INTEGRATING FIREWALL SERVICES IN THE DATA CENTER NETWORK ARCHITECTURE USING SRX SERIES SERVICES GATEWAY

Although Juniper Networks has attempted to provide accurate information in this guide, Juniper Networks does not warrant or guarantee the accuracy of the information provided herein. Third party product descriptions and related technical details provided in this document are for information purposes only and such products are not supported by Juniper Networks. All information provided in this guide is provided “as is”, with all faults, and without warranty of any kind, either expressed or implied or statutory. Juniper Networks and its suppliers hereby disclaim all warranties related to this guide and the information contained herein, whether expressed or implied of statutory including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement, or arising from a course of dealing, usage, or trade practice.
Table of Contents

Introduction ................................................................. 4
Challenges for Deploying Firewalls in the Data Center .............................................. 4
Scope .................................................................................. 4
Target Audience ............................................................... 5
SRX Technical Concepts ..................................................... 5
Security Zones and Interfaces ................................................ 5
Security Policy ...................................................................... 6
High Availability (HA) Chassis Cluster .......................................... 6
Redundancy Groups .............................................................. 6
Redundant Ethernet Interfaces .................................................. 7
Redundancy Group Failover ...................................................... 7
Design Considerations ......................................................... 7
Physical Placement of Firewalls .................................................. 7
Inline Firewall Deployment ..................................................... 8
One-Arm Firewall Deployment .................................................. 8
High Availability Configuration .................................................. 9
Active/Passive Firewall Cluster Deployment with Active/Passive Data Center Network Infrastructure .................................................. 10
Active/Passive Firewall Cluster Deployment with Active/Active Data Center Network Infrastructure .................................................. 11
Active/Active Firewall Cluster Deployment with Active/Active Data Center Network Infrastructure .................................................. 12
Integrating a Firewall in the Data Center Network Infrastructure ......................... 12
Access Tier VLAN Termination at the Firewall .............................................. 13
Access Tier VLAN Termination Access/Aggregation Tier ........................................ 13
Implementation ..................................................................... 14
Physical Connection Between SRX Series Nodes for Cluster .................................. 14
Configuring a Cluster on the SRX Series Device ............................................... 15
Creating a Redundancy Group ........................................................................ 15
Creating a Redundant Ethernet Interface ......................................................... 15
Configuring Dynamic Routing Protocol and Enabling a Graceful Restart .............. 16
Creating a Security Zone .................................................................. 16
Creating a Security Policy .................................................................. 16
Implementing Three Different Types of Deployment Scenarios ......................... 17
1. Active/Passive Firewall Cluster Deployment with Active/Passive Data Center Network Infrastructure .................................................. 17
Redundancy Group Configuration: .................................................................. 18
Logical Interface Configuration: .................................................................... 18
Security Zone Configuration: ....................................................................... 19
EX8200 Line Switch Configuration for Aggregation Tier—Interface Configuration: ............................................................................... 19
Routing Configuration: .............................................................................. 20
2. Active/Passive Firewall Cluster Deployment with Active/Active Data Center Network Infrastructure .................................................. 20
Redundancy Group Configuration: .................................................................. 21
Table of Figures

Figure 1: Deploying inline firewalls (physical view) ......................................................... 8
Figure 2: Deploying one-arm firewall ................................................................. 9
Figure 3: Active/passive firewall cluster deployment with active/passive
data center network infrastructure ................................................................. 10
Figure 4: Active/passive firewall cluster deployment with active/active
data center network infrastructure ................................................................. 11
Figure 5: Active/active firewall cluster deployment with active/active
data center network infrastructure ................................................................. 12
Figure 6: Access tier VLAN termination at firewall ......................................................... 13
Figure 7: Access tier VLAN termination access/aggregation tier ........................................ 14
Figure 8: Deploying active/passive firewall cluster ......................................................... 17
Figure 9: Active/passive firewall cluster deployment with active/active
data center network infrastructure ................................................................. 20
Figure 10: Active/active firewall cluster deployment with active/active
data center network infrastructure ................................................................. 24
Introduction

The data center is one of the most intensive deployment locations for networking equipment. It consists of thousands of servers that are accessed by tens of thousands of client systems. This need for large scale access creates a complex set of data flows, and makes it nearly impossible to clearly define the specific profile of network traffic. Because the determination of firewall deployment and sizing is a truly herculean effort, firewalls are often deployed in a limited fashion in the data center, if they are deployed at all.

Another driving factor in the limited use of firewalls in data centers has been the lack of performance. Not just raw bandwidth limitations, but connections per second as well as sustained connections have caused architects to distribute security or dispense with it altogether.

Juniper Networks® has created an entire new class of security products to address these challenges. Juniper Networks SRX Series Services Gateways provide the ability to scale in ways that were not thought possible in the past. Juniper has leveraged key technologies, such as Juniper Networks Junos® software and proven hardware architectures to create the SRX Series of products. The SRX Series has been designed to meet the demanding needs of data centers today, with the ability to expand and meet customers’ needs of tomorrow. With the high-end SRX Series gateway products, firewall deployment in the data center becomes natural and reasonable.

Challenges for Deploying Firewalls in the Data Center

Emerging applications dictate a very unpredictable and challenging traffic pattern in the data center. The traditional client/server connection models, in which clients communicate with a server using a single stream of data (or TCP session) to complete a request, are long gone. These days with the emergence of multi-node application clusters, server virtualization technologies, and storage over IP, applications tend to demand much more server-to-server resources from the network in terms of performance, and they tend to present much more challenging traffic patterns that involve communications between multiple servers over multiple sessions to fulfill a single user request. Today’s challenges include:

- Traffic requirements by multi-node applications
- Traffic requirements by server virtualization technologies
- Traffic requirements by storage over IP technologies

Scope

The purpose of this document is to provide readers with details about various design considerations and implementation guidelines to deploy firewall services in the data center core using high-end Juniper Networks SRX Series Services Gateways. The firewall services in the data center core can provide additional security and help meet compliance requirements by segmenting deployed server networks and by securing traffic within server networks.

This document briefly reviews the technical concepts of the SRX Series Services Gateways related to design and implementation of firewall services. Deployment scenarios are based on a logical 3-tier architecture (access, aggregation, and core) which can be collapsed physically into a 2-tier architecture (collapsed aggregation/core) or a single logical switch. The design principles discussed in this document are generic and can be applied to a customer’s respective physical network design as long as all traffic is received at the attachment layer of the firewalls to the network.

In this document, we review the following deployment scenarios and design considerations:

- Active/passive firewall cluster deployment with active/passive data center network infrastructure
- Active/passive firewall cluster deployment with active/active data center network infrastructure
- Active/active firewall cluster deployment with active/active data center network infrastructure

After reviewing deployment scenarios, implementation steps and validated configuration details are presented. The design is validated with Juniper Networks switching and routing products; however, the same design options can be applied for data center deployment with any other standard switching/routing platforms. This will help readers to compare different options related to their specific data center network design and make appropriate decisions for firewall deployment.
The following designs were tested for transit traffic latency over various paths that network traffic might take during normal operations in the event of a failure. The design was validated for convergence for various failure scenarios, such as link failure, network infrastructure device failure, or firewall node failure, to ensure required resiliency in the design. The SRX Series Services Gateways support all major dynamic routing protocols. For network integration, we used OSPF as the dynamic routing protocol.

The SRX Series firewall cluster designs specifically included the following:
- SRX Series firewall cluster with Juniper Networks EX8200 line of Ethernet switches as aggregation tier
- SRX Series firewall cluster with Juniper Networks MX960 Ethernet Services Router as collapsed aggregation/core tier

For performance and scalability details concerning the SRX Series Services Gateways, contact your local Juniper account representative.

Target Audience
- Systems engineers who need to understand data center deployment strategies
- System integrators who need to deploy firewalls in data center networks
- Network architects who need to understand the implications of deploying firewalls in data centers
- Network architects evaluating new design approaches to data center security
- Network engineers implementing a network design with a core attached firewall
- Security engineers and operators implementing and troubleshooting firewall issues in the data center core.

SRX Technical Concepts
In this section, we will briefly review technical concepts related to Juniper Networks SRX Series Services Gateways which are relevant to firewall deployment:
- Security zones and interfaces
- Security policy
- High availability (HA) chassis cluster
- Redundancy groups
- Redundant Ethernet interfaces
- Redundancy group failover

Security Zones and Interfaces
Interfaces act as a doorway through which traffic enters and exits an SRX Series gateway appliance. Many interfaces can share exactly the same security requirements; however, different interfaces can also have different security requirements for inbound and outbound data packets. Interfaces with identical security requirements can be grouped together into a single security zone. Security zones are logical entities to which one or more interfaces are bound. On a single device, you can configure multiple security zones, dividing the network into segments to which you can apply various security options to satisfy the needs of each segment. Security zones also allow administrators to group network addresses in an abstract construct of security zones and define security policies for inter-zone traffic. This approach reduces or eliminates the need for maintaining address lists for security policy. To achieve this, you must define two security zones at a minimum, basically to protect one area of the network from the other. If all interfaces on the firewall share a single security zone, then the security policy is defined as an intra-zone policy, and administrators will need to maintain an address list to specify source and destination for these security policies. This may be helpful for migrating existing security policies from another firewall platform.
Security Policy

Security zones are the building blocks for security policies. They are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts (user systems and other hosts such as servers) and their resources from one another in order to apply different security measures to them. Active security policies enforce rules for the transit traffic in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall. By default, a device denies all traffic in all directions. Through the creation of policies, you can control the traffic flow from zone to zone by defining the kinds of traffic permitted to pass from specified sources to specified destinations at scheduled times. At the broadest level, you can allow all kinds of traffic from any source in one zone to any destination in all other zones without any scheduling restrictions. At the narrowest level, you can create a policy that allows only one kind of traffic between a specified host in one zone and another specified host in another zone during a scheduled interval of time.

High Availability (HA) Chassis Cluster

To form a chassis cluster, a pair of identical SRX Series devices are combined to act as a single system that enforces the same overall security. For Juniper Networks SRX5600 Services Gateway and Juniper Networks SRX5800 Services Gateway chassis clusters, the placement and type of Services Processing Cards (SPCs) must match in the two clusters. When a device joins a cluster, it becomes a node of that cluster. With the exception of unique node settings and management IP addresses, nodes in a cluster share the same configuration.

Redundancy Groups

Chassis clustering provides high availability (HA) of interfaces and services through redundancy groups and primacy within groups. A redundancy group is an abstract construct that includes and manages a collection of objects. A redundancy group contains objects on both nodes. A redundancy group is primary on one node and backup on the other at any point in time. When a redundancy group is said to be primary on a node, its objects on that node are active. Redundancy groups are independent units of failover. Each redundancy group fails over from one node to the other, independent of other redundancy groups. When a redundancy group fails over, all of its objects fail over together.

Three characteristics determine the primacy of a redundancy group:

- the priority configured for the node
- the node ID (in case of tied priorities)
- the order in which the node comes up.

NOTE: If a lower priority node comes up first, then it will assume the primacy for a redundancy group (and will stay as primary if preempt is not enabled).

A chassis cluster can include many redundancy groups, some of which might be primary on one node and some of which might be primary on the other. Alternatively, all redundancy groups can be primary on a single node. One redundancy group’s primacy does not affect another redundancy group’s primacy. You can create up to 128 redundancy groups.

When you initialize a device in chassis cluster mode, the system creates a redundancy group referred to in this document as redundancy group 0. Redundancy group 0 manages the primacy and failover between the Routing Engines on each node of the cluster. As is the case for all redundancy groups, redundancy group 0 can be primary on only one node at a time. The node on which redundancy group 0 is primary determines which Routing Engine is active in the cluster. A node is considered the primary node of the cluster if its Routing Engine is the active one.

You can configure one or more redundancy groups numbered 1 through 128, referred to in this section as redundancy group x. Each redundancy group x acts as an independent unit of failover and is primary on only one node at a time.

Each redundancy group x contains one or more redundant Ethernet interfaces. A redundant Ethernet interface is a pseudo interface that contains a pair of physical Gigabit Ethernet interfaces or a pair of Fast Ethernet interfaces. If a redundancy group is active on node 0, then the child links of all associated redundant Ethernet interfaces on node 0 are active. If the redundancy group fails over to node 1, then the child links of all redundant Ethernet interfaces on node 1 become active. You can configure multiple redundancy groups to load-share traffic across the cluster. For example, you can configure some redundancy groups x to be primary on one node, and some redundancy groups x to be primary on the other node. You can also configure a redundancy group x in a one-to-one relationship with a single redundant Ethernet interface to control which interface traffic flows through.
The traffic for a redundancy group is processed on the node where the redundancy group is active. Because more than one redundancy group can be configured, it is possible that the traffic from some redundancy groups will be processed on one node, while the traffic for other redundancy groups is processed on the other node (depending on where the redundancy group is active). Multiple redundancy groups make it possible for traffic to arrive over an interface of one redundancy group and egress over an interface that belongs to another redundancy group. In this situation, the ingress and egress interfaces might not be active on the same node. When this happens, the traffic is forwarded over the fabric link to the appropriate node.

When you configure a redundancy group x, you must specify a priority for each node to determine the node on which the redundancy group x is primary. The node with the higher priority is selected as primary. The primacy of a redundancy group x can fail over from one node to the other. When a redundancy group x fails over to the other node, its redundant Ethernet interfaces on that node are active and their interfaces are passing traffic.

**Redundant Ethernet Interfaces**

A redundant Ethernet interface is a pseudo interface that includes a physical interface from each node of the cluster. A redundant Ethernet interface can contain either a pair of Fast Ethernet interfaces or a pair of Gigabit Ethernet interfaces that are referred to as child interfaces of the redundant Ethernet interface (the redundant parent). Each redundant Ethernet interface can contain only two interfaces because a cluster contains only two nodes. A redundant Ethernet interface’s child interface is associated with the redundant Ethernet interface as part of the child interface configuration. The redundant Ethernet interface’s child interface inherits most of its configuration from its parent. A redundant Ethernet interface inherits its failover property from the redundancy group x to which it belongs. A redundant Ethernet interface remains active as long as its primary child interface is available/active.

**Redundancy Group Failover**

For a redundancy group x to automatically fail over to another node, its interfaces must be monitored. When you configure a redundancy group x, you can specify a set of interfaces that the redundancy group x is to monitor for status (or health) to determine whether the interface is up or down. A monitored interface can be a child interface of any of its redundant Ethernet interfaces. When you configure an interface for a redundancy group x to monitor, you give it a weight.

Every redundancy group x has a threshold tolerance value initially set to 255. When an interface monitored by a redundancy group x becomes unavailable, its weight is subtracted from the redundancy group x’s threshold. When a redundancy group x’s threshold reaches 0, it fails over to the other node. For example, if redundancy group 1 was primary on node 0, on the threshold-crossing event, redundancy group 1 becomes primary on node 1. In this case, all of the child interfaces of redundancy group 1’s redundant Ethernet interfaces begin traffic handling.

A redundancy group x failover occurs because the cumulative weight of the redundancy group x’s monitored interfaces brings its threshold value to 0. When the monitored interfaces of a redundancy group x on both nodes reach their thresholds at the same time, the redundancy group x is primary on the node with the lower node ID, in this case node 0.

**Design Considerations**

In this section, we first review the options for physical placement of firewall devices. For data center network design, we will only review the firewall cluster deployments, as resiliency and high availability are quite critical for data center resources. Next we will review the configuration options for active/passive and active/active HA chassis cluster configurations for various data center infrastructure designs. At the end of the section, we will review network integration of firewall services with the option of Layer 3 termination at the firewall, or Layer 3 termination at aggregation or collapsed aggregation/core tier devices.

**Physical Placement of Firewalls**

Physical placement of firewall devices in the data center network infrastructure is one of the most important decisions network and security architects have to make. There are primarily two options for firewall placement:

- Physically inline
- Logically inline with one arm of the firewall physically connected to the network core

We will review both options below for comparison.
Inline Firewall Deployment

As outlined in the Enterprise Data Center Reference Architecture, firewall services are part of the network services tier attached to the core network infrastructure. The network services tier can be attached to the collapsed aggregation/core Layer (2-tier data center architecture) or to the aggregation layer (in a 3-tier data center design).

The firewall can be placed physically inline for all data traffic between the aggregation and core layers. This placement ensures that all traffic between the core and access layer is protected by the firewall. This connectivity will also allow firewall protection for intra-security segment traffic within the access layer. For intra-segment traffic firewall protection, such segments should be logically terminated at the firewall (typically this is achieved by routing the VLANs on the firewall and making the firewall as default gateway for all servers.

Another option to provide firewall services for intra-security segmentation at the access layer is to use the virtual router capability of collapsed aggregation/core layer devices. The system within one security segment is contained in a virtual router, and intra-segment traffic bypasses the firewall and the inter-segment traffic is controlled through firewall policy.

The physically inline firewall deployment requires fewer ports on aggregation devices; however, it reduces the flexibility of bypassing the firewall for access to core layer traffic. Figure 1 shows how to deploy inline firewalls from a physical perspective.

One-Arm Firewall Deployment

Another option is to connect the firewalls as a one-arm solution, sometimes referred to as a firewall on a stick configuration. With this approach, administrators have the flexibility to selectively define what traffic gets protection through the firewall or bypasses the firewall for certain types of traffic using routing policy configuration. With this configuration, Layer 3 termination can be at the firewall and inter VLAN traffic is routed by the firewall. This configuration ensures that traffic to/from such VLANs is always protected using firewall services. For any applications which do not require firewall protection, or in cases where sending traffic through firewalls breaks the application (legacy application), then VLANs hosting these applications can be terminated at aggregation devices, and communication among such VLANs can bypass the firewalls.
As noted earlier, another option is to use the virtual router capability of aggregation layer devices, if multiple VLAN segments are required to be part of a single security segment and no firewall services are required. For this configuration, all such VLANs should be contained within a virtual router, and one interface from the virtual router connects to a firewall. With this configuration, inter-virtual routing traffic is protected through firewall services.

With a one-arm firewall deployment, administrators can virtually keep the firewall inline by terminating VLAN at the firewall, or by configuring the routing (in case of VLAN termination at adjacent aggregation/core tier) to always send inter-virtual routing traffic through the firewall.

Administrators can also selectively bypass traffic via routing policy control. As this configuration provides flexible deployment options, we will explore the design options with one-arm firewall deployment solutions. The design options and configuration steps can also be adapted for physical inline firewall deployment options. Figure 2 illustrates a one-arm firewall deployment solution.

![Figure 2: Deploying one-arm firewall](image)

**High Availability Configuration**

Any device deployed in the data center must ensure consistent service delivery, and the accessibility of the network dictates the availability of the data center’s services. For a highly available security infrastructure, there is one word that describes its biggest challenge—state. Most modern devices track the state of the traffic going through the device. When a failure occurs between two active security devices, the state also must be shared between them. If the state is not shared, the secondary firewall will drop the existing sessions because it is not aware of the state. When any stateful device is deployed, it is important to ensure service continuity so that state can be shared between devices.

In a data center, ensuring availability is a key design principle. The primary goal is to ensure that the SRX Series services gateway can survive losing either the data or control plane in the event of a failure. The SRX Series platform brings in a new idea to HA design. The SRX Series can failover the control plane and/or the data plane between chassis. This new hybrid design allows the two individual devices to act as one large chassis. In doing so, it allows the two different systems to spread across the two units. In this scenario, it is not like a traditional active/backup cluster where one device does all of the work while the other device remains idle.

The control plane portion of the cluster is the Routing Engine (RE). The Routing Engine can fail over between the two chassis, with the first node passing traffic while the second node maintains the active RE. Therefore, in the event of a failure, the system that is running on the failed chassis fails over to the second chassis. This is done in a stateful manner for all traffic passing through the device. The only traffic that is lost is what is in the device or wires that fail.

In the data center, this provides ease of deployment of active/backup, with the flexibility that the second chassis can provide some backup services.
Active/Passive Firewall Cluster Deployment with Active/Passive Data Center Network Infrastructure

There are a few different approaches to firewall deployment, especially concerning guaranteed availability. The most basic deployment is an active/backup deployment. The overall concept is that one device is actively passing traffic, while the second device waits until the primary device fails. This is a simple deployment, and it reduces the possibility of issues that can surround a highly available deployment.

As illustrated in Figure 3, the data center network infrastructure is deployed in active/backup mode, where the device located on the left side is the active aggregation device, and the device located on the right side is the backup. With this configuration, the SRX Series can be connected to each aggregation device using one or more physical interfaces. The physical interfaces can be further divided using logical interfaces and can be assigned to different zones for security policy configuration purposes. The interfaces on the SRX Series are defined as redundant Ethernet interfaces, and the backup interface on the other node (SRX Series located on right side) connects to the aggregation device (located on right side) with similar logical interfaces. With this design, all redundant interfaces will belong to a single redundant group which will be active on the SRX Series device on the left side. With this configuration, a failure on an active interface, aggregation device, or SRX Series device results in a redundant group failover on the backup SRX Series node in the cluster, and all traffic will now be serviced by the SRX Series (right side).

---

**Figure 3: Active/passive firewall cluster deployment with active/passive data center network infrastructure**

With the design shown above, SRX Series integration in a routing environment can be achieved with any routing protocol including static. The load balancing is managed at the aggregation device and the SRX Series does not influence any inbound/outbound traffic load balancing, as only one SRX Series device is active at a time.

Because only one SRX Series device is active at any time, the traffic on the fabric link is minimized and mainly consists of dynamic runtime environment session state synchronization. For uplink traffic, the SRX Series can maintain Layer 3 routing adjacencies with both the aggregation device and load balancing across all uplinks from the aggregation to the core layer. This is important to minimize oversubscription for access to the core uplink. As traffic is forwarded by either SRX Series (left side) or SRX Series (right side), the firewall latency is minimized and remains consistent even after any failure causes a firewall failover.
Active/Passive Firewall Cluster Deployment with Active/Active Data Center Network Infrastructure

Many data center designs deploy an active/active load balancing network infrastructure. With such designs, both aggregation devices are actively passing traffic, and traffic between access and aggregation layers are load balanced using a VLAN. One can still deploy an SRX Series Services Gateway in the active/backup mode, where one SRX Series node in a cluster is actively processing all traffic while the other node acts as a backup device. We can use the cluster configuration described earlier to support the active/active aggregation layer configuration. The traffic for the aggregation device (located on the right) will be switched through the aggregation device (located on the left) which then adds microsecond latency and increases link utilization.

To address latency and link utilization concerns, one can also deploy a firewall cluster, as illustrated in Figure 4.

![Diagram of active/passive firewall cluster deployment with active/active data center network infrastructure]

Figure 4: Active/passive firewall cluster deployment with active/active data center network infrastructure

A set of VLANs are active on the aggregation device (located on left side), and another set of VLANs are active on the aggregation device (located on right side). For the SRX Series deployment, we have used two physical interfaces between each SRX Series and aggregation device. The physical interfaces are grouped using two redundant groups.

The outbound traffic from access layer to the core can be load balanced using equal-cost multipath across two uplinks. The inbound traffic from core to access layer is load balanced using an active link connection to the respective aggregation devices. As all groups are active on a single SRX Series node, intra-segment traffic, as well as access to core traffic, does not traverse through the fabric link. This load balanced configuration can reduce traffic latency.

If any link in a redundant group or aggregation device fails, the redundant group will fail over to the backup node, allowing service and new sessions to be established. The result is in an active redundant group distributed between two SRX Series nodes in the cluster. As in this design, a link failure on one SRX Series device can cause active redundant groups on both firewalls, and traffic between interfaces of such groups (one group active on the SRX Series located on the left side and another group active on the SRX Series located on the right side) passes through the fabric link and will increase latency as it traverses both firewalls.
Active/Active Firewall Cluster Deployment with Active/Active Data Center Network Infrastructure

With an active/active network infrastructure, the SRX Series cluster can also be deployed within an active/active mode. In this deployment, both firewalls are actively passing traffic. The challenge in this design has more to do with the surrounding environment than with the actual firewalls themselves. There are many outlying factors, such as dynamic routing protocols, surrounding routers, or switches. Configuring all of the surrounding devices and ensuring that they can work in unison is the difficulty. If all of the surrounding challenges can be resolved, the largest reward for this type of deployment is that both devices pass traffic. Figure 5 illustrates this deployment scenario.

