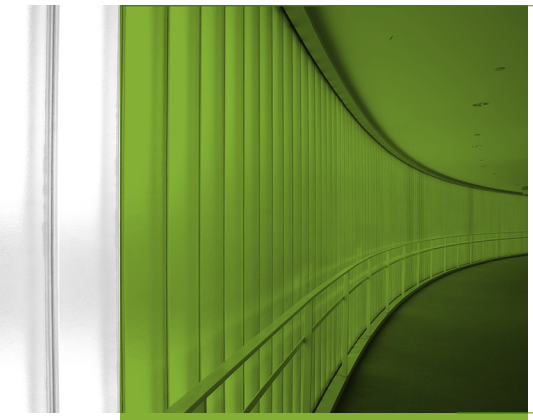

vSRX VIRTUAL FIREWALL WITH AWS SECURITY HUB

Enhance threat protection by exporting Juniper security findings to Amazon Web Services Security Hub

Challenge

With many workloads residing in Amazon Web Services (AWS), organizations have difficulty understanding the full spectrum of security threats across their accounts. Correlating and consolidating the security findings from Juniper Connected Security with other security alerts is essential to threat protection.

Solution

The vSRX Virtual Firewall deployed in AWS exports security findings to AWS Security Hub. Network administrators gain a single view of all security findings from their deployments across AWS.

Benefits

- *Easily imports findings from the vSRX to AWS Security Hub*
- *Combines centralized firewall and policy management*
- *Enables a consolidated view of security events across the network*
- *Strengthens security posture for AWS workloads*

Many organizations have workloads in a public cloud like AWS, and they struggle to correlate security events from multiple accounts and virtual private clouds (VPCs). AWS Security Hub provides a single view of these security events to help organizations better understand dangerous threats and attacks. To further improve security visibility, Juniper has integrated Juniper Networks® vSRX Virtual Firewall with the AWS Security Hub, enabling Juniper and AWS customers to access a broader range of security findings and take appropriate action to reverse or prevent incoming threats. With a few commands in the CLI or clicks on the Management UI of the vSRX, organizations can easily export security findings directly into AWS Security Hub for a quick response.

The Challenge

Organizations with workloads in AWS rely on AWS Security Hub to correlate and consolidate security events from across their AWS deployments. When the events are collected in one platform, security actions can be automated and appropriate actions can be taken on reported events. Juniper Networks vSRX Virtual Firewall provides a range of security findings in AWS environments that can now be shared with AWS Security Hub.

These security findings can be events ranging from traffic control profile (TCP), UDP attacks, blocked Web requests, distributed denial of service (DDoS) attacks, and many more. The vSRX reports these attack events in the security logs on the device and, if configured, on the Security Director logging console. These logs can also be exported to any third-party log collection device for analysis in either system logs or structured system logging formats.

The Juniper Networks vSRX Virtual Firewall with AWS Security Hub

Organizations are steadily moving more of their workloads onto AWS. With more virtual machines, databases, applications, and code in AWS, protecting these resources is becoming more complicated. AWS Security Hub provides a comprehensive view of security threats to these critical resources. The vSRX Virtual Firewall is expanding the AWS Security Hub knowledge base by providing built-in integration that imports security findings from vSRX to the AWS Security Hub.

With the integration of vSRX and AWS Security Hub, organizations can automate their responses to network threats and take the necessary actions to secure their networks. Organizations can add security reports to the AWS Security Hub that address workload protection, secure connectivity from on premises/private cloud to AWS, manage network segmentation, and secure SD-WAN.

Features and Benefits

- **Built-in Integration**. With the implementation of a new cloud agent daemon in the vSRX, the integration with AWS Security Hub is seamless for the end user. Using a simple configuration, the vSRX imports the security findings to Security Hub in structured system log formats.
- **Integration with Amazon CloudWatch**. The cloud agent daemon in the vSRX acts as a single resource for interacting with AWS services such as Amazon CloudWatch. Metrics such as input/output bytes, CPU utilization, and other valuable metrics can now be exported to Amazon CloudWatch for event-based automated actions by administrators. In addition, logs from the vSRX are sent to CloudWatch logs.
- **Easy to Deploy**. Deploying vSRX on AWS is readily available using Cloud Formation Templates, and the integration with Security Hub is seamless. After entering only a few configuration commands on the vSRX, security findings from the vSRX will appear in the AWS Security Hub.

Solution Components

The vSRX provides advanced security and VPN features that allow network and security administrators to quickly and efficiently provision firewall protection and scale VPNs to meet the dynamic needs of cloud environments. By combining the vSRX with Security Director or Contrail® Service Orchestration, administrators can significantly improve policy configuration, management, and visibility into both physical and virtual assets from a common, centralized platform. With the integration of the vSRX and AWS Security Hub, network administrators have another platform with a richer set of security findings that provide visibility into any security event threatening their workload deployment.

