Cisco Cloud Email Security CLI 액세스 요청

목차

소개

이 문서에서는 CES(Cloud Email Security) CLI에 대한 액세스를 요청하는 방법에 대해 설명합니다.

배경 정보

Cisco CES 고객은 키 인증을 사용하여 SSH 프록시를 통해 제공되는 ESA 및 SMA의 CLI에 액세스할 수 있습니다. 호스팅된 어플라이언스에 대한 CLI 액세스는 조직 내의 주요 담당자로 제한되어야 합니다.

Linux 및 Mac 사용자

Cisco CES 고객의 경우:
CES 프록시를 통해 CLI 액세스를 설정하기 위해 SSH를 사용하는 셸 스크립트에 대한 지침.

사전 요구 사항

CES 고객으로서 SSH 키를 교환하고 배치하려면 CES On-Boarding/Ops 또는 Cisco TAC와 계약해야 합니다.

1. 개인/공용 RSA 키를 생성합니다.
2. Cisco에 공개 RSA 키를 제공합니다.
3. Cisco가 저장할 때까지 기다린 후 키가 CES 고객 계정에 저장되었음을 알립니다.
4. connect2ces.sh 스크립트를 복사하고 수정합니다.

프라이빗/퍼블릭 RSA 키는 어떻게 생성합니까?

Unix/Linux/OS X의 경우 터미널/CLI에서 'ssh-keygen'을 사용하는 것이 좋습니다. ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NAME> 명령을 사용합니다.

참고: 자세한 내용은 https://www.ssh.com/academy/ssh/keygen을 참조하십시오.
RSA 개인 키에 대한 액세스를 항상 보호해야 합니다.
Cisco에 개인 키를 보내지 말고 공개 키(.pub)만 보내십시오.
공개 키를 Cisco에 제출할 때 해당 키의 이메일 주소/이름/성을 확인하십시오.

공개 키를 제공하기 위해 Cisco 지원 요청을 열려면 어떻게 해야 합니까?

이 링크로 이동합니다.

SR을 'Cisco CES 고객 SSH/CLI 설정' 등으로 올바르게 식별해야 합니다.

설정

시작하려면 제공된 스크립트를 opencopy하고 호스트 이름에 이러한 프록시 호스트 중 하나를 사용합니다.

해당 지역의 올바른 프록시를 선택했는지 확인합니다. 즉, 미국 CES 고객인 경우 F4 데이터 센터 및 어플라이언스에 연결하려면 f4-ssh.iphmx.com을 사용하십시오. 독일 DC에서 어플라이언스를 사용하는 EU CES 고객인 경우 f17-ssh.eu.iphmx.com.)을 사용하십시오.

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

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

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

EU(eu.iphmx.com)(독일 DC)
f17-ssh.eu.iphmx.com을 참조하십시오.
f18-ssh.eu.iphmx.com을 참조하십시오.

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

둘 이상의 ESA(Email Security Appliance) 또는 SMA(Security Management Appliance)에 연결하려면 어떻게 해야 합니까?

connect2ces.sh의 두 번째 복사본(예: connect2ces_2.sh)을 복사하여 저장합니다.

참고: 액세스하려는 추가 어플라이언스가 되도록 'cloud_host'를 수정하려고 합니다. 'local_port'를 2222가 아닌 다른 값으로 수정할 수 있습니다. 그렇지 않으면 "경고: 원격 호스트 ID가 변경되었습니다!"

비밀번호를 입력하지 않고 로그인하도록 ESA 또는 SMA를 구성하려면 어떻게 해야 합니까?

이 가이드를 읽어보십시오.

필수 구성 요소를 완료한 후에는 어떻게 보일 수 있습니까?

joe.user@my_local > ~ ./connect2ces
[-] 프록시 서버(f4-ssh.iphmx.com)에 연결하는 중...
[-] 프록시 연결 성공 이제 f4-ssh.iphmx.com에 연결되었습니다.
[-] PID에서 실행 중인 프록시: 31253
[-] CES 어플라이언스(esa1.rs1234-01.iphmx.com)에 연결하는 중...

마지막 로그인: 2019년 4월 22일 월요일 10.123.123.123에서 11:33:45
AsyncOS 12.1.0 for Cisco C100V 빌드 071

Cisco C100V Email Security Virtual Appliance 시작

참고: 이 세션은 1440분 동안 유휴 상태로 두면 만료됩니다. 커밋되지 않은 모든 컨피그레이션 변경 사항은 손실됩니다. 컨피그레이션 변경 사항이 발생하는 즉시 커밋합니다.

(컴퓨터 esa1.rs1234-01.iphmx.com)>
(컴퓨터 esa1.rs1234-01.iphmx.com)> exit(종료)

127.0.0.1에 대한 연결이 닫혔습니다.
[-] 프록시 연결을 닫는 중...
[-] 완료되었습니다.

connect2ces.sh

참고: 해당 지역의 올바른 프록시를 선택해야 합니다(즉, 미국 CES 고객인 경우 F4 데이터 센터 및 어플라이언스에 연결하려면 f4-ssh.iphmx.com을 사용하십시오. 독일 DC에서 어플라이언스를 사용하는 EU CES 고객인 경우 f17-ssh.eu.iphmx.com.)을 사용하십시오.

```
#!/bin/bash

#-- 값 편집 ----------------------
# 다음 값은 CES에서 이미 설정되어야 합니다.
# cloud_user="username"
# cloud_host="esaX.CUSTOMER.iphmx.com" 또는 "smaX.CUSTOMER.iphmx.com"
## [적절한 지역별 CES 데이터 센터를 보유하고 있는지 확인!]
# private_key= " LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY "
# proxy_server="PROXY_SERVER" [하나만 선택!]
#
## 'proxy_server'의 경우 SSH 프록시입니다.
##
## 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)(독일 DC)
## f17-ssh.eu.iphmx.com
## f18-ssh.eu.iphmx.com
##
## 미국(iphmx.com)
## f4-ssh.iphmx.com
## f5-ssh.iphmx.com

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

#-- 값은 그대로 --------------------
# 'proxy_user'는 변경할 수 없습니다.
# 'remote_port'는 22(SSH) 유지
필요한 경우 # 'local_port'를 다른 값으로 설정할 수 있습니다.
```

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

이 행 ---------- 아래에 편집할 #-- 없습니다.

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

printf "[-] 프록시 서버($proxy_server)에 연결하는 중...\n"
$proxycmd >/dev/null 2>&1
nc -z 127.0.0.1 $local_port >/dev/null 2>&1인 경우 그런 다음
printf "[-] 프록시 연결에 성공했습니다. $proxy_server에 연결되었습니다.\n"
그렇지 않으면
printf "[-] 프록시 연결에 실패했습니다. 끝내는 중...\n"
exit
피

# 프록시 ssh 프로세스 찾기
proxypid=`ps -xo pid,명령 | grep "$cloud_host" | grep "$proxy_server" | 머리 -n1 | sed "s/^[\t]*//" |
잘라내기 -d " -f1`
pid에서 실행 중인 printf "[-] 프록시: $proxyid\n"

printf "[-] CES 어플라이언스($cloud_host)에 연결하는 중...\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

printf "[-] 프록시 연결을 닫는 중...\n"
$proxypid를 삭제합니다.

인쇄 "[-] 완료.\n"

#-- 매번 비밀번호를 입력하지 않으시겠습니까?
#--: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-technote-esa-00.html
둘 이상의 ESA 또는 SMA에 액세스해야 #--? 동일한 스크립트를 복사하고 이름을
connect2ces_2.sh 또는 이와 유사하게 변경합니다.

원본 문서: https://github.com/robsherw/connect2ces.

Windows 사용자

CES 프록시를 통해 CLI 액세스를 만들기 위해 PuTTY를 사용하고 SSH를 사용하기 위한 지침.

사전 요구 사항

CES 고객으로서 SSH 키를 교환하고 배치하려면 CES On-Boarding/Ops 또는 Cisco TAC와 계약해야 합니다.

1. 개인/공용 RSA 키를 생성합니다.
2. Cisco에 퍼블릭 RSA 키 제공
3. Cisco에서 키를 저장할 때까지 기다린 후 키가 CES 고객 계정에 저장되었음을 알립니다.
4. 이 지침에 자세히 설명된 대로 PuTTY를 설정합니다.

프라이빗/퍼블릭 RSA 키는 어떻게 생성합니까?

Cisco에서는 Windows용 PuTTYgen(https://www.puttygen.com/)을 사용할 것을 권장합니다.

자세한 내용은 https://www.ssh.com/ssh/putty/windows/puttygen를 참조하십시오.

참고: RSA 개인 키에 대한 액세스를 항상 보호해야 합니다.
Cisco에 개인 키를 보내지 말고 공개 키(.pub)만 보내십시오.
공개 키를 Cisco에 제출할 때 해당 키가 필요한 이메일 주소/이름/성을 확인하십시오.

공개 키를 제공하기 위해 Cisco 지원 요청을 열려면 어떻게 해야 합니까?

이 링크로 이동합니다.

SR을 'Cisco CES 고객 SSH/CLI 설정' 등으로 올바르게 식별해야 합니다.

비밀번호를 입력하지 않고 로그인하도록 ESA 또는 SMA를 구성하려면 어떻게 해야 합니까?

이 가이드를 읽어보십시오.

PuTTy 컨피그레이션

시작하려면 PuTTY를 열고 호스트 이름에 다음 프록시 호스트 중 하나를 사용합니다.

해당 지역의 올바른 프록시를 선택했는지 확인합니다. 즉, 미국 CES 고객인 경우 F4 데이터 센터 및 어플라이언스에 연결하려면 f4-ssh.iphmx.com을 사용하십시오. 독일 DC에서 어플라이언스를 사용하는 EU CES 고객인 경우 f17-ssh.eu.iphmx.com.)을 사용하십시오.

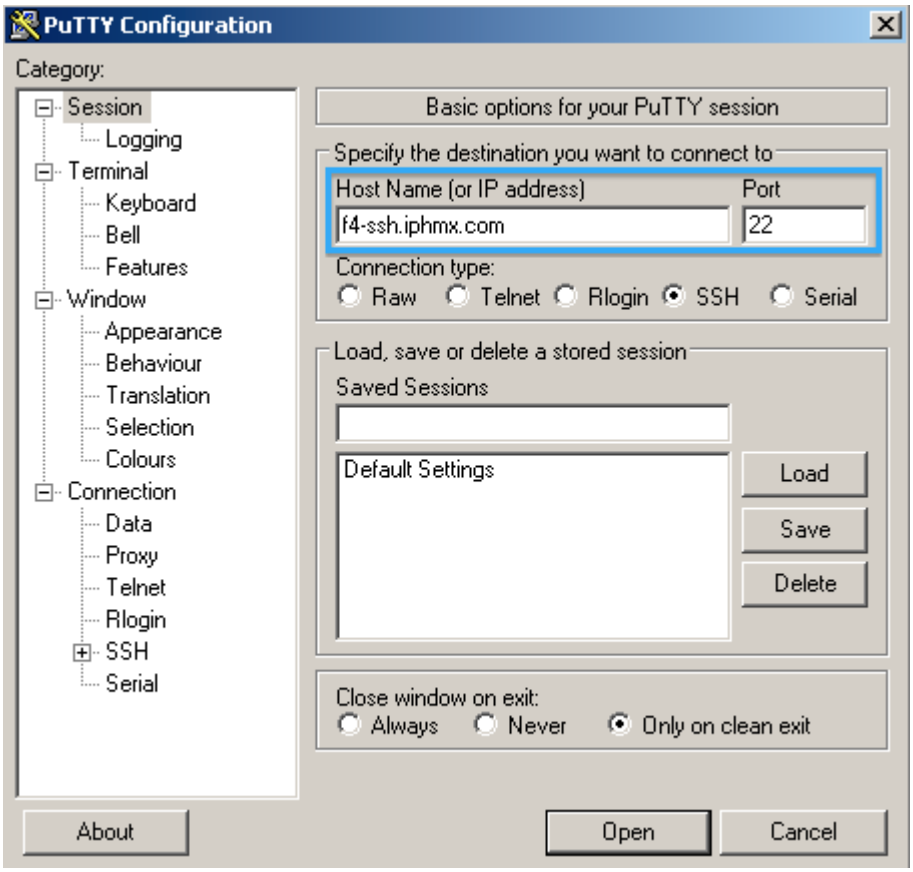
AP(ap.iphmx.com)
f15-ssh.ap.iphmx.com을 참조하십시오.
f16-ssh.ap.iphmx.com을 참조하십시오.

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

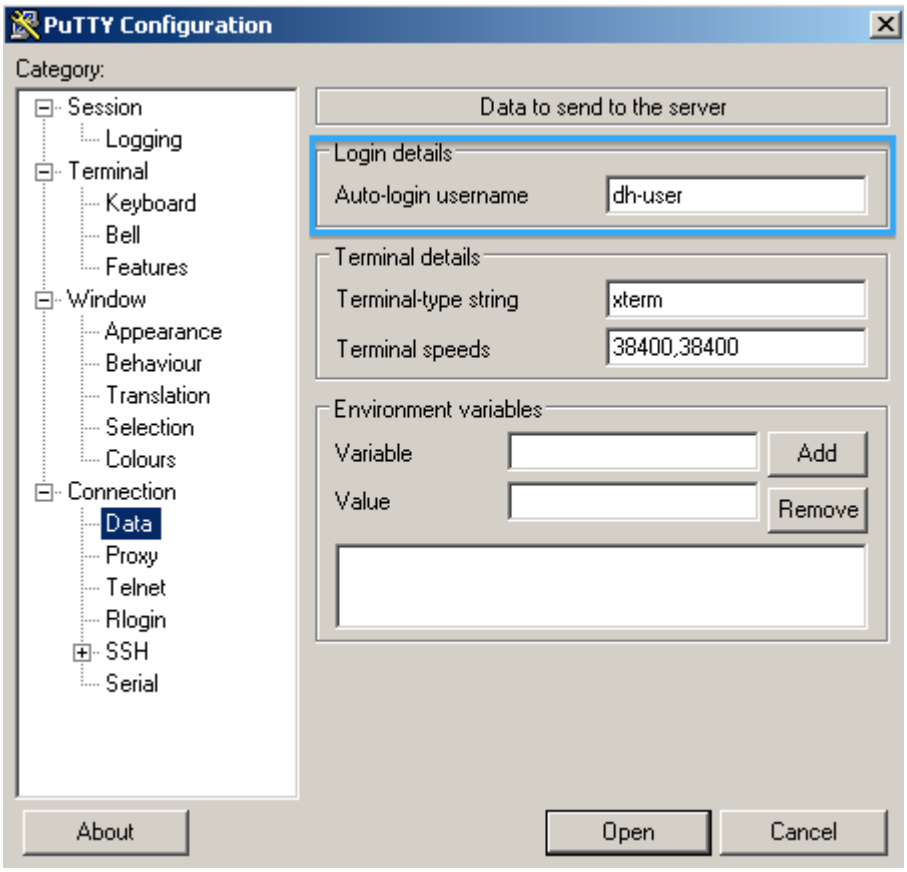
EU(c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

EU(eu.iphmx.com)(독일 DC)
f17-ssh.eu.iphmx.com을 참조하십시오.
f18-ssh.eu.iphmx.com을 참조하십시오.