![Figure 5: Active/active firewall cluster deployment with active/active data center network infrastructure](image)

A set of VLANs are active on the aggregation device (left side), and another set of VLANs are active on the aggregation device (right side). For the SRX Series deployment, we have used two physical interfaces between each SRX Series and aggregation device. The physical interfaces are grouped using two redundant groups. One redundant group is active on the SRX Series (left side) and the other redundant group is active on the SRX Series (right side) by using different node priorities for the redundant groups.

With this configuration, both SRX Series nodes in the cluster are actively passing traffic. This also results in cross cluster node traffic for inter-redundant group traffic that is active on different nodes. Using routing policy aggregation devices can load balance the inbound traffic. Alternatively, we can also use BGP between the SRX Series and the aggregation device for deterministic next-hop selection for inbound load balancing.

Integrating a Firewall in the Data Center Network Infrastructure

In this section, we review the firewall deployment for different data center deployment environments. Data center network infrastructure may deploy Layer 2 switching within the access and aggregation layer, or it may terminate VLANs at the access or aggregation layer and perform Layer 3 routing within the access layer or aggregation layer. The firewall deployment options described earlier can be supported with both data center network infrastructure architectures.
Access Tier VLAN Termination at the Firewall

In a Layer 2 switching at the aggregation device facing the access layer architecture, the firewall acts as a default gateway for servers connected at the access layer, and the VLANs span from the access layer to aggregating layer up to the firewall. The servers within the same VLAN communicate to each other without firewall services, and the communication among such servers can be controlled through the access control list (ACL) on the access or aggregation devices. Juniper switching/routing platforms (Juniper Networks EX Series Ethernet Switches and Juniper Networks MX Series Ethernet Services Routers) do not introduce any performance hits due to ACL configuration, and they support line rate forwarding for traffic controlled through the access control list. The firewall to the aggregation uplink interface can be a routed interface, and hence can load balance the traffic towards the core using both aggregation devices. The aggregation device will terminate the core-facing VLAN between both aggregation devices and extend it to the firewall cluster.

![Figure 6: Access tier VLAN termination at firewall](image)

Access Tier VLAN Termination Access/Aggregation Tier

With Layer 3 routing termination at the aggregation tier, inter VLAN traffic for VLANs terminated at an aggregation device will not be diverted to the firewall. The traffic from the access layer VLAN to the core can also bypass the firewall based on the configuration. Network administrators can use the following mechanism on the aggregation device to direct traffic to the firewall.

- Filter based forwarding—An administrator can apply access control rules and packets matching the defined criteria, and the packets can be routed, dropped, or redirected to the firewall based on the defined action. This requires ACL maintenance on the aggregation device to meet data center security requirements.

- Virtual router—An administrator can terminate a set of VLANs on the aggregation device and assign them to a virtual router. VLANs belonging to the same virtual router can communicate with each other within the aggregation device and with traffic not secured by the firewall. The virtual router can extend one VLAN interface to the SRX Series cluster and to another matching virtual router on other aggregation devices. This approach ensures that any traffic leaving the virtual router (security segment/functional area) will be protected through the firewall. Any exception to this rule can be supported using filter-based forwarding. This reduces the number of ACL rules on the aggregation device.
Figure 7: Access tier VLAN termination access/aggregation tier

**Implementation**

In this section, we review the implementation steps for deploying SRX Series Services Gateways for firewall services in the data center. The primary configuration steps include the following:

- Configuring SRX Series nodes for chassis cluster
- Configuring redundancy groups
- Configuring redundant Ethernet interfaces
- Network integration using logical interfaces and dynamic routing protocol
- Enabling graceful restart
- Configuring security zones
- Configuring security policy

**Physical Connection Between SRX Series Nodes for Cluster**

To configure two SRX Series nodes as a high availability chassis cluster, connect the chassis control port to the data port using fiber cable for the cluster. The cluster ID must be defined between 1 and 15, and the node ID must be defined between 0 and 1 in each cluster. Cluster ID 0 unsets the cluster. These steps are common for all deployment scenarios. Below are the configuration details for reference.
Configuring a Cluster on the SRX Series Device

To configure a chassis cluster, you need to configure the following parameters:

- Cluster ID and Node ID
- Control port
- Fabric port

Below are the commands to configure these parameters:

```bash
set chassis cluster cluster-id <0 and 15> node <0 and 1> reboot
set chassis cluster control-ports fpc 6 port 0
set chassis cluster control-ports fpc0 port0
set interfaces fab0 fabric-options member-interfaces xe-3/0/0
set interfaces fab1 fabric-options member-interfaces xe-9/0/0
```

Creating a Redundancy Group

Next, we configure redundancy groups. Redundancy group 0 is used for the routing engine, and group 1 to 127 can be used for the interfaces. The node priority determines which node is active for any given redundancy group. The active/passive and active/active SRX Series chassis cluster configuration is achieved by setting appropriate node priority for different redundancy groups. In the following section, we discuss in detail node priority.

```bash
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 1
set chassis cluster redundancy-group 1 node 0 priority 254
set chassis cluster redundancy-group 1 node 1 priority 10
```

Creating a Redundant Ethernet Interface

Now we can configure the redundant Ethernet interfaces and assign the child interfaces (physical interfaces) to the parent redundant Ethernet interface. The redundant Ethernet interface is assigned to a redundancy group, while the active node of the redundancy group determines which interface will forward traffic between the pair of physical interfaces that belong to the redundant Ethernet interface.

```bash
set interfaces xe-3/1/0 gigether-options redundant-parent reth1
set interfaces xe-9/1/0 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1
```

Next we need to configure logical interface properties for the redundant Ethernet interface. The logical interface is assigned an IP addresses and runs dynamic routing protocols for network integration. The child interfaces inherit this configuration.

```bash
set interfaces reth1 VLAN-tagging
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 10 VLAN-id 10
set interfaces reth1 unit 10 family inet address 10.10.0.1/24
set interfaces reth1 unit 11 VLAN-id 11
set interfaces reth1 unit 11 family inet address 10.11.0.1/24
```
Configuring Dynamic Routing Protocol and Enabling a Graceful Restart

As a next step, we will enable dynamic routing protocol (as an example OSPF) on interfaces. When you use dynamic routing protocol with a high availability chassis cluster, we recommend enabling graceful restart for such protocols. When a router enabled for OSPF graceful restart restarts, it retains routes learned before the restart in its forwarding table. The router does not allow new OSPF link-state advertisements (LSAs) to update the routing table. This router continues to forward traffic to other OSPF neighbors (or helper routers), and sends only a limited number of LSAs during the restart period. To re-establish OSPF adjacencies with neighbors, the restarting router must send a grace LSA to all neighbors. In response, the helper routers enter helper mode and send an acknowledgement back to the restarting router. If there are no topology changes, the helper routers continue to advertise LSAs as if the restarting router had remained in continuous OSPF operation.

When the restarting router receives replies from all of the helper routers, the restarting router selects routes, updates the forwarding table, and discards the old routes. At this point, full OSPF adjacencies are re-established and the restarting router receives and processes OSPF LSAs as usual. When the helper routers no longer receive grace LSAs from the restarting router or the topology of the network changes, the helper routers also resume normal operation.

```
set protocols ospf area 0.0.0.0 interface all
set protocols ospf graceful-restart
```

Creating a Security Zone

Next, create the required security zones and assign logical interfaces to each security zone. You also need to enable the protocols supported on these interfaces.

```
set security zones security-zone zone-10 interfaces reth1.10 host-inbound-traffic system-services ping
set security zones security-zone zone-10 interfaces reth1.11 host-inbound-traffic system-services ping
set security zones security-zone zone-10 interfaces reth1.12 host-inbound-traffic system-services ping
set security zones security-zone uplink host-inbound-traffic system-services ping
set security zones security-zone uplink host-inbound-traffic protocols ospf
set security zones security-zone uplink interfaces reth3.500 host-inbound-traffic system-services ping
set security zones security-zone uplink interfaces reth3.500 host-inbound-traffic protocols ospf
set security zones security-zone uplink interfaces reth4.600 host-inbound-traffic system-services ping
set security zones security-zone uplink interfaces reth4.600 host-inbound-traffic protocols ospf
```

Creating a Security Policy

As a default, all transit traffic is blocked on the firewall. You need to configure security policy to permit the allowed traffic. Below is an example of security policy to permit all traffic from zone-10 to zone-10. Similar steps can be followed for permitting/denying traffic to/from other zones.

```
set security policies from-zone zone-10 to-zone zone-10 policy rule1 match source-address any
set security policies from-zone zone-10 to-zone zone-10 policy rule1 match destination-address any
set security policies from-zone zone-10 to-zone zone-10 policy rule1 match application any
set security policies from-zone zone-10 to-zone zone-10 policy rule1 then permit
```
Implementing Three Different Types of Deployment Scenarios

In this section, we review implementation details for the following deployment scenarios:

- Active/passive firewall cluster deployment with active/passive data center network infrastructure using EX8200 line devices as aggregation tier switches
- Active/passive firewall cluster deployment with active/active data center network infrastructure using EX8200 line devices as aggregation tier switches
- Active/active firewall cluster deployment with active/active data center network infrastructure using the MX960 Ethernet Services Router with Layer 3 termination at the aggregation tier using virtual router configuration.

Below are the common configuration details for all deployment options we have discussed.

- VLAN 10, 11, 12, 20, 21, 22 are access layer VLANs, and all servers are hosted in these VLANs.
- All other VLAN references are for interconnection between various devices within the data center network.
- The server networks are divided into two network security segments: VLAN 10, 11, 12, and VLAN 20, 21, 22.
- OSPF is used as a dynamic routing protocol with area 0.0.0.0.

1. Active/Passive Firewall Cluster Deployment with Active/Passive Data Center Network Infrastructure

The data center network infrastructure is active/passive. Aggregation tier devices are the EX8200 line of Ethernet switches.

As illustrated in Figure 8, this is an active/passive network infrastructure with the left side of the network actively passing traffic, whereas the right side of the network devices are standing by and will forward traffic in case of failure of corresponding active devices.

All of the VLANs extend to SRX Series devices. The solid line denotes the active interface and the dotted line shows the passive interface on the SRX Series cluster. As shown, all active interfaces are on the SRX Series (located on left side).

As this is a one-arm firewall deployment, the core-side interface on the SRX Series is shown with a purple line (VLAN 500). Both aggregation tier network devices have a routed interface on VLAN 500 and can create routing adjacency with the SRX Series for outbound traffic load balancing.
All redundant interfaces are assigned to redundancy group 1, as only one node is active at a time with this design. The priority of node 0 (SRX left side) is set lower to ensure that it is active for all interfaces. With this design, only one SRX Series node is active at a time, so there is no data traffic over the fabric link and traffic latency is the lowest when compared to all other designs.

For redundancy group failover, all interfaces are monitored and have interface priority set to 255. Therefore, in case of interface failure, the redundancy group will fail over to the SRX Series (right side), and all traffic will now be forwarded through the SRX Series (right side).

The logical interfaces on the redundant Ethernet interfaces are assigned to different zones which are used for defining security policy.

Below are the chassis cluster configuration details for reference.

**Redundancy Group Configuration:**

```plaintext
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 1
set chassis cluster redundancy-group 1 node 0 priority 254
set chassis cluster redundancy-group 1 node 1 priority 10
set chassis cluster redundancy-group 1 preempt
set chassis cluster redundancy-group 1 interface-monitor xe-3/1/0 weight 255
set chassis cluster redundancy-group 1 interface-monitor xe-3/2/0 weight 255
set chassis cluster redundancy-group 1 interface-monitor xe-3/3/0 weight 255
set interfaces xe-3/1/0 gigether-options redundant-parent reth1
set interfaces xe-3/2/0 gigether-options redundant-parent reth2
set interfaces xe-3/3/0 gigether-options redundant-parent reth3
set interfaces xe-9/1/0 gigether-options redundant-parent reth1
set interfaces xe-9/2/0 gigether-options redundant-parent reth2
set interfaces xe-9/3/0 gigether-options redundant-parent reth3
set interfaces fab0 fabric-options member-interfaces xe-3/0/0
set interfaces fab1 fabric-options member-interfaces xe-9/0/0
```

**Logical Interface Configuration:**

```plaintext
set interfaces reth1 VLAN-tagging
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 10 VLAN-id 10
set interfaces reth1 unit 10 family inet address 10.10.0.1/24
set interfaces reth1 unit 11 VLAN-id 11
set interfaces reth1 unit 11 family inet address 10.11.0.1/24
set interfaces reth1 unit 12 VLAN-id 12
set interfaces reth1 unit 12 family inet address 10.12.0.1/24
set interfaces reth2 VLAN-tagging
set interfaces reth2 redundant-ether-options redundancy-group 1
set interfaces reth2 unit 20 VLAN-id 20
set interfaces reth2 unit 20 family inet address 10.20.0.1/24
set interfaces reth2 unit 21 VLAN-id 21
set interfaces reth2 unit 21 family inet address 10.21.0.1/24
set interfaces reth2 unit 22 VLAN-id 22
set interfaces reth2 unit 22 family inet address 10.22.0.1/24
set interfaces reth3 VLAN-tagging
set interfaces reth3 redundant-ether-options redundancy-group 1
set interfaces reth3 unit 500 VLAN-id 500
set interfaces reth3 unit 500 family inet address 172.16.30.2/24
```
Security Zone Configuration:

```plaintext
set security zones security-zone zone-10 interfaces reth1.10 host-inbound-traffic system-services ping
set security zones security-zone zone-10 interfaces reth1.11 host-inbound-traffic system-services ping
set security zones security-zone zone-10 interfaces reth1.12 host-inbound-traffic system-services ping
set security zones security-zone uplink host-inbound-traffic system-services ping
set security zones security-zone uplink host-inbound-traffic protocols ospf system-services ping
set security zones security-zone uplink interfaces reth3.500 host-inbound-traffic system-services ping
set security zones security-zone uplink interfaces reth3.500 host-inbound-traffic protocols ospf system-services ping
set security zones security-zone zone-20 interfaces reth2.20 host-inbound-traffic system-services ping
set security zones security-zone zone-20 interfaces reth2.21 host-inbound-traffic system-services ping
set security zones security-zone zone-20 interfaces reth2.22 host-inbound-traffic system-services ping
```

EX8200 Line Switch Configuration for Aggregation Tier—Interface Configuration:

```plaintext
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan10
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan11
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan12
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan21
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan20
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan22
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan10
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan11
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan12
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan21
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan20
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan22
set interfaces ge-0/0/2 vlan-tagging
set interfaces ge-0/0/2 unit 100 vlan-id 100
set interfaces ge-0/0/2 unit 100 family inet address 172.16.10.1/30
set interfaces ge-0/0/3 vlan-tagging
set interfaces ge-0/0/3 unit 200 vlan-id 200
set interfaces ge-0/0/3 unit 200 family inet address 172.16.20.1/30
set interfaces ge-0/0/47 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan10
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan11
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan12
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan21
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan20
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan22
set interfaces xe-1/0/1 unit 0 family ethernet-switching port-mode trunk
set interfaces xe-1/0/1 unit 0 family ethernet-switching vlan members vlan10
set interfaces xe-1/0/1 unit 0 family ethernet-switching vlan members vlan11
set interfaces xe-1/0/1 unit 0 family ethernet-switching vlan members vlan12
set interfaces xe-1/0/2 unit 0 family ethernet-switching port-mode trunk
set interfaces xe-1/0/2 unit 0 family ethernet-switching vlan members vlan20
set interfaces xe-1/0/2 unit 0 family ethernet-switching vlan members vlan21
```
set interfaces xe-1/0/2 unit 0 family ethernet-switching vlan members vlan22
set interfaces xe-1/0/3 unit 0 family ethernet-switching port-mode trunk
set interfaces xe-1/0/3 unit 0 family ethernet-switching vlan members vlan500
set interfaces lo0 unit 0 family inet address 172.16.127.127/32
set interfaces vlan unit 500 family inet address 172.16.30.1/24

Routing Configuration:

set protocols ospf area 0.0.0.0 interface ge-0/0/2.100
set protocols ospf area 0.0.0.0 interface ge-0/0/3.200
set protocols ospf area 0.0.0.1 interface vlan.500
set vlans vlan10 vlan-id 10
set vlans vlan100 vlan-id 100
set vlans vlan11 vlan-id 11
set vlans vlan12 vlan-id 12
set vlans vlan20 vlan-id 20
set vlans vlan200 vlan-id 200
set vlans vlan21 vlan-id 21
set vlans vlan22 vlan-id 22
set vlans vlan500 vlan-id 500
set vlans vlan500 l3-interface vlan.500

2. Active/Passive Firewall Cluster Deployment with Active/Active Data Center Network Infrastructure

As illustrated in Figure 9, this is an active/active network infrastructure with the left side of the aggregation tier network device actively forwarding traffic for a set of VLANs 10, 11, 12, and the right side of the network device forwarding traffic for a set of VLANs 20, 21, 22. Both devices are in standby mode for each other and will forward traffic for all VLANs, should any one of the aggregation devices fail.

