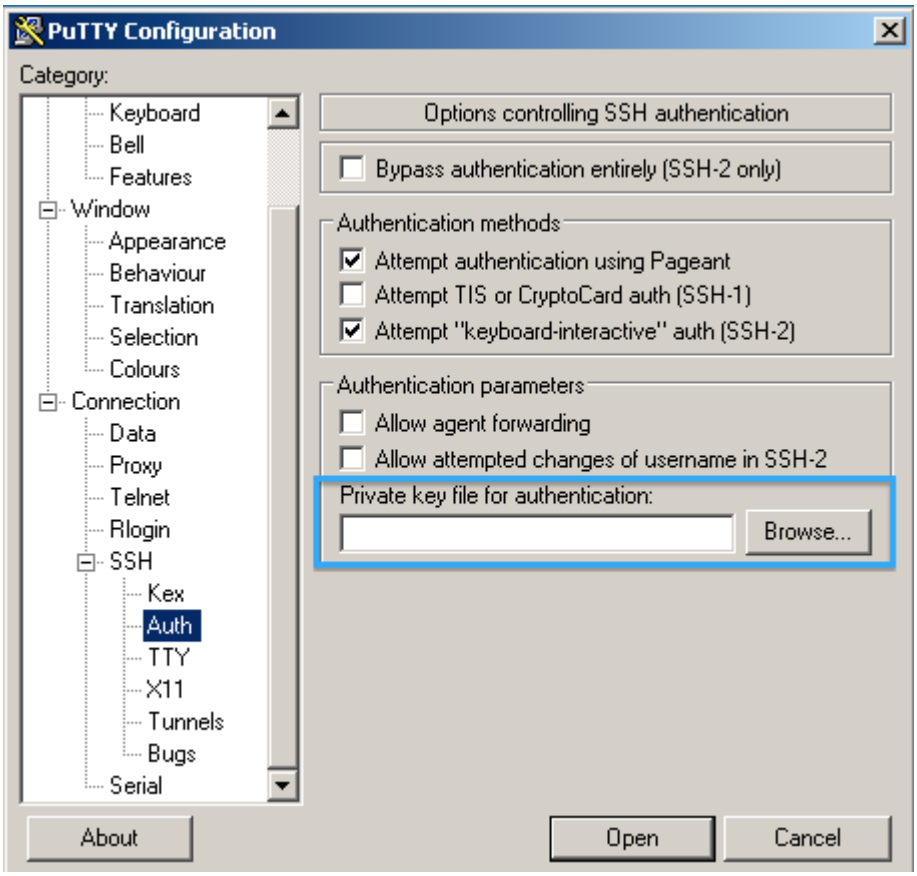
Fare clic su Datae per i dettagli di accesso, utilizzare il nome utente di accesso automatico e immettere dh-user.