To enable the vSRX to import security alerts into the Security Hub, a cloud agent process (daemon) runs within the vSRX. This daemon is responsible for collecting all the security log events and forwarding them to the AWS Security Hub at preconfigured intervals. Many different security events are logged and enabled for import to Security Hub. The alerts are broadly classified into these categories:

- Screens
- Intrusion detection and prevention (IDP)
- Juniper Advanced Threat Prevention Cloud
- Content security

The vSRX also sends metadata information to help identify and correlate the security alerts along with the events. The complete list of information provided includes:

- Identification
- ProductARN
- GeneratorId
- Title
- Description
- AWSAccountId
- Types
- FirstObservedAt/LastObservedAt
- CreatedAt/UpdatedAt
- Resources
- Severity
- Confidence
- Criticality

To learn more about configuring and deploying the vSRX to import events into Security Hub, please refer to the Juniper documentation.

Use Case

In the AWS Public Cloud, the vSRX addresses the following use cases:

- Workload protection
- Secure connectivity from on premises/private cloud to AWS
- Network segmentation or east-west firewall
- Secure SD-WAN

The network admin choosing the vSRX for any of these four use cases on AWS now does so with the added benefit of integrations into multiple AWS native services such as Amazon Elastic Load Balancer/Auto Scaling Group, Amazon CloudWatch Metrics and Logs, Amazon GuardDuty, and the AWS Security Hub.

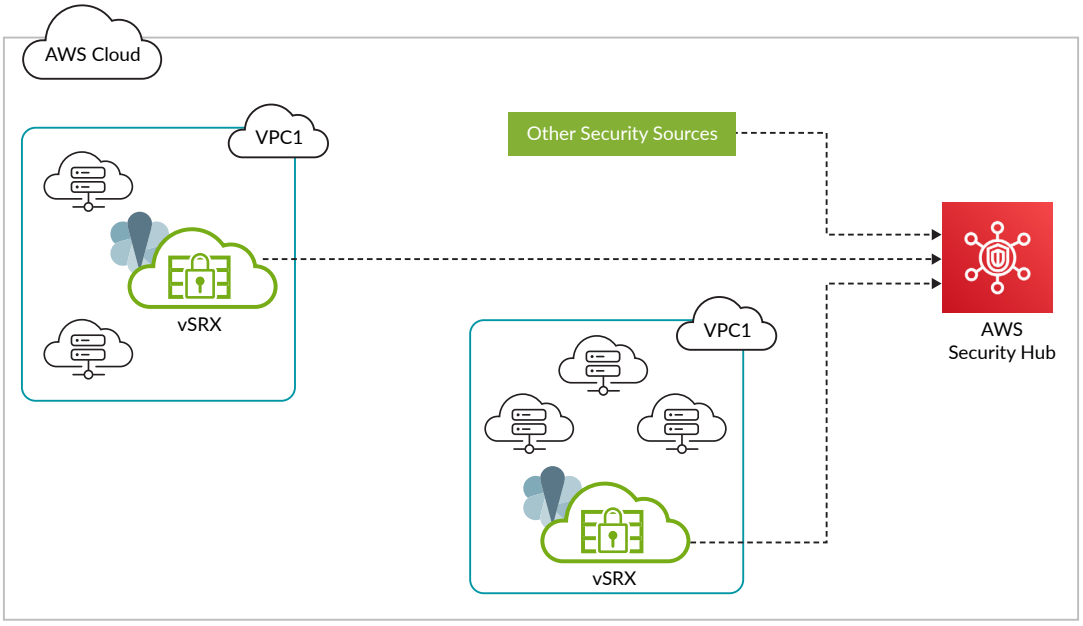

Figure 1: vSRX integrated with AWS Security Hub in an AWS deployment

Summary—vSRX/AWS Security Hub Integration Improves Security by Identifying and Correlating Security Alerts and Events in AWS

The vSRX Virtual Firewall significantly improves security posture for workloads deployed in Amazon Web Services. Deployed in a customer-defined VPC in AWS, vSRX delivers advanced security inspection not found natively on the AWS Security Hub. Working in conjunction with the AWS Security Hub, the vSRX ensures that all major security events are detected so they can be acted upon quickly—with event correlation, compliance, and automated remedial steps.

Next Steps

To learn more about Juniper security solutions, please visit us at www.juniper.net/us/en/products-services/security and contact your Juniper account representative.

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: +31.207.125.700
Fax: +31.207.125.701

JUNIPER NETWORKS | Engineering Simplicity