FORTINET

WHITE PAPER

A Network Operations Guide for Internal Segmentation

Essential Practices for Risk Mitigation and Compliance Across the Attack Surface

Executive Summary

Segmentation of networks, devices, users, and applications has long been a best practice for supplementing edge security and breaking up flat internal networks. However, for network engineering and operations leaders who prioritize risk mitigation, achieving compliance and effective security posture management, current segmentation approaches fall short.

Traditional approaches control access at a level that is too coarse-grained to fulfill business requirements. They rely on trust assessments that are quickly outdated and assume that threat protection exists, even when the organization has gaping holes in its growing attack surface. This kind of environment renders network engineering and operations leaders unable to manage their security posture proactively and leaves their organization open to greater security risk.

As multi-cloud, mobile-first, Internet-of-Things (IoT), and other digital transformation initiatives bloat attack surfaces, Internal Segmentation offers a vital new approach. It addresses segmentation's current shortcomings and is applicable to a wide range of access-control scenarios.

With an average of 75 different security tools deployed, how can an enterprise expect to have transparent, end-to-end visibility?[1]

Effective segmentation must leverage business goals to establish where, how, and what for effective security execution.

Fundamentals of Internal Segmentation

Internal Segmentation efficiently translates the network leader's business goals into the "where," "how," and "what" of security segmentation:

- **"Where"** establishes the locations of segment demarcation and the logic by which the IT assets will be segmented.
- **"How"** implements the business goals with fine-grained access control and maintains it using continuous, adaptive trust.
- **"What"** enforces the access control by applying high-performance advanced (Layer 7) security across the network.

These three elements operate within the context of an integrated fabric of security components, which connects to and communicates with other network and infrastructure devices. Thus, without altering their network architectures, network leaders can effectively improve their security posture, mitigate risks, and support compliance and operational efficiency across the enterprise.

Segmentation That Fulfills Business Goals

Internal Segmentation supports prevailing **macro- and micro-segmentation architectures,** as well as **application-, process-, and endpoint-level segmentation**. By segmenting a flat network using one of these segmentation techniques, a network operator can create smaller, more manageable attack surfaces that can be further protected using high-performance advanced (Layer 7) security.

Internal Segmentation allows network operators to create security domains or segments based in accordance with business goals. To achieve business goals, however, segmentation must provide a more fine-grained access control that is based on **user identity or a business logic** and the ability to adjust access control based on recent trust by querying an external trust database that collects continuous trust assessment.

Adaptive Trust for Informed Risk Management

Traditionally, access control assumes unchanging trust values for users, devices, and applications. In reality, the trustworthiness of all these elements changes frequently, either due to normal changes in business operations or as a result of developing threats. Because changes in trust level dramatically affect the organization's security posture and the inherent risk in the network, using static trust leaves network leaders dangerously uninformed.

For this reason, Internal Segmentation links access control to continuously updated trust levels. In the more comprehensive Internal Segmentation solutions, this information is acquired from both internal and external sources.

In addition to enabling a more accurate picture of the inherent risks in the network, Internal Segmentation also relies on the ability to assess security posture continuously. **Security rating services** are available to evaluate the network's security configuration and provide meaningful insights into risk and vulnerability, as well as best practices for remediating configuration deficits. 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. Organizations should look for solutions that deliver real-time threat-intelligence capabilities, enabling them to have full visibility of threats across the entire attack surface from a single pane of glass. Additionally, with security rating capabilities, network engineering and operations teams can prioritize vulnerability patching and pinpoint new threats as changes occur—both internal to the network and externally.

72% of internet traffic is now encrypted, and cyber criminals are exploiting it to infiltrate networks and exfiltrate data.

Due to the advanced threat landscape, network engineering and operations leaders must assess their network's security posture continuously.

Potent, Pervasive Threat Protection

Many organizations that implement access control do not have all the necessary security components in place to enforce it. And those components that are in place are not necessarily integrated. This impairs the ability of network engineering and operations leaders to detect developing threats and prevent attacks from reaching their targets or infecting the entire network.

Always-on SSL across the network. To enforce the access policies and defend the entire attack surface, Internal Segmentation prescribes highly cost-effective and high-performance advanced (Layer 7) threat protection in next-generation firewalls (NGFWs), which provide secure sockets layer (SSL) inspection as an integral component.

As 72% of internet traffic is now encrypted, inspecting SSL- or transport layer security (TLS)-encrypted traffic across the network is no longer optional.[2] The exposure of malware such as Heartbleed, Poodle, and Zeus has shown just how vulnerable the encryption standard is to exploitation.[3] Still, many organizations hesitate to apply SSL inspection full force because of its potential impact on network throughput and user experience. For this reason, NGFWs used in Internal Segmentation should feature **purpose-built, high-performance processors** that minimize throughput degradation. With such processors, the SSL inspection function in all the NGFWs may be turned on at all times.

