

Who Goes There? An Introduction to Policy Networking

High-speed broadband, remote and wireless access to company networks can help boost business productivity, but they also make IT systems vulnerable to attack. Scan the headlines of any IT journal and it's obvious that network security is a hot topic for many businesses. If companies aren't motivated to protect their data centers, compliance regulations—like Sarbanes Oxley, HIPAA, and GLB—are reason enough to take action.

The growing awareness of network security threats have businesses looking for outside help to solve their network security challenges. In fact, Yankee Group analysts have identified outsourced security services as one of the fastest growing segments of the service provider market.

As a Managed Service Provider, what can you do? We already know firewalls and password protection don't cut it. They aren't enough to keep hackers, disgruntled employees and self-propagating attacks at bay.

This short article will bring you up-to-speed on the next generation of security technologies that can help lock down your customers' networks more effectively.

Policy Networking, What is It and Why is It Better?

Policy networking is the industry's most sophisticated network security strategy. It's the overarching theory for the technologies discussed below. Simply put, policy networking regulates who can access private computer networks based on policies defined by a business.

In a perfect world, a policy-based network:

1. Defines identity and trust policies for an organization. These policies define who gets access to the corporate network.
2. Stores the identity of every user in a directory.
3. Authenticates a user's identity before allowing them to access the network.
4. Compares the user's computer to the network's software security policies to make sure the computer joining the network has up-to-date virus protection and won't infect the corporate network.
5. Provides connectivity depending on the user's identity and system profile. For example, if the user only has permission to access email, then they won't be able to retrieve billing data or certain software applications.

Policy networking is currently regarded as the most effective way to secure networks. That's because it initiates more rigorous authentication controls than password protection, and also attempts to protect networks from virus-laden devices.

SSL VPNs: Balancing Remote Access with Security Concerns

The work-a-day world has changed considerably in the last decade. Today, many users exist outside the company building—they access data and applications from other offices, from home and from

around the world. This shift in work culture gives workers more flexibility, but opens a can of worms when it comes to network security.

A popular remote access technology that goes a long way to balance demands for anytime/anywhere access to corporate software applications and data with concerns for privacy and infrastructure protection is the Secure Sockets Layer (SSL) VPN.

Originally developed by Netscape, SSL has evolved into one of the leading security protocols on the web. SSL supports millions of online transactions daily and is the de facto standard for secure online credit card purchases, stock trading and banking.

By using an SSL VPN to deliver company software applications to remote users (or in-house users), you can control who has access to specific applications by setting-up authentication policies.

One reason SSL VPNs have become popular with Managed Service Providers, is because they are typically fast and cost-effective to set-up. They are often easier to manage and maintain than traditional IPsec VPNs. For example, you don't have to configure each company computer or laptop to remotely access company data and applications. Instead, an SSL VPN lets any computer with a standard Internet connection automatically connect to a company's server and access data and applications based on the users' policy networking credentials.

Network Admission Control: Putting Policies in Place

Unless you've been living under a rock, you've read or heard about Network Admission Control, or NAC. In essence, NAC:

- Enforces security policies, and restrict prohibited traffic types
- Identifies users or devices that break rules or are noncompliant with policies
- Stops and mitigates malware and other threats

In other words, NAC appliances quarantine devices (laptops, home computers, handheld PDAs) trying to enter the network that don't meet system health requirements. NAC helps keep viruses and malware out of the corporate network.

Identity-Based Security Gateways

A close cousin to NAC, identity-based gateways sit in front of software applications being protected. They're similar to firewalls, but include user identity information in IP packets to track that only authorized users are gaining access to the applications.

ID gateways are designed to protect hyper-sensitive data and applications while still letting users access certain information based on policy networking authentication profiles.

A benefit of identity-based security is that it provides network managers with a way to track who accesses the network, what they see and which applications they use. This kind of technology is especially useful for businesses trying to meet corporate governance regulations.

Why Does This Matter to MSPs?

With more pressure on businesses to lock down their networks, MSPs have an opportunity to meet the demand. Next generation network security technologies—SSL VPNs, NAC and identity-based gateways—could be the answer for your customers.

Reginald Best is Chief Operating Officer of network security company AEP Networks. As an engineer and entrepreneur, Reggie has pushed the boundaries of network technology for almost 30 years. AEP Networks provides organizations with comprehensive policy networking computer security solutions.