FORTINET

PROTECTING YOUR NETWORK FROM THE INSIDE-OUT

Internal Segmentation Firewall (ISFW)

WHITE PAPER

PROTECTING YOUR NETWORK FROM THE INSIDE-OUT

Internal Segmentation Firewall (ISFW)

TABLE OF CONTENTS

SUMMARY

For the last decade organizations have been trying to protect their networks by building defenses across the borders of their networks. This includes the Internet edge, perimeter, endpoint, and data center (including the DMZ). This "outside-in" approach has been based on the concept that companies can control clearly defined points of entry and secure their valuable assets. The strategy was to build a border defense as strong as possible and assume nothing got past the firewall.

As organizations grow and embrace the latest IT technology such as mobility and cloud the traditional network boundaries are becoming increasingly complex to control and secure. There are now many different ways into an enterprise network.

Not long ago, firewall vendors marked the ports on their appliances "External" (untrusted) and "Internal" (trusted). However, advanced threats use this to their advantage because, once inside, the network is very flat and open. The inside of the network usually consists of non security-aware devices such as switches, routers, and even bridges. So once you gain access to the network as a hacker, contractor, or even rogue employee, then you get free access to the entire enterprise network including all the valuable assets.

The solution is a new class of firewall – Internal Segmentation Firewall (ISFW), that sits at strategic points of the internal network. It may sit in front of specific servers that contain valuable intellectual property or a set of user devices or web applications sitting in the cloud.

Once in place, the ISFW must provide instant "visibility" to traffic traversing into and out of that specific network asset. This visibility is needed instantly, without months of network planning and deployment.

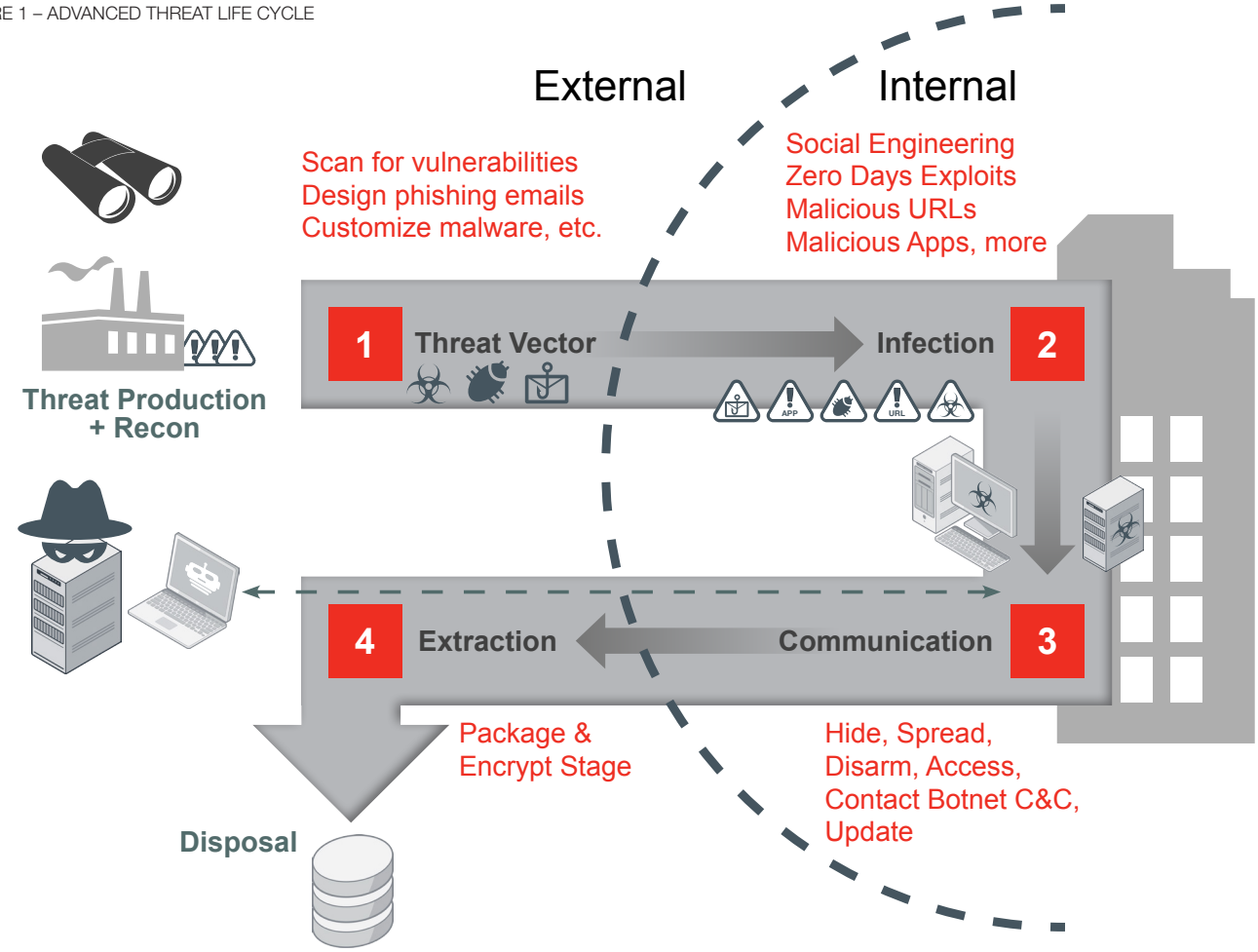
Most importantly the ISFW must also provide "protection" because detection is only a part of the solution. Sifting through logs and alerts can take weeks or months. The ISFW needs to deliver proactive segmentation and real-time protection based on the latest security updates.