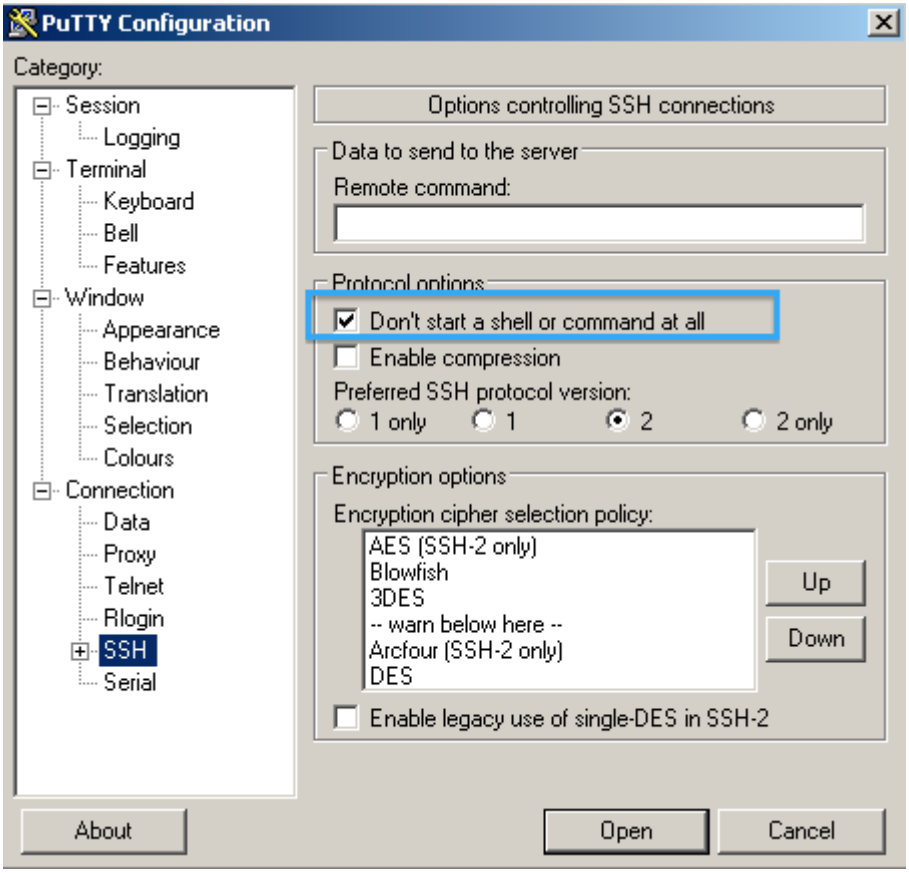
미국(iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



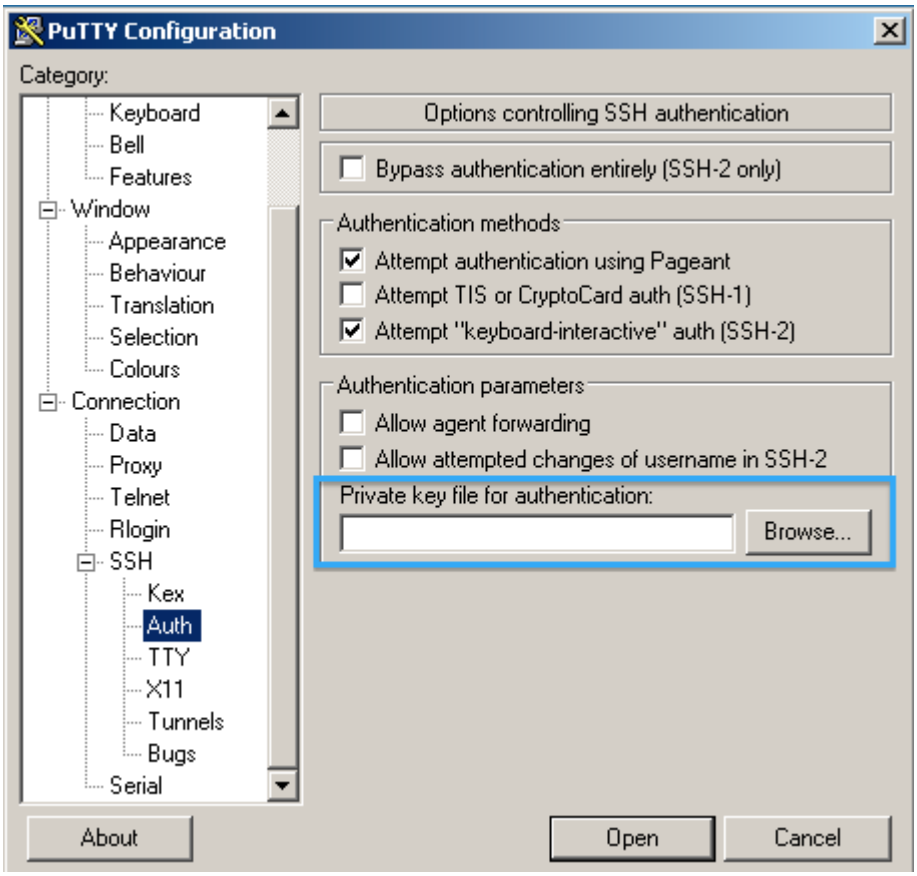
Data(데이터)를 클릭하고 로그인 세부 정보를 보려면 자동 로그인 사용자 이름을 사용하고 dh-user를 입력합니다.



