PALO ALTO NETWORKS AND INFOBLOX

Increased Visibility and Information Sharing Improves Security Posture and Maximizes ROI

Key Benefits

Infoblox sends information on new and compromised devices to Palo Alto Networks next-generation firewalls for enforcement on the fly. The joint solutions enables organizations to:

- Gain visibility into new and compromised devices.
- Implement dynamic policies (access lists) on Palo Alto Networks next-generation firewalls with automated policy management instead of a standard, static configuration approach.
- Improve security posture while maximizing return on investment for both products.

The Challenge

Today's enterprise network consists of many network and security devices that each generate their own incidents but don't always share information. This lack of interoperability and inability to share event data results in network and security teams working in silos with no context. According to the 2017 ESG research report, "Security Operations Challenges, Priorities and Strategies,"[1] keeping up with the volume of security alerts and lack of integration between security tools are the biggest challenges for security operations. The same report also says the top security operations priority should be to invest in technologies that can automate security operations and threat detection by integrating multiple tools. Organizations are investing heavily in automation and orchestration of incident response to improve collaboration between cybersecurity and IT operations teams, keep up with the volume of security alerts, prioritize alerts, and shorten incident response times.

To help enterprises improve their security operations and reduce time to containment, Infoblox, the market leader in Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and IP address management (IPAM)—collectively known as DDI—has integrated with Palo Alto Networks next-generation firewalls. The integration allows network and security administrators to automatically share information, such as which IP addresses join or disconnect from a network, as well as any compromised IP addresses that trigger security events on DNS.

Infoblox Ecosystem Exchange

Infoblox Ecosystem Exchange is a highly interconnected set of ecosystem integrations that extend security, increase agility, and provide situational awareness for more efficient operations, both on-premises and in the cloud. Infoblox Ecosystem Exchange provides visibility across the entire network, including virtualized or cloud deployments; removes silos between network and security teams; improves agility; automates IT workflows; enables faster remediation to threat and network changes; and provides better return on investment for existing IT and security investments.

Palo Alto Networks

The Palo Alto Networks Security Operating Platform prevents cyberattacks through intelligent automation. The platform combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyber breaches. Tight integration throughout the platform and with ecosystem partners delivers consistent security across clouds, networks, and mobile devices, natively providing the right capabilities at the right place across all stages of an attack lifecycle.

1. "2017: Security Operations Challenges, Priorities, and Strategies," ESG Research, March 2017, https://resources.siemplify.co/hubfs/PDF%20Downloads/ESG-Research-Insights-Report-Siemplify.pdf?t=1530479670970.

The platform was built from the ground up with breach prevention in mind. It incorporates important threat information shared across security functions system-wide and is architected to operate in modern networks with new technology initiatives like cloud and mobility. Platform customers benefit from better security than legacy or point security products provide, while enjoying lower total cost of ownership.

Palo Alto Networks and Infoblox

Infoblox manages addresses and address groups on Palo Alto Networks next-generation firewalls (NGFWs) with a list of devices that are currently connected and/or compromised. For example, devices may be associated with identified malicious DNS requests and/or DNS data exfiltration—allowing customers to specify dynamic security policies for every device. The integration with Palo Alto Networks provides a huge advantage over a more standard approach, which entails static security policies configured to grant access for whole networks, whether IP addresses are utilized or not.

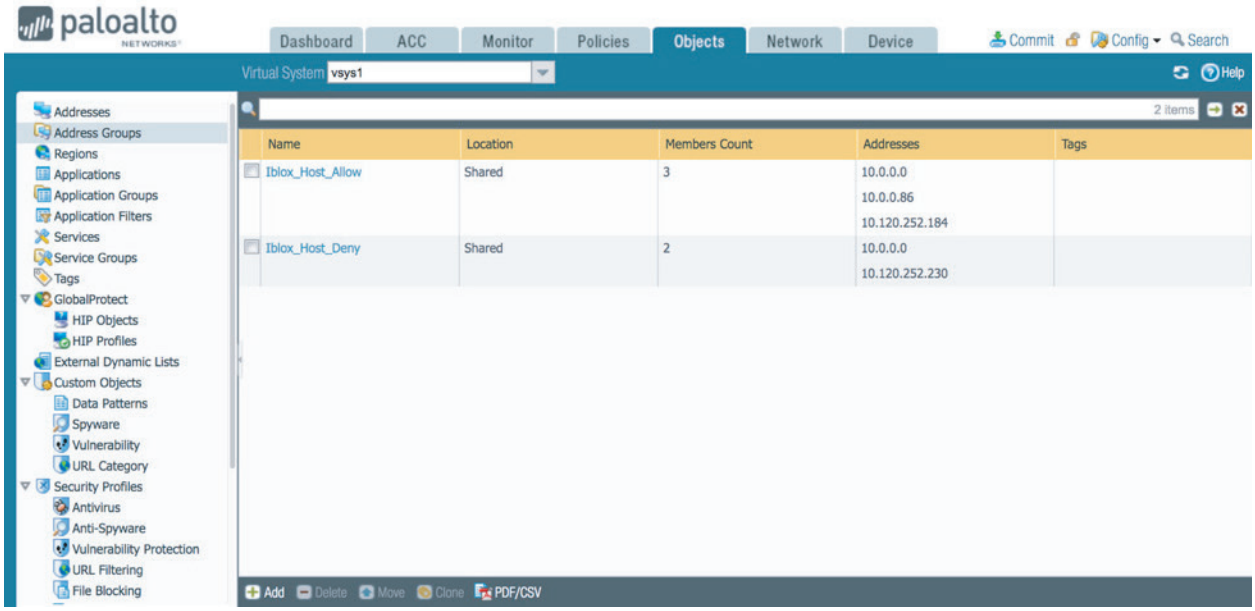

Figure 1: Infoblox updates address groups on Palo Alto Networks NGFWs

After Infoblox updates an address group on a Palo Alto Networks next-generation firewall (see Figure 1), the group can be used to implement and enforce specific policies on the firewall (see Figure 2).

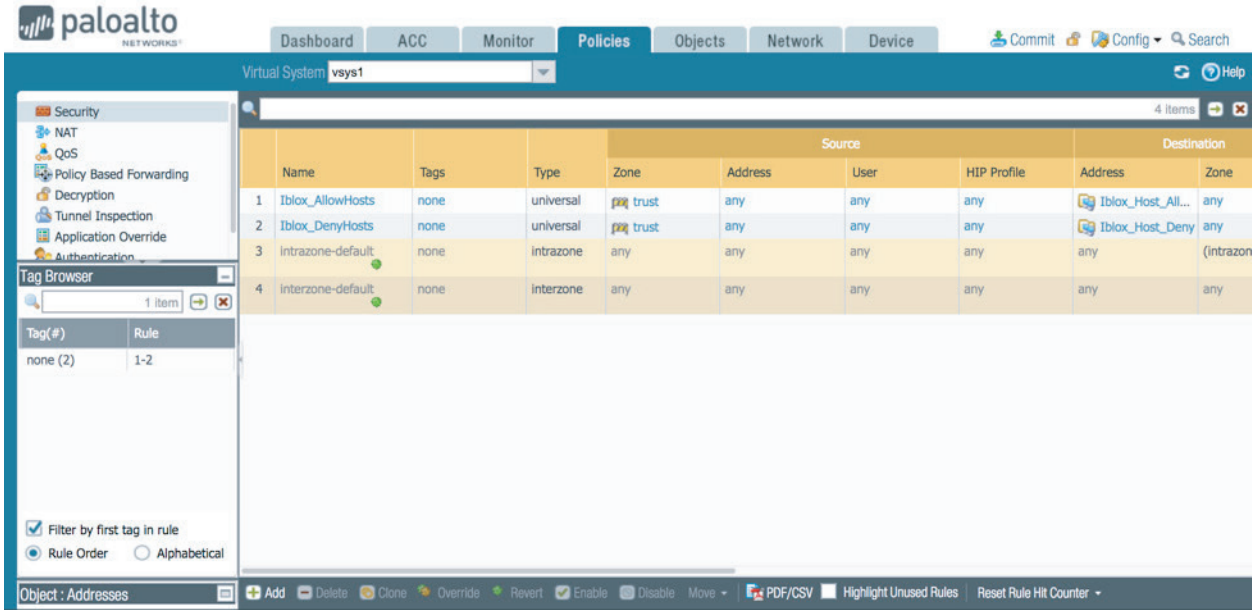

Figure 2: Address groups as a function of NGFW policy

Use Case: Automatic Address Groups Management Challenge

Challenge

An enterprise is having trouble gaining complete visibility into its entire network. It is also challenged to eliminate data silos, respond more quickly to security and network changes, and shorten incident response times.

Answer

Infoblox, using the Outbound Notifications framework, updates address groups on Palo Alto Networks next-generation firewalls with information about currently connected and/or compromised devices. Security policies on Palo Alto Networks next-generation firewalls can be configured to use dynamically updated address groups to provide or restrict access to specific resources as well as turn on monitoring of compromised devices.

Benefits for Organizations

- Manage address objects and automate remediation.
- Improve overall security by automatically adding address objects to dynamic security policy.
- Improve security posture while maximizing return on investment for both products.

Figure 3: Infoblox and Palo Alto Networks integration

About Infoblox

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500. Learn more at www.infoblox.com.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices. Find out more at www.paloaltonetworks.com.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com