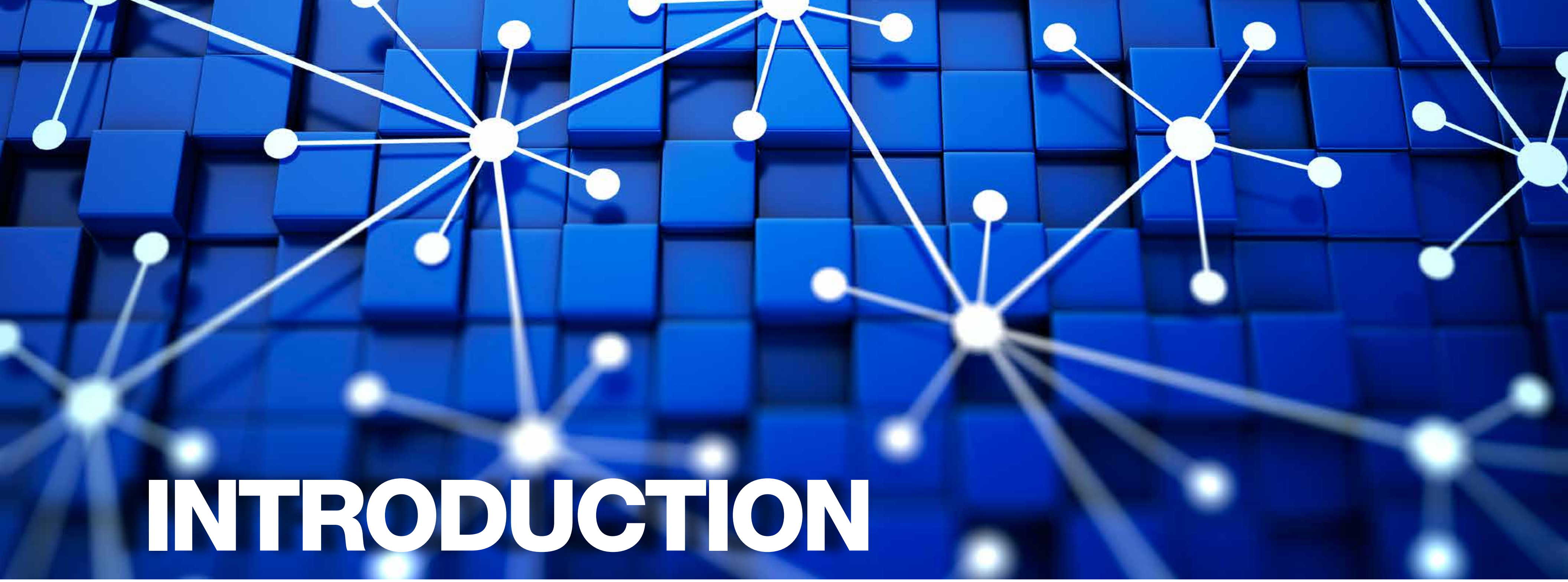
FORTINET

TRANSFORMING YOUR SECURITY

A NEW ERA IN ENTERPRISE FIREWALLS

Security Without Compromise

CONTENTS



INTRODUCTION

Security professionals at enterprises of all sizes worry about the expanding network attack surface, applications, data, and users in a borderless environment. From the mobile workforce to the data center, public, private, and hybrid clouds, SaaS apps, and the Internet of Things (IoT)—all have dramatically increased the attack surface while making it much harder to define and secure.

As organizations grow larger over time, perhaps acquiring other companies in the process, they find they have many security vendors' products deployed at different points across the enterprise. You may recognize this situation and these products may be operating as silos on your network.

Unfortunately, security products don't communicate with each other in the accidental architectures of today. They must all be managed separately, increasing complexity and leaving gaps in security across the dynamic attack surface.

The enterprise perimeter has stretched so far, it's no longer recognizable. It's clear that firewall technology must evolve with the borderless enterprise.

01 FIREWALL TECHNOLOGY EVOLVES WITH BORDERLESS ENTERPRISE

Although the NGFW is still the primary means of defense at the enterprise perimeter, security experts know that a borderless enterprise must consider users and deployment needs as well as network size. While the environment is changing, threat actors are targeting weak points—often where IT security has not been invested.

Security experts see that many vendors are not able to provide flexibility in deploying firewalls to the extended enterprise locations, which can result in multiple operating systems with different management consoles. Adding complexity kills security. This explains why organizations are still being breached today.

As cyberthreats continue to grow in sophistication, firewall technology must evolve beyond applications and network traffic to address the entire threat surface. The need to secure borderless environments is what's driving this evolution.

This is why IT organizations are looking for greater security effectiveness including compatibility across form factors, consolidation of security areas, a high level of reliable network performance, and simplified security management within a single pane of glass.

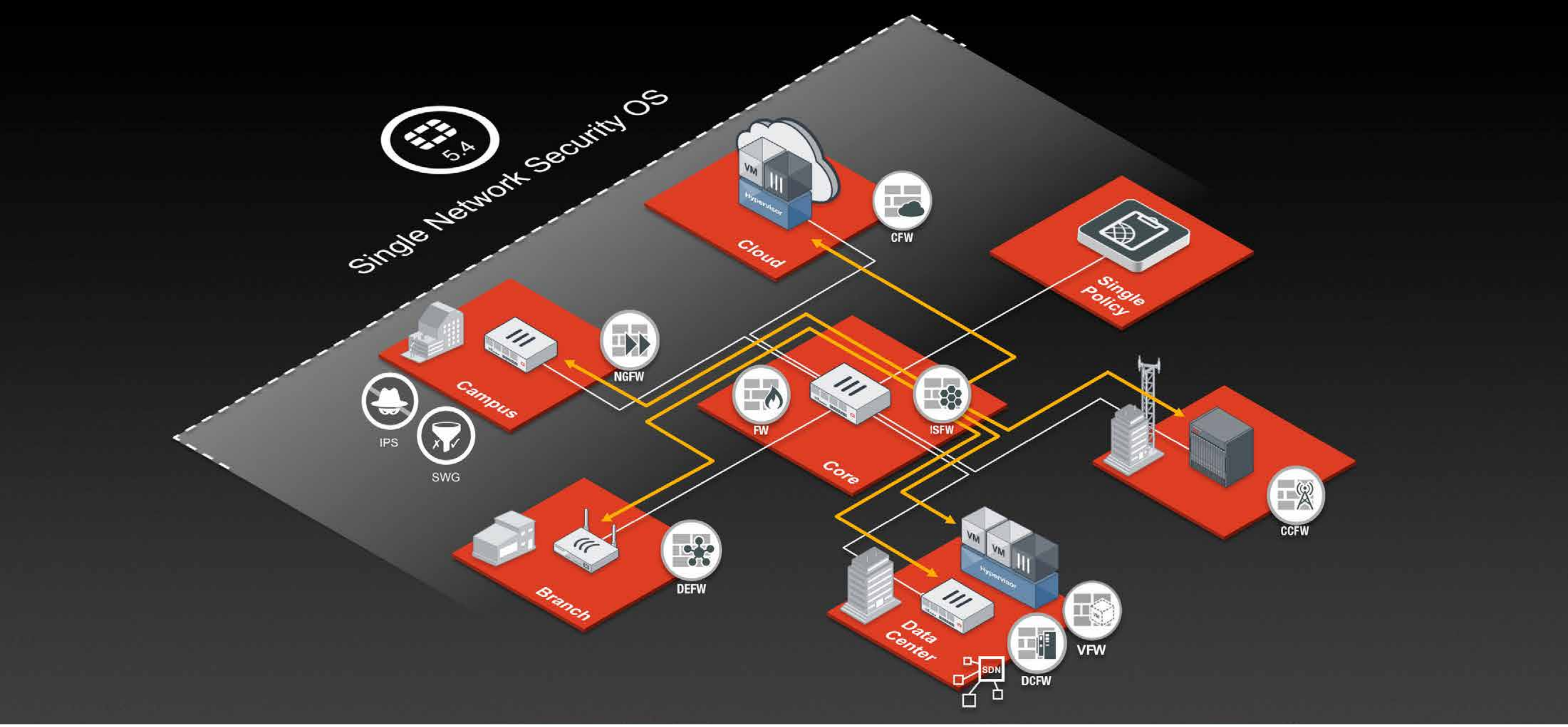
The Fortinet Enterprise Firewall Solution represents a new era of firewall technology by deploying enterprise firewalls strategically in a collective security fabric that stretches across the expanding network attack surface.

