FORTINET

SOLUTION GUIDE

Protecting the Distributed Enterprise

Network Security for the Distributed Enterprise

Table of Contents

Introduction

The Changing Enterprise Network

The geographical and organizational structure of business has always evolved according to a shifting balance of economics and technology. Before the age of IT networking, any business functions dependent on the rapid exchange of information had to be collocated – typically at the Enterprise HQ. Even if the business as a whole was distributed across multiple sites, for example manufacturing plants, regional sales offices, or retail outlets, the majority of business functions were still centralized.

Consequently, the first IT networks mirrored this structure, with the most critical resources located centrally. Network security was therefore largely a matter of erecting a secure perimeter around these resources by means of a firewall.

Distribution of Intelligence

As wide area networks became both faster and less expensive, enabling the migration of application intelligence from the network center out to the edge, two distinct security philosophies began to emerge: enlargement of the centralized security infrastructure to support the expanding network, and the decentralization of the security infrastructure by replicating security functions at each remote site. Each approach had its drawbacks – the centralized model left the remote sites unprotected, increasingly an issue with the exponential

Protection at the Edge of the Network

IT technology has had a profound impact on how business has evolved. There are very few, if any, businesses or industries that have not been touched by IT. Both evolutionary and revolutionary, IT has enabled new business models that could not have existed 20 years ago, a concept aptly summed up by a well known cartoon “On the Internet no one knows that you’re a dog”.

But that evolution also has a downside, reminders of which appear with alarming frequency; a never ending string of high profile cyber attacks and data breaches which are compounded by the vast majority that never make the headlines. The distributed enterprise is particularly at risk of being successfully breached – with the typical network made up of tens, hundreds or even thousands of sites there is bound to be a weak link in the chain to exploit. Add to this the nearly universal presence of wireless connectivity, for internal use as well as for providing guest Internet access and it’s clear to see why the distributed enterprise, regardless of the industry, is such an attractive target for the cyber criminal and hacker communities.

increase in cyber-attacks and data breaches, and the decentralized model proved both costly and too complex to manage.

Evidence of this can be seen in the increasing number of highly publicized data thefts – most notably in the retail sector – where usernames, passwords and credit card details for millions of customers around the world have been stolen and sold to the highest bidder. Many of these breaches result from targeted attacks, using a combination of infection vectors that exploit the weaker security of remote sites, and often transcend the technological silos upon which most security solutions have been designed.

The impact of Mobility and Public Cloud Access

But the joint technological disruptions that have put the final nails in the coffin of perimeter security for the distributed enterprise have been the explosion in mobility and public cloud access.

As well as having to meet the rapidly increasing demand for high speed wireless access, IT managers have had to come to terms with an unprecedented loss of control – not only over the devices from which access is made, but also the location and management of many of the key IT resources being accessed. This has implications for both security and service level management.

To meet the mobility challenge, IT managers have resorted to wireless overlay networks with access security policies different to those of the existing wired infrastructure. This not only greatly complicates the task of management, but opens up more vulnerabilities, further compromising the overall security of the network (Figure 1).

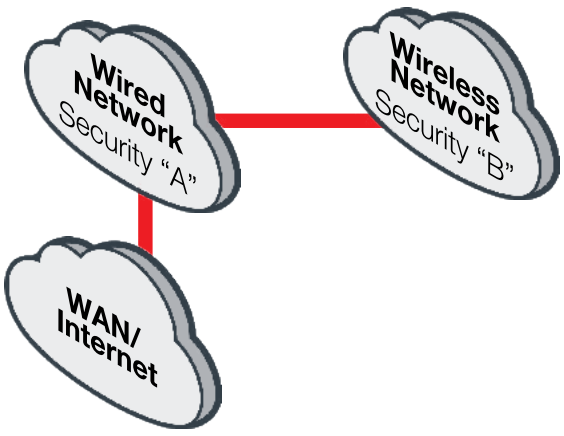

FIGURE 1 – Wireless Overlay Network

In addition to this, service levels need to be maintained across hybrid infrastructures comprising both public and private WAN links, presenting the challenge of finding cost-effective ways to dovetail external SLAs with internal Quality of Service assignments.

The Big Problem

Attempting to secure the modern distributed enterprise with a traditional centralized security approach is like trying to keep rain off a football game using umbrellas.

