



## Network-Based Firewall: Extending the Firewall into the Cloud

---

By Ted Ritter, CISSP, senior analyst, Nemertes Research

---

### Executive Summary

Network-based firewall services (NBFW) are gaining momentum. By their location in the cloud, NBFW services offer advantages related to scalability, availability, extensibility, accessibility and maintainability. Also on the list of potential benefits are compelling cost advantages. Yet, the decision to move to NBFW is based on more than simple return on investment. It is also a trust decision. Achieving an acceptable level of trust comes through paying close attention to service level commitments, the credentials and references of the service provider, network infrastructure, and security staffing options.

---

### The Issue

Firewalls have been a mainstay of IT security for more than 20 years and their primary function, making inbound/outbound decisions on user and application data, is still the same. Of course, firewalls now offer packet inspection that supports the full protocol stack and policy enforcement/management that is light years ahead of the early days of access control list (ACL) as the primary control. Still, all of these changes are evolutionary. Revolutionary changes to firewalls are in management and location options, giving IT-security management a spectrum of choices: Do-it-yourself (DIY); on-premise outsourced management; cloud-based; and, hybrid. How does an enterprise choose one over the other? It turns out there are three key factors to address when making the choice: trust, staffing and cost. To frame this discussion it is best to compare and contrast the two ends of the firewall outsourcing spectrum: DIY versus cloud.

### The Drivers to Outsource Security Management

Every security team has one or more firewall specialist that spends time updating software, monitoring logs and tweaking rule settings for on-premise firewalls to continually manage risk by balancing openness with protection. For operations that manage 24 x 7, their firewalls teams may consist of six or more people.

In recent years, Nemertes has found a growing interest in outsourcing security management to third parties. More than half of benchmark participants in Nemertes' Security and Information Protection benchmark say they are already

using managed or carrier-based security services. (Please see Figure 1: Plans for Managed Security Services, Page 2.)

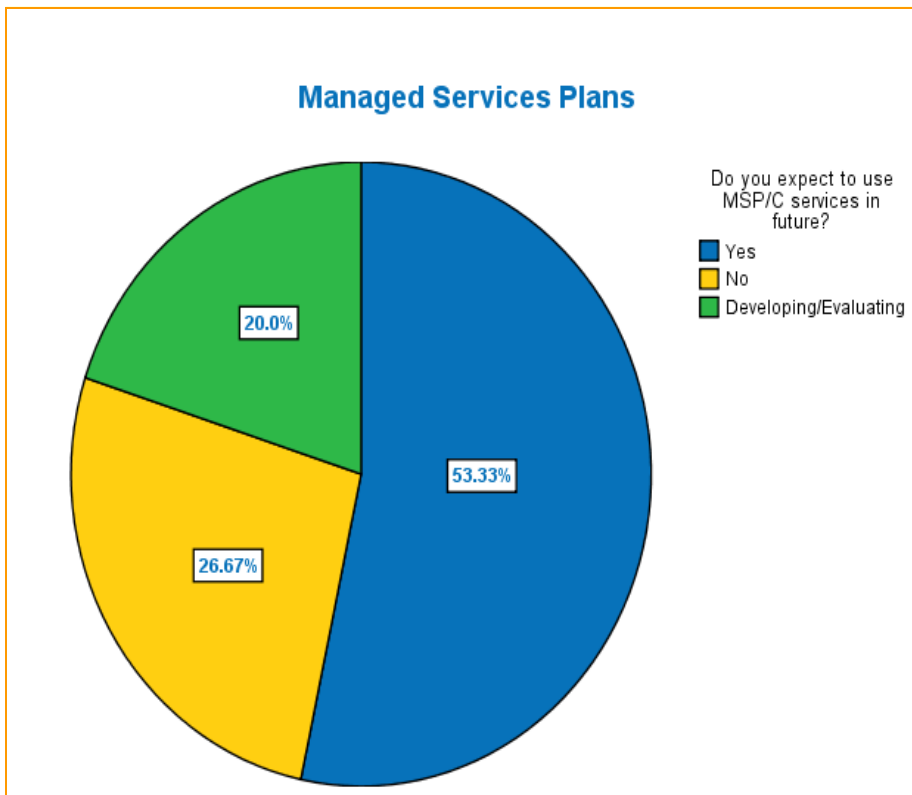


Figure 1: Plans for Managed Security Services

So, what's driving people to managed security services? Clearly, cost is a significant factor, and today's economic conditions will keep this issue top of mind for the next few years. A greater factor, though, is lack of skills. Even if organizations can afford staff, they can't find them. "The thought was that we could do it just as well ourselves, but it's been made abundantly clear that's not the case," says one IT executive from higher education, indicating why her organization is considering outsourced services. The next most commonly cited driver is availability of 24 x 7 support; both a cost and staffing issue. "I do require a little sleep. It's nice having people monitor 24 x 7 who have a clue—it's a wonderful thing," says the security executive for a financial-services firm.

