Distributing and Stacking EndaceProbes with EndaceFabric

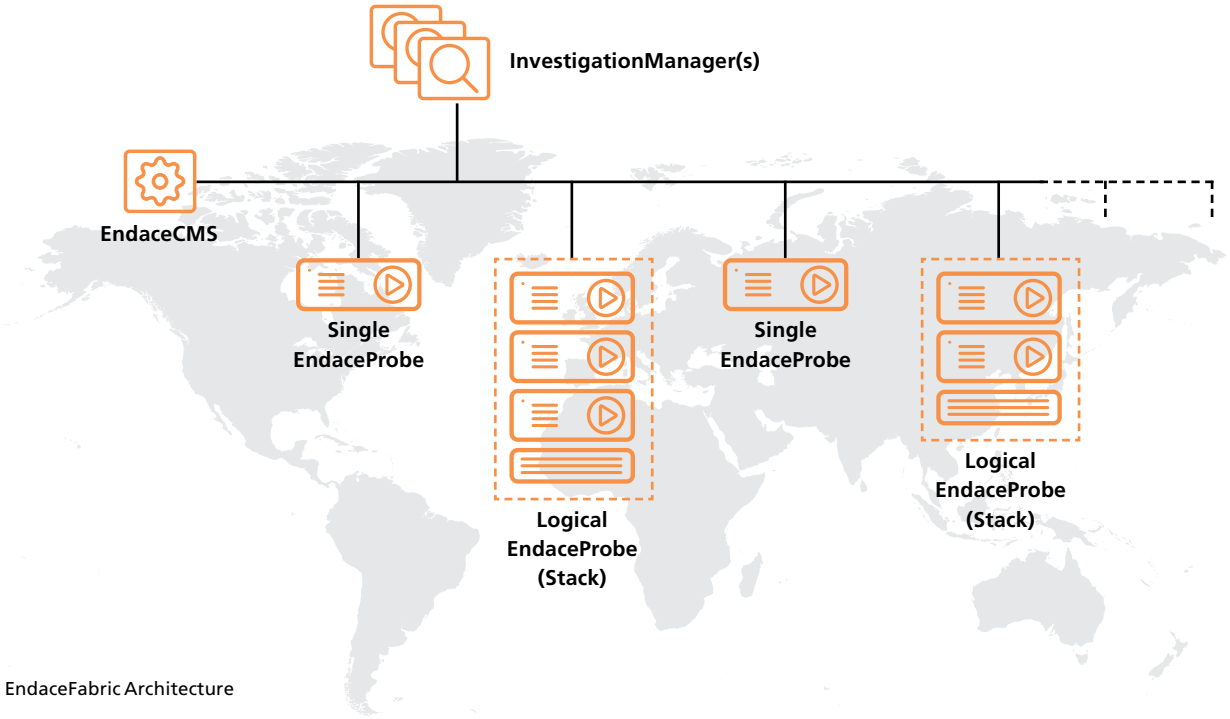

Diagram 1. EndaceFabric Architecture

Enabling rapid, centralized investigations across a fabric of globally distributed EndaceProbes and leveraging the scalable architecture of EndaceFabric to create logical EndaceProbes with massive throughput and capacity

The challenge for SecOps teams

Fast and effective response to security and network performance issues means being able to see what's happening on the network, and quickly identifying the root cause of issues when they are detected. With surety.

To become truly agile and responsive, global organisations proactively capture and record network traffic so they can identify and respond to issues quickly and efficiently. Bandwidth explosion, global footprints and the need to record up to a month of network history have driven Endace to develop the EndaceFabric™ architecture and EndaceProbe™ stacking with lightning-fast, global search.

How stacking can address this challenge

Over the last decade, Endace's EndaceProbe™ Analytics Platforms have earned a reputation for high-performance and reliability. They are available in a range of models to suit deployments from the edge to the core of the network, with the new, petabyte-capable 9200 Series setting new industry benchmarks for throughput, capacity and affordability.

Combining lossless, high-speed packet capture with the ability to host a wide range of network security and performance analytics solutions, EndaceProbes give customers the freedom to deploy their choice of best-of-breed network security and performance analytics solutions on a common hardware platform.

To enable SecOps and NetOps teams to rapidly remediate security events, performance issues or network problems, a network recording solution must be able to:

- monitor any network link, of any speed
- monitor various points throughout a network - which may be global in scale
- enable visibility into encrypted traffic
- provide the ability to quickly and easily search for packets of interest anywhere across the network.

The EndaceFabric architecture makes this all possible. EndaceProbes can be deployed at various points throughout a network to provide a network-wide fabric that delivers centralized visibility. The architecture also enables groups consisting of multiple EndaceProbes to be "stacked" to create logical EndaceProbes capable of massive throughput and capacity. Stacking also increases the hosting capacity available for deploying third-party network security and performance analytics solutions.

This document gives an overview of the EndaceFabric architecture and two of its key components, EndaceCMS™ and InvestigationManager™, and shows how this architecture can scale to enable sustained recording at 100Gbps and beyond, with capacity to store weeks or months of network history.

END_sb_distributing_and_stacking_endaceprobes_with_endacefabric_1.0_0119

Introducing EndaceFabric

To ensure end-to-end visibility across the network, EndaceProbes are typically deployed in various locations, often at points of interconnect with the public internet, subnetworks, branch offices and private data centers.

Endace created the EndaceFabric™ architecture (see Diagram 1) to solve the challenge of managing large numbers of distributed EndaceProbes and performing investigations that span multiple physical EndaceProbes at the same time. An EndaceFabric consists of multiple physical and/or virtual EndaceProbes, managed by EndaceCMS, with network-wide investigation, search and data-mining provided by instances of InvestigationManager.

EndaceCMS is designed for Operations and/or IT staff. It enables central management of a fabric of physical and virtual EndaceProbes and InvestigationManager instances. EndaceCMS allows administration functions - such as user administration, remote software upgrades and remote configuration - to be performed on multiple appliances simultaneously. An instance of EndaceCMS can be used to manage a fabric of appliances and may be deployed as either a physical or virtual appliance.

InvestigationManager is designed to be used by analysts performing investigations and offers network-wide search and visualization from a single pane of glass.

At the heart of InvestigationManager is EndaceVision™, a built-in, browser-based investigation tool that allows analysts to select data sources from multiple EndaceProbes and analyze recorded traffic from all these sources simultaneously. EndaceVision provides a variety of data visualization tools, including traffic breakdowns, top talkers, flows and conversations. Users can drill-down by time, user, server, protocol, application, or a variety of other attributes.

Once they have identified the 'packets of interest' relevant to a particular investigation analysts can view these packets directly in a Wireshark UI – removing the need to download large packet capture files across the network to a local host for analysis.

Multiple instances of InvestigationManager can be deployed as required – increasing the number of investigations that can be conducted simultaneously by different users. InvestigationManager instances are deployed as virtual appliances and have a no-cost license.

Distributed Processing for Amazingly Fast Search

Due to the distributed, parallel nature of the EndaceFabric architecture, searches can be conducted on a hundred EndaceProbes simultaneously in much the same time as it takes to perform a search on a single EndaceProbe. InvestigationManager queries each EndaceProbe involved in the search and consolidates the results, distributing the workload.

A single needle-in-a-haystack search for specific packets-of-interest across a hundred EndaceProbes and a hundred petabytes of recorded packet data can take less than a minute, with interim responses from individual EndaceProbes being displayed in InvestigationManager as they complete. See Diagram 2.

