

DC Firewall Hardening Guide

Cloud Execution Environment

USER GUIDE

Copyright

© Ericsson AB 2016, 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
2	Overview	2
2.1	Logical Firewall Types	2
2.2	Connectivity	3
2.3	Security Domains	4
3	Atlas Firewall Rules	7
4	Configuration	8
4.1	Traffic Flow	8
4.2	Perimeter Protection	8
5	Hardening	9





1 Introduction

This document describes how the Data Center Firewall (DC-FW) is connected to the network architecture of the Cloud Execution Environment (CEE). As the firewall is not part of the CEE region in the current solution, this document can only provide a high-level overview about the external DC-FW solution.

2 Overview

The access to the components of the system can be protected by different firewall layers. The DC-FW provides protection for system, Operation and Maintenance (O&M) and tenant traffic.

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

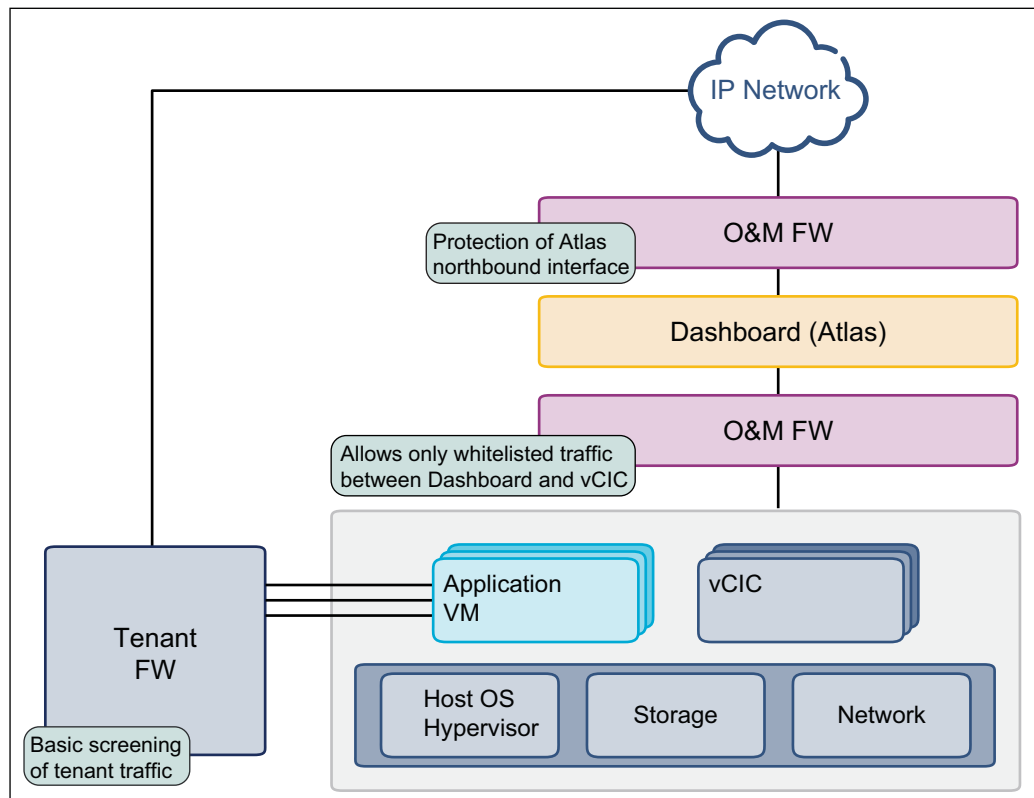


Figure 1 Firewall Solution Overview

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 that of the tenant FW.

2.2

Connectivity

The DC-FW is directly connected to the Data Center Gateway (DC-GW).

The overview of the DC-GW and DC-FW connectivity is shown in Figure 2.

