Hillstone T-Series Intelligent Next-Generation Firewall Whitepaper: Configuration and Operation Analysis using Packet Route Inspection

Keywords: Intelligent Next-Generation Firewall (iNGFW), Packet Route Inspection, Online Inspection, Inspection Simulation, Import Inspection, Operation Visualization.

Abstract: This paper describes the packet inspection analysis and troubleshooting capabilities of the Hillstone T-Series Intelligent Next Generation Firewall (iNFW). The firewall automatically traces and collects information on packet processing and inspection. With the firewall's report on this analysis, the administrator can quickly discover misconfigurations, resolve network issues and simulate planned future deployments. With these iNGFW capabilities you can proactively avoid security compromises as well as reduce the risk of launching new services in your network.

1 Overview

A misconfigured firewall results in interrupted security services and compromises security protection against ever-present threats. It is imperative that network administrators have advanced tools at their disposal to proactively verify existing firewall configurations, test planned configuration changes, and troubleshoot issues rapidly to their root causes.

The Hillstone T-Series intelligent Next-Generation Firewall (iNGFW) includes patented Packet Route Inspection technology that provides the administrator with superior capabilities to verify and troubleshoot firewall configuration and packet inspection.

2 Using Firewall Analysis on the iNGFW Product

The iNGFW system allows you to trace packet interactions as they pass through the processing modules of the system. Within minutes, the iNGFW system displays the results in a graphic report, automatically troubleshoots any issues found, and presents root causes and resolution recommendations. Figure 1 shows the sequence of steps during firewall packet inspection.

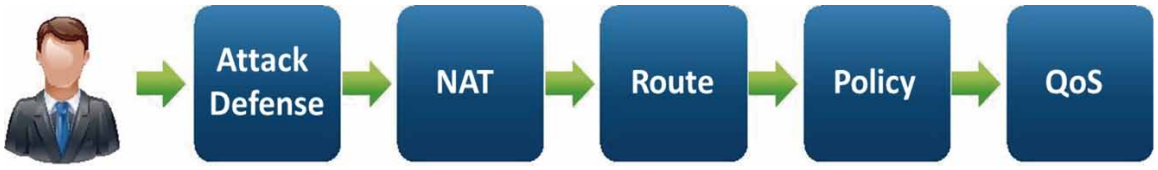

Figure 1: Steps in Packet Processing Analysis

The Packet Route Inspection capability of the iNGFW significantly reduces time spent troubleshooting and resolving issues related to firewall configuration or operation. The iNGFW analysis and reporting tools allow you to resolve issues quicker, more accurately and reduce or avoid impacts to business services.

The iNGFW collects data from the packet processing done in each of the firewall's modules. Along with configurations, device resource data, threat data and other stored information, the iNGFW system is able to conduct a comprehensive analysis of packet processing. The results are presented in a graphic report, shown in Figure 2, and include a packet route diagram, the inspection source, the inspection time, the inspection results, the inspected packets, issue causes, and resolution recommendations.

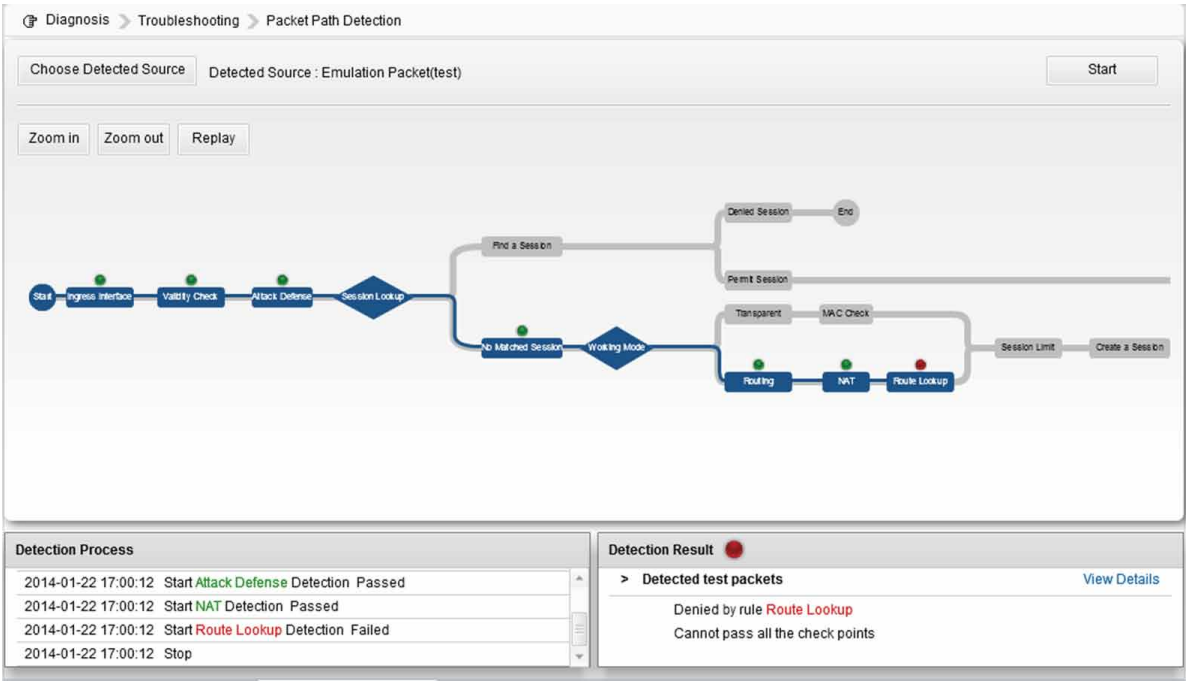

Figure 2: Packet Inspection report Example

The iNGFW Packet Route Inspection capability benefits you in three specific areas of network administration:

- **Verify firewall configuration and operation** and proactively discover issues during scheduled maintenance windows
- **Resolve issues quickly** with rapid root cause identification
- **Test new services** with simulated network traffic before making them active

2.1 Verify Operation and Configuration

During a scheduled maintenance window the administrator can proactively run iNGFW Packet Route Inspection tools to verify that the current configuration is operating as intended. Firewall misconfigurations, or unintended gaps in security protection can be discovered quickly and remedied before they impact business services.

