Engineering
Simplicity

vSRX Deployment Guide for AWS Quick Start

Published
2020-12-28

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

vSRX Deployment Guide for AWS Quick Start

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

Table of Contents

About This Guide | iv

1 vSRX Test Environment on AWS Quick Start

Overview | 2

- AWS Quick Start Overview | 2
- vSRX Overview | 3
- vSRX Architecture on AWS Quick Start | 4

2 Deploying the vSRX Virtual Appliance on AWS Quick Start

Deploying the vSRX Virtual Appliance on AWS Quick Start | 6

- Before You Deploy the vSRX Virtual Appliance on AWS Quick Start | 6
- Deploy the vSRX Virtual Appliance on AWS Quick Start | 7

3 Setting Up Attacks Using the AWS Quick Start

Setting Up Attacks Using the AWS Quick Start | 10

About This Guide

This guide describes how to deploy and test a Juniper Networks® vSRX Virtual Firewall in the AWS Quick Start environment. The guide includes vSRX configuration information to test examples related to security attacks.

After completing the deployment and examples covered in this guide, refer to the vSRX documentation for information about software features and configuration.

1

CHAPTER

vSRX Test Environment on AWS Quick Start

Overview | 2

Overview

IN THIS SECTION

- AWS Quick Start Overview | 2
- vSRX Overview | 3
- vSRX Architecture on AWS Quick Start | 4

The following topics provide more information about AWS Quick Start and vSRX.

AWS Quick Start Overview

IN THIS SECTION

- Benefits | 2

Amazon Web Services (AWS) Quick Starts enable you to deploy popular solutions on AWS, based on AWS best practices for security and high availability. These reference deployments implement key technologies automatically on the AWS Cloud, often with a single click and in less than an hour. You can build your test or production environment in a few steps, and start using it immediately. For more information about AWS Quick Starts, see frequently asked questions about AWS Quick Starts.

Benefits

When a product is provisioned on AWS Quick Start, you can test the product in a simulated environment.

vSRX Overview

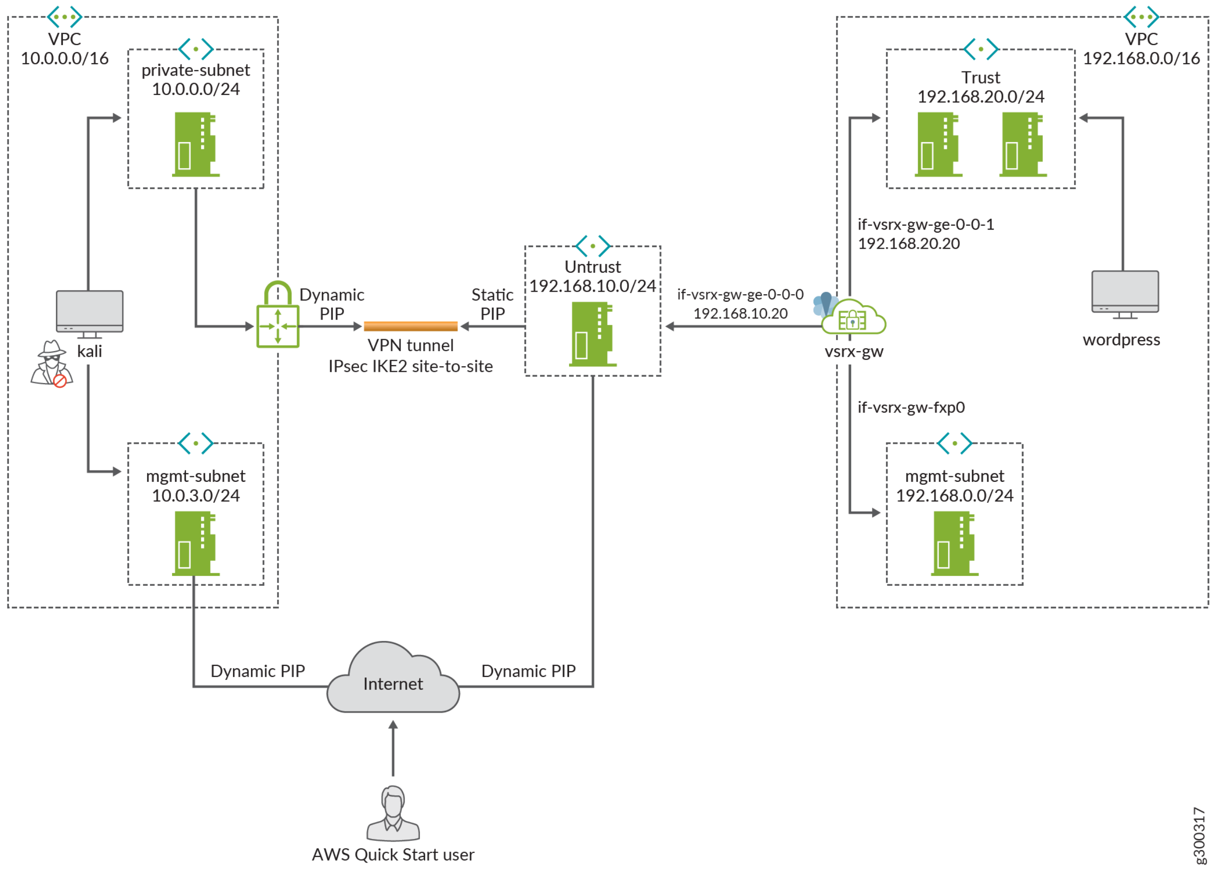
Juniper Networks vSRX Virtual Firewall is a virtual security appliance that provides security and networking services at the perimeter or edge in virtualized private or public cloud environments. vSRX runs as a virtual machine (VM) on a standard x86 server. vSRX is built on the Junos operating system (Junos OS) and delivers networking and security features similar to those available on the software releases for the SRX Series Services Gateways. For more information about vSRX, see vSRX Overview.

You can set up a vSRX virtual security appliance on AWS Quick Start. You can test the key features of the vSRX appliance in the Quick Start test environment.

vSRX Architecture on AWS Quick Start

Figure 1 on page 4 illustrates the vSRX architecture that is automatically deployed on AWS Quick Start.

Figure 1: AWS Quick Start Environment



The AWS Quick Start environment has the following two virtual private clouds (VPCs):

- The left VPC includes a Kali linux virtual machine (VM) called *kali*, which has two interfaces—one on the private subnet and the other on the management subnet that has a public IP address.
- The right VPC includes the following two VMs:
  - An Ubuntu VM with WordPress, *wordpress*.
  - A Juniper Networks vSRX virtual security appliance, *vsrx-gw*, with three interfaces—one each on the untrusted subnet, trusted subnet, and management subnet. The one on the untrusted subnet has a public IP address.

2

CHAPTER

Deploying the vSRX Virtual Appliance on AWS Quick Start

Deploying the vSRX Virtual Appliance on AWS Quick Start | 6

Deploying the vSRX Virtual Appliance on AWS Quick Start

IN THIS SECTION

- Before You Deploy the vSRX Virtual Appliance on AWS Quick Start | 6
- Deploy the vSRX Virtual Appliance on AWS Quick Start | 7

Before You Deploy the vSRX Virtual Appliance on AWS Quick Start

IN THIS SECTION

- User Credentials for VMs in the AWS Quick Start Environment | 6
- Deployment Instructions for the VMs in the Quick Start Environment | 7

You can deploy a vSRX virtual appliance directly on AWS Quick Start. Use a browser-based UI to deploy and configure virtual machines (VMs) and all related resources.

Before you deploy the vSRX virtual appliance on AWS Quick Start:

- See "vSRX Architecture on AWS Quick Start" on page 4.
- See "Deployment Instructions for the VMs in the Quick Start Environment" on page 7
- See Table 1 on page 7.

User Credentials for VMs in the AWS Quick Start Environment

Table 1 on page 7 lists the user credentials used for accessing the VMs in the AWS Quick Start environment.

Table 1: User Credentials for VMs in the Quick Start Environment?

Virtual Machine Name	Username	Password	Role
kali	ec2-user	(Private key) demoJuniper.pem	Attacker This VM launches the attack.
wordpress	ec2-user	(Private key) demoJuniper.pem	Victim This VM receives the attack.
vsrx-gw	ec2-user	(Private key) demoJuniper.pem	vSRX Appliance

NOTE: The public IP addresses required to remotely access each VM are dynamic and are provided after the Quick Start is deployed on the AWS Quick Starts website.

A file named demoJuniper.pem is available as an output and is provided after the Quick Start is deployed on the AWS Quick Starts website This file is a private key required to remotely access each VM.

Deployment Instructions for the VMs in the Quick Start Environment

To access the kali, wordpress, and vsrx-gw VMs in the Quick Start environment:

1. Open a Linux terminal console.

2. Use the following command to access each VM:

```
ssh -l ec2-user -I demoJuniper.pem public ip of the virtual machine
```

Deploy the vSRX Virtual Appliance on AWS Quick Start

To deploy the vSRX Virtual Appliance on AWS Quick Start:

1. Access the AWS Quick Starts website.

2. Select **vSRX Quickstart** from Juniper.

3. Follow the instructions to deploy the vSRX Virtual Appliance.

You have now successfully deployed the vSRX Virtual Appliance on AWS Quick Start.

After you complete deploying the vSRX Virtual Appliance, you receive a security private key, along with three public IP addresses, one for each of the following VMs:

- kali
- wordpress
- vsrx-gw

3

CHAPTER

Setting Up Attacks Using the AWS Quick Start

Setting Up Attacks Using the AWS Quick Start | 10

Setting Up Attacks Using the AWS Quick Start

IN THIS SECTION

- SQL Injection Attack | 10
- Nmap Attack | 19

As the final step in the deployment of the AWS Quick Start, you run different types of attacks on the virtual machines (VMs). You accomplish this goal by performing the following tasks:

- Set up attacks from one VM to another.
- Verify the attacks on the vSRX virtual security appliance, vsrx-gw, located before the wordpress VM.

The deployment described in this guide uses an SQL injection attack and an Nmap (Network Mapper) attack.

SQL Injection Attack

SQL injection attack is a code injection technique that inserts SQL statements in an entry field for running the attack. For more information about SQL injection, see SQL injection.

Run an SQL Injection Attack

To run an SQL injection attack:

1. Log in to the kali and vsrx-gw VMs.
2. Reset the root password on the vsrx-gw VM on first login.
   a. Enter configuration mode.

```
ec2-user@vsrx-gw> configure
```

b. Reset the root password.

```
ec2-user@vsrx-gw# set system root-authentication plain-text-password
```

```
New password:
Retype new password:
```

3. Run the attack procedure from the kali VM. At this time, no firewall policies are configured on the vsrx-gw VM.

   a. Use the following command to initiate the SQL injection attack:

```
[ec2-user@ip-10-0-0-64 /]$sqlmap -u http://192.168.20.166/index.php?id=1--dbs --risk=3 --
level=5
```

NOTE: The private IP address for this command is provided at the end of the Quick Start deployment.

   b. Type **Y** and press **Enter**.

```
[ec2-user@ip-10-0-0-64 /]$ sqlmap -u http://192.168.20.166/index.php?id=1--
dbs --risk=3 --level=5

         _
 ___ ___| |_____ ___ ___ {1.0.4.0#dev}
|_ -| . | | | .’| . | . |
|___|_  |_|_|_|_|__,| _ |
      |_|           |_|   http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior
mutual consent is illegal. It is the end user’s responsibility to obey all
applicable local, state and federal laws. Developers assume no liability
and are not responsible for any misuse or damage caused by this program

[*] starting at 15:20:23 /2019-02-06

[15:20:24] [INFO] testing connection to the target URL
sqlmap got a 301 redirect to 'htttp://192.168.20.166/?id=1--dbs'. Do you
wont to follow? [Y/n] y
```

```
[15:21:59] [INFO] checking if the target is protected by some kind of WAF/
IPS
[15:21:59] [INFO] testing if the target URL is stable
[15:21:59] [WARNING] GET parameter ’id’ does not appear dynamic
[15:21:59] [WARNING] heuristic (basic) test shows that GET parameter ’id’
might not be injectable
[15:21:59] [INFO] testing for SQL injection on GET parameter ’id’
[15:21:59] [INFO] testing ’AND boolean-based blind - WHERE or HAVING
clause’
[15:21:59] [INFO] testing ’OR boolean-based blind - WHERE or HAVING clause’
[15:22:13] [INFO] testing ’OR boolean-based blind - WHERE or HAVING clause
(NOT)’
[l5:22:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING
clause (subquery - comment)'
[l5:22:26] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause
(subquery - comment)’
[15:22:29] [INFO] testing 'ANO boolean-based blind - WHERE or HAVING
clause (comment)'
[l5:22:31] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause
(comment)
[l5:22:32] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause
(NOT - comment)
[l5:22:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING
clause (MySQL - comment)
```

The sqlmap application searches for vulnerabilities and this leads to a timeout. This procedure can take one hour to complete. You can proceed to the next step without waiting for the timeout.

c. To stop the attack, press **Ctrl+c** and wait for a few seconds.

d. Type **E** and press **Enter**.

4. Enable Intrusion Prevention Systems (IPS) rules.

   Download and install the latest Intrusion Detection and Prevention (IDP) security package to configure the necessary policies to stop the attack.

a. Download the IDP security package.

```
ec2-user@vsrx-gw> request security idp security-package download full-update
```

```
Will be processed in async mode. Check the status using the status
checking CLI
```

NOTE: Wait for the download process to complete before trying to install the security package. Otherwise, the following message is displayed:

```
ec2-user@vsrx-gw> request security idp security-package install

Download is in progress. Please try again later.
```

b. Check the download status.

```
ec2-user@vsrx-gw> request security idp security-package download status
```

```
Done; Successfully downloaded from(https://signatures.juniper.net/cgi-bin/
index.cgi)
Version info:3135(Fri Jan 18 05:03:55 2019 UTC, Detector-12.6.130180509)
```

The status shows that the download is successful.

c. Install the IDP security package.

```
ec2-user@vsrx-gw> request security idp security-package install
```

```
Will be processed in async mode. Check the status using the status
checking CLI
```

d. Check the installation status.

```
ec2-user@vsrx-gw> request security idp security-package install status
```

```
Done;Attack DB update : successful - [UpdateNumber=3135,ExportDate=Fri Jan
18 05:03:55 2019 UTC,Detector=12.6.130180509]
        Updating control-plane with new detector : successful
        Updating data-plane with new attack or detector : not performed
due to no active policy configured.
```

The installation of the IDP signatures is successful. The data plane is not updated because no policies are configured or enabled.

e. Enter configuration mode.

```
ec2-user@vsrx-gw> configure
```

```
Entering configuration mode
```

f. Enable logs to track traffic sessions coming from the untrust zone to the trust zone, and commit the configuration.

```
ec2-user@vsrx-gw# set security policies from-zone untrust to-zone trust policy default-permit
then count
ec2-user@vsrx-gw# set security policies from-zone untrust to-zone trust policy default-permit
then log session-init
ec2-user@vsrx-gw# set security policies from-zone untrust to-zone trust policy default-permit
then log session-close
ec2-user@vsrx-gw# commit
```

```
commit complete
```

g. Create a custom IDP policy.

This procedure creates the signature to associate to the firewall rule that detects the SQL injection attack.

```
ec2-user@vsrx-gw# set security log mode stream
ec2-user@vsrx-gw# set security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ
match application junos-http attacks predefined-attacks HTTP:SQL:INJ:GENERIC
ec2-user@vsrx-gw# set security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ
match from-zone untrust to-zone trust
ec2-user@vsrx-gw# set security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ
then action drop-packet
ec2-user@vsrx-gw# security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ then
severity critical
ec2-user@vsrx-gw# set security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ
then notification log-attacks
ec2-user@vsrx-gw# set security idp active-policy DEMOATTACK
ec2-user@vsrx-gw# set security policies from-zone untrust to-zone trust policy default-permit
then permit application-services idp
ec2-user@vsrx-gw# commit
```

5. Run the SQL injection attack again from the kali VM. The vsrx-gw VM now has firewall policies configured.

```
[ec2-user@ip-10-0-0-64 /]$sqlmap -u http://192.168.20.166/index.php?id=1--dbs --risk=3 --
level=5
```

```
[ec2-user@ip-10-0-0-64 /]$ sqlmap -u http://192.168.20.166/index.php?id=1--
dbs --risk=3 --level=5

         _
 ___ ___| |_____ ___ ___ {1.3.2#zip}
|_ -| . | | | .’| . | . |
|___|_  |_|_|_|_|__,| _ |
      |_|           |_|   http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior
mutual consent is illegal. It is the end user’s responsibility to obey all
applicable local, state and federal laws. Developers assume no liability and
are not responsible for any misuse or damage caused by this program

[*] starting @ 17:30:44 /2019-02-06/
```

```
[17:30:44] [INFO] testing connection to the target URL
[17:31:14] [CRITICAL] connection timed out to the target URL or proxy. sqlmap
is going to retry the request(s)
[17:31:14] [WARNING] if the problem persists please check that the provided
target URL is reachable
In case that it is, you can try to rerun with the switch '--random-agent'
turned on and/or proxy switches ('--ignore-proxy', '--proxy',...)
```

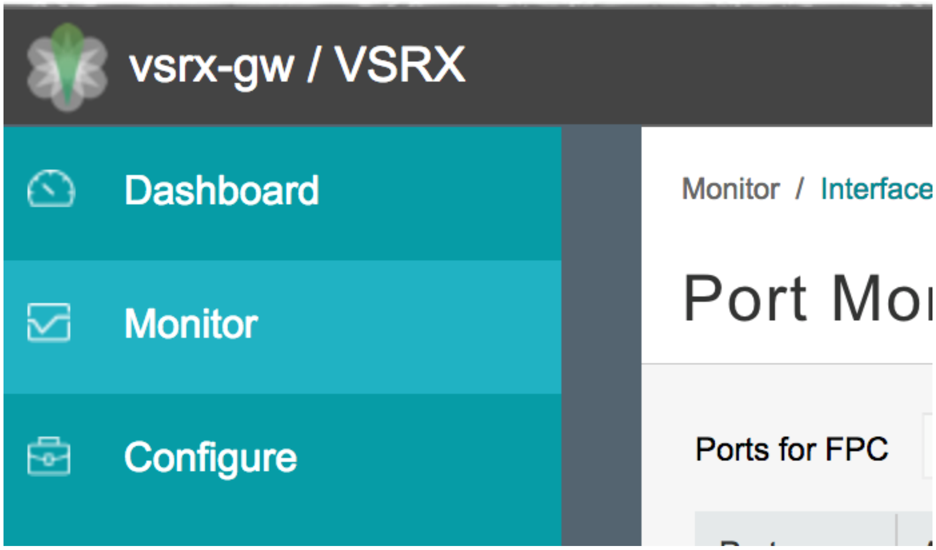
vSRX stops the SQL injection attack.

