Building a Security Fabric for Today's Network

Enterprise Firewall Solutions Must Be as Borderless as the Enterprise

Security professionals at large enterprises worry about the expanding attack surface, which spans the network, applications, data and users in a borderless environment.

From the mobile workforce to the data center, public and private clouds, and the Internet of Things (IoT)—all have dramatically increased the attack surface while making it much harder to define and secure. For example, IoT devices rely on the access network for security. And while both software as a service (SaaS) and infrastructure as a service (IaaS) have generally been accepted by enterprises, the unsanctioned use of third-party shadow IT applications threatens data security.

The enterprise perimeter has been stretched so far it's no longer recognizable.

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. Unfortunately, in an "accidental architecture" like this, security products don't communicate with each other and must all be managed separately, increasing complexity and leaving gaps in security.

How We Got Here: The Accidental Architectures of Today

To see how we got where we are today, take a look at the timeline in Figure 1 and then fast forward through the evolution of the significant network security technology developments of the past two decades.

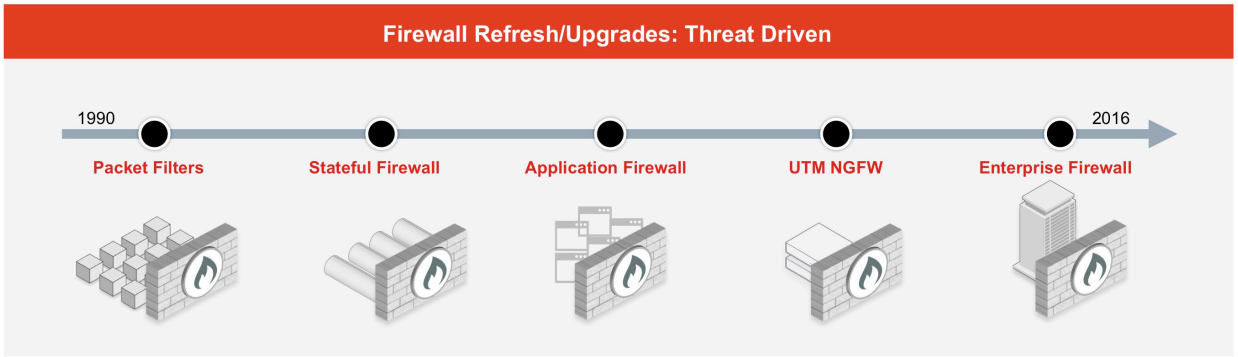

Figure 1. Timeline of Firewall Technology Evolution

Packet Filters

In the early 1990s, one of the first firewall technologies (called packet filters) was made commercially available and existed primarily in routers and switches as a means to filter out certain IP addresses and protocols. Then an improved version of packet filters was developed called the stateful inspection.

Stateful Inspection Firewall

Unlike simple packet filters, the stateful inspection firewall was capable of maintaining state information that allowed it to be more secure in its inspection methodology. Although stateful inspection was good at performing lower-layer checks within the OSI stack, it wasn't proficient at understanding and securing data at the application layer.

Application Firewall, IPS and Web Filtering

A few years later, application firewalls were built to understand certain protocols and applications that were most commonly seen in enterprise environments. While application firewalls are very capable of understanding and deciphering traffic like HTTP (web) or SMTP (email), they can be a drag on network performance and require significant tuning and updates to work correctly. Application context awareness also drove the development of point security solutions like intrusion prevention systems (IPS) and web filtering products that eventually became security products within their own space.

Frequently, enterprise security managers would deploy both **stateful inspection and application firewalls** for their main perimeter defenses. This led to overcomplexity and challenges with management and configuration between the various network security technologies.

Unified Threat Management Firewall

Around 2000, unified threat management (UTM) technology came onto the scene, where both stateful and application inspection could be combined, processed and managed from a single platform. The UTM firewall (coined by IDC) referred to an all-inclusive security product combining network firewall and other application-based inspection technologies, such as **IPS, web filtering, anti-spam, and antivirus,** into a single form factor.

Because all-inclusive UTM firewalls required tremendous processing, they were adopted by the small-to-medium enterprise where bandwidth requirements were lower. However, due to cost savings and consolidation of the various application security technologies, the IT organizations within these budget-constrained markets took this solution on in a big way.

Since UTM firewalls lacked the necessary granularity and controls that enterprises needed for some of the more advanced security functions (i.e., IPS, web filtering, anti-spam), larger enterprises continued with the **legacy defense model** of having both a **stateful firewall and various forms of application-based security technologies** deployed across their larger enterprise perimeters. With all the security controls in silos, this did not solve the problem of management sprawl or address the complexity of maintaining multiple vendors' solutions.

