Cisco EPN Manager Security

This chapter consists of the following topics:

Security Overview

Cisco EPN Manager requires a high level of security to ensure that your network and its data are not compromised. This is especially important because it has full management control over your network and stores device credentials. To this end, Cisco EPN Manager leverages the following security approaches:

- **Secure architecture**: The Cisco EPN Manager architecture is designed to limit access to any unknown software flaws that may be present so they cannot be used for a malicious purpose.
- **Secure default configurations**: Cisco EPN Manager is shipped with a default configuration that enhances the security of the product. For example, even though insecure FTP and TFTP services are supported, they are not activated in the default configuration.
- **Installation hardening**: Cisco's Advanced Services team can evaluate the specifics of your Cisco EPN Manager installation and complete the additional security hardening tasks that may be needed.
- **Cisco Secure Development Lifecycle (CSDL) process**: From development to release, the CSDL process is followed to improve security of Cisco EPN Manager .

The following sections describe these approaches in more detail.

Secure Architecture

Cisco EPN Manager 's architecture design is based on the premise that 3 conditions must exist simultaneously in order for an attacker to breach a system:

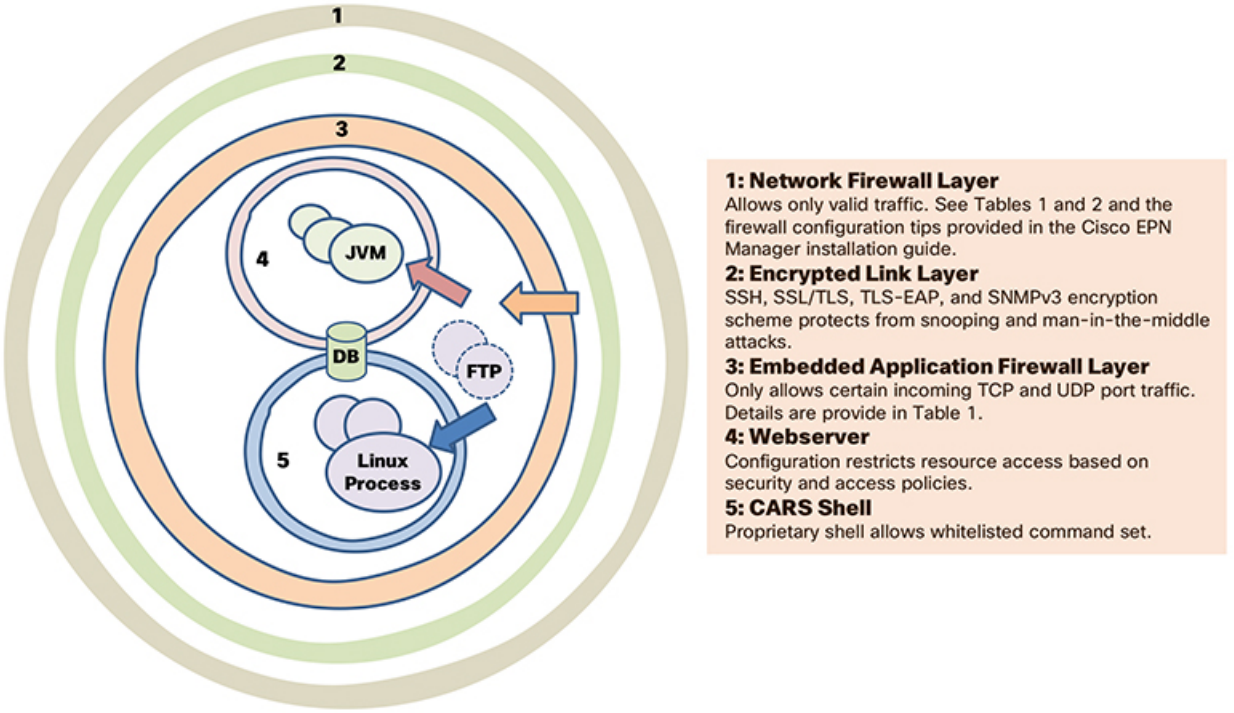
- The system has a flaw.
- The attacker has access to that flaw.

- The attacker is capable of exploiting the flaw for a malicious purpose. (Hughes, J., & Cybenko, G. 2013. Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. *Technology Innovation Management Review*, 3(8): 15-24.)

