FORTINET

Reducing Complexity with Intent-based Segmentation

Best Practices for CIOs

Table of Contents

Executive Overview 3

Conquering Complexity for Secure DX 4

The Principles of Intent-based Segmentation 6

The Importance of Business Intent 6

Comprehensive Visibility and Control with Centrally Managed Security 9

Enable Continuous Trust Monitoring 11

Conclusion 12

FORTINET

Executive Overview

Digitally transforming organizations, which rank security as their number one concern, are finding that perimeter security is inadequate. The reason is that threats penetrating perimeter defenses find it easy to move laterally throughout the internal network. Although internal segmentation promises to provide the necessary second line of defense, current segmentation solutions are too complex for CIOs to sustain in their growing enterprises.

An alternative approach, Intent-based Segmentation, helps reduce this complexity and provide more effective tools to manage both security posture and compliance. It relies on business logic rather than the network architecture definitions to separate assets and define access-control policies. This gives CIOs greater freedom to implement policy changes inexpensively and quickly. Access rights are updated without manual intervention, based on continuous trust assessments from multiple internal and external sources.

Security issues are the biggest barrier to digital transformation efforts; 85% of organizations say it is "a large impact."[1]

Conquering Complexity for Secure DX

In an environment of digital transformation (DX), where mobile computing, multi-cloud deployments, bring your own device (BYOD), and Shadow IT are the norm, enterprise networks are becoming increasingly vulnerable to accelerating and more sophisticated threats. Numerous business policies are introduced and updated to protect networked assets and to comply with growing regulatory burdens. These often require the separation of assets, both to isolate intellectual property and customer data and to secure critical applications from attacks.

CIOs are often stymied, however, by the constraints of the network architecture and the time and effort it takes to reconfigure the network to achieve their DX objectives. Three-quarters of CIOs see IT complexity as an overwhelming obstacle to doing so.[2]

Intent-based Segmentation was conceived as a way to overcome such obstacles, so that security can become the foundation for network initiatives rather than detracting from them.

To achieve DX success, organizations need high-performance, low-TCO security that is not only ubiquitous but also integrated and easy to manage.

Maintaining adequate security is a challenge for organizations when a single web application now crosses an average of 35 different technology systems or components.[3]

The Principles of Intent-based Segmentation

With Intent-based Segmentation, CIOs are able to translate business and DX intent into the network security configurations and controls needed to fulfill that intent. Three principles govern Intent-based Segmentation:

- It uses business needs, rather than network architecture alone, to establish the logic by which digital assets are grouped and isolated.
- It provides finely tunable access controls and uses those to achieve continuous, adaptive trust.
- Using high-performance, advanced Layer 7 (application-level) security across the network, it performs comprehensive content inspection to attain full visibility and prevent attacks.

The components that perform the security function, next-generation firewalls (NGFWs), are the keystones of the segmented network. To successfully implement Intent-based Segmentation to support DX, organizations need high-performance, low total-cost-of-ownership (TCO) NGFWs that are not only ubiquitous but also integrated and easy to manage.

For this reason, the NGFWs operate as part of a fabric of security components. All the NGFWs connect to and communicate with the others, whether they are on-premises, at a branch or a remote site, or in the multi-cloud. They are centrally orchestrated with a high degree of automation, reducing the IT resources needed to manage them. They also benefit from external resources (threat intelligence, security ratings, trust-level assessments, and more) that are seamlessly integrated into the fabric, minimizing the integration of disparate solutions that delays so many IT projects.

The Importance of Business Intent

Network and infrastructure assets must be isolated and access-controlled for a number of reasons. These may include global data privacy regulations such as the European Union's General Data Protection Regulation (GDPR), vendor system integration, merger and acquisition (M&A)-related network consolidation, and the introduction of Internet-of-Things (IoT) devices. In the case of the latter, they lack the robust security controls found in other devices and are typically more vulnerable to cyberattacks.

In meeting these varying requirements, Intent-based Segmentation is unique in its ability to define assets according to their role in the business rather than their location on the network—whether on-premises or in the cloud, in the data center or at the network edge, and so on. Intent-based Segmentation integrates with existing networks, and thus it does not require changes to network architecture or equipment. CIOs can see their network security, compliance, or other directives implemented more quickly and with fewer glitches.

PCI DSS Compliance Use Case

Consider the Payment Card Industry Data Security Standard (PCI DSS) as an example. In traditional security scenarios, when business intent is to achieve and maintain PCI DSS compliance, standard practice is to isolate the subnet where payment and customer personally identifiable information (PII) resides.

But networks are not typically configured for a specific compliance purpose. Assets and users required to meet PCI DSS compliance standards might reside in several subnets and across geographical locations. Complicating matters further, the subnets and locations where PCI-related assets and users reside could also contain assets and users that are not subject to PCI restrictions.

With Intent-based Segmentation, assets and users can be tagged for PCI DSS compliance needs, regardless of their location on the network and any other compliance controls or access policies that apply to them. This reduces the time and cost of compliance implementation efforts, especially in periods of organizational restructuring. It also gives organizations the agility they need to quickly comply with new regulations and updates.

