

Was bedeutet der Fehler "jemand versucht, die verschlüsselte Verbindung zu entschlüsseln"?

Inhalt

[Einführung](#)

[Was bedeutet der Fehler "jemand versucht, die verschlüsselte Verbindung zu entschlüsseln"?](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird der Fehler "Möglicherweise versucht jemand, die verschlüsselte Verbindung zum Remote-Host zu entschlüsseln" und die Korrekturmaßnahmen für Ihre Cisco Email Security Appliance (ESA) und Cisco Security Management Appliance (SMA) beschrieben.

Was bedeutet der Fehler "jemand versucht, die verschlüsselte Verbindung zu entschlüsseln"?

Wenn Sie die ESA-Kommunikation mit Ihrem SMA konfigurieren, wird möglicherweise der folgende Fehler angezeigt:

```
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.
```

Dies kann auftreten, wenn eine ESA ersetzt wird und den gleichen Hostnamen und/oder die gleiche IP-Adresse wie die ursprüngliche ESA verwendet. Die zuvor gespeicherten SSH-Schlüssel, die für die Kommunikation und Authentifizierung zwischen der ESA und SMA verwendet werden, werden im SMA gespeichert. Die SMA erkennt dann, dass sich der Kommunikationspfad der ESA geändert hat, und ist der Ansicht, dass eine nicht autorisierte Quelle nun die mit der ESA verknüpfte IP-Adresse kontrolliert.

Melden Sie sich zur Behebung dieses Problems bei der CLI der SMA an, und führen Sie die folgenden Schritte aus:

1. Geben Sie den Befehl **logconfig** ein.
2. Geben Sie **hostkeyconfig** ein.
3. Geben Sie **delete** ein, und wählen Sie die Nummer aus, die der aktuell installierten Hostschlüsselliste für die ESA-IP zugeordnet ist.
4. Kehren Sie zur Haupt-CLI-Eingabeaufforderung zurück, und geben Sie den **Commit**-Befehl ein.

```
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. sibld_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. euggui_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**

Wählen Sie schließlich in der SMA-GUI **Zentrale Services > Security Appliances** aus, und wählen Sie dann die ESA in der Liste aus, in der der ursprüngliche Fehler angezeigt wurde. Wenn Sie **Verbindung herstellen** möchten... und **Test Connection** authentifiziert, erstellt ein neues SSH-Hostschlüsselpaar und speichert dieses Hostschlüsselpaar im SMA.

Überprüfen Sie die CLI für SMA, und führen Sie **logconfig > hostkeyconfig** erneut aus, um das neue Hostschlüsselpaar anzuzeigen.

Zugehörige Informationen

- [Cisco Email Security Appliance - Benutzerhandbücher](#)
- [Cisco Security Management Appliance - Benutzerhandbücher](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)