The three domains of the Fortinet Enterprise Firewall Solution operate as one to remove complexity and increase security.

Management Domain. This single pane of glass gives security managers a "true north" reference point for security-based logging, configuration, and reporting. Sharing threat intelligence and data across the enterprise via APIs speeds up incident response times and mitigates risk by giving security managers the ability to unify security policy configuration across their infrastructure.

Security Domain. A consolidated security environment helps reduce or prevent security incidents with layered security modules and maintains performance expectations while being able to apply deeper levels of inspection. Considerations involve: Is this a data center firewall deployment or an internal segmentation firewall deployment? And, what security inspection technologies will need to be enabled? Is malware inspection needed? What about application control?

Fabric Domain. The Fortinet Security Fabric is the communication and collaboration interface of the Fortinet Enterprise Firewall Solution. It determines where network and threat intelligence should be shared across the enterprise. The Security Fabric can extend security controls beyond the network layer to the access layer where the endpoint resides, to the application layer where data and information services are presented.



Enterprise Firewall Solution

The Fortinet Security Fabric combines with the Fortinet Enterprise Firewall Solution to enable an immediate, responsive, and intelligent defense against malware and emerging threats. This interconnectedness allows firewalls to work together across the entire network attack surface, reducing the need for multiple touch points and policies across the enterprise. Together, they form the backbone of the enterprise network security infrastructure.

The **Fortinet Security Fabric** helps enterprise security managers build a true end-to-end collaborative defense infrastructure. A policy created in one section of the Security Fabric is contextually applied across the entire domain.

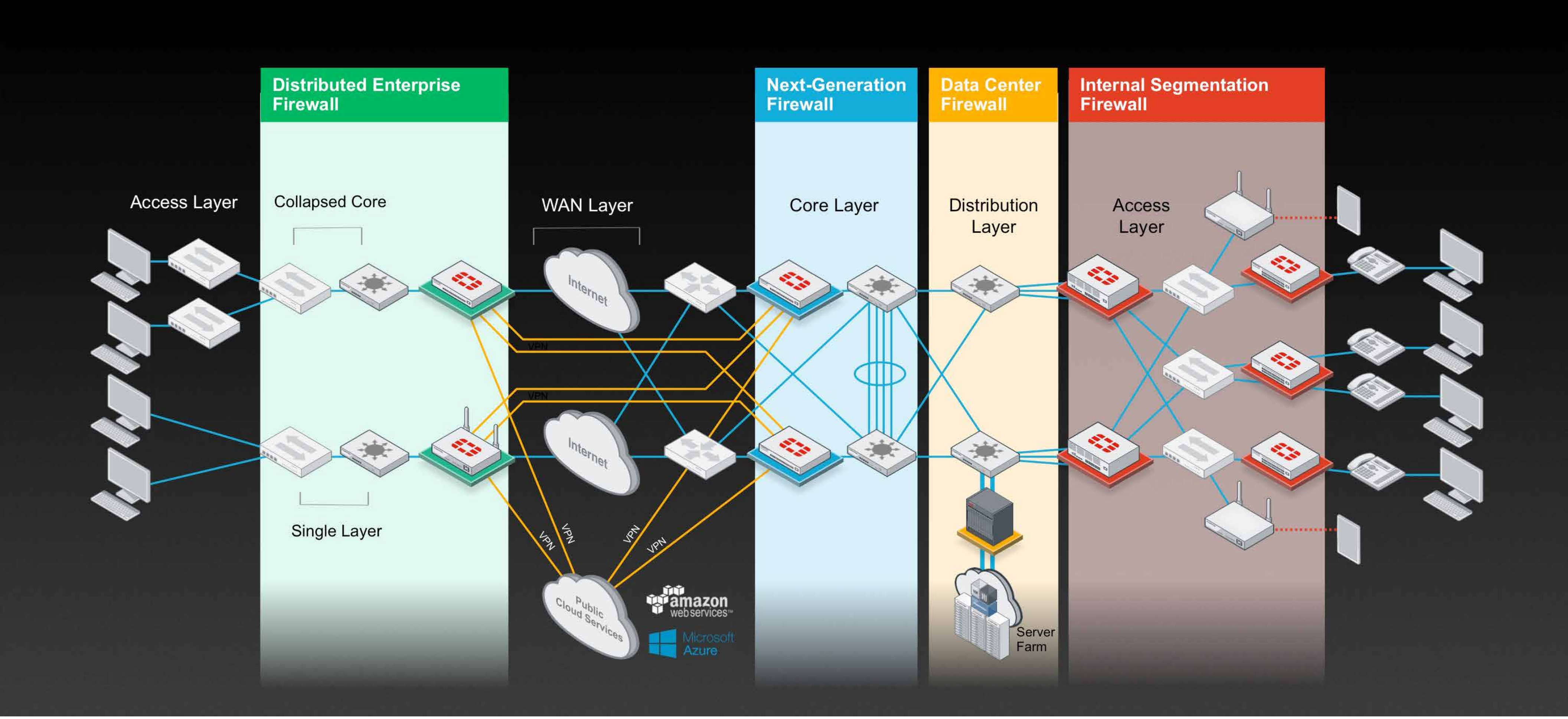
02 ENTERPRISE FIREWALL STRATEGY

In the new era of firewall technology, enterprise firewalls are a key component of the Fortinet Security Fabric. Instead of operating in silos, they work together, enabled by the communication and collaboration of the Security Fabric. The more firewalls there are strategically placed and communicating with each other throughout your borderless network infrastructure, the faster your response and breach mitigation times will be.

In borderless enterprise network environments, your data center and distributed enterprise are just as important as your enterprise perimeter and core placements and should be treated with the same security requirements. Attackers assume there will be a weaker security posture at these sites and that makes them prime targets.

The four primary enterprise firewall deployment modes are:

- Next-Generation Firewall (NGFW)
- Data Center Firewall (DCFW)
- Internal Segmentation Firewall (ISFW)
- Distributed Enterprise Firewall (DEFW)



Enterprise Firewall Deployment Strategy

When it comes to deployment strategy, the key to selecting the deployment mode is the location of the firewall in the network environment. Your strategy should consider not only the network environment (WAN/LAN), but also how malware could access your data and most sensitive systems. The location of the firewall determines the deployment mode.

- Will the firewall be at a data center where servers will need to be protected at very fast rates?
- Will the firewall protect the edge of the campus and provide application visibility?
- Will the firewall protect the internal segments to prevent lateral movements of a threat?

03 HOW TO DEPLOY ENTERPRISE FIREWALLS

Strategy: Perimeter placement, Internet-focused, first line of defense

Traditionally, the NGFW is placed at the perimeter as the first line of defense. It is an enterprise firewall with various security functions enabled that are focused on perimeter requirements. Because it is mostly Internet-facing, many enterprise security managers focus their entire security postures here and unfortunately make it their first and last line of defense against intruders.

In a standard enterprise environment, the NGFW is deployed between the Core Layer and Internet or WAN of the enterprise network. And since Internet speeds are slower than network speeds, NGFW performance requirements range on average from 1 G to 40 G in security throughput.

As a security and network gateway for the corporate environment, the NGFW is usually the default gateway or gateway of the network path and therefore may need to participate in dynamic routing protocols like BGP and OSPF. Of course, the most common security functions of the NGFW are firewall policies, application control services, SSL inspection, intrusion prevention service, anti-malware/antivirus service, and web/content filtering.

