SOLUTION BRIEF

FortiNAC: Role-based Dynamic Network Access Control

Executive Summary

With the cost of an endpoint-based breach reaching into the millions of dollars per event, it is critical for security architects to understand and address network access control (NAC) vulnerabilities that cannot be secured by outdated solutions. Part of the Fortinet Security Fabric, FortiNAC provides comprehensive device visibility, dynamic controls, and automated responses that can reduce threat containment from days to seconds. It features a policy-based network access control engine that enhances security by enabling network segmentation for controlling access to network segments with sensitive information.

FortiNAC provides:

- Complete visibility and automated onboarding for endpoints
- Pre-connect and post-connect device monitoring
- Granular network access controls to enforce minimum security requirements
- Custom access levels by user or role
- Automated threat responses to quarantine suspicious endpoints/users
- Quick and easy scalability—up to 10,000 devices from a single solution instance

A majority (83%) of organizations report that they are at risk from mobile threats—and two-thirds (67%) say that they are less confident about the mobile asset security than other devices.[3]

Endpoint Vulnerability Puts Enterprises at Risk

According to recent IDC research, 70% of all breaches originate at endpoints.[1] With the average cost of a single successful data breach last year growing to $3.92 million,[2] security leaders should carefully evaluate their current NAC defenses. Networks are rapidly evolving as a result of digital innovations—including an increasing volume and diversity of mobile devices, Internet-of-Things (IoT) products, and cloud innovations like Software-as-a-Service applications. And at the same time, targeted threats against endpoints grow more frequent and sophisticated—while outdated access controls expose enterprises to undue risks.

First-generation NAC products functioned to authenticate and authorize endpoints (primarily managed PCs) using simple scan-and-block technology. The evolution to second-generation NAC solutions addressed the emerging demand for managing guest access, such as visitors, contractors, and business partners, to corporate networks.

FortiNAC offers a third-generation NAC solution that identifies, validates, and controls every wired, wireless, or VPN connection before access is granted. As part of the Fortinet Security Fabric, FortiNAC leverages the built-in commands of network switches, routers, and access points to establish a live inventory of network connections and enforce control over network access. Its flexible and highly scalable architecture enables FortiNAC to be deployed as a hardware appliance, virtual appliance, or cloud service. This ensures that FortiNAC can adapt to the unique needs of any network environment.

Visibility: Comprehensive Endpoint Identification

With the rapid proliferation of personal mobile devices, IoT products, and Shadow IT (technologies added to the network without involving IT/cybersecurity staff), protecting countless endpoint types that are not owned, managed, or updated by corporate IT has become a significant challenge for security leaders. FortiNAC addresses this challenge in a couple of different ways:

Device-to-User Profiling

FortiNAC uses multiple information and behavior sources to accurately identify everything on the network. It provides detailed profiling of wired, wireless, and even headless devices. This comprehensive agentless scanning process automatically discovers endpoints, classifying them by type and determining if the device is corporate-issued or employee-owned. FortiNAC supports enhanced profiling capabilities to ensure the trust of Windows Remote Management (WinRM) and Windows Management Instrumentation (WMI) devices. FortiNAC also offers passive scanning capabilities for identifying sensitive devices without disruption—such as industrial control systems (ICS) and their supervisory control and data acquisition (SCADA) subset systems within operational technology (OT) networks.

FortiNAC also identifies individual users of devices to apply the appropriate role-based network access policies to protect critical data and sensitive assets, while ensuring compliance with all applicable industry regulations and standards. Additionally, FortiNAC gives security management teams centralized administration and reporting from a single console.

Continuous Risk Assessment

FortiNAC validates an endpoint's configuration as it attempts to join the network. If the configuration is found to be noncompliant, the connection is either prevented or the device is isolated or granted limited-access VLAN. Users are then warned that their device must be remediated. Access is granted only after corrective measures have been taken. Even then, FortiNAC performs ongoing deep information scanning to provide continuous evaluation post-connection.

The cost of malware attacks per organization increased by 11% last year to reach an average of $2.6 million annually.[4]

Enforcement: Granular Access Controls

In addition to the breadth of devices connecting to corporate networks, security architects must also manage an expanding variety of users, groups, and applications—which results in a dramatically higher level of network complexity. As part of the Fortinet Security Fabric architecture, FortiNAC's tight integration with the FortiGate next-generation firewall (NGFW) enables dynamic access controls that ensure that users and devices only have access to the resources they need. Specific features include:

Segmentation Based on Business Intent

A flat and open internal network makes it easy for hackers, malicious users, or automated malware to roam freely across the organization in search of sensitive data and IP to exfiltrate. Supporting intent-based network segmentation, FortiGate NGFWs dynamically retrieve device details (e.g., user group, tagged information) from FortiNAC as devices connect or disconnect. FortiGate then uses this information to apply policies in order to segment network access for that specific device. Network access policies defined in FortiNAC determine the type of segmentation based on the specific business needs.

FortiNAC can implement segmentation policies and change configurations on switches and wireless products from more than 70 vendors. Dynamic role-based network access controls logically create network segments that group applications, link data together, and limit access to specific groups that enhance internal network security.

Simplified Guest Access

FortiNAC streamlines the secure registration process of guest users, while keeping them safely away from any parts of the network containing sensitive data. When appropriate, users can self-register their own devices (laptops, tablets, or smartphones), shifting the workload away from IT staff. If preferred, the simplified task of onboarding guests can also be delegated to designated network administrators.

Automated Responsiveness

Automation is the "holy grail" of an integrated security architecture. Instituting policy-based automated security actions helps the connected security solutions share real-time intelligence to contain potential threats before they can spread. This also helps security leaders reduce their strain on overburdened/under-resourced support teams. Without human involvement to bog down the response time, attacks and breaches can be handled with speed, efficiency, and efficacy. FortiNAC delivers real-time, automated threat responses that can immediately quarantine any suspicious endpoints or users (including IoT)—to reduce containment time from days to seconds. FortiNAC automation capabilities include:

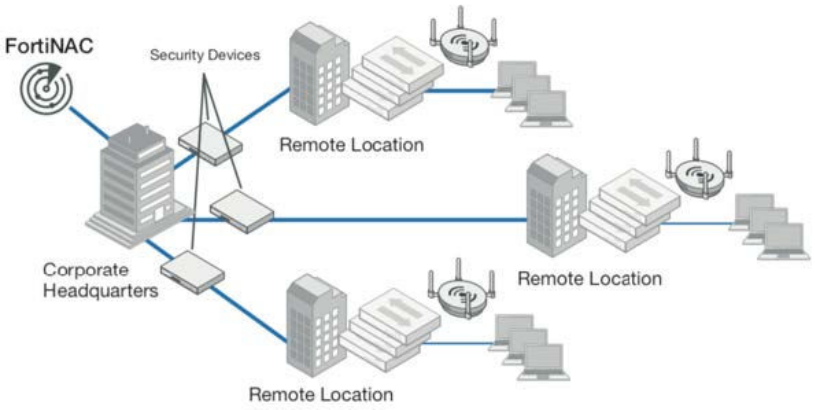

Figure 1. FortiNAC provides security and network teams with transparent visibility across all devices on the network as well as centralized policy management.

Instantaneous Containment and Compliance

FortiNAC offers a broad and customizable set of automation policies that can instantly trigger containment settings across other Security Fabric elements (e.g., FortiGate, FortiSwitch, FortiAP) when a targeted behavior is observed. Potential threats are contained by isolating suspect users and vulnerable devices, or by enforcing a range of responsive actions. As a compensating control for IoT devices with weak security, FortiNAC monitors for unusual behavior and automatically quarantines suspicious endpoints. For example, if an IoT device starts pinging a DNS server, it will be tracked, an alert will be generated, and the port can be immediately locked down while awaiting analyst review.

One primary goal of a well-designed NAC is to make tasks easier by automating the process of restricting network access and providing context-sensitive remediation guidance.[5]

Control features are accessed via a highly customizable, easy-to-use, web-based administrative dashboard. FortiNAC also features comprehensive history tracking and built-in analytics to accelerate forensic investigation and remediation efforts. It helps streamline analyst reviews by leveraging contextual awareness surrounding an alert to help quickly locate problem devices, diagnose problems, and prioritize security events. This, in turn, helps to accelerate time to resolution while reducing the burden on staff.

Policy Simulation

FortiNAC enables "what-if" scenarios when defining network access policies. By test-driving policies, administrators can evaluate the impact of making changes before implementing them. This feature helps organizations avoid implementing a policy that is too restrictive or too open and adversely impacts users and their devices.

Scalable Access Control for Every Connected Endpoint

Endpoint devices will remain a prime target for cyber criminals as long as they offer an easy, exploitable pathway to valuable data and intellectual property. FortiNAC helps security architects protect their connected endpoints from threats. Beyond its robust validation and continuous monitoring capabilities, FortiNAC uses dynamic role-based network access control to create network segments that keep compromised devices from causing extended problems across the organization. Automated containment responses across the Fortinet Security Fabric go even further to protect enterprises from the onslaught of sophisticated, endpoint-targeted attacks.

Beyond these core capabilities, FortiNAC can be deployed as a hardware appliance, a virtual appliance, or a cloud service—offering security architects a flexible, third-generation NAC solution that can adapt to the unique needs of any environment. Designed with scalability in mind, FortiNAC also helps lower total cost of ownership by not requiring a server in every deployment location. It also leverages existing directory, networking, and security infrastructures to protect existing investments and minimize disruption.

[1] Louis Columbus, "Improving Endpoint Security Needs To Be A Top Goal In 2020," Forbes, October 27, 2019.

[2] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, July 2019.

[3] "Mobile Security Index 2019," Verizon, March 2019.

[4] "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon Institute, March 6, 2019.

[5] Kirk Anderson, "NAC: Usability and Security for Users," Security Boulevard, October 3, 2019.

Copyright © 2019 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.

December 20, 2019 2:20 AM

571854-0-0-EN

D:\Fortinet\Solution Briefs\purple solution briefs\FortiNAC Update\sb-fortinac-role-based-dynamic-network-access-control-v2.1