Firewall Evolution

Evolving firewalls in a world without perimeters

By Andreas M. Antonopoulos
SVP and Founding Partner, Nemertes Research

Executive Summary

The virtual enterprise has brought with it new ways of working, a huge expansion of the footprint of the network and erosion of the perimeter, rendering traditional firewall solutions insufficient. Today's firewall must evolve to meet completely new requirements, in the data center, in the branch and for the roaming user on the road. The next evolution of the firewall has to combine dynamic policy-based security with performance, rapid scaling, high availability and application intelligence. Firewalls are no longer just perimeter devices for the data center, but should be weaved into the fabric of the network from edge to edge, offering security that is layered in-depth and ubiquitous.

The Issue

When firewalls were first introduced in the industry, they represented a bastion of security, a single bottleneck repelling the hordes of "wily hackers"[1] on the boundary between a corporate network and the Internet. There was *the* Internet connection and protecting it was *the* firewall. There was only one Internet connection and only one firewall, and the *perimeter security model* was the dominant security model for almost two decades. Nowadays, however, the perimeter has been eroded by the forces of globalization, ubiquitous connectivity, mobility, teleworking, virtualization, and cloud computing. As the perimeter security model is rapidly becoming obsolete, is the firewall following it into obsolescence? Not quite: firewalls are evolving to take on new roles, distributed throughout the network. The firewall is now at the core of a new *ubiquitous security model* where it acts as traffic director, separating regulated systems from public systems, guarding protected information, and supporting virtualized and

[1] From the first book on the subject of firewalls, considered the birth of the firewall when published in 1994: Firewalls and Internet Security: Repelling The Wily Hacker (ISBN 0201633574)

mobile systems. As the firewalls of the '90s deployed according to the needs of the '90s become obsolete, they are replaced by the next evolution of firewalls.

Historical Perspective - The Eroding Perimeter, the Virtualizing Corporation

If you imagine a corporation as a collection of people working in the same place towards the same goal, you are imagining a construct that is quickly disappearing from our world. Today's corporations are very distributed, spanning multiple locations, countries, and even continents. The vast majority of work in a modern corporation now spans multiple locations, and may soon occur primarily *externally*, in collaboration with partners, suppliers and customers. The corporation is turning itself inside-out, becoming communication-centric and collaboration-centric, and delivering most of its value through interactions with others. The concept of a "perimeter" becomes difficult to define when the concepts of *inside* and *outside* change rapidly and fluidly. Insiders can be mobile and roaming everywhere *but* headquarters: more than 89% of employees work away from headquarters. Outsiders are invited into the business as contractors, consultants and partners. Data and applications are no longer internal; they are *shared* with the mobile workers and external partners over the Web.

Nearly 90% of Nemertes research participants say they operate a "virtual" organization in which members of distributed workgroups must collaborate with each other across multiple locations, as well as with partners, suppliers and customers. Virtual workplaces include branch offices, home offices, hotels, airports, etc. Additionally, a majority of companies (52%) have a global presence. This goes for both large and small organizations. Twenty-five percent of small companies (less than 250 employees) support global locations, while 77% of very large companies (more than 10,000 employees) do.

Branch office scope is broadening to include the "micro-branch," mobile worker or single-person telecommuter site. An overwhelming majority of companies (85.6%) increased the number of telecommuters in 2009, after two years of relatively mild growth in the number of telecommuters (17% in 2007 and 20% in 2008).

A major indication of how critical mobility has become is the dramatic leap in percentage of organizations that have a mobility strategy in 2009 versus 2008. Now, 59.5% of organizations say they had a mobility strategy in 2010. That compares with just 40.6% in 2008. That's a 46% jump in one year, and it indicates how critical mobility has become. Another metric is spending. In 2009 when IT spending was crashing, mobility represented the one bright spot. Organizations spent a median of 13% more on mobility than they did in 2008, with a median spend per mobile employee of $2,883. This year, companies spent 13% more on average than 2010, at $412 per employee. Clearly, mobility is not an exception to the norm–it is rapidly becoming the norm.

The distributed, virtualizing corporation brings with it a distributed workforce, distributed applications and distributed data. The corporation no longer has *the* Internet connection – it has hundreds if not thousands of constantly

moving Internet connections. As a result, the modern corporation doesn't really have a defined perimeter, it has many overlapping, constantly moving mini-perimeters. These extend out of the corporate network to encompass mobile workers, VPNs and extranets.

Meanwhile, data centers are changing dramatically, too. Most companies are in their second or third wave of data-center consolidation and virtualization. Data centers have been reduced in number while they simultaneously increase in size and density. More and more applications are concentrated in fewer and fewer data centers. The applications within data centers are also becoming more distributed. Internal traffic flows between both physical and virtual servers are increasing, replacing traditional "north/south" traffic (up and down the layers in a hierarchical network) with "east/west" traffic. Data center network architecture is changing as a result as network architects collapse switching layers and consolidate layer-2 networks using 10-gigabit Ethernet.

