
# Standing at a security crossroads

## Deciding between do-it-yourself or network-based firewalls

Whether it's dealing with an increasing number of locations needing any-to-any connectivity, the challenge of managing widely dispersed firewalls, or keeping up with never-ending security threats, you may be at a crossroads: Do you continue on a "do it yourself" security path, or take a different road?

For many, that different road may lead to network-based firewall services, managed by a provider. But before making any decisions, it's important to weigh the options.

To help you make the right choice for your organization, and to understand the factors driving these decisions, we consulted with Imre Solymosi, Associate Director and Product Manager for firewall technology at AT&T.

**Q: Imre, it might be helpful to start with a description of what is meant by a "network-based" firewall service.**
A: Sure. You may have also heard network-based firewalls referred to as cloud-based firewalls or security-as-a-service.

Basically, it is a fully managed firewall service that helps protect your network by providing secure inbound and outbound Internet access through security gateways. Rather than having the firewall reside in a traditional on-premises solution, network-based firewalls are deployed in the service provider's cloud infrastructure.

**Q: What are the most common reasons customers are thinking about moving away from a do-it-yourself solution?**
A: Sometimes, they've had a bad experience with their existing firewalls. It may have been an attack or some other security event that left them exposed to a financial or legal risk. Or, there could be a shortage of on-staff professionals, which makes it hard to handle the growth of firewall threats, like malware or botnets, and to keep firewall devices and policies updated.

When it comes to protecting your business, it's not just a decision about firewalls. It's a decision about how firewalls fit into your overall security strategy.

Another factor may be that they want to evolve their security solutions to add new functionality, such as application control, but their firewall devices aren't equipped to handle it. In that situation, there may be no way to introduce that new functionality into their on-premise security infrastructure without making a large capital investment.


Imre Solymosi, Associate Director and Product Manager for firewall technology, AT&T

**Q: So, cost is also a big factor in the decision process?**
A: Yes, especially now, when IT budgets are being so closely watched. Upfront capital costs for equipment and on-going software and hardware maintenance fees can drive up the costs of deploying or expanding onsite firewalls to more users or locations.

With network-based firewalls, there's no need for you to buy or install additional devices onsite, or to invest in a staff to maintain and troubleshoot them around the clock. You subscribe to a firewall security solution, rather than buy a firewall device. It becomes a predictable operating expense.

There can also be a costs savings when it comes to resiliency. Instead of duplicating your own equipment, facilities and network connections to guard against denial of service or other attacks, you can choose a provider that offers a fully redundant infrastructure.

**Q: How does a firewall service improve how customers can keep on top of new threats?**
A: When customers manage their own firewalls, they have to be equipped to track and prepare for the latest security risks and trends. They also need a way to filter out potentially harmful threats from the hundreds that attempt to break into their network everyday.

The trouble hits when they can't do this because they are short-staffed, or because people are on vacation or out sick. But threats don't wait; there are security cases that need to be worked every day. And it's not just a matter of dealing with new threats. Many of the oldest, well-known viruses and worms are still very active.

Firewall service providers have highly specialized staffs devoted to updating devices and policies and to monitoring, analyzing and managing threats on a 24x7x365 basis – and that's included in your subscription.

**Q: Can customers apply their own security controls and policies?**
A: Yes, customers put a lot of thought and work into defining what their security policies should be to meet their specific needs, from both a business and compliance standpoint. A firewall service provider should offer the flexibility to configure your firewall service to support your policies and to change policies and configurations as you need to.

If you have multiple locations, network-based firewall services can also make it easier to deploy consistent global or region-specific security policies. You can add regional, cloud-based firewall locations – and without the need for localized security staff or bringing all traffic back to headquarters.

**Q: How much flexibility is there to add new features or functionality?**
A: Your ability to deploy new security features and capabilities with on-premises firewalls is often limited by the staff you have on hand to implement, update and support them, as well as capital constraints.

With network-based firewalls, you can "turn on" the features you need with the speed and efficiency of any cloud service. So, it's much easier to add the security solutions you need – like intrusion detection, malware scanning, web filtering or application controls. This means you can increase protection more quickly, which is important since the threat landscape is always changing.

**Q: Any other thoughts about easing the decision process?**
A: Realize it's not an all-or-nothing decision. For example, AT&T offers managed firewall services that are network-based, but we also offer a premises-based firewall service. We can help you design a hybrid solution that leverages both your existing on-site devices and solutions and our managed security services.

It's also helpful to work with a provider with an end-to-end approach to security. Because when it comes to protecting your business, it's not just a decision about firewalls, it's a decision about how firewalls fit into your overall security strategy.

If you're looking for the network-based firewall solution that's right for you, read *Simplifying your Search for a Network-Based Firewall.*

Find out more about AT&T Firewall Services, including Network-Based and Premises-Based managed firewall services.

Share this with your peers

For more information contact an AT&T Representative or visit www.att.com/firewall-security.

09/19/13 AB-2783