White Paper

EXTENDING JUNIPER CONNECTED SECURITY TO CONTAINERS

How cSRX Protects Workloads Running in Containers

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Network and security administrators today are challenged to manage and secure a mix of physical and virtual form-factor appliances in their networks, which span on-premises and public cloud environments.

Adding to the complexity of the network is the introduction of containers. If organizations are already struggling with deploying and managing a large number of security solutions for each part of the network and now need a new or additional solution to secure containers, it's up to the staff to shoulder the burden.

With Juniper Networks® cSRX Container Firewall, extending security to workloads running in containers is just another benefit provided by Juniper Connected Security that safeguards users, applications, and cloud workloads to all connection points throughout the network. The cSRX finds applicability in use cases such as microsegmentation that provides threat detection for east-west traffic within a Kubernetes cluster. Other use cases include deployment as an application protection gateway for north-south traffic; this provides the ability to control the applications that are allowed to interact with the apps running in the container.

To simplify security management, Junos Space® Security Director provides a single pane of glass view that enables uniform policy enforcement across physical, virtual, and container security. While the cSRX secures workloads in a container form factor, it was built to take advantage of the benefits of containers: lightweight and fast, taking less than a minute to boot-up, service, and secure traffic.

This white paper explores how customers can leverage the cSRX to extend security and increase visibility to workloads running within containers. It covers the features and benefits of the cSRX and highlights use cases such as microsegmentation and providing additional application protection. In addition, cSRX is based on the Junos® operating system, so customers already familiar with Juniper Networks SRX Series Services Gateways hardware or virtual appliances can extend that same security to containers, reducing complexity and risk.

Introduction

Application and service delivery has evolved over the past few decades. As software architectures have changed from monolithic to modular, the form factor of the mode of delivery has followed a similar trend, moving from physical to virtual to containers. Since their introduction in the early 2010s, containers have captured the imagination of IT professionals and developers around the globe because they are:

- Portable across hosts
- Lightweight
- Provide quick boot times

Containers inherit these properties because they abstract the operating system (OS) that they run on. Whereas virtual machines (VMs) package the entire OS for porting applications across different platforms, containers use the common kernel parameters of the underlying OS wherever necessary. Container images package only the essential files needed by the application to operate, making them much smaller than the images that package VMs.

As workloads migrate from VMs to containers, security threats follow. External known and unknown threats that may exploit a weakness in an application are still a challenge, even with containers. These application weaknesses can be exploited by malware, which spreads through lateral propagation and provides unauthorized access to applications running within the containers.

Looking at the network side of things, due to digital initiatives and greater reliance on the cloud, modern network architectures are complex, diverse, and multifaceted, consisting of physical, virtual, and container workloads spread across multiple geographies. Increasingly, networks have the added complexity of being hosted in multiple clouds ranging from on-premises to different Infrastructure as a Service (IaaS) providers, often protected by similarly disparate and dispersed security solutions. Enterprises today have many security solutions; in the case of large enterprises, they could number in the thousands. While security spending is increasing to counter the evolving threat landscape, a single comprehensive and consistent security policy enforcement mechanism is missing. The situation has gotten worse with the advent of workloads running in containers.

Trends in the way applications are delivered through the cloud and in network evolution have led to a need for security solutions that protect workloads within containers and are easy to automate and deploy. Such a solution must address existing security challenges such as:

1. **Lack of visibility across the network**: IT professionals struggle with a lack of visibility into threats within their networks. There are many reasons for this, but as is often the case with different security solutions for different parts of the network, intelligence regarding malicious network threats is not shared and therefore goes undetected. Hidden blind spots in the network abound, and network security engineers have a tough time reconciling information from the multitude of security solutions.

2. **Inconsistent policy enforcement**: Isolated security functions result in gaps when attempting to enforce a consistent security policy across the network. In today's complex and hybrid networks, physical, virtual, and container workloads coexist, and inconsistent policy enforcement leads to less effective security, resulting in greater risk.

