For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

The Scenario

Now that your Palo Alto firewall(s) are in place and giving your more visibility into the traffic that is traversing your network, people in your organization are starting to notice. As is often the case, every issue encountered with an application's performance starts with a finger pointing at the firewall as the source of the problem. Your mission is to determine whether or not the firewall is indeed having an impact. If it is, you need to identify where the issue lies so you can rectify it. If it isn't, you need the empirical proof to prove the firewall's innocence.

The Mission

Your mission, should you choose to accept it, is to leverage global counters, the test command, and the flow basic capabilities via the CLI to get a deeper view into what is happening to the packets traversing the firewall.

The Tools of the Trade

Completing this mission will require you to perform the following tasks in the firewall's CLI:

- ✓ Use the test command
- ✓ Configure packet filters
- ✓ Explore global counters
- ✓ Run a flow basic capture

The Target Devices

This lab can be performed on any firewall. The test and global counter commands do not have any performance impact. Flow basic can cause performance degradation, so running it on a non-production firewall to execute this lab would be advisable. The step by step directions of this lab will be for an individual firewall running PANOS 8.0.5.

The Information You Need

To complete these lab steps, you will need the following information readily available:

- ✓ IP Address of the management interface of the firewall
- ✓ Your administrator credentials to access said firewall
- ✓ Access to a terminal emulator such as Putty to initiate an SSH session into the firewall from
- ✓ Access to a client behind the firewall that can generate traffic to/from the internet through the firewall
- ✓ The IP address of the client you are generating your traffic from (which will be referred to as *<CLIENT-IP>* from this point on)

The Lab Configuration Steps

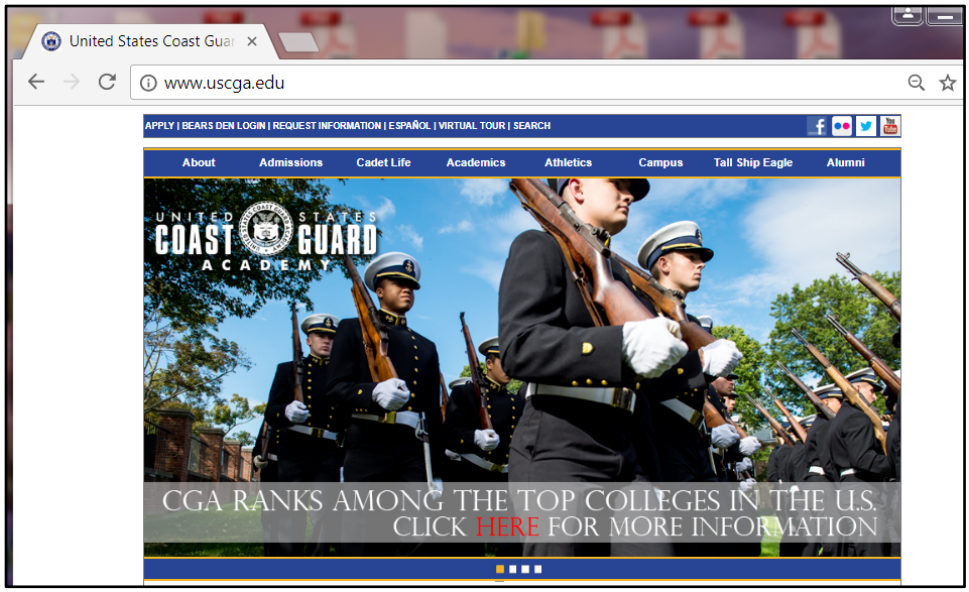
1. Firewall Preparation

a. Purpose

This is make sure that you can generate meaningful traffic through the firewall (preferably to the Internet) to be able to exercise the tasks in the rest of the lab

b. Tasks

i. From the client behind the firewall, attempt to connect to www.uscga.edu from a web browser



ii. From the command line of the client behind the firewall, attempt to perform a DNS A record lookup for the above URL against the google DNS server at 8.8.8.8

```
C:\Users\William Kintz>nslookup www.uscga.edu 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.uscga.edu
Addresses:  138.29.1.1
          138.29.1.6
```

iii. If either of those tests are unsuccessful, either alter the ruleset of the firewall until they are or pick a different website and/or external DNS server that will work for you and use those values moving forward in defining your filters and testing connectivity.

