ERICSSON

DC Firewall Hardening Guide

Cloud Execution Environment

USER GUIDE

4/1553-CRA 119 1864/5 Uen A

Contents

1 Introduction

This User Guide (UG) provides the connectivity and network description of the Data Center Firewall (DCFW) to the Cloud Execution Environment Network (CEE Network) architecture. In the current system, the Firewall is not part of the CEE Region, therefore this UG gives a high-level overview about the external DCFW solution.

2 Overview

The access to the components of the system can be protected by different Firewall layers. The DCFW provides protection for both system, O&M and tenant traffic.

The general overview of the Firewall solution is shown in Figure 1.

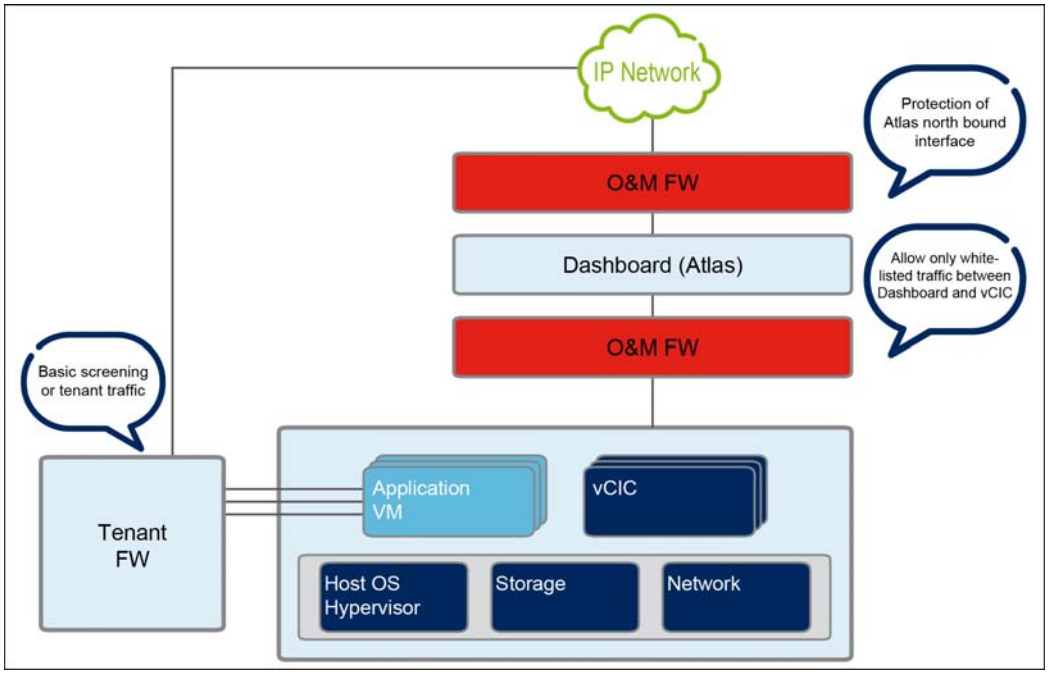

Figure 1 Firewall Solution Overview

2.1 Logical Firewall Types

The following two logical firewall types are protecting the system:

Tenant FW

The Tenant FW protects the DC from external attacks by performing the basic screening of the tenant traffic.

This Firewall typically supports multi-Gbps of traffic.

Cloud O&M FW

The Cloud O&M FW protects the O&M cloud management infrastructure.

The capacity need for this type of Firewall is lower than for the Tenant FW.

2.2 Connectivity

The DCFW is directly connected to the Border Gateway (BGW).

The overview of the BGW and DCFW connectivity is shown in Figure 2.

