Securing Networks with

Cisco FTD

Chapter 6

Capturing Traffic for Advanced Analysis

Mohsen Kheradmand

Packet Capture Essentials

FTD has various advanced security technologies, such as:

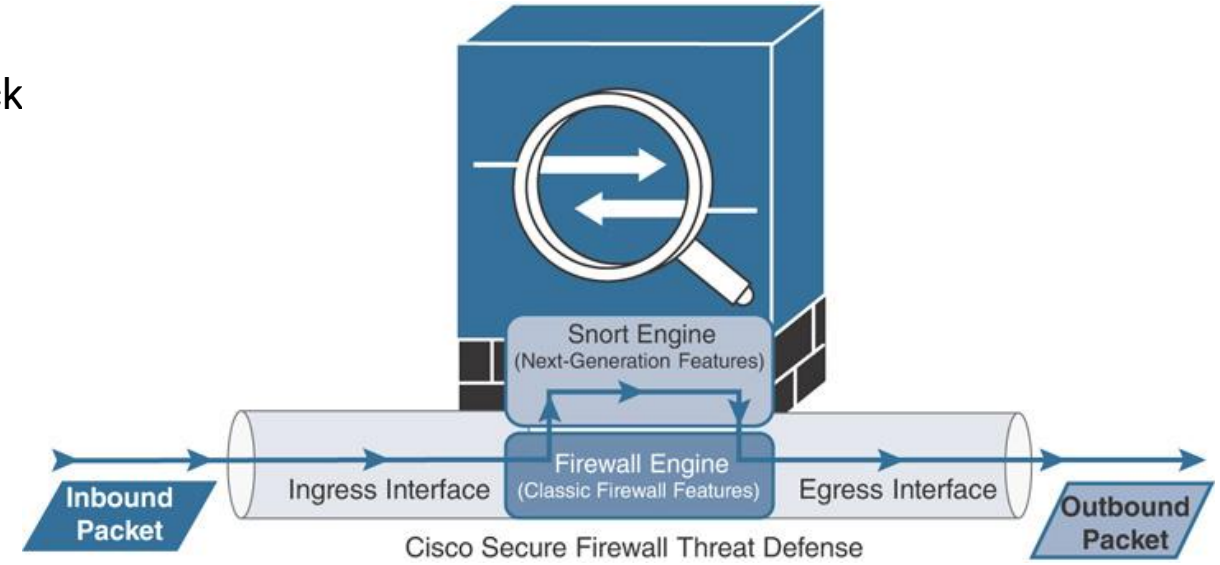
Network discovery, security intelligence, application control, file control, and an intrusion detection and prevention system

- Any of these security components could Block the traffic from the ingress to the egress interface
- In this case , it is essential to analyze packets to determine the root cause of the issue

