



Network Access Management: Moving from Implicit to Explicit Permissions

A Vernier Networks White Paper



Vernier Networks, Inc.
490 East Middlefield Road
Mountain View, California 94043

www.verniernetworks.com

Introduction

The explosion of fast, reliable network connectivity in the form of the Internet and the enterprise LAN over the last 20 years has transformed the world of business, creating new opportunities and making organizations fast, agile, and efficient. The challenge for corporate IT departments is to meet the ever increasing demands of an “always connected” user base that includes employees, partners, and customers, while keeping networks and the intellectual assets they carry secure.

Unfortunately, the combination of powerful, portable end users computers and the corporate dependency on networks for mission-critical operations is challenging traditional models of security. Threats are no longer isolated to a few attacks launched from outsiders, but may originate from our most trusted employees. Viruses, worms, “Warhol worms,” Trojan horses, DoS attacks—the range and number of attacks that can be launched from within the security perimeter are multiplying at a bewildering rate. While staving these off hostile attacks, network managers are also responsible for enforcing a host of other security policies, ensuring that users do not misuse network resources, wrongly distribute intellectual assets, or violate industry regulations.

With the frequency and severity of attacks increasing, and organizations relying increasingly on networked automation to gain a competitive edge, is it finally time to reconsider the prevailing approach to network security? How can corporations ensure that users get the network access they need, without jeopardizing the security of the network?

Connectivity versus Security

Optimizing network access in terms of connectivity and security is a classic case of balancing what are essentially opposing goals. Security is optimized by lack of access; connectivity is optimized by complete access.

In the design of the enterprise LAN, these optimizations lead to two different philosophical approaches. For *optimum connectivity*, we design a completely open network and then react to security concerns by selectively closing down areas of access. For *optimum security*, we design a completely closed network and react to connectivity requests by selectively opening areas of access.

Each of these approaches has merit. The choice between them really comes down to a simple decision of priorities. Historically, organizations have based this decision on the degree to which they trust their users. Organizations typically trust users who are located within the physical confines of a facility and optimize their network for connectivity. Thus, employees and welcome guests are often given convenient, unfettered access to the network. Organizations typically distrust users outside their facilities. These users typically have to take more steps to authenticate themselves, and their access may be limited to certain resources and certain access technologies, such as VPNs. Network access for these outsiders is optimized for security, at the expense of connectivity.

Trust Boundaries

IN BOTH THE
PHYSICAL AND
VIRTUAL WORLDS WE
IMPLEMENT
SECURITY SYSTEMS
AND PROCEDURES
AT THE DISTINCT
POINTS WHERE TWO
DIFFERENT TRUST
ZONES MEET.

It is not practical to implement the highest levels of security at every location for every type of user at every moment; instead we generally apply strict security measures at “trust boundaries.” **In both the physical and virtual worlds we implement security systems and procedures at the distinct points where two different trust zones meet.** For example, the boundary between an organization’s physical plant and the public domain is typically secured by doors, which can be locked, and by security personnel. In the enterprise LAN, the boundary between the LAN and the Internet is protected by security products such as firewalls. Data communications with remote users are secured by a digital boundary—a VPN tunnel—that separates trusted communications from the untrusted public channel through which the data is traveling.

In recent years, many IT departments have created an internal trust boundary where the LAN meets the data center. Using a combination of firewall and application access management technologies, this boundary strengthens the protection of critical computing and storage resources in recognition of growing exposure to internal risks presented by viruses, worms, non-employee users, etc.

One result of relying on firewalls and VPNs for trust boundaries is that the boundary configurations tend to be static. Even though security conditions may be changing rapidly (for example, because of different users logging on and off the network and because of viruses and worms appearing at new locations), the trust boundaries themselves rely on low-level rules and ACLs that can only be modified by a network administrator who has sufficient time and expertise.

The Threat from Within

Most IT departments are now aware of the internal security threats represented by worms, viruses, and other types of malware. The statistics are sobering: According to IDC, over 60% of all serious security threats come from internal users, including employees, partners and vendors. Mobile users who fail to apply the latest security patches to their laptops are re-infecting networks with worms and viruses and unleashing Trojan horse attacks.

In response to these threats, network managers have taken initial measures to protect their data centers from internally launched attacks. The situation is too complex, however, to be solved by creating yet another boundary, this time between the data center and the enterprise network. The attacks can just as easily wreak havoc on operations by ignoring the data center and destroying the network fabric itself.

WHEN ATTACKS
SUCH AS THE
SLAMMER WORM
CAN INFECT 75% OF
VULNERABLE HOSTS
WORLDWIDE WITHIN
15 MINUTES,
CORPORATIONS
CANNOT CONTINUE
TO RELY ON STATIC
SECURITY
ARCHITECTURES AND
OSSIFIED ACCESS
POLICIES TO
DEFEND AGAINST
SECURITY THREATS.