On its own, a flaw is benign. It is only when an attacker can access the flaw and knows how to exploit it that the flaw becomes a vulnerability. This distinction between a flaw and a vulnerability is important to understand. Just because a flaw has gone public does not automatically mean it has become a vulnerability. And a flaw may only be a vulnerability under certain circumstances.

Limiting access to system flaws is key to the approach Cisco EPN Manager uses to manage security risks. We have designed the Cisco EPN Manager architecture so that any flaws that may be found should not be readily accessible to an attacker. This is a practical and reasonable approach because you cannot always eliminate flaws or prevent an attacker from exploiting them. What you can do is limit access to certain flaws that exist by putting multiple layers of security in place. Cisco EPN Manager uses three layers of perimeter security, as illustrated in Figure 1.

Figure 1: Multilayer Secured Perimeter Architecture: A Closed System



425568

Of these three layers, one resides within and two reside outside of Cisco EPN Manager . The interior layer is preconfigured with Cisco EPN Manager and becomes operational after the installation is completed. The two exterior layers are not preconfigured and need to be implemented by creating an exterior network firewall and encrypted communication link layer. We recommend that your company's technical team works with Cisco Advanced Services to create these items.

Note You may need to modify some configurations within Cisco EPN Manager in order to choose the right kind of encryption protocols to use for your network.

The interior layer is built into Cisco EPN Manager and consists of the following components:

- Embedded firewall—Provides the first protective layer around the interior components. This allows only a few ports to be open to incoming traffic. This decreases the attack surface by limiting access to multiple flaws (both known and unknown) in the Linux OS and Oracle databases.
- CARS shell—Provides a protective layer around Linux by enforcing a whitelist of allowed commands that can be run on Linux, thus restricting interaction with the OS.
- Web server—Provides a protective layer around Linux, the Java virtual machine, and the database. This layer has security filters in place for restricting access to Java as well as the database resources and methods.

This interior layer protects the system against many risks, such as the ones described in the following examples. While these flaws are deemed vulnerabilities in an unprotected system, there are not in Cisco EPN Manager . In these examples (identified by their National Vulnerability Database ID), we will assume that the external firewall and encrypted links layer have either been breached by an attacker or are non-existent:

- CVE-2013-5211: Flaw in NTP's implementation of the Linux NTPD component—A DoS attack takes place after incoming NTP traffic is accessed from port 23. Since the embedded firewall disallows this traffic, this flaw is not accessible to an attacker and therefore not a risk in Cisco EPN Manager .
- CVE-2016-0634: Linux bash shell flaw—This attack can be made by an authenticated user that has targeted a bash shell through port 22. Cisco EPN Manager does not offer direct access to a bash shell via port 22. Instead, a CARS shell is accessible by regular authenticated users. As a result, this flaw is not a risk in Cisco EPN Manager .
- CVE-2017-12617: Apache Tomcat flaw—This attack can happen when a PUT request is made. Since Cisco EPN Manager 's webserver configuration does not allow this kind of access, this flaw is not a risk.
- CVE-2015-4863: Oracle database flaw—This attack can happen on a network via the Oracle Net protocol. This flaw is not a risk in Cisco EPN Manager since the Oracle database resides behind the built-in firewall and webserver. As a result, it is not possible to access the database over the network.

Ports Used by Cisco EPN Manager

Cisco EPN Manager ships with a built-in application firewall configuration to ensure that only legitimate traffic is allowed into the server. Table 1 lists the ports used to listen for connection requests from devices and accept incoming traffic. The opening and closing of these ports in the firewall is done automatically by Cisco EPN Manager when you enable or disable certain features. There is no need to enable or disable the ports within the firewall. If you try to specify any firewall configurations that circumvent Cisco EPN Manager , you may compromise its security and integrity.

Note Table 1 also provides information required to carry out post-installation security hardening (see Secure Default Configurations for more information).

Table 1: Listening Ports That Are Open Through Built-in Firewall

Port	Protocol	Usage	Safe to Disable?	Notes
21	TCP	To transfer files to and from devices using FTP.	Yes	Disable FTP from the web GUI under **Administration > Settings > System Settings**, then choose **General > Server**. After disabling FTP, as the CLI admin user, stop and restart the server.
22	TCP	To initiate SSH connections with the Cisco EPN Manager server, and to copy files to the Cisco EPN Manager server using SCP or SFTP.	Depends	This might be still needed by older managed devices that only support TFTP and not SFTP or SCP.
69	UDP	To distribute images to devices using TFTP.	Depends	Only if alternative protocols like SCP or SFTP or HTTPS are used for image distribution, and if supported by the managed devices.
162	UDP	To receive SNMP traps from network devices.	No	—
443	TCP	For browser access to the Cisco EPN Manager server via HTTPS.	No	—
514	UDP	To receive syslog messages from network devices.	No	—
1522	TCP	For High Availability (HA) communication between active and standby Cisco EPN Manager servers. Used to allow Oracle JDBC traffic for Oracle database synchronization.	Yes	If at least one Cisco EPN Manager server is not configured for HA, this port is automatically disabled.
2021	TCP	To distribute images to devices using FTP.	No	—
8082	TCP	For the HA Health Monitor web interface (via HTTP). Used by primary and secondary servers to monitor their health status via HTTP.	No (If HA configured)	—
8087	TCP	To update software on the HA secondary backup server (uses HTTPS as transport).	No	—

Port	Protocol	Usage	Safe to Disable?	Notes
9991	UDP	To receive Netflow data packets.	Yes	Cisco EPN Manager does not support Netflow. You should disable this traffic in the network firewall.
9992	TCP	To manage M-Lync using HTTP or HTTPS.	Yes	Cisco EPN Manager does not support M-Lync. You should disable this traffic in the network firewall.
11011 to 11014	TCP	For PnP operations for proprietary Cisco Network Service (CNS) protocol traffic.	Yes	Cisco EPN Manager does not support PnP. You should disable this traffic in the network firewall.
61617	TCP	For MTOSI NBI notification over Java Message Service (JMS) connections. Also used for PnP operations.	Yes	Cisco EPN Manager does not support MTOSI over JMS or PnP. You should disable this traffic in the network firewall.

Secure Default Configurations

Cisco EPN Manager ships with default application configurations that are as secure as possible. You should only modify them after you have analyzed the threat model and assessed the risks for your specific situation. With the default configurations, Cisco EPN Manager does its best to:

- Not use default passwords.
- Not make unnecessary OS and Oracle packages/services accessible.
- At the time of a Cisco EPN Manager release, the latest security patches are applied for the embedded OS and Oracle.
- Not allow the use of Oracle access passwords by human users. These passwords are machine-generated and used by internal components.

