SOLUTION BRIEF

FortiNAC Security Fabric Integrations Increase Capabilities

Introduction

The challenges facing cybersecurity experts are daunting. The attack surface is always expanding with more users and devices connecting to the network. Further, the "bolting" on of point security products over time has made security infrastructure so complex, there is limited or no visibility. Without an understanding of what's on the network, there cannot be automated policy enforcement or coordinated response to threats.

The Fortinet Security Fabric solves security infrastructure complexity by supporting integrations from hundreds of IT vendors to deliver the information sharing, automated response, and visibility needed to address today's issues. This brief will focus on one product, FortiNAC, and its various integrations with other elements in the Security Fabric.

Fortinet FortiNAC network access control integrates with the Fortinet Security Fabric to deliver visibility into all users and devices that try to connect to the network. Upon connecting, FortiNAC will identify the users and devices and then use that information to provide appropriate access to the network based on the relevant policies.

FortiNAC also has deep integrations with other Fortinet products, as described below:

Fabric Products	Integration	What FortiNAC Does
FortiGate	FortiSwitch managed by FortiGate	FortiNAC provides network visibility (where endpoints connect) and manages VLAN assignment at the point of connection for the endpoint. This is accomplished by sending the appropriate configuration commands to the device.
	FortiAP managed by FortiGate	FortiNAC provides network visibility (where endpoints connect) and manages VLAN assignment at the point of connection for the endpoint. This is accomplished by sending the appropriate configuration commands to the device.
	FortiGate ports and wireless (FortiWiFi)	FortiNAC manages endpoints directly connected to the FortiGate's wired and wireless interfaces. (FortiGate LAN ports/FortiWiFi wireless access points)
	FortiNAC/ FortiGate Fortinet Single Sign-On (FSSO) integration	FortiNAC provides automatic application of FortiGate firewall policies to hosts connecting to the network. This is achieved by using RADIUS accounting messages sent from FortiNAC to a single sign-on agent configured in the firewall. The agent contains the user ID and IP address of the connecting host. With this information, the firewall can apply user-specific policies (intent-based segmentation). This integration also includes the ability for FortiNAC to insert users into user groups.
	FortiGate VPN control by FortiNAC	ForitNAC controls network access by leveraging FSSO on the FortiGate. Network access is restricted for VPN users by default when users connect. Access is only modified if the user successfully authenticates through FortiNAC, runs an appropriate FortiNAC agent, and passes any required compliance checks. Once the user and host are identified and verified to be in compliance with the organization's prescribed policies, network access restrictions can be lifted. FortiNAC sends group and/or tag information to the FortiGate to adjust the user's network access according to the rules established in both FortiNAC and the FortiGate by the administrator.

Fabric Products	Integration	What FortiNAC Does
FortiSwitch	In standalone mode	FortiNAC provides network visibility (where endpoints connect) and manages VLAN assignment at the point of connection for the endpoint. This is accomplished by sending the appropriate configuration commands to the device.
FortiAP	In standalone mode	FortiNAC provides network visibility (where endpoints connect) and manages VLAN assignment at the point of connection for the endpoint. This is accomplished by sending the appropriate configuration commands to the device.
FortiClient EMS	MDM solution as trusted device onboarding	This integration speeds up the registration process of devices that have been registered with EMS. Devices connecting to the network can be registered in FortiNAC using host data from EMS.
FortiAnalyzer	Reporting	FortiAnalyzer provides centralized logging, analysis, and reporting across the Fortinet Security Fabric. The integration with FortiNAC enables FortiAnalzyer to receive information about and report on: ■ Events ■ FortiNAC alarms ■ Endpoint data, including inventory reports ■ Network infrastructure data
FortiSIEM	Incident response	Syslog integration enables FortiNAC to respond based on syslog messages sent from FortiSIEM. These messages provide information FortiNAC can use to send notifications (such as email) or take action against the associated host, such as disabling the host or marking it “at risk.”
FortiDeceptor	Incident response	The integration between FortiNAC and FortiDeceptor allows automatic isolation of any infected device from the network, based on FortiDeceptor alert detection. One of the compelling use cases for this integration is ransomware mitigation using an SMB deception token to lure the ransomware to encrypt fake files and raise alerts. FortiDeceptor will use FortiNAC to isolate the infected endpoint from the network automatically and prevent network damage.
FortiEDR	Incident response	Syslog integration enables FortiNAC to respond based on syslog messages sent from FortiEDR. These messages provide information FortiNAC can use to send notifications (such as email) or take action against the associated host, such as disabling the host or marking it “at risk.”

The above integrations enable FortiNAC to tightly interact with various products in the Fortinet Security Fabric, which both enhances the capabilities of FortiNAC and increases the capabilities of the Security Fabric.

FORTINET

www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® 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 may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

January 20, 2021 11:09 AM
D:\Fortinet\Solution Brief\Purple Solution Brief\FortiNAC Security Fabric Integrations\sb-fortinac-security-fabric-integrations-increase-capabilities-V1-1202021\sb-fortinac-security-fabric-integrations-increase-capabilities-V1-1202021