Defending Against Black Nurse DoS Attacks

Juniper Networks vSRX Virtual Firewall vs. the Competition

Table of Contents

©2017, Juniper Networks, Inc.

Executive Summary

Denial-of-service (DoS) attacks are a popular way to cause targeted service disruptions, typically for extended periods of time. The relative ease and low cost of launching such attacks, aided by a serious lack of any viable defense mechanisms, have made them one of the most common threats on the Internet. In the past, Internet Control Message Protocol (ICMP)-based DoS attacks have used multiple hosts infected with botnets to launch an overwhelming distributed DoS (DDoS) attack to take down major Web servers or perimeter firewalls.

Now, researchers have discovered a new attack technique, called "Black Nurse," that enables a single computer to generate 15 Mbps of bandwidth traffic and take down major network firewalls. This technique launches low-volume DoS attacks by sending specially formatted ICMP packets that overwhelm the processors on targeted firewalls, shutting them down. This white paper takes a detailed look at how Juniper Networks® SRX Series Services Gateways, as well as firewalls from other industry leaders, recently performed while under a Black Nurse DoS cyberattack.

Introduction

Although DoS attacks date back to the early days of the Internet, they remain one of the most disruptive and damaging assaults waged against networks and applications around the world. New security vulnerabilities are constantly being discovered in common IT infrastructure products, and new attack methods are quickly developed to exploit these weaknesses, increasing opportunities to expose the corporate infrastructure. Organizations must be diligent, continuously monitoring common network and server infrastructure products to identify and fix known vulnerabilities.

The Black Nurse cyberattack is an exploit-based attack that focuses on vulnerabilities in some of the industry's firewall operating systems. This means a number of organizations are potential victims, susceptible to the type of service disruptions that can affect business continuity and negatively impact customer perceptions.

Three Multivector Attack DoS Methods

Cyberattackers deploy multivector campaigns that target all layers of the IT infrastructure, including the network, server, and application layers. The tools required to launch such attacks are readily available and easily obtained. Attackers seek to exploit flaws in the software, network, and application layers in IT infrastructure. In general, these campaigns can be broken into three basic categories:

- **Volume-Based Infrastructure Attacks:** In a volume-based infrastructure attack, cyberattackers overwhelm the IT infrastructure by flooding resources with traffic, degrading access to unacceptable levels. These attacks coordinate thousands of compromised hosts, triggering them to launch a wave of SYN, UDP, and ICMP requests against the targeted device or network, exploiting inherent vulnerabilities in Internet protocols and IP packets such as TCP and HTTP, which are fundamental to the operation of the Internet. These sustained distributed DoS, or DDoS, attacks generate voluminous amounts of traffic, consuming bandwidth and buffer space on routers in the attack path or CPU and memory resources on the targeted server, preventing further processing of user requests.
- **Application Attacks:** Application attacks focus on specific vulnerabilities in applications running on a host server. A buffer overflow, one of the most common kinds of application attacks, sends excessive data to an application, either bringing the application down or forcing the data being sent to be executed on the host server. Sometimes, the excess data can crash a vulnerable system. Attackers can even execute specific code on the remote system via a buffer overflow vulnerability; sending too much information to the application actually overwrites the data that controls the program, and the hacker's code is executed instead.
- **Network Infrastructure Vulnerability Attacks:** This attack vector enables cyber hackers to exploit system vulnerabilities in the operating system of routers, switches, and firewalls. Each common network infrastructure product—routers, switches, and firewalls—has inherent vulnerabilities in each new software release, exposing it to attack and placing the entire IT infrastructure at risk. It takes just one compromised component to threaten the entire enterprise.

The impact of DoS attacks can vary widely. Users trying to access internal resources such as intranet pages can be faced with slow Web performance, which directly impedes productivity. For public cloud providers, who are frequent targets, a DoS attack can trigger costly SLA credits and tarnish their brand reputation, which leads to poor customer perception, increased IT costs, and potential litigation.

High-Volume-Based Network ICMP Attack

In the past, DDoS attacks were volume-based infrastructure attacks that used large volumes of network traffic—typically SYN, UDP, or ICMP packets—to flood a connection, overwhelming network resources and effectively denying service to users. With these kinds of attacks, thousands of computers unknowingly infected with malware (such as Trojan Horses or self-propagated worms) act on behalf of the attacker, launching coordinated attacks against the victim's website or IT infrastructure. Since the incoming attack traffic comes from literally thousands of sources, the attack cannot be thwarted by simply blocking a unique IP address.

©2017, Juniper Networks, Inc.

A New Low-Bandwidth ICMP Attack: Black Nurse

On Nov. 10, 2016, Danish researchers discovered a new type of DoS attack characterized by low-volume network traffic that targets vulnerabilities in popular firewalls from major network security vendors. With this new attack, low volumes of ICMP traffic overwhelm firewalls to the point where the firewalls simply shut down. This new attack was named Black Nurse.

The Black Nurse attack is based on ICMP with Type-3 Code-3 packets. Unlike traditional ICMP attacks, which rely on high volumes of traffic to cripple the network, Black Nurse is effective at low bandwidths ranging from 15 to 18 Mbps. In a Black Nurse attack, the firewall processing the ICMP packets is paralyzed with very high CPU utilization, preventing it from processing normal network traffic. Eventually, all firewall resources are exhausted and it crashes, preventing users from sending or receiving traffic. With Black Nurse, a single laptop can generate enough traffic to disable a firewall.

How a Black Nurse Attack Works

Black Nurse, or the low-rate "ping of death" attack, sends a specially formatted Type-3 ICMP packet with a code of 3 that overloads the CPU of certain types of firewalls, regardless of the amount of traffic being sent. Whether a firewall is susceptible to Black Nurse is entirely dependent on the device's architecture and its protocol stack implementation. The Black Nurse attack volume is very small—as stated earlier, 15 to 18 Mbps (40,000 to 50,000 packets per second) ICMP network traffic, which is minuscule compared to traditional DDoS attacks, which can scale up to 1.1 Tbps of traffic.

Figure 1 shows a Black Nurse packet:

```
˅ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x0d33 [correct]
    [Checksum Status: Good]
    Unused: 00000000
    > Internet Protocol Version 4, Src: 1.2.3.4 Dst: 5.6.7.8
    ˅ Transmission Control Protocol, Src Port: 0, Dst Port: 0
        Source Port: 0
        Destination Port: 0
        Sequence number: 585665
```

Figure 1: The Black Nurse packet

As long as a firewall is accepting Black Nurse attack traffic, its processors will continue to be overwhelmed. Eventually it will shut down completely, denying service to users.

Protection in the Architecture

The SRX Series architecture is designed for optimal performance and has been battle tested in some of the largest service provider and enterprise customer environments around the world. Since their inception, the SRX Series firewalls were built from the ground up with true control and data plane separation; the control plane is responsible for the management and system services that operate the device while the forwarding plane is responsible for moving data traffic as efficiently as possible. This clear separation of control and data planes protects SRX Series firewalls from direct attack and shields critical firewall management services from being affected when an attack is underway.

The SRX Series security architecture scales by processing traffic early in the pipeline, preemptively mitigating a cyberattack before affecting legitimate traffic and management services. In the case of a DoS attack, the SRX Series firewalls employ two primary security methods to protect critical services: firewall filters and screens.

Firewall Filters

Firewall filters are stateless filters that block or drop traffic based on Layer 2 or Layer 3 header information, akin to access lists used to protect routers from malicious traffic. Firewall filters can be applied to the ingress or the egress interface, and traffic can be dropped as quickly and efficiently as possible right at the interface.

Screens

Screens offer stateful protection that occurs at the beginning of the packet processing chain. The SRX Series has some of the most advanced attack prevention capabilities on the market, capable of efficiently blocking most well-known attacks—including large DoS and DDoS attacks—without any interruption to normal traffic processing. Screens are a

©2017, Juniper Networks, Inc.