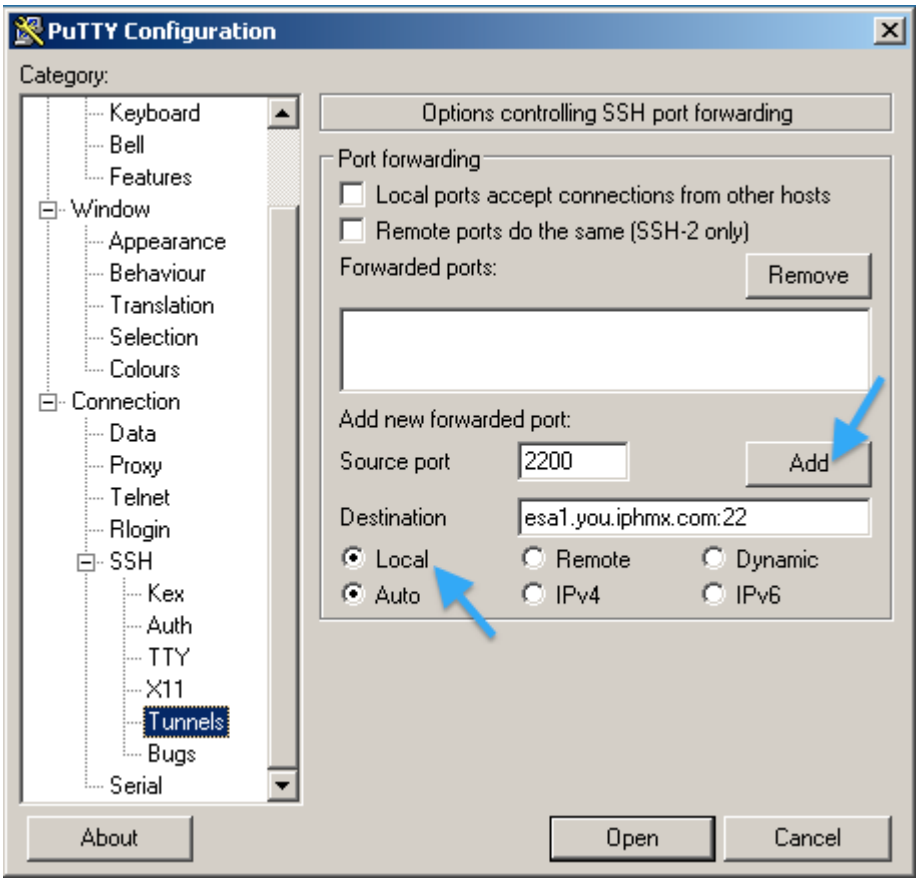
SSH를 선택하고 Don't start a shell or command at all.



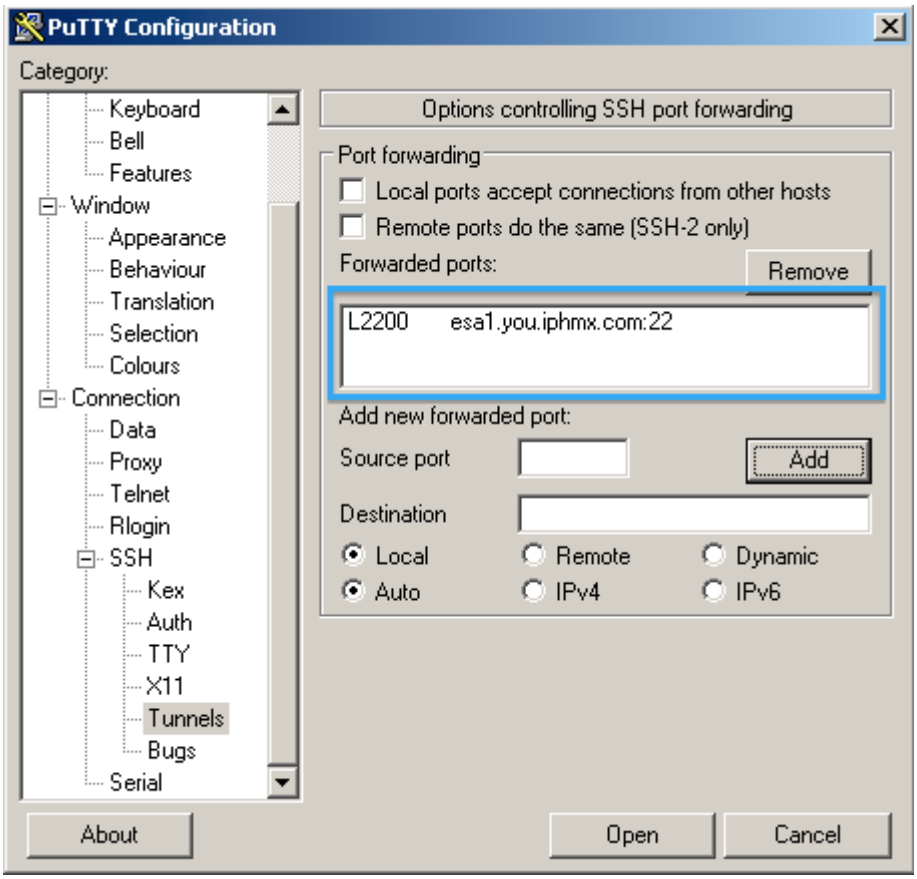
인증을 위해 개인 키 파일에 대해 Authand를 클릭하고 개인 키를 찾아 선택합니다.