2. Exploring Test Command

a. Purpose

The test command exists to validate which rule in a policy the firewall would apply to a session with the parameters you provide. This is useful in detecting undesired behavior being caused by misconfigured rules in a policy. Many policy types can be tested. Below you will find the most likely ones you will use, however there are many more available

```
wkintz@CayoLocoPA200> test
> custom-url                  Test custom URL categorization
> data-filtering              Test ccn/ssn match
> decryption-policy-match     Test ssl policy match
> dns-proxy                   Test DNS query
> dos-policy-match            Test DoS Policy match
> nat-policy-match            Test nat policy match
> nd                          IPv6 Neighbor Discovery
> nptv6                       NTPv6 related commands
> pbf-policy-match            Test Policy Based forwarding match
> qos-policy-match            Test qos policy match
> routing                     verify routing settings
> security-policy-match       Test security policy match
> ssl-exclude-list            Test hostname in SSL Exclude list
> url                         Test URL categorization
> url-info-cloud              Return detailed information about the URL in the cloud
> url-info-host               Return detailed information about the URL in the MP
> url-wpc                     Test Wildfire Private Cloud URL list
> user-id                     Test Userid
> vpn                         verify (IKE/IPSec) VPN settings
> wildfire                    Test wildfire
```

b. Location

The test command is run from the command line of the firewall in operational mode and requires a myriad of options:

```
wkintz@CayoLocoPA200> test security-policy-match
+ application          Application name
+ category             Category name
+ destination          destination IP address
+ destination-port     Destination port
+ from                 from
+ protocol             IP protocol value
+ show-all             show all potential match rules until first allow rule
+ source               source IP address
+ source-user          Source User
+ to                   to
```

c. Example Tasks

i. Determine which security rules would be triggered by outbound bittorrent and dns traffic.

```
> test security-policy-match application
bittorrent source <CLIENT-IP> destination
72.5.65.112 protocol 17 destination-port 53 from
inside to outside

> test security-policy-match application dns
source <CLIENT-IP> destination 4.2.2.1 protocol
17 destination-port 53 from inside to outside
```

ii. Determine which nat rule would be triggered by outbound traffic to udp/53

```
> test nat-policy-match source <CLIENT-IP>
destination 4.2.2.1 protocol 17 destination-port
53 from inside to outside
```

iii. Now make up your patterns to test and explore other testing options

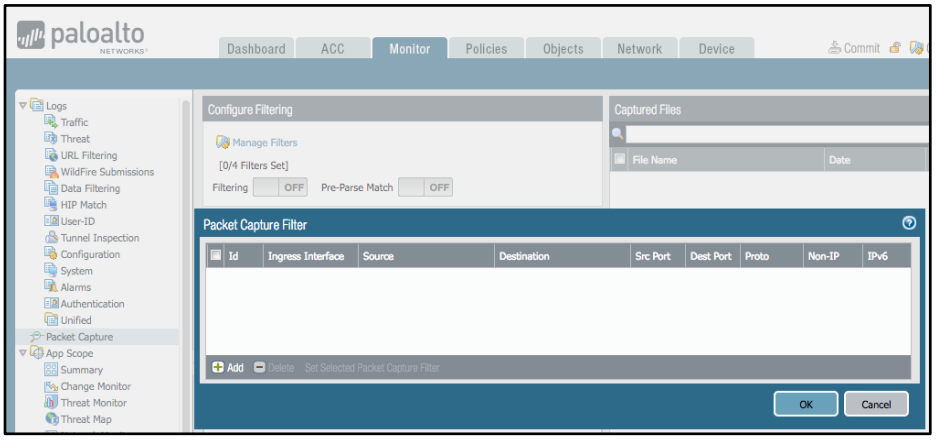
3. Creating Packet Filters

a. Purpose

Packet filters let you define the traffic you are interested in seeing in terms of packet header information. Well defined filters can minimize the resources consumed during a flow basic execution as well as serve as a noise filter when examining the global counters. Filters are global to the firewall and up to 4 filters can be configured at a time. Multiple filters are "OR'd" together when it comes to matching traffic

b. Location

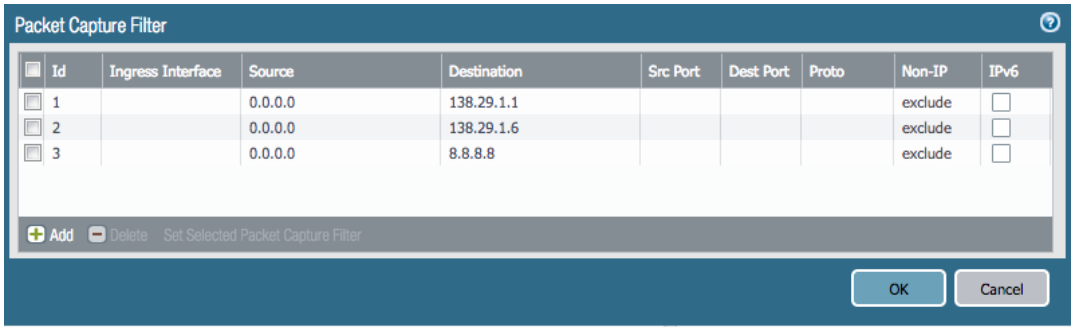
Packet filters are created either in Operational Mode of the command line or in the GUI under ***Monitor → Packet Capture → Configure Filtering → Manage Filters***



c. Building the Filters

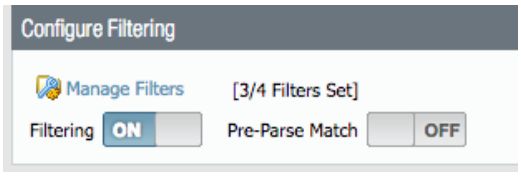
Set up a filter to only look at traffic going to Google DNS (8.8.8.8) and to the IP addresses that the US Coast Guard Academy (www.uscga.edu) website resolves to. (The first command deletes any already existing filters.)

```
> debug dataplane packet-diag clear all
> debug dataplane packet-diag set filter match
destination 138.29.1.1
> debug dataplane packet-diag set filter match
destination 138.29.1.6
> debug dataplane packet-diag set filter match
destination 8.8.8.8
```



d. Confirming and Activating the Filters

```
> debug dataplane packet-diag show setting
> debug dataplane packet-diag set filter on
```



Note: Activating the filters with the above command does not introduce any performance degradation into the system. It simply makes those filters available to the global counter, and packet-diag utilities (which includes flow basic and packet capture functionality)

4. Exploring Global Counters

a. Purpose

Global Counters are an excellent source of information as to why the firewall is taking the actions that it is, especially if the logs in the monitor tab of the firewall are not registering anything. Using global counters in tandem with the filters defined above helps you focus on only relevant data.

b. Location

Global counters can only be accessed from Operational Mode of the command line. There is no place within the GUI where they are visible.

If you use Chrome as a browser, you may want to consider the extension called “Pan(w)achrome” which gives you regularly updated browser access to view counters and other performance metrics from your firewall. More info about it can be found here: https://chrome.google.com/webstore/detail/panwachrome/bbjabfjlgajemfdkmmgjmjmhfaaicfph

c. The “delta” option

The addition of “delta yes” to the command gives you the counter data collected since the last time the command was run. This gives you the ability to see the rate at which counters are incrementing.

