Sun Blade 6000 Virtualized 40 GbE Network Express Module

Security Guide

September 2011

Part No.: E24668-01

Author: Tanli Chang
Contributor: Ajoy Siddabathuni

This document provides guidelines for securing the Sun Blade 6000 Virtualized 40 GbE Network Express Module and systems assisted with it.

Contents

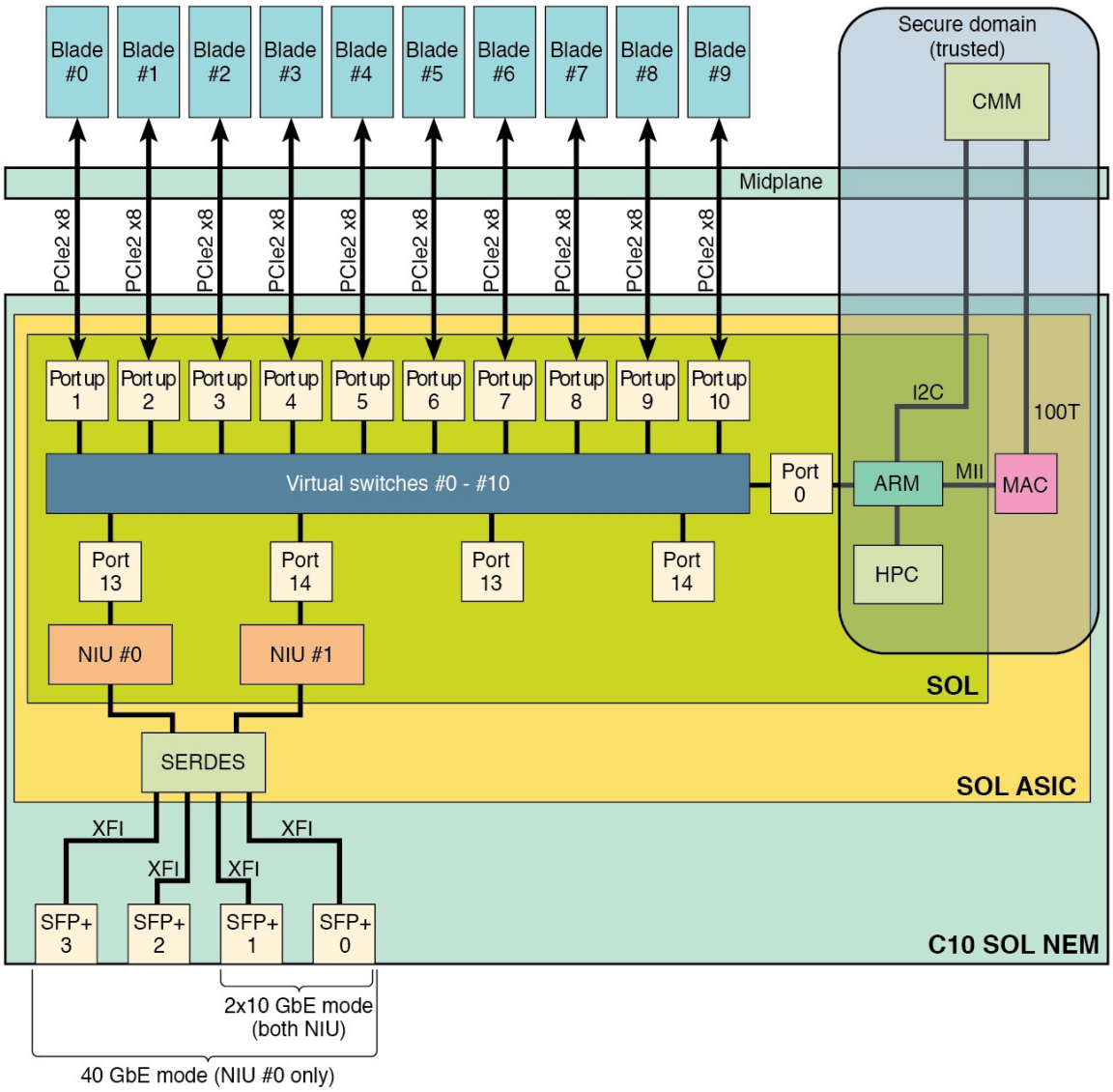
Table of Contents

Part 1: Overview

This section provides an overview of the product and explains the general principles of security.

