FORTINET

WHITE PAPER

Internal Segmentation Firewall

Security Where You Need It, When You Need It.

Internal Segmentation Firewall

Security Where You Need It, When You Need It.

Table of Contents

Executive Summary

Area 51 is one of the most secure facilities in the world. While it has acres of land surrounding the base, a perimeter fence, keycard, door locks, biometric scanners, and multiple alarms—none of these features individually keeps Area 51 safe. Each one is a strand that helps to weave an exceptionally strong web of security for protection inside and out.

Enterprise networks can benefit from the same kind of security philosophy. While an edge firewall can do an excellent job of protecting the network perimeter, it can't help with attacks on the inside, after a breach occurs.

Today's threats are designed to slip past traditional edge firewalls to reach the unprotected internal network. The notion of the "Trusted" internal network is now archaic. Relying on perimeter security is no longer sufficient as there are many vectors that can circumvent the perimeter firewall. BYOD, wireless, and unprotected wired access are just a few ways that malicious code can make its way into an internal network.

Fortinet believes that there is a strong need to address internal network security before the quantity of networks and devices makes it too complex to introduce new components or establish a new architecture. Based on the feedback from our customers, we know that companies of all sizes are facing similar challenges and are looking for an immediate solution. The good news is that Enterprises can do a lot more to protect their assets and data from within.

Historically, trying to implement internal security has been problematic due to high performance requirements and/or limited capital resources. But today, Fortinet has solved this problem with a new class of device that removes the constraints and limitations of what a firewall can do for the enterprise. The **Internal Segmentation Firewall (ISFW)** is designed to protect network segments from malicious code that makes its way to the internal network.

Fortinet's ISFW architecture delivers maximum performance and maximum security, while still offering the flexibility of being placed anywhere in the enterprise. Fortinet's enterprise management solution creates simple ways to manage the overall policy for multiple devices securing the enterprise's internal network security.

This white paper presents both a design approach as well as a reference architecture for implementing an ISFW strategy for your enterprise with Fortinet's proven security solutions.

Increasing Attack Surfaces

Threat vectors are coming in increasing numbers, and from multiple directions. Given the advent of many new and not so new technologies and practices within the enterprise, most networks have not adopted new strategies to deal with the current situation. As a result, there seems to be more exposure than ever to security threats.

Cloud computing has been on the rise for several years now, but the ability to see what's coming in and out of them has not improved. For example, SaaS vendors sell a service, hosted external to the enterprise. They are most likely not providing the details of their implementation nor the "secret sauce" of their technology—customers must trust that the vendor is able to deliver the service in a secure manner. This is not unlike any other type of traditional B2B trust relationship—assumptions are often made that the partner is doing all the right things in terms of security.

Even if one assumes that the partner's security efforts are effective, it's still a black box. Many cloud computing companies can serve as a gateway in and out of your enterprise network—one that the end customer has no visibility into. Is intellectual property being exfiltrated? Is malicious code flowing in? Without visibility, there is no possibility for attack prevention, let alone detection or forensics.

The issue of BYOD is another fact of life for enterprise networks, regardless of whether or not the policy is officially embraced. The blurred line between what's part of the enterprise and what's not has never been more unclear. The ways in which firewall administrators assume a level of security or a zone of trust are often rooted in security hardening philosophies from the early 2000s. User laptops, phones, and wireless access points are all implicitly placed in a zone of trust based solely on their physical locality to the network. This results in a level of trust being given to devices of which the enterprise administrator has no control. The countless number of devices that are introduced into modern networks make for ever-increasing challenges for policing and control.

Virtualization has also had an unexpected side effect of making security operations more difficult. The transitory nature of a lot of virtual machines makes doing any routine security audits difficult, if not constantly outdated. Movement and workload shifts within the virtual environment can spell disaster should a host become infected and security controls not dynamically shifted with the virtual environment. Synergies between security controls and virtualized environments can help mitigate those risks.

These few example cases offer a sample of the attack surfaces that modern networks face. While most modern networks appear with a generally similar set of tools protecting their edge, internal networks are much more varied in components and operation—rendering the implementation of security tools more complex and often times less effective. These are clear indicators that the Internet edge is no longer the only place that needs to be secured.

Infrastructure Reality

There is always a great difference between security in theory and security in practice. This isn't to say that there are no tools and mechanisms that can be put in place to limit exposure, or processes that can be enacted to reduce the attack surface. For cloud services, one can manage which SaaS providers are supported and find ways of improving the visibility of what goes in and out. BYOD can be managed with on-box agents, network access control, and corporate policies. Virtualization is a tougher nut to crack, not just because it's virtual, but because of who maintains it. A virtual host can be secured much in the same way a physical host is, but teams responsible for virtual environment management need to consider security as a forefront item of importance. Virtual environments can be transitory, and this makes it harder to clean an infected virtual host because malicious code can re-emerge suddenly in an unexpected part of the network.

Theoretically, many of these problems can be addressed; in reality, it's not always practical or even possible to do so. Tactically addressing security issues with point products and/or patchwork solutions often results in operational complexity. Upgrade cycles can become convoluted and ripple through multiple components due to interoperability dependencies—even requiring updates to every piece of the infrastructure. Last and most important, the end goal of every enterprise running a business—making a theoretical "best" the enemy of the "good" can disrupt core operations indefinitely.

Another truth that should be acknowledged concerns operating systems. It's a security best practice to keep the network operating system up to date with all of the latest security patches. Enterprises know this, but there are times when this simple practice can become difficult or even impossible.

The enterprise resource planning (ERP) system can be one of the most business critical systems to maintain. It's composed of many components and uses a number of protocols (both open and proprietary) to do its job. There will be supported OS versions for each of the components, but not all of them are the same. There may be different underlying software stacks that are fully integrated within each component.

When a new security vulnerability is discovered, there can often be an OS-level patch or even an application patch that addresses the problem. But the new OS patch may not be supported yet by various ERP components or IT may not have the ability to update the component's underlying software to the latest release. For example, perhaps the new OS version

for one component is incompatible with another component. These kinds of very common conundrums can lead to a choice between living with a known but unaddressed security flaw in a mission critical system or having that system break altogether.

"Performance versus cost" has been another reality that enterprises must face. LAN speeds found on the internal side of the network are orders of magnitudes higher than those at the edge. To keep up with higher traffic rates on the LAN, many enterprises choose speed over security. Until now, enterprise networks have not been able to seriously consider internal segments as a viable place to put any stateful security device. Even in the cases that offered the possibility, a compromise was always required that reduced security functionality to increase speed. Furthermore, the cost of a device that could simultaneously meet security, control, and speed requirements would typically be out of reach for most enterprises. Fortinet now provides secure, cost-effective, and high performing security devices that are a perfect fit for this kind of enterprise-class internal network security.

Security can be achieved with different mechanisms. Visibility tools notify you of incidents so that action can be taken. Controls help you stop insecure behaviors before they start. Mitigation provides clean-up after something happens. Enterprises often make specific choices where they want to focus efforts, but a maximum level of all three would be the ideal solution. But even that core security balance must be weighed against the operational needs of running a business.

Internal Segmentation Firewall

Segmentation is not new, but effective segmentation has not been practical. In the past, performance, price, and effort were all gating factors for implementing a good segmentation strategy. But this has not changed the desire for deeper and more prolific segmentation in the enterprise.

An edge or border firewall at the perimeter of the network is a security best practice. These devices historically have protected against known external threats. More and more, edge firewalls are looking deeper at a broader spectrum of relatively new threats that try to enter (or exit) networks at the edge. While it's still critical to have an optimum of security at the edge (and Fortinet delivers best-in-class products to do exactly that), security at the perimeter can only spot things that cross that threshold. In addition, the edge firewall is often not directly connected to end user network segments. Typically there is physical and logical separation required between user communities and core infrastructure (where edge firewalls typically reside). This poses a great challenge in trying to gain more visibility into what is going on inside a network.

While one might assume that the only way into the network is via the edge firewall, the reality is that there are many ingress and egress points on the network—and not all of them are governed by an edge firewall. Another assumption is that all attacks come from the outside. But in today's environment, an attack from the inside (knowingly or unknowingly) is almost as likely as one that originates from the outside.

With no other safeguards beyond perimeter protection in place, once something malicious has internal access to the network there is little to stop it from eventually making it to critical systems. Until recently, very little thought had been put into firewalling the internal network due to the aforementioned technical challenges.

Many networks have a large flat layer 2 (L2) infrastructure behind the firewall, where everyone is on one large network with little to no segmentation. This type of topology is typically not suited for introducing additional traditional layer 3 firewalls as there are no obvious segmentation points. In larger enterprise networks, there are often a few levels of layer 3 (L3) network segments, but still there are large L2 flat networks segments below. Most enterprises treat these different segments the same, often having no security between them, depending solely on the edge firewall to do the protection for the entire network.

The L3 portions of the network might have some existing security, but typically edge firewalls are where the largest investment in security happens. The L3 gateways provide a single point in which one internal network can gain access to another internal network. This is what's known as a North/South segment. These points are fairly easy to identify in an enterprise network and provide a natural location for segmentation.

The L2 portions of the network almost never have any security associated with them. Unlike the L3 portions of the network, there is often no obvious single point in which one part of the L2 network talks to another part of the L2 network. These portions are normally large aggregation switches designed for speed. The switches themselves don't include any places for easy internal segmentation, but some segmentation can be done between different L2 switches on a network. These locations for placing some controls within an L2 network are called East/West segments. Once an intruder makes it into one of these

areas, then everything within that area is wide open for probing and attack. These are the places where attackers are most likely to display malicious behavior out in the open because traditionally no one is watching there.

An internal segmentation firewall is designed to sit between two or more points on the internal network to allow visibility, control, and mitigation of traffic between those segments. The ISFW can handle traditional North/South segmentation as well as emerging East/West segmentation. Because of where it's placed in the network, ISFWs can focus on looking at and detecting things that are traversing the internal portions of the enterprise network. Different levels of visibility, control, and mitigation can be utilized in multiple places within the network. Similar to an edge firewall, not all ISFW policies require the same level of inspection. The ability to put the security where you want it, when you want it is one of the greatest benefits of an ISFW.

An internal segmentation firewall can be planned into the network from the very beginning. Being positioned as the North/South gateway between different L3 IP blocks is a perfect place to have security since this is where some segmentation has already been done in enterprise networks. North/South segmentation follows these logical network boundaries. Where the network is divided often reflects organizational separations within the enterprise, which offers an ideal location for increased visibility, control, and mitigation.

It's common for different departments within an enterprise to be placed on different L3 segments—examples of this could be the company's CFO or a guest on the network. While both of these users require extra levels of security, they should not be treated the same. The CFO is likely to need critical systems access to deal with the company's finance—so providing and securing that access is a large task. The guest on the other hand is a non-trusted source, and therefore should be given no critical system access. In fact, even more security should be applied to this kind of traffic because it is untrusted. Both of these users can be secured with an ISFW at the North/South segment for the L3 guest network and the L3 executive network.

However not all segments follow standard network boundaries. In many cases there are devices on the network that have some differentiated security needs which happen to be in the same network boundary. This is the emerging East/West segmentation. Hosts in the same network boundary sometimes need additional visibility and control. Historically, this could be accomplished with an end point solution but unfortunately not all endpoints can use this approach. The common element is the network—and an ISFW offers the option of placing it in between those endpoints.

In this situation, IT may have an L2 segment for much of the server infrastructure, but the duties of each of the servers varies. It may be the case that CRM server requires access to an internal database machine, but the help desk system does not. Because the L2 segment has no singular gateway between these three assets, a set of East/West segments need to be created within the L2 segment. An ISFW can provide this level of separation and security for these different critical end points.

Having an ISFW that sits in the middle of the network as a L3 gateway or bump on the wire enables enterprises to monitor different users, give them the access to critical systems they require, or keep them from accessing things they should not. Even critical systems on the network often will benefit from individual protection between each other. A single ISFW can be configured to handle all of these segments, but because of the very nature of multiple segments, multiple ISFWs can also be deployed to spread the load and scale individual segments as necessary.

A Fortinet ISFW can apply security best practices throughout a network. Fortinet provides a best-of-breed security solution that delivers the features, performance, and cost that makes internal segmentation protection a reality for today's enterprise networks.

The concept of "least privilege" is an old one—only providing the access people need and nothing more. It's a great idea in theory, but it can be very tough to enforce. By having an ISFW at various points within the network, an enterprise gives itself extra layers of protection from various attack vectors. This in turn enables not only visibility within the network, but also the enforcement that allows "least privilege" to be effective.

With a default transparent mode, Fortinet's ISFW solution can be rapidly deployed into existing environments with minimal disruption, while keeping up the multi-gigabit speeds of internal networks. Fortinet ISFWs deliver intelligent, adaptive, and advanced threat protection from the inside out, thereby shortening the window of exposure and limiting potential damage.

Fortinet ISFWs supplement existing NGFW edge deployments by providing enhanced visibility throughout the internal network. As hackers attempt to locate assets and data of value, spreading internally from a compromised host to other hosts, a Fortinet ISFW will segment the internal network and restrict lateral movement and propagation of malicious code. This complementary approach applies seamless, comprehensive security to the entire attack surface—a consistent threat posture, end-to-end across the network.

From visibility components like Application Control, FortiView, and the proven threat intelligence of FortiGuard, one can increase awareness of what's going through the network. User authentication, traffic shaping, and even high-speed security policies control user access to only what's required. The Fortinet ISFW can mitigate incidents by using network quarantining, actionable security, and complete logging and auditing.

Architecture Overview

In this architecture, the focus is on security behind the edge firewall and in front of any endpoint protection that may be in place. An ISFW does not replace the edge firewall, just as it does not replace the end point protection. Instead, a single ISFW or multiple ISFWs provide multiple touch points within a network that provide security between existing network boundaries or by creating entirely new segments inside of existing network boundaries.

Depending on the security required between each of these segments, the types of protection enabled will vary. When requiring the highest levels of performance, L4 firewall policies would apply. When requiring the highest levels of security, the full deep inspection feature set can be enabled. These features can mix and match to provide the exact levels of security required for the specific enterprise environment.

In a full ISFW deployment, all of the North/South areas would segment at the logical network boundaries. For today's enterprise networks, this would be at each L3 gateway. An ISFW can act as this gateway and perform any of the functions that a traditional L3 device (such as a router or L3 switch) can do, but with the added benefits of visibility, control, and mitigation.

Emerging East/West boundaries would segment in front of or between the items of critical importance. This would entail placing an ISFW in front of a host via transparent mode or in between hosts by placing it between two L2 switches on the same segment.

Virtual infrastructures can cause particular challenges because the East/West boundaries are on a virtual switch inside the main hypervisor. To insert an ISFW there would require bringing those internal virtual switch connections out of the virtual infrastructure to a physical ISFW and then back in again. Another option would be to use an ISFW that is hypervisor-aware and therefore interoperable within the hypervisor itself. Fortinet has a hypervisor aware VM version of the FortiGate that can be used within a virtual environment.

Each area of importance requires its own segment. Deciding how to divide up the duties of the segmentation inside a single or multiple ISFWs depends on a number of factors:

- How much performance does each set of segments require?
- What is the physical proximity of the aggregation points?
- Are there different assets within an L2 network that require different levels of visibility or security?

Ecosystem Connectivity

An ISFW is a boon to any enterprise, but it does not (and should not) operate in a vacuum. There are a number of other pieces that can make any ISFW deployment better.

Threat intelligence is one very important example. The security efficacy of your ISFW directly correlates to the quality of the threat intelligence powering it. Threat intelligence keeps the ISFW current on today's advanced persistent threats—allowing it to view and detect threats, put policies in place to block those threats, and to perform some level of mitigation of it if they've already made it onto the network.

FortiGuard Labs delivers the most advanced threat intelligence available, with independently validated 97%+ breach detection. FortiGuard takes information from global sources, using analytics and machine learning to turn big data into near real-time updates for Fortinet appliances—assuring some of the fastest response times in the industry to new vulnerabilities, attacks, viruses, botnets, and zero-day exploits.

The ability to hand off potential threats for deeper analysis allows the ISFW to continue performing its main task without compromise, to tap into specific analysis with the same controls in place for dealing with threats.

FortiSandbox is a key part of Fortinet's integrated and automated advanced threat protection. FortiSandbox detects and analyzes advanced attacks designed to bypass traditional security defenses. In independent NSS Labs testing, FortiSandbox demonstrated 97.3% Breach Detection effectiveness. With Fortinet's unique, multi-layered sandbox analysis approach, FortiSandbox detects the majority of threats within one minute.

With more security enforcement points within the network, device management, as well as policy management becomes more critical. Fortunately, Fortinet's enterprise management solution can scale to thousands of devices with tens of thousands of policies. Additional security does not need to mean exponential operational costs.

FortiManager network security management appliances provide security management for large enterprise organizations and service providers. They enable centralized management for any number of Fortinet devices. In addition, FortiAnalyzer network security logging, analysis, and reporting appliances securely aggregate log data from Fortinet devices. It delivers a comprehensive suite of easily customable reports, allowing quick analysis and visualization of network threats, inefficiencies, and usage.

Lastly, integration with third-party components is a must. As previously mentioned, the ISFW covers the area behind the edge firewall and in front of the end point protection, but that doesn't mean it shouldn't cooperate with those pieces to provide a full, end-to-end solution for the enterprise.

Fortinet has joined the VMware NSX™ partner ecosystem to provide advanced security and layered defense through segmentation in VMware NSX-enabled data centers. Integration of Fortinet's FortiGate with Cisco's Application Centric Infrastructure (ACI) offers enterprises high levels of Software Defined Networking (SDN) security, privacy and compliance in cloud and data center environments.

Internal Segmentation Assessment

Some of the use cases for the ISFW are obvious. But if additional justification is required, this list of questions can help determine an enterprise's particular needs.

The first questions to ask start with: Can I see what's going on in my network? Not just what's going in and out of the edge, but also what servers are being accessed and by whom? Are they critical? What protocols are going over my network—and should they be?

With those answers in hand, the next questions to ask include: How can I stop a particular user from accessing certain material? How would I limit bandwidth for unknown protocols on my network? Can I be sure that my CFO is protected from having our financial data accidentally leaked out?

And then come the hard questions that no one wants to ask: What will I do if there's some sort of malicious traffic on my network? How can I isolate an attacker to just one low criticality segment? Can I track an infected host and evaluate if other hosts have been compromised as well?

If any of these questions can't be answered, then the visibility, control, and mitigation provided by an internal segmentation firewall is needed. Fortinet can provide companies with a similar detailed assessment through its Cyber Threat Assessment Program (CTAP). This program offers a quick, easy, and comprehensive test where a FortiGate is non-intrusively placed into an enterprise's network to monitor and report what's going on.

At the end of the data collection period, a detailed Risk Assessment Report is generated with analysis of the application traffic, user productivity, network utilization, the overall security risk, and the related business risk—as well as detailed, actionable mitigation recommendations. CTAP is part of a broader effort by Fortinet and its FortiGuard Labs threat research team, and a number of key partners to provide customers with greater insight into dynamically changing cyber risks that threaten their businesses.

ISFW Reference Architecture

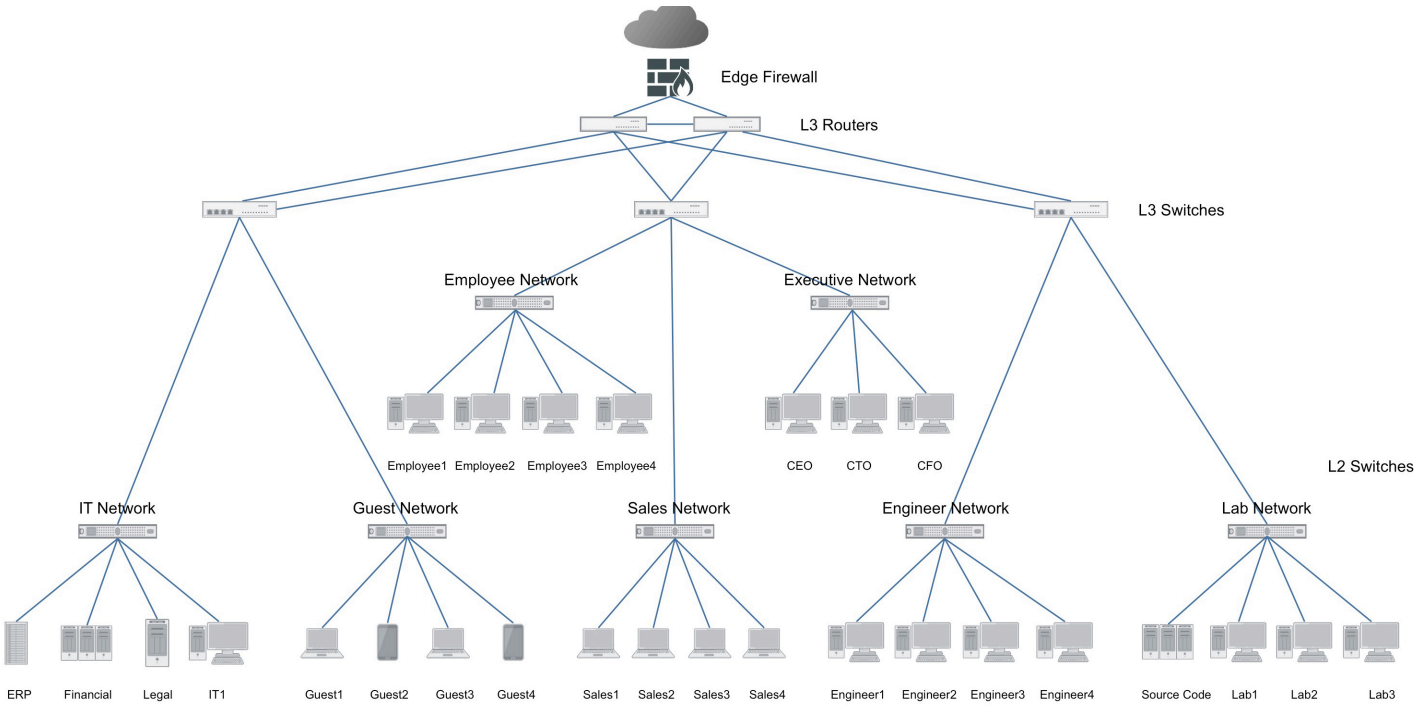


Figure 1

Figure 1 diagram represents a medium-sized enterprise network. It includes an edge firewall to secure the Internet and VPN connectivity. This edge firewall could be a Next Generation Firewall (NGFW) with advanced capabilities such as inspecting traffic going out to the Internet, as well as traffic coming back from it. Behind the edge firewall sits two core L3 routers which are connected via a full mesh to the L3 aggregation switches. From there, a number of L2 switches are situated in the wiring closet for different organizations of the enterprise. Below that are a number of endpoints, both wired and wireless devices.

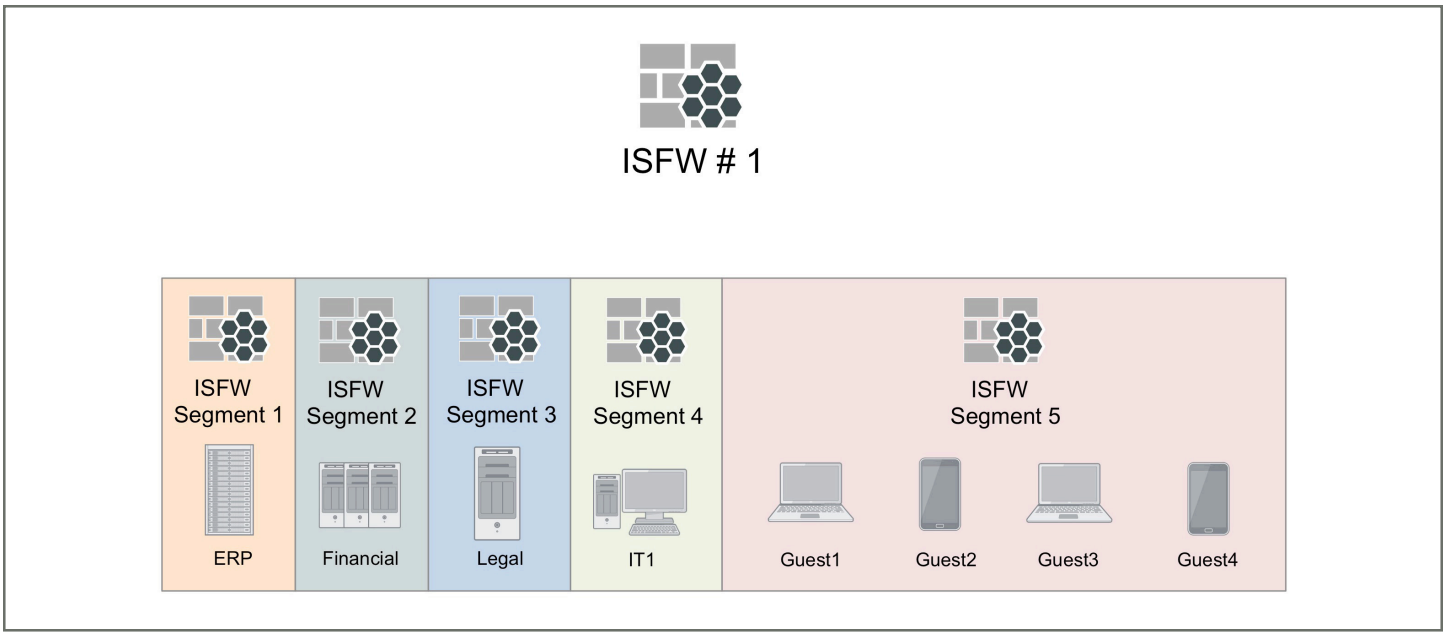
The IT and Guest networks come off of the first L3 switch. The second switch includes the General Employee, Sales, and Executive Networks. The third L3 switch supports the Engineering and Lab Networks. Each of these networks has an L2 switch and number of endpoints, but not all of them have equivalent security requirements. There are times when IT will want to segment by department (HR, Sales). There are times when they will want to segment by function (Engineering, Lab). They can also segment based upon the role (ERP server, Fiance server, CEO, CFO).

The North/South segments can be secured by partitioning them at the L3 switches. This allows for visibility, control, and mitigation between all of the different networks. This is an improvement from what was previously in place, where security was only present at the edge. But, not all devices in each network are equal.

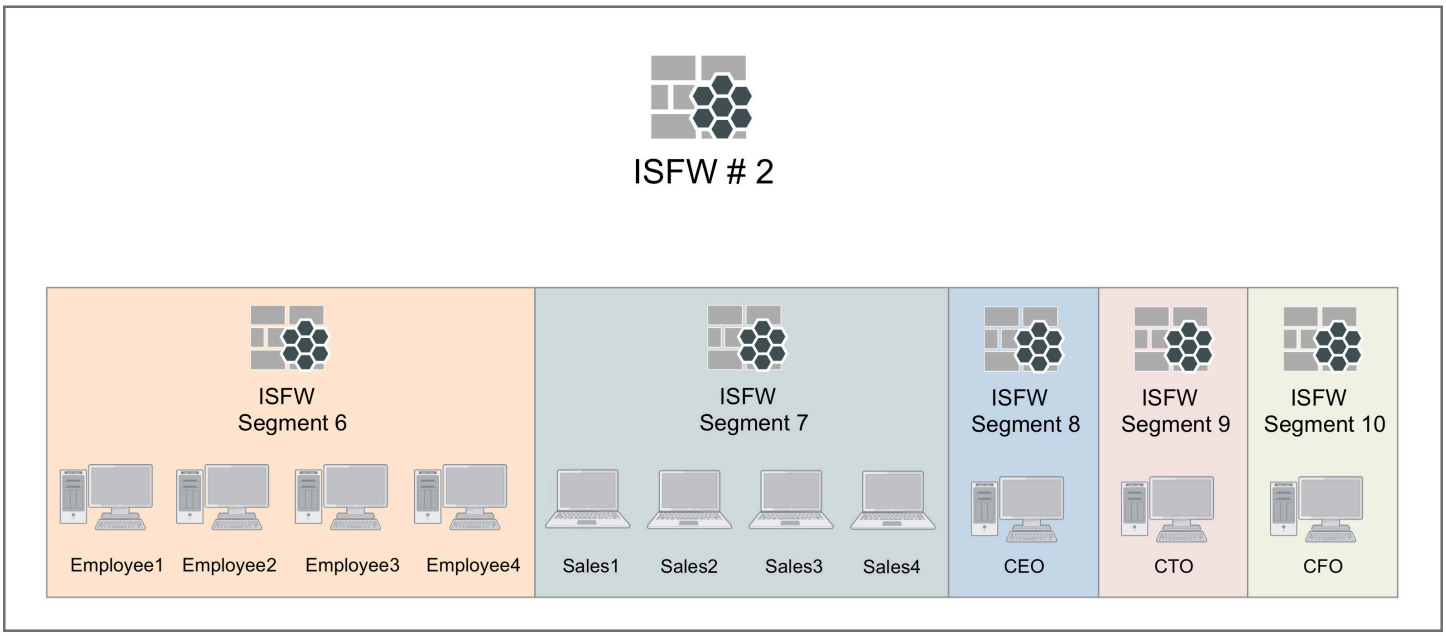
Certainly the ERP, Financial, and Legal servers should not only have greater security importance than an internal portal server on the IT network, but they should also be secure from each other. Similarly, various executives will often require additional access as well as increased security due to the nature of the information they access. A source code repository in the Lab Network is another place that just requires additional security.

Adding East/West security to these devices will secure them even further through the inclusion of a new point where an ISFW can perform its duties. Having visibility into whether the Financial and Legal servers are communicating over the network and what they might be sending can be highly useful. Creating new segments of security adds layers of visibility, control, and mitigation points throughout the enterprise.

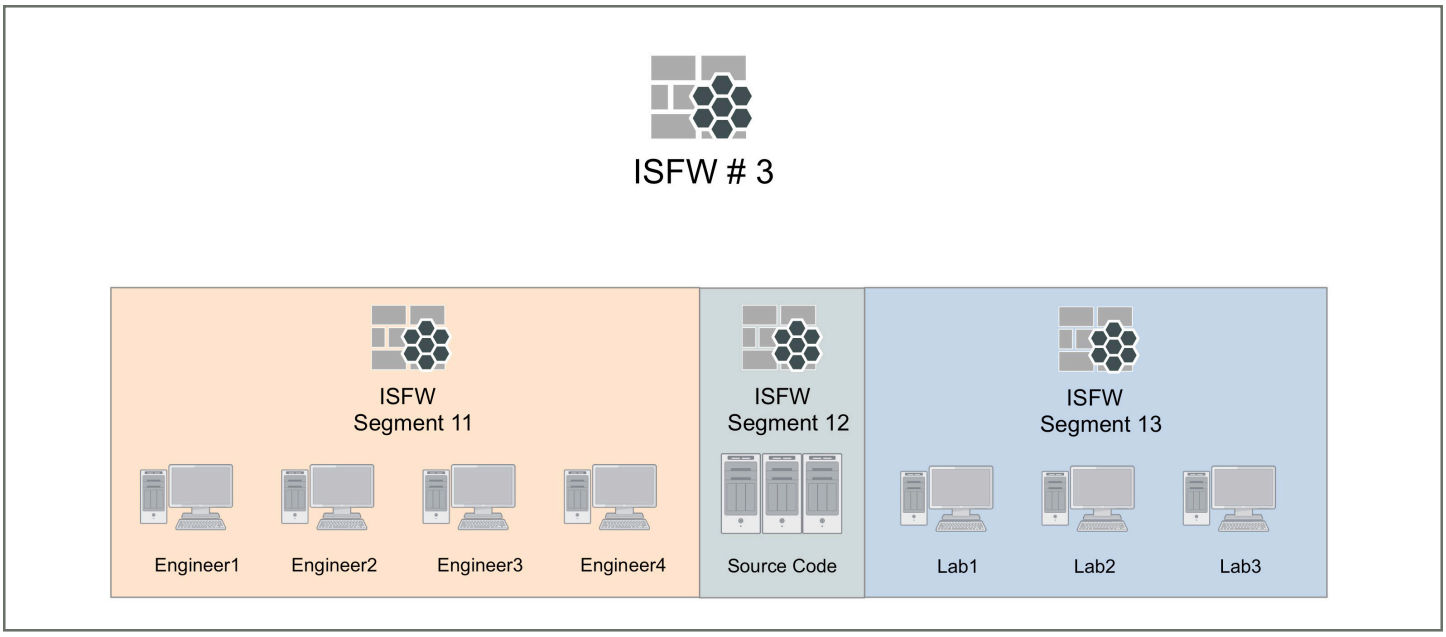
In the network below, three physical ISFWs have replaced the L3 switches. ISFW #1 handles the IT and Guest networks, ISFW #2 handles the Employee, Sales, and Executive networks. ISFW #3 is dedicated to the Engineering and Lab networks. Each network is further subdivided into different L2 secure segments.



ISFW #1 includes five segments. What was previously the IT network has now been divided into four parts. The ERP, Financial, and Legal servers each have their own segments. Each of these critical assets has a set of individual security policies.The rest of the IT network is on its own segment, but still has visibility, control, and mitigation available at the L3 North/South border. The fifth segment is for the Guest network, which is secured and separated from the other networks and segments.



ISFW #2 provides security for the Employee, Sales, and Executive networks utilizing five ISFW segments. The general employee network and sales network each has a dedicated segment. If, for example, a sales person walks in with their laptop fresh from some hotel or other outside network location, that ISFW segment can immediately see any potential threats brought in, control access to critical resources, and mitigate any problems that are found. For the executive network, a separate ISFW segment is dedicated to each of the three main executives (CEO, CTO, and CFO). Each can have individualized security tailored to his or her particular access needs.