i. Explore the current status of your global counters and the delta option

```
# exit
> show counter global filter severity drop
> show counter global filter severity drop delta yes

<WAIT ABOUT 10 SECONDS>

> show counter global filter severity drop delta yes
```

```
wkintz@prod2pa-500(active)> show counter global filter severity drop delta yes

Global counters:
Elapsed time since last sampling: 21.252 seconds

name                                value     rate severity  category  aspect    description
------------------------------------------------------------------------------
flow_ipv6_disabled                      2        0 drop      flow      parse     Packets dropped: IPv6 disabled on interface
flow_tcp_non_syn_drop                   1        0 drop      flow      session   Packets dropped: non-SYN TCP without session match
flow_fwd_l3_bcast_drop                  2        0 drop      flow      forward   Packets dropped: unhandled IP broadcast
flow_fwd_l3_mcast_drop                 35        1 drop      flow      forward   Packets dropped: no route for IP multicast
flow_fwd_l3_noarp                      14        0 drop      flow      forward   Packets dropped: no ARP
flow_tunnel_encap_err                   1        0 drop      flow      tunnel    Packet dropped: tunnel encapsulation error
------------------------------------------------------------------------------
Total counters shown: 6
------------------------------------------------------------------------------
```

ii. Explore other counter categories available, with and without the "delta yes," and the outputs produced.

```
> show counter global filter category ?
> show counter global filter severity ?
> show counter global filter aspect ?
```

iii. From a browser on your student desktop, generate web traffic of your choosing – http/https/dns/ping/etc and see how that impacts the counters using the above commands with the "delta yes" option

iv. Which counters might be useful for troubleshooting various different scenarios that you may encounter?

5. Creating a Flow Basic Capture

a. Purpose

The flow basic capture provides an in-depth and step-by-step visibility into every decision the firewall makes concerning a session as its processed through the device.

b. Location

Flow basic is executed from Operational Mode of the command line. There is no place within the GUI where it can be executed or the results viewed.

c. Enabling flow basic

i. The first step is setting up tight filters to hone in on the traffic sessions we are trying to analyze, which we already have

completed in step 3c above.

ii. Now, after clearing out any lingering data from a previous run, we activate the flow basic feature

```
> debug dataplane packet-diag clear log log
> debug dataplane packet-diag set log feature
flow basic
> debug dataplane packet-diag set log on
```

```
wkintz@prod2pa-500(active)> debug dataplane packet-diag clear log log

dataplane debug logs cleared
wkintz@prod2pa-500(active)> debug dataplane packet-diag set log feature flow basic

wkintz@prod2pa-500(active)> debug dataplane packet-diag set log on

Packet log is enabled
wkintz@prod2pa-500(active)>
```

iii. Once activated, generate some traffic that matches your filters. In our case based on the filters we defined in step 3c, browsing around the CGA website a few clicks will do the trick.

iv. Once we are done testing, we need to turn flow basic logging off

```
> debug dataplane packet-diag set log off
```

```
wkintz@prod2pa-500(active)> debug dataplane packet-diag set log off

Packet log is disabled
wkintz@prod2pa-500(active)>
```

v. Wait 15-20 seconds for caches to flush

vi. Separate log files are generated for each data plane on the appliance (the 5000 series and above all have multiple data planes). We need to aggregate that data together to get a full view of what is going on

```
> debug dataplane packet-diag aggregate-logs
```

```
wkintz@prod2pa-500(active)> debug dataplane packet-diag aggregate-logs


pan_packet_diag.log is aggregated


wkintz@prod2pa-500(active)>
```

vii. Now we can view the results. Pick a session and trace the path the session is taking through the firewall. The command you use is platform dependent. The vm, 200, & 220 series all use the mp-log variant. All other platforms use the dp-log variant.

```
> less mp-log pan_packet_diag.log
```

or

```
> less dp-log pan_packet_diag.log
```

You can follow along this output, matching packets to a session via the session ID, in the flowchart contained in the "PANOS Packet Flow" tech note, which is available both from the PAN community forum (https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081) as well as at the end of this lab exercise. Some examples of what the flow basic output looks like are below:

```
== 2017-12-01 15:05:42.540 -0500 ==
Packet received at ingress stage
Packet info: len 60 port 17 interface 17 vsys 1
  wqe index 228061 packet 0x0x8000000416a690ce
Packet decoded dump:
L2:     00:a0:c8:d7:de:a9->00:1b:17:00:01:11, type 0x0800
IP:     65.55.44.109->74.202.224.196, protocol 6
        version 4, ihl 5, tos 0x00, len 40,
        id 27625, frag_off 0x4000, ttl 112, checksum 1460
TCP:    sport 443, dport 63563, seq 2325853110, ack 1783021297,
        reserved 0, offset 5, window 513, checksum 45833,
        flags 0x0010 ( ACK), urgent data 0
TCP option:
Flow lookup, key word0 0x1bbf84b00020600 word1 0
Flow 102145 found, state 2, HA 0
Active flow, enqueue to fastpath process
```

```
== 2017-12-01 15:05:42.541 -0500 ==
Packet received at fastpath stage
Packet info: len 60 port 17 interface 17 vsys 1
  wqe index 228061 packet 0x0x8000000416a690ce
Packet decoded dump:
L2:     00:a0:c8:d7:de:a9->00:1b:17:00:01:11, type 0x0800
IP:     65.55.44.109->74.202.224.196, protocol 6
        version 4, ihl 5, tos 0x00, len 40,
        id 27625, frag_off 0x4000, ttl 112, checksum 1460
TCP:    sport 443, dport 63563, seq 2325853110, ack 1783021297,
        reserved 0, offset 5, window 513, checksum 45833,
        flags 0x0010 ( ACK), urgent data 0
TCP option:
Flow fastpath, session 51072
NAT session, run address/port translation
0%
```

```
== 2017-12-01 15:05:42.541 -0500 ==
Packet received at forwarding stage
Packet info: len 139 port 0 interface 17 vsys 1
  wqe index 225991 packet 0x0x80000004169fa8c6
Packet decoded dump:
L2:     00:1b:17:00:01:11->00:70:76:69:66:00, type 0x0800
IP:     74.202.224.194->73.129.41.234, protocol 6
        version 4, ihl 5, tos 0x00, len 125,
        id 12494, frag_off 0x0000, ttl 64, checksum 43701
TCP:    sport 443, dport 56130, seq 2499651571, ack 504653042,
        reserved 0, offset 5, window 65535, checksum 12702,
        flags 0x0018 ( ACK PSH), urgent data 0
TCP option:
Forwarding lookup, ingress interface 17
L3 mode, virtual-router 4
Route lookup in virtual-router 4, IP 73.129.41.234
Route found, interface ethernet1/2, zone 2, nexthop 74.202.224.193
Resolve ARP for IP 74.202.224.193 on interface ethernet1/2
ARP entry found on interface 17
Transmit packet on port 17
```

viii. Matches against policy rules are displayed in terms of rule index numbers which are not visible in the GUI. To obtain the mapping of index number to rule name, use these following commands:

```
> debug device-server dump idmgr type nat-rule
all
> debug device-server dump idmgr type security-
rule all
```

```
wkintz@prod2pa-500(active)> debug device-server dump idmgr type security-rule all

ID         Name
---------- --------------------
1          rule1
2          general interest
3          deny the rest
4          protect-all
5          Block-1.254
6          general internet
7          DENY THE REST
8          attack test
9          attack
10         vwire_traffic
11         log_traffic
12         inbound traffic protection
13         Microsoft Product Updates
14         outbound traffic protection
15         Block Malicious Sites
16         allow safe social networks
17         alert-all
18         deny p2p
19         Allow MKT Google
20         allow skype-probe
```

or if you have a specific index you need to look up

```
> debug device-server dump idmgr type nat-rule id XX
> debug device-server dump idmgr type security-rule
id XX
```

```
wkintz@prod2pa-500(active)> debug device-server dump idmgr type security-rule id 23

website access
```

to see all the different mappings you can cross reference in this way, perform this command:

```
> debug device-server dump idmgr type ??
```

ix. Interfaces are also numbered in this output. The mapping of interfaces to their id numbers can be found vis this command:

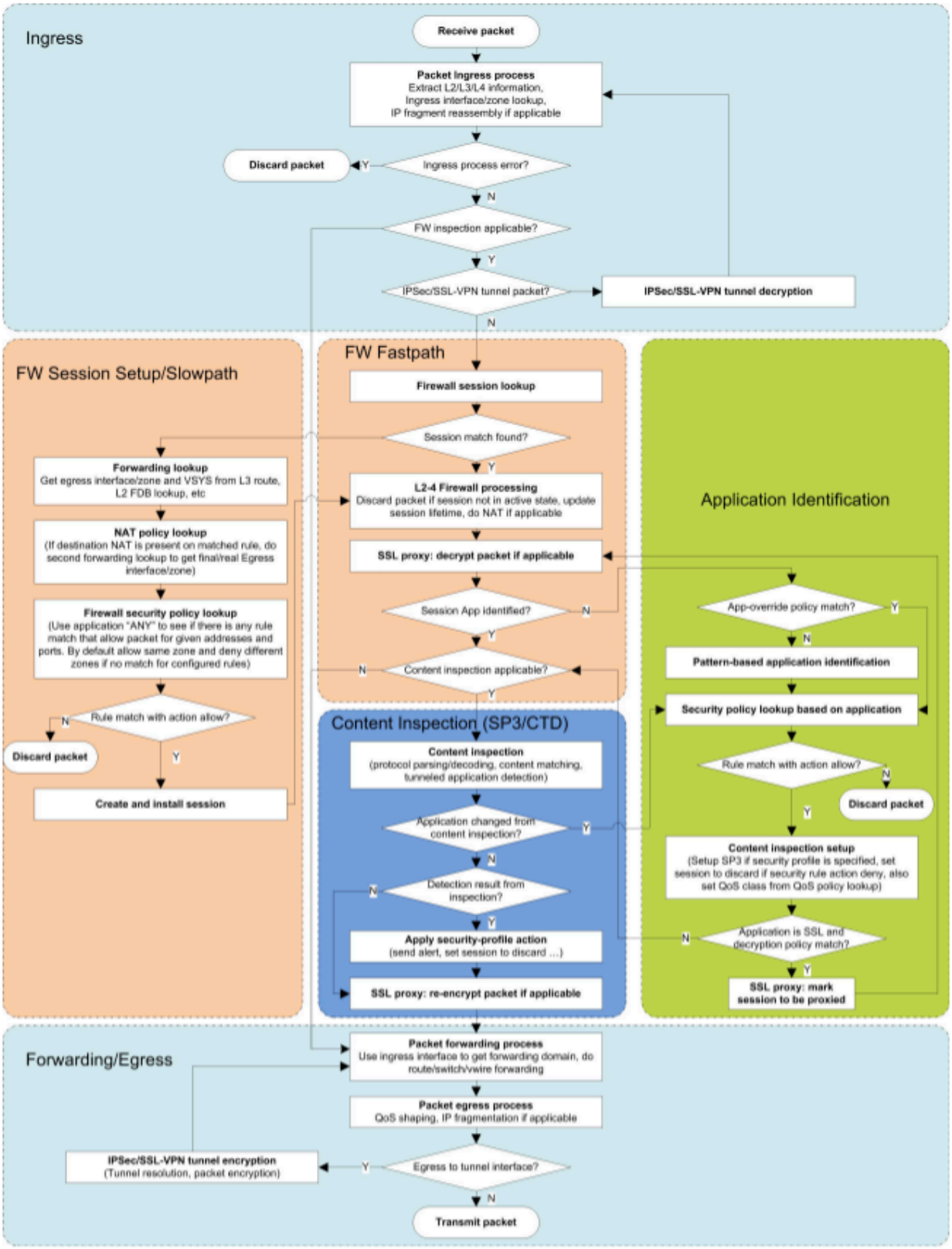
```
> show interfaces all
```

```
wkintz@prod2pa-500(active)> show interface all

total configured hardware interfaces: 11

name                    id    speed/duplex/state        mac address
--------------------------------------------------------------------------------
ethernet1/1             16    1000/full/up              00:1b:17:00:01:10
ethernet1/2             17    1000/full/up              00:1b:17:00:01:11
ethernet1/3             18    1000/full/up              00:1b:17:00:01:12
ethernet1/4             19    1000/full/up              00:1b:17:00:01:13
ethernet1/5             20    1000/full/up              00:1b:17:00:01:14
ethernet1/6             21    ukn/ukn/down(autoneg)     00:1b:17:00:01:15
ethernet1/7             22    1000/full/up              00:1b:17:94:15:16
ethernet1/8             23    1000/full/up              00:1b:17:94:15:17
vlan                    1     [n/a]/[n/a]/up            00:1b:17:00:01:01
loopback                3     [n/a]/[n/a]/up            00:1b:17:00:01:03
tunnel                  4     [n/a]/[n/a]/up            00:1b:17:00:01:04

aggregation groups: 0
```


