LAT CONSULT · SAMPLE LAB

Multi-Vendor Firewalling in EVE-NG

Juniper SRX · Cisco ASA · Palo Alto — same DMZ policy, three CLIs

Objective

Build the same DMZ + Inside + Outside security policy on three different firewall vendors, then compare CLIs side-by-side. By the end of this lab you should be able to read and modify a basic policy on any of the three platforms.

Topology

Three zones — **OUTSIDE** (simulated internet, 198.51.100.0/24), **INSIDE** (corporate LAN, 10.10.10.0/24), **DMZ** (web server farm, 192.0.2.0/24). The firewall under test sits between all three. Only HTTPS (tcp/443) from OUTSIDE to DMZ is permitted; INSIDE may reach anything; DMZ may not initiate to INSIDE.

Pre-flight checklist

- EVE-NG running with vSRX 21.x, ASAv 9.16, and PA-VM 10.2 images imported
- 16 GB RAM available on host laptop
- Console access to all three firewalls via telnet
- Stopwatch (you'll be timing yourself in week 06 review)

Step 1 — Juniper SRX policy

Configure zones, then a single policy from untrust to dmz permitting HTTPS:

```
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone dmz interfaces ge-0/0/1.0
set security zones security-zone trust interfaces ge-0/0/2.0
set security policies from-zone untrust to-zone dmz policy web-in match source-address any
destination-address web-srv application junos-https
set security policies from-zone untrust to-zone dmz policy web-in then permit
commit
```

Step 2 — Cisco ASA policy

nameif your interfaces, set security-levels, then an ACL + access-group:

```
interface g0/0
 nameif OUTSIDE
 security-level 0
interface g0/1
 nameif DMZ
 security-level 50
object network web-srv
 host 192.0.2.10
access-list OUT_IN extended permit tcp any object web-srv eq 443
access-group OUT_IN in interface OUTSIDE
```

Step 3 — Palo Alto policy

Create zones, an address object, then a security rule referencing App-ID:

```
set zone OUTSIDE network layer3 ethernet1/1
set zone DMZ network layer3 ethernet1/2
set address web-srv ip-netmask 192.0.2.10/32
set rulebase security rules web-in from OUTSIDE to DMZ source any destination web-srv
application ssl service application-default action allow
commit
```

Vendor comparison cheat-sheet

Concept	Juniper SRX	Cisco ASA	Palo Alto
Zone construct	security-zone	nameif + sec-level	zone
Policy unit	policy in from/to zone	ACL + access-group	security rule
NAT	source/static NAT rules	object NAT	NAT rule (pre/post)
App awareness	AppID via UTM	Limited (modular)	App-ID native
Commit model	candidate + commit	running config live	candidate + commit

Validation tests

✓ From OUTSIDE: curl -k https://192.0.2.10 → expect 200 OK on all three vendors

✓ From OUTSIDE: ssh 192.0.2.10 → expect TCP reset / dropped

✓ From INSIDE: ping 8.8.8.8 → expect echo replies

✓ From DMZ: telnet 10.10.10.10 22 → expect denied (no reverse rule)

Deliverable

Submit a screen-recording (5 min max) walking through your config on all three vendors and the four validation tests above. Email to **cohort@latconsult.com** by Sunday 23:59 ET of Week 06.