CHECKLIST

How Fortinet Intent-based Segmentation Helps CIOs Manage Increased Security Complexity

Digital transformation (DX) initiatives such as cloud adoption, DevOps, growth in Internet-of-Things (IoT) devices, and proliferation of data ratchet up the complexity of managing security that spans many point products that do not communicate with each other and require sophisticated custom-built automation and orchestration tools across distributed locations. These factors are further complicated by evolving government and industry regulations and security standards, not to mention demands from the C-suite and board of directors to measure and report on risk.

Intent-based Segmentation enables CIOs to reduce security complexity by improving security visibility, adapting access permissions to current levels of trust, and enforcing access control effectively and efficiently.

5 Reasons to Leverage Fortinet Intent-based Segmentation

Following are five ways CIOs can leverage Intent-based Segmentation to overcome the obstacles associated with network security management.

☑ Consolidate end-to-end visibility and threat protection.

Intent-based Segmentation is an architecture built on the components of the Fortinet Security Fabric that comprises an extensive range of security products, all of which intercommunicate to enable real-time threat intelligence and automated protection. The Intent-based Segmentation architecture is flexible, as it relies on Security Fabric connectors to integrate with external orchestration systems to further improve visibility and enable more effective threat response. All of the Fortinet and third-party components are managed from a single pane of glass, minimizing IT staffing and training costs.

☑ Always know who and what to trust.

Because even the most trusted users or widely used applications can be compromised, trust must be verified continually. To maintain security while avoiding the burdens of prolonged sign-on procedures, the Fortinet Security Fabric integrates with several third-party trust monitoring engines. This Intent-based Segmentation model continually gathers threat intelligence from outside sources, which is used to automatically update access permissions.

☑ Let the business—not the network—drive compliance.

Intent-based Segmentation enables business and compliance needs to drive access control policies. It leverages various features of the Security Fabric to perform tagging and categorizing of users, devices, and applications without concern for the underlying network architecture. These tags are automatically disseminated throughout the Security Fabric and used to enforce access control policies consistently across the network. Thus, with a very lean IT staff, CIOs can ensure the ongoing compliance of their large and growing networks.

☑ Automate security posture assessments and audit trails.

Fortinet leverages various forms of automation as part of its Intent-based Segmentation solutions to facilitate compliance enforcement and auditing. To help CIOs demonstrate compliance and manage the organization's security posture, the Security Fabric contains built-in controls and reporting capabilities for regulatory and industry standards. Compliance checks may also be run to satisfy auditors' requirements. Because in-house security experts are often in scarce supply, Fortinet provides for the continual monitoring of network configurations, translates discovered vulnerabilities into specific risks on a dynamic dashboard, and provides step-by-step remediation checklists.

☑ Lower the TCO of deep and broad threat protection.

Access control enforcement is a key pillar of the Intent-based Segmentation approach. Fortinet implements Intent-based Segmentation enforcement with threat protection components that inspect every packet traversing the network, even encrypted traffic, without compromising productivity or user experience. A broad selection of form factors and sizes means CIOs can keep equipment costs in line with traffic volumes and site characteristics. Moreover, Fortinet next-generation firewalls (NGFWs) deliver the lowest total cost of ownership (TCO) per protected Mbps of network throughput in the industry.[1]

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

FORTINET®

www.fortinet.com

August 6, 2019 1:19 AM

D:\Fortinet\Checklist\IBS\ch-FA-ibs-cio-sol-selection-complexity-080119\ch-FA-ibs-cio-sol-selection-complexity-080119

364547-0-0-EN