Ingress
Receive packet
Packet Ingress process
Extract L2/L3/L4 information,
Ingress interface/zone lookup,
IP fragment reassembly if applicable
Discard packet
Y
Ingress process error?
N
FW inspection applicable?
Y
IPSec/SSL-VPN tunnel packet?
IPSec/SSL-VPN tunnel decryption
N
FW Session Setup/Slowpath
FW Fastpath
Application Identification
Firewall session lookup
Session match found?
Y
Forwarding lookup
Get egress interface/zone and VSYS from L3 route, L2 FDB lookup, etc
L2-4 Firewall processing
Discard packet if session not in active state, update session lifetime, do NAT if applicable
NAT policy lookup
(If destination NAT is present on matched rule, do second forwarding lookup to get final/real Egress interface/zone)
SSL proxy: decrypt packet if applicable
Firewall security policy lookup
(Use application "ANY" to see if there is any rule match that allow packet for given addresses and ports. By default allow same zone and deny different zones if no match for configured rules)
Session App identified?
N
Y
App-override policy match?
Y
N
Pattern-based application identification
Content inspection applicable?
N
Y
Security policy lookup based on application
Rule match with action allow?
N
Y
Discard packet
Create and install session
Content Inspection (SP3/CTD)
Content inspection
(protocol parsing/decoding, content matching, tunneled application detection)
Application changed from content inspection?
Y
N
Rule match with action allow?
N
Y
Discard packet
Content inspection setup
(Setup SP3 if security profile is specified, set session to discard if security rule action deny, also set QoS class from QoS policy lookup)
Detection result from inspection?
N
Y
Apply security-profile action
(send alert, set session to discard ...)
Application is SSL and decryption policy match?
N
Y
SSL proxy: re-encrypt packet if applicable
SSL proxy: mark session to be proxied
Forwarding/Egress
Packet forwarding process
Use ingress interface to get forwarding domain, do route/switch/vwire forwarding
Packet egress process
QoS shaping, IP fragmentation if applicable
IPSec/SSL-VPN tunnel encryption
(Tunnel resolution, packet encryption)
Y
Egress to tunnel interface?
N
Transmit packet

The Next Steps

If you want to test this on your own and do not have access to a lab environment to do so, you have a couple options:

a. Contact your Sun Management Account Rep to get pricing on a lab bundle. The newly released PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

If you are unsure who your Account Rep is or do not have one yet, you can reach out to **sales@sunmanagement.net** for assistance.

b. Reach out through the free Fuel Users Group (www.fuelusersgroup.org) which at the time this lab is being written is offering limited free access to a virtual lab environment, which they refer to as their "Virtual Test Lab," in which you can practice the steps outlined above. (Note: The Fuel Users Group may alter or discontinue offering their "Virtual Test Lab" at any time)

If you feel Sun Management brings value to you and your organization with these labs, please keep us in mind for other network and network security related requirements. We are here to help you. Thank you for your business.

Please direct any questions/comments/feedback on this lab exercise to:
education@sunmanagement.net

Lab Author: *William J Kintz*
Sun Management's Chief Instructor and Director of Engineering

Last Modified: *Nov 30, 2017*