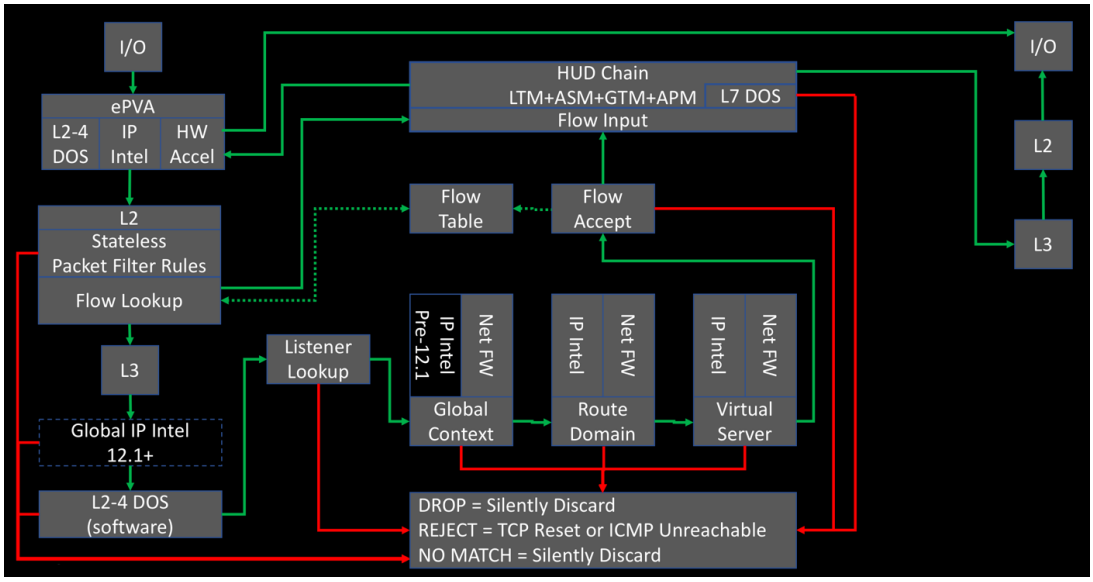
Packet Tracing in BIG-IP AFM

Jason Rahm, 2017-30-03

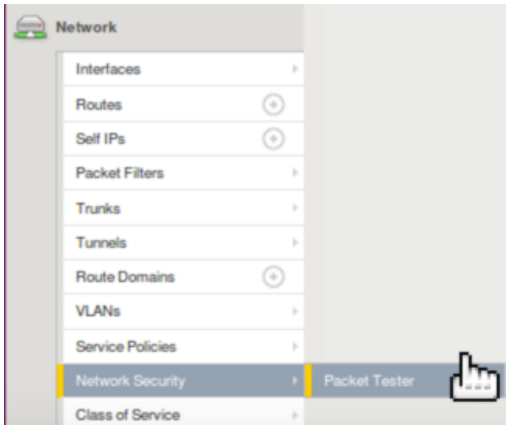
New in the v13 release of the BIG-IP Advanced Firewall Manager is the capability to insert a packet trace into the internal flow so you can analyze what component within the system is allowing or blocking packets based on your configuration of features and rule sets.

If you recall from our Lightboard Lesson on the BIG-IP Life of a Packet, the packet flow diagram looks like this:

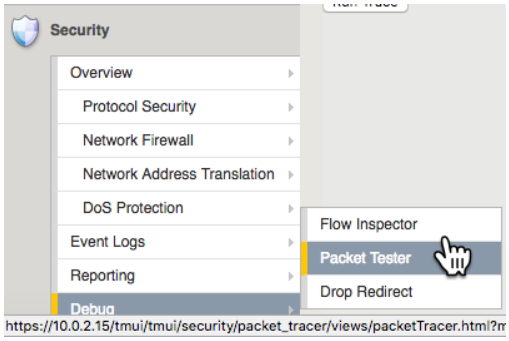


The packet tracing is inserted at L3 immediately prior to the Global IP intelligence. Because it is after the L2 section, this means that a) we cannot capture in tcpdump so we can't see them in flight and b) no physical layer details will matter as it relates to testing. That said, it's incredibly useful for what is and is not allowing your packets through. You can insert tcp, udp, sctp, and icmp packets, with a limited set of (appropriate to each protocol) attributes for each.

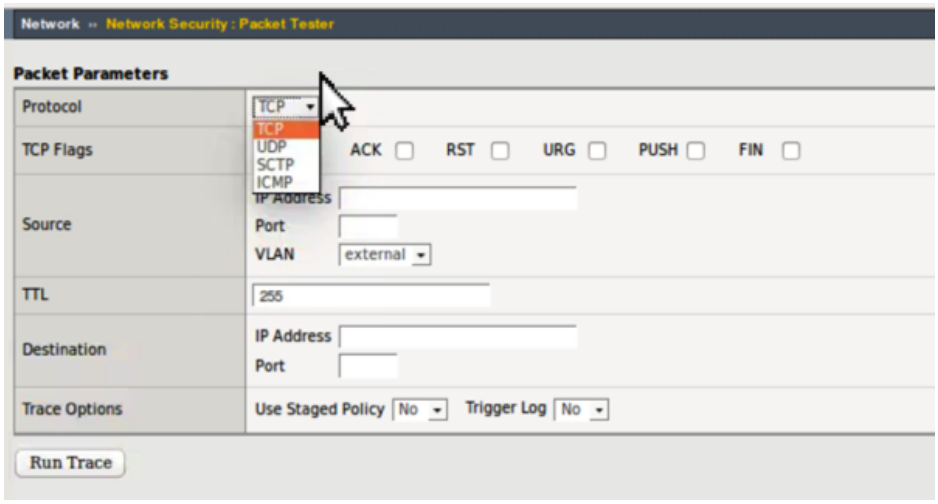
To get to the packet trace utility in the GUI, navigate to Network->Network Security->Packet Tester as show below.



Note: In v13.1 this feature has been moved to Security -> Debug -> Packet Tester.

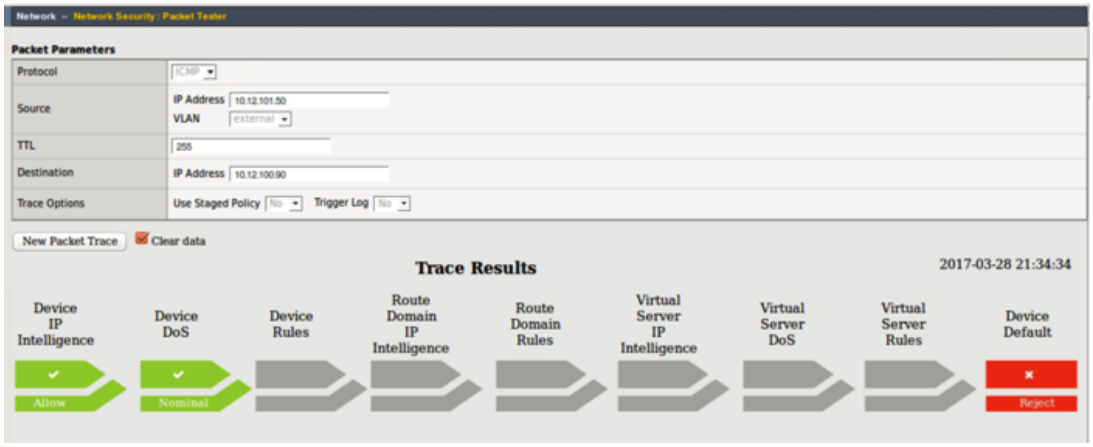


This will launch the packet testing tool as shown here:



Note with this tcp selection, in addition to setting the flags, you can configure the source and destination ip/port, source vlan, and trace options as it relates to policy and logging.

An example packet trace shows the output of the trace after it completes:



You'll notice here that IP Intelligence and DoS have no beef with the packet, but there is no virtual match so the default action at the end of the path is to reject.

Note that you can also use the packet trace utility in tmsh. The command is `tmsh show net packet-tester security` and results in an output like below.

```
tmsh show net packet-tester security protocol tcp syn src-addr 192.168.101.2 src-port 21233 dst-addr

************************
Packet Tester Data:
************************
```

```
Packet SrcIP/Port:192.168.101.2/21233 Src Vlan external
Packet DstIP/Port:192.168.101.55/8080
Packet Protocol: tcp
Packet Trace Option: Check Staged:Disable, Trigger Log:Disable

Stage:Device-IP Intelligence
Result: Default

Stage:Device-DoS
Result: Default

Stage:Device-Access Control
Result: Drop

Stage:Route Domain-IP Intelligence (unset)
Result: Default

Stage:Route Domain-Access Control (unset)
Result: Drop

Stage:Listener-IP Intelligence (No Listener)
Result: Default

Stage:Listener-DoS (No Listener)
Result: Default

Stage:Listener-Access Control (No Listener)
Result: Drop

Stage:Device Default
Result: Drop

Final Result
Packet SrcIP/Port:192.168.101.2/21233 Src Vlan external
Packet DstIP/Port:192.168.101.55/8080
Packet Protocol: tcp
Packet Trace Option: Check Staged:Disable, Trigger Log:Disable
Stage:Device-Access Control
Policy Name: unset
Rule Name: unset
Stage:Route Domain-Access Control
Route Domain name: unset
Policy Name: unset
Rule Name: unset
Stage:Listener-Access Control
Listener name: unset
Policy Name: unset
Rule Name: unset
Default Rule : No
Device Default Rule
Final Action : Drop
Total records returned: 1
```

And because of tmsh, you can easily script packet generation with bash or even a tmsh script if you're feeling the Tcl love.

Current Limitations

Current Limitations

- Only one packet can be inserted at a time, so even a scripted experience via tmsh will result in very low packets per second, which isn't likely to really impact DoS for valid tests.
- Only valid headers are allowed, so a large part of typical red team attack vectors are not covered.
- No tcpdump visibility.
- No hardware paths.

Basic visibility tools like the packet tester are great additions to the BIG-IP AFM. Whether it's for testing new rules, validating existing ones, or simply throwing a bone over the fence to your operational security team to know where in your configuration an isolated action is being trapped, the v13 AFM packet tester has you covered!

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com