3. **Multiple management applications**: With distinct security solutions for separate networks, including virtual workloads or containers across the network or cloud, IT professionals must deal with multiple unique management applications to configure and monitor the various security solutions. This rapidly devolves into missing security alerts and a lack of context for identifying and stopping threats due to manual consolidation efforts of threat log correlation and console fatigue.

Juniper Connected Security

At Juniper, we believe that for security to be effective, it must be built into the network and not added as an afterthought. Juniper Connected Security addresses these challenges with the powerful tenets of see, automate, and protect.

- Junos Space Security Director extends visibility and creates unified policies that can be applied across connection points throughout the network and cloud. With Policy Enforcer, a component within Security Director, policy enforcement on multivendor network elements becomes a reality. The feed collector consolidates threat intelligence from different sources, both internal and external. A single pane of glass can monitor and manage physical, virtual, and containerized SRX Series firewalls to ensure consistent policy enforcement across all points of the network.
- SRX Series firewalls provide feature-rich next-generation firewall (NGFW) capabilities that include Juniper Networks AppSec, intrusion prevention system (IPS), and Juniper Advanced Threat Prevention. The SRX Series devices come in multiple form factors—physical, virtual, and container—to ensure that all points of the network can be secured and there are no blind spots.
- Security policy automation is made possible through a rich set of APIs, allowing for configuration and monitoring of the SRX Series firewalls, in addition to offering full CLI or local GUI. Using Juniper Advanced Threat Prevention Cloud or Policy Enforcer, SRX Series firewall threat intelligence feeds can be updated with threat data from Juniper Threat Labs, or third-party threat data can be added. Network Configuration Protocol (NETCONF) support is available across all SRX Series products, including the cSRX, providing an additional tool for automating deployment and configuration. When deployed in Kubernetes orchestration environments, the cSRX supports native constructs such as ConfigMap that provide the ability to load predefined configurations, enabling the rapid instantiation of the cSRX.

The cSRX offers NGFW capabilities that include AppSec, IDP/IPS, and UserFW, along with deployment modes that support either secure wire or static route forwarding modes. During launch time, cSRX can be configured with environmental variables that include core affinity, forwarding modes, size, and number of ports. These environmental variables provide configuration flexibility to suit the use case and deployment scenarios. For a complete list of these variables, please refer to the cSRX deployment guide documentation.

Being in a container form factor, the cSRX has many advantages.

1. It is based on the award-winning Junos OS, retaining only the security and management components needed to be effective against the latest known and unknown threats that may affect applications running in containers.
2. It provides quick boot time; once container resources are available, the cSRX is able to instantiate in less than a minute to secure workloads.
3. It is lightweight and portable; the size of the cSRX image is only a few hundred megabytes, making it easy to port across hosts.
4. It will run on any standard Linux or Docker host with sufficient resources to launch the cSRX. Utilizing Docker bridges or MacVLAN networking, the cSRX will be ready to service and transit traffic in less than a minute.

Use Cases

Microsegmentation

As networks grow more complex, network admins segment the network based on either the servers or applications that are deployed. Using the ability of the Multus CNI to create multiple interfaces in a container deployed in Kubernetes, the cSRX can be used as an east-west firewall between different network segments. The cSRX can support up to 15 revenue interfaces when specified at instantiation; the containerized NGFW can effectively protect the network from lateral threat propagation and restrict access to certain sections of the network based on policies. Support for Dynamic Address Groups means that tag-based policies can be applied through Security Director. All of this in addition to the NGFW features brings true L7 firewalling capabilities to the container deployments in a Kubernetes environment. Table 1 lists other key features that make the cSRX an ideal choice for the microsegmentation use case.