Companies are also consolidating branch office networks. For years, Nemertes' research has shown more and more features consolidated into multi-purpose gateway devices in the branch. Security functions like firewalling, intrusion prevention, VPNs and anti-malware are increasingly purchased as features on a multi-function branch device instead of separate appliances.

The traditional security perimeter model is becoming more difficult to apply. The perimeter itself is re-defined, stretching like a rubber band to encompass roaming workers and remote offices all around the world. But the perimeter is also eroded because the simplistic view of "inside" versus "outside" is disappearing in a fully interconnected world of ubiquitous networks. The separation of the perimeter is more illusory than real. Depending on your perspective, everything is on the "inside", or if you prefer, everything is on the "outside." Networks today are perimeter-less, borderless, unified, interconnected and seamless. Even the word "networks" is gradually being superseded by the singular form: "the network" is singular, shared and everywhere.

Security Implications of the Eroding Perimeter

Consolidation is helpful in addressing the most pressing security need of most organizations: regulatory compliance. When data and applications were scattered across company networks, it was very difficult to control and monitor access to them. With consolidation, data and applications are centralized in one or two data centers, making them much easier to identify, catalog, control and audit.

For the last several years, compliance has been the primary driver for security spending. In 2010, 57% of companies identified compliance as the primary security driver. All the compliance initiatives that companies face fall into two major categories: privacy regulations and accountability regulations.

Privacy regulations require that private information, especially financial or health information about individuals is kept private. Companies meet their privacy requirements in part by segregating sensitive data from publicly accessible systems

and controlling the flow of sensitive data. Most companies use firewalls to separate systems that are subject to regulations from systems that are not. By segregating systems, companies not only protect the sensitive data on those systems but they also contain the scope of regulations thereby reducing the cost of those regulations. For example, if a company is subject to PCI-DSS, the payment card industry regulations, they often will corral all systems handling credit card information onto a separate logical network and separate those systems from everything else. That allows them to apply the onerous PCI regulations on only a subset of their total infrastructure.

Accountability regulations require that companies track activities on their networks and applications in order to be able to report who had access to information at a certain point in time (e.g. Sarbanes-Oxley or HIPAA-HITECH). Companies will again use VLANs and firewalls, coupled with identity management systems to separate the regulated systems and track any attempts to access those systems. The firewall logs provide the necessary information for auditors and compliance reporting.

The traditional firewall is stretched out of shape and yanked out of place by these changes. Within the data center, the mobility of virtual servers, the changing relationships among virtual servers as distributed applications evolve, and the flattening of networks make using a traditional firewall to segment the data-center network difficult. IT is left with the choice of hobbling the dynamic data center with static security, or loosening the security among servers to enable fully agile computing.

Likewise, the spread of the enterprise over more locations, some with little or no infrastructures, possibly operating over an Internet VPN, means that the firewall has to be in more places to serve as filter for and protector of users.

Evolving Firewall Functions

With an eroding perimeter in a virtualized enterprise, the core challenge is *where* to put the firewall. The answer is gradually becoming clear – *everywhere*. As the perimeter erodes, firewall functionality needs to be distributed throughout the corporate network, in appliances, gateways, routers and switches, from data center core to branch-office edge. The reach of these firewalls extends through VLANs and VPNs to encompass mobile endpoints and virtualized servers, effectively acting as a traffic cop for the endpoints.

The need for compliance creates further pressure to place firewalls in different parts of the network infrastructure. Compliance is as much about insider threat as it is about outside attacks. Monitoring the use of systems by employees means that the internal network requires segmentation, as much if not more than the Internet connections. Firewalls are therefore deployed in layers, not only around the data-center perimeter (DMZ and egress connections) but also deep within the network, between virtual servers, in branch offices and reaching out to roaming users. The need to position firewalls in different parts of the network also means that these firewalls must come in different form factors. In some locations,

firewalls will be in the form of a traditional appliance (big box firewall), in the data center DMZ for example. In other locations, the firewall functionality must be built into a router, a core switch, a distribution switch, an access layer switch or a campus switch. These distributed firewalls can enforce traffic segregation, extending VLANs from the endpoints (users and virtual servers) across the internal network and in many cases mapped out to MPLS labels spanning the WAN. In the data center, server virtualization has blurred the line between physical and virtual networks. Virtual servers on virtual networks still need access control and segmentation and this is achieved by a combination of physical firewalls, VLANs and virtual firewalls, possibly incorporated into virtual switches.

Firewalls in branch offices must bring multi-function security in easy-to-deploy, minimal-maintenance platforms with central management. As branch offices get smaller, companies need a broader range of firewall form-factors, from large branch VPN concentrators and Internet gateways, to home-office access firewall gateways, physical, virtual, or software clients.

The term "firewall" has evolved to include many other functions in addition to the traditional function of traffic control. Today's firewalls operate on all layers of the protocol stack, from layer 2 to layer 7, inspecting traffic and analyzing protocols for myriad applications. Attackers have moved up the protocol stack, exploiting vulnerabilities in applications, from IP to TCP, to HTTP to HTML, XML and beyond. Firewalls have followed, securing application traffic up the stack with deep inspection of the protocols and stateful handling of the application flows.

