Checklist: How Fortinet Helps CIOs Adapt to an Expanding Attack Surface

Digital transformation (DX) is increasing both the opportunities and the vulnerabilities of the enterprise. Explosive adoption of mobile and Internet-of-Things (IoT) devices, applications, and services from multiple clouds are pushing the attack surface beyond the traditional network boundaries. The traditional perimeter has morphed into a sum of many microperimeters that all must be protected. As a result, CIOs are challenged to meet aggressive application performance service-level agreements (SLAs) while providing rock-solid security.

Intent-based Segmentation is a new approach to protecting the expanding attack surface. Leveraging next-generation firewalls (NGFWs), it specifies a comprehensive framework of business-driven segmentation, dynamically monitored and updated access control, integration with third-party orchestration systems, threat-intelligence sharing, high-performance automated threat protection.

7 Ways That Fortinet Simplifies Security

Following are seven key advantages that CIOs can derive from Fortinet Intent-based Segmentation:

☑ 1. Increased end-to-end visibility

Segmenting a flat network with Intent-based Segmentation reduces the risks associated with the expanding attack surface. Specifically, deep and broad visibility from security fabric components and from the data traversing the network is achieved by inspecting both clear text and packets encrypted using secure sockets layer (SSL)/transport layer security (TLS) protocols.

☑ 2. Proactive audit control and risk management

The **Fortinet Security Rating Service**, included in the Enterprise Protection Bundle subscription service, offers a self-assessment that helps CIOs catch configuration problems before they result in a security incident. CIOs can also leverage audit trails for compliance tracking and reporting.

☑ 3. Segmentation driven by business logic

Intent-based Segmentation enables organizations to employ flexible, business-driven segmentation that categorizes users, assets, and devices based on business logic—based on their role and access level in the organization—rather than their location on the network. Access permissions are then defined in terms of this business logic and propagated over the Fortinet Security Fabric to all the FortiGate NGFWs, wherever they reside, on corporate premises or in the multi-cloud.

☑ 4. Access control based on dynamically earned trust

Fortinet provides access to multiple validation sources through open APIs that connect with identity and access management (IAM) systems that integrate with third-party trust monitoring engines to proactively gather threat intelligence. Trust enforcement can also be adjusted based on user and entity behavior analytics (UEBA) services. Due to integration with the Fortinet Security Fabric, trust assessment and enforcement occurs in real time across each security element.

☑ 5. Minimal gaps between multivendor security solutions

Open API connections within the Fortinet Security Fabric provide two-way communications with and between all Fortinet security solutions as well as third-party security solutions. Integration with Nozumi Networks enables development of Intent-based Segmentation business logic that reflects the most recent trust-level information for man-to-machine and machine-to-machine access control.[1]

☑ 6. The lowest TCO for advanced security

Intent-based Segmentation hinges on the ability to deploy advanced threat protection wherever it is needed. This requires careful attention to total cost of ownership (TCO), something at which Fortinet excels. For example, in the 2018 NGFW NSS Labs Group Test, Fortinet NGFWs—the underlying engine behind Intent-based Segmentation—achieved the lowest TCO per protected Mbps among the participating vendors.[2]

☑ 7. Rigorous and automated threat protection

FortiGate NGFWs perform intrusion protection system (IPS), antivirus, and web filtering, as well as SSL/TLS inspection, to detect known malware such as Zeus, TrickBot, and Dridex. Fortinet Intent-based Segmentation capabilities integrate with artificial intelligence (AI)-based FortiGuard Services and Advanced Threat Protection Services, in addition to third-party threat-intelligence services, to automatically detect and protect against known and unknown threats.

Comprehensive Support for Defense-in-Depth Strategies

Intent-based Segmentation is a promising approach that CIOs can use to protect their networks and digital assets as their organizations press forward with ambitious DX initiatives. Specifically, Fortinet Intent-based Segmentation allows business logic to drive segmentation, leading to more nimble and manageable security zones. These zones can be protected by employing dynamic access control, applying security policies consistently across multiple enforcement points, and performing rigorous, high-performance threat protection, leveraging highly cost-efficient NGFWs.

[1] "Fortinet and Nozomi Comprehensive OT Security Solution," Fortinet, September 11, 2018.

[2] Thomas Skybakmoen, "Next Generation Firewall Comparative Report: Total Cost of Ownership (TCO)," NSS Labs, July 17, 2018.

FORTINET®

www.fortinet.com

June 27, 2019 10:59 PM

364587-0-0-EN

D:\Fortinet\Work\2019\June\062719\checklist-intent-based-segmentation-solution