Next-Generation Firewall

The NGFW terminology came about in late 2000, coined by an analyst firm, Gartner, who built on the UTM concept of an all-in-one security solution, but geared it more towards the **scalability requirements** of the larger enterprise environments. And for many years NGFW technology expanded on application security functions by increasing the amount of controls and granularity the enterprise security experts were seeking. In addition to more security controls, the NGFW also provided a boost **in network security processing power** to keep pace with the high throughput requirements of larger environments.

Firewall Technology Must Evolve with the Borderless Enterprise

Although the UTM and NGFW are still the primary means in which enterprise security managers defend the enterprise perimeter, what these security experts know is that the perimeter is always changing. Larger enterprises can no longer be defined by network size or footprint, but must also consider users and deployment needs.

Today, we are in a new era for firewall technology. In the borderless enterprise, while business needs are changing, threat actors are targeting the weak points—usually where IT security has not invested. This is one of the main reasons why organizations are still being breached today.

As the sophistication in attacks continues to evolve, the base capabilities of firewall technology can no longer be limited to applications and network traffic, but must be shifted to address the entire threat surface. This is what's driving the evolution in firewall technology.

Collapsing multiple security functions into a single firewall unit leads to misconfiguration, missed log incidents and increases the chance that breaches will go undetected. Complexity kills security.

In addition to increasing security effectiveness, enterprise security professionals are looking for greater compatibility across form factors, consolidation of security areas, a high level of reliable network performance and simplified security management, ideally within a single pane of glass.

Creating a Collaborative Defense to Fight Fire with Fire

As enterprises add additional layers of defense, it doesn't matter how quickly threats are detected when security operators have to manually review logs in multiplicity before they can be aware of or react to incidents.

Consider the Target data breach of a couple of years ago. For Target, all systems were in place, including many of the latest security solutions, but the human reaction factor was caught off guard because the breach information was buried in manual logs.

These types of missed opportunities are common today, as in the recent Verizon breach involving an apparent back door in Verizon's MongoDB. As reported by Brian Krebs, the vulnerability "enabled a prominent member of a closely guarded underground cybercrime forum to post a new thread advertising the sale of a database containing the contact information on some 1.5 million customers of Verizon Enterprise."[1] For more studies of actual breaches that shed light on today's security challenges, see Verizon's annual Data Breach Investigations Report (DBIR).[2]

The use cases above illustrate the need for a collaborative defense strategy that is enabled by the security products themselves. How can next-generation firewall technology move away from being a point solution for a single ingress and egress point of a network to becoming aware of and responsive to the entire attack surface?

We can take a page out of the bad actors' book to see how they leverage collaborative processes, as illustrated in Figure 2. See how many steps are taken in a matter of milliseconds—to deliver, exploit and then install malicious code. An example would be a DDoS attack, when automated bots enlist in a collaborated attack to overwhelm servers until they cease to function properly.

