FORTINET

SOLUTION GUIDE

ISFW Solution Guide

Introduction

Cyber attacks are on the rise. Breaches draw unwanted public attention, loss of reputation and customer confidence, and may result in heavy recovery costs for the enterprise. At the same time, as organizations embrace the latest technologies (BYOD, cloud-based apps, Internet of Things), traditional network boundaries are becoming increasingly difficult to control and secure.

Companies have been investing in perimeter security protection at different levels of the enterprise network – branches, campus and the data center – to prevent threats from entering their internal infrastructure. For the last decade, this has proven to be a valuable and effective strategy. In addition to firewalls at the network perimeter, purpose-build security solutions can provide application-level and multi-layered advanced persistent threat protection. Today's increasingly sophisticated attacks, however, are still able to penetrate the enterprise network in many cases. Once inside, exploits (such as malware) can remain hidden and dormant within the network for extended periods of time before launching opportunistic attacks.

Accepting the fact that some threats will penetrate the perimeter, an additional security layer needs to be added in the internal network—one that segments access to critical resources, provides next-generation security, offers greater visibility, and contains potential threats to mitigate breach damage.

Threats Visibility and Segmentation

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 solution will segment the internal network and restrict lateral movement and propagation of hackers and malicious code. This complementary approach applies seamless, comprehensive security to the entire attack surface—a consistent threat posture, end-to-end across the network.

The Challenges: Why the Era of Perimeter-Only Security is Over

Fact #1: The quantity, sophistication, and impact of threats are on the rise. In today's environment, access points to the enterprise network have multiplied exponentially. Mobility, smart devices, and the cloud all represent a growing attack surface through which an increasing number of sophisticated threats can enter the network.

Fact #2: The internal network is flat and open. To facilitate flexibility and agility, networks have become progressively more flat and open. Security implementation within the internal network is, in most cases, basic and limited to Virtual LANs and layer 4 access lists. Therefore, once beyond the security perimeter, hackers can easily spread and freely gain access to credentials, resources, and data. The lack of security infrastructure within the internal network also significantly limits the enterprise's visibility into suspicious traffic behaviors and data flows, which hinders the ability to detect a breach.

Fact #3 - Virtual LAN (VLAN) Segmentation is Just Not Enough - Traditionally, internal network segmentation has been done via VLANs deployment with intra-VLAN communication carried out by a routing function. VLAN segmentation may limit the spread of a simple threat to members within the same VLAN. However, more sophisticated threats can easily spread between VLAN as routers are not security appliances and do not have the security services and awareness required to effectively identify and block threats.

The VLAN segmentation model also has very limited scalability and can only support up to 4K VLANs, which inhibits the level of micro segmentation required in today's enterprise environments, which may contain thousands of servers and virtual machines.

The Solution: Internal Segmentation Firewalls

To help resolve the above challenges, enterprises can deploy a new class of firewall at strategic points within the internal network. Fortinet's Internal Segmentation Firewall (ISFW) solution offers an additional security layer to complement existing boundary protections with several unique benefits.

Benefit #1: Controls access to critical resources/assets as close as possible to the user via policy-driven segmentation

Benefit #2: Establishes security barriers to stop and limit the uncontrolled spread of threats and hacker activity within the internal network via the implementation of physical segmentation with advanced security mechanisms

Benefit #3: Limits the potential damage of threats inside the perimeter

Benefit #4: Increases threat visibility and enhances breach discovery and mitigation

Benefit #5: Strengthens the enterprise's overall security posture

To maximize threat control and potential damage limitation, the deployment of an ISFW relies on two foundations:

- Policy-driven firewall segmentation
- Physical & virtual firewall segmentation

Policy-driven Security Segmentation

The objective of policy-driven security segmentation is to control access to the network, applications, and resources by automatically associating each user's identity with security policies that limit the potential attack vectors and threats carried by the user.

A user's identity may be defined as a set of attributes, such as physical location, the type of device used to access the network, or the application used. The enforced security policy must automatically follow the user's identity as it dynamically changes in context. For example, a user may have different policies enforced based on the type of device used to access the network.

In order to achieve the required user identification and the overall parameters needed to create and enforce granular security policies, the ISFW must be able to:

1. Allow user, device, and application identification
2. Provide integration with the enterprise's directory services solution (such as Microsoft Active Directory) to dynamically identify users
3. Dynamically map each user's identity to a specific security policy and enforcement

The association of a user profile upon which a specific security policy will be enforced should happen as close as possible to the source or access point. Therefore, all firewalls deployed at the various levels of the organization—from the branch office to the campus/HQ—must have the ability to dynamically identify users and enforce the appropriate policies throughout the organization. In effect, the entire firewall infrastructure turns into an intelligent policy-driven segmentation fabric.

Physical & Virtual Security Segmentation

Policy-driven security segmentation also defines the security services applied by the firewall, such as AV, IPS, and Application Control. No matter how efficient these may be, an unknown threat may still enter the network. Physical security segmentation must be put in place to maximize detection and protection to limit a threat's spread within the internal network. The need for physical security segmentation is driven by the severe damage potential that breaches carry, plus growing adoption of the "zero-trust" concept.

A physical and/or virtual ISFW provides security segmentation and micro-segmentation of assets, users and resources residing within the enterprise network via the deployment of an adapted architecture to effectively and securely isolate servers, data repositories, and applications from potential exploitation.

Protection

Fortinet ISFWs deliver intelligent, adaptive threat protection from the inside out, shortening the window of exposure and limiting damages. Fortinet ISFWs mitigate threats and protect critic assets and data by using network quarantining, actionable security, and complete logging and auditing. From visibility components like FortiView, through security controls like Application Control, and the proven threat intelligence of FortiGuard—enterprises can increase awareness of what's going through the network at all times.

ISFW Functionality Throughout the Enterprise

Virtual ISFWs for the Software-Defined Data Center (SDDC) - With virtualization and software-defined computing massively deployed in enterprise data centers around the globe, micro-segmentation is already implemented via the deployment of advanced virtual firewall appliances, segmenting each virtual machine (VM). Virtual ISFWs, such as the FortiGate-VM and FortiGate-VMX, provide the required security services for visibility, analysis and protection of traffic flows between virtual machines—also known as "east-west" traffic.

Physical ISFWs - For traffic flows entering and exiting the network perimeter and the data center, (also known as "north-south" traffic) the implementation of physical ISFWs provides a cost-effective and scalable way to extend security segmentation and visibility throughout the enterprise—from the end user to network and compute resources, applications, and data.

Unlike the implementation of virtual ISFWs—where a single virtual FortiGate ISFW segments and protects all the VMs, or segments within a server—determining physical firewall security segmentation granularity (server/network segment/workgroup/department, etc.) depends upon multiple factors such as the firewall's physical location, network architecture, the trust structure of the enterprise, and the criticality and location of datacenter assets.

FortiGate firewalls deployed as ISFWs provide the advantage of simplicity with Virtual Wire Mode for rapid deployment. In this mode, the firewall acts as a “bump in the wire” and is not seen as a router hop to connected devices, and therefore IP address modifications are not required.

Key Considerations - Whichever deployment option is chosen, the following criteria should be evaluated:

- Combining virtual and physical ISFWs offers a complete, end-to-end solution
- Integration with directory services
- Enhancement of the security policies in place to allow policy-driven segmentation
- ISFW performance must meet the throughput and latency required while providing next-generation security in a highly segmented environment

Fortinet’s ISFW Solution Advantage

Fortinet has pioneered the concept and deployment of ISFWs as part of its Advanced Threat Protection (ATP) framework, protecting organizations against today’s most sophisticated threats.

Fortinet FortiGate firewalls are dynamic, manageable and scalable ISFW solutions that:

1. Offer user/device/application-aware firewall policies for policy-driven segmentation
2. Support integration with RADIUS, LDAP, Active Directory for user authentication and management
3. Enable a rich set of security services, including AV, IPS and Application Control, to provide maximum internal network protection
4. Provide an ASIC-based physical appliance with the performance, speed, and low latency required in highly segmented environments
5. Include virtual firewall options for ISFW functionality in the SDDC and public clouds
6. Cover a wide range of physical and virtual appliances to fit performance and scalability required for optimized segmentation throughout the network
7. Complement a scalable, manageable, and automated end-to-end solution with FortiManager, FortiAnalyzer/FortiView, and FortiAuthenticator

Easy Deployment

With a default virtual wire mode, Fortinet ISFWs can be rapidly deployed into existing environments with minimal disruption. Keeping it simple for IT means being able to deploy with minimum configuration requirements and without having to re-architect the existing network.

Wire-speed Performance

Fortinet ISFWs operate at multi-gigabit speeds to provide deep packet/connect inspection without slowing down the internal network. Our ISFWs deliver very high performance in order to meet the demands of internal “east-west” traffic.

Management Tools for ISFW

ISFW is a component within Fortinet's end-to-end security platform—from secured wireless access to physical and virtual datacenter firewalls and application-level security appliances, all managed under a single pane of glass with FortiManager and FortiAnalyzer.

In the context of an ISFW deployment, the number of defined policies is expected to grow with policy-driven internal segmentation. In addition, any firewall in the enterprise network should be capable of dynamically enforcing policy-based segmentation, requiring every firewall to be aware of the entire range of policies defined. Such requirements can potentially create a management nightmare and impact the firewalls resources.

Fortinet's FortiManager, FortiAnalyzer and FortiAuthenticator address these issues by:

1. Defining policies once through FortiManager
2. FortiManager automatically distributes the policies to the firewalls participating in the ISFW functional segmentation
3. User awareness and policy-based segmentation scalability is achieved via the integration of FortiAuthenticator – providing integration & automation of FortiGate firewalls and the Directory Services
4. FortiAnalyzer and FortiView provide a granular and aggregated traffic visibility (users, devices, applications, threats, etc.) throughout the enterprise

Real-time Security

Fortinet ISFWs deliver a full spectrum of advanced security services (IPS, application visibility, antivirus, anti-spam, integration with sandboxing for Advanced Threat Protection) to allow the enforcement of policies within the internal network. This real-time visibility and protection is critical to limiting the spread of malware inside the network.

Summary

As threats grow in numbers, sophistication and impact, it is clear that placing all the security emphasis at the network perimeter is an outdated practice that leaves sensitive data on the internal network unprotected in the likely event of a breach.

Internal Segmentation Firewalls provide organizations with an additional layer of protection inside their network perimeters, protecting critical assets while enhancing their ability to detect breaches and shorten mitigation delays.

With high-performance virtual and physical ISFWs under single-pane-of-glass management, Fortinet leads the way and provides a granular, cost-effective and high-performance end-to-end ISFW solution for the most demanding organizations and environments.

FORTINET®

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
Valbonne
06560, Alpes-Maritimes,
France
Tel: +33.4.8987.0500

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

Feb 05, 2016