Strategy: Protects servers, low latency, focus on inbound security

The primary purpose of a data center firewall (DCFW) is to protect data and application resources in cloud or network environments.

Because data centers usually house the application and server resources of an enterprise infrastructure, the protection policies implemented on data center firewalls are mostly inbound-focused to protect server operating systems and applications. These servers are accessed by many users on a global network, forcing stringent requirements for throughput and latency speeds. For this reason, not all security functions should be enabled when deploying data center firewalls.

As data center firewalls are placed in the fastest portion of a network, the performance requirements are the highest of the enterprise firewall deployment modes: ranging from 10 G all the way up to 1 TB of security throughput. Due to these high-performance requirements, most DCFWs focus on three major functions only: firewall policies, application control services, and intrusion prevention services.

In a standardized enterprise campus network, DCFWs are usually placed in data centers between the distribution and services layers, and on the demilitarized zone (DMZ).

Strategy: Zero trust, submarine network–breach containment, security switch

In a standard campus network, the ISFW provides the security needed to divide and segment off portions of the network to prevent malware from spreading or hackers from accessing other parts of the enterprise.

Fortinet's unique ASIC design enables the ISFW to provide a nice balance of network inspection and port density. Deployed between switches and devices on the enterprise LAN, the ISFW enables a zero-trust security strategy where even your internal devices are not trusted. To help mitigate breaches and external influences, each ISFW becomes a "security switch" responsible for the passing and clearing of each device or switch connected to it.

An ISFW has 1 G to 100 G in security throughput requirements and will need to interconnect switches or directly connect devices, which could significantly increase throughput requirements. Due to its high-performance placement, it is advised to enable firewall, application control services, and intrusion prevention services. However, ISFWs also can be used for malware and sandbox inspection by zeroing in on a specific device that is propagating malicious code.

Strategy: Enable Software Defined-WAN (SD-WAN) for enterprise, VPN-Dependent and simplified deployment

The Distributed Enterprise Firewall (DEFW) is placed at the edge or perimeter of a Distributed Enterprise WAN. From the perspective of the Enterprise Firewall Solution, the Distributed Enterprise Firewall is an extension of the enterprise network that uses VPN technology or a dedicated MPLS circuit to create a network pathway between disparate locations. This collapsed network provides VPN links, intelligent load balancing for applications, and simplified zero touch deployment to enable SD-WAN for branch offices.

The Distributed Enterprise Firewall essentially links network and security paths across the world through the Internet or private WAN links, making it a truly borderless infrastructure for the enterprise. Consolidation and control of network security features in a centralized environment via the Fortinet Security Fabric is a major play for Distributed Enterprise Firewall deployments.

A DEFW requires less than 1 G in security throughput, as smaller sites don't require high performance. All-in-one security features are commonly applied including firewall policies, application control services, VPN, intrusion prevention services, and antivirus services. A DEFW is likely to deploy advanced features in small offices as well, such as SSL inspection, CASI, cloud sandbox, and even DNS proxies.

CONCLUSION

In a borderless enterprise, organizations must understand where their critical assets are and shore up defenses to be able to respond quickly with continuous security and monitoring across the entire network infrastructure.

The Fortinet Enterprise Firewall Solution represents a new era in firewall technology for the borderless enterprise. It increases security effectiveness and reduces complexity by consolidating network security across the entire threat surface. Enterprise firewalls are deployed based on their specific locations and focus in the enterprise, but the network security fabric that connects them stretches across the entire infrastructure.

Fortinet enterprise firewalls deliver a high level of reliable network performance, and the Fortinet Security Fabric allows organizations to take a holistic approach, with central visibility and control of the borderless enterprise managed through a single pane of glass.

FORTINET®

ENTER THE NEW ERA: FORTINET ENTERPRISE FIREWALL SOLUTION

ENABLE A BROAD AND DYNAMIC DEFENSE STRATEGY FOR THE LONG TERM BY TAKING A MORE COLLABORATIVE APPROACH ACROSS YOUR ENTIRE NETWORK SECURITY INFRASTRUCTURE

Security Without Compromise

www.fortinet.com