# Qual è il significato dell'errore "prova a dirottare la connessione crittografata"?

## Sommario



## Introduzione

In questo documento viene descritto l'errore "È possibile che qualcuno stia tentando di dirottare la connessione crittografata all'host remoto" e vengono indicate le azioni correttive da intraprendere su Cisco Email Security Appliance (ESA) e Cisco Security Management Appliance (SMA).

## Qual è il significato dell'errore "prova a dirottare la connessione crittografata"?

Quando si configura la comunicazione ESA con l'SMA, è possibile che venga visualizzato questo errore:

```
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.
```

Questa situazione può verificarsi quando un'ESA viene sostituita e usa lo stesso nome host e/o indirizzo IP dell'ESA originale. Le chiavi SSH precedentemente memorizzate utilizzate nella comunicazione e nell'autenticazione tra l'ESA e l'SMA vengono memorizzate nell'SMA. L'SMA rileva quindi che il percorso di comunicazione dell'ESA è cambiato e ritiene che una fonte non autorizzata abbia ora il controllo dell'indirizzo IP associato all'ESA.

Per risolvere questo problema, accedere alla CLI dello SMA e completare i seguenti passaggi:

1. Immettere il comando **logconfig**.
2. Immettere **hostkeyconfig**.
3. Immettere **delete** (Elimina) e scegliere il numero associato alla chiave host attualmente installata per l'indirizzo IP ESA.
4. Tornare al prompt della CLI principale e immettere il 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
```

Infine, dalla GUI di SMA, selezionare **Centralized Services > Security Appliance** (Servizi centralizzati > Appliance di sicurezza), quindi selezionare l'ESA nell'elenco che ha presentato l'errore originale. Dopo aver scelto **Stabilisci connessione...** e **Test Connection**, esegue l'autenticazione, crea una nuova coppia di chiavi host SSH e archivia questa coppia di chiavi host nello SMA.

Rivedere la CLI per lo SMA ed eseguire nuovamente **logconfig > hostkeyconfig** per visualizzare la nuova coppia di chiavi host.

# Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Cisco Security Management Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems