FORTINET

Fortified Security Enabled Through Intent-based Segmentation

Protecting Digital Assets with an Efficient Operational Approach

Table of Contents

Executive Overview

To meet the time-to-market pressures of digital transformation (DX) and to spur organizational growth, CIOs are directing their teams to move beyond perimeter security. Their aim is to respond more assertively to attack surfaces that are expanding on all fronts across the enterprise. This typically involves segmenting the network and infrastructure and providing defense in depth with multiple forms of security.

Because traditional segmentation methods have proven to be insufficient in meeting DX security and compliance demands and too complicated to be sustainable, many organizations are turning to Intent-based Segmentation. What sets this approach apart is that it enables business intent to drive segmentation of the network and controls access using continuous trust assessments. It also provides comprehensive visibility of everything flowing across the network, enabling real-time access control tuning and threat mitigation. For the CIO, Intent-based Segmentation translates into more effectively managed network security risk.

As multi-cloud, mobile-first, Internet-of-Things (IoT), and other DX initiatives bloat attack surfaces, Intent-based Segmentation offers a vital new approach.

Intent-based Security: The Big Picture

Intent-based Segmentation emerged in response to three flaws in traditional methods of internal network security segmentation: limited ability to adapt to business and compliance requirements, static or implicit trust, and poor security visibility and enforcement. Addressing these shortcomings has led to the following principles:

- Intent-based Segmentation uses business needs, rather than the network architecture alone, to establish the logic by which users, devices, and applications are segmented, 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, Intent-based Segmentation performs comprehensive content inspection to attain full visibility and prevent attacks.

The architecture that supports these principles is a security fabric, an extensible set of integrated security components, which connects to and communicates with on-premises and cloud network and infrastructure devices. Such a fabric also seamlessly integrates with third-party solutions, including trust databases. This enables real-time adjustment of access permissions based on current trust status. The result is end-to-end visibility of all types of traffic flowing across the network, automated advanced threat protection, and a low total cost of ownership (TCO) impact. The following sections describe these principles in more detail:

First Principle: Segmentation Driven by Business Intent

Intent-based Segmentation enables the creation of security domains or segments in accordance with business intent. For example, as cloud services become an increasingly large component of the network infrastructure, Shadow IT and spending on cloud services are growing as well, often bypassing the CIO. This can lead to spiraling IT costs and security issues related to cloud sprawl. In response, organizations can leverage Intent-based Segmentation to control cloud spend and Shadow IT activities. This is achieved by relying on security fabric open APIs to acquire application usage metering information from the cloud service. This information can then be compared with allotted utilization quotas and, when needed, used to limit access if set quotas are exceeded. Such access controls work across cloud providers, supporting the needs of DX enterprises operating in multiple clouds.

The increasing deployment of Internet-of-Things (IoT) devices presents another significant segmentation challenge. It is well known that IoT devices are highly vulnerable to cyberattacks. IT teams that rely heavily on IoT security best practices, such as those developed by the National Institute of Standards and Technology (NIST), may wind up developing highly restrictive network segmentation rules that lead to operational disruptions. Such is the case with wireless infusion pumps and other critical-care devices in hospitals. When medical staff cannot access these devices over the network because of certain rigidities in the VLAN-based segmentation design, patients' lives may be at risk.[1] With Intent-based Segmentation, these devices would be tagged according to their medical use, regardless of their location on the network. Access permissions would then be tailored to those devices.

"The three most important aspects of any IoT security strategy will be device identification, network segmentation, and network traffic analytics."[2]

Second Principle: Fine-grained Access Control Maintained Through Adaptive Trust

To achieve business intent, segmentation must not only define where to draw the lines of demarcation but also how to control who or what can cross these lines. Intent-based Segmentation enables very fine-grained access control. Organizations can permit or deny access based on individual user identities, device types, or specific business policies not accounted for in the network design. Consider the hospital infusion pumps mentioned in the previous section. These can be automatically categorized and tagged as a type of medical device by network access control (NAC) components of the security fabric. The NAC components pass the tags to next-generation firewalls (NGFWs) located throughout the network, which use them to define the access control permissions based on the hospital's policies.

But knowing what is connected to the network is just the first step in access control. To determine the appropriate level of access for every user, device, or application, an Intent-based Segmentation solution must also assess their level of trustworthiness. Various trust databases exist that provide this information. Trust, however, is not an attribute that is set once and forgotten. Trusted employees and contractors can go rogue and inflict extensive damage before they are discovered, as several large corporate breaches have proven. Similarly, IoT devices can be manipulated for attacks, data exfiltration, and takeovers.[3] Furthermore, business-critical applications—especially those used by suppliers, customers, and other players in the supply chain—can inflict damage far and wide if their trust status is only sporadically updated.

Some organizations have considered solving the trust problem by blocking all access pending verification of trust status. But this can be overwhelmingly complicated to implement and costly to maintain. Intent-based Segmentation takes a trust-and-verify approach, linking access control to continuously updated and earned trust, verified by multiple internal and external sources.

Half a billion smart devices—including 75% of IP cameras and 66% of printers—are susceptible to a type of attack in which remote attackers get around firewalls and gain access to vulnerable devices on a local network."[4]

Third Principle: Pervasive, High-performance Threat Protection

Organizations that implement NAC often do not have all the necessary security components in place to enforce it, while those components that are in place do not provide full visibility into all types of traffic flowing across the network.

To address these issues, Intent-based Segmentation stipulates the broad deployment of advanced threat protection NGFWs—from the data center to the network edges and in every cloud service in which the organization operates. Plus, the entire network of NGFWs should be visible and controllable in a consistent fashion from a single management console. Crucially, the corresponding TCO of this broad security fabric should not be prohibitive.

Visibility should also extend deep into the data traversing the network. Now that more than 72% of network traffic is encrypted using secure sockets layer/transport layer security (SSL/TLS) protocols,[5] CIOs have increasing cause for concern. Cyberattackers commonly hide malware, such as Zeus, TrikBot, and Dridex, in encrypted packets.[6] They calculate that organizations assume encrypted traffic to be safe and would not tolerate the potential network slowdowns associated with decrypting and inspecting every SSL/TLS packet.

Intent-based Segmentation eliminates the security-performance trade-off. NGFWs with purpose-built security processors minimize the latency associated with the packet decryption and inspection process. Thus, SSL/TLS inspection can operate continuously, and access policies can be rigorously enforced without any appreciable impact on network performance.

With SSL/TLS inspection enabled, the NGFWs can inspect both encrypted and nonencrypted traffic for known and unknown malware and isolate threats so that they do not spread to other network and IT assets. This is accomplished by leveraging artificial intelligence (AI)-powered threat intelligence and remediation, which are part of the security fabric. It also simultaneously relies on sandboxing to inspect traffic for unknown and zero-day threats.

In addition to enabling a more accurate picture of the inherent risks in the network, Intent-based Segmentation also relies on the ability to assess the organization's security posture continuously. Security rating services allow CIOs to evaluate their network's security configuration and gain meaningful insights into risk and vulnerability. Such services also track the security posture over time, compare the organization's overall security posture with that of similar organizations, and measure it against accepted security standards.

Choosing a vendor with a broad selection of appropriately sized physical and virtual NGFWs allows organizations to deploy NGFWs wherever they are needed for Intent-based Segmentation at a reasonable TCO.

The broad network of NGFWs should be visible and controllable in a consistent fashion from a single management console. Visibility should also extend deep into the data traversing the network.

70%

of CISOs see network visibility blind spots as a “somewhat large” or “extremely large” security concern.[7] An integrated fabric of encryption-inspecting firewalls provides an end-to-end view, in real time.

Conclusion

Expanding attack surfaces should not impose barriers to DX—even with ambitious time-to-market objectives. As they work toward these objectives, CIOs can respond to their corporate stakeholders' demands for rock-solid security with Intent-based Segmentation.

This new approach to reducing attack surfaces specifies a comprehensive framework of business-driven segmentation, dynamically revised access control, and automated threat protection. End-to-end visibility into every user, application, device, and data that impacts the network—without network performance degradation—is a signature aspect of this approach.

[1] Kevin Townsend, "NIST's New Advice on Medical IoT Devices," SecurityWeek, August 27, 2018.

[2] Ibid.

[3] Ms. Smith, "Half a billion smart devices vulnerable to decade-old DNS rebinding attacks," CSO Online, July 22, 2018.

[4] Ibid.

[5] "Q3 2018 Threat Landscape Report," Fortinet, November 2018.

[6] Omar Yaacoubi, "Uncovering the hidden risks in encrypted data," ITProPortal, January 3, 2019.

[7] "2018 Security Implications of Digital Transformation Report," Fortinet, July 25, 2018.

www.fortinet.com

476454-0-0-EN

August 15, 2019 11:36 PM

FA - eb-fortified-security-enabled-through-intent-based-segmentation