When your assets are distributed across multiple dispersed sites, any of which could become the next point of entry for a cyber-attack, centrally-deployed perimeter defenses are no longer effective. Yet replicating these defenses in their entirety at hundreds or even thousands of remote locations is not only costly, but can greatly increase management complexity, which in turn creates new vulnerabilities through the inevitable human error that ensues.

What's needed is a new distributed security architecture that mirrors and complements the new distributed enterprise – an architecture in which the entire network infrastructure is protected through a common, integral security fabric.

This, in a nutshell, is the essence of Fortinet's Distributed Enterprise Firewall (DEFW) – one of the available Deployment modes for Fortinet's Enterprise Firewall (Figure 2).

Enterprise Firewall				
Distributed Enterprise	NGFW	ISFW	Data Center	Cloud

FIGURE 2 – Enterprise Firewall

The 5 Key Requirements for a Distributed Enterprise Firewall

Security

Effective protection of enterprise data and applications comprises a number of successive security measures:

- First, users must be identified, authenticated (preferably via 2-factor authentication, using both password and token), and checked for authorization to access the requested data, applications or URLs.

- Throughout the session, the user's pattern of behavior should be checked against known intrusion prevention techniques, with any anomalies flagged or logged for later analysis as required.
- Due to the existence of zero-day exploits, social engineering, and polymorphic viruses, to name but a few of the tactics employed by cyber-criminals, intrusions and malware will still occasionally slip through. When they do, it is essential to minimize the time taken to detect them, so they can be dealt with swiftly and efficiently.
- Finally, the network administrator needs to be alerted to the nature and potential impact of any detected threat, and any infected systems need to be quarantined and cleaned.

In most large organizations, the majority of these security measures will already be applied centrally, but as we've just seen, with the recent proliferation of wireless access, this is no longer effective. Unless a common unified security policy can be applied to all new points of access, wired and wireless, wherever they may be throughout the distributed enterprise, the risk of leaving open an unguarded backdoor remains unacceptably high.

Connectivity

There are two main connectivity challenges for the distributed enterprise. The first is to provide a user access experience that is both consistent and transparent. The second is to interconnect remote sites in such a way as to meet the first challenge without over-reliance on expensive private-circuit WAN services.

- **Consistent, Transparent User Access**

Fundamental to any distributed enterprise security solution is the provision of flexible wired and wireless connectivity options that can scale as new equipment and personnel are added or moved from one location to another.

Authentication aside, all network access needs to be transparent to the user. Whether querying the customer database or making an IP voice call, response times need to be as fast and reliable via WiFi as via Ethernet.

With WiFi speeds soon to exceed 1.3 Gbps and most large organizations now embracing 'Bring Your Own Device' (BYOD) policies to a greater or lesser degree, this is not only achievable, but increasingly the most cost-effective option for new network builds, with some organizations now foregoing wired connections altogether. Integrated 802.11ac WiFi access should therefore be a mandatory requirement for the distributed enterprise.

- **Reliable, Cost-effective WAN Connectivity**

To address the challenge of maintaining inter-site connectivity and quality of service without over-reliance on expensive circuits such as MPLS, the router or firewall responsible for WAN connectivity needs to intelligently balance Internet and intranet traffic across the available WAN services. An effective solution to this challenge, capable of providing load balancing at an application level as well as overall traffic, is SD-WAN technology (Figure 3).

Alternative WAN connectivity options such as 3G/4G or ADSL, delivered through integrated modems, can also increase the overall flexibility and resilience of the distributed enterprise network.

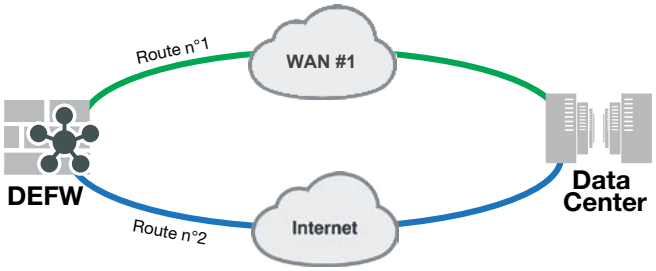

FIGURE 3 – SD-WAN

Performance

Although high-speed wired and wireless access devices are now readily available and relatively inexpensive to deploy, the challenge comes when you start to integrate the aforementioned security measures. This is because the kind of traffic analysis required to provide protection such as Application Control can be highly processor-intensive.
It is therefore critical that any unified access and security solution not only meets current requirements in terms of bandwidth and latency, but has the architecture to scale to future demands as well.

Cost

Security will always represent a compromise between risk and cost. Spend nothing at all on security and the risk of serious breach approaches certainty. Impose too many hurdles between users and the data and applications they need to do their jobs, and the cost, both in financial and productivity terms, becomes prohibitive.

But calculating the true cost of a security solution is not straightforward. Not only are there capital and operating costs to consider, but also the potential cost to the business resulting from each breach. In today's landscape of advanced persistent threats, some level of intrusion is inevitable, but for any given attack, its subsequent impact on the business can

vary enormously depending on how it is managed. The longer it takes to detect, quarantine and eradicate the problem, the greater the impact to productivity, and the higher the subsequent clean-up costs.

But the cost is not the same for all industries or vertical markets. According to the Poneman 2016 Cost of Data Breach Study the three vertical markets with the highest cost per capita (per compromised record) are those who are typically classified as being a distributed enterprise; Financial, Education and Healthcare. Retail, another distributed enterprise market segment had the 11th highest cost per capita out of a total of 16 segments.

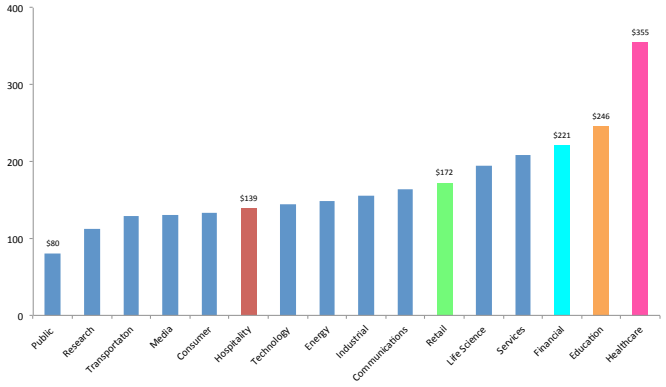

FIGURE 4 – Data Breach Per Capita Cost

Manageability

In addition to the basic requirements of central configuration and monitoring, the management of large distributed enterprise networks presents three additional challenges:

- Device Provisioning

With tens of thousands of potential devices, automatic provisioning should be mandatory.

- Device Deployment

Similarly, it should be possible to deploy key devices without the need for skilled network engineers to be sent to each location.

- Policy management

To avoid the inherent vulnerabilities of overlay networks and to ensure a consistent user experience across the distributed enterprise, it must be possible to create and maintain universal security policies.

To integrate these security policies with third-party authentication servers, the solution will also need to support Radius, Active Directory or both. Additionally, in the event of a security breach, the network administrator not only needs to be alerted, but presented with a range of remedial actions to resolve the problem. Furthermore, to remain effective, the system needs to be able to learn from past breaches and ideally, the input for this learning should come not only from your network, but from thousands of others just like it.

The Solution

With Fortinet's DEFW, every remote site of the network, regardless of size, is protected under a common, scalable security fabric, the Fortinet Security Fabric. As the network expands, through new sites added to the network or through new wired or wireless connections, the fabric extends automatically, securing each new site and connection.

Central to this unique advantage is FortiOS, the core security software for Fortinet's flagship products, FortiGate and FortiWiFi. Unlike other security appliances, in which full multi-layered security is only provided to those devices directly connected, the Fortinet Security Fabric extends through all Fortinet switches and wireless access points (FortiSwitch and FortiAP) to provide a secure unified access layer across the entire infrastructure.

Due to the Fortinet Security Fabric, each FortiGate and FortiWiFi in the network is also part of a higher level Advanced Threat Protection framework through the addition of FortiSandbox, either physically in the same network or through a cloud-based capability.

At each remote site, WAN utilization is optimized through the SD-WAN capabilities of Fortinet's DEFW. With easy-to-use multi-WAN management and a flexible policy-based performance management system, the DEFW intelligently balances Internet and intranet traffic across multiple WAN connections to lower bandwidth costs and keep users connected.