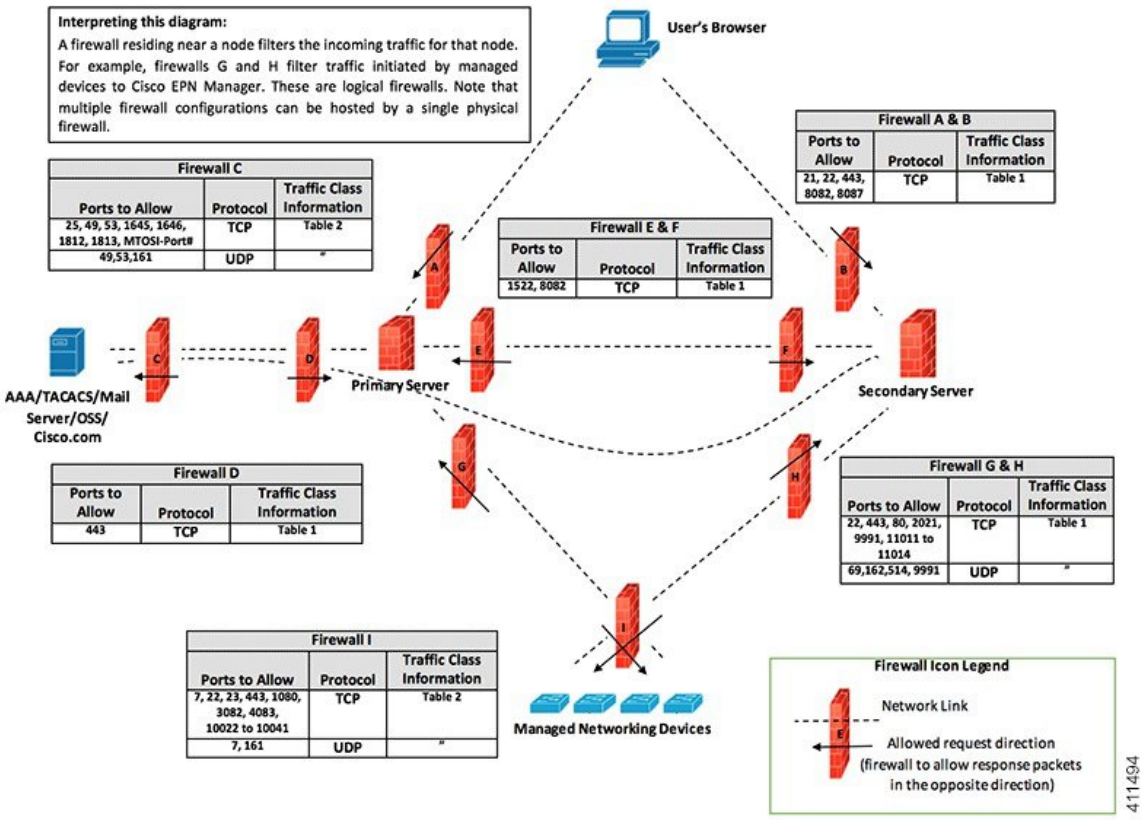
Harden Your Installation

To harden your Cisco EPN Manager installation, you need to complete the following tasks:

1. Configure the built-in interior and exterior network firewalls to allow only legitimate traffic.
2. Use encryption for all incoming and outgoing traffic.
3. Configure Cisco EPN Manager and its peer systems to allow the transmission of only legitimate transactions.

Before you proceed, you should first understand how Cisco EPN Manager interacts with peer systems. This, along with management traffic flows and the exterior network firewalls for a generic HA deployment, is illustrated in the following figure.

Note Although we recommend that you implement these firewalls, you are not required to do so.



Depending on your installation, you may need to customize the firewall configuration to further improve security. As a general policy, any ports that are not needed and not secure (i.e. do not transmit encrypted traffic) should be disabled.

Configure the Built-In Application Firewall

To configure the application firewall, you need to disable the Cisco EPN Manager features that your installation does not need to run. This will automatically shut down the corresponding listening ports in the firewall.

Step 1 Identify the ports that are currently enabled:

a) To view a list of the ports used in your deployment that are exposed externally, log in as a Cisco EPN Manager CLI admin user and then run the **show security-status** command.

b) To view a list of all open listening ports at the OS level, including those that are blocked by the built-in firewall, log in as the Linux CLI admin user and then run the **netstat -aln** command.

Step 2 Using Table 1 for guidance, determine which of these ports can be safely disabled without disrupting the normal functioning of Cisco EPN Manager .

Note the following:

- Cisco EPN Manager uses some of the listening ports for its internal operations. These ports are kept hidden behind the built-in firewall.
- You should only use the procedure provided in Table 1 to enable or disable ports.

Set Up Exterior Network Firewalls

In addition to the built-in firewall, you can also deploy network firewalls that only allow traffic targeted at the listening ports used by Cisco EPN Manager and its peer systems. The figure provided in the Harden Your Installation topic illustrates how the port information listed in Tables 1 and 2 are used to set up firewall rules. Use this figure to decide on the appropriate firewall configurations for your management network.

- To identify the traffic class, refer to the **Usage** column in Table 1. We recommend that you disable the ports used by the services that are not used by your Cisco EPN Manager installation.
- You should also enable the destination ports that Cisco EPN Manager uses for outgoing traffic (to connect to network devices or peer systems) in your network firewalls. Refer to Table 2 for a listing of these destination ports and their purpose.

Table 2: Destination Ports Used by Cisco EPN Manager

Port	Protocol	Used to:
7	TCP/UDP	Discover endpoints using ICMP.
22	TCP	Initiate SSH connections with managed devices.
23	TCP	Communicate with managed devices using Telnet.
25	TCP	Send email using an SMTP server.
49	TCP/UDP	Authenticate Cisco EPN Manager users using TACACS.
53	TCP/UDP	Connect to DNS service.
161	UDP	Poll using SNMP.
443	TCP	Upload or download images and perform configuration backup-restore for Cisco NCS 2000 devices using HTTPS.
1522	TCP	Communicate between primary and secondary HA servers (allows Oracle JDBC traffic for Oracle database synchronization between primary and secondary servers).
1080	TCP	Communicate with Cisco Optical Networking System (ONS) and Cisco NCS 2000 series devices using Socket Secure (SOCKS) protocol.