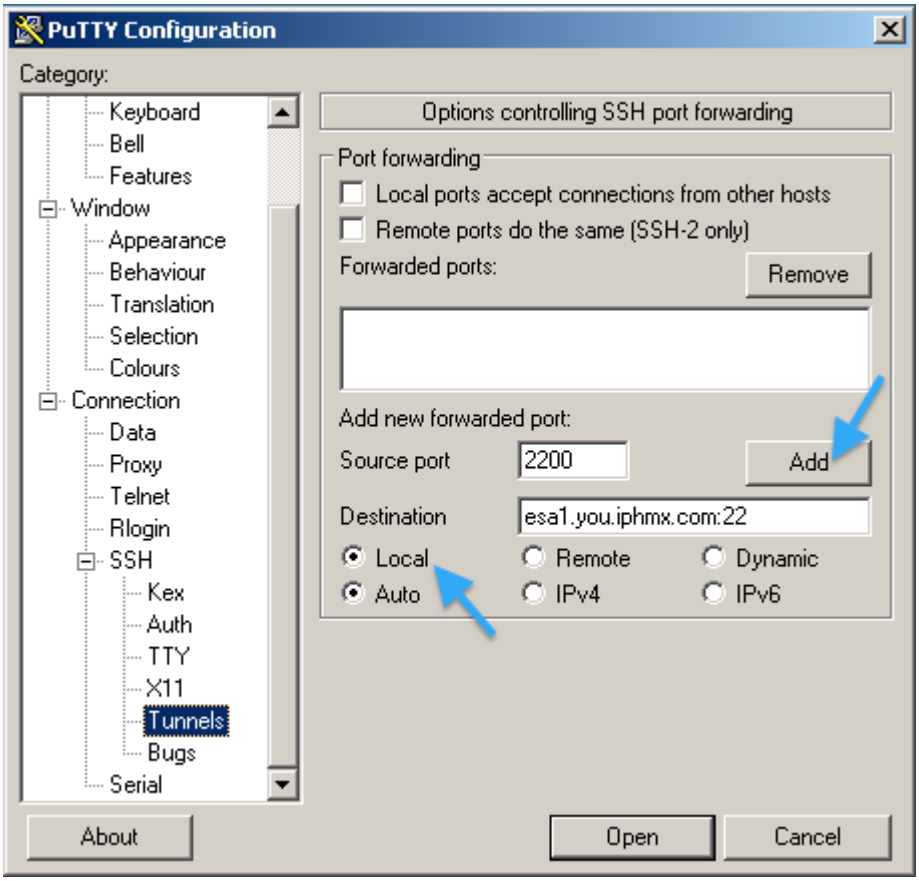
Scegliere SSH e selezionare Non avviare affatto una shell o un comando.



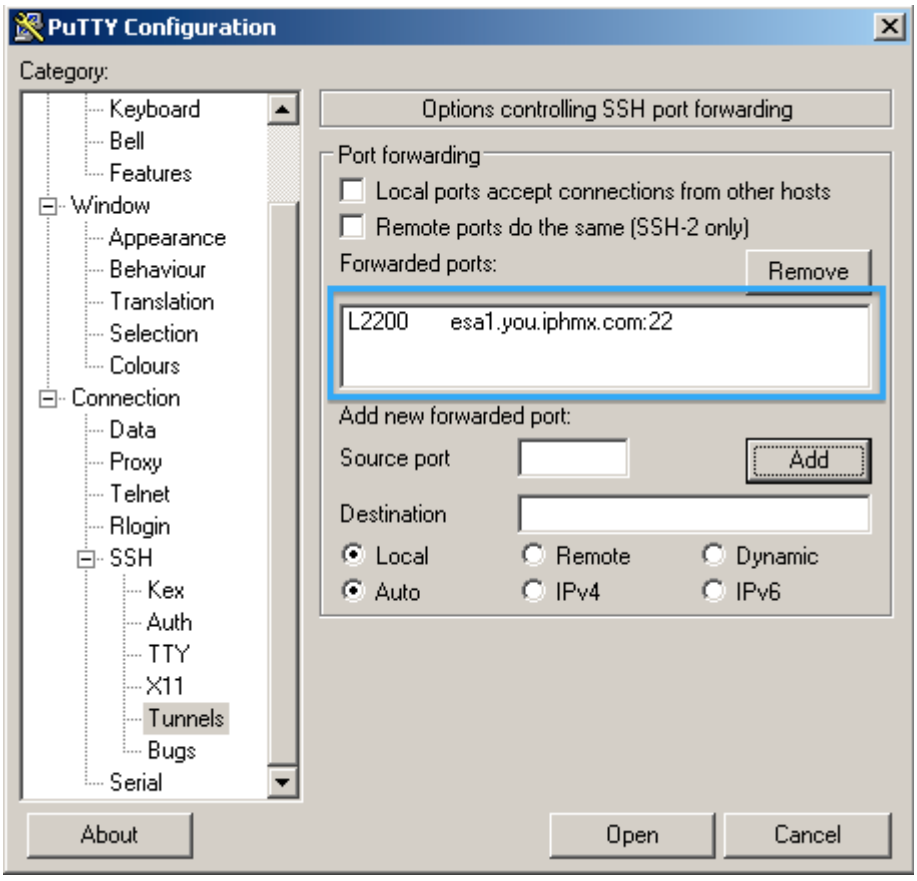
Fare clic su Autorizza per file di chiave privata per l'autenticazione, sfogliare e scegliere la chiave privata.



