Security Target

Juniper Networks vGW Series Version 5.5

Document Version 0.5

March 22, 2013

Prepared For:

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

www.juniper.net

Prepared By:

Apex Assurance Group, LLC

530 Lytton Ave, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the vGW Series Version 5.5. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

1 Introduction 6
1.1 ST Reference 6
1.2 TOE Reference 6
1.3 Document Organization 6
1.4 Document Conventions 7
1.5 Document Terminology 7
1.6 TOE Overview 8
1.7 TOE Description 8
1.7.1 Physical Boundary 8
1.7.2 Logical Boundary 10
1.7.3 TOE Product Documentation 10

2 Conformance Claims 12
2.1 CC Conformance Claim 12
2.2 PP Claim 12
2.3 Package Claim 12
2.4 Conformance Rationale 12

3 Security Problem Definition 13
3.1 Threats 13
3.2 Organizational Security Policies 13
3.3 Assumptions 14

4 Security Objectives 15
4.1 Security Objectives for the TOE 15
4.2 Security Objectives for the Operational Environment 15
4.3 Security Objectives Rationale 16
4.3.1 Rationale for Security Threats to the TOE 16

5 Extended Components Definition 19
5.1 Anti-Virus (FAV) Class of SFRs 19
5.1.1 FAV_ACT.1 Anti-Virus Actions 19
5.1.2 FAV_SCN.1 Anti-Virus Scanning 20
5.2 Intrusion Detection (IDS) Class of SFRs 20
5.2.1 IDS_ANL.1 Analyzer Analysis 20
5.3 Extended Security Assurance Components 21

6 Security Requirements 22
6.1 Security Functional Requirements 22
6.1.1 Security Audit (FAU) 22
6.1.2 Information Flow Control (FDP) 24
6.1.3 Identification and Authentication (FIA) 25
6.1.4 Security Management (FMT) 25
6.1.5 Protection of the TSF (FPT) 27
6.1.6 Traffic Analysis (IDS) 27
6.1.7 Anti-Virus (FAV) 28

6.2 Security Assurance Requirements 28
6.3 CC Component Hierarchies and Dependencies 28
6.4 Security Requirements Rationale 29
6.4.1 Security Functional Requirements 29
6.4.2 Sufficiency of Security Requirements 30
6.4.3 Security Assurance Requirements 34
6.4.4 Security Assurance Requirements Rationale 35
6.4.5 Security Assurance Requirements Evidence 35

7 TOE Summary Specification 37
7.1 TOE Security Functions 37
7.2 Security Audit 37
7.3 Information Flow Control 38
7.4 Identification and Authentication 39
7.5 Security Management 39
7.6 Virus Scanning 41
7.7 Traffic Analysis 41

List of Tables

Table 1 – ST Organization and Section Descriptions 6
Table 2 – Acronyms Used in Security Target 7
Table 3 – Evaluated Configuration for the TOE 10
Table 4 – Logical Boundary Descriptions 10
Table 5 – Threats Addressed by the TOE 13
Table 6 – OSP 14
Table 7 – Assumptions 14
Table 8 – TOE Security Objectives 15
Table 9 – Operational Environment Security Objectives 15
Table 10 – Mapping of Assumptions, Threats, and Policies to Security Objectives 16
Table 11 – Mapping of Objectives to Threats 17
Table 12 – Mapping of Threats, Policies, and Assumptions to Objectives 18
Table 13 – TOE Security Functional Requirements 22
Table 14 – Auditable Events 23
Table 15 – Management of TSF data 26
Table 16 – TOE SFR Dependency Rationale 29
Table 17 – Mapping of TOE Security Functional Requirements and Objectives 30
Table 18 – Rationale for TOE SFRs to Objectives 32
Table 19 – Rationale for TOE Objectives to SFRs 34
Table 20 – Security Assurance Requirements at EAL2 35
Table 21 – Security Assurance Rationale and Measures 36

List of Figures

Figure 1 – TOE Boundary 9

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: Juniper Networks vGW Series Version 5.5
ST Revision	0.5
ST Publication Date	March 22, 2013
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Juniper Networks vGW Series Version 5.5

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text in square brackets, i.e., [*selection*].
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
NTP	Network Time Protocol
OSP	Organizational Security Policy
RFC	Request for Comment
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Function
vGW	Virtual Gateway

Table 2 – Acronyms Used in Security Target

1.6 TOE Overview

Security and compliance concerns are first-order priorities for virtualized data center and cloud deployments. Virtual Gateway (vGW) is a comprehensive security solution for virtualized data centers and clouds capable of monitoring and protecting virtualized environments while maintaining the highest levels of VM host capacity and performance. vGW includes a high-performance hypervisor-based stateful firewall, integrated intrusion detection (IDS), and virtualization-specific antivirus (AV) protection.

