Wat betekent de fout "iemand probeert de versleutelde verbinding te kapen"?

Inhoud

Inleiding

Dit document beschrijft de fout "Het is mogelijk dat iemand de versleutelde verbinding met de externe host probeert te kapen" en de corrigerende stappen die u kunt uitvoeren op uw Cisco e-mail security applicatie (ESA) en Cisco Security Management-applicatie (SMA).

Wat betekent de fout "iemand probeert de versleutelde verbinding te kapen"?

Wanneer u de ESA communicatie met uw SMA aanpast, zou u deze fout kunnen zien:

```
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.
```

Dit kan gebeuren wanneer een ESA wordt vervangen en hetzelfde hostname- en/of IP-adres gebruikt als het oorspronkelijke ESA. De eerder opgeslagen SSH-toetsen die gebruikt worden voor communicatie en authenticatie tussen de ESA en de SMA, worden opgeslagen op de SMA. De SMA ziet dan dat het ESA communicatiepad is veranderd en gelooft dat een niet-geautoriseerde bron nu de controle heeft over het IP-adres dat aan de ESA is gekoppeld.

Om dit te corrigeren, logt u in bij de CLI van de SMA en voert u deze stappen uit:

1. Voer het **logconfiguratie** opdracht in.
2. Voer **hostkeyfig in**.
3. Typ de **schrapping** en kies het nummer dat bij de momenteel geïnstalleerde host-toetstitel voor de ESA IP hoort.
4. Ga terug naar de belangrijkste CLI prompt en voer de **toegewijde** opdracht in.

```
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
```

Ten slotte kies vanuit de SMA GUI, **Gecentraliseerde services > security applicaties** en selecteer vervolgens het ESR in de lijst met de oorspronkelijke fout. Zodra u hebt gekozen om **verbinding tot stand** te **brengen...** en **Test Connection**, deze authentiek, creëert een nieuw SSH host-toetsenpaar en slaat dit host-key paar op de SMA op.

Revisit de CLI voor het SMA, en rerun **logfig > hostkeyfig** om het nieuwe host-key paar te bekijken.

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Cisco Security Management-applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems