The complete approach to data center security?

Poll reveals that it is time to replace piecemeal security tools with a comprehensive enterprise solution.

Preparing to really push the virtualization envelope? Check!
Readying an aggressive cloud strategy? Check!
Gearing up to embrace mobility and consumerization of IT? Check!
Having a datacenter network capable of securely supporting all this? Maybe not.

Data centers have become the hub of business activity for many organizations as applications are deployed that can help them quickly gain a competitive edge. Virtualization, private clouds and mobile computing are providing the agility, flexibility and scalability needed to make the fast, informed decisions that enable quick responses to business conditions.

JUNIPER NETWORKS

CIO Custom Solutions Group

This growth brings major security concerns, though. A recent *CIO* Magazine Custom Solutions Group survey by IDG Research shows wariness among respondents about being able to protect business-critical data in the cloud computing environment. Almost half say they are only somewhat confident that they can provide adequate security in this arena.

At the same time, CIOs know that their current security technologies are due for a refresh. For instance, 52 percent say that mobile device security needs to be reconsidered. Almost half—49 percent—report that IPS and access control measures are out of date in their organization. Just a slightly smaller number, 44 percent, claim they need to install new firewalls, and 41 percent are looking at revamping protections for servers and storage. Their concerns map closely to what is known about emerging threat vectors cropping up in mobile, virtual and cloud environments.

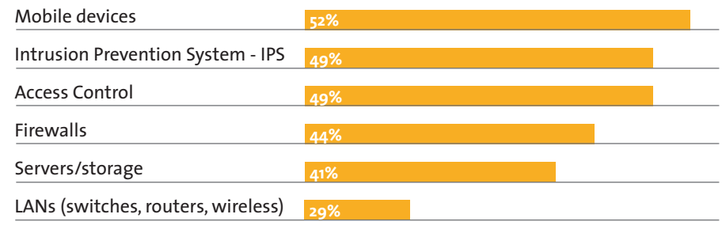
Juniper understands that threats can mean more harm if security devices are kept separate from one another and that has guided the design of the SRX gateway. For instance, if organizations have to deal with multiple products and multiple consoles that can't communicate, they can't apply consistent policies to virtual machines, mobile devices and data in the cloud. This leaves holes that can lead to a data breach, leakage, and compliance and reporting issues.

"You never want security to become the bottleneck. Otherwise, management will start making trade-offs in which some systems might not get protection because the performance hit is unacceptable," says Peter Lunk, director of product marketing at Juniper Networks.

Scaling reveals security holes

The simple fact for CIOs to grasp is that traditional data center security solutions do not make managing security as a whole an easy proposition. Instead, because they involve multitudes of hardware and software products, you have to monitor numerous consoles and develop specialized skills for each product. And, those are characteristics that are untenable for budget-conscious organizations that are trying to consolidate while operating with a limited staff, or that simply see complexity as an effective enemy of good security.

What types of security technologies or capabilities in your network need to be refreshed?



Source: IDG Research, April 2011

In a virtual environment it is critical for IT to maintain control and uniformly deploy corporate security policies across the organization to ensure business continuity. Extending this complexity to virtual environments, makes it nearly impossible to gain the visibility across the enterprise required for proper end-to-end data protection, reporting and compliance.

The survey shows further that rather than targeting one area, a majority of organizations—55 percent—are investing in a handful of solutions that secure applications, the network and content.

"Businesses can't support the sprawl of individual security products. They want a holistic solution that addresses all these areas—network, application and content security—to simplify management and improve visibility," says Lunk.

Juniper Networks' SRX Series high-performance, scalable security services gateway integrates firewalls, virtual private network (VPN), application security, content filtering, IPS and other tools into a single product. Its high port density, chassis-based form factor is four to five times as fast as the leading competitor and is engineered to reduce security overhead.

With this all-in-one, full-featured gateway, Juniper has solved the problem of patch worked network security.

Juniper Networks' holistic security solution

The Juniper SRX has been engineered from the ground up to ensure maximum protection that is transparent to the user. With SRX, security is never the bottleneck. For example, packets are opened once and then passed along to the appropriate area for inspection. "Once a packet is opened and decoded, each security service—IPS, firewall, and so on—can read it," Lunk says. Potential logjams are eliminated, enabling IT to secure all systems instead of having to prioritize.

Juniper's fully integrated firewalls and IPS systems can also correlate events and take action to stop threats. Network and mobile researchers are constantly working behind the scenes to look for new attack vectors and share that data so that security defense can be automatically coordinated in a unified manner. "This level of information sharing and visibility is unprecedented and leads to better protection," Lunk says.

As new threats continue to surface in the data center and throughout the network, choosing consolidated systems with the scale to address all aspects of security is a smart decision that will simplify data protection. The SRX promotes visibility and end-to-end control, which leads to improved compliance and reporting. Policies can be created, applied and enforced within the SRX across virtual, cloud and mobile environments. By employing a single multifaceted security product, deployment and management of concurrent services becomes much easier and enables data centers to remain lean. The SRX supports the common data center mission of fast and consistent service quality regardless of user location.

With all these attributes, it's clear that Juniper Networks is the strategic partner IT executives need for help in rolling out innovative features and gaining optimal performance.

"YOU NEVER WANT SECURITY TO BECOME THE BOTTLENECK. OTHERWISE, MANAGEMENT WILL START MAKING TRADE-OFFS IN WHICH SOME SYSTEMS MIGHT NOT GET PROTECTION BECAUSE THE PERFORMANCE HIT IS UNACCEPTABLE."

— Peter Lunk, director of product marketing at Juniper Networks

To read more about Juniper Networks, click here.

2000417-001-EN