Firewalls can no longer stay isolated from the rest of the world. Rather than closed systems, today's firewalls are enforcers in a global intelligence network that collects, shares and updates information about applications, attack signatures, attacker addresses and reputations. The firewall is just one part of this global "conversation" about attacks and is only as good as the latest update. Because of zero-day attacks and rapidly propagating malware, firewalls must be able to respond the latest threats with great speed. Firewall administrators need to be able to manage firewalls as a "fleet" deploying new access control restrictions, patterns, signatures and policies across a global infrastructure. The firewalls must also be able to receive updates automatically, to counter distributed threats like botnets. Botnets evolve very rapidly and can attack from multiple directions at the same time. In order to defend against such threats, firewalls need to be able to receive automatic reputation updates that can identify and counter the latest botnets as they are discovered.

Evolving firewall requirements: In the data center

- **Performance.** In the data center, firewalls are facing two significant challenges: the increase in internal machine-to-machine traffic and the broad deployment of 10 gigabit Ethernet. The result of these two trends is that they place enormous performance demands on firewalls. Not only do firewalls need to manage line-rate inspection of traffic at the Internet ingress point, they also

need to manage flows between tiers of virtualized servers at line-rate.

- **Consolidation.** Firewalls are no longer just about separating external and internal networks. Companies have been consolidating data centers, and within them consolidating servers into large pools. Data-center networks are now much more complex than they used to be, with a large number of external connections to partners, suppliers, and customers. The de-militarized zone architecture, which is based on physically separate networks with firewalls in between, is becoming too cumbersome. The single firewall, single Internet connection, single DMZ data center is only found on architecture drawings today. In the real world, companies have to deal with dozens of connections (Internet, leased line, MPLS, and legacy connections), dozens of DMZs (partner extranet DMZ, remote access DMZ, public Web DMZ) and as a result dozens or even hundreds of firewalls. For example, an energy company data center we reviewed had more than 20 DMZs, more than 200 different connections and more than 200 firewalls. While this sounds extreme, it is surprisingly common. Just as the single firewall/single Internet connection architecture can become unrecognizable with growth, a single DMZ architecture becomes unwieldy and unmanageable when multiplied to this extent. Data-center firewalls must segment and control traffic from hundreds of different external connections, DMZs, and server pools. Increasingly, they must do so at 10-gigabit connections. The performance and complexity challenges imposed by these requirements are staggering.

- **Virtualization.** Companies have readily adopted virtualization, which is now found in more than 90% of IT environments, to simplify and consolidate data centers. Server managers are consolidating servers into larger and larger virtualized pools of resources. Meanwhile, security architects, care increasingly collapsing and consolidating DMZs using virtualization. Within the virtualized pools, different levels of trust are no longer on separate networks, as they were in physically separated 3-tier networks. Instead, most companies use VLANs to keep virtual servers logically segmented. Firewalls in the core switches, the distribution layers and in the form of virtual appliances must manage traffic flows while maintaining logical segmentation throughout this complex architecture.

- **Growth and Scalability.** As companies consolidate data centers, they put more traffic on the data-center network. More storage protocols, more application data, more machine-to-machine traffic, more extranets, more VPNs and more partner connections all lead to the need for scalable firewall platforms that can grow to meet growing needs.

- **Clustering and Availability**. To address both growing scale and the need for high availability and business continuity, many companies are using clustering technology to link firewalls together. Clustered firewalls cannot only balance

the traffic loads but they can also increase availability by acting as a highly available active-active or active-standby pair. Because of consolidation, companies have put more and more of their assets into fewer data centers. That makes high availability a critical requirement for the core firewalls.

Evolving Firewall Requirements: In the Branch

- **Feature consolidation.** Key to a multi-function branch box is the need to meet throughput requirements with all features in use. Experience shows that when performance suffers too much, security features get turned off. It is likewise important that management of all features be meaningfully integrated. IT realizes little management improvement over a stack of separate boxes if a multifunction box has to be managed like a stack of separate boxes.

- **Central management and control.** In addition to each device being manageable as a single, integrated system, it is crucial that managing a broad deployment across multiple sites be easy from a central console. Security managers should manage their security policy and then extend and map that policy across all devices, rather than managing multiple devices separately.

- **Central reporting and log collection.** Branch office security devices are part of a companywide monitoring network. As such, they need to be able to efficiently collect logs and report back to a central location, such as a Network Operations Center (NOC) or Security Operations Center (SOC).

- **Scaling Down.** It is essential that devices be supplemented with virtual appliances and even soft clients, to accommodate micro branches and teleworkers.

Conclusions and Recommendations

As company networks have evolved, firewalls have been under pressure to meet new levels of performance, scale, availability, and application intelligence. In these new enterprise networks with virtualized data centers, distributed branch offices and roaming workers, firewalls must evolve to be more dynamic and reach further into the network than ever before. Companies must layer firewalls deeper into the network, offering ubiquitous security from the data-center perimeter, to the branch and reaching out to the endpoints.