The bottom line is that the lack of skills is the weak link, setting up a dilemma for information security management. Organizations that want to pay for a DIY firewall-management program may not be able to find the human resources to do so. And, organizations that can find the human resources may not be able to afford DIY firewall management. In both cases, organizations must evaluate

outsourcing firewall management and operations. In the first case, this requires a service that achieves the desired level of trust. In the second case, it requires finding a service that achieves the desired level of trust and shows a significant return. Let’s look at the investment return potential of DIY versus a managed solution, followed by the risk.

### Cost-Basis for Firewall Comparison

We modeled a simple network to illustrate the potential cost and staffing return with NBFWS versus DIY. Nemertes derives the numbers from extensive benchmark research of enterprise spending on equipment and services, as well as service provider pricing.

| Component             | Return       | DIY          | NBFWS        |
|-----------------------|--------------|--------------|--------------|
| One-Time Costs        |              |              |              |
| FW Appliance Cost     |              | \$7,500      |              |
| FW Installation       |              | \$375        |              |
| Annual Costs          |              |              |              |
| Annual FW Mgmt        |              | \$13,500     |              |
| HW/SW Support         |              | \$4,700      |              |
| M-F, 9-5 SOC (1 Seat) |              | \$90,000     |              |
| Annual NBFWS Fee      |              |              | \$68,580.00* |
| First-Year Total      |              | \$116,075.00 | \$68,580.00† |
| 1-Year Return         | \$47,495.00  |              |              |
| Second-Year Total     |              | \$108,200.00 | \$68,580.00  |
| 2-Year Return         | \$87,115.00  |              |              |
| Third-Year Total      |              | \$108,200.00 | \$68,580.00  |
| 3-Year Return         | \$126,735.00 |              |              |

Table 1: DIY Versus NBFWS Return

The baseline is a midsize, U.S. company with a data center in the U.S. with 5 Mbps of Internet connectivity, and 20 branch offices, each connecting to HQ via IP VPN service. We assume a 9 a.m. to 5 p.m., Monday through Friday security operations center (SOC) with engineers on call in the evenings, typical of many small to midsize business IT shops. We calculate one additional SOC seat for FW management.

The three-year return for NBFWS is estimated at \$126,735; a 38% savings versus DIY. (Please see Table 1: DIY Versus NBFWS Return, Page 3.) The NBFWS offers a 24x7 SOC versus the simple DIY example of M-F, 9-5. This is a significant

\* Annual NBFWS does include Internet access fees

† Annual NBFWS fee does not include costs for relationship and contract management



differentiator since a 24x7 DIY SOC seat would add \$450,000 per year to cover the five staff required.

This model assumes that the organization must invest in new firewall technology for DIY. The returns are still strong for organizations that already have firewalls. As discussed below, there are other factors to consider, including staffing and the unique characteristics of cloud-based security services.

### Network-Based Firewall

A NBFW can offer the same functions as a DIY firewall. Table stake features include access controls, stateful packet filtering, URL white listing, and network address translation (NAT). In addition, some service providers expand beyond classic firewall functionality to include a host of options, including distributed denial of service (DDoS), IDS/IPS, anti-virus, anti-spam and VPN.

More importantly, there are unique dynamics associated with NBFW because of its existence in the cloud. These include:

- ⊕ Scalability – The NBFW is a resource managed, maintained and scaled by the service provider. The service provider builds out the network and NBFW to support the service level agreement (SLA) with customers. As the business needs change, the service can scale accordingly in either direction. With DIY firewalls, the IT staff must manage the capacity and cost of the firewall.
- ⊕ Availability – Network service providers offer extremely high availability (> 99.99%) through an infrastructure with fully redundant power, HVAC, and network services and backup strategies in the event of a site failure. In contrast, DIY firewalls are only as reliable as the existing IT infrastructure, which may not be an issue at the data center but could be at the branch. High availability for the DIY firewalls is not in the pricing models above. Depending on manufacturer, high availability can double the cost of hardware, potentially increasing the three-year return by 6% or more.
- ⊕ Extensibility – NBFW is available anywhere the network operator can provide a protected communications path. Given that NBFW providers have trusted relationships with other network providers, the footprint of the service may extend well beyond the boundaries of the service provider's network. The DIY firewall may be at any corporate location, but not unless there is enough space or a necessary out-of-band management connection.
- ⊕ Accessibility - By nature, firewalls protect Internet egress/ingress. The example provided is simple with all remote sites connecting to HQ for Internet access. More complex networks require Internet connectivity at multiple locations, potentially requiring multiple



Internet service provider (ISP) contracts. The NFW model inverts the relationship so there is only one Internet connection regardless of the number of locations. The caveat is each location must be serviced with a secure connection, typically MPLS.

