ERICSSON

System Hardening Guideline

Cloud Execution Environment

USER GUIDE

2/1553-CRA 119 1864/5 Uen C

Contents

1 Introduction

This user guide contains general information about the hardening processes, and helps to understand the purpose of product hardening. The document gives an overview of the hardening activities that are performed during the product development, and defines hardening activities that need to be performed during and after the installation.

The first and one of the most important step of hardening is to understand the security risks threatening the system. Therefore these threats, the probability of them happening, and the impact on the Cloud Execution Environment (CEE) must be identified. Based of the likelihood and impact, the risk of the vulnerabilities are determined. If some risks are assessed as non-acceptable, controls must be applied to mitigate those risks. This document collects the available controls to mitigate the risk.

Attention!

Hardening is not an optional feature or function. Assessment of the security risks in an operational environment must be performed according to the ISO 27011 standard, refer to Section 4.2.4.2 of the ISO27011 documentation, Reference [1]. If the result of the assessment contains some acceptable risks, the corresponding control mitigating the non-important risk may not be applied, refer to Section 4.2.4.3 of the ISO27011 documentation, Reference [1]. The owner or the responsible of the CEE must assess the risks to have clear responsibility and accountability, refer to Section 6.1.1 of the ISO27011 documentation, Reference [1].
Use the *CEE Hardening Checklist* to collect the result of the assessment and based on that perform the required steps.

For more information on how to manage information security in telecommunications organizations, refer to ISO 27011, Reference [1].

1.1 Purpose

The purpose of this document is to describe the hardening procedures and available controls of CEE.

1.2 Scope

This user guide provides a high-level overview of the security of CEE, enumerates the hardening areas, provides detailed background information about the required hardening steps and the required command to perform them.

The hardening procedures of the Extreme switch, EMC VNX, and the Data Center Firewall (DCFW) are out of the scope of this document.

1.3 Target Groups

This document is primarily intended to be used by the staff responsible for CEE. This includes operational personnel performing installing, updating, or maintaining activities. Furthermore, security administrators managing security and IT and Telecom (security) operational managers responsible for Information Security Management Systems (ISMS) according to section 6.1.1 in the ISO 27011 standard, Reference [1] and section 6.1.1 b) in ISO 27002 standard, Reference [2].

1.4 Prerequisites

This section states the prerequisites that have to be fulfilled.

1.4.1 Required Competence

The following sections describe the required competences for operational personnel and decision makers.

1.4.1.1 Operational Personnel

It is required for operational personnel, performing the installing, updating, or maintaining activities to understand the security concepts before handling security. For that reason, the intended audience of the document must be skilled in security and have at least CISSP certificates or equivalent. Furthermore, deep domain knowledge on Cloud and security is required, especially on those components on which the hardening steps are to be performed. The security topics are, for example, cryptography, secure protocols (IPSec, TLS, SSH, and so on), security architecture, security operations management, firewall configuration, key management, security log analysis, user management, web server security, certificate management, OpenStack, Linux, LDAP and SNMP protocols.

1.4.1.2 Decision Makers

It is required for the decision makers, who identify operational risks and decide required controls, such as security administrators managing security and IT, and Telecom (security) operational managers responsible for Information Security Management System (ISMS), that they understand the security concepts before taking responsibility and making decisions. At least CISSP, CISM, and ISO27001 lead auditor certificates or equivalent are required. Furthermore, deep domain knowledge on Cloud and security is required, especially on those components on which the hardening steps are to be performed. The security topics are, for example, cryptography, secure protocols (IPSec, TLS, SSH,

and so on), security architecture, security operations management, firewall configuration, key management, security log analysis, user management, web server security, certificate management, OpenStack, Linux, LDAP and SNMP protocols.

1.4.2 Documents

Ensure that the following documents have been read:

- *CEE Hardening Checklist*
- *Security User Guide*
- *Infrastructure Administrator Management Guide*
- *DC Firewall Hardening Guide*

2 General

The following sections give a general overview of the system from a security point of view and define the main hardening areas.

2.1 System Overview

An overview of the security services is shown in Figure 1.

