Use Cases

- **Decrease time and increase accuracy for forensics analysis:** Emulex platforms use the Cisco® Identity Services Engine (ISE) user, device type, and access level information to provide user and device context that expedites the forensic analysis of packet capture data and reduces the mean time to respond to a security or network performance issue.
- **Facilitate network response:** Take action on the results of the forensics investigation by performing network quarantine or disconnect actions from within the Cisco ISE management console for fast, closed-loop management of the event.

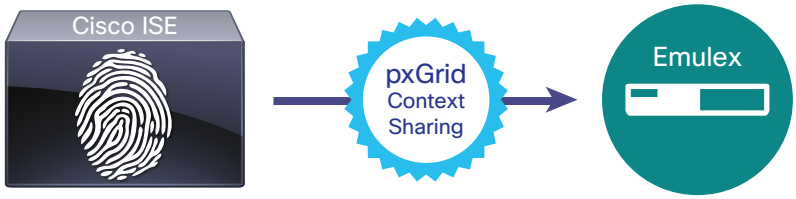
Cisco Identity Services Engine and Emulex Integration

Identity- and Device-Aware Packet Capture and Forensics

Network environments have become increasingly complex. The proliferation of more network-enabled devices, among other things, has led to increased management issues when supporting enterprise security, endpoint analysis, and regulatory compliance. Network activity in the past could be sufficiently analyzed with broad identifiers, such as IP addresses. However, today's increased network activity, all those devices, the broad adoption of software as a service (SaaS) and the use of virtualization have led to new requirements for deeper network security visibility and analysis.

The Cisco® Identity Services Engine (ISE) integrates with Emulex EndaceProbe Intelligent Network Recorder (INR) to deliver in-depth network forensics supplemented with relevant identity and device context. This integration provides network and security analysts with the context they need to quickly assess the significance of forensics analysis by correlating identity context with forensics. Cisco ISE provides the Emulex EndaceVision Network Visibility console with the contextual information about an event, such as user identity and the device type used. This helps network and security analysts quickly assess the significance of forensics analysis.

Context Information from Cisco ISE Promotes Identity - and Device-Aware Forensics in Emulex



The addition of Cisco ISE user and device context to the Emulex EndaceProbe INR packet capture platform also enables a new suite of network monitoring capabilities such as mobility-aware forensics. Dynamic network control capabilities within the Cisco ISE console allow Emulex Endace users to respond to a forensics investigation by taking action against users and devices within the Cisco network infrastructure.

Solution Highlights and Components

This solution is composed of Cisco ISE running the Cisco Platform Exchange Grid (pxGrid) context exchange capabilities and the Emulex EndaceProbe INR. Cisco pxGrid is a unified framework that enables multivendor, cross-platform network system collaboration among IT infrastructure such as security monitoring and detection systems, network policy platforms, identity and access management platforms, and almost any other IT operations platform.

The integration enabled by Cisco pxGrid technology in Cisco ISE allows Emulex to supplement its packet capture and forensics visibility with information from Cisco ISE about user identity and endpoint device identification. This reduces the need for manual processes, provides a complete view of packet capture, and enables IT to take mitigation actions on users or devices – all from the Emulex Endace management console.

Some of the Cisco ISE attributes used by Emulex Endace include the following:

- User name, IP address, authentication status, and location
- Authorization group, guest, and quarantine status
- Device manufacturer, model, OS, OS version, MAC address, IP address, network connection method (wired or wireless), and location
- Posture compliance status, antivirus installed, antivirus version, OS patch level, and mobile device posture compliance status (through MDM ecosystem partners)

Supported Products

- Cisco ISE 1.3 or later
- EndaceProbe INR OSm 5.2.2

Integration Details

Cisco ISE integration with Emulex is accomplished through the following:

- Cisco ISE provides user identity and device information to Emulex EndaceProbe INR through Cisco pxGrid.
- This contextual data is used to provide a complete view of packet capture and identity and device data for use in forensics analysis within the Emulex Endace management console. Analysts can then correlate this contextual data with packet capture data in one interface to enhance their forensics analysis of the packet capture data.
- If the results of the forensics investigation justify taking an action on the offending user or device, network quarantine or disconnect actions may be taken from within the Cisco ISE management console. This provides closed-loop management of the event.

Next Steps

For additional integration information, visit the Cisco Marketplace Solutions Catalog at http://marketplace.cisco.com/catalog and search for “Emulex.”

C45-732921-00 10/14