1.7 TOE Description

1.7.1 Physical Boundary

The TOE is a software TOE and is defined as the vGW Series Version 5.5. The TOE comprises the following components:

- The vGW Security Design VM that provides a central management server. It consists of a number of modules that you use to configure the vGW Series features overall and to view information that they provide about your deployment. Using it, you can manage one or more vGW Security VMs.

  You use the vGW Security Design VM for many purposes, including configuring firewall security policies for vGW Security VMs and deploying them to the hosts or nodes that they will protect.

- The vGW Security VM that is installed on each host or node to be secured. The vGW Security VM is used as a conduit to the vGW Kernel module that is inserted into the hypervisor of each host or node, which is where connections are processed.

  The vGW Security Design VM pushes the appropriate security policy to the vGW Security VM which, in turn, inserts it into the vGW Kernel module. The virtualized network traffic is secured and analyzed against the security policy in the vGW Kernel module.

    - The Introspection module of the vGW Security Design VM lets you monitor the software within the virtual infrastructure that is installed in all MS Windows and all Linux guest virtual machines (VMs) that support RPM package manager. Without installing endpoint software in the guest VMs, vGW Series can determine which applications are installed, the operating system type (for example, for MS Windows, XP, 2003), and identify registry values and applied updates (hotfixes).

    - The Compliance module of the vGW Security Design VM that lets you monitor the compliance of your overall system with regard to industry standards best practices. The Compliance module relies on a rule editor that allows you to use multiple attributes about the VMware infrastructure and associated VMs to establish criteria for each designed rule.

The TOE boundary is shown below:

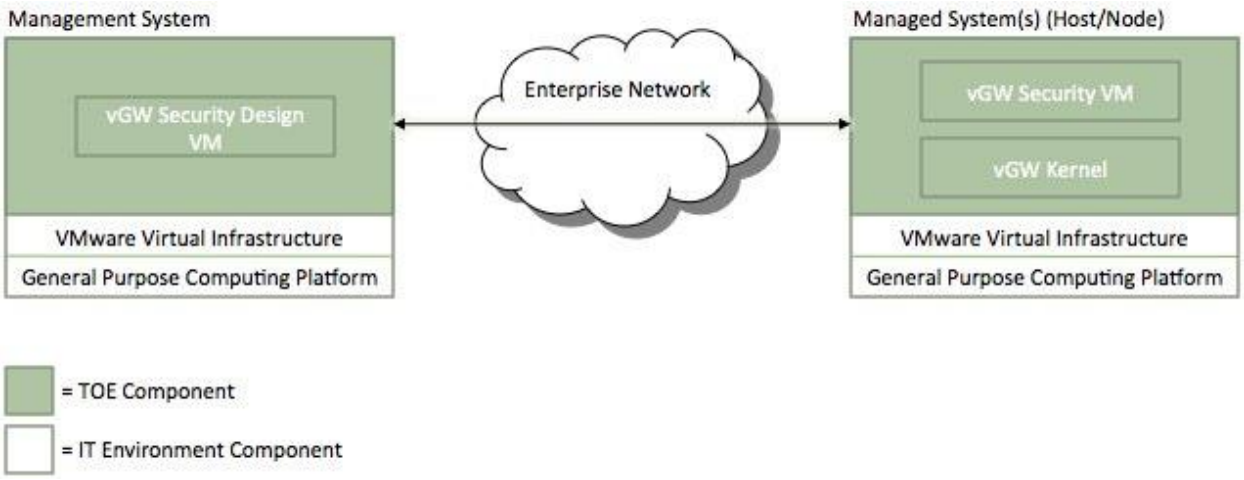


Figure 1 – TOE Boundary

In order to comply with the evaluated configuration, the following hardware and software components should be used:

COMPONENT	VERSION/MODEL NUMBER
TOE Software	Version 5.5
IT Environment	The TOE requires the following: • One or more vSphere ESX/ESXi 4 or 5.0 hosts. We recommend that you use more than one host for your deployment. You use the VMware vSphere Client software to integrate the vGW Series with the VMware infrastructure. • A VMware Virtual Center (vCenter) server, version 2.5. The *vCenter* VMware management server oversees the virtualization data center. The vCenter can be a physical server or a VM running on an MS Windows server. The vGW Series uses the vCenter server to automatically import vGW Series and adapt security as necessary when changes are made to the virtual environment. • Network connectivity. o The vGW Security Design VM must be accessible through HTTPS to allow access to the VMware Virtual Infrastructure API. Access to the VMware Virtual Infrastructure API is also required for autodiscovery of VM resources. o If you have access to the VMware Virtual Infrastructure API, you can connect a Web browser to the vCenter host

COMPONENT	VERSION/MODEL NUMBER
	(https://vCenter--IP--address). • Domain Name System (DNS) and Network Time Protocol (NTP) services for some components. The vGW Security VM requires NTP access to the center. • One of the following supported Web browsers is required: o Microsoft Internet Explorer 7 or 8 o Mozilla Firefox 3 or later Size requirements of the virtual appliances: • vGW Security Design VM o memory: 2 GB o disk space: 11 GB • vGW Security VM o memory: 512 MB o disk space: 1.5 GB