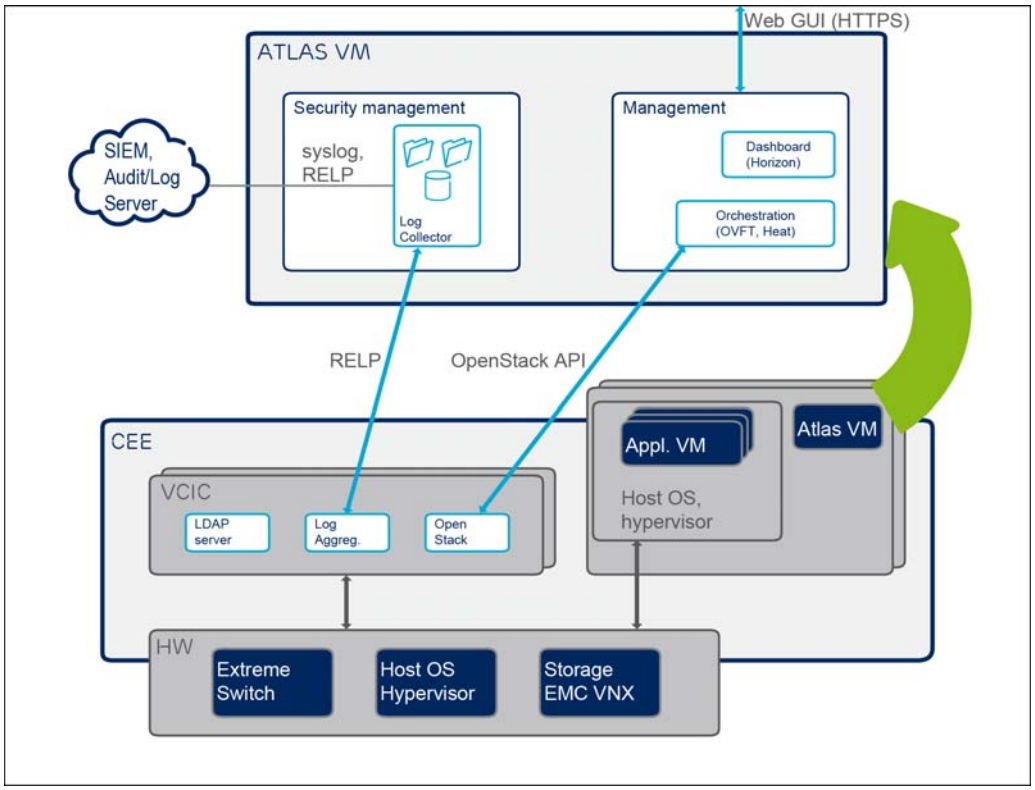

Figure 1 Current Security Solution

Note: The security service overview shown in Figure 1 is only valid if EMC VNX storage solution is used. EMC VNX and EMC ScaleIO are mutually exclusive.

For an overview of the system, refer to *CEE Technical Description*.

For an overview of the DCFW solution, refer to *DC Firewall Hardening Guide*.

2.2 Hardening Areas

The following hardening areas are defined:

Identity and Access Management

Credentials management includes the handling of infrastructure and OpenStack credentials, and the adherence to the password policies.

Prehardening of System Components

The prehardening of the system components ensures that only the required services are enabled on the Atlas management node, the Compute hosts, the Cloud Infrastructure Controller (CIC) hosts, the VNX storage array, Extreme switches, and on the Fuel node.

Allowed Traffic Flows Through the DC Firewall between Security Domains

The configuration of the DCFW is defined in a way to enable only the allowed traffic flows between the various Security Domains.

Certificate Management for the Northbound Interface

Managing the certificates for the northbound interface.

3 Hardening Activities

This section presents the various hardening activities that take place before, during, and after the installation and integration.

Note: If any of these hardening activities are not performed, the security of the system is degraded.

3.1 Hardening Before Installation and Integration

This section contains information about the hardening activities that are performed before the installation and integration of the system.

3.1.1 System and Initial User Accounts

The initial administrator and system account credentials that are created during the system installation are shown in Table 1.

