

Security Forensics with EndaceProbe™ and Cisco Firepower™



Combining Endace Network Recording with Cisco Firepower's Next Generation Intrusion Prevention Systems (NGIPS) streamlines investigation workflows for rapid response to security threats.

Cisco Firepower NGIPS products provide continuous threat protection before, during and after an attack. The Cisco Firepower Management Console (FMC) is the “nerve center” of the Firepower system. It correlates attacks with real-time network and user intelligence and centrally manages network security and operational functions, including event monitoring, incident prioritization, forensic analysis and reporting.

When it comes to investigating security incidents, access to an accurate, detailed and complete history of network traffic is an unparalleled resource. Detailed packet history provides definitive evidence of what happened, how it happened and what was compromised. It provides the context behind the security alerts raised by Cisco Firepower NGIPS and lets analysts investigate events quickly and respond with the confidence of knowing exactly what took place.

Deploying EndaceProbe Network Recorders alongside Firepower NGIPS appliances or hosting virtual NGIPS (NGIPSV) on EndaceProbes in Application Dock, ensures a complete, hi-fidelity history of network activity is immediately available for security investigations. Packets are timestamped to nanosecond level accuracy, ensuring accurate event reconstruction even for ultra-short-lived events.

Streamlining Security Investigations

The Network History recorded by EndaceProbes can be integrated with Cisco Firepower NGIPS and NGIPSV using the Pivot-To-Vision™ function of the EndaceProbe's powerful API.

Pivot-To-Vision lets security analysts pivot directly from alerts in the Firepower Management Console dashboard to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History. Using the IP address and time range of the trigger, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data. EndaceVision lets analysts dissect and review terabytes of network history down to microsecond level with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

PRODUCTS

- Cisco Firepower Management Console
- Cisco Firepower NGIPS and NGIPSV
- EndaceProbe Network Recorders
- Endace Fusion Connector for Cisco Firepower

BENEFITS

- Accurate, granular and complete network history provides definitive evidence for security analysts
- Streamlined investigation workflow improves SecOps efficiency and ensures faster investigations
- More effective detection tuning reduces false-positives
- Network packets provide a definitive evidentiary trail

FURTHER INFORMATION

<https://www.endace.com/cisco-firepower.html>

Being able to get directly to the related packets lets security analysts quickly and conclusively establish the root cause of issues and respond appropriately, dramatically reducing the time to investigate and resolve critical incidents.

Access to a 100% accurate record of network history, and a streamlined investigation workflow, enables SecOps analysts to quickly identify, prioritize and respond to real threats and flag false positives for detection tuning.

Increasing Detection Visibility with Application Dock

Cisco Firepower NGIPSV can be hosted in the EndaceProbe's Application Dock built-in hosting environment. Every packet captured and recorded by the EndaceProbe can also be streamed to hosted Firepower NGIPSV instances in real-time.

Security Operations teams can dynamically deploy Firepower NGIPSV anywhere on the network that they have EndaceProbe Network Recorders deployed, allowing them to increase their detection footprint without truck rolls or lengthy hardware deployments.

EndaceProbes are designed to ensure system resources used for capture and recording are separated from the resources used by hosted applications. This means capture performance is never impacted by hosted applications and vice-versa, guaranteeing 100% accurate recording even when the hosted Firepower NGIPSV instance is processing heavy traffic loads.

Conclusion

Recorded network history provides the high-fidelity packet-level detail necessary for the conclusive investigation of security incidents. The combination of EndaceProbe Network Recorders and Cisco Firepower NGIPS delivers a powerful, end-to-end detection, alerting and

investigation solution. It gives SecOps teams industry-leading security monitoring and alerting, with access to the detailed data they need for fast, conclusive threat investigation and response.

How it works

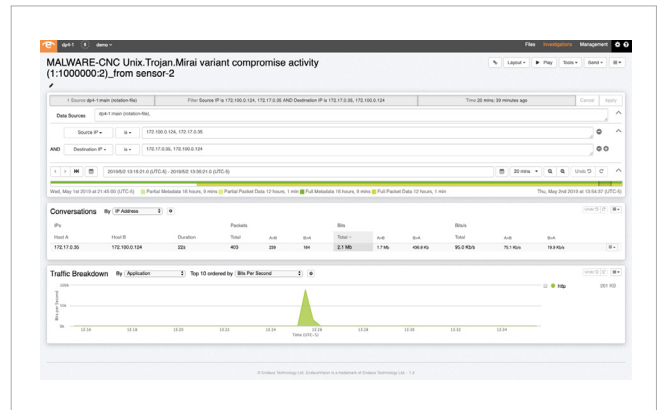
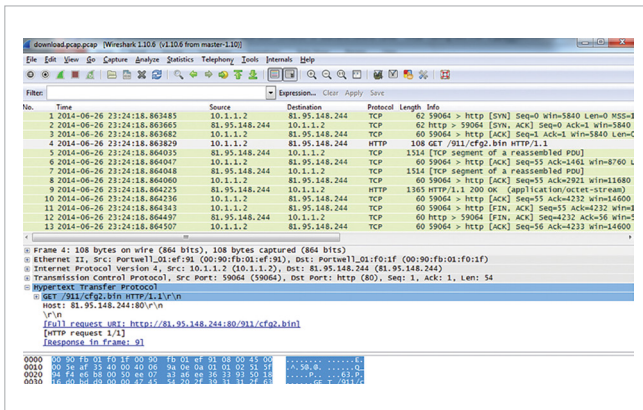
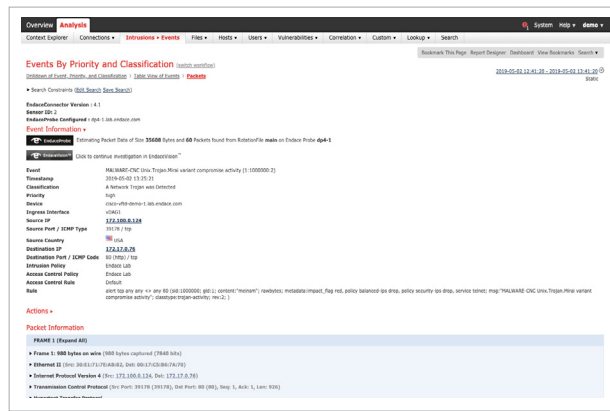
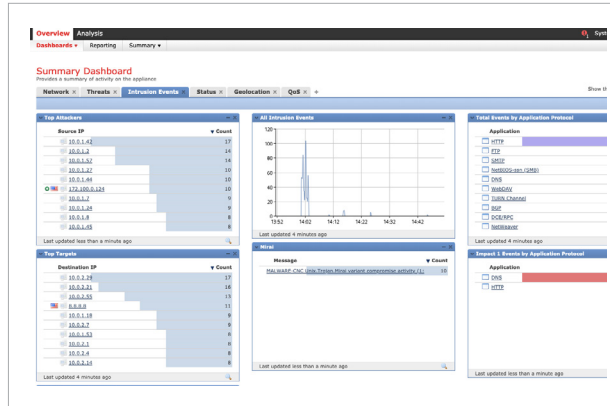


Figure 1 - Streamlined workflow from an alert in the Cisco Firepower console, to the alert detail, to related packets or network visualizations.

Endace™, the Endace logo, DAG™ and Provenance™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

For more information on the Endace portfolio of products, visit:
endace.com/products

For further information, email: info@endace.com