Finally, the ISFW must be flexible enough to be placed anywhere within the internal network and integrate with other parts of the enterprise security solution under a single pane of management glass. Other security solutions can also provide additional visibility and protection. This includes the email gateway, web gateway, border firewalls, cloud firewalls, and endpoints. Further, Internal Segmentation Firewalls need to scale from low to high throughputs allowing deployment across the global network.

KEY REQUIREMENTS

- **COMPLETE PROTECTION** – Continuous inside-out protection against advanced threats with a single security infrastructure
- **EASY DEPLOYMENT** – Default Transparent Mode means no need to re-architect the network and centrally deployed and managed
- **HIGH PERFORMANCE** – Multi-gigabit performance supports wire speed east-west traffic

FIGURE 1 – ADVANCED THREAT LIFE CYCLE



INTERNAL NETWORK

Cybercriminals are creating customized attacks to evade traditional defenses, and once inside, to avoid detection and enable egress of valuable data. Once inside the network there are few systems in place to detect or better still protect against APTs.

It can be seen from the threat life cycle in Figure 1 that once the perimeter border is penetrated, the majority of the activity takes place inside the boundary of the network. Activities include disabling any agent-based security, updates from the botnet command, and control system, additional infection/recruitment and extraction of the targeted assets.

THE ANSWER IS A NEW CLASS OF FIREWALL – INTERNAL SEGMENTATION FIREWALL (ISFW)

Most firewall development over the past decade has been focused on the border, the Internet edge, perimeter (host firewall), endpoint, data center (DMZ), or the cloud. This started with the stateful firewall but has evolved to include Unified Threat Management (UTM) for distributed networks, which brought together the firewall, intrusion detection, and antivirus. Later came the Next Generation Firewall (NGFW), which included intrusion prevention and application control for the Internet edge. More recently because of the huge increase in speeds, Data Center Firewalls (DCFW) have arrived to provide more than 100 Gbps of throughput. All of these firewalls have in common an approach designed to protect from the "outside-in."

For rapid internal deployment and protection, a new class of firewall is required – Internal Segmentation Firewall (ISFW). The Internal Segmentation Firewall has some different characteristics when compared to a border firewall. The differences are laid out in figure 2.

FIGURE 2 – FIREWALL TYPE DIFFERENCES

Deployment Mode	ISFW	NGFW	DCFW	UTM	CCFW
Purpose	Visibility & protection for internal segments	Visibility & protection against external threats and internet activities	High performance, low latency network aprotection	Visibility & protection against external threats and user activities	Network security for Service Providers
Location	Access Layer	Internet Gateway	Core Layer/DC Gateway	Internet Gateway	Various
Network Operation Mode	Transparent Mode	NAT/Route Mode	NAT/Route Mode	NAT/Route Mode	NAT/Route Mode
Hardware Requirements	Higher port density to protect multiple assets	GbE and 10GbE ports	High speed (GbE/10 GbE/40 GbE/100) & high port density, hardware acceleration	High GbE port density, integrated wireless connectivity and POE	High speed (GbE/10 GbE/40 GbE) & high port density, hardware acceleration
Security Components	Firewall, IPS, ATP, Application Control	(User-based) Firewall, VPN, IPS, Application Control	Firewall, DDoS protection	Comprehensive and extensible, client and device integration	Firewall, CGN, LTE & mobile security
Other Characteristics	Rapid Deployment – near zero configuration	Integration with Advanced Threat Protection (Sandbox)	High Availability	Different WAN Connectivity Options such as 3G4G	High Availability

THE ISFW NEEDS TO PROVIDE COMPLETE PROTECTION

The first element of security is visibility. And visibility is only as good as network packet knowledge. What does a packet stream look like for a specific application, where did it come from, where is it going, even what actions are being taken (download, upload…).

The second and equally important element is protection. Is the application, content or actions malicious? Should this type of traffic be communicating from this set of assets to another set of assets? While this is very difficult across different content and application types, it is an essential part of the ISFW. The ability to detect a malicious file, application, or exploit gives an enterprise time to react and contain the threat. All of these protection elements must be on a single device to be effective.

Both visibility and protection are heavily reliant on a real-time central security threat intelligence service. A question that always needs to be posed – how good is the visibility and protection? Is it keeping up with the latest threats? That's why all security services should be measured on a constant basis with 3rd party test and certification services.

THE ISFW NEEDS TO PROVIDE EASY DEPLOYMENT

The ISFW must be easy to deploy and manage. Keeping it simple for IT means being able to deploy with minimum configuration requirements and without having to re-architect the existing network.

The ISFW must also be able to protect different types of internal assets placed at different parts of the network. It could be a set of servers containing valuable customer information or a set of endpoint devices that may not be able to be updated with the latest security protection.

Additionally, the ISFW must be able to integrate with other parts of the enterprise security solution. Other security solutions can also provide additional visibility and protection. This includes the email gateway, web gateway, border firewalls, cloud firewalls, and endpoints. This all needs to be managed with a 'single pane of glass' approach. This allows security policies to be consistent at the border, inside the network, and even outside the network in clouds.

Traditional firewalls are usually deployed in routing mode. Interfaces (ports) are well defined with IP addresses. This often takes months of planning and deployment. This is valuable time in today's instant cyber attack world. An ISFW can be deployed in the network rapidly and with minimum disruption. It must be as simple as powering on a device and connecting. It must be transparent to the network and application.

THE ISFW NEEDS TO PROVIDE WIRE-SPEED PERFORMANCE

Because internal segmentation firewalls are deployed in-line for network zoning, they must be very high performance in order to meet the demands of internal or "east-west" traffic, and to ensure they do not become a bottleneck at these critical points. Unlike firewalls at the border that deal with Wide Area Network (WAN) access or Internet speeds of less than 1 gigabit per second, internal networks run much faster – multi-gigabit speeds. There, ISFWs need to operate at multi-gigabit speeds and be able to provide deep packet/connect inspection without slowing down the network.

ISFW TECHNOLOGY REQUIREMENTS

A FLEXIBLE NETWORK OPERATING SYSTEM

Almost all firewall "deployment modes" require IP allocation and reconfiguration of the network. This is known as network routing deployment and provides traffic visibility and threat prevention capabilities. At the other end of the spectrum is sniffer mode, which is easier to configure and provides visibility, but does not provide protection.

Transparent mode combines the advantages of network routing and sniffer modes. It provides rapid deployment and visibility plus, more importantly, protection. The differences are summarized in Figure 3.

FIGURE 3 – FIREWALL TYPE DIFFERENCES

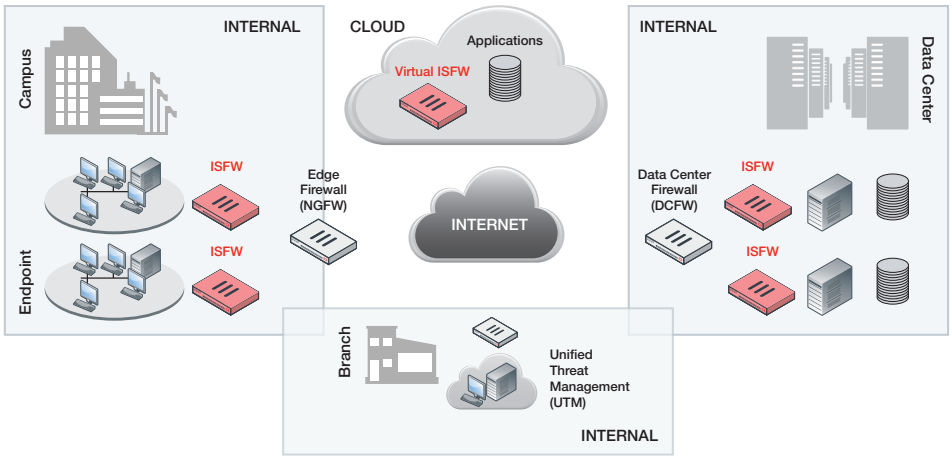
Deployment Mode	Deployment Complexity	Network Functions	High Availability	Traffic Visibility	Threat Protection
Network Routing	High	L3-Routing	✔	✔	✔
Transparent	Low	L2-Bridge	✔	✔	✔
Sniffer	Low	X	X	✔	X

A SCALABLE HARDWARE ARCHITECTURE

Because internal networks run at much higher speeds the ISFW needs to be architected for multi-gigabit protection throughput. Although CPU-only based architectures are flexible they become bottlenecks when high throughput is required. The superior architecture still uses a CPU for flexibility but adds custom ASICs to accelerate network traffic and content inspection.

Because the ISFW is deployed in closer proximity to the data and devices, it may sometimes need to cope with harsher environments. Availability of a more ruggedized form factor is therefore another requirement of ISFWs.

FIGURE 4 – Internal Segmentation Firewall - ISFW DEPLOYMENT (ISFW) DEPLOYMENT



NETWORK SEGMENTATION – HIGH SPEED INTEGRATED SWITCHING

An evolving aspect of transparent mode is the ability to physically separate subnetworks and servers via a switch.

Firewalls are starting to appear on the market with fully functional, integrated switches within the appliance. These new firewalls, with many 10 GbE port interfaces, become an ideal data center "top-of-rack" solution, allowing servers to be physically and virtually secured. Also, similar switch-integrated firewalls with a high density of 1 GbE port interfaces become ideal for separation of LAN subsegments. ISFWs should be able to fulfill both of these roles, and as such should ideally have fully functional, integrated switching capabilities.

REAL-TIME SECURITY

Internal Segmentation Firewalls must be able to deliver a full spectrum of advanced security services, including IPS, application visibility, antivirus, anti-spam, and integration with cloud-based sandboxing, allowing for the enforcement of policies that complement standard border firewalls. This real-time visibility and protection is critical to limiting the spread of malware inside the network.

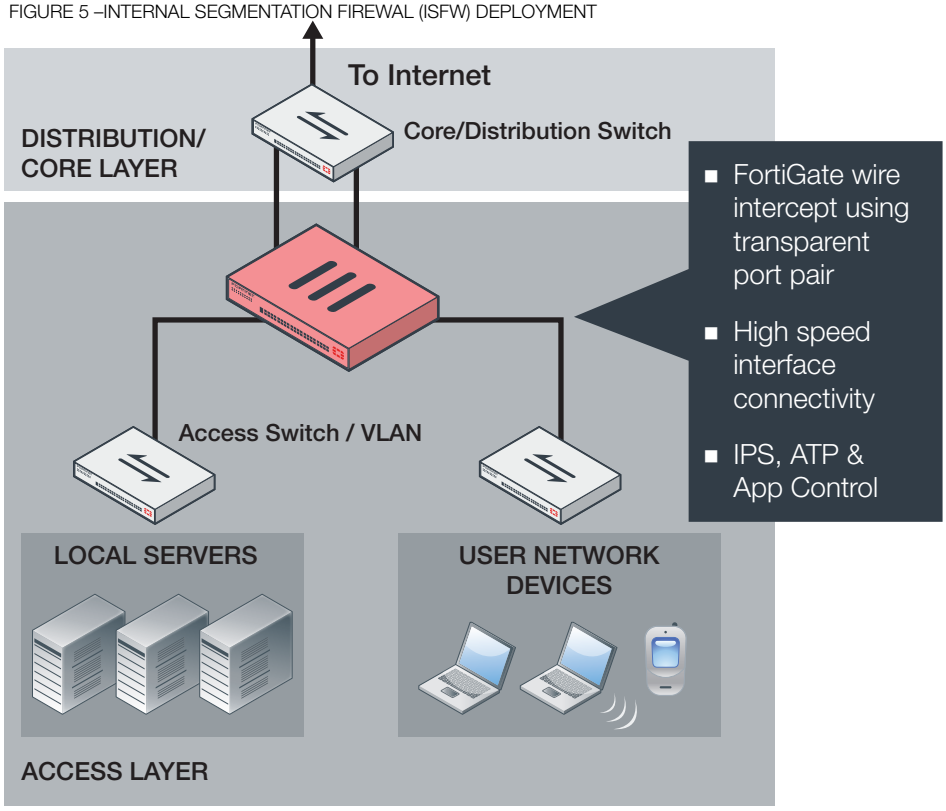
NETWORK WIDE ISFW DEPLOYMENT EXAMPLE

Most companies have set up border protection with firewalls, NGFWs, and UTMs. These are still critical parts of network protection. However, to increase security posture, Internal Segmentation Firewalls can be placed strategically internally. This could be a specific set of endpoints where it is hard to update security or servers where intellectual property is stored.

SEGMENT ISFW DEPLOYMENT EXAMPLE

The ISFW is usually deployed in the access layer and protects a specific set of assets. Initially the deployment is transparent between the distribution and access switches. Longer term the integrated switching could take the place of the access and distribution switch and provide additional physical protection.

FIGURE 5 –INTERNAL SEGMENTATION FIREWAL (ISFW) DEPLOYMENT



ENHANCING ADVANCED THREAT PROTECTION WITH INTERNAL VISIBILITY

A proper approach to mitigating advanced threats should include a continuous cycle of prevention, detection, and mitigation. Very typically a next-generation firewall would serve as a key foundation of the prevention component, enabling L2/L3 firewall, intrusion prevention, application control and more to block known threats, while passing high-risk unknown items to a sandbox for detection. But with NGFW's deployed traditionally at the network edge, this only provides partial visibility into the attack life cycle by primarily observing ingress and egress activity.

Deployment of an ISFW can provide more complete visibility into the additional internal activity of the hackers once they've compromised the edge. Lateral movement can account for a significant portion of the malicious activity as the hackers try to identify valuable assets and extract data, and having a complete picture of both internal and edge activity enhances all phases of a complete ATP framework. With internal network traffic often being several times the bandwidth of edge traffic, an ISFW can provide many more opportunities to limit the spread of the compromise from known techniques and more high-risk items to be passed to sandboxes for deeper inspection.

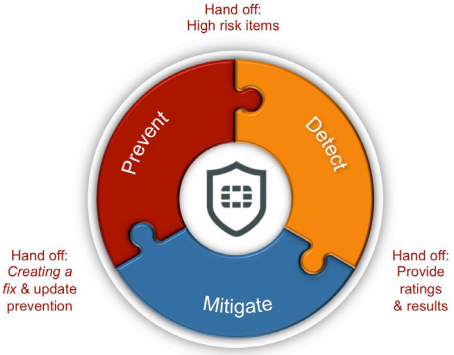


FIGURE 5 – ADVANCED THREAT PROTECTION (ATP) FRAMEWORK

CONCLUSION

Advanced Threats are taking advantage of the flat Internal network. Once through the border defense there is little to stop their spread and eventual extraction of valuable targeted assets. Because traditional firewalls have been architected to slower speeds of the Internet edge it's hard to deploy these security devices internally. And firewall network configuration deployments (IP addresses) take a long time to deploy.

Internal Segmentation Firewalls are a new class of firewall that can be deployed rapidly with minimum disruption while keeping up the multi-gigabit speeds of internal networks. Instant visibility and protection can be applied to specific parts of the internal network.

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

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

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

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

December 2016