Figure 9: Active/passive firewall cluster deployment with active/active data center network infrastructure
All of the VLANs are extended to the SRX Series. The solid line denotes the active interface and the dotted line shows the passive interface on the SRX Series cluster. As shown in Figure 9, all active interfaces are on the SRX Series (left side) device. To achieve this, both aggregation tier devices and SRX Series nodes in the clusters are connected with full mesh connectivity.

As this is a one-arm firewall deployment, core-side interfaces on the SRX Series are shown with VLAN 500 and VLAN 600. Both aggregation tier network devices will have a routed interface on VLAN 500 and VLAN 600 and can create routing adjacency with the SRX Series for outbound traffic load balancing.

With this design, two redundancy groups are configured on the SRX Series cluster. Redundancy group 1 contains redundant Ethernet interface 1, and redundancy group 2 contains redundant Ethernet interface 2.

Logical sub interfaces are created on both redundant Ethernet interfaces—reth1 has a logical interface for the access tier VLANs 10, 11, 12, and the core uplink VLAN 500. The access tier VLAN 20, 21, 22 and core-uplink VLAN 600 are configured on redundant Ethernet interface 2.

The priority of the node 0 device (SRX Series located on left side) for both redundancy group 1 (which contains reth1) and redundancy group 2 (which contains reth2) is low; both reth1 and reth2 are active on the node 0 device (SRX Series located on left side), and in case of failure, the respective group will fail over to the passive SRX Series node (located on right side).

For redundancy group failover, respective interfaces are monitored and have their interface priority set to 255. In case of any interface failure, the redundancy group will fail over to the other SRX Series node.

With this design, when all devices and connections are up, only one SRX Series node is actively passing traffic, keeping latency low. However, in case of link failure, one of the redundancy groups may fail over to another node and both SRX Series nodes can actively forward traffic for different access tier segments. With this scenario, access tier inter-segment traffic (for example VLAN 10 and VLAN 20) will transit through the fabric link on the SRX Series cluster between both nodes in the cluster. This design may increase traffic latency as it passes through two physical devices.

**NOTE:** With this design, if we assign all interfaces to a single redundancy group in case one of the aggregation tier devices fails, one segment might not converge so it is important to use multiple redundancy groups even though all groups are active on one node.

Below are the chassis cluster configuration details for reference:

**Redundancy Group Configuration:**

```plaintext
set chassis cluster redundancy-group 1 node 1 priority 10
set chassis cluster redundancy-group 1 preempt
set chassis cluster redundancy-group 1 interface-monitor xe-3/1/0 weight 255
set chassis cluster redundancy-group 1 interface-monitor xe-9/1/0 weight 255
set chassis cluster redundancy-group 2 node 0 priority 10
set chassis cluster redundancy-group 2 node 1 priority 254
set chassis cluster redundancy-group 2 preempt
set chassis cluster redundancy-group 2 interface-monitor xe-3/2/0 weight 255
set chassis cluster redundancy-group 2 interface-monitor xe-9/2/0 weight 255
set interfaces xe-3/1/0 gigether-options redundant-parent reth1
set interfaces xe-3/2/0 gigether-options redundant-parent reth2
set interfaces xe-9/1/0 gigether-options redundant-parent reth1
set interfaces xe-9/2/0 gigether-options redundant-parent reth2
set interfaces fab0 fabric-options member-interfaces xe-3/0/0
set interfaces fab1 fabric-options member-interfaces xe-9/0/0
```
Logical Interface Configuration:

```
set interfaces reth1 VLAN-tagging
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 10 VLAN-id 10
set interfaces reth1 unit 10 family inet address 10.10.0.1/24
set interfaces reth1 unit 11 VLAN-id 11
set interfaces reth1 unit 11 family inet address 10.11.0.1/24
set interfaces reth1 unit 12 VLAN-id 12
set interfaces reth1 unit 12 family inet address 10.12.0.1/24
set interfaces reth1 unit 500 VLAN-id 500
set interfaces reth1 unit 500 family inet address 172.16.30.2/24
set interfaces reth1 unit 500 VLAN-tagging
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth2 VLAN-tagging
set interfaces reth2 redundant-ether-options redundancy-group 2
set interfaces reth2 unit 20 VLAN-id 20
set interfaces reth2 unit 20 family inet address 10.20.0.1/24
set interfaces reth2 unit 21 VLAN-id 21
set interfaces reth2 unit 21 family inet address 10.21.0.1/24
set interfaces reth2 unit 22 VLAN-id 22
set interfaces reth2 unit 22 family inet address 10.22.0.1/24
set interfaces reth2 unit 600 VLAN-id 600
set interfaces reth2 unit 600 family inet address 172.17.30.2/24
```

Security Zone Configuration:

```
set security zones security-zone zone-10 interfaces reth1.10 host-inbound-traffic
set security zones security-zone zone-10 interfaces reth1.11 host-inbound-traffic
set security zones security-zone zone-10 interfaces reth1.12 host-inbound-traffic
set security zones security-zone uplink host-inbound-traffic system-services ping
set security zones security-zone uplink host-inbound-traffic protocols ospf
set security zones security-zone uplink interfaces reth1.500 host-inbound-traffic
set security zones security-zone uplink interfaces reth1.500 host-inbound-traffic protocols ospf
set security zones security-zone uplink interfaces reth2.600 host-inbound-traffic
set security zones security-zone uplink interfaces reth2.600 host-inbound-traffic protocols ospf
set security zones security-zone zone-20 interfaces reth2.20 host-inbound-traffic
set security zones security-zone zone-20 interfaces reth2.21 host-inbound-traffic
set security zones security-zone zone-20 interfaces reth2.22 host-inbound-traffic
```
EX8200 Series Switch Configuration for Aggregation Tier—Interface Configuration:

```plaintext
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan10
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan11
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan12
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan21
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan20
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members vlan22
set interfaces ge-0/0/1 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan10
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan11
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan12
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan21
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan20
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan22
set interfaces ge-0/0/2 unit 100 vlan-id 100
set interfaces ge-0/0/3 unit 200 vlan-id 200
set interfaces ge-0/0/3 unit 200 family inet address 172.16.10.1/30
set interfaces ge-0/0/3 vlan-tagging
set interfaces ge-0/0/3 unit 200 family inet address 172.16.20.1/30
set interfaces ge-0/0/47 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan10
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan11
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan12
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan21
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan20
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan22
set interfaces ge-0/0/47 unit 0 family ethernet-switching vlan members vlan500
set interfaces xe-1/0/1 unit 0 family ethernet-switching port-mode trunk
set interfaces xe-1/0/1 unit 0 family ethernet-switching vlan members vlan10
set interfaces xe-1/0/1 unit 0 family ethernet-switching vlan members vlan11
set interfaces xe-1/0/1 unit 0 family ethernet-switching vlan members vlan12
set interfaces xe-1/0/2 unit 0 family ethernet-switching port-mode trunk
set interfaces xe-1/0/2 unit 0 family ethernet-switching vlan members vlan20
set interfaces xe-1/0/2 unit 0 family ethernet-switching vlan members vlan21
set interfaces xe-1/0/2 unit 0 family ethernet-switching vlan members vlan22
set interfaces xe-1/0/3 unit 0 family ethernet-switching port-mode trunk
set interfaces xe-1/0/3 unit 0 family ethernet-switching vlan members vlan500
set interfaces lo0 unit 0 family inet address 172.16.127.127/32
set interfaces vlan 500 family inet address 172.16.30.1/24
```

Routing Protocol Configuration:

```plaintext
set protocols ospf area 0.0.0.0 interface ge-0/0/2.100
set protocols ospf area 0.0.0.0 interface ge-0/0/3.200
set protocols ospf area 0.0.0.1 interface vlan.500
set vlans vlan10 vlan-id 10
set vlans vlan100 vlan-id 100
set vlans vlan11 vlan-id 11
set vlans vlan12 vlan-id 12
set vlans vlan20 vlan-id 20
set vlans vlan200 vlan-id 200
set vlans vlan21 vlan-id 21
set vlans vlan22 vlan-id 22
set vlans vlan500 vlan-id 500
set vlans vlan500 l3-interface vlan.500
```
3. Active/Active Firewall Cluster Deployment with Active/Active Data Center Network Infrastructure

This active/active network infrastructure with an active/active firewall cluster configuration is tested with the MX960 Ethernet Services Router as a collapsed aggregation/core layer data center network design with VLANs terminating at the MX960 using virtual routers. See Figure 10.