Port	Protocol	Used to:
1645, 1646, and 1812, 1813	UDP	Authenticate Cisco EPN Manager users using RADIUS.
3082	TCP	Communicate with Cisco ONS and Cisco NCS 2000 devices using TL1 protocol.
4083	TCP	Communicate with Cisco ONS and Cisco NCS 2000 series devices using TL1 protocol.
8082	TCP	Communicate between primary and secondary HA servers to monitor each other's health using HTTPS.
10022 to 10041	TCP	Passive FTP file transfers (for example, device configurations and report retrievals).
MTOSI/RESTCONF TCP port number	TCP	Listen at NBI client connected to the Cisco EPN Manager server (after this port is configured by NBI client system, a registration notification message containing the port number is sent to Cisco EPN Manager server); refer to the MTOSI or RESTCONF API guide for more information.

Set Up Traffic Encryption

You will need to encrypt the following traffic groups:

- Northbound traffic—This group consists of either client-server traffic from a human user's browser or NBI traffic from a Business Support System/Operational Support System (BSS/OSS). This traffic is transmitted over HTTP, so you need to implement HTTPS (HTTP encrypted by TLS). For a description of how to set up HTTPS, see Set Up HTTPS to Secure the Connectivity of the Web Server.
- Southbound traffic—This group consists of management traffic that queries or configures managed devices using a wide range of protocols such as SNMP and HTTP. Protocols such as SSH and SNMPv3 may be used to secure this traffic. For a description of the configuration steps that need to be completed in order to encrypt this traffic, see Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices.
- East-West traffic between peer systems—This group consists of traffic between Cisco EPN Manager and a variety of other supporting systems like an external authentication server (secured by TLS-EAP) or a SMTP mail server (secured by TLS). Different encryption protocols are used, depending on the application protocol that needs to be protected. Some of the application protocols may also have built-in encryption.
- East-West traffic between a primary and secondary server in an HA deployment—This group consists of traffic between two Cisco EPN Manager servers running in primary and secondary mode. Each server monitors the other's health and keeps database and other file content synchronized over a connection secured by HTTPS.

Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices

SNMPv3 is a higher security protocol than SNMPv2. If your devices support SNMPv3, configure the devices to use SNMPv3 to communicate with the Cisco EPN Manager server. The following procedures explain how to specify SNMPv3 when adding new devices.

Method for Adding Devices	How to Specify SNMPv3	For more information, see:
Add a single device	In the **Add Device** dialog box, go to the **SNMP Properties** page and choose **v3** from the **Versions** drop-down list.	Add Devices Manually (New Device Type or Series)
Add multiple devices (bulk import)	When you edit your CSV file, enter the following: • Enter **3** in the **SNMP Version** column. • Enter the appropriate values for these columns: **snmpv3_user_name**, **snmpv3_auth_type**, **snmpv3_auth_password**, **snmpv3_privacy_type**, and **snmpv3_privacy_password**	Import Devices Using a CSV File
Add multiple devices using discovery	In the **Discovery Settings** dialog box, go to the **Credential Settings** area and click **SNMPv3 Credentials**. Click the + sign to add the device credentials.	Run Discovery With Customized Discovery Settings

Before you begin

Make sure SNMPv3 is enabled (with the appropriate security algorithm, such as HMAC-SHA-96) on the network devices that support it.

Set Up External Authentication Using the CLI

We recommend that you manage user accounts and passwords using a dedicated, remote authentication server running a secure authentication protocol such as RADIUS or TACACS+. In addition to setting up authentication using the following procedure, contact your external authentication vendor for additional security hardening suggestions.

Note If you decide to use local user authentication, check the default password policies to determine whether you want to make them stronger. See Configure Global Password Policies for Local Authentication.

Configure Cisco EPN Manager to authenticate users using an external AAA server. You can configure the server using the web GUI or by using the command line interface (CLI). To set up remote user authentication via the GUI, see Configure External Authentication.

To configure external authentication using the CLI, follow these steps. In this example, external authentication will be done by an external TACACS+ server.

Step 1 Log in to Cisco EPN Manager using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server.

Step 2 Enter config mode.

Step 3 Enter the following command to setup an external authetn TACACS+ server:

```
aaa authentication tacacs+ server tacacsIP key plain shared-secret
```

Where:

- *tacacsIP* is the IP address of an active TACACS+ server.
- *shared-secret* is the plain-text shared secret for the active TACACS+ server.

