SOLUTION NOTE

DDI Integration for Cisco ISE and pxGrid Platform

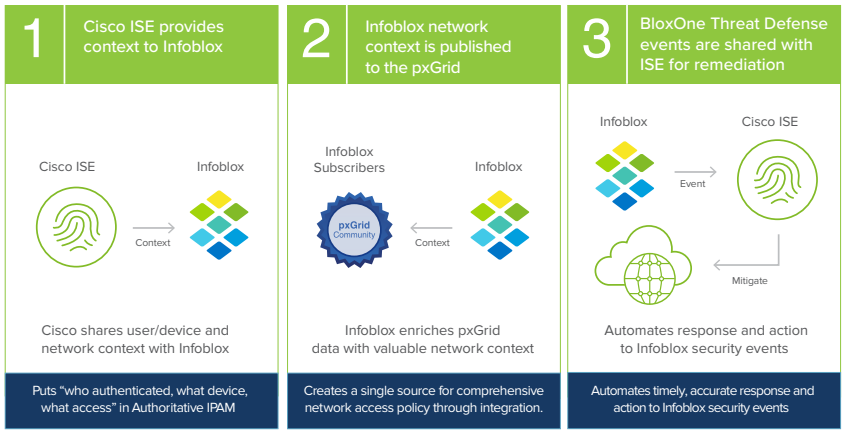
The integrated Infoblox/Cisco Identity Services Engine (ISE) solution uses the Cisco Partner Exchange Grid (pxGrid) to share information between Cisco ISE, Infoblox and other pxGrid participants. Together, they enable users to create a unified, automated solution that enhances security-response accuracy and timeliness; expands network, user and device visibility; and improves overall network operations. The solution enriches the overall pxGrid data, providing key benefits that point products alone cannot deliver. The publish/subscribe architecture enables configurable, scalable solutions; the shared data enables network and security teams to access each other's information. Infoblox's participation in the pxGrid community makes Infoblox data indispensable for Cisco ISE customers.

cisco Preferred Solution Partner

The Challenge

In today's dynamic IT environments, multiple teams must collaborate regularly to ensure consistent IT service delivery from core network services to critical enterprise applications. In addition to maintaining a high standard of service delivery, those teams are constantly challenged to ensure the security of their environments. To completely secure an enterprise, businesses deploy a wide range of tools from various vendors. Tools such as identity and access management (IAM), security information and event management (SIEM), threat defense, policy platforms and others are necessary to protect the enterprise, but they don't share information—creating a significant operational challenge with multiple silos of information.

The job of correlating data from various tools adds to the complexity, ultimately requiring considerable manual effort. This inefficiency not only drives up costs but also heightens the risk involved, with longer response times to security events. The longer it takes to execute the appropriate security actions, the deeper an advanced attack can dig into an enterprise's environment, in some cases exfiltrating sensitive business intelligence.



Why Infoblox: A Leader in Core Network Services

- The only DDI vendor to publish network data into the Cisco pxGrid ecosystem
- The only solution to combine DNS security event data with pxGrid ecosystem vendors, providing a means to automate security responses
- The only DDI solution to subscribe to the Cisco pxGrid— enriching IPAM data with user, device and TrustSec tag data shared by ISE

The Solution

Infoblox Publishes Valuable Network Data

The publish/subscribe architecture of the pxGrid enables Infoblox to share rich IP address, DNS, DHCP and network data with the pxGrid community, enhancing the data sets of pxGrid participants.

With DHCP lease data, such as time of issue and length of lease, network access control administrators can fine tune policies and optimize event response processes.

The pxGrid provides a common transport language between IT systems, a much better way to share information than conventional APIs for several reasons. Cisco pxGrid:

- Supports many-to-many communication among platforms, making it scalable beyond architectures based on polling
- Enables detailed customization, allowing each connected system to pull the specific information it needs from other systems and share only the specific information relevant to the other pxGrid participants
- Supplies the necessary security and control, preserving the integrity of each system's data through tightly controlled access, authentication and authorization for each member of the pxGrid ecosystem.

