# Security Best Practices Overview



## Software Version

The recommendations made in this document are for the following software version:

- Cisco Modeling Labs 1.0 Corporate Edition

## Cisco Modeling Labs Client

The Cisco Modeling Labs client interface is built using the Eclipse platform. (Refer to https://www.eclipse.org/ for information about Eclipse.) The client provides the GUI for Cisco Modeling Labs and runs on a personal computer using Microsoft Windows or Apple Mac OS X.

Using the GUI, the user designs a network topology. The topology configuration file is saved to a local file and has the filename extension **.virl**. For example, a topology named Test_Network is stored in the file Test_Network.virl. To verify the location of the file, right-click the filename where it is shown in the **Projects** view in the Cisco Modeling Labs client and display the file properties. The default directory locations are noted below:

On a Windows operating system, the Test_Network.virl file is stored in the directory c:\Users\<*userid*>\cml\workspace\<*project folder*>\.

On a Apple Mac OS X, the Test_Network.virl file is stored in the directory /Users/<*userid*>/cml/workspace/<*project folder*>/.

We recommend that you secure this file so that your IP addresses are not exposed. How you choose to secure the file is based on your local security practices that may include the following policies:

- Password protection

- Data encryption
- Disk encryption
- File backup

# Cisco Modeling Labs Server

The Cisco Modeling Labs Server consists of several components, including the following:

- Operating System
- OpenStack

# Linux-based Operating System

Cisco Modeling Labs server uses a Linux-based operating system. The services that are not required to support Cisco Modeling Labs have been disabled.

The server administrator can install and remove applications, and perform software updates.

**Caution** Operating system updates may cause loss of function within Cisco Modeling Labs. Before performing any update, contact the Cisco Technical Assistance center (TAC) for further information and assistance.

When the Cisco Modeling Labs server is deployed in a nonproduction lab environment, the impact of a security breach is limited by the confidentiality of the configurations stored in the environment, the loss of time invested in building and configuring the environment, and potentially using the environment as a jump host to other parts of the network if external connections are established.

When setting security on the Cisco Modeling Labs server, we recommend that you perform the following security tasks:

- Install and configure the firewall.
- Secure shared memory.
- Protect the substitute user **su** command by limiting access to the admin group only.
- Harden network access with the **/etc/sysctl.conf** settings.
- Prevent IP spoofing.
- Restrict Apache information leakage.
- Install and configure the Apache web application firewall.
- Ban suspicious hosts.
- Monitor intrusion detection.
- Scan for rootkit software.
- View and analyze log files.
- Scan open ports on the system.

For Cisco Modeling Labs 1.0, the active ports in the Linux-based operating system are shown in the following table:

***Table 1: Cisco Modeling Labs 1.0 Active Ports***

| Port Number | Description |
|---|---|
| 22 | SSH |
| 80 | HTTP |
| 8080 | HTTP |
| 3306 | MySQL |
| 8000 | HTTP |
| 5000 | UPnP |
| 8081 | HTTP |
| 3333 | HTTP |
| 443 | Default port for Telnet over Web Socket (ws:// and wss://) |

# OpenStack Security Overview

Cisco Modeling Labs 1.0 uses the following components of OpenStack:

- Dashboard (Horizon)
- Compute (Nova)
- Networking (Neutron)
- Image Service (Glance)
- Identity Server (Keystone)

# OpenStack Dashboard Security

The OpenStack Dashboard provides administrators with an interface for provisioning and accessing cloud-based resources. Cisco Modeling Labs User Workspace Management interface is a modified version of the OpenStack dashboard. See Accessing the User Workspace Management Interface for additional information about the interface and how it is used.

**Note** The User Workspace Management interface in Cisco Modeling Labs uses HTTP rather than the more secure HTTPS.

When creating user accounts, consider the following recommendations:

- Verify the access privileges to avoid assigning administrator access to nonadministrator accounts.
- Limit the resources allocated to each user to ensure that services do not become constrained and stop server operations.
- Assign expiry dates.
- Review user accounts regularly.

# OpenStack Compute Security

The Nova OpenStack Compute Service is a cloud-computing fabric controller that manages and automates pools of computing resources. Nova is designed to work with virtualization technologies, and is subject to the same security risks that confront non-virtual environments.

No specific recommendations are provided for hardening the OpenStack Image Service as deployed for Cisco Modeling Labs.

# OpenStack Networking Security

The Neutron OpenStack Networking Service, (formerly Quantum), manages networks and IP addresses.

To ensure network security:

- Change the default passwords for administrator access to virtual network computing (VNC) and Telnet sessions.
- Ensure that connections between the production network environments and the Cisco Modeling Labs network do not bypass firewalls and other network perimeter security policies.

# OpenStack Image Service Security

The Glance OpenStack Image Service provides the discovery, registration, and delivery services for disk images and server images. Within Cisco Modeling Labs, Glance stores the Cisco Modeling Labs server images and the Cisco node images for the supported image types, such as Cisco IOSv, Cisco IOSXRv, and Cisco CSR1000v.

No specific recommendations are provided for hardening the OpenStack Image Service as deployed for Cisco Modeling Labs.

# OpenStack Identity Service Security

The Keystone OpenStack Identity Service is used to authenticate users. Within Cisco Modeling Labs, user authentication is performed on the server, rather than by LDAP or other external methods.

Perform these tasks for identity service security when user authentication is performed on the server:

- Monitor logs for activity that indicate brute-force attacks. You can perform the monitoring manually, or use a third-party product.

- Register internal endpoints. By registering an internal URL as an endpoint, API communications are restricted, which increases security. Refer to the *OpenStack Security Guide*, which is available at http://docs.openstack.org/security-guide/
- Each OpenStack service has a policy file called **policy.json** that specifies the rules that govern each resource.

# OpenStack Database Security

All information in a .virl network topology file is maintained in a database that is managed within the OpenStack compute component. The information includes the names of nodes and their connections, and the initial node configurations. User names and project names are also included. Passwords are not the same for projects added through the User Workspace Management interface.