6. Verify the attack procedure by using the vSRX GUI.

   Log in to the vSRX GUI by using a Web browser, specifying the vsrx-gw public IP address in the URL. The IP address is provided at the end of the AWS Quick Start deployment. Use the new root password configured in Step "2" on page 10. Perform the following steps to obtain the detailed event information:

   a. Click **Monitor** in the left-nav bar on the vsrx-gw/VSRX page as shown in Figure 2 on page 16.

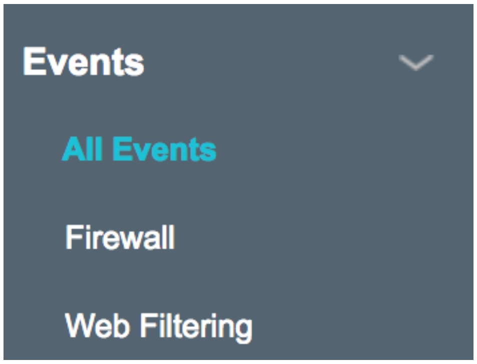
      Figure 2: Monitor

      The Events screen is displayed.

b. Click **All Events** under **Events** as shown in Figure 3 on page 17.

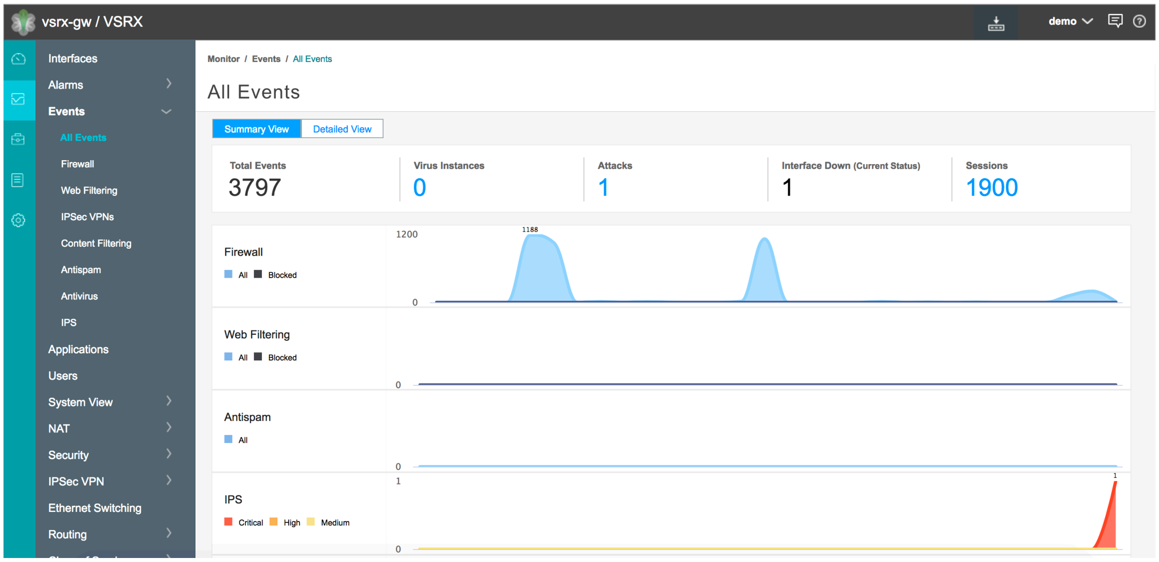
Figure 3: All Events



The Attacks screen is displayed.

c. Click the number under **Attacks**. This number indicates the number of attacks as shown in Figure 4 on page 17.