Infoblox Subscribes to ISE User and Device Data

By subscribing to pxGrid data, Infoblox IPAM data is enhanced with device and identity data captured by Cisco ISE. The enriched IPAM data gives network administrators greater insight across wireless and wired networks, resulting in better decision-making. Having user and device data along with network, IP and MAC address data enables network teams to quickly connect the dots in identifying infected devices and the users associated with those devices.

ISE Data Subscribed to by Infoblox	Infoblox Data Subscribed to by ISE	BloxOne® Threat Defense Event Data Reported to ISE
User, domain, SSID or VLAN, device type, session state, security group, OS, TrustSec	IP address, Infoblox Grid member, MAC/DUID, DHCP fingerprint, host name, DHCP lease start/end, NetBIOS, client ID	IP address, MAC/DUID, host name, severity, policy state

Infoblox Deepens Visibility and Control

NIOS DDI integrates with Cisco ISE to provide contextual data visibility and automatic threat detection alerts for faster threat response, prioritization and increased ROI on ISE investments. NIOS maintains ongoing software concurrency with ISE for deeper visibility, control and identity management across network applications, routers, switches and other devices.

Cisco TrustSec Visibility Integrated with Infoblox DDI

In Cisco environments that use TrustSec tagging, those tags are also correlated with user and device data. With access to TrustSec tags, network teams can quickly troubleshoot a user's connectivity issues that are related to security tags.

Infoblox Issues Security-Event Data

BloxOne Threat Defense identifies infected devices in real time. When a device queries DNS to reach a malware site identified in one of the response policy zones, the query is blocked, and the device is labeled as infected.

By blocking the query, BloxOne Threat Defense prevents the infected device from "calling home" and can report the event. However, those actions alone still leave the infected device on the network. At best, direct port control can quickly isolate a wired device by setting the port admin status to "down," but that does not work with wireless devices. By pushing BloxOne Threat Defense indicator of compromise (IoC) information from Infoblox into ISE, a rapid, focused response can be automated, maximizing security incident-response performance and efficiency.

The combination of BloxOne Threat Defense and Cisco ISE is a perfect example of crafting a solution across pxGrid participants. In this case, when BloxOne Threat Defense detects a bad query or identifies a DNS tunneling event, Infoblox can immediately notify ISE. Depending on the event severity and the policies deployed, ISE can quarantine the device. The solution can be expanded with the addition of other pxGrid participants. With Rapid7, for instance, ISE could request Rapid7 to immediately scan the device and mitigate the threat—all automatically, with visibility for both the network team and the security response team.

Solution Components

Solution products	Infoblox DDI, Network Insight, BloxOne Threat Defense
Delivery options	Physical or virtual appliances
Feeds and services, etc	Real-time threat feed for BloxOne Threat Defense

Summary

The problem of siloed data in IT still plagues many organizations with unsatisfactory ways to share data, troubleshoot issues and respond to security events. The broadening landscape of necessary tools makes the traditional API integration approach a less-than-ideal solution with little upside. Cisco pxGrid provides the means to have a many-to-many communication platform with a common data transport language.

Infoblox integration with pxGrid enables Infoblox and Cisco ISE to exchange valuable networking, user, device and security-event information, enriching both Infoblox DDI and ISE data. The pxGrid's publish/subscribe architecture enables users to combine pxGrid ecosystem products into a unified solution that enhances security-response accuracy and timeliness; expands the visibility of networks, users and devices; and improves overall IT operations by sharing information between network and security teams. Infoblox participation in the pxGrid community makes Infoblox data indispensable for Cisco ISE customers.

Next Steps

Cisco ISE users can download virtual evaluations of the Infoblox DDI solution, Network Insight and BloxOne Threat Defense from the Infoblox Download Center.

For more information or to get answers on how visibility and shared data can improve your network operations and security posture, connect with your Infoblox account team, see our core network integrations or contact us at Infoblox.com.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com