Understand SSH Crypto Algorithms on ISE 3.3 Patch 4

Contents

Introduction

This document describes about SSH Crypto Algorithms on ISE version 3.3 Patch 4

Pre-Requisites

You must have the basic knowledge of the Cisco Identity Service Engine (ISE)

Knowledge on SSH Protocol

Knowledge on Host-Key Algorithms

Components Required

The information in this document is based on these software and hardware versions

- Cisco Identity Services Engine 3.3 Patch 4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Objectives

Develop and Implement CLI Commands to Support Configurable SSH Algorithms, Addressing Security Vulnerabilities as per your requirements.

Functional Benefits

1. Enhanced SSH Security Compliance with NIST guidelines.
2. Flexible Configuration options for SSH Algorithms to meet specific security policies.

Key Features Implemented

1. Configurable HostKey and Hostkey Algorithm from CLI.
2. Support for ecdsa-sha2-nistp256 and ed host key.
3. Support for hmac-sha2-256 and hmac-sha2-512 for Secure SSH Connections

CLI Commands

- Service ssh host-key-algorithm
- Service sshd host-key
- Service sshd host-key-algorithm
- Service sshd mac-algorithm

Configurable SSH HostKey Algorithm

To Configure the SSH HostKey Algorithm for External Server Communication

Command: **asc-ise33p4/admin(config)# service ssh host-key-algorithm ?**

```
Possible completions:

  ecdsa-sha2-nistp256   Configure ecdsa-sha2-nistp256 algo

  rsa-sha2-256          Configure rsa-sha2-256 algo

  rsa-sha2-512          Configure rsa-sha2-512 algo

  ssh-rsa               Configure ssh-rsa algo
```

Note: This is for SSH

Configurable SSHD HostKey Algorithm

To Configure the SSHD HostKey for SSH Server Authentication.

Command: **asc-ise33p4/admin(config)# service sshd host-key ?**

Possible completions:

```
  host-ecdsa-256      Configure ssh host ecdsa 256 key
  host-ed25519        Configure ssh host ed25519 key
  host-rsa            Configure ssh host rsa key
```

To Configure the SSHD Host Key Algorithm for SSH Server Authentication.

Command: **asc-ise33p4/admin(config)#service sshd host-key-algorithm ?**

```
Possible completions:
  ecdsa-sha2-nistp256   Configure ecdsa-sha2-nistp256 algo
  rsa-sha2-256          Configure rsa-sha2-256 algo
  rsa-sha2-512          Configure rsa-sha2-512 algo
  ssh-ed25519           Configure ssh-ed25519 algo
```

To Configure SSHD MAC Algorithm for SSH Server Authentication.

Command: **asc-ise33p4/admin(config)#service sshd mac-algorithm ?**

```
Possible completions:
  hmac-sha1                      Configure hmac-sha1 algo
  hmac-sha1-etm-openssh.com      Configure hmac-sha1-etm-openssh.com algo
  hmac-sha2-256                  Configure hmac-sha2-256 algo
  hmac-sha2-256-etm-openssh.com  Configure hmac-sha2-256-etm@openssh.com algo
  hmac-sha2-512                  Configure hmac-sha2-512 algo
  hmac-sha2-512-etm-openssh.com  Configure hmac-sha2-512-etm@openssh.com algo
```

Note: This is for SSHD

Troubleshooting

Verify

SSH:

```
isepri33/admin(config)#service ssh host-key-algorithm ecdsa-sha2-nistp256
```

```
isepri33/admin#show running-config service ssh
service ssh host-key-algorithm ecdsa-sha2-nistp256
```

SSHD:

```
isepri33/admin(config)#service sshd host-key-algorithm ecdsa-sha2-nistp256
```

```
isepri33/admin#show running-config service sshd
service sshd enable
service sshd encryption-algorithm aes128-ctr aes128-gcm-openssh.com aes256-ctr aes256-gcm-openssh.com chacha20-poly1305-openssh.com
service sshd host-key-algorithm ecdsa-sha2-nistp256
service sshd mac-algorithm hmac-sha1 hmac-sha2-256 hmac-sha2-512
service sshd host-key host-rsa
```

Log Snippet:

```
isepri33/admin#show logging system confd/confd.log
2025-03-18 08:35:25,241 [INFO] service_conf.py update_host_key_algorithms line:575 Updated SSH Host Keys Algorithms successfully
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithms: ecdsa-sha2-nistp256
2025-03-18 08:35:39,260 [INFO] service_conf.py restart_sshd line:259 Restarted sshd successfully

2025-03-18 08:48:20,194 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithms: ecdsa-sha2-nistp256
2025-03-18 08:48:20,396 [INFO] service_conf.py restart_sshd line:259 Restarted sshd successfully
2025-03-18 08:48:20,400 [INFO] service_conf.py update_host_key_algorithms line:575 Updated SSH Host Keys Algorithms successfully
2025-03-18 08:49:00,442 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithms: ecdsa-sha2-nistp256
2025-03-18 08:49:00,672 [INFO] service_conf.py restart_sshd line:259 Restarted sshd successfully
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algorithms line:575 Updated SSH Host Keys Algorithms successfully
```

FAQ

Question: What is the default SSH Host Key Algorithm enabled on ISE?

Answer: They are:

- rsa-sha2-256
- rsa-sha2-512

Question: What are the default SSHD MAC Key Algorithm?

Answer: They are:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

Question: What is the default SSHD host-key?

Answer: host-rsa

Question: Whar are the Default SSH Host Key?

Answer: They are:

- rsa-sha2-256
- rsa-sha2-512
- ssh-rsa