Figure 4: Attacks



Total Events 3797

Virus Instances 0

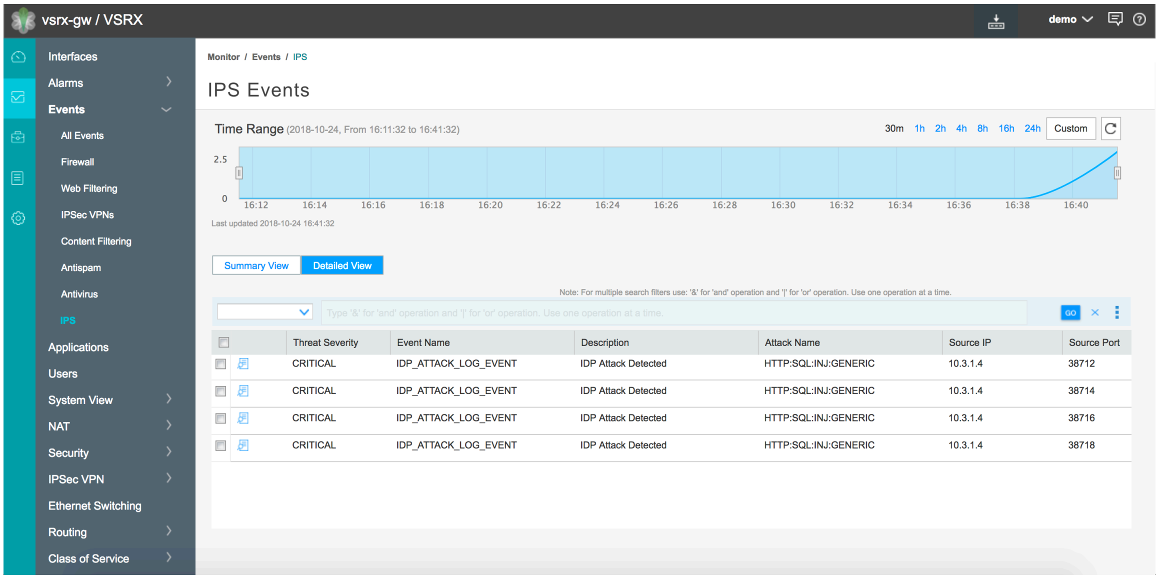
Attacks 1

Interface Down (Current Status) 1

Sessions 1900

All events are displayed in a table.

Figure 5: Event Table



IPS Events

Time Range (2018-10-24, From 16:11:32 to 16:41:32)

Last updated 2018-10-24 16:41:32

Note: For multiple search filters use: '&' for 'and' operation and '|' for 'or' operation. Use one operation at a time.

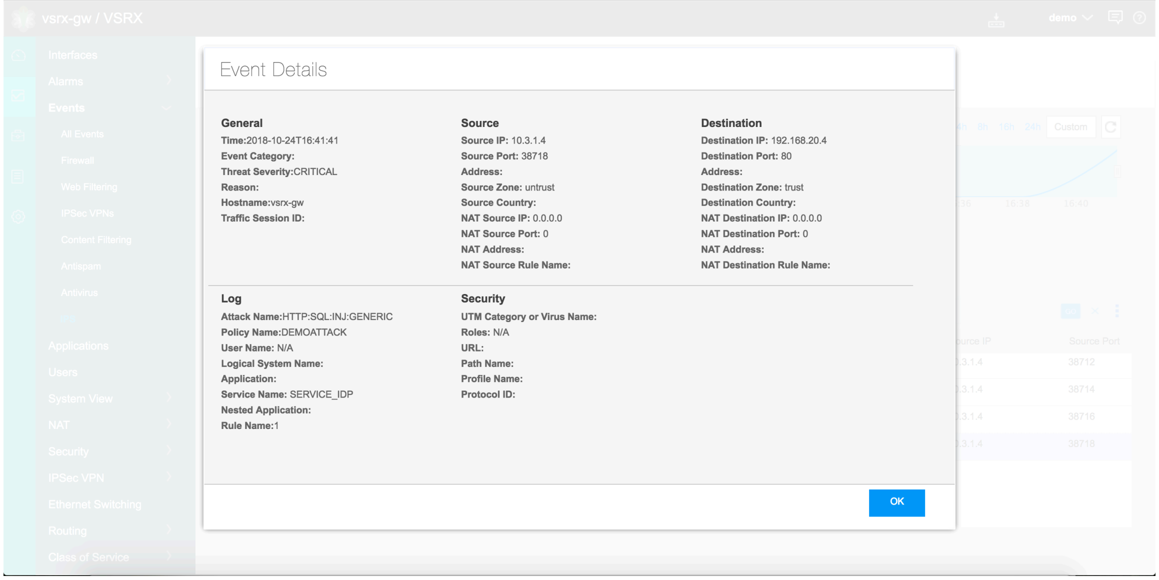
Type '&' for 'and' operation and '|' for 'or' operation. Use one operation at a time.

□	Threat Severity	Event Name	Description	Attack Name	Source IP	Source Port
□	CRITICAL	IDP_ATTACK_LOG_EVENT	IDP Attack Detected	HTTP:SQL:INJ:GENERIC	10.3.1.4	38712
□	CRITICAL	IDP_ATTACK_LOG_EVENT	IDP Attack Detected	HTTP:SQL:INJ:GENERIC	10.3.1.4	38714
□	CRITICAL	IDP_ATTACK_LOG_EVENT	IDP Attack Detected	HTTP:SQL:INJ:GENERIC	10.3.1.4	38716
□	CRITICAL	IDP_ATTACK_LOG_EVENT	IDP Attack Detected	HTTP:SQL:INJ:GENERIC	10.3.1.4	38718

d. Click the magnifying glass icon in the first row of the table.