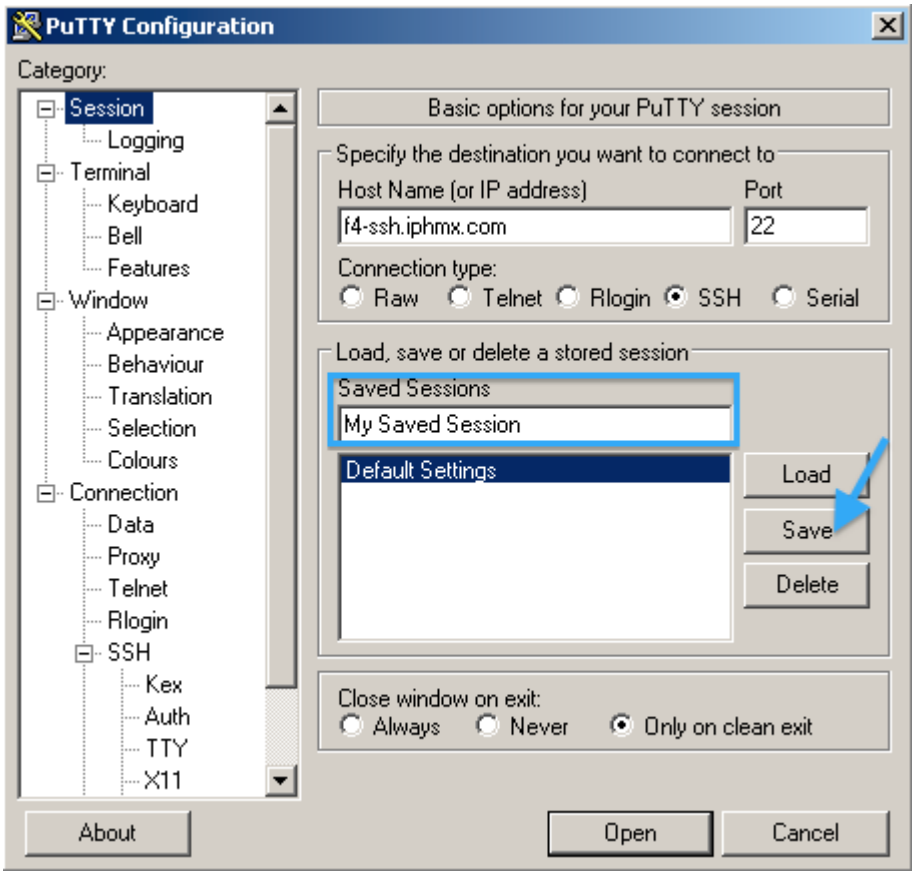
Tunnels를 클릭합니다.
소스 포트에 를 입력합니다. 임의의 임의의 포트(예: 2200 사용)입니다.
Destination(대상)을 입력합니다. ESA 또는 SMA + 22(SSH 연결 지정)입니다.



Add(추가)를 클릭한 후에는 다음과 같이 표시되어야 합니다.

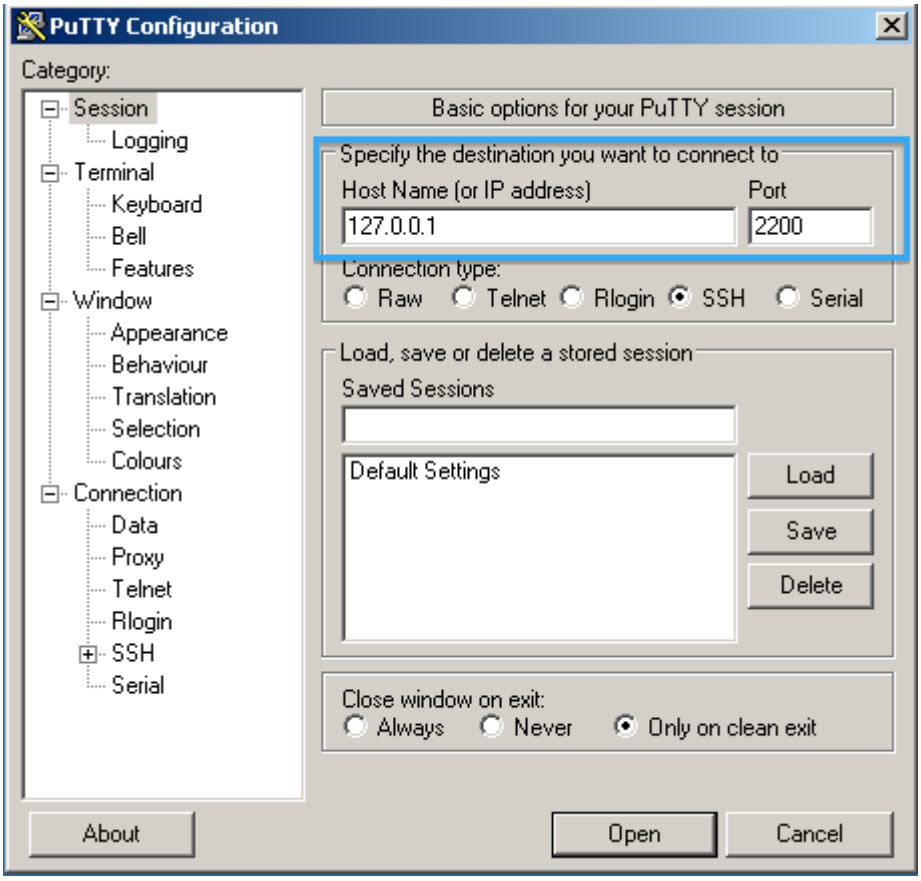


나중에 사용할 수 있도록 세션을 저장하려면 Session을 클릭합니다.
'저장된 세션'의 이름을 입력하고 저장을 클릭합니다.



이때 Open(열기)을 클릭하고 프록시 세션을 시작할 수 있습니다.
로그인 또는 명령 프롬프트가 없습니다. 이제 ESA 또는 SMA에 대한 두 번째 PuTTY 세션을 열어야 합니다.

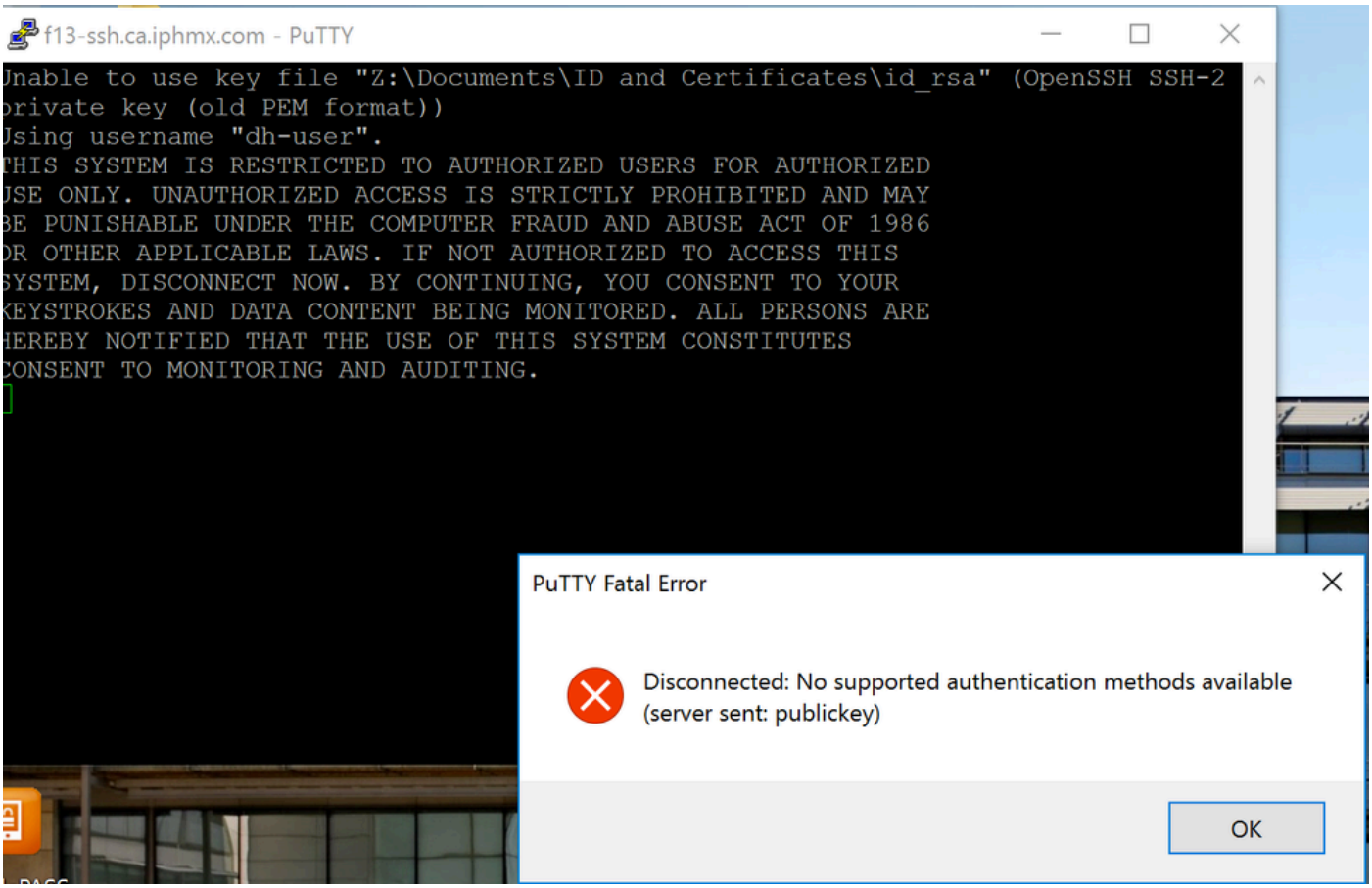
호스트 이름 127.0.0.1을 사용하고 앞에서 설명한 터널 컨피그레이션에서 소스 포트 번호를 사용합니다.
이 예에서는 2200이 사용됩니다.
어플라이언스에 연결하려면 Open을 클릭합니다.



