FORTINET

FORTINAC: ROLE-BASED DYNAMIC NETWORK ACCESS

EXECUTIVE SUMMARY

Explosive device proliferation and continuously evolving sophisticated threats have kept endpoints a top target for cyberattacks. With the cost of an endpoint-based breach reaching into the millions of dollars per event, it is critical for security teams to understand and address network access control (NAC) vulnerabilities that can't be secured by outdated solutions. As 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.

THIRD-GENERATION NAC

Last year, 53% of organizations reported an increase in the number of malware-infected endpoints.[1] And with the average cost of a successful endpoint attack in 2017 reaching $5 million, organizations should carefully evaluate their current NAC defenses.[2] With network infrastructures changing via digital transformation (e.g., bring your own device [BYOD], Internet of Things [IoT], and cloud) and targeted threats against endpoints growing more frequent and sophisticated, outdated access controls are exposing enterprise networks to undue risk.

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.

COMPREHENSIVE VISIBILITY ACROSS THE NETWORK

With growth in both BYOD and IoT, protecting countless device types that aren't owned, managed, or updated by corporate IT has become a significant challenge for security teams. FortiNAC addresses this challenge in a couple of different ways.

DEVICE-TO-USER PROFILING

FortiNAC provides detailed profiling of even headless devices using multiple information and behavior sources to accurately identify everything on the network. This comprehensive agentless scanning process automatically discovers endpoints, classifying them by type and determining if the device is corporate-issued or employee-owned.

The user is also identified in order 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 offers 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 forced to an isolated or 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.

GRANULAR ACCESS CONTROLS

In addition to the breadth of devices that access corporate networks, the diversity of users, groups, and ever-evolving applications being accessed results in a dramatically higher level of complexity. A third-generation NAC solution must provide dynamic NAC controls and segmentation to keep pace.

SEGMENTATION CONTROLS THAT SECURE SENSITIVE DATA

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. 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, which enhances internal network security. This extends the reach of the Security Fabric within heterogeneous environments.

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 reduces the strain on overburdened/under-resourced IT teams. Without human involvement to bog down the response time, attacks and breaches can be handled with speed, efficiency, and efficacy.

INSTANTANEOUS CONTAINMENT AND COMPLIANCE

FortiNAC offers a broad and customizable set of automation policies that can instantly trigger containment settings in other Security Fabric elements such as FortiGate, FortiSwitch, or FortiAP when a targeted behavior is observed. This extends to all Fabric-Ready elements, including third-party solutions. Control features are accessed via a highly customizable, easy-to-use, web-based administrative dashboard. Potential threats are contained by isolating suspect users and vulnerable devices, or by enforcing a range of responsive actions. FortiNAC reduces containment time from days to seconds—while maintaining compliance with increasingly strict industry regulations and protecting critical data and IP.

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 impacting users and their devices.

NEXT-GENERATION CONTROL FOR BYOD AND IOT DEVICE ACCESS

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 reduces the strain on overburdened/under-resourced IT teams. Without human involvement to bog down the response time, attacks and breaches can be handled with speed, efficiency, and efficacy.

[1] "The Cost of Insecure Endpoints" Ponemon Institute, June 2017.

[2] Charlie Osborne, "Fileless attacks surge in 2017, security solutions are not stopping them," ZDNet, November 15, 2017.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

August 31, 2018 12:22 PM

247164-0-0-EN Macintosh HD:Users:bhoulihan:Documents:_Projects:Solution Brief:FortiNAC - Role-based Dynamic Access:sb-fortiNAC-role-based-dynamic-access-:sb-fortiNAC-role-based-dynamic-access