Comment adresser l'intégration SMA et ESA devant introduire la panne d'algorithme d'échange/chiffrement.

Contenu

Introduction

Couvertures de ce document comment adresser des pannes d'intégration des appareils de Gestion de la sécurité (SMA) et des appareils de sécurité du courrier électronique (ESA) ayant pour résultat des erreurs : « *(3, « ne pourraient pas trouver l'échange clé assorti algorithm.") ou « l'EOF inattendu se connectent en fonction* » et des symptômes supplémentaires.

Informations générales

La connexion SMA à l'ESA tout en d'abord intégrant, SMA offre les chiffrements/les algorithmes suivants échange de clé à l'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
```

Après SMA et ESA la connexion est établie, le SMA offre les chiffrements/les algorithmes suivants échange de clé à l'ESA :

```
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
```

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Problème

La question existe en intégrant le SMA à l'ESA du l'**appliance GUI > de Gestion > a centralisé des services > des dispositifs de sécurité ou CLI > applianceconfig**. La question incitera une erreur sur la connexion, ceci est due à l'ESA manquant certains des algorithmes de kex/d'algorithmes de chiffrement.

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

Solution

Pour résoudre ceci, la configuration de chiffrement de ssh ESA doit être achetée de nouveau aux valeurs par défaut fournies :

```
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
```

La sortie du **CLI > sshconfig > sshd** sur l'installation pas à pas :

```
[]> 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]>
```

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems
- Pratique pour la quarantaine centralisée de virus et d'épidémie de stratégie
- Le guide complet pour la quarantaine de Spam ESA a installé avec SMA