Management of the infrastructure, which is all consolidated through the FortiGate, is accomplished via FortiManager and FortiAnalyzer, combining centralized configuration with reporting, event logging and analysis, to create a comprehensive, real-time network monitoring and control center.

Key Benefits

Security

Embedded into every network infrastructure component, and tied together via FortiGate's centralized management portfolio, a comprehensive range of security measures are applied with each new connection, wired or wireless.

Furthermore, through the 24/7, automatic, threat response services of FortiGuard, the solution becomes part of a much larger, self-learning enterprise safety-net spanning thousands of Fortinet customers around the globe and thereby greatly reducing the time taken to respond to new threats.

URL Filtering	URL Filtering				
Antivirus	Antivirus				
Endpoint Control	Endpoint Control				
Application Control	Application Control		Single Sign-on		Continuous security updates
Intrusion Prevention	Intrusion Prevention	802.1x Port Access Control	Strong 2-factor Authentication	Strong 2-factor Authentication	Threat Intelligence
FortiGate	FortiWiFi	FortiSwitch	FortiAuthenticator	FortiToken	FortiGuard

Connectivity

Fortinet DEFW offers a wide range of cost-effective wired and wireless connectivity options to suit all possible requirements, for both end-user and WAN connectivity.

	Integrated WiFI		
Integrated Ethernet ports	Integrated Ethernet ports	High Density Ethernet switching	Interior and Exterior WiFi Access Points
Power over Ethernet (PoE)	Power over Ethernet (PoE)	Power over Ethernet (PoE)	Maximum WLAN performance via 802.11ac
FortiGate	FortiWiFi	FortiSwitch	FortiAP

Performance

To ensure optimal throughput, even when the full range of security measures are enabled, the solution makes use of dedicated Application-Specific Integrated Circuits (ASICs) to provide hardware acceleration of key network processing functions.

NP6 CAPWAP Hardware Acceleration		
FortiASIC Hardware Acceleration	FortiASIC Hardware Acceleration	1.3 Gbps WiFi via 802.11 ac
FortiGate	FortiWiFi	FortiAP

Cost

Due to the tight integration of connectivity and security, the solution requires fewer devices than competitive offerings with no additional licensing fees for wireless access, and the flexibility to license only the specific functionality required at each location.

Fewer devices integrating multi-layered security with high-performance connectivity	Fewer devices integrating multi-layered security with high-performance connectivity
Flexible licensing of features as required	Flexible licensing of features as required
No licensing cost for wireless access	No licensing cost for wireless access
FortiGate	FortiWiFi

Manageability Although able to extend the full range of security features with each new network connection, wired or wireless, the solution is designed to be fully managed from a central location, greatly reducing the chance of having to send trained personnel to remote sites.			Hyperscale Management	
	Support for Radius and Active Directory authentication	Support for Radius and Active Directory authentication	Zero-touch Deployment	
	Web GUI	Web Gui	Centralized configuration and monitoring	Centralized reporting, event logging and analysis
	FortiGate 	FortiWiFi 	FortiManager 	FortiAnalyzer 

SD-WAN Fortinet's DEFW enables Software-defined WAN (SD-WAN), linking network and security paths through the Internet or private WAN links, making it a truly borderless infrastructure for the enterprise.	WAN Cost Optimization	WAN Cost Optimization
	Integrated Security and Networking	Integrated Security and Networking
	App visibility and intelligent load balancing	App visibility and intelligent load balancing
	FortiGate 	FortiWiFi 

Summary

Today's distributed enterprise demands fast, transparent access to critical applications and data, from anywhere, and from a range of devices over which administrators no longer have full control. Fortinet's DEFW provides a tightly integrated infrastructure – access, networking and security - capable of meeting these demands without compromising either performance or security.

As security threats increase in number, risk, and sophistication, Fortinet's distributed enterprise customers can rest assured that their data protection obligations to customers, business partners and shareholders can be honored, and that maximum business continuity will be maintained.

Above all, Fortinet's DEFW perfectly complements the distributed enterprise architecture, extending Fortinet's Security Fabric across the organization, and uniting the various solution components to deliver combined benefits greater than the sum of their parts.

www.fortinet.com

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, Sophia Antipolis,
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
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480