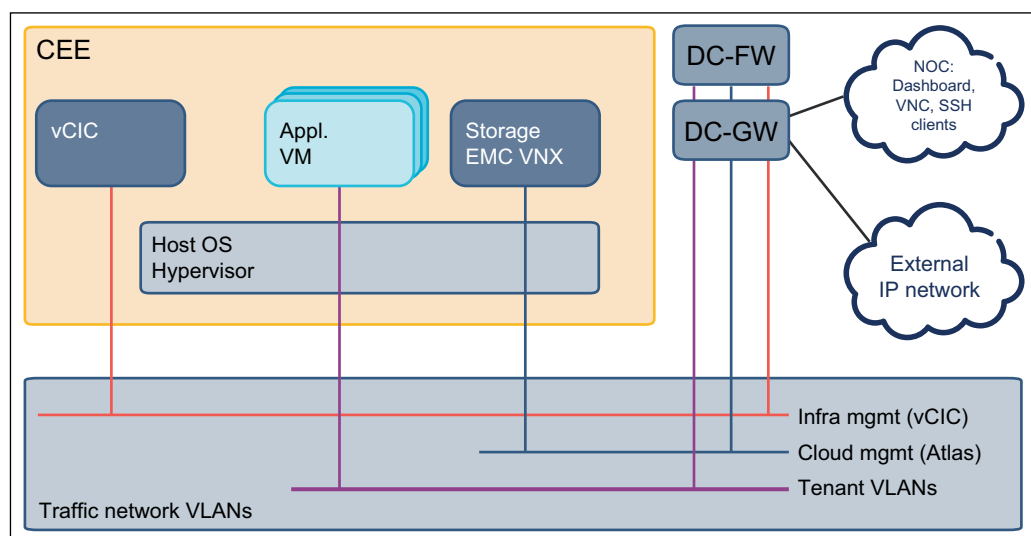


Figure 2 DC-GW and DC-FW Connectivity Overview

Note: The ScaleIO distributed storage component is accessible with GUI or CLI on the public_vip network (port 6611).

DC-GW and DC-FW provide traffic screening and isolation, and are 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 DC-GW and the DC-FW. 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 DC-GW and DC-FW connectivity is shown in Figure 3.

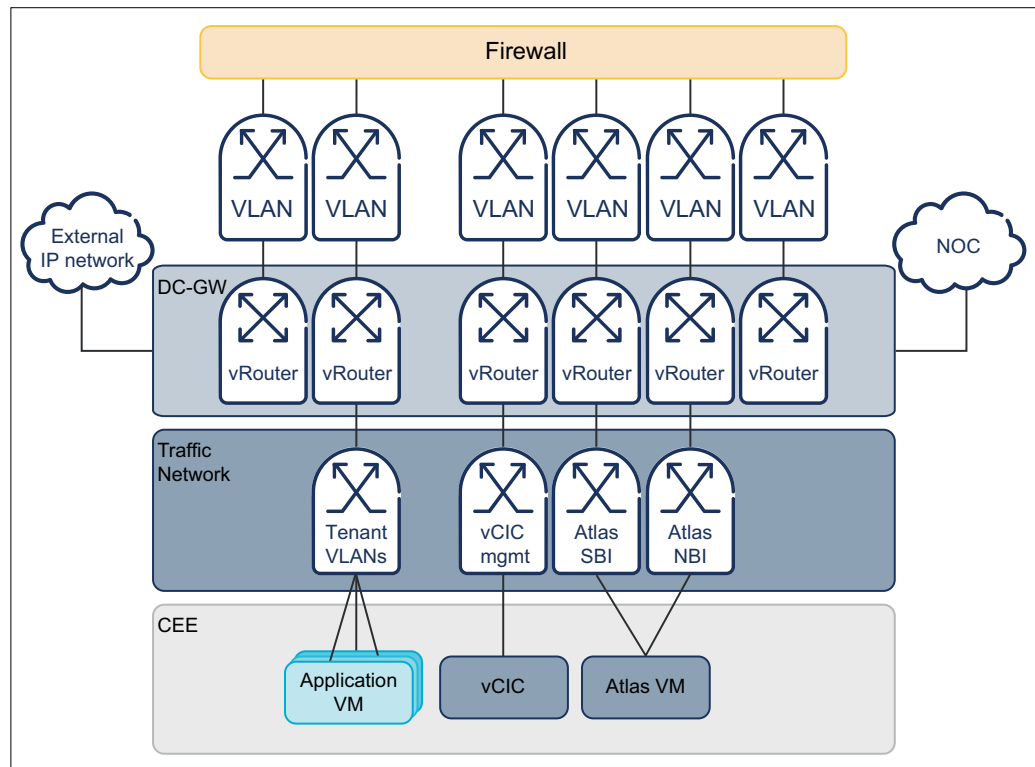


Figure 3 Detailed DC-GW and DC-FW Connectivity

2.3 Security Domains

Access control between the different Security Domains (SDs) can be implemented centrally in a DC-GW and the firewall nodes. By default, no traffic is allowed between any SD unless specifically configured.

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

Figure 4 shows an overview of the recommended minimum set of SDs.