Table 1. Features and Benefits

Feature	Feature Description	Benefit
Dynamic address allocation to network interfaces at boot-up	Boots up with the ease of a variable passed at instantiation using the IP addresses configured to the ge-0/0/x interfaces once the network-attachment-definitions have been created in Kubernetes.	The allocation of IP addresses be-comes seamless for administrators to implement, freeing them up to focus on other important tasks.
Self-registration with Juniper Security Director	Allows the cSRX to self-register with Juniper Security Director and in-cludes all the environmental varia-bles set during instantiation.	Instant security management of the cSRX from instantiation en-sures consistent security posture to all SRX Series firewalls across the network and cloud infrastructure.
Support for ConfigMap con-struct in Kubernetes	Ensures the cSRX can boot up with a predefined configuration and appropriate licenses.	The cSRX is ready to go as soon as it is deployed, providing a level of automation that is as easy as it gets.
Predefined signature package installation	Provides the ability for the cSRX to be deployed with AppID and IDP/IPS signatures as a predefined package during instantiation.	Zero-hour protection starts as soon as the cSRX is deployed, re-ducing the time required to down-load and install the signature pack for every cSRX instantiation across containers.

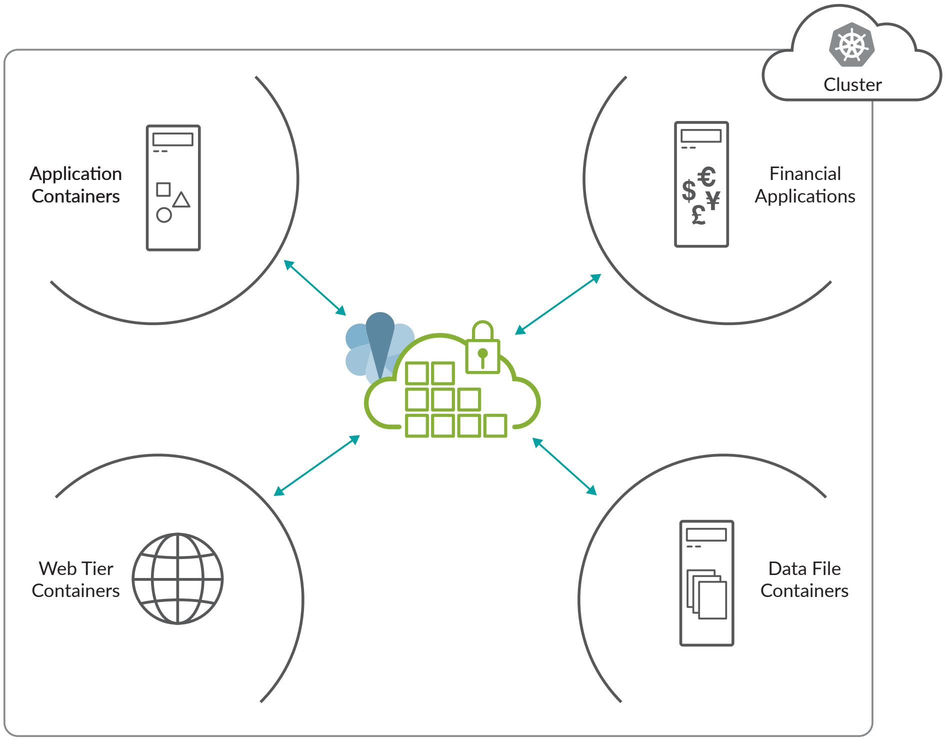

Figure 1: Microsegmentation

Figure 1 shows a typical scenario where the network has been divided into four segments: Financial, Applications, Web Tier, and Data File Containers. The cSRX can be configured with policies to prevent access to the financial applications from any other network segment. Similarly, the web-tier segment can only receive traffic and not initiate a connection to the Internet from the Web Tier container. Only the application servers are allowed to access the data store container. These policies can be preconfigured on the cSRX at launch time, configured using Security Director or on the cSRX via the CLI.

Application Protection

The cSRX uses standard Kubernetes APIs to deploy in the Kubernetes cluster and leverages Kubernetes tools to monitor status, upgrade image, and scale up/down according to performance requirements. Working with the Nginx Ingress Controller and Ingress object in Kubernetes, the cSRX can be deployed as an application protection gateway in the scenario shown in Figure 2. Using the replica-sets constructs in Kubernetes, the cSRX can be seamlessly scaled up or down based on the load.