To protect both the network and the business operations that rely on the network, an additional trust boundary must be erected between the network and the user. In addition, boundaries must be created to prevent the propagation of threats from one user to another. Security measures must ensure that a user with legitimate access to resources does not inadvertently enable malware to reach those resources, taking advantage of the user's security clearance to propagate an attack.

The Emergence of Explicit Permission and Network Access Management

All of these changes in the security threats facing the enterprise are causing a series of changes in how aggressively we must protect our infrastructure. Attack mitigation is now discussed in terms of "zero hour" response. When attacks such as the Slammer worm can infect 75% of vulnerable hosts worldwide within 15 minutes, corporations cannot continue to rely on static security architectures and ossified access policies to defend against security threats.

Two changes are necessary to provide the network security corporations need.

First, IT organizations must change today's network access model from one of implicit permission to one of explicit permission. Network access must be adapted to each user's logon attempt. Users must be given personalized access to (or "views of") the network with explicit permission to the resources they can use. Only with this more precise permissions model can IT departments begin to reduce the potential damage from rapidly spreading viruses, worms, and Trojan horses.

Second, this explicit permission must be managed through an appliance that grants or denies access based on a real-time assessment of security requirements, network status, and user status. In contrast to static rules and fixed policies, an adaptive security solution would evaluate each user's network access on the basis of parameters such as:

- User ID and group ID
- Time of access
- Location of access
- Security status of the user's device (infected vs. clean)
- Threat status of the network (whether the network is under attack, nature of the attack, etc.)

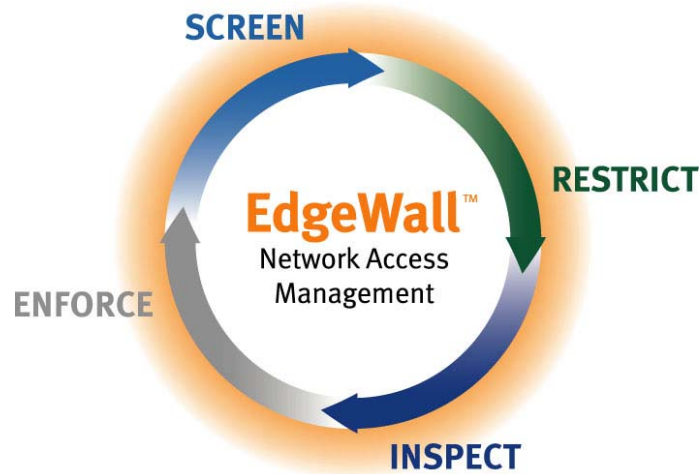
Network Access Management for Business Continuity

To deliver services and run daily operations, corporations rely on today's fast networks and powerful computing devices. By acknowledging the complex, ever-changing relations of users to these networks and to other users, IT departments can begin working from a more precise and constructive security model based on 1) explicit permissions for users accessing resources, and 2) adaptivity to changing conditions. Using this model, corporations can benefit from the speed and connectivity of the wired world without succumbing to the threats and attacks that can make that world so perilous.

The Vernier Networks' Approach

The Vernier EdgeWall uses enforcement systems distributed at the access edge to secure both wired and wireless access for users with all type of devices. These edge enforcement systems protect both the data center and the LAN itself in a naturally scalable and affordable manner. With its interfaces to additional security verification systems, such as patch management and vulnerability assessment systems, and its unique ability to dynamically steer suspicious or sensitive traffic to additional processing and/or inspection systems, the Vernier EdgeWall provides the missing link in typical "best of breed" security implementations: integration.

Vernier's EdgeWall is a NAM appliance that is deployed at the network edge within the switching fabric and provides comprehensive network access management to defend against intrusions and attacks on the network. EdgeWall's NAM offers 4 key access management functions:



- **Screen:** The Vernier EdgeWall screens the user and device to assure they are authenticated and clean of viruses and worms.
- **Restrict:** The Vernier EdgeWall restricts network access to only those resources the user is authorized to use.

- **Inspect:** The Vernier EdgeWall continuously inspects traffic from client devices to defend against worms/viruses and unauthorized sessions.
- **Enforce:** The Vernier EdgeWall enforces policy to assure user and device compliance.

The Vernier EdgeWall is the industry's first NAM appliance that enables businesses and organizations to assure continuous, secure network availability on their wired and wireless networks.

About Vernier Networks, Inc.

Vernier's EdgeWall is a network access management (NAM) appliance that is deployed at the network edge and provides comprehensive NAM to defend against intrusions and attacks on the network by screening users and devices, restricting access, inspecting traffic for worms and viruses, and enforcing access policy. Complementary to firewalls, which are deployed at the perimeter of the network to protect the corporate network from intrusions from the Internet, EdgeWall NAM appliances are deployed at the network edge to protect the network from intrusions from endpoints without disrupting network performance.

Vernier Networks products are distributed direct and by a network of strategic OEMs and Value Added Resellers and deployed at over 300 customers, worldwide. The company is headquartered in Mountain View, CA and has sales offices in Europe and Japan.

For more information, visit the Vernier Networks Web site at: www.vernietworks.com or contact a Vernier representative at info@vernietworks.com