The detailed event information is displayed as shown in Figure 6 on page 18.

Figure 6: Detailed Event Information



Event Details

General
Time:2018-10-24T16:41:41
Event Category:
Threat Severity:CRITICAL
Reason:
Hostname:vsrx-gw
Traffic Session ID:

Source
Source IP: 10.3.1.4
Source Port: 38718
Address:
Source Zone: untrust
Source Country:
NAT Source IP: 0.0.0.0
NAT Source Port: 0
NAT Address:
NAT Source Rule Name:

Destination
Destination IP: 192.168.20.4
Destination Port: 80
Address:
Destination Zone: trust
Destination Country:
NAT Destination IP: 0.0.0.0
NAT Destination Port: 0
NAT Address:
NAT Destination Rule Name:

Log
Attack Name:HTTP:SQL:INJ:GENERIC
Policy Name:DEMOATTACK
User Name: N/A
Logical System Name:
Application:
Service Name: SERVICE_IDP
Nested Application:
Rule Name:1

Security
UTM Category or Virus Name:
Roles: N/A
URL:
Path Name:
Profile Name:
Protocol ID:

You can obtain detailed event information for each event by repeating step "6.d" on page 18.

The vSRX appliance detects and stops the SQL injection attack.

Nmap Attack

Nmap (Network Mapper) is a free, open-source tool for vulnerability scanning and network discovery. Nmap identifies the devices are running on the network, discovers hosts that are available and the services they offer, finds open ports, and detects security risks.

Run an Nmap Attack

In this procedure, you test whether the vSRX appliance detects and blocks the TCP port scan and UDP port scan Nmap attacks.

To run an Nmap attack:

1. Log in to the kali and vsrx-gw VMs.

2. (Optional) Enable the IPS rules.

   NOTE: This step is not required if you had enabled the IPS rules while running the SQL injection attack.

   Download and install the latest IDP security package to configure the necessary policies to stop the attack.

   a. Download the IDP security package.

   ```
   ec2-user@vsrx-gw> request security idp security-package download full-update
   ```

   ```
   Will be processed in async mode. Check the status using the status
   checking CLI
   ```

   NOTE: Wait for the download process to complete before trying to install the security package. Otherwise, the following message is displayed:

```
ec2-user@vsrx-gw> request security idp security-package install

Download is in progress. Please try again later.
```

b. Check the download status.

```
ec2-user@vsrx-gw> request security idp security-package download status
```

```
Done; Successfully downloaded from(https://signatures.juniper.net/cgi-bin/
index.cgi)
Version info:3135(Fri Jan 18 05:03:55 2019 UTC, Detector-12.6.130180509)
```

The status shows that the download is successful.

c. Install the IDP security package.

```
ec2-user@vsrx-gw> request security idp security-package install
```

```
Will be processed in async mode. Check the status using the status
checking CLI
```

d. Check the installation status.

```
ec2-user@vsrx-gw> request security idp security-package install status
```

```
Done;Attack DB update : successful - [UpdateNumber=3135,ExportDate=Fri Jan
18 05:03:55 2019 UTC,Detector=12.6.130180509]
        Updating control-plane with new detector : successful
        Updating data-plane with new attack or detector : not performed
due to no active policy configured.
```

The installation of the IDP signatures is successful. The data plane is not updated as no policies are configured or enabled.

e. Enter configuration mode.

```
ec2-user@vsrx-gw> configure
```

```
Entering configuration mode
```

f. Enable logs to track traffic sessions coming from the untrust zone to the trust zone, and commit the configuration.

```
ec2-user@vsrx-gw# set security policies from-zone untrust to-zone trust policy default-permit
then count
ec2-user@vsrx-gw# set security policies from-zone untrust to-zone trust policy default-permit
then log session-init
ec2-user@vsrx-gw# set security policies from-zone untrust to-zone trust policy default-permit
then log session-close
ec2-user@vsrx-gw# commit
```

```
commit complete
```

g. Create a custom IDP policy.

> **NOTE**: This step is not required if you had created a custom IDP policy while running the SQL injection attack.

