Что делает, "кто-то пытается угнать зашифрованное соединение" ошибочное среднее значение?

Содержание

Введение

Этот документ описывает ошибку, "Возможно, что кто-то пытается угнать зашифрованное соединение к удаленному хосту" и корректирующие шаги для принятия Cisco Email Security Appliance (ESA) и Устройство менеджмента Cisco Security (SMA).

Что делает, "кто-то пытается угнать зашифрованное соединение" ошибочное среднее значение?

При настройке связи ESA с SMA вы могли бы видеть эту ошибку:

```
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.
```

Когда ESA заменен и использует то же имя хоста и/или IP-адрес как исходный ESA, это может произойти. Ранее сохраненные SSH-ключи, используемые в связи и аутентификации между ESA и SMA, сохранены на SMA. SMA тогда видит , что путь соединения ESA изменился и полагает, что неавторизованный источник теперь контролирует IP-адрес, привязанный к ESA.

Для исправления этого, входят к CLI SMA, и для выполнения этих шагов:

1. Введите **logconfig** команду.
2. Введите **hostkeyconfig**.
3. Войдите **удаляют** и выбирают номер, привязанный в в настоящее время устанавливаемой распечатке ключа хоста для IP ESA.
4. Возвратитесь к основному CLI, вызывают и вводят команду **передачи**.

```
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
```

Наконец, от GUI SMA, выберите**> Security Centralized Serivces Устройства** и затем выберите ESA в распечатке, которая представила исходную ошибку. Как только вы принимаете решение **Установить Соединение...** и **Тестовое подключение**, оно аутентифицирует, создает новую пару ключа хоста SSH и хранит эту пару ключа хоста на SMA.

Пересмотрите CLI для SMA и повторно выполните **logconfig> hostkeyconfig** для просмотра новой пары ключа хоста.

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Устройство менеджмента Cisco Security - руководства пользователя
- Cisco Systems – техническая поддержка и документация