Table 1 Initial Administrator and System Account Credentials

Username	Where	Type	Initial Password and Public Key Set	Password Access Allowed (1)	Place of Use	Allowed Human Interface
ceeadm	vCIC, Compute, vFuel	Linux	Initial factory password; initial public key is generated at installation time.	Yes	Initial non-root administrator account for example for the following: • Update • LDAP accou nt	SSH, console access
ceebackup	vCIC, vFuel	Linux	Initial factory password; initial public key is generated at installation time.	Yes	Backup and restore processes	SSH, console access
ceecore	vCIC	Linux	Initial password for login locked by default, initial public key is generated at installation time.	No	Crash and core manag ement	System account, not for human operation
cmha	vCIC, Compute, vFuel	Linux	Initial password for login locked by default, initial public key is generated at installation time.	No	System account, not for login.	System account, not for human operation
Service user accounts, for example nova and slapd in `/etc/shadow`	vCIC, Compute (slapd), vFuel (no OpenStack users)	Linux	No passwords, some of them have public keys if communication is required.	No	Running system daem ons, system account, not used for login.	System account s, not for human operation

Table 1 Initial Administrator and System Account Credentials

Username	Where	Type	Initial Password and Public Key Set	Password Access Allowed (1)	Place of Use	Allowed Human Interface
root	vFuel	Linux	Initial factory password	Yes	Manage CIC, Compute, Fuel	SSH, console access
root	vCIC, Compute	Linux	Initial factory password, public key based login available only from Fuel.	Yes, but console only access (no SSH)	Mainly for Fuel to manage CIC and Compute	Console access (no SSH)
root	Atlas VM	Linux	No public key based authentication.	No	System account, not for login.	System account, not for human operation
atlasadm	Atlas VM	Linux	Initial password to log into Atlas, no public key based authentication by default.	Yes	Initial account in Atlas VM.	SSH
admin	vCIC, Host, Atlas	OpenStack	Initial factory passwords, no public keys.	Yes	OpenStack management	Atlas dashboard, OpenStack CLI (restful interfaces)
Service accounts within OpenStack.	vCIC, Compute	OpenStack	Randomly generated passwords during installation.	No	System accounts	System account s, not for human operation.

(1) The value of this field is "YES" in case it is a human access account. The value is "NO", if it is a system account.

Note: All these credentials are mandatory for the system to function correctly.

There are different kind of credentials in the system for machine to machine and for human intended usage. All machine to machine passwords are updated or randomly generated during the time of the deployment in order to avoid well-known passwords that would cause privilege escalation and security issues.

3.1.2 Prehardened System Components

The following components are subject to prehardening in the system:

- Compute HW
- Compute OS
- CIC OS
- Atlas OS
- Fuel OS
- Extreme switches
- EMC VNX storage

- EMC ScaleIO storage

Note: EMC VNX storage solution and EMC ScaleIO storage solution are mutually exclusive.

3.1.2.1 Compute HW Hardening

The compute hardware equipment is prehardened by the original vendor. For more information refer to the documentation of the manufacturer.

3.1.2.2 Compute OS Hardening

The Compute host uses Ubuntu 14.04 Linux, and is, for most parts, prehardened.

All services that are running on the Compute host after installation are required, and must not be disabled.

All available but unnecessary services and ports have already been disabled.

For a list of the Compute host ports and services, refer to the *Security User Guide*.

For the Compute host, only Secure Shell (SSH) version two (SSH-2) is allowed as a network access protocol.

3.1.2.3 CIC OS Hardening

The CIC hosts use Ubuntu 14.04 Linux, and are, for most parts, prehardened.

All services that are running on the CIC host OS after installation are required, and must not be disabled.

All available but unnecessary services and ports have already been disabled.

For a list of the CIC ports and services, refer to the *Security User Guide*.

For the CIC, only SSH-2 is allowed as a network access protocol.

3.1.2.4 Atlas OS Hardening

The Atlas host uses Ubuntu 14.04 Linux, and is, for most parts, prehardened.

All services that are running on Atlas after installation are required, and must not be disabled.

All available but unnecessary services and ports have already been disabled.

For a list of the Atlas ports and services, refer to the *Security User Guide*.

For Atlas, only SSH-2 is allowed as a network access protocol.

3.1.2.5 Fuel OS Hardening

The Fuel node uses CentOS, and is, for most parts, prehardened.

All services that are running on the Fuel node after installation are required, and must not be disabled.

All available but unnecessary services and ports have already been disabled.

For a list of the Fuel ports and services, refer to the *Security User Guide*.

For the Fuel, only Secure Shell (SSH) version two (SSH-2) is allowed as a network access protocol.

3.1.2.6 Extreme Switch Hardening

The Extreme switches are prehardened by Extreme Networks.