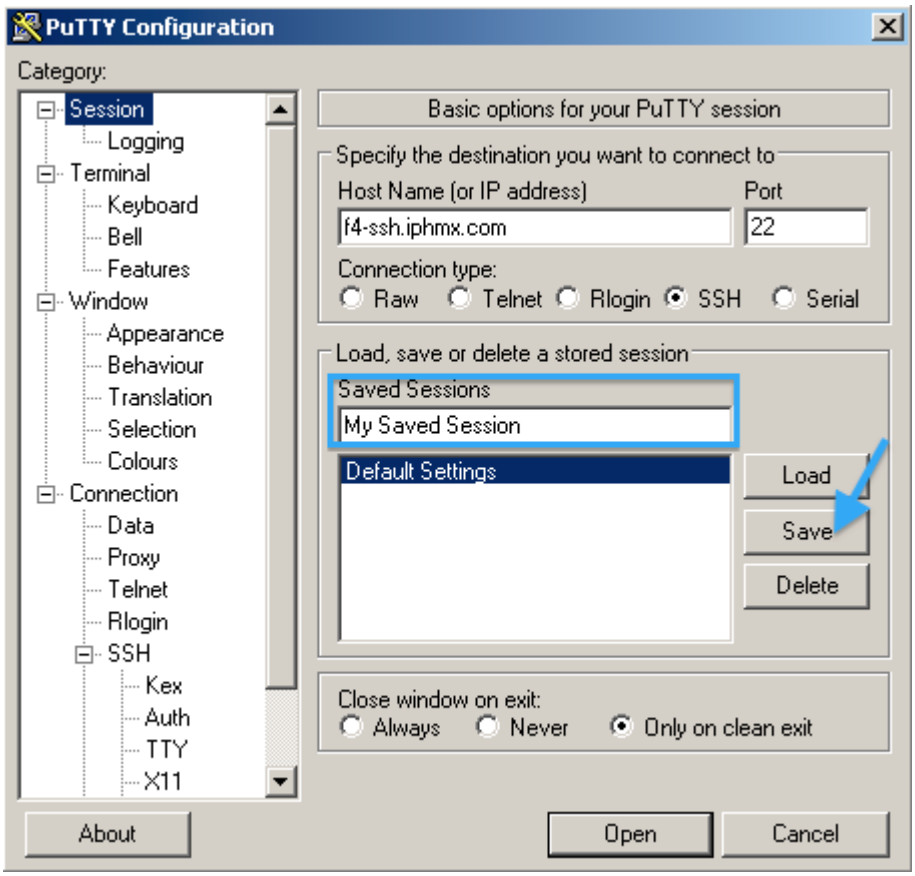
Fare clic su Tunnel.
Accedere a una porta di origine; si tratta di una porta arbitraria a scelta (ad esempio, viene utilizzato 2200).
Inserire in una destinazione; si tratta dell'ESA o SMA + 22 (specificando la connessione SSH).



Dopo aver fatto clic su Aggiungi, il file deve avere questo aspetto.

