

**DEPLOYMENT GUIDE** 

# **Fortinet and Attivo Networks**



# **Table of Contents**

Overview	3
Deployment Prerequisites	3
About Attivo Networks	3
Fortinet Configuration	4
Attivo BOTsink Configuration	4
Summary	7

#### **Overview**

Fortinet secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface, and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number 1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at <a href="https://www.fortinet.com">https://www.fortinet.com</a>, the Fortinet Blog, or FortiGuard Labs.

#### **About Attivo Networks**

Attivo Networks is the leader in deception for cybersecurity defense. Founded on the premise that even the best security systems cannot prevent all attacks, Attivo provides the required in-network visibility and substantiated, actionable alerts to detect and analyze cyberattacks, and accelerates defense through integration with prevention systems.

The core solution offered is the ThreatMatrix Deception-based Threat Detection and Continuous Response Platform, which is a comprehensive deception platform for detecting all types of threat vectors in user networks, data centers, and specialty environments of supervisory control and data acquisition (SCADA), Internet of Things (IoT), and point of sale (POS).

#### **Deployment Prerequisites**

- 1. Fortinet FortiGate—Supported versions are 5.2.0 to 5.6.1
- 2. Attivo Networks—Supported version is 4.0.1.34

For an Attivo BOTsink license, please contact the appropriate channels through Attivo. To request an evaluation of Attivo's Botsink, contact <u>support@</u> attivonetworks.com.



Attivo's BOTsink integrates with the Fortinet FortiGate firewall. Through this integration, BOTsink can provide the details of compromised endpoints such that they are immediately quarantined by the Fortinet FortiGate.

Fortinet and Attivo Networks have partnered to deliver an industry-leading security solution that addresses these challenges. The Attivo dynamic deception solution provides organizations with a way to complement their existing security infrastructure by continuously detecting and alerting them to breaches that have bypassed perimeter solutions. Fortinet's award-winning FortiGate Enterprise Firewall Platform provides the industry's highest-performing firewall capabilities and Fortinet's FortiGuard Security Subscription Services provide the industry's highest level of threat research, intelligence, and analytics. Bringing Fortinet and Attivo products together into one integrated solution delivers comprehensive endpoint and network security protection.



Figure 1: Architecture overview.

### **Fortinet Configuration**

1. Log in to the FortiGate.

User Name	
D 1	
Password	 

2. Whenever endpoint is quarantined from Attivo's BOTsink, it would create a dynamic access rule on FortiGate to block the endpoint. Below is the screenshot:

FortiGate 1500D NG	FW-	PRI			0	<u>-</u> Δ· @·∶	≻_ [] admin-
🚖 Favorites	>	+ Create New - & Edit 🗐 Clone 🔒 Dek	ete Q Search			A	ddress Group All
2 Dashboard	>	Name 🗢	Type 🗘	Details 🗢	Interface 🗘	Visibility	≎ Ref. ≎
E FortiView	>	adobe	Wildcard FQUN	"adobe.com	U any		1
+ Network	>	Adobe Login	Wildcard FQDN	".adobelogin.com	U any		1
Ö Sustem	>		Subnet	0.0.0/0	U any		28
- System		android	Wildcard FQDN	".android.com	U any	0	1
Policy & Objects	~	2 apple	Wildcard FQDN	*apple.com	U any	•	1
IPv4 Policy		appstore.	Wildcard FQDN	appstore.com	O any	•	1
IPud Access Control List		Ettivo-addr1	Subnet	(192.168.114.102/32	any	•	1
IF PROCESS CONTRICTORS		authighems	FQDN	authgrams	any any	0	1
IPv4 DoS Policy		autoupdate.opera.com	FQDN	192.168.114.102/32     any       authorsene     any       autoupdate.opera.com     any       *citribonline.com     any       *dropbox.com     any       *dropbox.com     any       *eease.com     any	•	1	
Addresses	습	🛱 citrix	Wildcard FQDN	".citrixonline.com	any	•	1
Internet Service Database		dropbox.com	Wildcard FQDN	*.dropbox.com	any	•	1
England		🔀 eease	Wildcard FQDN	*.eease.com	any	•	1
Services		B firefox update server	Wildcard FQDN	aus*.mozilla.org	any	0	1
Schedules		FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0	any		0
Virtual IPs		🗄 fortinet	Wildcard FQDN	".fortinet.com	any	•	1
IP Pools		google-drive	Wildcard FQDN	*drive.google.com	C any	•	1
Traffic Shanner		google-play	FQDN	play.google.com	any	•	1
trainc snapers		B google-play2	Wildcard FQDN	*ggpht.com	any	•	1
Traffic Shaping Policy		google-play3	Wildcard FQDN	".books.google.com	any	0	1
Security Profiles	>	B googleapis.com	Wildcard FQDN	*.googleapis.com	any	•	1
D VPN	>	B Gotomeeting	Wildcard FQDN	*.gotomeeting.com	any	•	1
Liser & Device	>	🔛 icloud	Wildcard FQDN	".icloud.com	C any	•	1
- un abente		🔀 itunes	Wildcard FQDN	"itunes.apple.com	O any	•	1
♥ WiFi & Switch Controller	>	🗄 live.com	Wildcard FQDN	".live.com	any	•	0
M Los C Depart	1				0		

## **Attivo BOTsink Configuration**

1. Log in to the Attivo BOTsink console.

**Note:** You will need to log in to Attivo BOTsink using a user with admin privileges.

	BOTsink <sup>®</sup> for VMware
User Name	Username
Password	Password
	Sign In

 To enable the FortiGate integration, navigate to Configuration → Blocking → Fortinet. Add FortiGate IP in the Server Name/IP Address tab and also place the username as admin and password: FortiGate Password. Save the configuration by clicking Save.

vCenter	Fortinet Configuration	Enabled	🖺 Save			
Monitoring Rules	Configuration					
Sinkhole Gateway	Server Name/IP Address: 10.101.24.27					
Threat Detection	Username: admin					
Customization	Password:					
Endpoint	TTL (Seconds): 60					
Malware Analysis	* All Fields are Required	- N <u>u</u>				
Policy		Test and Ge	Domains			
Central Manager						
Connect	Auto Blocking					
SIEM						
Blocking	Enabled:					
Palo Alto Networks	Severity: High					
Juniper Networks						
Blue Coat	Domains	🖾 Enable	Diasble			
Check Point	# Name		Status			
Carbon Black	1 root		2			
Cisco ISE						
ForeScout						

3. Create a monitoring rule to deploy an engagement VM in the required subnet. Click the Configuration button, select Monitoring Rules, and click Rule. Click Save in the Monitoring Rules page for the engagement VMs to acquire the configured IP addresses.

Attivo networks BOTsink VMware	<b>26 A</b>	lik 🔹	Configuration	20	*			-					•	0 4-
<ul> <li>vCenter</li> <li>Engagement</li> </ul>	Monitor	ing Rule	es								4	1	H Sov	0
Monitoring Rules	Rules					+	ule	∕ Rule	E Selected	₿ AI	DHCP B	CP Events	C Renew	w
Sinkhole Gateway	All VMs		a) Al Type											
Threat Detection	# - NetBIC	S Name	VM Name		Type	IP Address O		Netmask :	Galeway	Port Group		MAC	Address	0
<ul> <li>Customization</li> </ul>	1		Default-CentOS-NBNS		DHCP	U 192.168.114.100		255.255.255.0	192.168.114.99	ISFW-Sales-SV	i-PG	00:50:5	id:b9:86:e1	
k Endnalist	2		Ubuntu-3-24317-15-12	-53	DHCP	U 192.168.114.110		255.255.255.0	192.168.114.99	ISFW-Sales-SV	4.PG	00:50:5	6:09:78:11	
<ul> <li>Molware Analysis</li> </ul>	• 🖸 - Dynamic	Engagement	• External Trigger • 🕃	User D	efned									

4. The BOTsink dashboard gives Attack Phases and Top 5 Infected Systems.



5. Dashboard  $\rightarrow$  Events gives an option to Whitelist/Quarantine Attacker IP/Trigger Forensics.

Attiv BO	<b>10 networks</b> Tsink v <i>M</i> wc	are 🚳	A Events	lin oo	20	±							0 4
7)	Keywords	- Search f	ext	۵)				Month	Medium	•	Alerts	• 🕲	
k Counts												1.	Access
Attac								May "17					
1	everity: Medium	Time Period: Mo	onth ]    Acknowled	ged: Unacknowle	ed				1.	12 of 12 <<	< 1 > >> Num	Go Ø	*
	Severity A	tack Phase	Timestamp 👻	Attacker 0	Service	Target O	Target IP 0	Target OS	Interface 0	Device	Description		0
0	Medium	Access	20:35:38 05-10- 2017	192.168.114.1 02	Whitelist	Default-Cen-	192.168.114.106	CentOS 7.0	1002	local	Teinet connection end 03:35:37: E01: teinet sto 33 duration=10(sec) )	ed ( 17/5/11@ itus=0 pid=203	D.1
	Medium	Access	20:35:28 05-10-	192.168.114.1	Trigger For	rensics	2.168.114.106	CentOS 7.0	1002	local	Teinet connection start	ed ( 17/5/118	D.4.

6. A topology diagram is created dynamically on the BOTsink.



#### Summary

- Access to FortiGate Demo: <u>https://fortigate.fortidemo.com</u>
- FortiGate Administration Guide: http://docs.fortinet.com/fortigate/admin-guides
- Contact <u>support@attivonetworks.com</u> (or your sales representative/sales engineer) if you need any assistance with the Attivo Networks solution or for any guides/documents.



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet\*, FortiGate\*, FortiGate\*, and FortiGuard\*, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results. Moting uray. Network environments and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network environments and other results. Nothing verses or implied, except to the except to except the except to except the except to except the except to the except to except the except to except