메시지가 표시되면 어플라이언스 사용자 이름 및 비밀번호를 사용합니다. 이는 UI 액세스와 동일합니다.

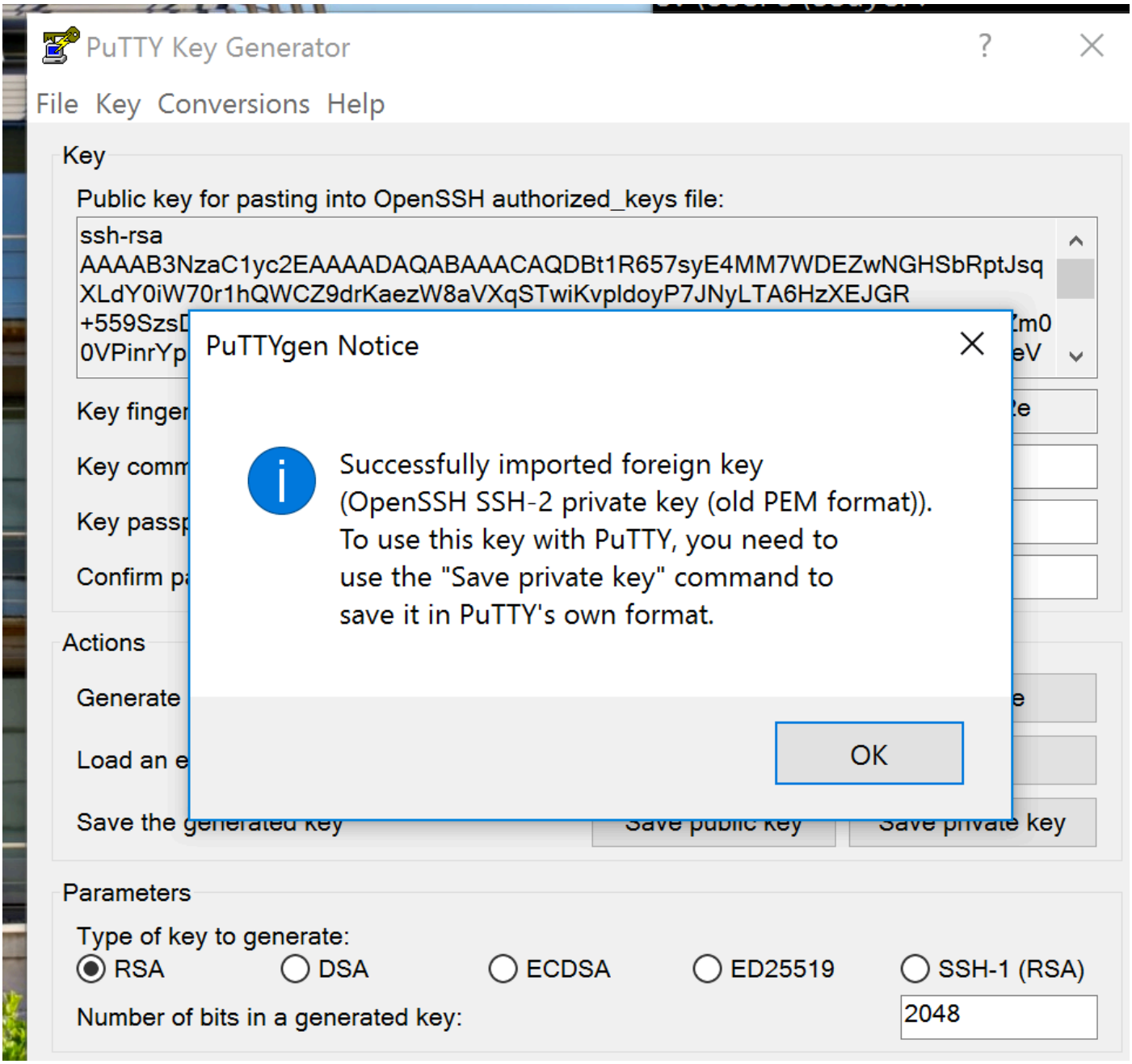
문제 해결

SSH 키 쌍이 OpenSSH(비 PuTTy)를 사용하여 생성된 경우 연결할 수 없으며 "이전 PEM 형식" 오류가 표시됩니다.



개인 키는 PuTTY 키 생성기를 사용하여 변환할 수 있습니다.

- PuTTy 키 생성기를 엽니다.
- 기존 개인 키를 찾아 로드하려면 Loadin을 클릭합니다.
- 개인 키를 찾을 수 있도록 드롭다운을 클릭하고 모든 파일(.)을 선택해야 합니다.
- 개인 키를 찾았으면 Open을 클릭합니다.
- Puttygen은 이 이미지와 같은 알림을 제공합니다.



- 개인 키 저장을 클릭합니다.
- PuTTY 세션에서 이 변환된 개인 키를 사용하고 세션을 저장합니다.
- 변환된 개인 키로 다시 연결하십시오.

명령줄을 통해 어플라이언스에 액세스할 수 있는지 확인합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.