Table 3 – Evaluated Configuration for the TOE

1.7.2 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Security Audit	The TOE generates audit records for security events. The administrator and read-only administrator are the only roles with access to the audit trail and have the ability to view the audit trail.
Information Flow Control	The TOE has the capability to regulate the information flow across its interfaces; traffic filters can be set in accordance with the presumed identity of the source, the identity of the destination, and protocol.
Identification and Authentication	All users are required to perform identification and authentication before performing any administrative functions.
Security Management	The TOE provides a wide range of security management functions. Administrators can configure the TOE, manage TOE operators, the information flow policy, and audit among other routine maintenance activities.
Virus Scanning	The TOE provides for scanning and detection of file-based viruses.
Traffic Analysis	The TOE collects information on traffic flowing from TOE ingress points to egress points and analyzes the data against rules defined by an administrator to determine whether the traffic should be allowed or should be dropped.

Table 4 – Logical Boundary Descriptions

1.7.3 TOE Product Documentation

The TOE includes the following product documentation:

- Operational User Guidance and Preparative Procedures Supplement: Juniper Networks vGW Series Version 5.5

- Juniper Networks vGW Series Installation and Administration Guide

1.7.4 Excluded From the Evaluated Configuration

The following features are excluded from the evaluated configuration:

- Any CLI interface to the ESX client

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant.

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the EAL2 assurance package augmented with ALC_FLR.2 defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to modify the behavior of TSF data without being detected.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

Table 5 – Threats Addressed by the TOE

The IT Environment does not explicitly addresses any threats.

3.2 Organizational Security Policies

The TOE addresses the following organizational security policies:

OSP	DESCRIPTION
P.ANTIVIRUS	Files should be scanned either on-demand or in real-time for viruses.
P.IDS	Traffic should be analyzed and compared against known signatures that may indicate a security violation.

Table 6 – OSP

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.PHYSEC	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PUBLIC	The TOE does not host public data.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 7 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.MEDIAT	The TOE must mediate the flow of all information from users on an external network to resources on an internal network.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.ANTIVIRUS	The TOE will detect and take action against known viruses introduced to the workstation.
O.ANALYSIS	The TOE will analyze traffic and compare against known signatures that may indicate a security violation.

Table 8 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMTRA	Authorized administrators are trained to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.PHYSEC	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.PUBLIC	The operating system the TOE resides on does not host public data.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 9 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

THREATS/ ASSUMPTIONS / OBJECTIVES	T.AUDACC	T.AUDFUL	T.MEDIAT	T.NOAUTH	T.TUSAGE	P.IDS	P.ANTIVIRUS	A.GENPUR	A.NOEVIL	A.PHYSEC	A.PUBLIC	A.SINGEN
O.ACCOUN	✓											
O.AUDREC	✓											
O.IDAUTH				✓								
O.MEDIAT			✓									
O.SECFUN		✓										
O.ANTIVIRUS							✓					
O.ANALYSIS						✓						
OE.ADMTRA					✓				✓			
OE.GENPUR								✓				
OE.GUIDAN					✓							
OE.PHYSEC										✓		
OE.PUBLIC											✓	
OE.SINGEN												✓

Table 10 – Mapping of Assumptions, Threats, and Policies to Security Objectives

4.3.1 Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.AUDACC	This threat is completely countered by • O.ACCOUN which ensures the TOE provides user accountability for information flows through the TOE and for Administrator use of security functions related to audit. • O.AUDREC which ensures The TOE provides a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes
T.AUDFUL	This threat is completely countered by • O.SECFUN which ensures the TOE provides functionality that enables an Administrator to use the TOE security functions and also ensures that only Administrators are able to access such functionality

THREAT	RATIONALE
T.MEDIAT	This threat is completely countered by • O.MEDIAT which ensures the TOE mediates the flow of all information from users on an external network to resources on an internal network
T.NOAUTH	This threat is completely countered by • O.IDAUTH which ensures the TOE uniquely identifies and authenticates the claimed identity of all users before granting a user access to TOE functions.
T.TUSAGE	This threat is completely countered by • OE.ADMTRA which ensures the operational environment provides well-trained administrators to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE. • OE.GUIDAN which ensures the operational environment provides a secure manner of TOE delivery, installation, administration, and operation

Table 11 – Mapping of Objectives to Threats

4.3.1.1 Rationale for Security Objectives of the TOE

OBJECTIVE	RATIONALE
O.ACCOUN	This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that administrators, read-only administrators, and user admins are accountable for the use of security functions related to audit.
O.AUDREC	This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search the information contained in the audit trail.
O.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.
O.MEDIAT	This security objective is necessary to counter the threats: T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
O.SECFUN	This security objective is necessary to counter the threat T.AUDFUL by requiring that the TOE provides functionality that ensures that only the an authorized operator has access to the TOE security functions.
O.ANTIVIRUS	This security objective is necessary to enforce the policy for ensuring files are scanned either on-demand or in real-time for viruses (P.ANTIVIRUS).
O.ANALYSIS	This security objective is necessary to enforce the policy for ensuring traffic is analyzed and compared against known signatures that may indicate a security violation. (P.IDS)

