

JOINT SOLUTION BRIEF

Fortinet and Infoblox Security Solution

Broad, integrated and automated solution for increased visibility, information sharing and enhanced security posture

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

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

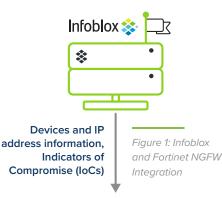


creates silos between network and security teams. In a 2017 ESG report, keeping up with an increasing volume of security alerts and a lack of integration between security tools are two of the biggest challenges that security operations teams face.¹ In response, organizations are investing heavily in 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





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.

Dishboard	> + Create New+ ≠ Lot 1a Close	B Delete Search		Q							
W Security Fabric	> Name	Troe	Details	Comments	Interface	Vicibility	Ref.				
 Fort/New 	Address O										
Network	FREEWAL AUTH POSTAL ADDRESS	Subort	00000			O Hidden	0				
O System	SSIVEN TUNNEL ADDRS	IP Range	10,212,134,200 10,212,134,210		(0.55). VFN turned interface (ut/root)	Visble	2				
Pulicy & Objects					(0.5% www.sanetintermact(0.700)						
IPv4 Policy	■ 4	Subnet	0.0.0.0			 Visible 	0				
IPv6 Policy	dumms_address	Subnet	1111/22			 Visible 	2				
IN4 Do5 Policy	google play	FOON	play.google.com			 Visible 	2				
IPv6 Do5 Policy	B none	Subret	0.0.0.92			 Visible 	0				
	Strategy and the second sec	FOON	swscan.apple.com			 Visible 	2				
Wildcard EQON Addresses	augdate.microsoft.com	FOON	update microsoft.com			 Visible 	2				
Internet Service Database	Address Conce 🕑										
Services	💈 allow, group	Address Group	dummy_address			 Visible 	0				
Schedulen Versal IPs	😼 dery_group	Address Group	dummy_address			 Visible 	0				
IP Pools	E INSAMES O										
Traffic Shapers	SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Subnet	fottmt:/120			 Visible 	2				
Traffic Shaping Policy	8 -	IPv6 Subnet	J0			 Visble 	0				
Security Profiles	5 D dummy_address_jpv6	IPv6 Subnet	2001.650:1/128			 Visible 	2				
D WN	> B none	IPv6 Subnet	1/128			Visible	0				
User & Device	D Pvi Address Group (3)										
♥ WFL& Switch Controller	* Salay gang javi	IPv6 Address Group	B durnery address lovo			 Visible 	0				
at Log & Report	dery,group,javá	Puó Addres Group	D dummy, address, jowd			• Visible	0				
C Monitor											

Figure 2: Infoblox updates address groups on Fortinet NGFW

B Dashboard	>	+ Create New + 2 Edit 5 Gine	Delete Search		Q					
& Security Fabric	>	Name	Type	Details	Comment	loterface				
FortiView	>	Address O								
Network System	2	FIREWALL, AUTH, PORTAL, ADDRESS	Subnet	0.0.0.00						
Policy & Objects IPv4 Policy		SSUPN_TUNNEL_ADDR1	IP Range	10.212.134.200 10.212.134.210		③ SSL VPN tunnel interface (ssl.root)				
		E 31	Subnet	0.0.0.0						
IPv6 Policy		dummy_address	Subnet	1.1.1.1/32						
IPv4 DoS Policy		🖀 google play	FQDN	play.google.com						
IPv6 DoS Policy		Ø none	Subnet	0.0.0.0/32						
Addresses	☆	swscar.apple.com	FQDN	swscan.apple.com						
Wildcard FQDN Addresses Internet Service Database Services		update.microsoft.com	FQDN	update.microsoft.com						
		E Address Group 🕤								
		🝓 allow_group	Address Group	dummy_address						
Schedules Virtual IPs IP Pools		💁 deny_group	Address Group	dummy_address						
		E IPvó Address O								
Traffic Shapers		SSUVPN_TUNNEL_IPv6_ADDR1	IPv6 Subnet	fdff:ffff:/120						
Traffic Shaping Policy		C al	IPv6 Subnet	0						
Security Profiles	>	dummy_address_ipv6	IPv6 Subnet	2001;db0::1/128						
2 VPN	3	Ø none	IPv6 Subnet	::/128						
User & Device	>	E IPvő Address Group 🤉								
WiFi & Switch Controller	>	Nov.group.jpv6	IPv6 Address Group	dummy_address_ipv6						
d Log & Report	>	a deny group javó	IPv6 Address Group	B dummy_address_ipv6						
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: www.fortinet.com/enterprisefirewall.



Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com

f y in D

© 2021 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).