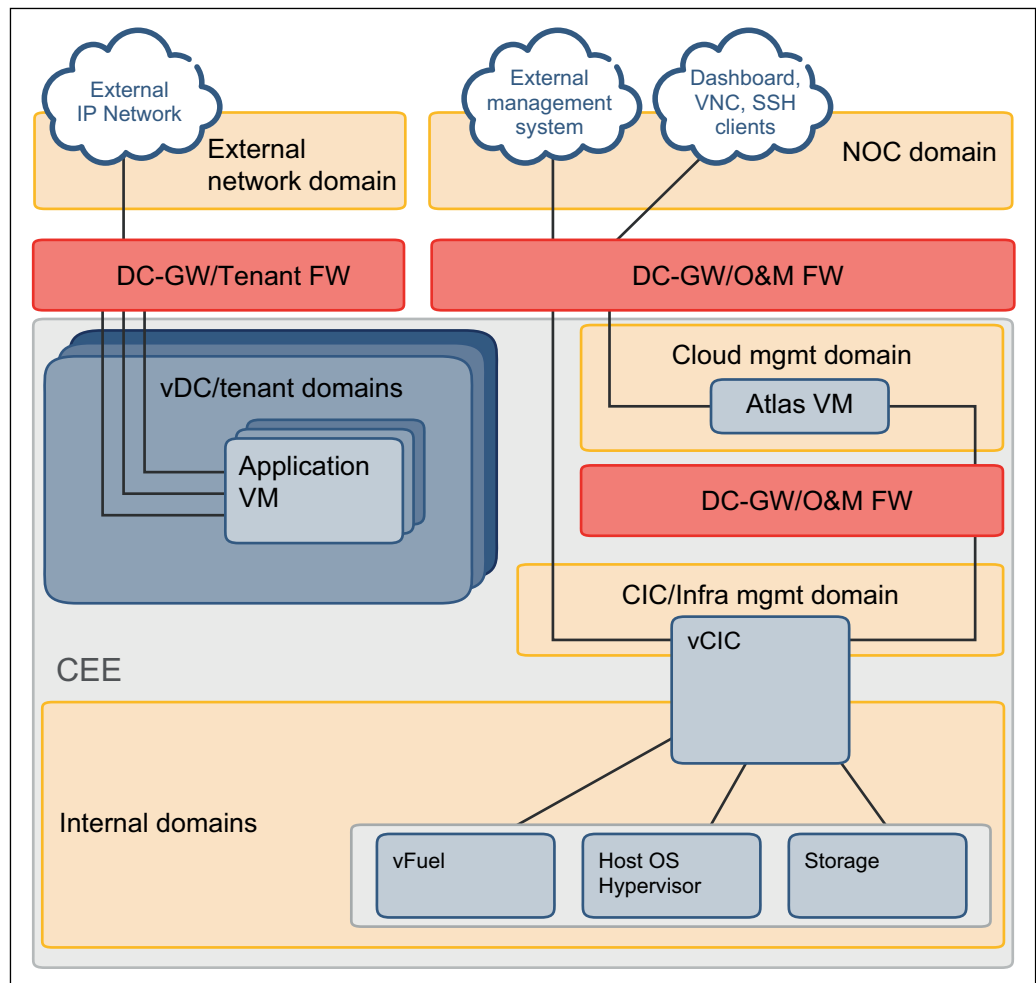


Figure 4 Security Domains

The following SDs are identified:

External network

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

Network Operator Control

The Network Operator Control (NOC) SD 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 SD instance. The traffic in this domain contains tenant payload traffic to and from external IP networks.



Cloud management

The cloud management SD contains management traffic from NOC to the Atlas VM Northbound Interface (NBI) and from the Atlas VM Southbound Interface (SBI) to the virtual Cloud Infrastructure Controller (vCIC) node.

CIC / Infra Management

The CIC / Infra management SD includes the vCIC 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 (vFuel, compute node, hypervisors, vCIC node, storage) that are not directly accessible from any external networks.



3 Atlas Firewall Rules

The iptables rules for Atlas are the following:

Table 1 Atlas Firewall Rules

Protocol	Service	Port	Description	Action
All	All	All	Traffic on loopback interface (127.0.0.1)	ACCEPT
All	All	All	RELATED ⁽¹⁾ and ESTABLISHED ⁽²⁾	ACCEPT
All	All	All	Ping requests	ACCEPT
All	All	22	SSH connections	ACCEPT
TCP	All	80 and 443	HTTP and HTTPS connections	ACCEPT
TCP	RabbitMQ	4369 ⁽³⁾ , 5672 ⁽⁴⁾ , and 15671 ⁽⁵⁾	-	ACCEPT
TCP	OVFT	8888	-	ACCEPT
TCP	heat-api	8004	-	ACCEPT
TCP	heat-api-cfn	8000	-	ACCEPT
TCP	heat-api-cloudwatch	8003	-	ACCEPT
TCP	Mistral	8989	-	ACCEPT
TCP	rsyslogd	20514	-	ACCEPT
All	All	All	Default for packets that are not for the whitelisted ports	DROP

(1) The packet is starting a new connection, but is associated with an existing connection, such as an FTP data transfer, or an ICMP error.

(2) The packet is associated with a connection which has seen packets in both directions.

(3) epmd port

(4) rabbitmq-node port

(5) rabbitmq-management port



4 Configuration

This section describes the required configuration of the hardware firewall (HW FW) that is needed to enable access control between the different SDs.

4.1 Traffic Flow

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

4.2 Perimeter Protection

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

At the outer perimeter, for example, DC-GW, 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-FW 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 and 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.



5 Hardening

This section contains general information about the hardening of the HW FW.

As a minimum requirement, the hardening of the HW FW 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](#).