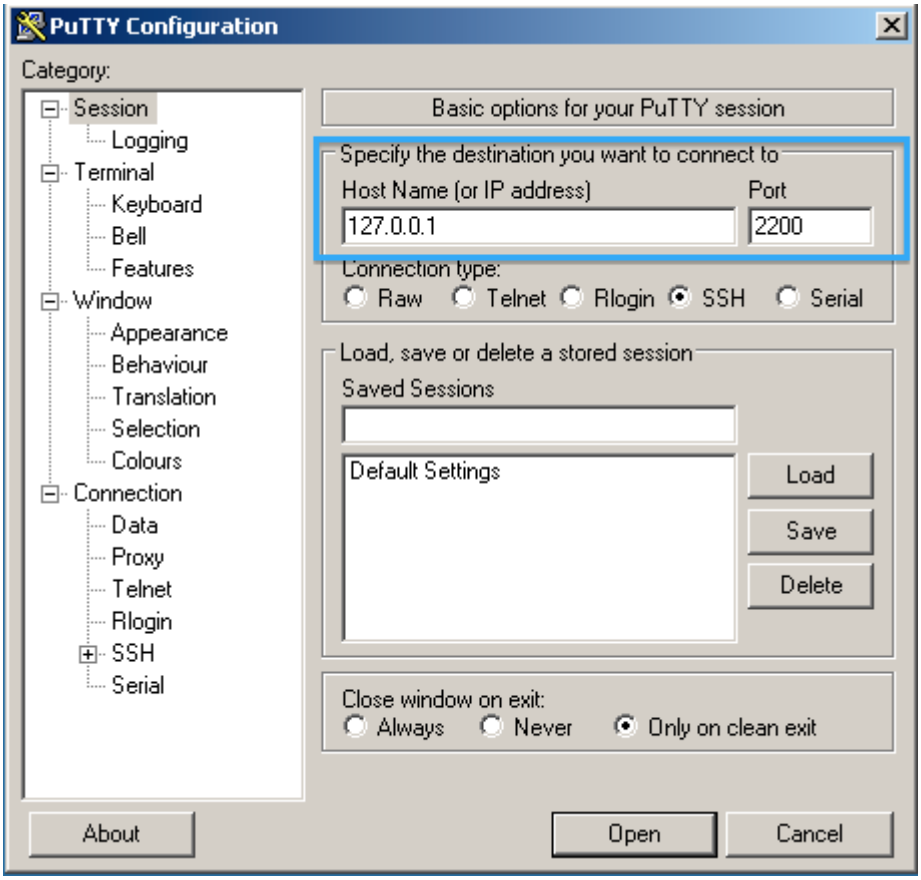


Per salvare la sessione per un utilizzo futuro, fare clic su Sessione. Immettere un nome per la sessione salvata e fare clic su Salva.



A questo punto è possibile fare clic su Apri e avviare la sessione proxy.
Non saranno presenti login o prompt dei comandi. A questo punto, è necessario aprire una seconda sessione PuTTY per l'ESA o l'SMA.