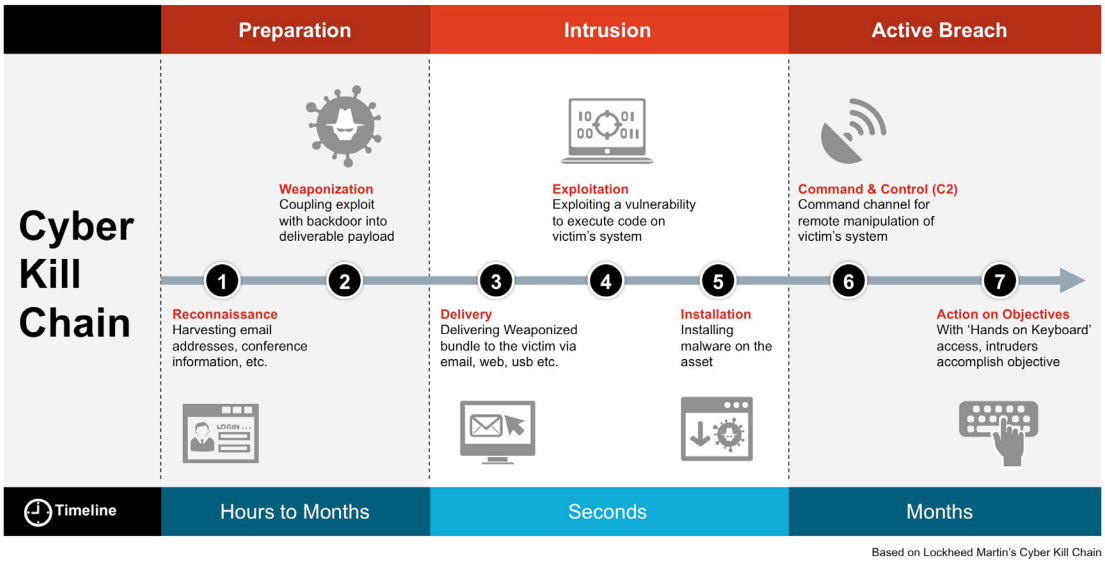

Figure 2. The Militarized Cyberattack Process

As you can see in Figure 3, the enemies' tech is organized, responsive and sharing information, while most borderless networks are not. Enterprises need to fight fire with fire, or collaboration with collaboration, and connect and share security just like the bad guys connect and share malware.

[1] Crooks Steal, Sell Verizon Enterprise Customer Data, KrebsonSecurity, March 24, 2016

[2] Verizon 2015 Data Breach Investigations Report (DBIR), Verizon, 2015

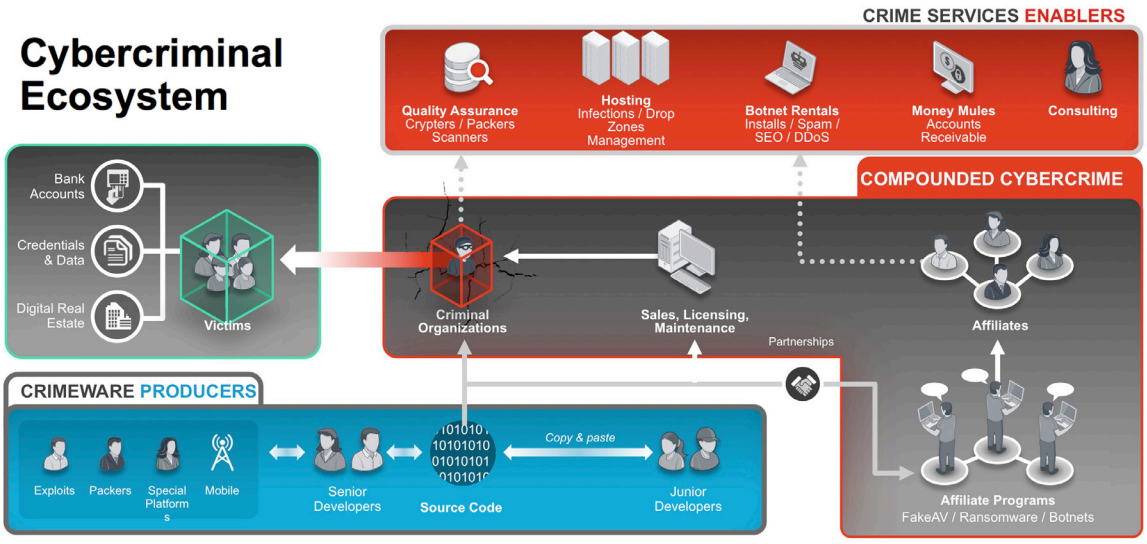

Figure 3. Cybercriminal Ecosystem

The Three Key Functional Domains of Fortinet Enterprise Firewall Solution

The key functional domains of Fortinet Enterprise Firewall Solution work as one to remove complexity and increase security, as shown in Figure 4. Each functional domain is explained below.

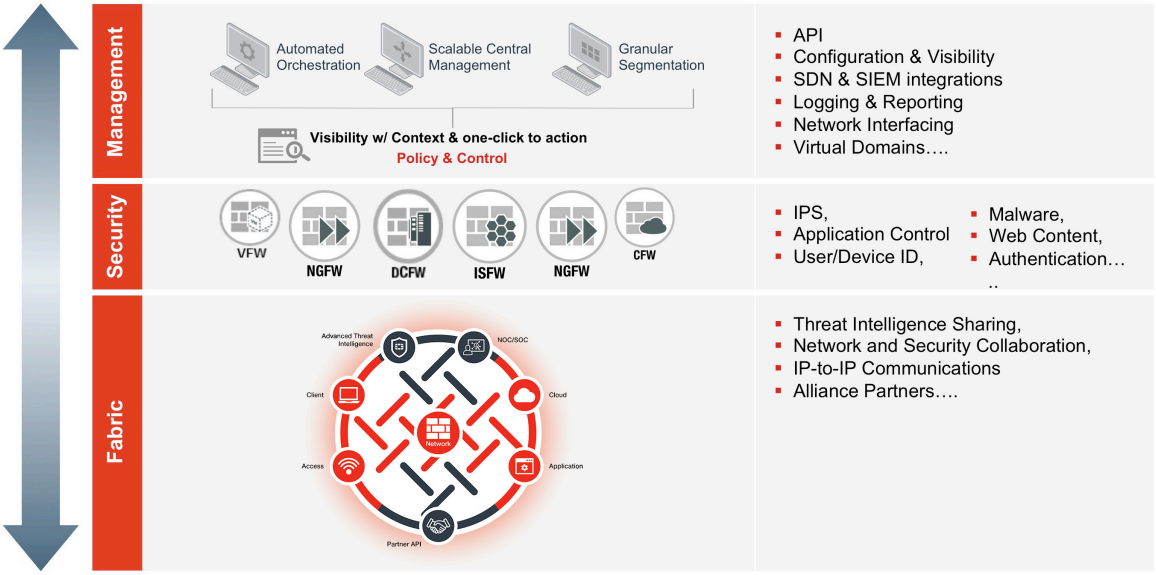

Figure 4. The Three Functional Domains of Fortinet Enterprise Firewall

Management

This domain pertains to all things related to the automated management, provisioning and controlling of the firewall solution from **API orchestration** to the creation of virtual domains to the structuring of logging mechanisms. **Scalable central management** overlays can be consolidated to reduce complexity or expanded to provide **contextual visibility via one-click automation.** 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

The various **deployment modes and security-level functions** are applied in this domain. 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?

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**.

Fabric

In this domain, the firewall solution interfaces and networks with the **communication and collaboration** elements contained in the fabric to determine which **network intelligence** is shared across the enterprise. Fortinet refers to this as the Fortinet Security Fabric. This includes communicating **threat intelligence** to a policy created in one section of the Security Fabric, which is then contextually applied across the entire enterprise, thus reducing the need for multiple touch points and policies across the entire infrastructure.

The Fortinet Security Fabric also can extend the security controls beyond the network layer to the access layer, where the end point resides, to the application layer, where data and information services are presented.

The **"Security Fabric"** functions as a communication interface for today's enterprise firewall technology, and this strategy helps enterprises build a true end-to-end collaborative defense infrastructure. When the enterprise firewall technology communicates with the Fortinet Security Fabric, it determines what information will be shared across the enterprise. For example, when malware is detected in one area, the Security Fabric shares threat intelligence with the rest of the enterprise infrastructure. Another example is when a policy created in one section of the Security Fabric is contextually applied across the entire domain. This interconnectedness reduces the need for multiple touch points and policies across the enterprise.

The Fortinet Enterprise Firewall Solution, as shown in Figure 5, combines with the Fortinet Security Fabric to enable an immediate, responsive and intelligent defense against malware and emerging threats. They are the backbone of the enterprise network security infrastructure.

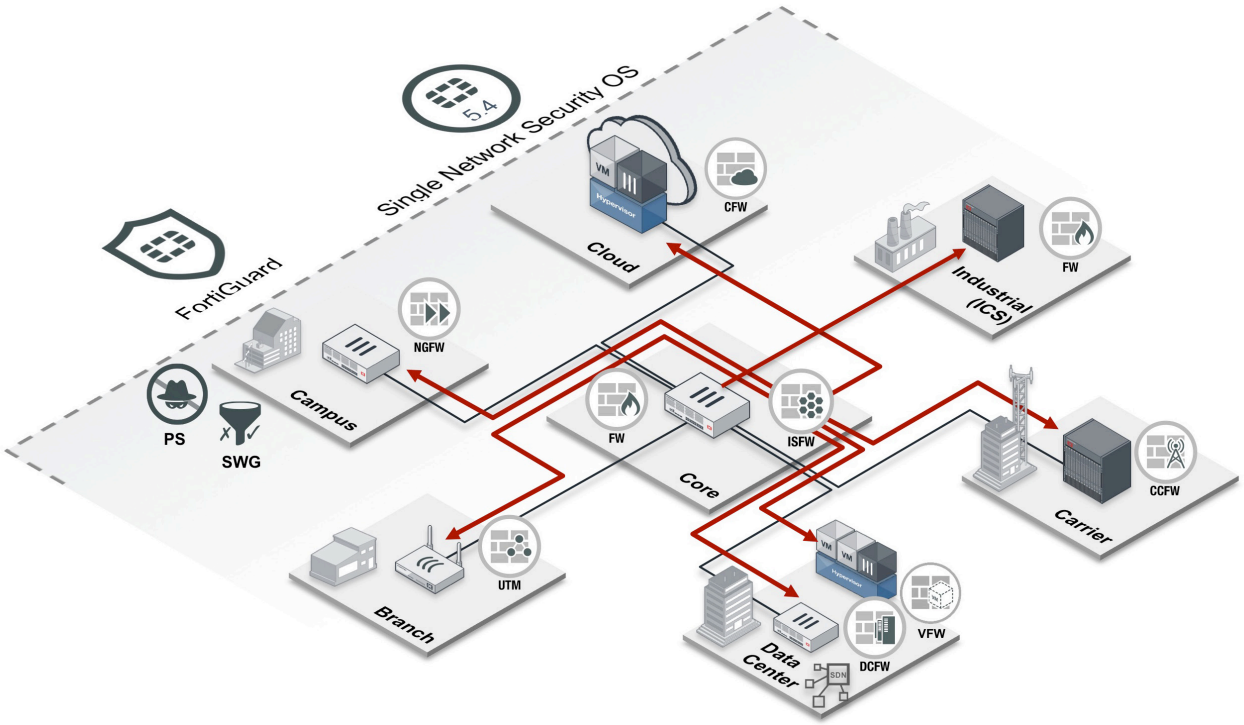

Figure 5. Enterprise Firewall Solution

Enterprise Firewall Strategies and Deployment Modes

When strategizing on deployment, it is important to consider not only where the perimeter is (WAN /LAN points), but also how malware could get to the data and most sensitive systems. Despite their different locations, the 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 weaker security posture at these sites and that makes them prime targets.

Instead of operating in silos, consider enterprise firewalls as part of the Fortinet 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.

The location of the firewall in the network environment is the key to selecting the deployment mode, as shown in Figure 6. For example, will it be located at a data center, where servers need to be protected at very fast rates, or is this firewall meant to protect a few hundred users at a corporate office?

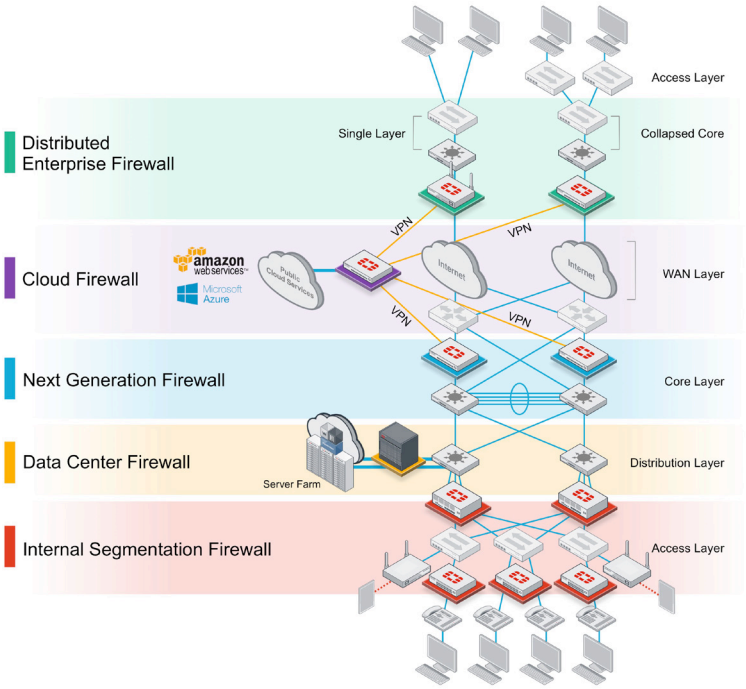

Figure 6. Enterprise Firewall Deployment Modes

Security managers will want to automate security infrastructure and response because machine responses are faster than human responses. However, automation requires preplanning and selecting the right supportive technology to implement a Security Fabric. Make sure the network security solution is the cornerstone of this strategic planning phase.

Fortinet Enterprise Firewall Solution

The Fortinet Security Fabric for the Borderless Network

Fortinet's Enterprise Firewall Solution increases security effectiveness and reduces complexity by consolidating network security technologies across the entire infrastructure, no matter the placement or location of the system in the extended enterprise. The solution delivers a high level of reliable network performance, and the Fortinet Security Fabric allows security managers to take a holistic approach to security with visibility and control managed through a single pane of glass.

Today, threat actors can strike anywhere at any time, at will. And that means enterprise security professionals must apply the same mentality to defense strategies and structure as that put into place during wartime scenarios. Organizations must shore up their defenses—understanding where their critical assets are—and respond quickly with continuous security and monitoring across the borderless network.

By taking a more collaborative approach across the entire infrastructure, network security managers can enable a broad and dynamic defense strategy for the long term.

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

Dec 12, 2016