What does the "someone is trying to hijack the encrypted connection" error mean?

Document ID: 119177

Contributed by Fraidoon Sarwary and Robert Sherwin, Cisco TAC Engineers.
Jul 16, 2015

Contents

Introduction

This document describes the error "It is possible that someone is trying to hijack the encrypted connection to the remote host," and the corrective steps to take on your Cisco Email Security Appliance (ESA) and Cisco Security Management Appliance (SMA).

What does the "someone is trying to hijack the encrypted connection" error mean?

When you configure your ESA communication with your SMA, you might see this 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.
```

This can occur when an ESA is replaced and uses the same hostname and/or IP address as the original ESA. The previously stored SSH keys used in communication and authentication between the ESA and SMA are stored on the SMA. The SMA then sees that the ESA communication path has changed, and belives that an unauthorized source is now in control of the IP address assocaited to the ESA.

In order to correct this, login to the CLI of the SMA, and complete these steps:

1. Enter the ***logconfig*** command.
2. Enter ***hostkeyconfig***.
3. Enter ***delete*** and choose the number associated in the currently installed host key listing for the ESA IP.
4. Return to the main CLI prompt and enter the ***commit*** command.

```
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
```

Finally, from the SMA GUI, choose ***Centralized Serivces*** > ***Security Appliances*** and then select the ESA in the listing that had presented the original error. Once you choose to ***Establish Connection...*** and ***Test Connection***, it authenticates, creates a new SSH host key pair, and stores this host key pair on the SMA.

Revisit the CLI for the SMA, and re−run ***logconfig*** > ***hostkeyconfig*** in order to view the new host key pair.

Related Information

- ***Cisco Email Security Appliance − End−User Guides***
- ***Cisco Security Management Appliance − End−User Guides***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Jul 16, 2015 Document ID: 119177