Queest-ce que « quelqu'un essaye l'erreur de détourner connexion cryptée » fait signifie ?

Contenu

Introduction

Ce document décrit l'erreur « qu'il est possible que quelqu'un essaye de détourner la connexion cryptée au serveur distant, » et aux étapes correctives de prendre votre appliance de sécurité du courrier électronique de Cisco (ESA) et appliance de Gestion de sécurité Cisco (SMA).

Queest-ce que « quelqu'un essaye l'erreur de détourner connexion cryptée » fait signifie ?

Quand vous configurez votre transmission ESA avec votre SMA, vous pourriez voir cette erreur :

```
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.
```

Ceci peut se produire quand un ESA est remplacé et utilise la mêmes adresse Internet et/ou adresse IP que l'original ESA. Les ssh key précédemment enregistrés utilisés dans la transmission et l'authentification entre l'ESA et le SMA sont enregistrés sur le SMA. Le SMA voit alors que l'artère de communications ESA a changé, et croit qu'une source non autorisée est maintenant aux commandes de l'adresse IP assocaited à l'ESA.

Afin de corriger ceci, ouvrez une session au CLI du SMA, et terminez-vous ces étapes :

1. Sélectionnez la commande de **logconfig**.
2. Écrivez le **hostkeyconfig**.
3. Écrivez l'**effacement** et choisissez le numéro associé dans la liste actuellement installée de clé de hôte pour l'IP ESA.
4. Revenez à la demande principale CLI et sélectionnez la commande de **validation**.

```
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
```

En conclusion, du GUI SMA, choisissez **Serivces centralisé > dispositifs de sécurité** et puis sélectionnez l'ESA dans la liste qui avait présenté l'erreur d'origine. Une fois que vous choisissez **d'établir la connexion…** et la **connexion de test**, elle authentifie, crée une nouvelle paire de clé de hôte de SSH, et enregistre cette paire de clé de hôte sur le SMA.

Revisitez le CLI pour le SMA, et réexécutez le **logconfig > le hostkeyconfig** afin de visualiser les nouvelles paires de clé de hôte.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Appliance de Gestion de sécurité Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems