

Mass High Tech: The Journal of New England Technology - May 8, 2006
<http://masshightech.bizjournals.com/masshightech/stories/2006/05/08/focus2.html>



Security or shutdown?

Pick the right level of security to protect your network

Mass High Tech: The Journal of New England Technology - May 5, 2006 by [Dave Dubois](#) Mass High Tech
News reports about network security breaches have become commonplace. Accompanying these reports is usually a staggering price tag for network down time, lost productivity, lost revenue and in the case of compromised customer data, loss of customer trust. Each time business leaders and IT professionals read one of these reports they probably ask themselves, "Exactly where on the security spectrum should my organization be?"

If you choose the "belt-and-suspenders" approach and install the most impregnable -- and usually most expensive -- security devices, you may lock up your network so tight that you cripple productivity. Choose the low end of the security spectrum and your employees may be more productive, but it's probably just a matter of time before you're hit by a potentially catastrophic security breach.

The right security posture for your network doesn't have to be an all-or-nothing proposition. Securing your IT infrastructure doesn't mean you have to install chokepoints so one or more devices can perform deep, intensive inspection of every single data packet that traverses the network. The best way to maximize network security without smothering performance is to distribute policy enforcement across the entire network. Policies, which can be tailored to meet your company's specific needs, are rules that tell the network how to treat individual users, types of traffic, devices and more.

Most network experts agree that it's unwise to rely solely on perimeter security devices such as firewalls. In the same vein, it's unwise to only enforce policies at certain points of the network. Ideally, policy enforcement should occur on the routers and switches deployed across infrastructure. Attacks can come from virtually anywhere, inside or outside your organization. With a granular, policy-based approach to security, policy decisions can be made across all the ports on a network at the same time the packets and flows are being controlled by the infrastructure devices.

For cost-conscious businesses, it's possible to deploy inexpensive Layer 2 switches at the edge of the network and larger, more feature-rich switches at the distribution layer for effective policy enforcement. With either architectural approach, policy enforcement is spread across many devices. This avoids bottlenecks that can easily develop when all data packets have to travel through the same security checkpoint to ensure they do not contain viruses or other threats. With this approach, not only does your business take advantage of the best approach to network security, it also eliminates the cost of purchasing and configuring specialized policy-enforcement hardware. Centralized policy deployment also makes the entire network easier to manage.

At most companies, people perform a variety of jobs and have different requirements for network connectivity and varying levels of access to customer data or proprietary information. Therefore, the best approach to network security is to enforce policy using highly granular rules on a per-user basis. You need to ensure that your employees have access to the network services and data they need to do their jobs, while also ensuring that malicious attacks or unauthorized access to sensitive information are prevented.

Configuring this level of user and device granularity using traditional DOS or Unix line commands is impractical. Customizing all the different user roles and associated policies would be time-consuming and very expensive. Tools exist today that can abstract highly complex, role-based policy into easy-to-use drag-and-drop commands. These represent the best value when adopting a distributed infrastructure-based policy enforcement model.

The management tools that create and distribute policy should ideally use a client-server model that can scale to the largest enterprises to ensure easy migration as an organization expands. Another benefit of a highly scalable management tool is that role-based policies can be made consistent and repeatable throughout the network. This approach makes reporting more effective as well. Reports can show the overall state of a network, or they can pinpoint certain areas of the network for further analysis.

Network architectures that integrate security directly into the infrastructure are less expensive to acquire, deploy and manage. They eliminate the need for expensive

specialized security devices, and because policy enforcement is distributed across the enterprise, network performance isn't dragged down and you can get more done with a smaller IT staff.

Dave Dubois is vice president of product marketing and product management for Andover-based Enterasys Networks Inc.

[Contact the Editor](#) [Need Assistance?](#) [More Latest News →](#)

[Subscribe or renew online](#)

All contents of this site © American City Business Journals Inc. All rights reserved.