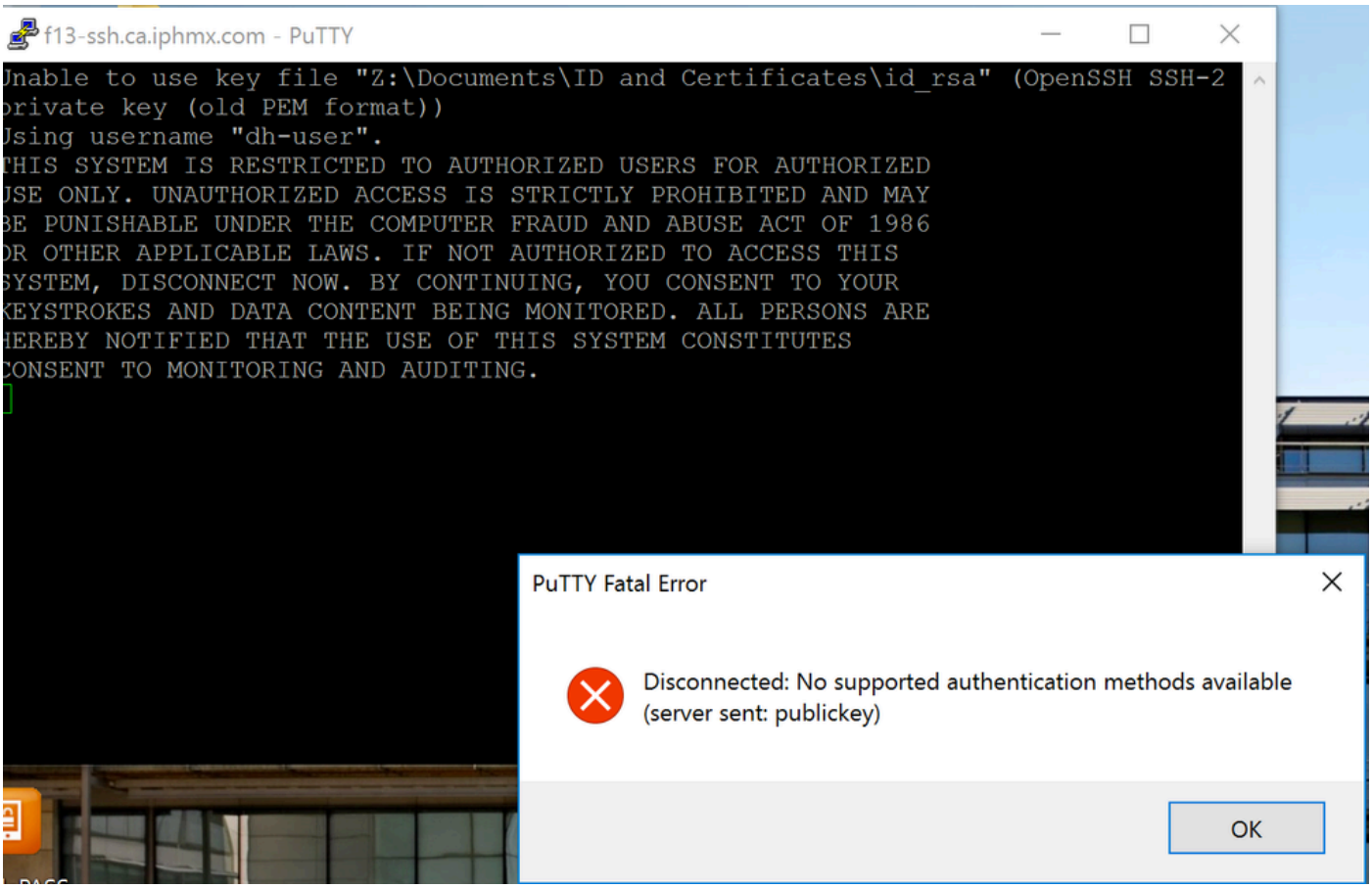
Utilizzare il nome host 127.0.0.1 e il numero della porta di origine nella configurazione del tunnel mostrata in precedenza.
In questo esempio il prefisso utilizzato è 2200.
Per collegarsi all'accessorio, fare clic su Apri.



Quando richiesto, utilizzare il nome utente e la password dell'accessorio, come per l'accesso all'interfaccia utente.