This procedure creates the signature to associate to the firewall rule that detects the Nmap attack.

```
ec2-user@vsrx-gw# set security log mode stream
ec2-user@vsrx-gw# set security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ
match application junos-http attacks predefined-attacks HTTP:SQL:INJ:GENERIC
ec2-user@vsrx-gw# set security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ
match from-zone untrust to-zone trust
ec2-user@vsrx-gw# set security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ
then action drop-packet
ec2-user@vsrx-gw# security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ then
```

```
severity critical
ec2-user@vsrx-gw# set security idp idp-policy DEMOATTACK rulebase-ips rule DEMOSQLINJ
then notification log-attacks
ec2-user@vsrx-gw# set security idp active-policy DEMOATTACK
ec2-user@vsrx-gw# set security policies from-zone untrust to-zone trust policy default-permit
then permit application-services idp
ec2-user@vsrx-gw# commit
```

3. Configure the vSRX port scan protection.

   A port scan occurs when one source IP address sends an IP packet containing TCP or UDP SYN segments to a defined number of different ports at the same destination IP address within a defined interval.

   ```
   ec2-user@vsrx-gw# set security screen ids-option DDOSDEMO tcp port-scan
   ec2-user@vsrx-gw# set security screen ids-option DDOSDEMO udp port-scan
   ec2-user@vsrx-gw# set security zones security-zone untrust screen DDOSDEMO
   ec2-user@vsrx-gw# set security log mode event
   ec2-user@vsrx-gw# set system syslog file idptraffic.log user info
   ec2-user@vsrx-gw# set system syslog file idptraffic.log match "RT_IDP|RT_IDS"
   ec2-user@vsrx-gw# commit
   ```

4. Use the vSRX CLI to verify that the Nmap port scan is blocked.

   Start logging the attack activity in listen mode. Listen mode is the Nmap network scanning mode.

   ```
   ec2-user@vsrx-gw# exit
   ```

   ```
   Exiting configuration mode
   ```

   ```
   ec2-user@vsrx-gw> monitor start idptraffic.log
   ```

   This log shows how vSRX detects and blocks the attack.

5. Run an Nmap TCP port scan attack from the kali VM.

```
[ec2-user@ip-10-0-0-64 /]$# nmap -sT 192.168.20.166
```

```
Starting Nmap 6 .40 ( https://nmap.org ) at 2019-01-22 18:10 UTC
Nmap scan report for 192-168-20-166
Host is up (0.0037s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
8Ø/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds
```

6. Verify that the Nmap port scan is blocked. To do this, use the vSRX CLI to check the logs in the session from Step "4" on page 22.

```
ec2-user@vsrx-gw> monitor start idptraffic.log
```

```
***idptraffic.log ***
Jan 22 18:10:27 vsrx-gw RT_IDS: RT_SCREEN_TCP: TCP port scan! source:
10.3.1.4:55568, destination 192.168.20.4:111, zone name: untrust, interface
name: st0.0, action: drop
Jan 22 18:10:28 vsrx-gw RT_IDS: RT_SCREEN_TCP: TCP port scan! source:
10.3.1.4:53284, destination 192.168.20.4:2022, zone name: untrust, interface
name: st0.0, action: drop
Jan 22 18:10:29 vsrx-gw RT_IDS: RT_SCREEN_TCP: TCP port scan! source:
10.3.1.4:51264, destination 192.168.20.4:10628, zone name: untrust, interface
name: st0.0, action: drop
```

The log confirms that:

- TCP port scan is running.
- vSRX detects the TCP port scan attack.

7. Run an Nmap UDP port scan attack from the kali VM.

```
[ec2-user@ip-10-0-0-64 /]$# sudo su -
[rootr@ip-10-0-0-64 /]$# nmap -sU 192.168.20.4
```

```
Starting Nmap 7 .01 ( https://nmap.org ) at 2019-01-22 18:12 UTC
Nmap scan report for 192.168.20.4
Host is up (0.0040s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
68/udp openfiltered dhcpc
517/udp openfiltered dhcpc

Nmap done: 1 IP address (1 host up) scanned in 1086.13 seconds
```

8. Verify that the Nmap port scan is blocked. Use the vSRX CLI to check the logs in the session from Step "4" on page 22.

```
ec2-user@vsrx-gw>  monitor start idptraffic.log
```

```
***idptraffic.log ***
Jan 22 18:12:27 vsrx-gw RT_IDS: RT_SCREEN_UDP: UDP port scan! source:
10.3.1.4:52474, destination 192.168.20.4:687, zone name: untrust, interface
name: st0.0, action: drop
Jan 22 18:12:29 vsrx-gw RT_IDS: RT_SCREEN_UDP: UDP port scan! source:
10.3.1.4:52476, destination 192.168.20.4:48186, zone name: untrust, interface
name: st0.0, action: drop
Jan 22 18:12:29 vsrx-gw RT_IDS: RT_SCREEN_UDP: UDP port scan! source:
10.3.1.4:52477, destination 192.168.20.4:47765, zone name: untrust, interface
name: st0.0, action: drop
```

The log confirms that:

- UDP port scan is running.

- vSRX detects the UDP port scan attack.

This test confirms that the vSRX appliance detects and blocks the Nmap attack and that you can monitor the attack activity logs.