An important principle of Internal Segmentation is the ability to deploy threat protection wherever it is needed, both on-premises and in all the clouds in which the organization operates. Some network engineering and operations leaders may balk at the potential cost of such a policy. However, selecting NGFWs from a vendor that offers a variety of physical and virtual form factors and port densities minimizes total cost of ownership (TCO), making widespread deployment feasible.

End-to-end management. The deployment of diverse threat-protection solutions across the network requires effective end-to-end visibility and management. To proactively protect the entire network from threats originating in any part of it, Internal Segmentation solutions should be deployed as part of an integrated security fabric. In this case, it must provide comprehensive, end-to-end visibility and consistent policy controls across every security enforcement point.

Use Cases

Internal Segmentation is applicable to a wide variety of access-control scenarios. Following are two examples that illustrate how appropriate access-control classifications and advanced, high-performance threat protection give network engineering and operations leaders better control over their security architecture and help them to more effectively mitigate risk.

Use Case: Reducing Attack Surface

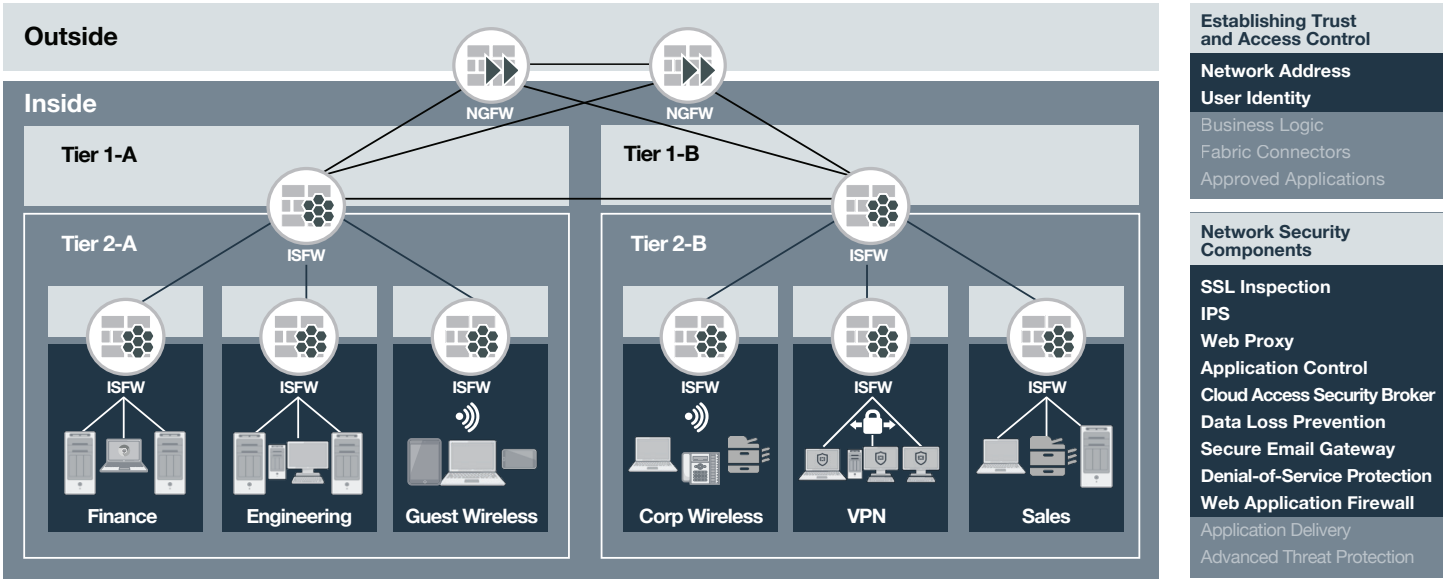

Figure 1. Use Case: Mitigating Risk by Reducing the Attack Surface

Most enterprises cannot rely on perimeter defenses alone to protect their network assets. When breaches occur—due to improper configuration, compromised devices connecting to the internal network, or zero-day attacks that bypass security controls—the network must be ready with **additional layers of defense** (shown in Figure 1 on the boundaries between Tiers 1 and 2, as well as within Tier 2).

These additional internal segmentation firewalls apply a variety of security controls to contain any malicious activity that occurs within the zones they protect. Authentication, in this case, is typically based on asset ID (network address) or user identity. Note that the addition of the security segmentation does not require changing the network architecture itself.

All the firewalls communicate with each other and with the single-pane-of-glass management system, resulting in end-to-end visibility of traffic on the network. The fabric-based management system consolidates the threat-protection activity from all the security components to create a full audit trail.

Use Case: Achieving Compliance

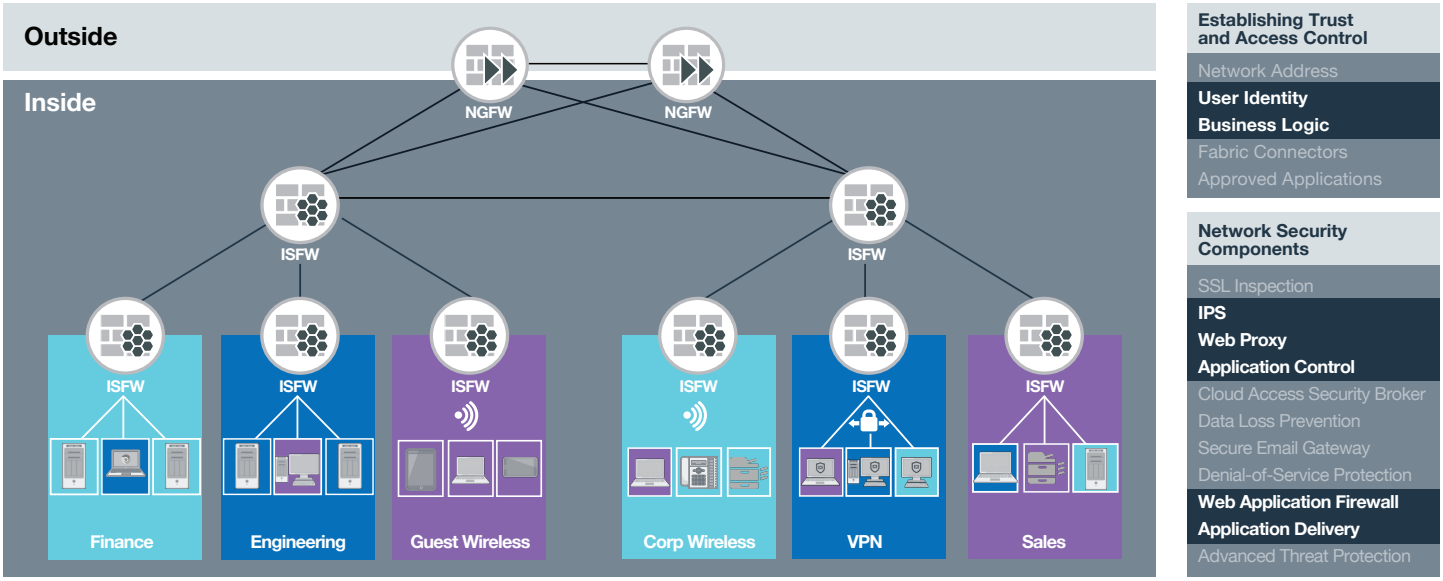

Figure 2. Use Case: Responding to a Complex Web of Compliance Requirements

Compliance with government and industry regulations is rarely optional. It is impractical, however, to reconfigure the network every time compliance rules change or new regulations go into effect.

For example, it would be extremely difficult to segment assets for Payment Card Industry Data Security Standard (PCI DSS) compliance just by isolating the finance subnet, shown in Figure 2. In real organizations, not all devices in the finance subnet may be subject to PCI compliance; some that are subject to PCI may be on other subnets, or even in remote locations.

With Internal Segmentation, access policies can be defined and enforced through the fabric-connected security components. Assets and users can be tagged for PCI compliance needs, regardless of their location on the network and regardless of other compliance controls or access policies that apply to them.

Conclusion

Although Internal Segmentation is a new approach, it is nonetheless a production-ready solution. The products and services needed to implement Internal Segmentation are widely available, and the list of fabric-connected threat protection components is growing steadily.

Network engineering and operations leaders are encouraged to implement Internal Segmentation proofs of concept, either by following the use cases presented here or by using their current business requirements. Upon request, Fortinet will demonstrate how to take a stepwise, measured approach to Internal Segmentation by implementing core components and connecting them to the networking technologies an organization already has in place.

[1] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO Online, March 14, 2016.

[2] "Q3 2018 Threat Landscape Report," Fortinet, November 6, 2018.

[3] Ananda Rajagopal, "How SSL encryption gives a false sense of security," CSO Online, accessed February 4, 2019.

FORTINET

www.fortinet.com

348072-A-0-EN February 14, 2020 7:48 AM

Macintosh HD:Users:ckluck:Documents:FORTINET_ck:2019:wp-solution-research-network-director:final:final-2:wp-solution-research-network-director