3.1.2.7 EMC VNX Storage Hardening

Note: This section is only applicable if EMC VNX storage solution is used.

The VNX storage solution is prehardened by EMC. For more information refer to *Security Configuration for VNX* on the EMC documentation web page, Reference [3].

3.1.2.8 EMC ScaleIO Storage Hardening

Note: This section is only applicable if EMC ScaleIO storage is used.

The ScaleIO storage solution is prehardened by EMC. For more information refer to *ScaleIO Security Configuration Guide*, Reference [4].

3.2 Hardening During Installation and Integration

This section contains information about the hardening activities that are performed during the installation and integration.

3.2.1 Initial Administrator Credentials

The initial credentials for all of the predefined local administrators are configured in `config.yaml` during the system installation. The default passwords for the following human access accounts must be changed before installing the system, or immediately after the system deployment:

- `ceeadm`, for more information, see Section 3.4.5 on page 17.
- `ceebackup`, for more information, see Section 3.4.5 on page 17.

- `root` user for Fuel, for more information, see Section 3.4.5 on page 17.
- `root` user for CIC host and Compute host, for more information, see Section 3.4.3 on page 16.
- `atlasadm`, for more information, see Section 3.4.4 on page 17.
- `admin`, for more information, see Section 3.4.6 on page 18.

For detailed instructions on how to manage administrator passwords, refer to the *Infrastructure Administrator Management Guide* and the *Security User Guide*.

3.2.2 DCFW Configuration

In the current system, the DCFW is located outside the Cloud Execution Environment (CEE).

The DCFW provides protection for the system, and also acts as an O&M firewall.

The DCFW is used to enforce access control between Security Domains.

In the DC FW two logical firewall instance types can be defined, one is responsible for controlling the CEE management traffic, another is responsible for the protection of the tenant.

The Security Domains, and their relations are shown in Figure 2. The O&M-FW is a logical instance in the DCFW. Tenant firewall is another logical instance in the DCFW, that protects the data center from external attacks, by performing basic screening of tenant traffic.

Settings of the tenant firewall is out of the scope of this document, as the exact settings depend on the security expectations of the tenant. The tenant traffic must not be mixed with the O&M traffic.

At the perimeter of CEE, a BGW and DCFW protects the internals of the CEE. For more information refer to the *DC Firewall Hardening Guide*.

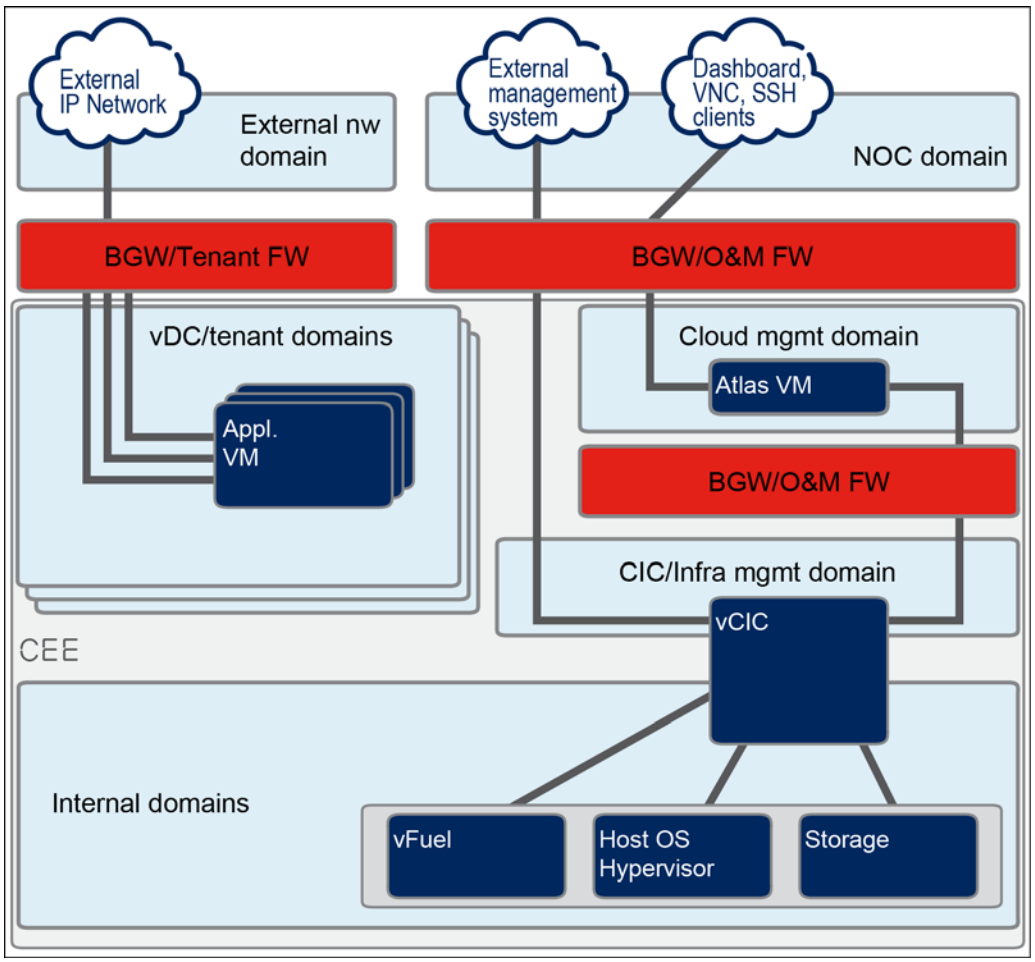

Figure 2 Security Domains

For the logical configuration of the O&M-FW during the installation (grouped by outbound direction), use Table 2, Table 3, and Table 4 as references.

Table 2 Traffic Flows from the NOC Domain

Source			Destination			Service		
Security Domain	**Address**	**Port**	**Security Domain**	**Address**	**Port**	**Proto**	**Application**	**Information**
NOC	Admin Clients	Any	Cloud management domain	Atlas Northbound	443	TCP	HTTPS	Atlas Horizon service
NOC	Admin Clients	Any	CIC/infra management domain	CIC Northbound Public IP	5900: 6100	TCP	HTTPS	VNC Console Address

Table 2 Traffic Flows from the NOC Domain

Source			Destination			Service		
Security Domain	**Address**	**Port**	**Security Domain**	**Address**	**Port**	**Proto**	**Application**	**Information**
NOC	Admin/browser	Any	CIC/infra management domain	CIC Northbound Public IP	8774	TCP		Nova
					8775			Nova
					8776			Cinder
					6080			Nova
					10080 (1)		HTTPS	EMC VNX
					10443 (1)		HTTPS	EMC VNX
					20080 (1)		HTTP	EMC VNX
					20443 (1)		HTTPS	EMC VNX

(1) Assuming that NAT is done before filtering. Otherwise, ports are 80/443 and IP addresses are "VNX_SP-A_Public_IP" and "VNX_SP-B_Public_IP". For more information see Section 3.2.3.2 on page 14.

Table 3 Traffic Flows from Cloud Management Domain

Source			Destination			Service		
Security Domain	**Address**	**Port**	**Security Domain**	**Address**	**Port**	**Proto**	**Application**	**Information**
Cloud management domain	Atlas Southbound	Any	CIC/infra management domain	CIC Northbound Public IP	22	TCP	SSH SCP, SFTP	Non-REST API access to the CIC
Cloud management domain	Admin/browser	Any	CIC/infra management domain	CIC Northbound Public IP	5900:6100	TCP	HTTPS	OpenStack VNC support
Cloud management domain	Cloud Management System	Any	CIC/infra management domain	CIC HA-proxy	5000	TCP	HTTPS	Keystone-1
					6080			Nova-novncproxy
					8052			Watchmen
					8054			Watchmen
					8080			Swift
					8773			Nova-1
					8774			Nova-2
					8776		HTTPS	Cinder
					8777			Ceilometer
					9292			Glance
					9696			Neutron
					35357			Keystone-2
					30165	UDP	SNMP	Watchmen

Table 3 Traffic Flows from Cloud Management Domain

Source			Destination			Service		
Security Domain	**Address**	**Port**	**Security Domain**	**Address**	**Port**	**Proto**	**Application**	**Information**
Cloud management domain	Browser/Client	Any	Cloud management domain	Atlas Southbound	8888	TCP	HTTPS	ovtf API
					8004			heat API
					8003			heat API cloudwatch
					8000			heat API cnf

Table 4 Traffic Flows from CIC/Infra Management Domain

Source			Destination			Service		
Security Domain	**Address**	**Port**	**Security Domain**	**Address**	**Port**	**Proto**	**Application**	**Information**
CIC/infra management domain	CIC public API address	Log aggregator	Cloud management domain	Atlas Southbound	20514	TCP	RELP	Log collector in Atlas
CIC/infra management domain	Browser/Client	Any	Cloud management domain	Atlas Southbound	8053	TCP	HTTPS	watchmen history API
CIC/infra management domain	CIC public API address	NMS Server	NOC	NOC	162	UDP	SNMP v2	FM:SNMP traps
CIC/infra management domain	Extreme Switch	123	NOC	NOC	123	UDP	ntp	ntp-server in NOC time server

For more information about how to set the rules in DC Firewall, refer to *DC Firewall Hardening Guide*.

3.2.3 Management Access of VNX from the Providers Management Network

Note: This section is only applicable if EMC VNX storage solution is used.

Apart from security policies in the DCFW, to allow VNX Management traffic to pass between security domains, the connectivity of VNX Management Tools and the VNX Management Server relies on two Network Address and Port Translation (NAPT) rule sets. The first set must be applied outside the CEE in the DCFW, and the second set is defined in the CIC hosts.

3.2.3.1 VNX Management Tools

Table 5 lists the Unisphere client components and the ports that are used for communication with the Unisphere Management Server, which resides in the VNX.

Table 5 VNX Management Tools

Tool	Port	Protocol	Functionality
naviseccli	443	TCP/SSL	Basic management, command line-based
Unisphere (Java applet)	80/443	HTTP/SSL	Basic management, GUI based
Unisphere Service Manager (USM)	443	TCP/SSL	Service tasks, Windows-based

3.2.3.2 VNX Management Tools to Management Server Connectivity

VNX management access requires two public IP addresses, denoted as "VNX_SP-A_Public_IP" and "VNX_SP-B_Public_IP", in order to reach the local IP addresses of the two Support Processors ("VNX SP-A" and "VNX SP-B" respectively) of the EMC VNX storage system individually.

The traffic flow is shown in Figure 3. The O&M-FW is an instance in the DCFW.

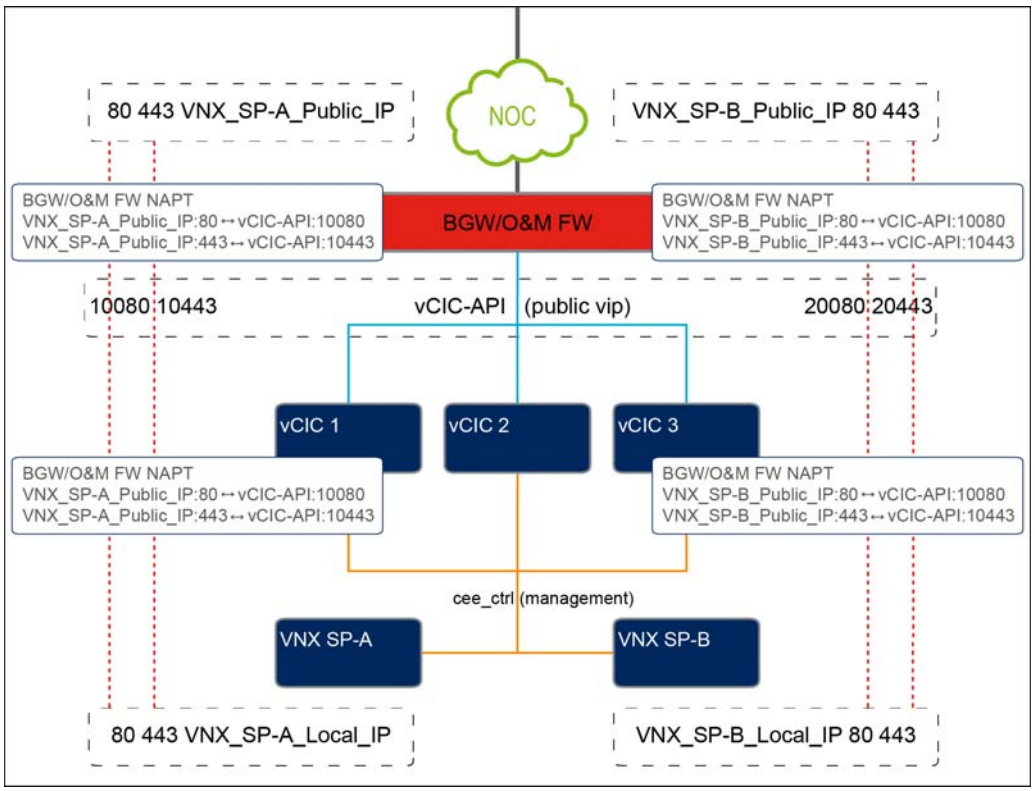

Figure 3 Network Address and Port Translation in the DCFW and the CIC Hosts

When an engineer from a Network Operations Center (NOC) initiates a connection to one of the VNX SPs, first the DCFW handles the network address and port translations after a successful authentication and authorization. The translated network address is then forwarded to one of the CIC hosts, where a second network address and port translation occurs to the SPs local address.

The destination network address and port translation rules, which must be applied in the DCFW, are shown in Table 6.

Table 6 Destination Network Address and Port Translation in DCFW

Destination IP	Destination Port	Translated to IP	Translated to Port
VNX_SP-A_Public_IP	80	CIC-API (public_vip)	10080
	443		10443
VNX_SP-B_Public_IP	80		20080
	443		20443

The destination network address and port translation rules, which are automatically configured in the CIC hosts, are shown in Table 7.

Table 7 Destination Network Address and Port Translation in the CIC Hosts

Destination IP	Destination Port	Translated to IP	Translated to Port
CIC-API (public_vip)	10080	VNX_SP-A_Local_IP	80
	10443		443
	20080	VNX_SP-B_Local_IP	80
	20443		443

3.3 ScaleIO Management Tools

Note: This section is only applicable if EMC ScaleIO storage solution is used.

The EMC ScaleIO GUI requires the MDM IP address.

3.4 Product Security Maintenance After Installation and Integration

This section contains information about the hardening activities that are performed after the installation and integration.

3.4.1 Administrator Credentials

This section describes the management of administrator credentials.

3.4.1.1 Changing the Password for the Predefined Administrator Credentials

The passwords for the predefined administrator credentials must be changed on a regular basis.

For the detailed procedure of managing the following predefined administrator credentials, and for the procedure of changing the passwords, refer to the *Infrastructure Administrator Management Guide* and the *Security User Guide*:

- `ceeadm`, for more information see Section 3.4.5 on page 17.
- `ceebackup`, for more information see Section 3.4.5 on page 17.
- `root` user for Fuel, for more information see Section 3.4.5 on page 17.
- `root` user for CIC host and Compute host, for more information see Section 3.4.3 on page 16.
- `atlasadm`, for more information see Section 3.4.4 on page 17.
- `admin`, for more information see Section 3.4.6 on page 18.

The passwords must fulfill the strong password conditions. For the strong password conditions, see Section 4 on page 20, or refer to your local company policy for defining strong passwords.

3.4.1.2 Changing the Password for the Operator Defined Administrator Credentials

It is strongly advised to regularly change the administrator passwords of the credentials that are defined by the operator in the system.

For detailed instructions on how to manage administrator passwords, refer to the *Infrastructure Administrator Management Guide* and the *Security User Guide*.

3.4.2 Creating Additional Credentials

During the first startup of the system, only the default administrator credentials are available. In addition to those credentials, each system administrator must use individual personal user accounts when logging in. The use of shared accounts is not recommended. For the CIC hosts, the Compute host, the storage solution, and for the Extreme switches, individual user accounts are provisioned in the LDAP server. For Atlas, user accounts are local.

For more information about credentials management, refer to *Infrastructure Administrator Management Guide*.

3.4.3 CIC Host OS Hardening

After the installation, the `root` password must be changed. For the procedure of changing the `root` password, refer to the documents *SW Installation in Multi-Server Deployment* and *SW Installation in Single Server Deployment*.

The `root` access with a password to CIC host is disabled by default, and only administrator accounts defined in the Lightweight Directory Access Protocol (LDAP) can be used for login.

The `ceeadm` account is not to be used for direct login after the administrator accounts in LDAP have been created.

3.4.4 Atlas User Management

For Atlas, user accounts are local. The initial system user, `atlasadm`, with sudo rights is created during the prehardening. The password of the `atlasadm` is set during the installation procedure.

For more information refer to *Atlas SW Installation*.

