At-a-Glance

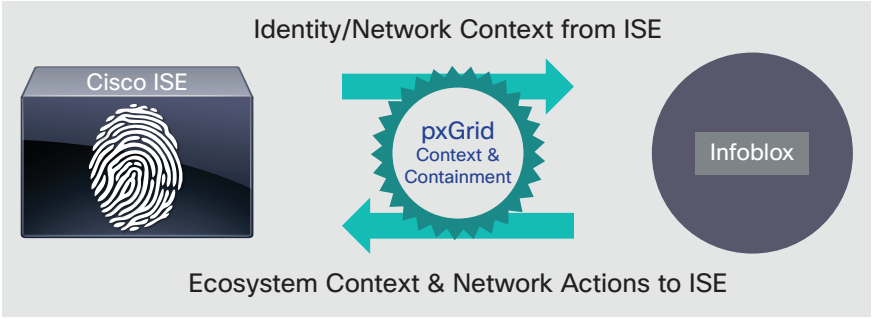
Cisco Identity Services Engine and Infoblox Integration

Gain Early Insight into Botnet Threats and Contain Them

If you can't see what's happening on your network, how can you protect it? Cisco® Identity Services Engine (ISE) provides a wealth of user identity, endpoint device, and network context information used by many IT management and security platforms. To bring greater insight to risky network user activities and take mitigation actions on those events, Cisco ISE uses Cisco Platform Exchange Grid (pxGrid) technology to share this contextual data with Infoblox, a Cisco partner with premier solutions for DNS, DHCP and IP address management (DDI) and DNS-based botnet detection.

For Infoblox DDI deployments, integration with ISE simplifies and expedites association of an IP address – in real time or in the past – with a specific user. This simplifies the often time-consuming task of answering legal or human resources questions regarding which user held a specific IP address at a specific point in time. ISE user identity information is also integrated in Infoblox Network Insight monitoring and reporting to give IPAM administrators easy real-time and historical access to user-to-IP associations for standard network planning and reporting.

Cisco ISE + Infoblox: Identity & Network Aware IPAM and Botnet Detection



For the Infoblox DNS Firewall platform, integration with ISE also associates user identity and network-privilege level with IP addresses to aid in early detection and response to botnet activity. The Infoblox DNS Firewall analyzes domain name resolution behavior to identify botnet command-and-control servers. Once they're identified, the DNS Firewall also identifies what internal endpoints are currently accessing or have accessed these command-and-control servers and which ones have potentially been infected by the botnet. If an infection has occurred, the user identity and network-privilege level from Cisco ISE are used by Infoblox to help determine which clients are the highest priority for potential malware remediation.

Benefits

- Detect first point of contact with Botnets with Infoblox DNS Firewall, thereby increasing the effectiveness of threat defense deployments
- Decrease time-to-event classification with Infoblox IP address management (IPAM) and DNS Firewall platforms that use Cisco Identity Services Engine (ISE) user, device type, and access-level data to answer common questions needed expedite the classification of and response to a security event
- Simplify and expedite security event response with Infoblox through support of Cisco Rapid Threat Containment, using the Cisco pxGrid Adaptive Network Control capabilities of Cisco ISE to take actions on high-severity security events in the Cisco network, such as quarantining a user or routing the traffic for deeper investigation

If the threat is urgent, the DNS Firewall administrator may use the pxGrid Adaptive Network Control feature of ISE to provide Rapid Threat Containment actions directly from the Infoblox management console.

How Cisco ISE and Infoblox Integration Works

With the ISE integration with Infoblox:

- Cisco ISE provides its user identity and network privilege information to Infoblox DDI and DNS Firewall via pxGrid.
- ISE contextual data is also appended to associated events in Infoblox to provide the additional context of the user and network-access level, so analysts can better understand the significance of a security or IPAM event.
- Infoblox DNS Firewall uses ISE as a conduit for taking Rapid Threat Containment actions within the Cisco network infrastructure. Infoblox can instruct ISE to undertake quarantine, investigation, or access-block actions on users and devices based on pxGrid Adaptive Network Control policies that have been defined in ISE.
- All of these functions can be logged and reported on within the Infoblox Network Insight console, providing unified user security threat and IP address leasehold reporting.

Some of the key ISE attributes available for use by Infoblox for user- and network-related context are:

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

This suite of user- and network-aware capabilities from the Cisco ISE and Infoblox integration streamline the process of threat detection and simplify the implementation of responses by IT. You are empowered to greatly reduce the time to remediation of network security threats and swiftly respond to inappropriate network use.

Next Steps

To learn more about the Cisco ISE, visit www.cisco.com/go/ISE

To learn more about Cisco pxGrid, visit http://www.cisco.com/go/ise

For additional information regarding ISE and other ecosystem partner integrations, visit http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html

C45-736068-00 10/15