2.2 Accelerate Issue Resolution

In the event that a network problem occurs, the iNGFW Packet Route Inspection tools can help troubleshoot the issue. The tools automatically analyze firewall packet processing and generate a report to help the administrator locate and resolve the issue.

2.3 Simulate New Services

New services and configuration changes present the potential to disrupt network operation. The iNGFW Packet Route Inspection tools allow the administrator to simulate traffic through a planned configuration and consult the report before the new configuration or traffic flow is activated. This allows the administrator to guarantee intended operation in the network when a new service is launched or a configuration change is implemented.

3 Packet Processing Analysis Tools

The iNGFW Packet Route Inspection capability traces packets as they pass through the firewall modules to provide a better understanding of internal packet processing. The technology includes three tools:

- Online inspection
- Simulation of imported data
- Simulation of generated data

3.1 Online Inspection

Online inspection comprises automatic analysis and reporting on actual network traffic through the firewall in real time. The administrator specifies traffic attributes (filter conditions) to be inspected and contained in the report. Examples of traffic attributes include source address, uniform resource locator (URL), source port, destination port, user name, protocol or application.

Any traffic that matches the filter criteria is inspected and included in the report, along with any problems located and recommended solutions for such problems. Figure 3 shows the steps in inspection of actual real-time traffic.

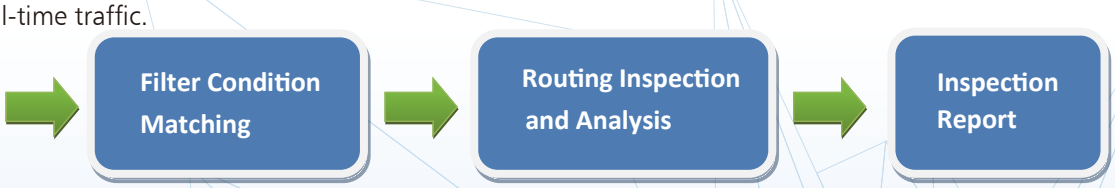

Figure 3: Online Inspection of Actual Traffic

3.2 Simulation of Imported Data

The iNGFW can import a packet from a data file, replay and inspect it, providing results in the same format as the online inspection function. The administrator configures a set of filter conditions for the simulation, such as port, source address, destination address, source port, destination port, application and protocol. The Packet Route Inspection capability then analyzes the data file and simulates the packet interactions that would occur if the firewall were to inspect such a packet. This capability helps the administrator to locate problems in firewalling before live traffic of this type is offered to the firewall.

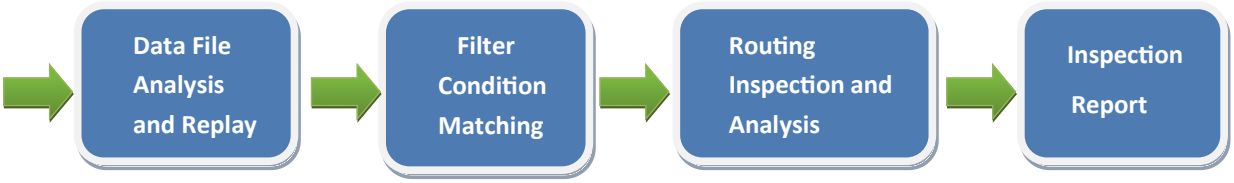

Figure 4: Simulated Inspection of a Packet Imported from a Data File

3.3 Simulation of Generated Data

The iNGFW can generate packet contents with various attributes such as port, source address, destination address, protocol, source port and destination port. The packet is then processed through a simulated inspection similar to that of a packet imported from a data file. This capability helps the administrator verify correct firewall treatment of this type of traffic (perhaps planned as part of a new service launch, or due to deploying a new application) before live traffic of this type is offered to the firewall.

Figure 5: Simulated Inspection of a Generated Packet

4 Conclusion

The iNGFW system offers powerful analysis and troubleshooting capabilities to the network administrator with its patented Packet Route Inspection technology, including:

- **Verifying correct firewall operation and configuration** by using online analysis and reporting of the firewall packet inspection process. Packet contents can also be imported from a data file to simulate, and report upon, the inspection of this imported traffic under various filter conditions.
- **Accelerating issue resolution** by using online analysis and reporting of the firewall packet inspection process. Part of the reporting includes self-analysis by the iNGFW to determine the root

cause as well as suggesting what issues may exist and providing recommendations for resolution.

- **Reduces risk of introducing new services** by using the simulation capabilities of how the firewall would inspect traffic that isn't live yet. The simulated traffic can either be imported from a data file or be auto-generated by the iNGFW. The simulation capabilities help in planning launches and verifying that the firewall configuration is correct before a new service is activated.

These iNGFW capabilities significantly reduce the risk of introducing new traffic and applications to the environment, ensuring that the firewall's configuration is correct to provide maximum security protection to your network and servers. The tools and reports also minimize the time to troubleshoot and correct a problem that may exist in the network or with the firewall's configuration.