Product Overview

Oracle's Sun Blade 6000 Virtualized 40 GbE Network Express Module (NEM) is a multi-purpose connectivity module for the Sun Blade 6000 modular system. The NEM provides network and storage connectivity between the blades in a Sun Blade 6000 modular system chassis and external devices. The NEM supports connection to external devices through 40 GbE small form-factor pluggable (SFP+) ports and 10/100/1000 TPE ports. Also, the NEM supports Sun ASIC Dual 10GbE Network Interface Card (NIC) virtualization.



The system diagram shows the general system security domains. The chassis management module (CMM) and NEM-EPS firmware are part of the secure domain. Only system administrators are allowed to access the CMM externally. The blades are connected to the Virtualized NICs via the PCI-E spigots.

It is important to understand that having access to the blades does not compromise the security of the NEM in general. The NEM is designed to run under a variety of operating systems (including VMs) on the blades and in general blades are protected from each other. Blades do not have direct access to the NEM-EPS firmware.

All policies that need to be set up in the NEM are only accessible via the CMM. Following are some of the policies that can be set up via the NEM-EPS only with access to the CMM:

- Bandwidth allocation
- VLAN membership
- SRIOV modes
- Promiscuous mode
- Link management
- Trunking/Link aggregation management
- Logging information
- NEM configuration
- Firmware/EEPROM upgrades

General Security Principles

The following principles are fundamental to using any NEM securely.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. The list of software is as follows:

- Solaris sxge driver
- Linux sxge/sxgevf driver
- VMWare and Windows drivers

The following software components are only accessible to system administrators having access to the CMM.

- NEM firmware
- EEPROM image

Monitor System Activity

1. CMM has message log to log system activity. NEM firmware upgrade activity will be included in system log.
2. The sxge driver has support for:
    - kstat, netstat, dladm, pcitool, ethtool
    - log/message (can be turned on or off)

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check product release notes often for updates.

Sun Blade 6000 Virtualized 40 GbE Network Express Module Product Notes

Part 2: Secure Installation and Configuration

Installation Overview

The NEM is shipped with all firmware installed. It does not require any installation or configuration. All software update components such as patches and new firmware releases must be downloaded from Oracle web download site after logging in using service contract information and credentials.

Note that NEM-EPS firmware is only upgradeable via the CMM.

To install new firmware and drivers, refer to:

Sun Blade 6000 Virtualized 40 GbE Network Express Module Product Notes

Installing Firmware

For detailed instructions, refer to:

Sun Blade 6000 Virtualized 40 GbE Network Express Module User's Guide

Installing Drivers

Please refer to:

Sun Blade 6000 Virtualized 40 GbE Network Express Module User's Guide

Part 3: Security Features

Users cannot access NEM directly. All the requests are by proxy through the CMM ILOM.

AAA

The critical security features provided by ILOM are as follows:

- Authentication: ensuring that only authorized individuals get access to the system and data.
- Authorization: access control to system privileges and data. This builds on authentication to ensure that individuals only get appropriate access.
- Audit: allows administrators to detect attempted breaches of the authentication mechanisms and attempted or successful breaches of access control.

ILOM information is located in the *Oracle Integrated Lights Out Manager 3.0* documentation collection at:

Integrated Lights Out Manager (ILOM) 3.0

NEM security features are only accessible via the CMM ILOM.

Bandwidth Allocation

Each blade is initially allocated 10% bandwidth per port. Administrators who have access to NEM-EPS (through CMM) can change the settings. Any excess bandwidth is available to blades as best effort.

VLAN Membership

VLAN memberships are only managed via the NEM-EPS (via CMM). Blades that are not part of a VLAN will not receive packets on that VLAN-ID.

SRIOV Modes

PCI functions visible from the blade (per port) are configured via the NEM-EPS. Only blades set up to be in SR-IOV mode can run VFs and VMs to share the Virtualized-IO domains per port.

Promiscuous Mode

Blades can be allowed to see all traffic from the network ports only if configured on the NEM-EPS

Link Management

Blades can be forced to see a Virtualized NIC as up, down, or auto (auto being the actual physical link status).

Trunking/Link Aggregation Management

Trunking/Link aggregation is having the ability to see both ports on the NEM as one logical trunk (for load sharing and failover purposes). These capabilities can only be set up via the NEM-EPS.

Logging Information

All logging information is only available via the NEM-EPS

NEM Configuration

Custom configurations can be saved, and settings can be reset to factory defaults.

Firmware/EEPROM Upgrades

Upgrades are only allowed via the CMM.

For more information refer to:

Sun Blade 6000 Virtualized 40 GbE Network Express Module User's Guide

Part 4: Security Considerations for Developers

All software and firmware running on Oracle's Sun Blade 6000 Virtualized Network Express Module (NEM) are provided by Oracle. Customers cannot develop their own software to run on the NEM.