OBJECTIVE	RATIONALE
OE.ADMTRA	This non-IT security objective is necessary to counter the threat T.TUSAGE and support the assumption A.NOEVIL because it ensures that authorized administrators receive the proper training in the correct configuration, installation and usage of the TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE (A.GENPUR).
OE.GUIDAN	This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.
OE.PHYSEC	The objective to provide physical protection for the TOE supports the assumption that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access (A.PHYSEC).
OE.PUBLIC	The TOE does not host public data. (A.PUBLIC)
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE. (A.SINGEN)

Table 12 – Mapping of Threats, Policies, and Assumptions to Objectives

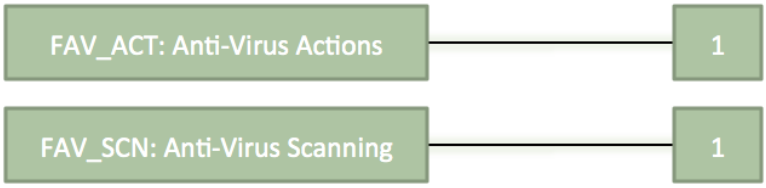
5 Extended Components Definition

5.1 Anti-Virus (FAV) Class of SFRs

The purpose of this class of requirements is to address the unique nature of anti-virus products and provide for requirements about detecting and responding to viruses on protected IT resources.

This class has the following objectives:

- detect known viruses introduced to a workstation
- take action against known viruses introduced to a workstation.



5.1.1 FAV_ACT.1 Anti-Virus Actions

Family Behavior

This family defines the requirements for actions the TOE should take when a virus is detected.

Hierarchical to: No other components.

Dependencies: FAV_SCN.1 Anti-Virus Scanning

FAV_ACT.1.1 Upon detection of a file-based virus, the TSF shall perform the action(s) specified by the [assignment: role]. Actions are administratively configurable on a per-workstation basis and consist of: [assignment: list of actions].

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the actions to be taken.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Action taken in response to detection of a virus.

5.1.2 FAV_SCN.1 Anti-Virus Scanning

Family Behavior

This family defines the requirements for scanning functions the TOE should provide in attempt to detect a virus.

Hierarchical to: No other components.

Dependencies: None

FAV_SCN.1.1 The TSF shall perform real-time scans and on-demand scans for file-based viruses based upon known signatures.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of parameters for all types of scans.

Audit:

There are no auditable events foreseen.

5.2 Intrusion Detection (IDS) Class of SFRs

The purpose of this class of requirements is to address the unique nature of intrusion detection products and provide for requirements for analyzing to traffic that may indicate an attack.

This class has the following objectives:

- Analyze traffic for potential malicious activity

5.2.1 IDS_ANL.1 Analyzer Analysis

Family Behavior

This family defines the requirements for how the TOE should analyze traffic and what if any actions should be performed.

Management: IDS_ANL.1

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed

Audit: IDS_ANL.1

There are no auditable events foreseen.

IDS_ANL.1 Analyzer Analysis

Hierarchical to:	No other components
Dependencies:	No dependencies
IDS_ANL.1.1	The System shall perform the following analysis function(s) on all IDS data received: a) [selection: *statistical, signature, integrity*]; and b) [assignment: *other analytical functions*].
IDS_ANL.1.2	The System shall record within each analytical result at least the following information: a. Date and time of the result, type of result, identification of data source; and b. [assignment: *other security relevant information about the result*].

5.3 Extended Security Assurance Components

None

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_STG.1	Protected Audit Trail Storage
User Data Protection	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.2	Secure Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_STM.1	Reliable Time Stamps
Antivirus	FAV_ACT.1	Anti-Virus Actions
	FAV_SCN.1	Anti-Virus Scanning
Traffic Analysis	IDS_ANL.1	Analyzer Analysis

Table 13 – TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 – Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*not specified*] level of audit; and

c) [The events in column two of Table 14 – Auditable Events]

FAU_GEN.1.2 The TSF shall record within each audit record at last the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 14 – Auditable Events].

SFR	EVENT	DETAILS
FMT_SMR.1	Modifications to the group of users that are part of a role.	The identity of the Administrator performing the modification and the user identity being associated with a role
FIA_UID.2	All use of the user identification mechanism.	None
FIA_UAU.2	Any use of the user authentication mechanism.	None
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Changes to the time.	The identity of the Administrator performing the operation
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit	The identity of the Administrator performing the operation
FAV_ACT.1	Detection of a virus and action taken	None

Table 14 – Auditable Events

6.1.1.2 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide [the Global Admin and Network Monitoring user] with the capability to read [all audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.3 FAU_STG.1 – Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorized modifications to the audit records in the audit trail.