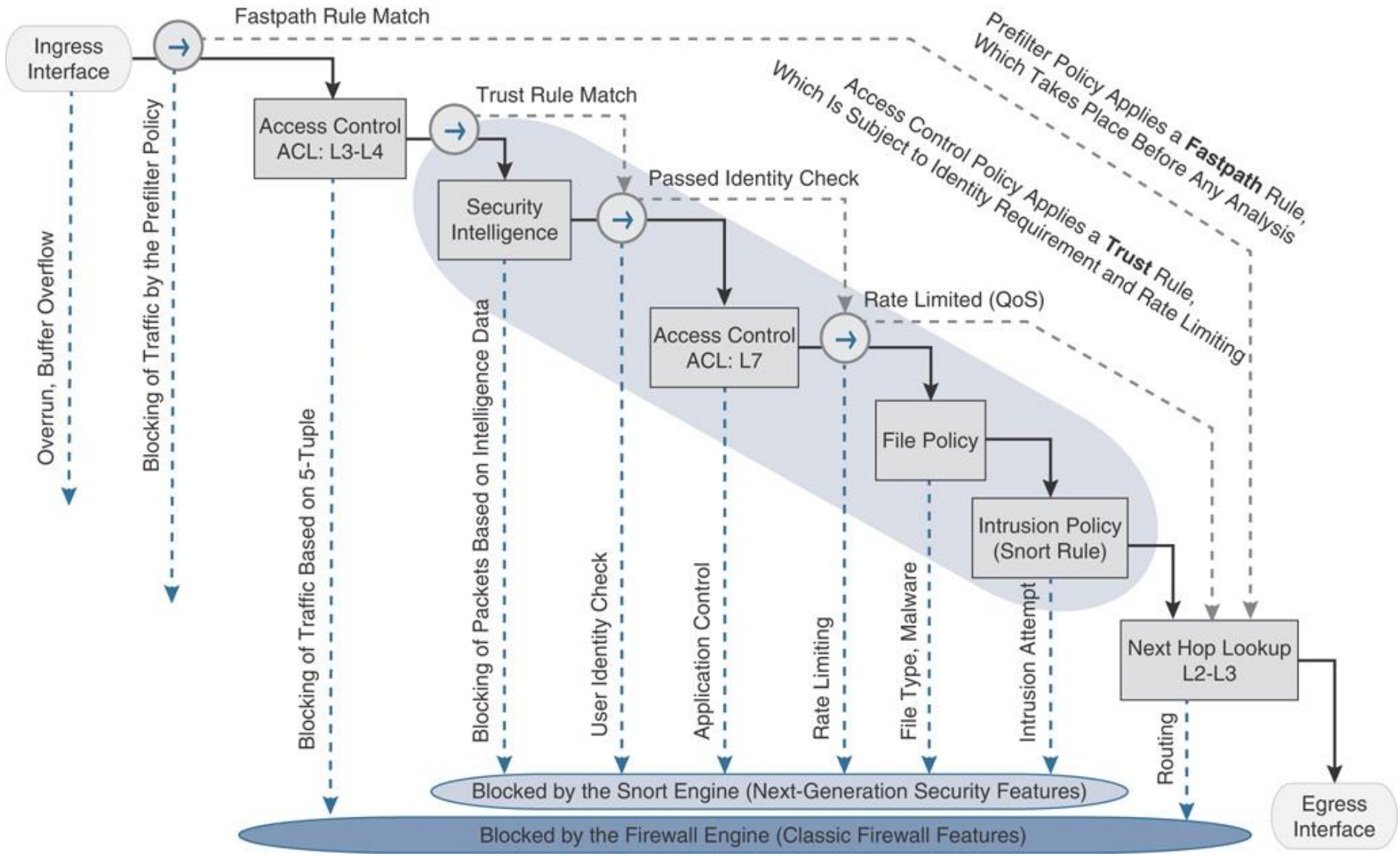
Primarily, two types of security engines analyze the pack

- Snort engine
- Firewall engine

Packet Analysis can be a great troubleshooting step to determine the engine or the component that is responsible for drops



Potential Reasons for a Packet Drop by a Threat Defense



Note : Before you consider capturing traffic

A. The primary goal of a FTD is controlling and inspecting traffic,capturing live traffic is only for troubleshooting purposes , to capture traffic for a long period, you need a dedicated system

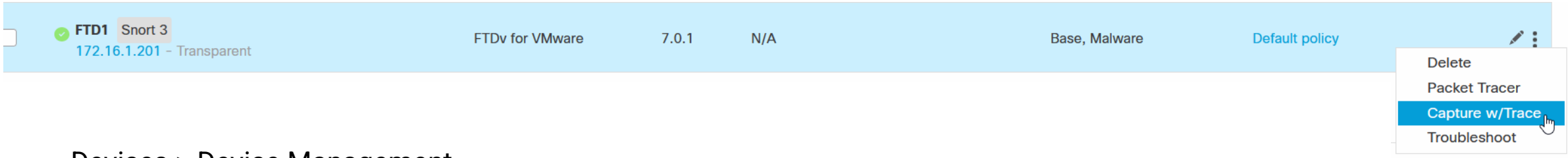
B. Capturing live traffic is CPU consumer (When necessary, capture traffic during a maintenance window)