The ingress object in Kubernetes works with the Nginx ingress controller to load-balance incoming traffic to multiple cSRX containerized firewalls exposed as a service. The cSRX instances perform Source Network Address Translation (SNAT), ensuring that session stickiness is maintained for the reverse traffic. The traffic is routed to the cSRX interface, such as ge-0/0/0, which is then forwarded to the Web application service after Layer 7 advanced service processing. This use case relies on many Kubernetes tools working seamlessly with the cSRX to ensure that the correct interface, such as ge-0/0/0, receives the traffic from the Internet. Junos Space Security Director can be deployed for visibility and management of the cSRXs on instantiation.

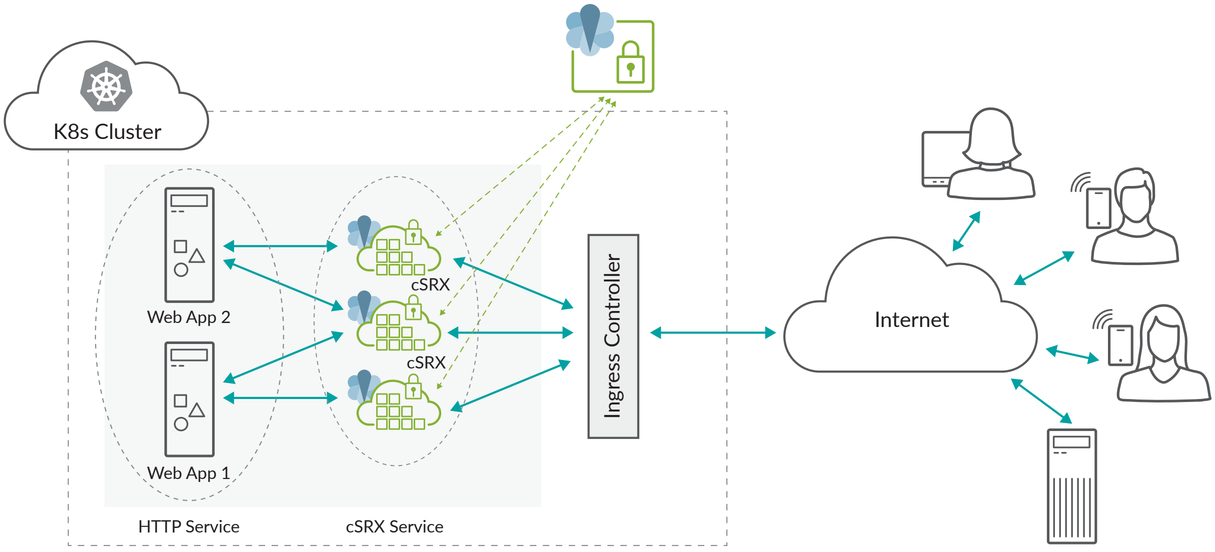

Figure 2: Application protection in north-south direction

Juniper Connected Security with cSRX

In a typical enterprise network consisting of layers such as the perimeter NGFW, aggregate switches, and access layer switches, Juniper Connected Security enables complete end-to-end visibility and policy enforcement across all points of the network and cloud, managed by a single pane of glass. In Figure 3, the components that make up a consolidated, single security solution come together to mitigate threats originating from the Internet.