6.1.2 Information Flow Control (FDP)

6.1.2.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [Information Flow Control SFP] on [

a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE from one subject to another;

c) operation: allow, drop, reject, send to external inspection device, analyze against IDS signatures as specified in IDS_ANL.1].

6.1.2.2 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [Information Flow Control SFP] based on the following types of subject and information security attributes:

[a) subject security attributes:

- source;
- no other subject security attributes

b) information security attributes:

- originating object;
- protocol;
- no other information security attributes].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator].

FDP_IFF.1.3 The TSF shall enforce the [Allow, deny rules based on the IPv6 multicast and broadcast parameters.].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [No additional rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [No additional rules].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [identity, association of a human user with a role, password].

6.1.3.2 FIA_UAU.2 – User Authentication before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 FIA_UID.2 – User Identification before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MOF.1 – Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behavior of, disable, enable, modify the behavior of*] the functions [

1. Start-up and shutdown;
2. Create, delete, modify, and view information flow security policy rules that permit or deny information flows;
3. Create, delete, modify, and view user attribute values defined in FIA_ATD.1;

4. Modify and set the time and date;

5. Manage introspection and compliance policies and rules] to [the Global Admin and VM Admin roles].

6.1.4.2 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Information Flow Control SFP] to restrict the ability to [*query, modify, delete*] the security attributes [information flow security policy rules that permit or deny information flows] to [the Global Admin and VM Admin roles].

6.1.4.3 FMT_MSA.2 – Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [security attributes listed with Information Flow Control SFP].

6.1.4.4 FMT_MSA.3 – Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Information Flow Control SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [the Global Admin and VM Admin roles] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.5 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to **control** the [data described in the table below] to [the Global Admin and VM Admin roles]:

DATA	CHANGE DEFAULT	QUERY	MODIFY	DELETE	CLEAR
Information Flow Control SFP	✓	✓	✓	✓	✓
User Account Attributes			✓		
Date/Time			✓		

Table 15 – Management of TSF data

6.1.4.6 FMT_SMF.1 - Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) Start-up and shutdown;

b) Create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) Create, delete, modify, and view user attribute values defined in FIA_ATD.1;

d) Modify and set the time and date].

6.1.4.7 FMT_SMR.1 – Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Global Admin, VM Admin, Network Monitoring].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_STM.1 – Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.6 Traffic Analysis (IDS)

6.1.6.1 IDS_ANL.1 – Analyzer Analysis

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:

a) [*signature*] and

b) [no other rules].

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [no other security relevant information about the result].

6.1.7 Anti-Virus (FAV)

6.1.7.1 FAV_ACT.1 – Anti-Virus Actions

FAV_ACT.1.1 Upon detection of a file-based virus, the TSF shall perform the action(s) specified by [the Global Admin]. Actions are administratively configurable and consist of: [Deny the operation, delete the file, or quarantine the file].

6.1.7.2 FAV_SCN.1 – Anti-Virus Scanning

FAV_SCN.1.1 The TSF shall perform both real-time and on-demand scans for file-based viruses based upon known signatures.

6.2 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.4.3 – Security Assurance Requirements.

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components	FPT_STM.1	Satisfied
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_STG.1	No other components	FAU_GEN.1	Satisfied
FDP_IFC.1	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied Satisfied
FIA_ATD.1	No other components	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2, which is hierarchical
FIA_UID.2	FIA_UID.1	None	n/a
FMT_MOF.1	No other components.	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FMT_MSA.1	No other components	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Satisfied
FMT_MSA.2	No other components	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Satisfied
FMT_MSA.3	No other components	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components	None	n/a
FMT_SMR.1	No other components	FIA_UID.1	Satisfied
FPT_STM.1	No other components	None	n/a
FAV_ACT.1	No other components	FAV_SCN.1	Satisfied
FAV_SCN.1	No other components	None	n/a
IDS_ANL.1	No other components	None	None

Table 16 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE / SFR	O.IDAUTH	O.MEDIAT	O.AUDREC	O.ACCOUN	O.SECFUN	O.ANTIVIRUS	O.ANALYSIS
FAU_GEN.1			✓	✓			
FAU_SAR.1			✓				

OBJECTIVE / SFR	O.IDAUTH	O.MEDIAT	O.AUDREC	O.ACCOUN	O.SECFUN	O.ANTIVIRUS	O.ANALYSIS
FAU_STG.1					✓		
FDP_IFC.1		✓					
FDP_IFF.1		✓					
FIA_ATD.1	✓						
FIA_UAU.2	✓						
FIA_UID.2	✓			✓			
FMT_MOF.1					✓		
FMT_MSA.1		✓			✓		
FMT_MSA.2		✓			✓		
FMT_MSA.3		✓			✓		
FMT_MTD.1	✓	✓	✓		✓		
FMT_SMF.1					✓		
FMT_SMR.1					✓		
FPT_STM.1			✓				
FAV_ACT.1						✓	
FAV_SCN.1						✓	
IDS_ANL.1							✓