ISFW #3 is dedicated to the Engineering and Lab networks. Because of the high-speed access required by these two networks, Engineering has its own segment; for the most part, the Lab does as well. Both of these are segmented at the North/ South border. But within the Lab network is a source code repository server containing the company's intellectual property, which requires the highest levels of protection. Therefore, this server gets its own dedicated segment inside this ISFW to provide visibility into threats and to audit access. It also controls users, groups, and appropriate applications and has the ability to mitigate threats from both inside and outside the segment.

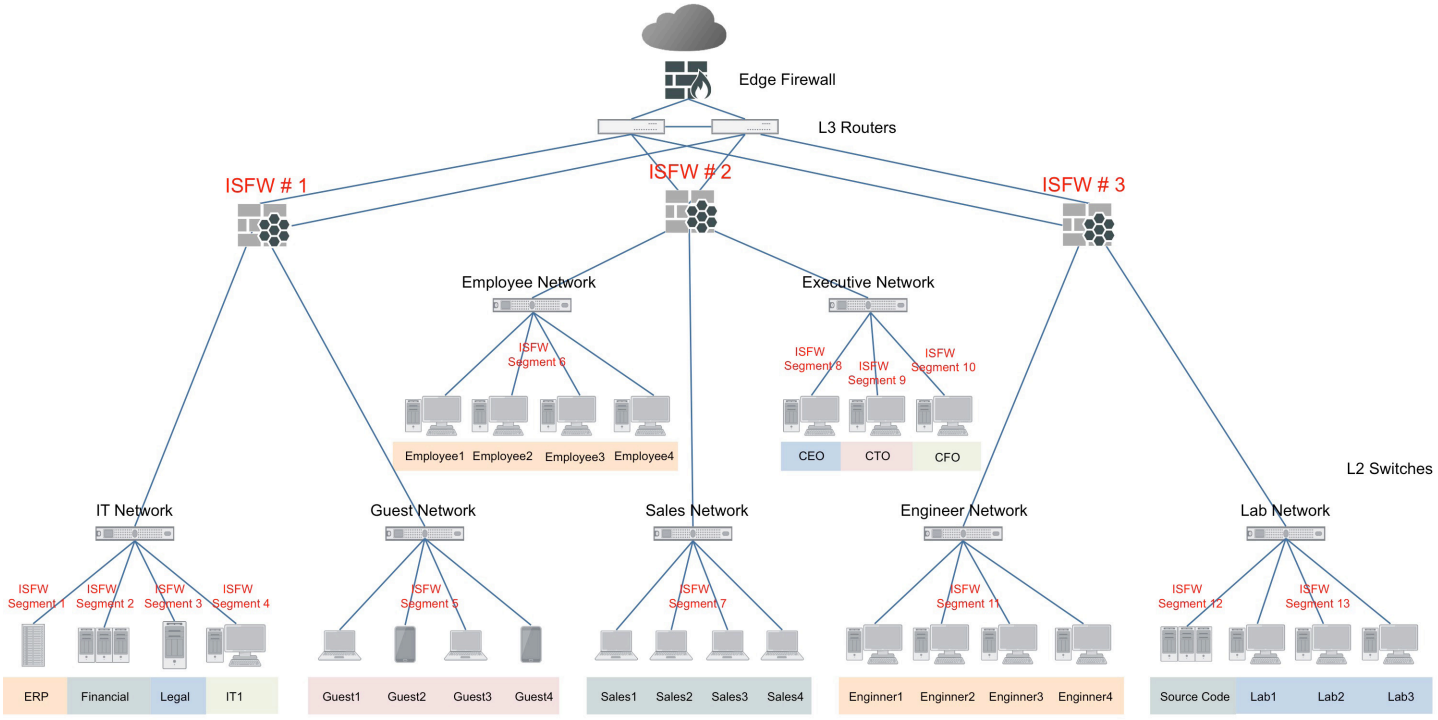
Conclusion

We know from experience that edge firewalls only have the possibility of preventing attacks from the outside. Once a threat makes it inside, very little can stop it from reaching every part of the enterprise. By reducing the attack surface, placing more secure areas, and moving away from a flat network, the addition of ISFWs to the network has increased visibility, control, and mitigation capabilities—making the enterprise much more resilient to today's threats.

With all of these different Fortinet ISFWs providing internal network security, having centralized enterprise management of all of these devices will help provide easy administration, cohesive policy, and streamlined operations of the entire security infrastructure. With an ISFW architecture, the entirety of your network can be secured and not just the edge.

Layering on additional security points utilizing a FortiSandbox for advanced threat protection and FortiMail for spam filtering can help fill out a robust enterprise security strategy. Integrating various authentication points and audit servers can provide a wide range of access, as well as deep analytic understanding of what's happening on an enterprise network.

Fortinet's ISFW architecture delivers maximum performance and maximum security, while still offering the flexibility of being placed anywhere in the enterprise. Having more security enforcement points within the network is now a practical reality for any enterprise network, and deploying them has never been easier.



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Dec 05, 2016