Layer 3 and Layer 4 intrusion prevention system (IPS) setting that can be used to detect and block anomalies or traffic exceeding certain thresholds.

As seen in Figure 2, screen processing can take place on both the control and data plane. SRX Series devices install an established stateful flow into the session table and continue to monitor that connection for any signs of malicious traffic or flooding beyond predetermined thresholds. If any malicious traffic is detected, it is blocked and packets are dropped without interrupting control or data plane processing.

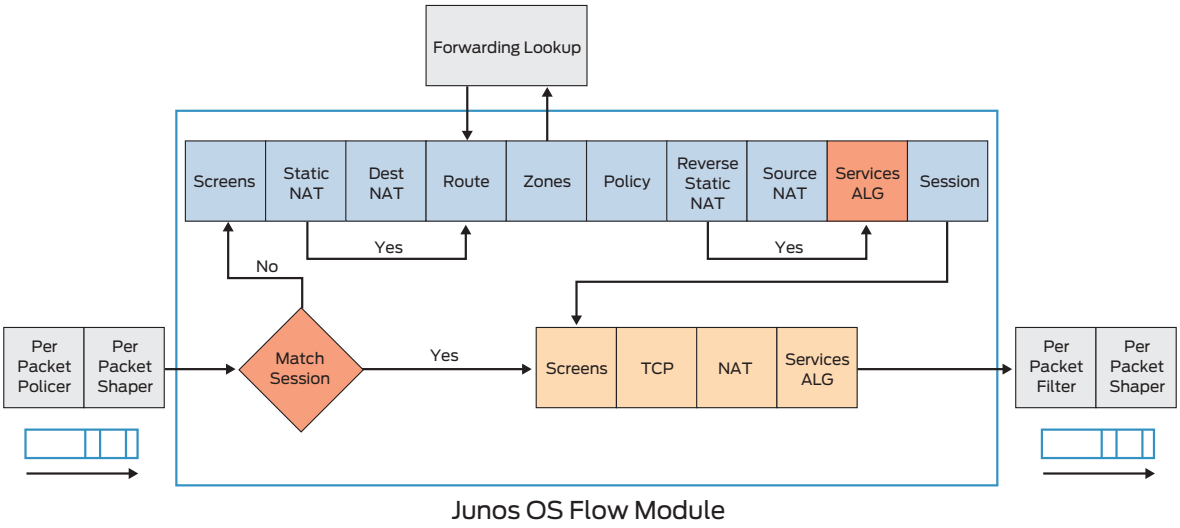

Figure 2: SRX Series security architecture—packet processing pipeline

Firewall Vendor Exposure to Black Nurse

When the Black Nurse attack was discovered, researchers found that it directly impacted many of the most popular firewalls used by customers throughout the industry, and lab tests were conducted against major firewall vendors to determine the magnitude of the problem. Upon discovery of this vulnerability, Juniper Networks immediately commissioned its own lab tests to see how its SRX Series Services Gateways fared under a Black Nurse attack. Competitive firewalls were also tested to see how they compared to the Juniper devices.

The lab tests found that the SRX Series firewalls—and the Juniper Networks Junos® operating system—performed flawlessly under a Black Nurse attack, with no interruptions in service.

By contrast, many of Juniper's major firewall competitors appeared to be susceptible to attack, even when exposed to low volumes of Black Nurse traffic.

For details on the full Black Nurse test plan, please refer to Appendix A. For additional information, please read the "Black Nurse in Review: Is Your NGFW Vulnerable?" blog.

Test Results

In order to conduct a true apples-to-apples comparison between Juniper and its closest competitors, it was decided that virtualized versions of the firewalls would be used to mitigate any differences in proprietary physical hardware. The Juniper Networks vSRX Virtual Firewall provides the same functionality as the physical SRX Series firewalls.