Table 17 – Mapping of TOE Security Functional Requirements and Objectives

6.4.2 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

SFR	RATIONALE
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
FAU_SAR.1	This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.
FAU_STG.1	This component is chosen to ensure that the audit trail is protected from tampering. Only the Administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SECFUN.
FDP_IFC.1	This component identifies the entities involved in the Information Flow Control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

SFR	RATIONALE
FDP_IFF.1	This component identifies the attributes of the users sending and receiving the information in the Information Flow Control SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH.
FIA_UAU.2	This component requires successful authentication of a role before having access to the TSF and as such aids in meeting O.IDAUTH.
FIA_UID.2	This component requires successful identification of a role before having access to the TSF and as such aids in meeting O.IDAUTH and O.ACCOUN.

SFR	RATIONALE
FMT_MOF.1	This component was chosen to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN.
FMT_MSA.1	This component restricts the ability to modify, delete, or query the parameters for the Information Flow Control SFP to a Global Admin and also assists in effective management, and as such aids in meeting O.MEDIAT, and O.SECFUN.
FMT_MSA.2	This component ensures that only secure values are accepted for the configuration parameters associated with the Information Flow Control SFP to a Global Admin and also assists in effective management, and as such aids in meeting O.MEDIAT, and O.SECFUN.
FMT_MSA.3	This component ensures that the TOE provides a default restrictive policy for the information flow control security rules, yet allows an Global Admin to override the default restrictive values with permissive values. This component traces back to and aids in meeting the following objectives: O.MEDIAT and O.SECFUN.
FMT_MTD.1	This component restricts the ability to modify the Information Flow Control SFP, and as such aids in meeting, O.MEDIAT and O.SECFUN. This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.IDAUTH, O.MEDIAT and O.SECFUN. This component restricts the ability to delete audit logs, and as such contributes to meeting O.MEDIAT and O.SECFUN. This component restricts the ability to modify the date and time, and as such contributes to meeting O.MEDIAT, O.AUDREC , and O.SECFUN.
FMT_SMF.1	This component was chosen in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_SMR.1	This component ensures that roles are available to allow for varying levels of administration capabilities and restricts access to perform TSF relevant functionality depending on the role assigned to an authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.
FPT_STM.1	FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.
FAV_ACT.1	This component ensures the TOE provides the following actions when a virus is detected: Deny the operation, delete the file, or quarantine the file. This component traces back to and aids in meeting O.ANTIVIRUS.
FAV_SCN.1	The TOE provides the capability for on-demand scanning and real-time scanning of viruses. This component traces back to and aids in meeting O.ANTIVIRUS.
IDS_ANL.1	This component ensures the TOE performs analysis function(s) on all IDS data received and records the result. This component traces back to and aids in meeting O.ANALYSIS.

Table 18 – Rationale for TOE SFRs to Objectives

The following table presents a mapping of the rationale of TOE Objectives to Security Requirements:

OBJECTIVE	RATIONALE
O.ACCOUN	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited • FIA_UID.2 ensures that users are identified to the TOE
O.AUDREC	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited • FAU_SAR.1 which requires that the audit trail can be read • FPT_STM.1 ensures that reliable time stamps are provided for audit records • FMT_MTD.1 which restricts the ability to modify the Information Flow Control SFP, restricts the ability to modify identification and authentication data, restricts the ability to modify the date and time
O.IDAUTH	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users • FIA_UAU.2 which ensures that users are authenticated to the TOE • FIA_UID.2 which ensures that users are identified to the TOE • FMT_MTD.1 which restricts the ability to modify the Information Flow Control SFP, restricts the ability to modify identification and authentication data, restricts the ability to modify the date and time
O.MEDIAT	This objective is completely satisfied by • FDP_IFC.1 which ensures the TOE supports an authenticated user information flow policy that controls who can send and receive network traffic • FDP_IFF.1 which ensures Information Flow Control SFP limits information flow based on user roles and resource types • FMT_MSA.1 which restricts the ability to modify, delete, or query the parameters for the Information Flow Control SFP to an Global Administrator • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Information Flow Control SFP • FMT_MSA.3 which ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Information Flow Control SFP, restricts the ability to modify identification and authentication data, restricts the ability to modify the date and time

OBJECTIVE	RATIONALE
O.SECFUN	This objective is completely satisfied by • FAU_STG.1 which ensures only the authorized administrator has access to the logs • FMT_MOF.1 which ensures the ability to perform security management functions is restricted to a Global Admin • FMT_MSA.1 which restricts the ability to modify, delete, or query the parameters for the Information Flow Control SFP to a Global Admin • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Information Flow Control SFP • FMT_MSA.3 which ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Information Flow Control SFP, restricts the ability to modify identification and authentication data, restricts the ability to modify the date and time • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.
O.ANALYSIS	This objective is completely satisfied by • IDS_ANL.1 which exists to ensure the TOE performs analysis function(s) on all IDS data received and records the result.
O.ANTIVIRUS	This objective is completely satisfied by • FAV_ACT.1, which exists to ensure the TOE provides the following actions when a virus is detected: Deny the operation, delete the file, or quarantine the file. This component traces back to and aids in meeting O.ANTIVIRUS. • FAV_SCN.1, which exists to ensure the TOE provides the capability for on-demand scanning and real-time scanning of viruses.