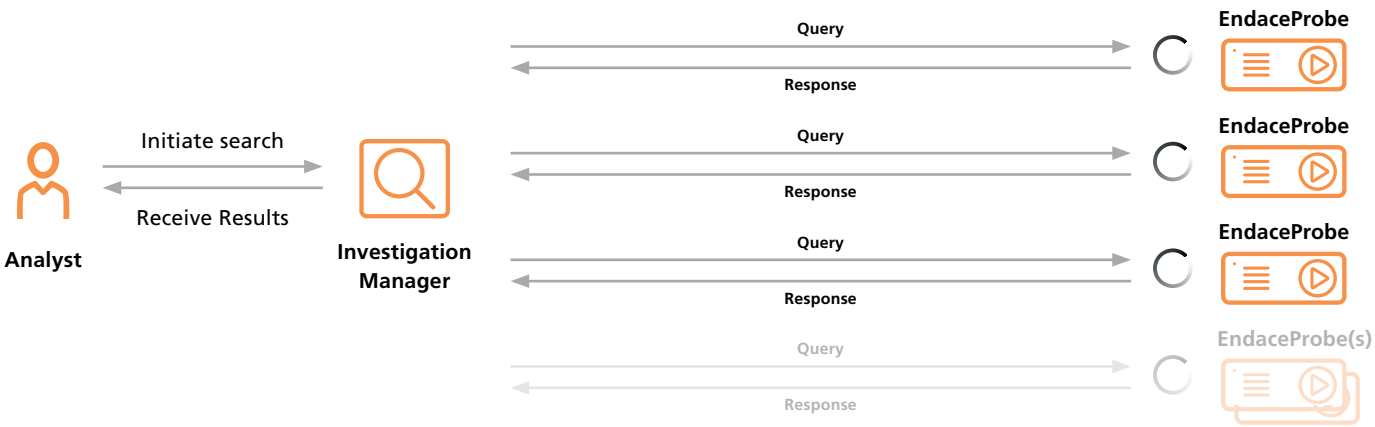

Diagram 2. EndaceFabric's Horizontally Scalable Architecture Enables Amazingly Fast Search

How "Stacks" Work

A Network Packet Broker supporting the required line rate (e.g. 100GbE) is used to load balance traffic from a TAP or SPAN port across each EndaceProbe in a stack. The Network Packet Broker may also be used to decrypt encrypted traffic before forwarding to the EndaceProbes for recording.

Searches and investigations are performed using InvestigationManager, selecting each EndaceProbe in the stack as a data source. In effect, InvestigationManager presents a stack, or even an entire fabric of EndaceProbes, as a single logical EndaceProbe. For analysts, the UI and workflow are practically identical to performing an investigation on a single EndaceProbe.

For ultra-high availability and hitless software upgrades, stacks may be deployed with N+1 redundancy so there is sufficient throughput and capacity even in the unlikely event that a hardware failure takes one of the EndaceProbes offline.

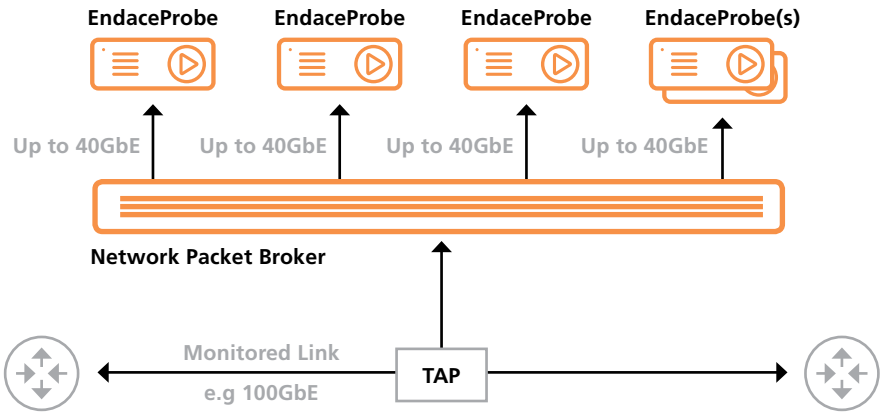

Diagram 3. Stacking EndaceProbes

Conclusion

The EndaceFabric architecture enables almost unlimited recording speed and capacity, scalable hosting and high-availability. EndaceProbes can be grouped or stacked to support sustained recording speeds of 100Gbps and beyond, and to provide storage capacity sufficient for months of full packet data.

As needs change, an EndaceFabric can be easily extended by incrementally adding more EndaceProbes to the stack to accommodate higher speed recording, increase hosting capacity, or provide deeper storage to enable network history to be retained for longer.

The following documents can be downloaded from the Endace Support Portal (https://support.endace.com) or obtained from your Endace sales representative. They provide further detail on how to deploy a fabric of EndaceProbes and EndaceProbe stacks, including architectural considerations, sizing parameters and hardware and software requirements.

- Technical brief: EndaceFabric Design Guidelines
- Technical brief: Design Guidelines for Stacking EndaceProbes

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

For further information, email: info@endace.com