**NOTE:** The same design principles can be applied to any previously discussed data center network architecture, or the previously discussed deployment can be supported on the collapsed tier data center network design.

![Diagram of Active/Active Firewall Cluster Deployment](image)

**Figure 10:** Active/active firewall cluster deployment with active/active data center network infrastructure

VLAN 10, 11, and 12 terminate on the virtual routing instance VR-10, and inter VLAN routing between these VLANs does not go through firewall services. Similarly, VLAN 20, 21, and 22 terminate on virtual routing instance VR-20.

**VR-10** on both MX960 routers are interconnected using the integrated routing and bridging (IRB) interface on VLAN 110, which also extends to the SRX Series chassis cluster. **VR-20** on both MX960s are interconnected using the IRB interface on VLAN 120, which also extends to the SRX Series chassis cluster.

The MX960 is also configured using virtual routing instance Core-VR for uplink connections, and it is connected to the SRX Series using IRB interfaces VLAN 500 and VLAN 600.
On the SRX Series chassis cluster, two redundancy groups are configured. The redundancy group 1 contains redundant Ethernet interface 1 and is active on node 0 (SRX Series located on left side), as node priority is set lower for redundancy group 1. Logical interface 110 and 500 are configured on redundant interface 1 for connection to VR-10 and core-VR on both MX960 devices. The passive interface for reth1 is on node 0 (SRX Series located on right side).

Similarly, the redundancy group 2 contains redundant Ethernet interface 1 and is active on node 1 (SRX Series located on right side) as node priority is set lower for redundancy group 2. Logical interface 120 and 600 are configured on redundant interface 2 for connection to VR-20 and core-VR on both MX960 devices. The passive interface for reth2 is on node 0 (SRX Series located on left side).

With this configuration, both SRX Series nodes in the chassis cluster are forwarding traffic for different access tier network segments, so inter VLAN traffic for such segments (example VLAN 10 to VLAN 20) will be forwarded over the fabric link between both SRX Series nodes. Hence, latency can be higher when compared to other firewall cluster deployment options considered earlier.

Below are the chassis cluster configuration details for reference.

Redundancy Group Configuration:

```
set chassis cluster redundancy-group 2 node 0 priority 10
set chassis cluster redundancy-group 2 node 1 priority 254
set chassis cluster redundancy-group 2 preempt
set chassis cluster redundancy-group 2 interface-monitor xe-3/2/0 weight 255
set chassis cluster redundancy-group 2 interface-monitor xe-9/2/0 weight 255
set chassis cluster redundancy-group 1 node 0 priority 254
set chassis cluster redundancy-group 1 node 1 priority 10
set chassis cluster redundancy-group 1 preempt
set chassis cluster redundancy-group 1 interface-monitor xe-3/1/0 weight 255
set chassis cluster redundancy-group 1 interface-monitor xe-9/1/0 weight 255
set interfaces xe-3/1/0 gigether-options redundant-parent reth1
set interfaces xe-3/2/0 gigether-options redundant-parent reth2
set interfaces xe-9/1/0 gigether-options redundant-parent reth1
set interfaces xe-9/2/0 gigether-options redundant-parent reth2
```

Logical Interface Configuration:

```
set interfaces reth1 VLAN-tagging
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 110 VLAN-id 110
set interfaces reth1 unit 110 family inet address 172.18.10.4/24
set interfaces reth1 unit 500 VLAN-id 500
set interfaces reth1 unit 500 family inet address 172.20.10.4/24
set interfaces reth2 VLAN-tagging
set interfaces reth2 redundant-ether-options redundancy-group 2
set interfaces reth2 unit 120 VLAN-id 120
set interfaces reth2 unit 120 family inet address 172.19.10.4/24
set interfaces reth2 unit 600 VLAN-id 600
set interfaces reth2 unit 600 family inet address 172.21.10.4/24
```

Security Zone Configuration:

```
set security zones security-zone zone-10 interfaces reth1.110
set security zones security-zone uplink host-inbound-traffic system-services ping
set security zones security-zone uplink host-inbound-traffic host-inbound-traffic protocols ospf
set security zones security-zone uplink interfaces reth1.500
set security zones security-zone uplink interfaces reth2.600
set security zones security-zone zone-20 interfaces reth2.120
```
## MX960 Collapsed Aggregation/Core Tier Device Configuration with Virtual Routers--Interface Configuration:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Flexible VLAN Tagging</th>
<th>Encapsulation</th>
<th>VLAN Bridge</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/5</td>
<td>flexible-vlan-tagging</td>
<td>flexible-ethernet-services</td>
<td>vlan-bridge</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 10</td>
<td>vlan-id 10</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 11</td>
<td>vlan-id 11</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 12</td>
<td>vlan-id 12</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 20</td>
<td>vlan-id 20</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 21</td>
<td>vlan-id 21</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 22</td>
<td>vlan-id 22</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 110</td>
<td>vlan-id 110</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 120</td>
<td>vlan-id 120</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 500</td>
<td>vlan-id 500</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 600</td>
<td>vlan-id 600</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 10</td>
<td>vlan-id 10</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 11</td>
<td>vlan-id 11</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 12</td>
<td>vlan-id 12</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 20</td>
<td>vlan-id 20</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 21</td>
<td>vlan-id 21</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 22</td>
<td>vlan-id 22</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 110</td>
<td>vlan-id 110</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 500</td>
<td>vlan-id 500</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td></td>
<td>unit 600</td>
<td>vlan-id 600</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td>flexible-vlan-tagging</td>
<td>flexible-ethernet-services</td>
<td>vlan-bridge</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td></td>
<td>unit 10</td>
<td>vlan-id 10</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td></td>
<td>unit 11</td>
<td>vlan-id 11</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td></td>
<td>unit 12</td>
<td>vlan-id 12</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td></td>
<td>unit 20</td>
<td>vlan-id 20</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td></td>
<td>unit 21</td>
<td>vlan-id 21</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td></td>
<td>unit 22</td>
<td>vlan-id 22</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td></td>
<td>unit 110</td>
<td>vlan-id 110</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td></td>
<td>unit 500</td>
<td>vlan-id 500</td>
<td></td>
</tr>
<tr>
<td>xe-1/0/0</td>
<td>flexible-vlan-tagging</td>
<td>flexible-ethernet-services</td>
<td>vlan-bridge</td>
<td></td>
</tr>
<tr>
<td>xe-1/0/0</td>
<td></td>
<td>unit 110</td>
<td>vlan-id 110</td>
<td></td>
</tr>
<tr>
<td>xe-1/0/0</td>
<td></td>
<td>unit 500</td>
<td>vlan-id 500</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>set interfaces xe-1/1/0 flexible-vlan-tagging</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>set interfaces xe-1/1/0 encapsulation flexible-ethernet-services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>set interfaces xe-1/1/0 unit 120 encapsulation vlan-bridge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>set interfaces xe-1/1/0 unit 120 vlan-id 120</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>set interfaces xe-1/1/0 unit 600 encapsulation vlan-bridge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>set interfaces xe-1/1/0 unit 600 vlan-id 600</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Integrated Routing and Bridging Interface Configuration:**