- ⊕ Maintainability –The NFW provider is responsible for firewall maintenance and support. DIY implementations require internal resources for maintenance—whether to resolve problems or manage a third-party company that provides maintenance services.

### Decision Factors for Network-Based Versus Do-It-Yourself Firewalls

There are some clear advantages to network-based firewall services. But there are other factors to consider. Moving into the cloud requires trust in the provider, the service and the ability to maintain the corporate risk profile. For the majority of IT executives that will consider NFW, there are some key points to meeting these objectives:

- ⊕ Service Level Agreement – The SLA must include guaranteed protection that meets the corporate risk profile. This requires technical, legal and risk management involvement.
  - The SLA must guarantee 99.99% availability.
  - The SLA must guarantee responsiveness that is in accordance with internal SOC standards. Response to potential attack should be within minutes, isolation and quarantine in less than one hour, and full resolution within four hours, for example.
- ⊕ Escalation procedures. It is critical that the escalation and notification procedures match internal SOC standards. This includes establishment of significant event-notification procedures (whether by email, phone, SMS), and escalation procedures in the NFW SOC. This can guarantee that the correct level of engineer addresses the organization's problems. We recommend integrating the corporate trouble-ticket system with the provider's event-notification system for better tracking of events.
- ⊕ Certification and Accreditation of the facilities and staff. Make sure the organization is certified for SAS-II, and know how many certified engineers are on staff: CISSP, CISM, or GIAC. Also, make sure any applicable compliance requirements such as the Payment Card Industry – Data Security Standard (PCI-DSS) are met.
- ⊕ References of other service provider NFW customers with similar requirements.

If these requirements can be met, the next decision is economics and resources.



## The Hybrid Factor

The relative value of DIY versus NBFW is directly proportional to the overlap between the NBFW reach and the organization's network topology. With 100% overlap, all the benefits of cloud described above come into play: availability, extensibility, accessibility and maintainability. The cost model shows significant returns for NBFW versus DIY, even with a simple network example. This becomes more challenging when there isn't 100% overlap, forcing the organization to either choose multiple NBFW offerings or a hybrid DIY/NBFW implementation.

A key issue is the benefits and disadvantages of choosing multiple NBFW offerings. Choosing multiple NBFW offerings can resolve the staffing shortage issue and may offer cost returns. The greatest challenge is the lack of continuous visibility and management because there are multiple NBFW SOC teams. This becomes notable in a distributed attack that targets the enterprise access points in both clouds. Also, this approach doubles the management burden. Finally, SLAs must be consistent between services: availability of service, rules of engagement, escalation policies, and guarantee of protection. By addressing these factors, the organization can decide whether multiple NBFW services are an option.

If multiple NBFW services are not acceptable, then one option is to redesign the network architecture and Internet access points to match with one NBFW provider. The other option is to deploy a hybrid – NBFW and DIY - solution.

The downside of a hybrid solution is it undermines the core value proposition of NBFW. The organization must still staff a SOC, and pay for equipment and operational expenses. If the enterprise needs to fully staff anyway, then why go with the NBFW at all? There are a number of points to consider:

- ⊕ **Staffing** – Most organizations have difficulty finding and keeping qualified security engineers, yet they still require 24x7 SOC operations.
- ⊕ **High Availability** – The real cost of high availability is not the doubling of the firewall cost, it is the underlying redundant infrastructure required to support it. If firewalls are co-located in main data centers, the infrastructure usually supports high availability.
- ⊕ **Firewall Upgrades** – All organizations today have some level of firewall on their Internet connections; even if it is router-based filters and ACLs. To keep up with escalating attacks companies must regularly upgrade their firewall functionality. Moving to a hybrid model facilitates upgrading some firewalls and replacing the rest in the cloud; thus mitigating a portion of potential DIY-based capital and operational expense.



## Conclusion

The decision to move to a NBFW is a multi-faceted decision. The gating factor is trust; trust in the provider, its service and its ability to maintain the corporate risk profile. This is a go or no-go decision. If it is a go, then the next step is to develop the SLAs and specific requirements that meet the corporate-risk profile. Staffing is a key issue to consider. If qualified security staff is not available, then a NBFW may be the only way to meet the corporate risk profile.

Multiple service providers offer these services. The best approach is to develop an RFP that explicitly states the locations, bandwidth requirements, and SLAs. With this approach, organizations may best determine if cloud-based firewall service is the right choice and which provider offers the highest level of service with the greatest return.

---

About Nemertes Research: Nemertes Research is a research-advisory firm that specializes in analyzing and quantifying the business value of emerging technologies. You can learn more about Nemertes Research at our Website, [www.nemertes.com](http://www.nemertes.com), or contact us directly at [research@nemertes.com](mailto:research@nemertes.com).