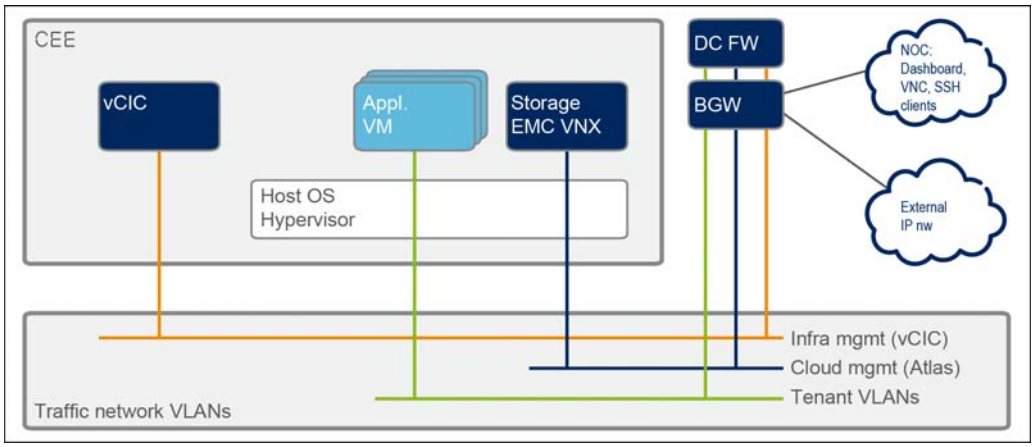

Figure 2 BGW and DCFW Connectivity Overview

The BGW/FW, which provides traffic screening and isolation, is connected to the CEE through the traffic network. This network type is used for external access and tenant data that is carried within the system.

Traffic to and from the system is passed through the BGW and the DCFW. All traffic identified as unwanted, based on security and network policies and rules, is dropped, and the remaining traffic is handled within the security domains defined by the network design.

The detailed BGW DCFW connectivity is shown in Figure 3.