"Focusing on annual compliance assessments can create a false sense of security. It's only by achieving, assessing, and maintaining compliance in a regular manner that your cyber defenses will be adequately primed against attacks aimed at stealing cardholder data."[4]

With Intent-based Segmentation, assets and users can be tagged for compliance needs, regardless of their location on the network. This reduces the time and cost of compliance implementation efforts.

Comprehensive Visibility and Control with Centrally Managed Security

Consistent policy management requires both visibility across the network and the ability to propagate policies with minimal human intervention. This is particularly important as cloud services become an increasingly large component of the DX network infrastructure. The use of disparate cloud security tools leads to inefficient, piecemeal risk assessment and unacceptably slow dissemination of policy and trust updates.

Using Intent-based Segmentation, organizations can control cloud spend and cloud-based Shadow IT by defining access controls for cloud app usage, new cloud service subscriptions, workloads, or whatever the business need dictates. These policies can be defined once, and the access controls automatically implemented across the on-premises network, private clouds, and public cloud providers. This more efficient, less labor-intensive method can significantly reduce the total cost of security management.

Inspect Everything Without Compromising Performance

What enables all this is a centrally managed security fabric comprising high-performance NGFWs. These NGFWs should be available in a variety of physical and virtual form factors (including adaptations for each public cloud service) with a low-enough TCO to justify deployment wherever necessary. The NGFWs are the “eyes and ears” of the security fabric, inspecting and collecting data on all the traffic, whether it is secure sockets layer (SSL)/ transport layer security (TLS) encrypted or clear text. They are also the agents through which the central security management system enforces the access policies.

The security fabric enables every security component to communicate with every other component in real time (as opposed to going through a traditional hub). Thus, when a threat is discovered in an application, remediation is automatically communicated to all other NGFWs that are part of the security fabric, so all of the servers running that application—whether in the data center or in any of several clouds—are protected immediately. Compromised assets or users that were the source of the threat are either banned or quarantined. Furthermore, if the affected application involves a sensitive business process or compliance-related data, the restrictions can cascade to other network assets that were defined as such.

Top-tier organizations—those that have had no outage, data loss, or compliance event in the past two years—are 34% more likely to make sure their safeguards work everywhere (on-premises, cloud, IoT, mobile, etc.).[5]

Enable Continuous Trust Monitoring

Traditionally, access control operates under the assumption of implicit trust, as if it is known which users, devices, and applications are trusted and which are not. But because trust is not static, it cannot be implicit. For example, trusted applications and devices may become infected by malware, while previously trusted users could turn against the organization. Such changes in trust levels dramatically affect the CIO's ability to assure compliance and meet privacy and security obligations to partners and customers. Relying on static, implicit trust puts the organization at risk.

Intent-based Segmentation relies on continuous trust assessments from multiple internal and external sources. Based on these assessments, Intent-based Segmentation provides network users, devices, and applications the minimum access they need. The tight integration of security components within the overall security fabric ensures that updated trust information is rapidly disseminated throughout the network.

Finally, it is essential to demonstrate to corporate stakeholders that the accepted trust levels and the associated access policies are achieving their business objectives. To this end, Intent-based Segmentation stipulates continual evaluation of the organization's network security posture. The most effective and efficient way to do this is through a trusted and actionable security rating service, which provides automated tracking and reporting for various compliance requirements.

"Least-privilege access to networked capabilities is dynamically extended only after an assessment of the identity of the entity, the system and the context."[6]

Conclusion

Network security is becoming a growing, complex challenge for CIOs. Mobile computing, multi-cloud operations, BYOD, and Shadow IT are proliferating, making compliance increasingly difficult. Even day-to-day security management is a struggle, as more than 80% of organizations are challenged to identify all of the connected devices in their network.[7] Complexity, therefore, is the enemy of security.

Intent-based Segmentation offers a solution to reduce security complexity by providing end-to-end comprehensive visibility, adaptive trust, cost-effective enforcement, and consistent security policy control through centralized management, irrespective of the location of an organization's digital assets.

[M]ore than 80% of organizations are challenged to identify all of the connected devices in their network. Complexity, therefore, is the enemy of security.[8]

[1] "2018 Security Implications of Digital Transformation Report," Fortinet, July 25, 2018.

[2] Ibid.

[3] "76% of CIOs Say It Could Become Impossible to Manage Digital Performance, as IT Complexity Soars," Dynatrace, January 31, 2018.

[4] "How to Secure with the PCI Data Security Standard," PCI Security Standards Council, accessed February 14, 2019.

[5] "2018 Security Implications of Digital Transformation Report," Fortinet, July 25, 2018.

[6] Neil MacDonald, "Zero Trust Is an Initial Step on the Roadmap to CARTA," Gartner, December 10, 2018.

[7] Nirav Shah, "The Security Risks Presented by Complex Networks," Fortinet, May 1, 2018.

[8] Ibid.

FORTINET

www.fortinet.com

352006-0-A-EN

April 5, 2019 7:36 AM

ebook-fortinet-solution-for-automation-CIO