SOLUTION BRIEF

Fortinet and Infoblox Security Solution

Broad, Integrated, and Automated Solution for Increased Visibility and Information Sharing and Enhanced Security Posture

Challenges

Today's enterprise network consists of many network and security devices that each generate their own incidents but don't always share the information with each other. This lack of interoperability and integration creates silos between network and security teams. In a 2017 ESG report, keeping up with an increasing volume of security alerts and a lack of integration between security tools are two of the biggest challenges that security operations teams face. In response, organizations are investing heavily in automation and orchestration of incident response to improve collaboration between IT and cybersecurity teams, keep up with an increasing volume of security alerts, prioritize alerts, and shorten incident response times.

Fortinet FortiGate NGFW and Infoblox Ecosystem Exchange Joint Solution

The Fortinet and Infoblox integrated solution enhances collaboration and breaks down silos by leveraging the Fortinet Security Fabric. Designed around a series of open application programming interfaces (APIs), open authentication technology, and standardized telemetry data, the Fortinet Security Fabric enables organizations to integrate existing security technologies via open interfaces and provide end-to-end security without compromise.

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 the Fortinet FortiGate Enterprise Firewall. This integration allows network and security administrators to automatically share information with Fortinet, such as DNS security events and details on which devices join or disconnect from a network.

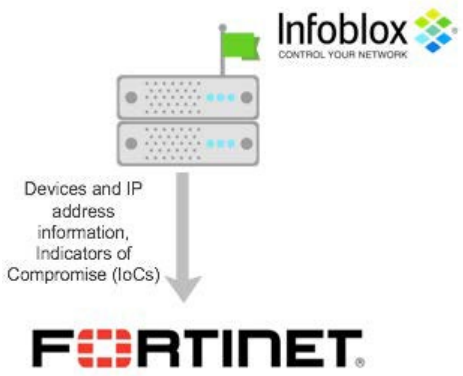

Figure 1: Infoblox and Fortinet NGFW configuration.

Joint Solution Components

- Fortinet FortiGate Next-Generation Firewall (NGFW)
- Infoblox Ecosystem Exchange

Joint Solution Benefits

Infoblox sends information on new devices and compromised hosts to Fortinet next-generation firewalls using Outbound Notifications. The joint solution enables organizations to:

- Improve overall security by automatically adding address objects to dynamic security policy
- Gain context for prioritization of threats
- Implement security policies dynamically on FortiGate to manage assets, ease compliance and automate remediation
- Enhance their security posture while maximizing return on investment

FORTINET FABRIC-READY

Infoblox manages addresses and address groups on the FortiGate Next-Generation Firewall (NGFW) with a list of devices connected or compromised—for example, devices associated with identified malicious DNS requests or DNS data exfiltration—allowing customers to block communications with specific resources.

The integration with Fortinet provides an advantage over the more standard approach of static security policies that are configured to grant access for whole networks, regardless of whether IP addresses and their ranges get used or not.

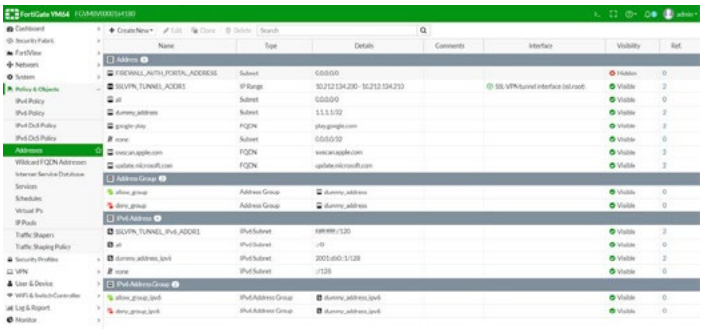

Figure 2: Infoblox updates addres groups on Fortinet NGFW.

After Infoblox updates an address group on a FortiGate NGFW, the group can be used to implement and enforce specific policies on the firewall.

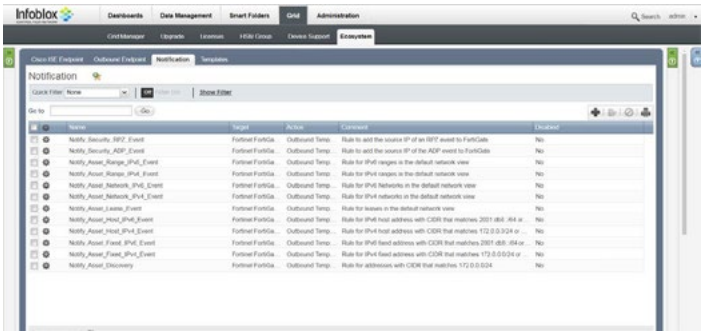

Figure 3: Address groups as a function of NGFW policy.

Use Case

Automatic Address Groups Management

An enterprise wants to gain complete visibility into its entire network. It would also like to eliminate data silos, respond quickly to security and network changes, and shorten incident response times.

Resolution With the Joint Solution

Infoblox, using the Outbound Notifications framework, updates address groups on the FortiGate NGFW with information about connected or compromised devices. Enterprises then configure security policies on the firewalls to provide or restrict access to specific resources and monitor compromised devices.

Key Components

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 virtual or cloud deployments; removes silos between network and security teams; improves agility; automates IT workflows; enables faster threat remediation and network changes; and provides a better ROI for existing IT and security investments.

FortiGate Next-Generation Firewall

The Fortinet Enterprise Firewall Solution offers universal platform support for all types of deployments, giving security professionals maximum latitude across the extended enterprise network. Security managers have the visibility and control they need to counter attackers with one network security operating system across the entire FortiGate family of appliances. And all the FortiGate appliances are interconnected with the Fortinet Security Fabric for automatic distribution of contextual security policy and threat intelligence throughout the enterprise. Using a single-pane-of-glass dashboard, security managers can consolidate their management views and implement security policies concisely. For more information, please visit www.fortinet.com/enterprisefirewall.

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 cloud and hybrid systems, 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.

October 25, 2021 2:26 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 6:sb-FA-fortinet-infoblox-102021:sb-FA-fortinet-infoblox-102021

438410-A-0-EN