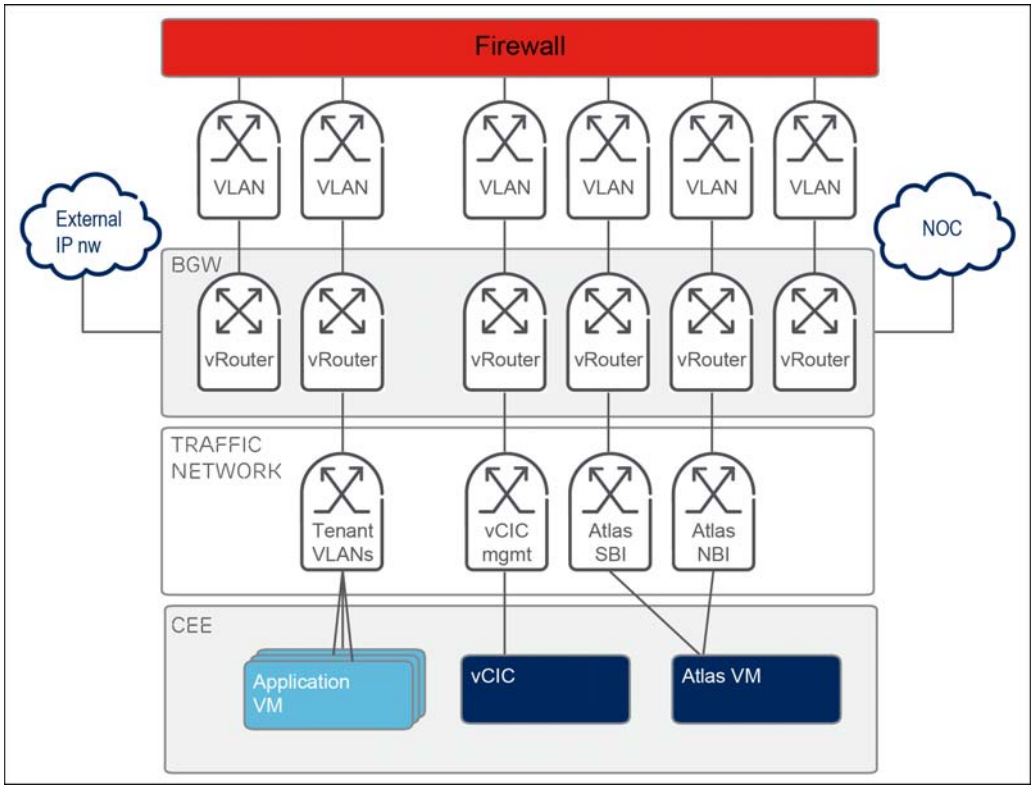

Figure 3 Detailed BGW and DCFW Connectivity

2.3 Security Domains

Access control between the different security domains can be implemented centrally in a BGW and the firewall nodes. By default, no traffic is allowed between any security domain unless specifically configured.

The different network elements are placed in different Security Domains based on their functionality and level of trust. Only legitimate traffic is allowed to pass from one Security Domain to another by enforcing control policies for all traffic between Security Domains. In case the security policy of the operator requires the sub-division of the currently presented Security Domains into multiple smaller zones, it will not contradict the current security architecture.

Figure 4 shows an overview of the recommended minimum set of Security Domains.