Step 4 Enter the following command to create a user with administrator privileges, who will be authenticated by the server specified in the previous step:

```
username username password remote role admin [email emailID]
```

Where:

- *username* is the name of the user ID.
- *password* is the plain-text password for the user.
- *emailID* is the email address of the user (optional).

Harden SSH Against Brute-Force Password Attacks

Since password-based SSH authentication is vulnerable to brute-force attacks, we recommend that you switch to RSA key-based SSH authentication after installing Cisco EPN Manager . To make the switch, do the following:

Step 1 Log in as the Linux CLI admin user:

a) Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
b) Run the following command: **shell**
c) Enter the shell access password.

Step 2 Check who the current user is:

```
# whoami
```

The resulting output should indicate that you are the Linux admin user, not the Linux root user.

Step 3 For the Cisco EPN Manager admin user, create RSA key pairs and an SSH string using a tool (such as puTTYgen) with at least 2048-bit strength.

The SSH string should look something like this:

```
ssh-rsa AAAAB3NzaC1y ... ..... 0Q== rsa-key-20180128
```

Tip Save the private key in a file, preferably in encrypted form with a passphrase. Also keep the passphrase handy.

Step 4 Create the authorized_keys file and assign the appropriate access privileges to the Cisco EPN Manager admin user:

a) In the admin user's home directory, create the .ssh directory and assign read, write, and execute privileges for this directory to only the admin user:

```
# cd ~
# mkdir .ssh
# chmod 700 ~/.ssh
```

b) Create the authorized keys file:

```
# cd .ssh
# vi authorized_keys
```

c) Copy and paste the SSH string you created in Step 3 in to the authorized_keys file and then save the file.

d) Assign read, write, and execute privileges for the authorized_keys file to only the admin user:

```
# chmod go= ~/.ssh/authorized_keys
# chmod u=rwx ~/.ssh/authorized_keys
```

e) Confirm you assigned the appropriate access privileges to the authorized_keys file:

```
# ls -al
```

The resulting output should look something like this:

```
total 6
drwx------. 2 admin gadmin 1024 May 10 00:25 .
drwx------. 6 admin gadmin 1024 May 10 00:24 .
-rwx------. 1 admin gadmin 398 May 10 00:25 authorized_keys
```

In this example, the Linux admin user is named `admin`

Step 5 Switch to the root user in a bash shell:

```
# sudo -i
```

Step 6 Update the sshd_config file:

a) Copy the current and original versions of the sshd_config file, located in the /etc/ssh directory:

```
# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.orig
```

b) Open the sshd_config file in a vi editor:

```
# vi /etc/ssh/sshd_config
```

c) Enter the following key-value pairs:

```
Protocol 2
KeyRegenerationInterval 1h
ServerKeyBits 2048
MaxAuthTries 4
PasswordAuthentication no
PermitRootLogin no
AuthenticationMethods publickey
PubkeyAuthentication yes
```

Important The default sshd_config file may already specify some of these key-value pairs. If this is the case, either:

- Change any values that do not match the ones listed above.
- Comment out the existing key-value pairs and specify the required entries on new lines.

Doing so will prevent conflicting or duplicate key-value pairs.

d) Save the file.

Step 7 Reload sshd:

```
# systemctl reload sshd.service
```

Caution Do not restart sshd. If any of the previous configuration steps are not completed correctly and you restart sshd, you will lose access to SSH. It is much safer to reload sshd because current SSH sessions are maintained (allowing you to make any necessary corrections).

The configuration of RSA key-based SSH authentication is complete. To confirm that configuration was successful, keep the existing SSH session open (in case you need to fix something) and try to open a new SSH session using the private key and passphrase you created in Step 3 of this procedure.

Harden NTP

Network Time Protocol (NTP) authenticates server date and time updates. We recommend you configure the Cisco EPN Manager server to perform time synchronization over NTP. Failure to manage NTP synchronization across your network can result in anomalous results. Management of network time accuracy is an extensive subject that involves your organization's network architecture and falls outside the scope of this guide. For more information on this topic, see (for example) the Cisco white paper Network Time Protocol: Best Practices.

Note the following:

- Because using NTP creates the possibility of security breach-related disruptions, you should also harden the NTP aspect of the Cisco EPN Manager server by using NTP version 4 (NTPv4). Cisco EPN Manager also supports NTPv3 because NTPv4 is backward compatible with NTPv3.
- You can configure a maximum of 3 NTP servers with Cisco EPN Manager .