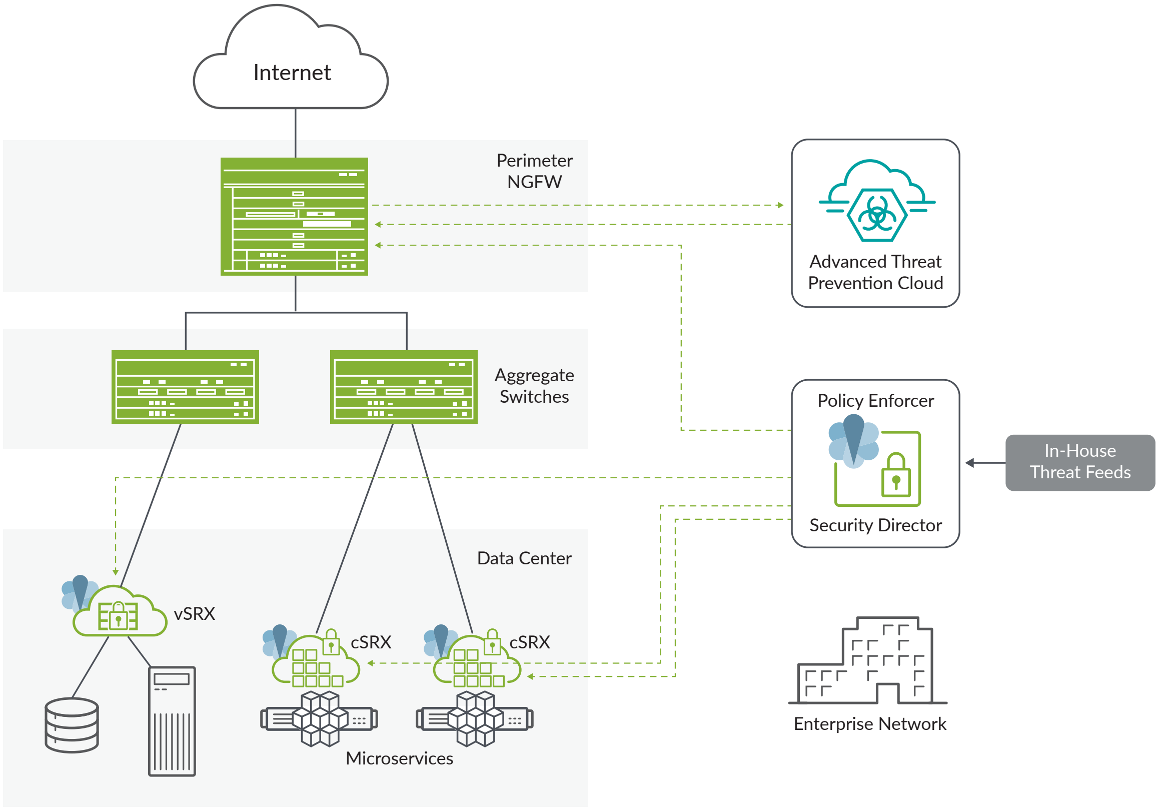

Figure 3: Juniper Connected Security extended to the cSRX

In the enterprise network, there is a high-end SRX Series perimeter NGFW, along with Juniper Networks EX Series Ethernet Switches in the aggregate and access layer. The data center deployments are secured with the Juniper Networks vSRX Virtual Firewall for workloads running in virtual form factors, and with the cSRX for workloads running in containers. The cSRX can be employed as an east-west firewall for the microservices being implemented. This network depicts a common scenario today with hybrid workloads, users, and applications all housed within an organization.

Let's take a look at a situation where Juniper Advanced Threat Prevention Cloud receives files being downloaded by a user which are sent to it by the perimeter NGFW. The Advanced Threat Prevention engine uses dynamic and static analysis, among other techniques, to determine if something malicious is hidden in the file. If a threat is detected, the metadata and IP address of the origin of the malicious file is passed on to the feed collector component in Policy Enforcer, which can also receive threat data from other sources, including Juniper Secure Analytics. This threat information allows Policy Enforcer to implement changes that can quarantine the affected user or device at the access switch and configure uniform policies to block lateral threat propagation across SRX Series firewalls deployed at the perimeter and in the data center, including the vSRX. Policy Enforcer also works with third-party network devices, ensuring that the enterprise network is protected across all connection points, safeguarding users, applications, and workloads everywhere.

Conclusion

For network security professionals faced with a lack of visibility, inconsistent policy application, and wariness with pursuing yet another security solution for securing container workloads, the capabilities of the cSRX coupled with the power of Juniper Connected Security provides visibility into network threats, consistent policies across the network, and NGFW capabilities into the container domain.

Learn more about the power of Juniper Connected Security at www.juniper.net/us/en/solutions/security/.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable, and secure networks to move at the speed of business.

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: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPER NETWORKS | **Engineering** Simplicity