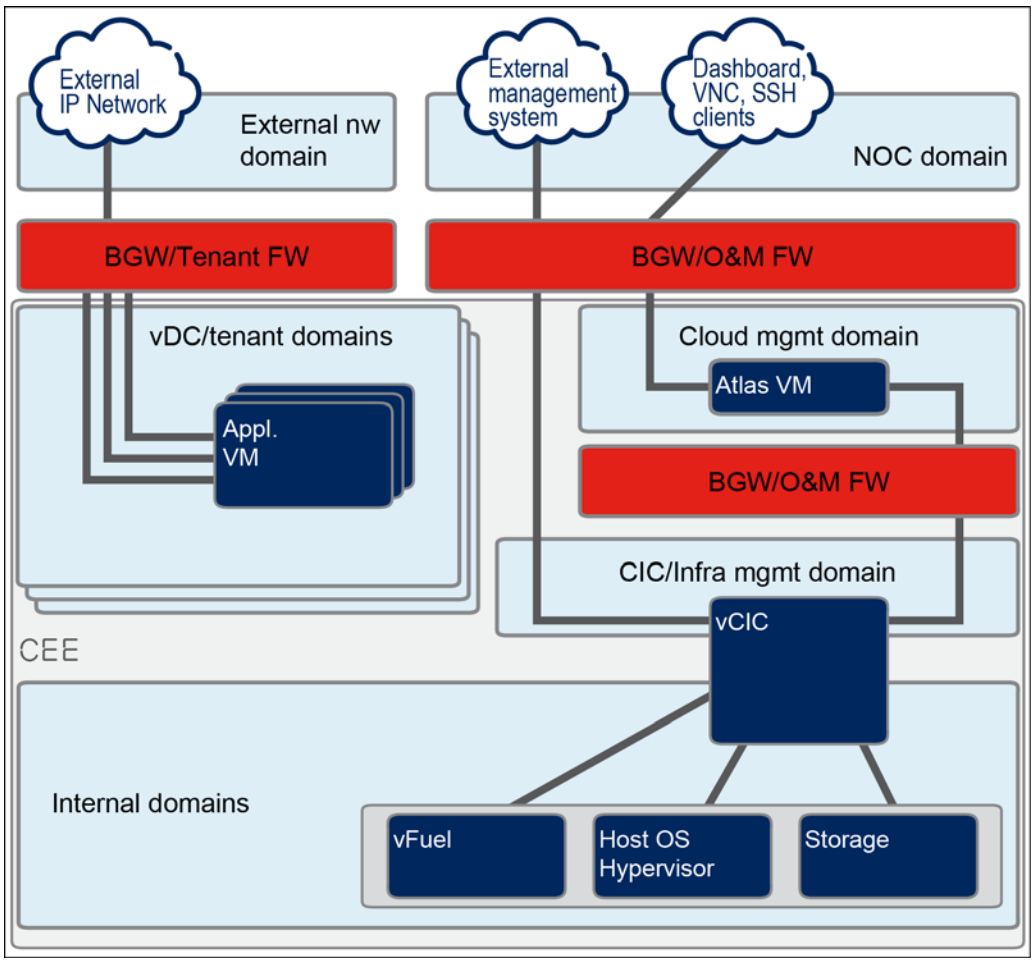

Figure 4 Security Domains

The following Security Domains are identified:

External Network

The domain that includes network to be used between the site and the outside world.

Network Operator Control

The Network Operator Control (NOC) security domain provides connectivity to the cloud operator NOC. This domain includes management traffic to and from the cloud manager and the administration clients.

vDC / tenant Traffic

Tenant VMs are connected to the vDC / tenant security domain instance. The traffic in this domain contains tenant payload traffic to and from external IP networks.

Cloud Management

The Cloud management security domain contains management traffic from NOC to the Atlas VM Northbound Interface (NBI) and from the Atlas VM Southbound Interface (SBI) to the Cloud Infrastructure Controller (CIC) / controller node.

CIC / Infra Management

The CIC / Infra management security domain includes the CIC Servers, and provides access to OpenStack APIs, VM consoles (VNC) and the Linux shell (SSH).

Internal Control

The internal control domain includes those CEE internal nodes (Fuel, Compute node, hypervisors, CIC/Controller node, storage) that are not directly accessible from any external networks.

3 Configuration

This section describes the required configuration of the Hardware Firewall that is needed to enable access control between the different security domains.

3.1 Traffic Flow

For the detailed description of the allowed traffic flows, refer to the ‘‘HW FW Configuration’’ section in *System Hardening Guideline*.

3.2 Perimeter Protection

Traffic to and from the CEE is passed through the BGW and the DCFW. All traffic identified as unwanted, based on security and network policies and rules, is dropped, and the remaining traffic is handled within Security Domains defined by the network design. The BGW/FW providing the traffic screening and isolation is connected to the CEE system through the traffic network.

At the outer perimeter, for example, BGW, access control plays the main role. Basic packet filtering and the protection against ‘‘Denial-of-Service’’ attacks by rate limiting reduce a large amount of unsolicited traffic and flooding-attacks before the packets can enter the next security perimeter of the network. Also, the DC firewall must filter for packets with IP options.

Policing and shaping are techniques used to enforce a maximum bandwidth rate on a traffic stream; while policing effectively does this by dropping out-of-contract traffic, shaping does this by delaying out-of-contract traffic.

The next security perimeter, such as the Firewall, usually focuses on ‘‘smarter’’ security features. Such features are Stateful Inspection, Reconnaissance Deterrence, Deep Packet Inspection, Intrusion Detection and Prevention, Antivirus, Content Filtering, and other security features that can be applied to an in-line security device.

The protection features on the network elements/host nodes themselves, including the Firewall hardening, constitute the last security perimeter. Such features comprise host access control as well as host-based intrusion detection or prevention systems, or both. In addition, all the other basic security features that are already deployed on the outer perimeters can be applied to the inner perimeters, as well.

4 Hardening

This section contains general information about the hardening of the Hardware Firewall.

As a minimum requirement, the hardening of the HW firewall must cover at least the following steps:

- Use a minimal level of privileges for administrators.
- Remove insecure services and plain text protocols such as telnet.
- Enable security features in user system account settings.
- Implement control plane protection, and allow only necessary traffic towards the control plane.
- Enable protocol authentication.
- Enable security features on out of band management interfaces.
- Enable centralized logging.

For general concepts and manufacturer specific syntax, refer to the manufacturer documentation.

For general security policies and allowed traffic flows towards the system, refer to *System Hardening Guideline*.