For the purposes of this white paper, the two leading firewall vendors that were compared to Juniper for these tests will be referred to as:

- Firewall Vendor #1
- Firewall Vendor #2

For the tests, the lab setup consisted of a protected Web server sitting behind the firewall; a virtual machine perpetuating a Black Nurse attack against the server; and a benign user attempting to access a webpage from the protected server. The firewall sits between the VM attacker and the protected server, where it processes the Black Nurse traffic while the benign user attempts to access the protected server's front HTML page.

For additional details about the test setup and the Junos OS configurations used in the tests, please refer to Appendix A at the end of this white paper.

©2017, Juniper Networks, Inc.

Firewall Performance

The fundamental tenet of SRX Series firewall architecture is the separation of the data and control planes. Since we are using the vSRX Virtual Firewall for the test, we are running on a multicore Intel X86 CPU processor. The vSRX is optimized to leverage multiple virtual CPU cores to maximize packet processing and overall throughput in a virtual environment. In the test scenario, the vSRX virtual machine (VM) has multiple virtual network interfaces (vNICs) which transport traffic from the outside network to the inside network where the protected server is hosted. The vSRX uses each available core on the Intel x86 chipset to scale traffic performance under the data plane while isolating the control plane traffic to a dedicated core on the chipset socket.

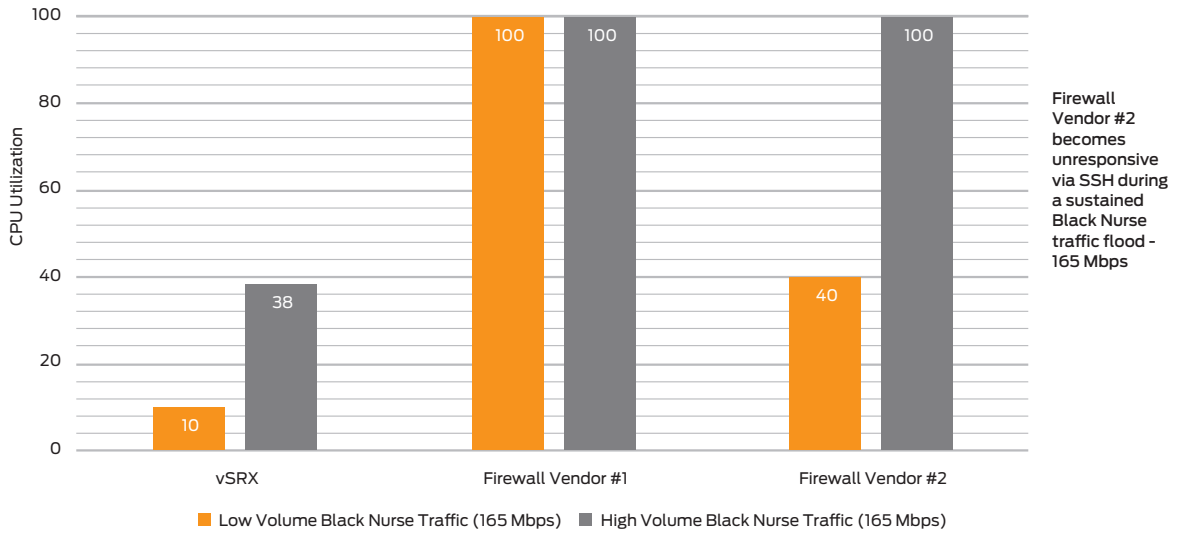

Figure 3: Data plane CPU utilization with default configuration

As shown in Figure 3, data plane utilization on the vSRX is far lower than the two leading competitors when the default firewall configuration is used. Additionally, data plane CPU utilization on the vSRX is also far lower than the competitive virtual firewalls when processing the low-volume Black Nurse traffic.

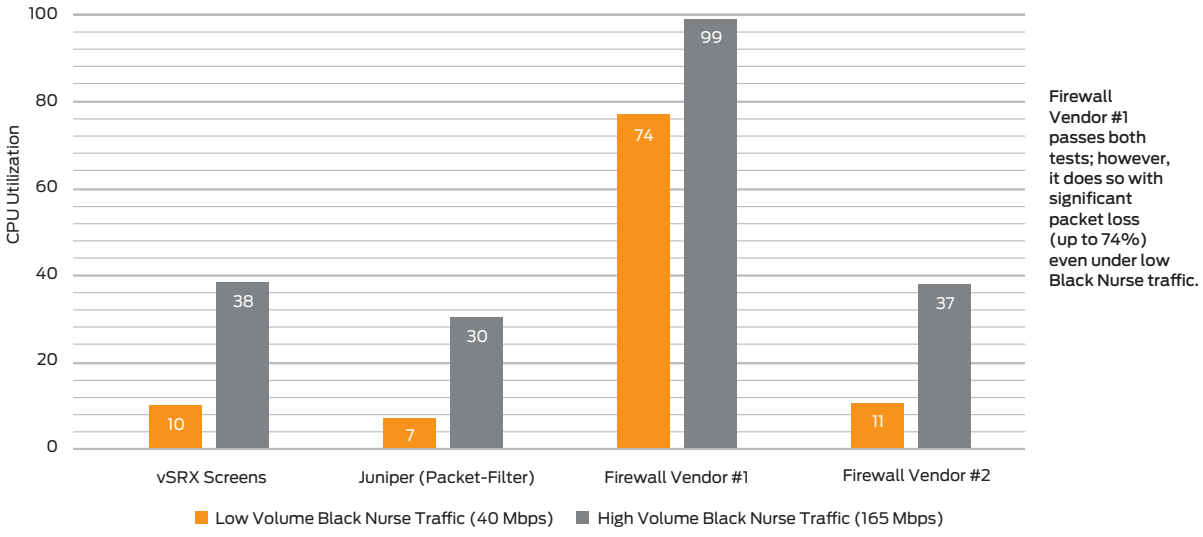

Figure 4: Data plane CPU utilization with recommended configuration

As shown in Figure 4, when the test was conducted with the recommended configurations stated by the Black Nurse advisories, the vSRX Virtual Firewall scaled in performance and experienced minimal data plane CPU utilization compared to the competition when the screens and packet filter features were enabled during the attack. In both cases, the other two leading firewall vendors struggled when under a Black Nurse attack.

©2017, Juniper Networks, Inc.

SRX Series Mitigation Performance

The SRX Series firewall packet filters are among the industry's most efficient mitigation solutions when handling DoS and DDoS cyberattacks. The optimized security architecture allows mitigation performance to scale, even on the vSRX.

Across both SRX Series physical and virtual firewall platforms, a session lookup is performed early in the packet processing pipeline, saving previous time and system resources when a large DoS attack occurs. On the high-end SRX Series hardware platforms, the firewall architecture has been designed to push screens processing directly onto hardware-based ASICs to scale mitigation at line-rate performance. For example, the high-end SRX5000 line of Services Gateways can scale up to 240 Gbps at line rate per line card without impacting system resources.

Test Summary

The results from the lab test indicate that, while many firewall vendors have internal architectures that prevent them from scaling with a Black Nurse attack, the vSRX was able to continue functioning and maintain uninterrupted performance under both low and high Black Nurse attack traffic conditions, minimizing the impact on CPU utilization on the Intel x86 processor.

The reason the vSRX Virtual Firewall is able to scale performance under a DoS attack is because its architecture isolates control and data plane functions. Furthermore, the Black Nurse ICMP traffic—normally processed by the control plane CPU, leaving the firewall vulnerable—is immediately dropped at the beginning of the packet pipeline, effectively thwarting the attack.

Enabling the packet filter or screens features had minimal impact on the vSRX Virtual Firewall when under a Black Nurse attack because the vSRX checks to see if the ICMP packet is legitimate by checking its session table and dropping it before it can get processed further by the firewall. This efficient implementation makes security mitigation as fast and efficient as possible, without affecting legitimate traffic or users on the network.

