Come affrontare l'integrazione di SMA ed ESA a causa di errori nell'algoritmo di scambio chiave/cifratura.

Sommario

Introduzione

In questo documento viene illustrato come risolvere i problemi di integrazione di Security Management Appliance (SMA) ed Email Security Appliance (ESA) che generano errori: "*(3, 'Impossibile trovare l'algoritmo di scambio chiavi corrispondente.') o "EOF imprevisto alla connessione*" e sintomi aggiuntivi.

Premesse

Connessione SMA all'ESA durante la prima integrazione, SMA offre i seguenti algoritmi di scambio di cifrari/chiavi all'ESA:

```
kex_algorithms string: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-
sha1,diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
encryption_algorithms_client_to_server string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-
cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-
cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

Una volta stabilita la connessione SMA ed ESA, l'SMA offre all'ESA i seguenti algoritmi di scambio di cifrari/chiavi:

```
kex_algorithms string: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-
sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-
hellman-group14-sha1,diffie-hellman-group1-sha1
encryption_algorithms_client_to_server string [truncated]: aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-
poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-
cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client string [truncated]: aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-
poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-
cbc,arcfour,rijndael-cbc@lysator.liu.se
```

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Il problema si verifica quando si integra lo SMA nell'ESA dalla **GUI > Management Appliance > Centralized Services > Security Appliance o dalla CLI > appliance config**. Il problema provocherà un errore sulla connessione, a causa della mancanza da parte dell'ESA di alcuni algoritmi di cifratura/algoritmi kex.

```
1. (3, 'Could not find matching key exchange algorithm.')
2. Error — Unexpected EOF on connect.
```

Soluzione

Per risolvere questo problema, è necessario riportare la configurazione della cifratura ESA ssh ai valori predefiniti forniti:

```
lab.esa.com> sshconfig


Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH whitelist/blacklist
[]> sshd

ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
```

L'output restituito da **CLI > sshconfig > sshd** nella configurazione dettagliata:

```
[]> setup

Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]>

Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-
cbc,aes256-cbc,rijndael-cbc@lysator.liu.se]>

Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-
96,hmac-md5-96]>

Enter the Minimum Server Key Size do you want to use
[1024]>

Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,diffie-hellman-group1-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521]>
```

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems
- Procedure ottimali per la quarantena centralizzata di virus ed epidemie
- Guida completa per la configurazione della quarantena della posta indesiderata ESA con SMA