Set Up NTP on the Cisco EPN Manager Server

To use the Network Time Protocol (NTP) to synchronize clocks on the server and network devices using an NTP server, NTP must first be set up on the Cisco EPN Manager server. For information on how to do this, see Set Up NTP on the Server.

Enable Authenticated NTP Updates

Complete the following procedure to set up authenticated NTP updates:

Step 1 Log in to Cisco EPN Manager using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server.

Step 2 Enter config mode.

Step 3 Enter the following command to setup an external NTPv4 server:

```
ntp server serverIP userID plain password
```

Where:

- *serverIP* is the IP address of the authenticating NTPv4 server you want to use.

- *userID* is the md5 key id of the NTPv4 server.
- *password* is the corresponding plain-text md5 password for the NTPv4 server.

For example:

```
ntp server 209.165.202.128 20 plain myPass123
```

Step 4 Perform these tests to ensure NTP authentication is working correctly:

a) Check the NTP update details:

```
show run
```

b) Check NTP sync details:

```
show ntp
```

Configure External NFS-Based Storage Servers

NFS servers may be used as external storage in a Cisco EPN Manager installation, especially for data backup. Since NFS does not have built-in security, you must implement as many of the following security measures as possible to secure the NFS server:

- Set up a firewall in front of the NFS server—To do this practically, tie down the ports that NFS will use in various configuration files and then specify those ports in the firewall configurations.
- Use a port mapper—On the NFS server, only allow NFS transactions that involve specific IP addresses.
- To prevent attacks via a compromised DNS, only specify IP addresses (and not domain names) when configuring NFS.
- When setting up the export of folders, use the **root_squash** option in the /etc/exports file.
- When configuring the /etc/exports file, use the **secure** option.
- When configuring the backup staging and storage folders, use the **nosuid** and **noexec mount** options.

Note It is not mandatory to configure a staging folder.

- For the storage folder (and optional staging folder), configure a file access permission value of **755** (which grants all users read and write privileges) and set userid **65534** (the user **nobody**, who does not have any system privileges) as the owner.
- Tunnel NFS traffic either through SSH or SSL/TLS. For SSH, use RSA key-based authentication instead of user authentication.

Do not rely on just one of these measures to secure your NFS-based storage. Your best bet is to implement the combination of measures that best suits your situation. Also keep in mind that this list is not an exhaustive one. To achieve a higher level of confidence when hardening your storage, we recommend that you discuss your situation with a Linux system admin and a security expert beforehand.

CSDL Process

Cisco EPN Manager development adheres to the Cisco Secure Development Lifecycle (CSDL) process. This covers the entire development-to-deployment timespan to improve product and installation security. Cisco EPN Manager 's product design is reviewed from a security viewpoint against specific criteria and the product is tested using security tools and test methods. In addition, Cisco EPN Manager is reviewed by external security experts and penetration testers. See Cisco Security Issue Resolution Process for a description of how security fixes are deployed (as part of the Cisco EPN Manager update lifecycle).

Cisco Security Issue Resolution Process

There are 2 types of defects and vulnerabilities: customer-found and Cisco-found. Let's cover how Cisco addresses them for Cisco EPN Manager .

Customer-Found Defects and Vulnerabilities

1. After a customer raises a service request with the Cisco Technical Assistance Center (TAC), the Cisco TAC opens a case with the support team who (depending on the problem) may open a Cisco Defect and Enhancement Tracking System (CDETS) defect report.
2. Cisco evaluates the defect to determine whether that defect poses a security risk to Cisco EPN Manager . If the defect does pose a security risk, then Cisco categorizes it as a vulnerability. Otherwise, Cisco treats the defect as a regular software defect.
3. Cisco does one of the following:
   - For security vulnerabilities, Cisco reports it to the Cisco Product Security Incident Response Team (PSIRT), develops a fix that adheres to Cisco PSIRT guidelines, and then allows Cisco PSIRT to handle both the disclosure of the vulnerability to the client and delivery of the patch.
   - For defects, Cisco determines its severity and schedules the release of a fix.

Cisco-Found Defects and Vulnerabilities

For the first year following the end-of-sale date for a Cisco EPN Manager version, Cisco provides bug fixes, maintenance releases, workarounds, or patches for critical bugs and security vulnerabilities reported via the TACS or Cisco.com Web site.