SRX Series Firewall Advantage

Performance is a critical factor in any security solution. If a security solution is unable to maintain high performance levels at all times, it becomes a hindrance to daily business activity. At the heart of all Juniper Network SRX Series Services Gateways is a high-performance platform designed from the ground up to accelerate security processing. With a security-specific processing architecture and an optimized data path designed to achieve and maintain high throughput levels for both large and small packet sizes, Juniper accelerates firewall, encryption, authentication, and packet processing, resulting in performance that far surpasses competitive security solutions in terms of throughput, mitigation, and low latency.

Controlling the high-performance SRX Series firewalls is Junos OS, a real-time, security-specific operating system that controls all aspects of the device including network integration and security applications. The combination of Junos OS and the high-performance firewall means that the Juniper solution does not suffer from the connection table and processing limits found in security solutions running on general-purpose operating systems. Tightly integrated with Junos OS is a set of robust security applications that can be deployed as the basis of any security solution.

Conclusion

In today's security landscape, one thing is certain—networks will remain the target of increasingly sophisticated types of attacks originating both internally and externally. Compounding the difficulty associated with protecting the network from new types of attacks is the scalability and performance of perimeter firewalls used as the first line of defense. Juniper Networks SRX Series Services Gateways enable security teams to implement solutions designed to defend against DoS attacks through built-in security and high performance. This eliminates any damage that may result from the attack, with the goal of establishing a trusted network.

Juniper offers its customers an industry-leading layered security solution that is highly effective at protecting the network from a never-ending wave of intrusions and attacks. With the SRX Series firewalls, enterprises can cost-effectively safeguard their applications and data, secure their communications, and protect their intellectual property from attack. They can create a network environment that can truly be trusted, and do so without sacrificing network performance, flexibility, reliability, or management control.

©2017, Juniper Networks, Inc.

Appendix A: Black Nurse Test Plan

Firewall Evaluation Black Nurse Attack: Lab Setup

Juniper Networks tested its SRX Series Services Gateways in a lab environment to determine their performance when under various types of attacks, including Black Nurse. The tests included an evaluation of how the Juniper products compared to firewalls from various competitors. As part of the base comparison, it was determined that the best way to make an apples-to-apples comparison was to use the competitors' virtualized firewall platforms. Virtualizing the test bed helped eliminate any abstract proprietary hardware advantages. If each firewall device has an identical amount of host compute assigned to it, it is relatively easy to determine which software architectures are most vulnerable to a Black Nurse attack.

Figure 4 shows the specifications of the testbed used to reproduce or analyze the results.

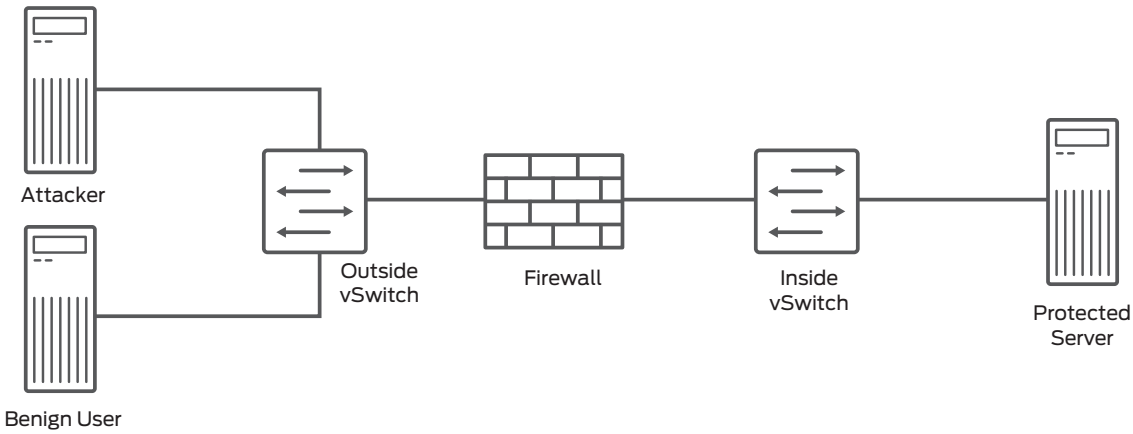

Figure 5: Black Nurse test lab setup

The test bed was set up with the following virtual components:

- **Attacker:** The virtual machine acting as the attacker perpetuating the Black Nurse traffic directed at the protected server
- **Benign user:** A virtual machine acting as a user trying to download a webpage that is behind the next-generation firewall (NGFW)
- **Protected server:** A virtual machine acting as the protected Web server sitting behind the NGFW

Host Specifications

For the purposes of this evaluation, a standard Intel x86 server host running VMware ESXi 5.5 was used as the virtualized platform.

Table 1 shows the server system specifications.

Table 1: Host Specifications:

Host Specifications	
Compute	2 core Intel Xeon L5520
Memory	82 GB of DDR3-1333 ECC

Virtual Machine Specifications

Each of the virtual machines—attacker, benign user, and protected server—were configured with relatively low specifications on the VMware ESXi host. The specifications for each are shown in Table 2.

Table 2: Virtual Machine Specifications:

Virtual Machine Specifications	
Compute	2x vCPU
Memory	2 GB RAM
Network Adaptor	1x VMXNET3 NIC

©2017, Juniper Networks, Inc.

The Black Nurse attack was staged from the attacker machine, a VM running Ubuntu Server 16.04 LTS (Xenial Xerus). The VM used the hping3 utility to generate the Black Nurse packets.

Next-Generation Firewall Virtual Machine

The vSRX is Juniper's virtual firewall which runs the same exact code base as the physical SRX Series firewalls, only in a virtual form factor. The vSRX virtual machine on the ESXi host was configured with the specifications shown in Table 3.

Table 3: vSRX Virtual Firewall Specifications:

vSRX Specifications	
Compute	2X vCPU
Memory	2 GB RAM
Network Adaptor	3x VMXNET3 NIC's (Management/Outside/Inside)

The vSRX VM utilized para-virtualized VMXNET3 interfaces to maximize its potential performance and interrupt handling.

SRX Series Firewall Operating System Version

Table 4 shows the Junos OS version used during the test.

Table 4: vSRX Virtual Firewall Junos Operating System Version:

vSRX Junos OS Version	
Junos OS Version	15.1X49-D60

The Test Plan

The test plan for this evaluation was created using ideal circumstances where it was possible to determine the maximum amount of traffic a given solution could support under a Black Nurse attack scenario.

Each of the NGFWs featured the following specifications:

1. A single rule which permits any source to any destination with any application
2. No Network Address Translation (NAT)
3. No logging
4. No advanced security services that might directly impact CPU performance

Default and Recommended Configuration

In order to properly compare how different firewalls were able to handle Black Nurse traffic, we selected two of the leading firewall competitors. In this white paper, these vendors will be identified as follows:

- Firewall Vendor #1
- Firewall Vendor #2

Comparisons were made using two different firewall configurations:

- Default configuration for each respective firewall vendor
- Recommended configuration suggested after the announcement of the Black Nurse threat

Along with these configurations, it was decided to test with two different levels of Black Nurse traffic:

- Low flooding
- High flooding

For the evaluation, two levels of Black Nurse traffic would be generated—low flooding and high flooding—under two configurations: default and recommended.

©2017, Juniper Networks, Inc.

Table 5 summarizes the test evaluation scenarios:

Table 5: Black Nurse Test Scenarios:

	Black Nurse Flooding (Stage 1)	Black Nurse Flooding (Stage 2)
Default NGFW Configuration	Low flooding	High flooding
Recommended NGFW Configuration	Low flooding	High flooding

Pass/Fail Test Criteria

A simple "pass" or "fail" grade was assigned to each firewall based on the benign user's ability to request the front webpage (index.html) from the Web server sitting on the protected server within a 15 second timeframe. The webpage request was executed only after the Black Nurse attack had been active for one minute. The test attempted to validate that resources were available on the protected host during the attack. If the benign user was able to successfully retrieve the index.html file on the protected server, it was considered a pass; if it was unable to obtain the index.html file within the 15-second time frame, it was considered a fail and the DoS attack was considered successful.

Successful Webpage Request

Before any tests were actually executed, each NGFW test bed was validated to ensure that the benign user was able to successfully request the index.html file in less than 0.01 seconds.

```
$ time wget 10.1.1.100
--2016-11-27 15:30:40--  http://10.1.1.100/
Connecting to 10.1.1.100:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 612 [text/html]
Saving to: 'index.html'

100%[======================================>] 612         --.-K/s   in 0s

2016-11-27 15:30:40 (74.8 MB/s) - 'index.html' saved [612/612]


real    0m0.005s  <----
user    0m0.000s
sys     0m0.000s
```

A strict timeout was enforced during the test through the "timeout" command. If the request was not completed within the specified time, the timeout utility would end the attempt and exit the process.

Unsuccessful Webpage Request

If during one of the test scenarios a webpage request was unsuccessful during a Black Nurse attack, it was expected that the firewall would not be able to process the webpage request and would time out.

An example of a failed attempt is as follows:

```
$ timeout 15 wget 10.1.1.100
--2016-11-27 15:34:32--  http://10.1.1.100/
Connecting to 10.1.1.100:80...
$
```

Black Packet Generation

In order to emulate a real Black Nurse attack, ICMP Type-3 Code-3 packets were generated using Hping3, which is a free and widely available packet generator utility.

Utilizing the Hping3 utility program, it was possible to generate 40 Mbps, or 75,000 packets per second (PPS), of Black Nurse attack traffic targeted at the protected server. Each generated packet was 70 bytes in length.

©2017, Juniper Networks, Inc.

Black Nurse Low-Packet Flooding

Following is the Hping utility command to generate the Black Nurse low-packet flooding:

```
hping3 --icmp -C 3 -K 3 -i u1 10.1.1.100
```

Black Nurse High-Packet Flooding

Following is the Hping command that generates the Black Nurse high-packet flooding:

```
hping3 --icmp -C 3 -K 3 --flood 10.1.1.100
```

The command above generated 165 Mbps/295,000 PPS from the attacker machine. This amount of traffic is more than enough to fully evaluate whether a firewall can properly handle Black Nurse traffic.

Appendix B: Junos OS Configuration on SRX Series Firewalls

The following is the baseline configuration used on the vSRX virtual firewall for the Black Nurse test:

```
set version 15.1X49-D60.7
set system host-name vSRX
set system root-authentication encrypted-password “$5$CM/
Zzr55$kET7anrM32v0KxpwOVyPJcT3HTALY9pNcdx.Rw8K6U3”
set system services ssh
set security policies global policy Permit_Any match source-address any
set security policies global policy Permit_Any match destination-address any
set security policies global policy Permit_Any match application any
set security policies global policy Permit_Any then permit
set security zones security-zone Outside interfaces ge-0/0/0.0
set security zones security-zone Inside interfaces ge-0/0/1.0
set interfaces ge-0/0/0 unit 0 family inet address 1.1.1.1/24
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24
set interfaces fxp0 unit 0 family inet address 192.168.0.5/24
```

In order to enable screens on the outside zone to enable ICMP flood protection, the following Junos OS commands were added:

```
set security screen ids-option BlackNurse icmp flood threshold 100
set security zones security-zone Outside screen BlackNurse
```

The following set of commands was used to implement a simple packet filter to discard all ICMP Type-3 Code-3 packets ingressing into the outside interface:

```
set firewall family inet filter BlackNurse term 1 from protocol icmp
set firewall family inet filter BlackNurse term 1 from icmp-type unreachable
set firewall family inet filter BlackNurse term 1 from icmp-code port-unreachable
set firewall family inet filter BlackNurse term 1 then discard
set firewall family inet filter BlackNurse term 2 then accept
set interfaces ge-0/0/0 unit 0 family inet filter input BlackNurse
```

©2017, Juniper Networks, Inc.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

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

Copyright 2017 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. 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.

2000665-001-EN Apr 2017