C. Specify a source and destination and protocol type about capturing traffic instead of all broadcast traffic

D. Use the “Stop When Full” feature to limit the number of packets to capture (prevent Buffer overflow)

E. Using FMC GUI , you can capture , manage and save the captured packets to PCAP file (better performance)

Capturing of Packets via FTD

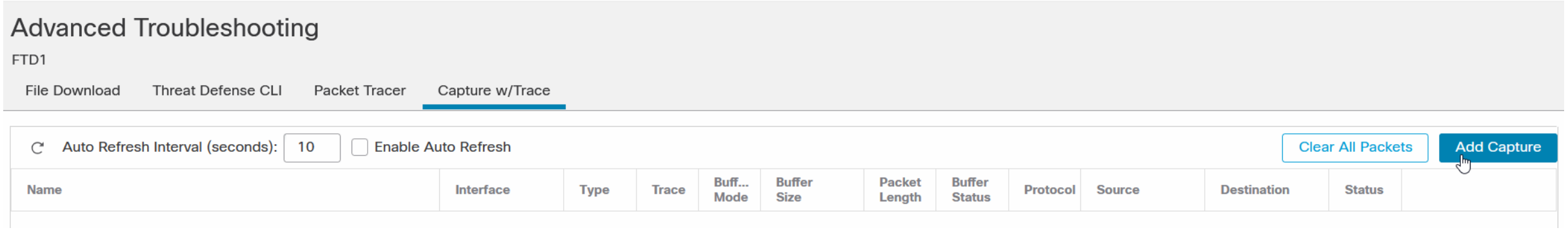


Devices > Device Management

Select the **Capture w/Trace** option by click on dotted icon

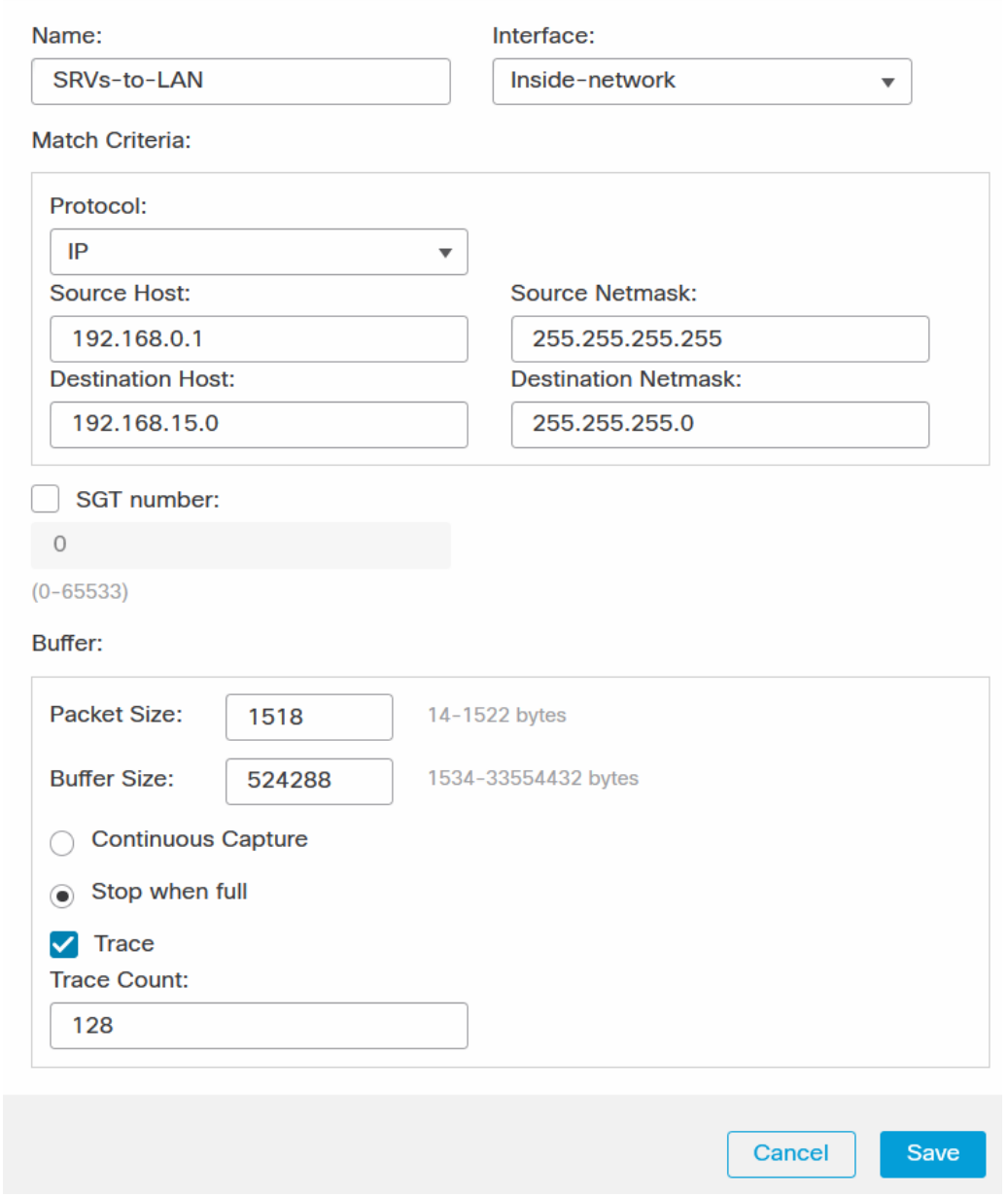
On the *Advanced Troubleshooting* page, go to the *Capture w/Trace tab*