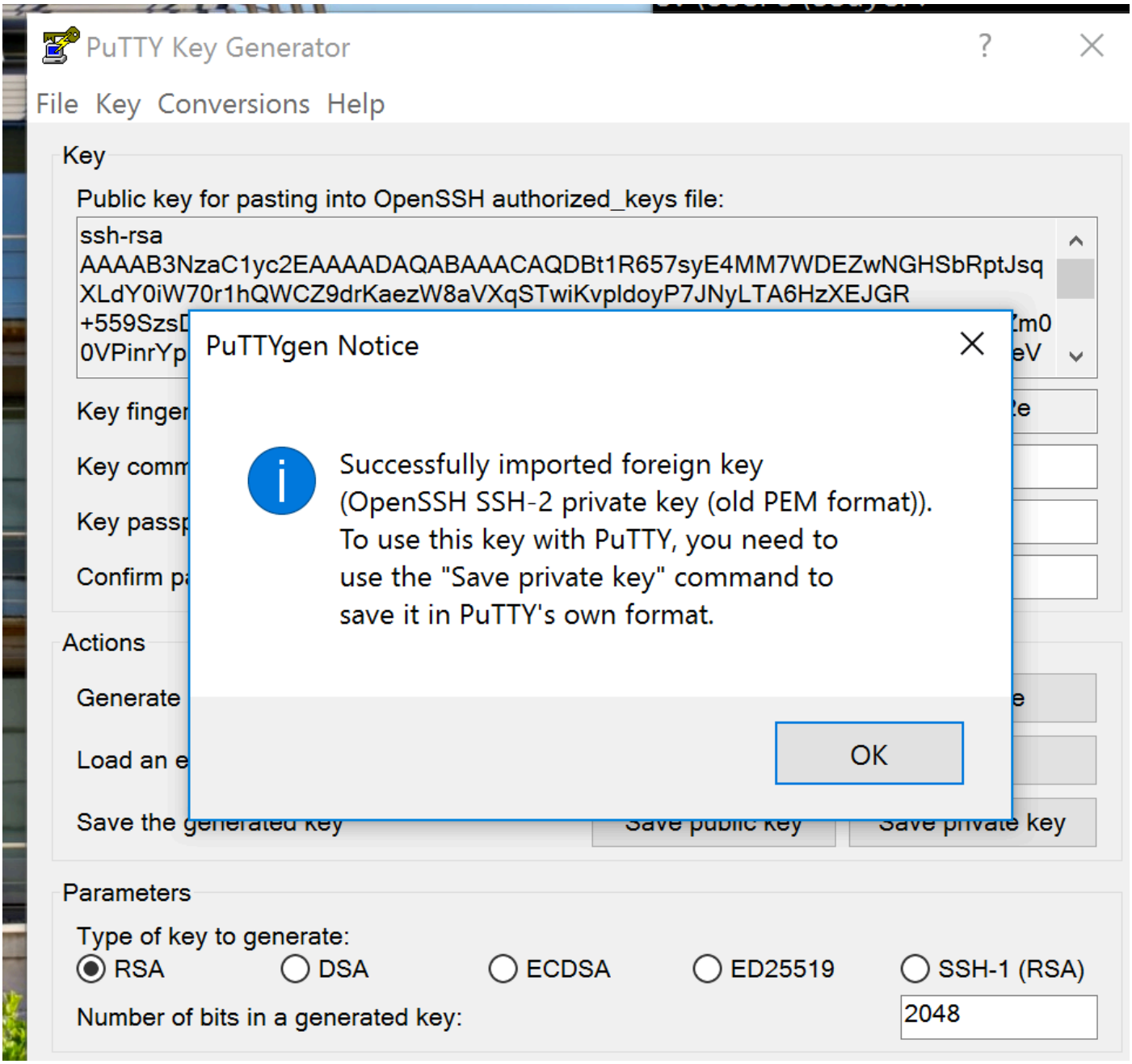
Risoluzione dei problemi

Se la coppia di chiavi SSH è stata generata utilizzando OpenSSH (non PuTTy), non è possibile connettersi e verrà visualizzato un errore del "vecchio formato PEM".



La chiave privata può essere convertita utilizzando il generatore di chiavi PuTTY.

- Aprire PuTTy Key Generator.
- Per individuare e caricare la chiave privata esistente, fare clic suCarica.
- Sarà necessario fare clic sull'elenco a discesa e scegliere Tutti i file (.)per poter individuare la chiave privata.
- Fare clic su Apri dopo aver individuato la chiave privata.
- Puttygen fornirà una nota come in questa immagine.



- Fare clic su Salva chiave privata.
- Dalla sessione PuTTY, utilizzare questa chiave privata convertita e salvare la sessione.
- Tentativo di riconnessione con la chiave privata convertita.

Verificare che sia possibile accedere agli accessori tramite la riga di comando.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).