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>set interfaces irb unit 10 family inet address 10.10.0.2/24 vrrp-group 0 virtual-address 10.10.0.1</td>
</tr>
<tr>
<td>set interfaces irb unit 10 family inet address 10.10.0.2/24 vrrp-group 0 priority 200</td>
</tr>
<tr>
<td>set interfaces irb unit 10 family inet address 10.10.0.2/24 vrrp-group 0 accept-data</td>
</tr>
<tr>
<td>set interfaces irb unit 11 family inet address 10.11.0.2/24 vrrp-group 0 virtual-address 10.11.0.1</td>
</tr>
<tr>
<td>set interfaces irb unit 11 family inet address 10.11.0.2/24 vrrp-group 0 priority 200</td>
</tr>
<tr>
<td>set interfaces irb unit 11 family inet address 10.11.0.2/24 vrrp-group 0 accept-data</td>
</tr>
<tr>
<td>set interfaces irb unit 12 family inet address 10.12.0.2/24 vrrp-group 0 virtual-address 10.12.0.1</td>
</tr>
<tr>
<td>set interfaces irb unit 12 family inet address 10.12.0.2/24 vrrp-group 0 priority 200</td>
</tr>
<tr>
<td>set interfaces irb unit 12 family inet address 10.12.0.2/24 vrrp-group 0 accept-data</td>
</tr>
<tr>
<td>set interfaces irb unit 20 family inet address 10.20.0.2/24 vrrp-group 0 virtual-address 10.20.0.1</td>
</tr>
<tr>
<td>set interfaces irb unit 20 family inet address 10.20.0.2/24 vrrp-group 0 priority 200</td>
</tr>
<tr>
<td>set interfaces irb unit 20 family inet address 10.20.0.2/24 vrrp-group 0 accept-data</td>
</tr>
<tr>
<td>set interfaces irb unit 21 family inet address 10.21.0.2/24 vrrp-group 0 virtual-address 10.21.0.1</td>
</tr>
<tr>
<td>set interfaces irb unit 21 family inet address 10.21.0.2/24 vrrp-group 0 priority 210</td>
</tr>
<tr>
<td>set interfaces irb unit 21 family inet address 10.21.0.2/24 vrrp-group 0 accept-data</td>
</tr>
<tr>
<td>set interfaces irb unit 22 family inet address 10.22.0.2/24 vrrp-group 0 virtual-address 10.22.0.1</td>
</tr>
<tr>
<td>set interfaces irb unit 22 family inet address 10.22.0.2/24 vrrp-group 0 priority 220</td>
</tr>
<tr>
<td>set interfaces irb unit 22 family inet address 10.22.0.2/24 vrrp-group 0 accept-data</td>
</tr>
<tr>
<td>set interfaces irb unit 110 family inet address 172.18.10.2/24</td>
</tr>
<tr>
<td>set interfaces irb unit 120 family inet address 172.19.10.2/24</td>
</tr>
<tr>
<td>set interfaces irb unit 500 family inet address 172.20.10.2/24</td>
</tr>
<tr>
<td>set interfaces irb unit 600 family inet address 172.21.10.2/24</td>
</tr>
</tbody>
</table>
Virtual Router Configuration:

```
set routing-instances VR-TEN instance-type virtual-router
set routing-instances VR-TEN interface irb.10
set routing-instances VR-TEN interface irb.11
set routing-instances VR-TEN interface irb.12
set routing-instances VR-TEN interface irb.110
set routing-instances VR-TEN protocols ospf area 0.0.0.0 interface all
set routing-instances VR-TWENTY instance-type virtual-router
set routing-instances VR-TWENTY interface irb.20
set routing-instances VR-TWENTY interface irb.21
set routing-instances VR-TWENTY interface irb.22
set routing-instances VR-TWENTY interface irb.120
set routing-instances VR-TWENTY protocols ospf area 0.0.0.0 interface all
set routing-instances core instance-type virtual-router
set routing-instances core interface ge-0/0/2.100
set routing-instances core interface ge-0/0/3.200
set routing-instances core interface irb.500
set routing-instances core interface irb.600
set routing-instances core protocols ospf area 0.0.0.0 interface all
```

Bridge Domain Configuration:

```
set bridge-domains VLAN10 domain-type bridge
set bridge-domains VLAN10 vlan-id 10
set bridge-domains VLAN10 interface ge-0/1/0.10
set bridge-domains VLAN10 interface ge-0/0/5.10
set bridge-domains VLAN10 interface ge-0/1/1.10
set bridge-domains VLAN10 routing-interface irb.10
set bridge-domains VLAN11 domain-type bridge
set bridge-domains VLAN11 vlan-id 11
set bridge-domains VLAN11 interface ge-0/1/0.11
set bridge-domains VLAN11 interface ge-0/0/5.11
set bridge-domains VLAN11 interface ge-0/1/1.11
set bridge-domains VLAN11 routing-interface irb.11
set bridge-domains VLAN110 domain-type bridge
set bridge-domains VLAN110 vlan-id 110
set bridge-domains VLAN110 interface ge-0/0/5.110
set bridge-domains VLAN110 interface xe-1/0/0.110
set bridge-domains VLAN110 routing-interface irb.110
set bridge-domains VLAN12 domain-type bridge
set bridge-domains VLAN12 vlan-id 12
set bridge-domains VLAN12 interface ge-0/1/0.12
set bridge-domains VLAN12 interface ge-0/0/5.12
set bridge-domains VLAN12 interface ge-0/1/1.12
set bridge-domains VLAN12 routing-interface irb.12
set bridge-domains VLAN120 domain-type bridge
set bridge-domains VLAN120 vlan-id 120
set bridge-domains VLAN120 interface ge-0/0/5.120
set bridge-domains VLAN120 interface xe-1/1/0.120
set bridge-domains VLAN120 routing-interface irb.120
set bridge-domains VLAN20 domain-type bridge
set bridge-domains VLAN20 vlan-id 20
set bridge-domains VLAN20 interface ge-0/1/0.20
set bridge-domains VLAN20 interface ge-0/1/1.20
set bridge-domains VLAN20 interface ge-0/0/5.20
set bridge-domains VLAN20 routing-interface irb.20
set bridge-domains VLAN21 domain-type bridge
```
Validation Testing and Convergence Testing

The designs listed above have been validated using full mesh access and core tier communication, as well as convergence testing which was performed for the following traffic flows to test high resiliency and availability for firewall deployment.

- Traffic between access tier VLAN-10 and access tier VLAN-20
- Traffic between access tier VLAN-10 and access tier VLAN-11
- Traffic between access tier VLAN-10 and core uplinks
- Traffic between access tier VLAN-20 and core uplinks

The following failure scenarios have been tested for full convergence of the network:

- Access to aggregation link failure
- Aggregation to active SRX Series link failure
- Active SRX Series device failure
- One aggregation device failure
- SRX Series chassis cluster control link failure
- SRX Series chassis cluster fabric link failure

For more details on configuration and convergence test results, please contact your local Juniper account representative.
Summary

In this document, we have explored the different options for integrating a high-speed firewall into the data center network. Essentially, the data center network presents multiple firewall integration points and possibilities for seamlessly fitting into specific customer environments. We have learned that state is the most challenging characteristic of firewall integration that must be addressed through network integration.

The different options for firewall integration primarily discussed include:

- Physical inline in which the firewall physically connects between two different data center network tiers. In this design, the flexibility to specify which traffic passes through a stateful firewall is diminished. However, network integration is fairly straightforward.

- Logical inline where the forwarding domains are separated in the device to which the firewall attaches (L2 VLANs or L3 virtual routers), and effectively the firewall connects the different forwarding domains statefully. With this option, it is easier to bypass the firewall using an explicit filter-based forwarding statement that allows traffic to be routed/switched directly between separate forwarding domains.

Regardless of the deployment model, the need for a high-speed, low latency, service-ready firewall system in the data center is paramount. More data centers are consolidating, and as more applications are being hosted within these data centers and as more complex traffic patterns in the data center evolve, more security and less compromise are required. Juniper Networks SRX5000 line offers purpose-built systems that are data center ready and are architected to support the data centers of today, as well as fulfill specific and individual customer requirements as your data center network transitions into the future.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.