Click the **Add Capture** button

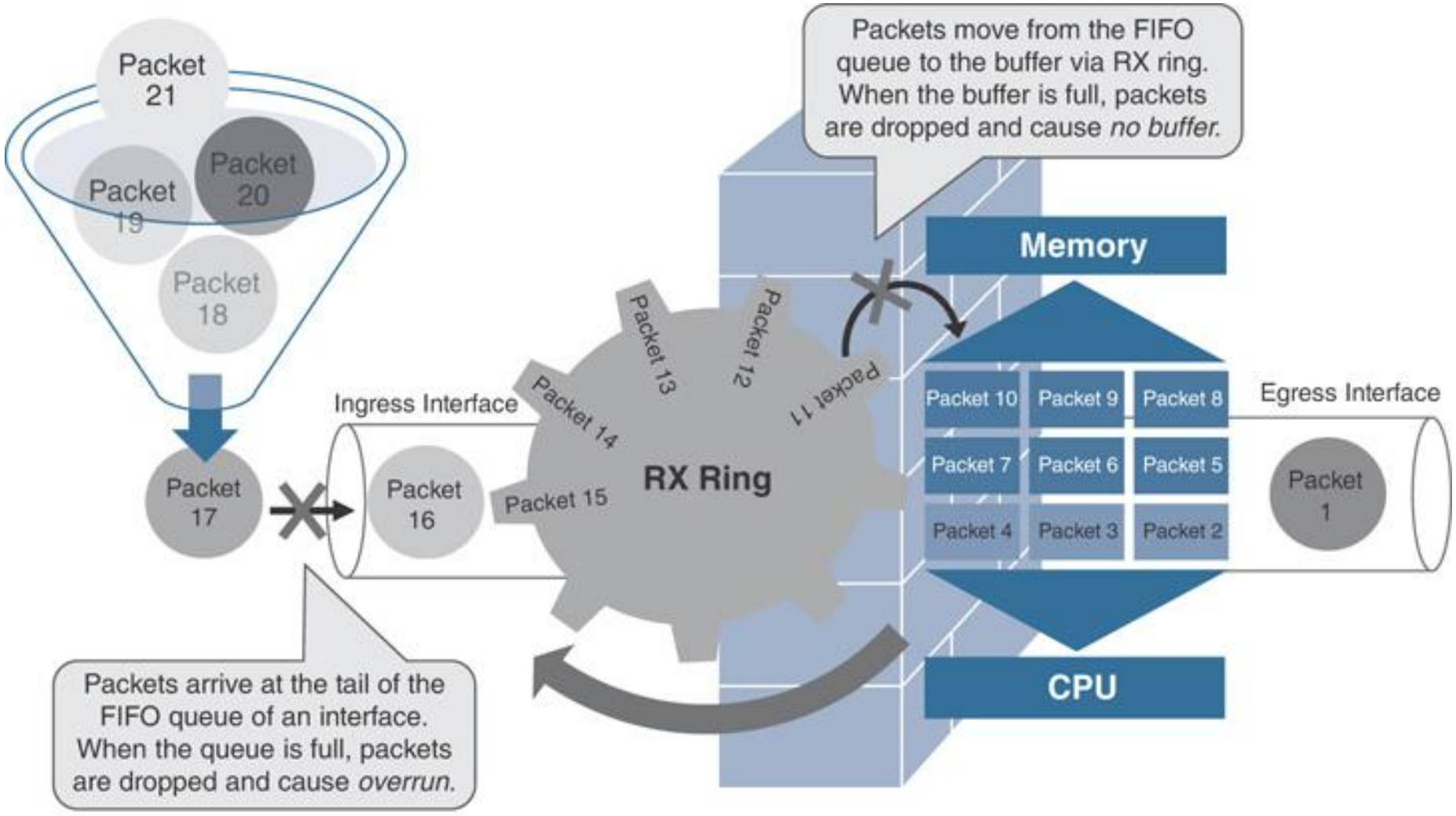


Capturing of Packets via FTD

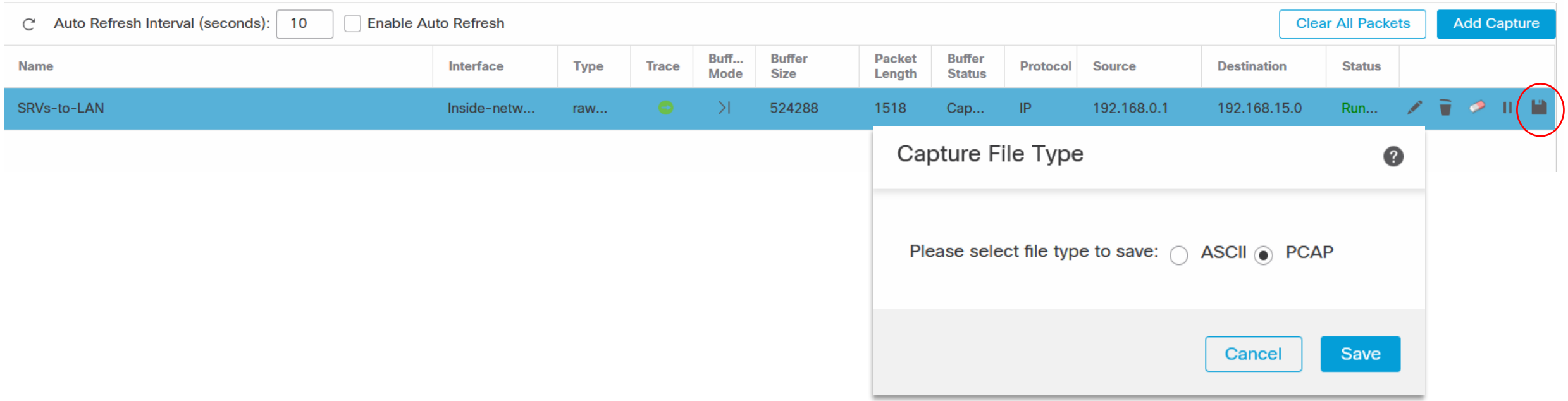
1. Enter a name for this process
2. Select an interface to capture traffic
3. Select protocol type from list to monitor (IP,GRE, TCP,UDP, …)
4. Enter Source and Destination of traffic to monitor
5. Packet size and Buffer size are optional
6. Select Stop when full (prevent buffer overflow)
7. Trace : view the action of FTD components about every packet
8. Trace count : limit the number of packet to trace
9. Click Save. The capture process should start automatically.



Impact on Packets When the Buffer Is Full

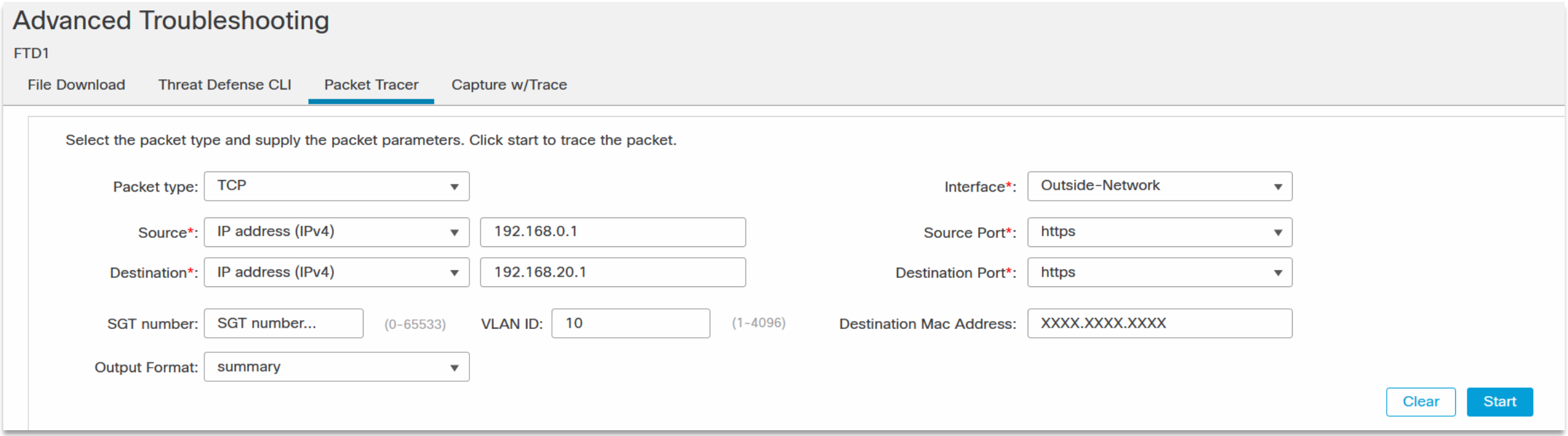


Verification and save to file



- You can also save the original packets in the PCAP / ASCII file
- It is usable to open the file in a packet analyzer like Wireshark
- PCAP files are critical to an incident response team for forensic analysis

Packet Capture versus Packet Tracer



- The packet tracer tool , simulate the flow of a packet based on the security policies you deployed on a FTD
- The tool uses that information to create a virtual packet.
- After you start, the virtual packet is evaluated against the security policies deployed on a threat defense.
- The impact on a virtual packet can enable you to predict the potential impact of the security policies on live traffic