Cisco Firepower Threat Defense (FTD) Packet Flow

It’s important to understand the packet flow for a FTD device. By understanding the flow you can both troubleshoot and create true policy, and knowing your detection process will impact 2 things:

• How you analyze the data
• How you tune your security appliance

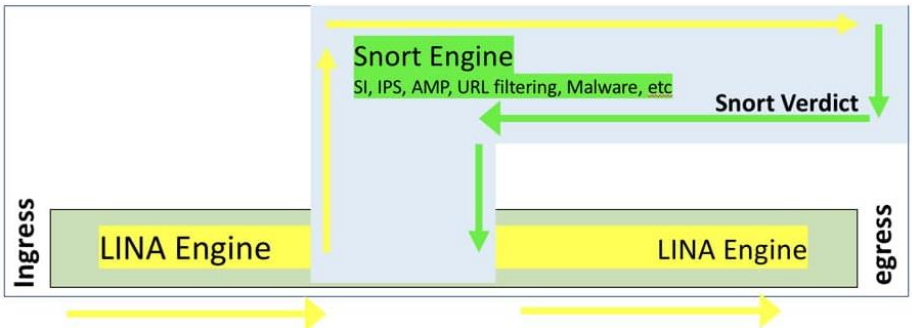
Optimizing detection also becomes easier when you understand the complete path a packet (and the flow) takes through the FTD device. Here are two key optimization points to remember:

- Layer 2-4 traffic that can be matched and either blocked or allowed with FastPath will be handled entirely in hardware.
- Layer 3 Security Intelligence is the first detection that occurs in the Snort process (Now called Firepower layer). All of this traffic will be blocked and no other additional inspection will occur. This optimized your treat monitoring by stopping active threat companies without the need for additional threat analysis.

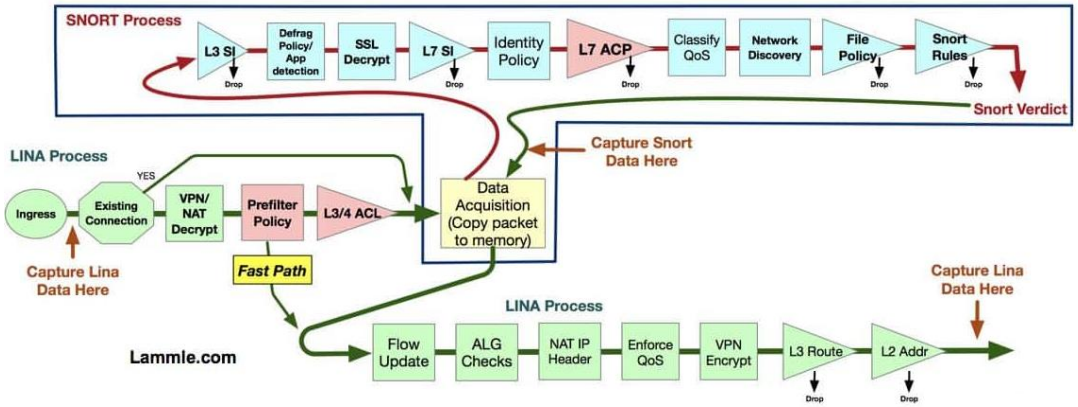
Understand that there are 2 main engines in the FTD unified software image: Lina and Snort. Lina is the ASA code that FTD runs on, and the snort process is the network analysis of the packets that goes from security intelligence (SI) through the ACP inspection of the traffic by the Snort IPS rules.

Here is an overview of the packet flow:

- When a packet enters the ingress interface and it is handled by the LINA engine
- The packet is inspected by the Snort engine, if configured to do so; this can include SI, IPS, AMP, URL filtering among other inspections.
- The Snort engine returns a verdict for the packet
- It’s important to note that the Snort engine does not drop anything, but instead marks the packet drop or forward, based on the snort verdict.



Lina does the process of layer 2, routing, NAT, VPN, PreFilter, and layer 3-4 access control policy rules before the snort process takes over the analysis. The Lina code takes over again after the default action of the ACP and again does layer 2, routing, NAT, VPN, etc.



After a packet makes it through the Lina without being killed by the PreFiler or layer 3/4 ACP, then it starts traversing the Snort process by going through the Layer 3 Security Intelligence (SI) White and Blacklist. If the packet does make it through the Blacklist, by either not being in the Blacklist or by being in the Whitelist (the Whitelist only exists to override the Blacklist), then application detection can take place.

If there is an SSL policy, the packets can be decrypted and possibly dropped here, if not, it will then go through the L7 SI URL and DNS list and feeds. Authentication can now take place, either actively or passively via an Identity Policy.

Now finally, the packets will be compared to the rules in the main Access Control policy (L7 ACL). Packets can be dropped, passed or even trusted and sent to Egress. It's important to understand that the packets can be passed before the Snort process by using the PreFilter FastPath rules, or ACP layer 3/4 trust rules. However, remember that the PreFilter is only layer 3/4 whereas the ACP is through L7.

Interface QoS policing can be applied here (but is actually enforced in LINA), and Network Discovery can be configured to either passively or actively gather host/user/application information to help in network analysis.

If configured, URL filtering and the Malware/file policy will be enforced as well as the IPS rules against the traffic. AMP takes the packets and assembles them into files if they match the protocol in the file policy rule. Files that match the malware and file policy can be inspected against data in the cloud, have local malware checks performed or the files themselves may be transfered to a sandbox for inspection. If traffic makes it through the file inspection process it will finally be evaluated against the enabled Snort IPS rules.

Finally, assuming the packets are still alive, the packets will be handed to the Lina process for layer 2, routing, NAT, VPN, etc.