Table 19 – Rationale for TOE Objectives to SFRs

6.4.3 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2 Flaw Reporting Procedures. The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 20 – Security Assurance Requirements at EAL2

6.4.4 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 2 augmented with ALC_FLR.2. EAL2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

6.4.5 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: Juniper Networks vGW Series Version 5.5
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: Juniper Networks vGW Series Version 5.5
ADV_TDS.1: Basic Design	Architectural Design: Juniper Networks vGW Series Version 5.5
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks vGW Series Version 5.5
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks vGW Series Version 5.5
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: Juniper Networks vGW Series Version 5.5
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: Juniper Networks vGW Series Version 5.5
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: Juniper Networks vGW Series Version 5.5
ALC_FLR.2 Flaw Reporting Procedures	Flaw Reporting Procedures: Juniper Networks vGW Series Version 5.5
ASE_CCL.1 Conformance claims	Security Target: Juniper Networks vGW Series Version 5.5
ASE_ECD.1 Extended components definition	Security Target: Juniper Networks vGW Series Version 5.5
ASE_INT.1 ST introduction	Security Target: Juniper Networks vGW Series Version 5.5
ASE_OBJ.2 Security objectives	Security Target: Juniper Networks vGW Series Version 5.5
ASE_REQ.2 Derived security requirements	Security Target: Juniper Networks vGW Series Version 5.5
ASE_SPD.1 Security problem definition	Security Target: Juniper Networks vGW Series Version 5.5
ASE_TSS.1 TOE summary specification	Security Target: Juniper Networks vGW Series Version 5.5
ATE_COV.1: Evidence of Coverage	Testing Evidence: Juniper Networks vGW Series Version 5.5

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ATE_FUN.1 Functional Testing	Testing Evidence: Juniper Networks vGW Series Version 5.5

Table 21 – Security Assurance Rationale and Measures

7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Information Flow Control
- Identification and Authentication
- Security Management
- Traffic Analysis
- Virus Scanning

7.2 Security Audit

The vGW Series collects information on events and posts it to the System Status and Events pane when administrative and policy operations occur. It posts event alerts on the following events:

- An administrator logs in or logs out, and when failed login attempts occur.
- An administrator changes vGW Security Design VM settings, including the following:
    - Changes to general system settings such as log connections, system reboots, license changes, and active directory.
    - Manual VM updates to VM.
    - Modifications to vGW Series objects, including networks, machines, groups, protocols, and administrator settings.
    - Updates to either the vGW Security Design VM or the vGW Security VM software.
    - Configuration changes to firewall.
    - Configuration changes to Syslog, Netflow, external inspection devices, and infrastructure reinforcement.
- Automatically secured VM configuration changes occur.
- IDS signatures are modified and new signatures are added.

- Introspection scans are started on Scan Now requests, scheduled events occur, and scheduled scan configurations are modified.
- Compliance Rule modifications are made.
- Reports are created or Reports configuration settings are modified.
- The Image Enforcer is configured, its configuration settings are changed, and Image Enforcer scans occur.
- AntiVirus is configured, changes are made to its configuration, and AntiVirus scans occur.
- SRX Series integration changes take place.
- Multi--Center and Split--Center settings are configured or changed.
- Backup and Restore is configured and when configuration changes are made.
- License settings are changed.
- Registry values are changed.

The logs are only accessible through the Web-Based administrative interface, which only authenticated Administrators are authorized access.

The TOE provides a timestamp for its own use. The timestamp is generated via calls to the host.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: the TOE generates all the audit events identified in this requirement. Within each event is the information listed above which addresses all required details.
- FAU_SAR.1: The Administrator has the ability to read all of the audit logs. Each log is presented to the administrator in a human-readable format.
- FAU_STG.1: Only the Administrator has access to the logs. The Administrator is not permitted to modify any information in the logs.
- FPT_STM.1: The TOE generates a reliable timestamp for its own use.

7.3 Information Flow Control

The TOE enforces an information flow policy between IT products. The TOE enforces the Information Flow Control SFP with stateful packet attributes, which include the source and destination network identifiers as well as the source and destination service identifiers. Traffic can be allowed, dropped, rejected, sent to external inspection device, or analyzed against IDS signatures as specified in Section 7.7.

The Information Flow Control function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE supports an authenticated user information flow policy that controls who can send and receive network traffic.
- FDP_IFF.1: The Information Flow Control SFP limits information flow based on user roles and resource types. Administrators have the ability to establish rules that permit or deny information flows based on the combination of attributes listed.