3.4.5 Fuel User Management

After the initial installation, only the `root` user exists in the Fuel server. The CEE deployment adds the `ceeadm`, `cmha`, and `ceebackup` users to the Fuel server.

It is possible to use the `ceeadm` user to access the Fuel server for creating the initial personal accounts. After that, the `ceeadm` user must only be used by infrastructure components, and during update and rollback.

It is recommended to create additional local Linux user accounts to the Fuel server for personnel administering the system.

It is possible to disable predefined users after the access is available with additional users, with the following command:

```
usermod -e 1 <username>
```

It is possible that `root` access is required during system update and expansion. In such cases, the `root` account must be enabled with the following command:

```
usermod -e "" root
```

Once the activities that require the `root` access have been completed, it is recommended to lock the account again.

The passwords for all Fuel administrators must be changed by using the **`passwd`** command on a regular basis.

It is possible to configure users with password expiry. Enter **`passwd -?`** for the available options.

3.4.6 Extreme Switch User Management

The Extreme switch default user account is defined as `admin` without a password defined. After the successful deployment of the system, it is recommended to change the password for the local `admin` user in the Extreme switch.

By default, CEE installation creates a user defined in the `config.yaml` system configuration, which is used by system components, such as OpenStack Neutron, for accessing and configuring the switch. This user must not be modified at runtime.

For managing the local switch accounts, refer to the Extreme EXOS documentation.

3.4.7 VNX User Management

Note: This section is only applicable if EMC VNX storage solution is used.

For more information about VNX user management, refer to the ‘‘VNX User Management’’ section of *Security User Guide*.

By default, CEE installation creates a user defined in the `config.yaml` system configuration, which is used by system components, such as OpenStack Neutron, for accessing and configuring the EMC VNX. This user must not be modified at runtime.

3.4.8 ScaleIO Access Control

Note: This section is only applicable if EMC ScaleIO storage solution is used.

For more information about ScaleIO user and access management, refer to the ‘‘Access Control Settings’’ section of the *ScaleIO Security Configuration Guide*, Reference [4].

3.4.9 Managing TLS Certificates in CEE

For more information on the necessary certificates and the tasks to perform before installation, refer to the ‘‘Conditions’’ section of the documents *SW Installation in Multi-Server Deployment* and *SW Installation in Single Server Deployment*.

3.4.9.1 Certificates for VNX Services

Note: This section is only applicable if EMC VNX storage solution is used.

Ensure that TLS certificates are available. For more information, refer to *Security Configuration for VNX* on the EMC documentation web page, Reference [3].

3.4.9.2 Certificates for ScaleIO

Note: This section is only applicable if EMC ScaleIO storage solution is used.

Ensure that TLS certificates are available. For more information, refer to the ‘‘Communication Security Settings’’ section of the *ScaleIO Security Configuration Guide*, Reference [4].

4 Strong Password Conditions

In order to set a strong password, the following conditions must be met:

- The length of the password must be at least 12 characters.
- The password must contain at least three of the following:
  - At least one lower-case alphabetic character
  - At least one upper-case alphabetic character
  - At least one numeric character
  - At least one special character
- The password must not contain more than three consecutive instances of the same character class.
- Real names or words must not be used.
- The password must not be the same as the user name.

5 Privacy

A variety of applications could be running on CEE processing the personal data of subscribers, however such data is not known, and cannot be managed by CEE directly. These applications that utilize CEE may affect subscriber privacy. Their impact on privacy is generally to be considered not under the control of CEE.

CEE provides security controls for applications in VMs that process personal data. It is the responsibility of each application to deploy those controls appropriately to protect subscribers personal data and mitigate any possible privacy impact.

Reference List

[1] *ISO27011: Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 ISO/IEC 27011 First edition 2008-12-15, http://www.iso.org*

[2] *ISO27002: Information technology — Security techniques — Code of practice for information security controls ISO/IEC 27002 Second edition 2013-10-01, http://www.iso.org*

[3] *Security Configuration Guide for VNX, https://mydocuments.emc.com/, navigate to "VNX Series", then "Related documentation: VNX for Block OE 5.33 and VNX for File OE 8.1", then "Security Configuration Guide for VNX" under the Security and Compliance section*

[4] *ScaleIO® Security Configuration Guide, http://www.emc.com/collateral/technical-documentation/scaleio-security-configuration-guide.pdf*