

# infoblox.

SOLUTION NOTE

### FORTINET AND INFOBLOX SECURITY SOLUTION

Broad, integrated and automated solution for increased visibility, 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.<sup>1</sup> 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.

### THE FORTIGATE NGFW AND INFOBLOX ECOSYSTEM EXCHANGE JOINT SOLUTION

The Fortinet and Infoblox integrated solution enhances collaboration and breaks down siloes by leveraging the Fortinet Security Fabric. Designed around a series of open 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 Infoblox.

Figure 1: Infoblox and Fortinet

FERTIDET

NGFW Integration

#### 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



<sup>1</sup> ESG research report, "Security Operations Challenges, Priorities and Strategies," 2017.

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.

Infoblox manages addresses and address groups on FortiGate's 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.

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

Dushboard	+ Create New- 2 Edit 1 Core 18 Delete Search			Q							
<ul> <li>Security Fabric</li> <li>Fort/View</li> </ul>	Name	Type	Details	Comments	Interface	Visibility	Ref.				
Port/View     Network	C Address 💿										
System	FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0			O Hidden	0				
Policy & Objects IPv4 Policy IPv4 Policy IPv4 Policy IPv4 DoS Policy	SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 10.212.134.210		③ SSLVPN tunnel interface (ssl.root)	<ul> <li>Visible</li> </ul>	2				
	E al	Subnet	0.0.0.00			<ul> <li>Visible</li> </ul>	0				
	dummy_address	Subnet	1.1.1.1/32			<ul> <li>Visible</li> </ul>	2				
	🖀 google play	FQDN	play.google.com			O Visible	2				
IPv6 DoS Policy	Ø none	Subnet	0.0.0.0/32			<ul> <li>Visible</li> </ul>	0				
Addresses	🕸 🖬 swscan.apple.com	FQDN	swscan.apple.com			O Visible	2				
Wildcard FQON Addresses	update.microsoft.com	FQDN	update.microsoft.com			<ul> <li>Visible</li> </ul>	2				
Internet Service Database	C Address Group 🚱										
Services Schedules	🔌 allow_group	Address Group	dummy_address			<ul> <li>Visible</li> </ul>	0				
Virtual IPs	🛸 deny_group	Address Group	dummy_address			<ul> <li>Visible</li> </ul>	0				
IP Pools	E IPv6 Address G										
Traffic Shapers	SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Subnet	fem:mm:/120			<ul> <li>Visible</li> </ul>	2				
Traffic Shaping Policy	D all	IPv6 Subnet				<ul> <li>Visible</li> </ul>	0				
Security Profiles	5 🖸 dammy_address_ipv6	IPv6 Subret	2001:00:1/128			O Visible	2				
VPN	> Ø none	IPv6 Subnet	::/128			<ul> <li>Visible</li> </ul>	0				
User & Device	2 🖸 Pró Address Group 🚳										
WIFI& Switch Controller	3 🐴 allow, group, jpv6	IPv6 Address Group	dummy_address_igv6			O Visible	0				
t Log & Report Monitor	> 💁 deny_group_jpv6	IPv6 Address Group	C dummy address javó			O Visible	0				

Figure 2: Infoblox updates address groups on Fortinet NGFW

FortiGate VM64 FGV								o 🕗 🕫
B Dashboard	>	+ Create New- / Edit - Fill Clone - 1	B Delete Search		Q			
🔆 Security Fabric	>	Name	Type	Details	Comments	Interface	Visibility	Ref.
FortiView     Network	>	C Address ()						
System		FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.00			O Hidden	0
Policy & Objects IPv4 Policy		SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 10.212.134.210		③ SSLVPN tunnel interface (ssl.root)	<ul> <li>Visible</li> </ul>	2
		E al	Subnet	0.0.0.00			<ul> <li>Visible</li> </ul>	0
IPvó Policy		dummy_address	Subnet	1.1.1.1/32			<ul> <li>Visible</li> </ul>	2
IPv4 Du5 Policy		🖀 google-play	FQDN	play.google.com			O Visible	2
IPv6 DoS Policy		8 none	Subrret	0.0.0.0/32			<ul> <li>Visible</li> </ul>	0
Addresses	- 6	Swscar.apple.com	FQDN	swscan.apple.com			O Visible	2
Wildcard FQDN Addresses		aupdate.microsoft.com	FQDN	update.microsoft.com			<ul> <li>Visible</li> </ul>	2
Internet Service Database		E Address Group 😨						
Services Schedules		allow_group	Address Group	dummy_address			Visible	0
Virtual IPs		😼 deny_group	Address Group	dummy_address			<ul> <li>Visible</li> </ul>	0
IP Pools		E IPv6 Address G						
Traffic Shapers		SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Subnet	fdtf:ttt:/120			S Visible	2
Traffic Shaping Policy		E all	IPvó Subnet				O Visible	0
Security Profiles	>	🕼 dummy_address_ipv6	IPv6 Subnet	2001;(b0:1/128			<ul> <li>Visible</li> </ul>	2
VPN	>	Ø none	IPv6 Subnet	::/128			O Visible	0
User & Device	>	E IPv6 Address Group 🕤						
WIFI-& Switch Controller	>	🗟 allow, group, ipvő	IPv6 Address Group	dummy_address_igv6			<ul> <li>Visible</li> </ul>	0
d Log & Report	>	a deny_group_ipv6	IPv6 Address Group	dummy_address_ipv6			O Visible	0
Monitor	>							

Figure 3: Address groups as a function of NGFW policy

#### **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: <a href="https://www.fortinet.com/enterprisefirewall">www.fortinet.com/enterprisefirewall</a>.

## infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier. Corporate Headquarters 2390 Mission College Blvd, Ste. 501 Santa Clara, CA 95054

+1.408.986.4000 www.infoblox.com

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).

Version: 20231030v