7.4 Identification and Authentication

The TOE performs identification and authentication of all users and administrators accessing the TOE. Users enter a username and password, which is validated by the TOE against the user information stored by the TOE. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: For each registered user, the TOE stores the following information: user identity, user name, user roles, and password.
- FIA_UAU.2: The TOE requires a valid password associated with a user name before providing access to the TOE.
- FIA_UID.2: The TOE requires a user name during the identification and authentication process. The username is entered, then a password. If the password is valid, the user will be associated with a role and set of privileges based on the username.

7.5 Security Management

The TOE provides security management functions via a browser interface. The Global Admin logs onto the TOE from a protected network and performs all management functions through the browser interface. The Global Admin has the ability to control all aspects of the TOE configuration including: user management, information flow policy management, audit management, and system start-up and shutdown.

Global Admins set the information flow policy rules on a per user basis. When the Global Admin adds a new user, the Administrator defines the user access. Although users are grouped into roles, Administrators can create rules that except specific users from the constraints of their role. By default, user access is restrictive but the Administrator may override the default upon rule creation.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: The ability to perform the following security management functions is restricted to an Global Admin role:
  a) start-up and shutdown;
  b) create, delete, modify, and view resource policy rules that permit or deny resource requests;
  c) create, delete, modify, and view user attribute values, which include a user's identity, association to a role, and authentication credentials;
  d) review the audit trail.
  e) manage introspection and compliance policies and rules.

- FMT_MSA.1: This component restricts the ability to modify, delete, or query the parameters for the Information Flow Control SFP to the Global Admin role
- FMT_MSA.2: This component ensures that only secure values are accepted for the configuration parameters associated with the Information Flow Control SFP
- FMT_MSA.3: The TOE allows restrictive access by default but the Global Admin role can assign more restrictive permissions.
- FMT_MTD.1: The TOE restricts the ability to modify the Information Flow Control SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, and restricts the ability to modify the date and time. All restrictions apply to unauthenticated or unauthorized users.
- FMT_SMF.1: The TOE supports the following security management functions:

  a) start-up and shutdown;
  b) create, delete, modify, and view resource policy rules that permit or deny resource requests;
  c) create, delete, modify, and view user attribute values, which include a user's identity, association to a role, and authentication credentials;

- FMT_SMR.1: The TOE supports the following roles:
  - Global Admin: Administrator with the highest level of system privileges, including the ability to create additional administrators. The global administrator can perform all operations in the product, including firewall installations and AntiVirus configurations. For example, he can select port groups and VMs for insertion and removal from a secured network.
  - VM Admin: Administrators who are allowed to have Modify policy and Settings permissions. This setting allows the administrator to change firewall security policies, including IDS, configure AntiVirus, and configure VM Introspection Compliance. They can configure mirroring of inter--vm traffic, which is the ability to configure rules with external inspection devices. Additionally, you can grant VM Admins the Install Firewall Policy privilege. This allows them to distribute a policy after it has been changed and saved by an administrator who has the privilege to modify security policies.

- Network Monitoring: Administrators who can see all network related screens (for example, statistics and graphs), all tabs of the Main module, including Status and Events and Alerts, and Logs. These administrators cannot modify any Settings screens, but they can view IDS Alerts, if IDS is configured, view AntiVirus scans, and they can view but not modify VM Introspection and Compliance results.

7.6 Virus Scanning

The TOE provides real-time virus detection on data flows through the TOE via on-demand and real-time scans. When an infection occurs, the TOE takes certain actions depending on what has been configured:

- Deletion of files automatically
- Denying access to infected files
- Move infected files to a quarantine folder (optional and in conjunction with one of the two actions above)

When a virus is detected (e.g. an infection occurs) a record is logged in System Events.

The Virus Scanning function is designed to satisfy the following security functional requirements:

- FAV_ACT.1: the TOE provides the following actions when a virus is detected: Deny the operation, delete the file, or quarantine the file.
- FAV_SCN.1: The TOE provides the capability for on-demand scanning and real-time scanning of viruses.

7.7 Traffic Analysis

The TOE continuously monitors network traffic from network resources and compares the packets to signatures and filters defined by administrators. Signatures identify packet and packet patterns (via an IT System's configuration information such as IP address, port, and usage statistics) that indicate a potential security violation to a resource accessible by the monitored network. The TOE has default, pre-defined signatures that include detection of denial of service, unauthorized access attempts, pre-attack probes, and suspicious activity. With each signature analysis result, the TOE records the date and time of the result, type of result, identification of data source

The Traffic Analysis Security Function provides the TOE's reaction capabilities when the analysis capability of the TOE has fired a rule and/or correlated an event (e.g., upon detection of an intrusion attempt). When this happens, the TOE will send an alert to the GUI where an authorized user can view it.

The Traffic Analysis function is designed to satisfy the following security functional requirements:

- IDS_ANL.1: the TOE performs analysis function(s) on all IDS data received and records the result.