Juniper® Validated Design

JVD Test Report Brief: Data Center Next-Generation Firewall Use Case

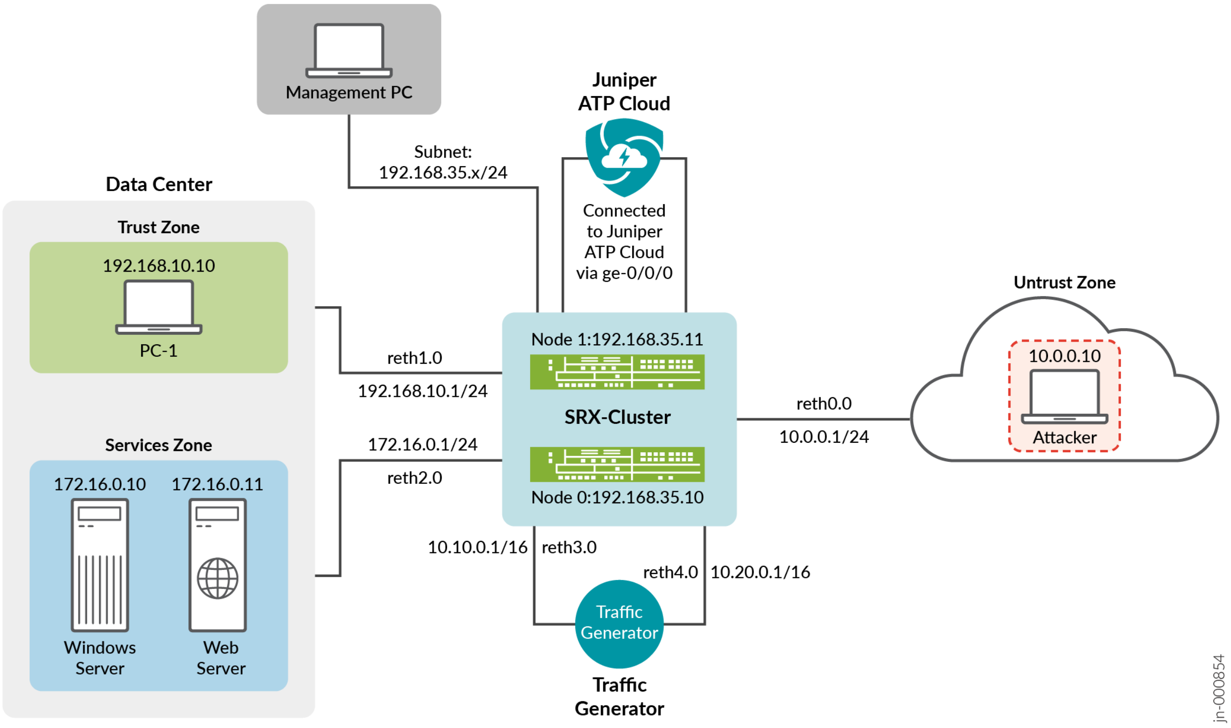
Introduction

This JVD demonstrates the next-generation firewall data center use cases. The use cases are focused on testing common data center services enabled on the SRX4600.

Data center firewalls configured in a Layer 2 chassis cluster environment perform full stack security on data center traffic traversing through the SRX Cluster.

Test Topology

Figure 1: Data Center Next-Generation Firewall Test Topology



Platforms Tested

Table 1: Platforms Tested

Role	Platform	Junos OS Release
Hub	SRX4600-HA	23.2R2
SRX4600	-	23.2R2

Version Qualification History

This JVD has been qualified in Junos OS Release 23.2R2.

Scale and Performance Data

Table 2: Scale Data

Users	Type of Traffic	Long-Lived Session	Short-Lived Session
20000	HTTP	200000	17000
20000	Non-HTTP	200000	0

The solution is tested using a background traffic profile of:

- 20000 users with 200000 long-lived and 17000 short-lived HTTP sessions.
- 20000 users and 200000 sessions of non-HTTP sessions.

Table 3: Performance Data

Type of Traffic	Type of Session	Session Count	SOF Session	Throughput	PPS	CPS	CPU	Memory
AppMix TCP (non-HTTP)	Long-lived	200000	200000	184 G	24 M	0	1	47%
HTTP	Long-lived	200000	0	18 G	2305000	0	91%	45%
HTTP	Short-lived	85000	0	4.7 G	670000	17000	70%	45%
HTTP	Long-lived and short-lived	286000	0	8.6 G	1200000	17000	90%	45%

High Level Features Tested

The following security features are validated as part of the JVD:

- Application Security
- Intrusion detection and prevention (IDP)
- Content Security (Web filtering)
- Advanced Threat Prevention using Juniper ATP Cloud

- Security Intelligence (SecIntel)
- Advanced anti-malware (AAMW)
- DNS security
- Screens

For Extension Mechanisms for DNS (EDNS) traffic, only SecIntel must be configured.

IoT is not qualified as part of this JVD. Currently from Junos OS, we have the ability to enforce this configuration.

Event Testing

Failover Events:

- Hub Cluster Node Failover - Node0 to Node1
  - Control plane failover
  - Data plane failover
  - Restart the logging daemon
  - Restart the security-intelligence daemon
  - Restart advanced-malware daemon

Traffic recovery was validated post all failure scenarios.

Tested Traffic Profiles

Table 4: Tested Traffic Profiles

Device	Traffic Profile	Protocol	Load
Hub	Long-lived session	Non-HTTP (AppMix)	200000 sessions
Hub	Long-lived session	HTTP (IxLoad)	200000 sessions
Hub	Short-lived session	HTTP (IxLoad)	17000 cps
Hub	Kali Linux Windows	Application flood-based Attack Wget DNS	100 cps

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701