# ¿Qué hace “alguien está intentando secuestrar el error de la conexión encriptada” significó?

## Contenido



## Introducción

Este documento describe el error “que es posible que alguien está intentando secuestrar la conexión encriptada al host remoto,” y los pasos correctivos a tomar en su Cisco envían por correo electrónico el dispositivo de seguridad (ESA) y el dispositivo de la Administración del Cisco Security (S A).

## ¿Qué hace “alguien está intentando secuestrar el error de la conexión encriptada” significó?

Cuando usted configura su comunicación ESA con su S A, usted puede ser que vea este error:

```
Error - The host key for 172.16.6.165 appears to have changed.
It is possible that someone is trying to hijack the encrypted
connection to the remote host.
Please use the logconfig->hostkeyconfig command to verify
(and possibly update) the SSH host key for 172.16.6.165.
```

Esto puede ocurrir cuando un ESA se substituye y utiliza el mismo nombre de host y/o dirección IP que el ESA original. Las claves previamente salvadas de SSH usadas en la comunicación y la autenticación entre el ESA y el S A se salvan en el S A. El S A entonces ve que el trayecto de comunicación ESA ha cambiado, y cree que una fuente no autorizada ahora está en control de la dirección IP assocaited al ESA.

Para corregir esto, inicie sesión al CLI del S A, y complete estos pasos:

1. Ingrese el comando del **logconfig**.
2. Ingrese el **hostkeyconfig**.
3. Ingrese la **cancelación** y elija el número asociado en el listado actualmente instalado de la clave de host para el IP ESA.
4. Vuelva al prompt principal CLI y ingrese el **comando commit**.

```
mysma.local> logconfig
```

```
Currently configured logs:
Log Name Log Type Retrieval Interval
-----------------------------------------------------------------------------
1. authentication Authentication Logs FTP Poll None
2. backup_logs Backup Logs FTP Poll None
3. cli_logs CLI Audit Logs FTP Poll None
4. euq_logs Spam Quarantine Logs FTP Poll None
5. euqgui_logs Spam Quarantine GUI Logs FTP Poll None
6. ftpd_logs FTP Server Logs FTP Poll None
7. gui_logs HTTP Logs FTP Poll None
8. haystackd_logs Haystack Logs FTP Poll None
9. ldap_logs LDAP Debug Logs FTP Poll None
10. mail_logs Cisco Text Mail Logs FTP Poll None
11. reportd_logs Reporting Logs FTP Poll None
12. reportqueryd_logs Reporting Query Logs FTP Poll None
13. slbld_logs Safe/Block Lists Logs FTP Poll None
14. smad_logs SMA Logs FTP Poll None
15. snmp_logs SNMP Logs FTP Poll None
16. sntpd_logs NTP logs FTP Poll None
17. system_logs System Logs FTP Poll None
18. trackerd_logs Tracking Logs FTP Poll None
19. updater_logs Updater Logs FTP Poll None
20. upgrade_logs Upgrade Logs FTP Poll None

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> hostkeyconfig

Currently installed host keys:
1. 172.16.6.165 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA0ilM...DVc7plDQ==
2. 172.16.6.150 ssh-dss AAAAB3NzaC1kc3MAAACBAODKHq6uakiM...cooFXzLHFP
3. 172.16.6.131 ssh-dss AAAAB3NzaC1kc3MAAACBAI4LkblFtidp...WhM5XLNA==


Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> delete

Enter the number of the key you wish to delete.
[]> 1

Currently installed host keys:
1. 172.16.6.150 ssh-dss AAAAB3NzaC1kc3MAAACBAODKHq6uakiM...cooFXzLHFP
2. 172.16.6.131 ssh-dss AAAAB3NzaC1kc3MAAACBAI4LkblFtidp...WhM5XLNA==

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
```

```
[]>

Currently configured logs:
Log Name Log Type Retrieval Interval
-----------------------------------------------------------------------------
1. authentication Authentication Logs FTP Poll None
2. backup_logs Backup Logs FTP Poll None
3. cli_logs CLI Audit Logs FTP Poll None
4. euq_logs Spam Quarantine Logs FTP Poll None
5. euqgui_logs Spam Quarantine GUI Logs FTP Poll None
6. ftpd_logs FTP Server Logs FTP Poll None
7. gui_logs HTTP Logs FTP Poll None
8. haystackd_logs Haystack Logs FTP Poll None
9. ldap_logs LDAP Debug Logs FTP Poll None
10. mail_logs Cisco Text Mail Logs FTP Poll None
11. reportd_logs Reporting Logs FTP Poll None
12. reportqueryd_logs Reporting Query Logs FTP Poll None
13. slbld_logs Safe/Block Lists Logs FTP Poll None
14. smad_logs SMA Logs FTP Poll None
15. snmp_logs SNMP Logs FTP Poll None
16. sntpd_logs NTP logs FTP Poll None
17. system_logs System Logs FTP Poll None
18. trackerd_logs Tracking Logs FTP Poll None
19. updater_logs Updater Logs FTP Poll None
20. upgrade_logs Upgrade Logs FTP Poll None

mysma.local> commit

Please enter some comments describing your changes:
[]> ssh key update
```

Finalmente, del S A GUI, elija los **dispositivos centralizados del > Security (Seguridad) de Serivces** y después seleccione el ESA en el anuncio que había presentado el error original. Una vez que usted elige **establecer la conexión…** y la **conexión de prueba**, autentica, crea un nuevo par de clave de host de SSH, y salva este par de clave de host en el S A.

Revisite el CLI para el S A, y vuelva a efectuar el **logconfig > el hostkeyconfig** para ver los nuevos pares de clave de host.

# Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Dispositivo de la Administración del Cisco Security - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems