HPC Network Security Analytics Using Virtual Appliances

Victoria Sasaoka | University of California – San Diego (vsasaoka@ucsd.edu) | HPC - SYS

UC San Diego

Goal of the Project

Los Alamos National Laboratory (LANL) wants to support IPv6 alongside IPv4 in a few years using their current network appliances. The project's task is to model the unclassified Turquoise network, which employs Juniper Networks' SRX (Security, Routing, and Switching) firewall and the JSA SIEM (Juniper Secure Analytics Security Information and Event Management) appliance, in a virtual environment. The goal is to test how a dual-stack IPv6/IPv4 configuration may operate and build traffic/log monitoring and analytics capabilities with the JSA.

Virtual Network Setup

Virtual network model located on Network-Test (CentOS7, approx. 1.6 TB storage, 128 GB memory)

- KVM hypervisor for hosting all the virtual machines
- Juniper's vSRX virtual firewall appliance
- Juniper's JSA virtual SIEM appliance attached to the vSRX
- 3 CentOS 7 VMs attached to the vSRX with static routes
- 3 security zones/network segments:
    - "green" for user accounts
    - "red" for admin accounts
    - "blue" for external traffic coming into vSRX
- JSA is attached to security zone "black-logs", and its management interface is on the "red" network
- Syslogs are streamed from vSRX to JSA and viewed on JSA web console
- IDP policy template: "Recommended"
- Screen options ("screen-config" attached to each zone)
- Zone to zone policies limit traffic to HTTP, HTTPS, SSH and ICMP traffic
- Ingress and egress firewall filters attached to management interface (fxp0)

Test Examples

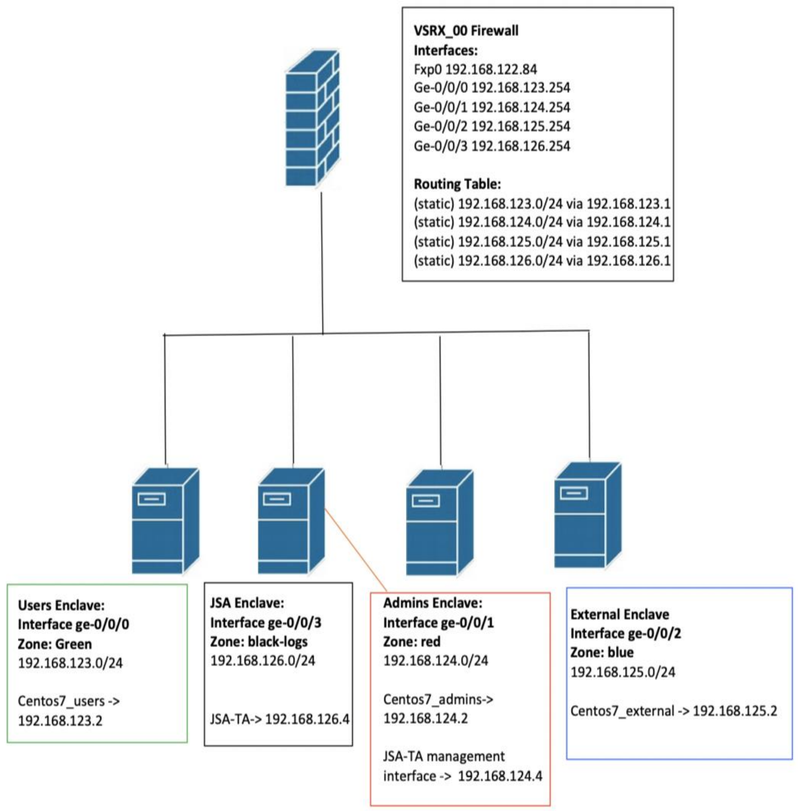
`nping -c 3 -tcp 80 192.168.124.2`

-> for generating 3 TCP packets headed to TCP port 80 from a certain VM in one zone to the centos7_admins VM with IP address 192.168.124.2

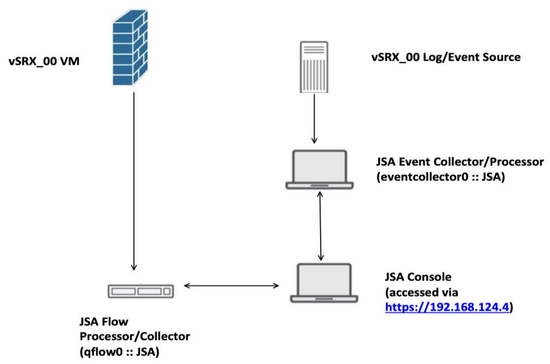
`nping -c 3 -udp -p 22,443 192.168.124.2`

-> same as above, sends 3 UDP (connectionless) packets to port 22 and port 443 of the VM with IP address 192.168.124.2

Current Test Network Layout



JSA Mechanics



Challenges/Setbacks So Far

- Failure to install the log source management app on JSA, which was a barrier to configuring log/flow sources
    - Resolved when network-test's storage was manually expanded by approx. 500GB, which allowed JSA to install with the log source management app
- Failure to see the correct log source (from vSRX) in the log activities tab on JSA console; only saw generic Health Monitoring logs sent to localhost
    - One issue was an incorrect destination for log streams; logs had to be streamed to the "black-logs" VM instead of the JSA management interface in "red" zone.
    - Another fix was adding the vSRX interface address for the "black-logs" zone (192.168.126.254) in the /etc/hosts file on the JSA

Going Forward

- Configure dashboard on JSA with security rules
    - Configuring scanners for ports and hosts
    - Set up denials for too many failed login attempts
    - Identify active hosts, open ports and potential vulnerabilities
    - Identify risky sources, dropped packets and vulnerability assessment information
- Finish configuring IPv6 policies in vSRX/JSA and testing connections
- More log traffic generation and analysis after dual-stack implementation and JSA are configured

JSA Log Snippet

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port
RT_FLOW_SESSION_CREATE"	Juniper JunOS Platform @ vSRX_00"	1	Aug 3, 2022, 2:19:59 PM	Session Opened	192.168.123.2	8902	92.168.124.2	127
Information Message	System Notification-2 :: JSA	1	Aug 3, 2022, 2:19:59 PM	Information	192.168.124.4	0	127.0.0.1	0
RT_FLOW_SESSION_CREATE"	Juniper JunOS Platform @ vSRX_00"	1	Aug 3, 2022, 2:19:58 PM	Session Opened	192.168.123.2	8902	92.168.124.2	126
RT_FLOW_SESSION_CREATE"	Juniper JunOS Platform @ vSRX_00"	1	Aug 3, 2022, 2:19:57 PM	Session Opened	192.168.123.2	8902	92.168.124.2	125
RT_FLOW_SESSION_CREATE"	Juniper JunOS Platform @ vSRX_00"	1	Aug 3, 2022, 2:19:56 PM	Session Opened	192.168.123.2	8902	92.168.124.2	124

Mentors: Jesse Martinez, Thomas Areba, Chase Harrison

Los Alamos NATIONAL LABORATORY
NNSA National Nuclear Security Administration
Managed by Triad National Security, LLC, for the U.S. Department of Energy's NNSA.
LA-UR-22-28114