

Bridging the Insider Security Gap with Network Identity Enforcement

By Dave Shay

info@trustednetworktech.com

For the past decade most security professionals have focused on defending the perimeter of their network. As they deal with an increasingly hostile and regulated environment, it is clear that this strategy alone is not effective for today's highly interconnected enterprises.

Security professionals have done their best to solve the problem with tools at hand, deploying perimeter security technologies on internal networks. While this has reduced some of the risk, those technologies were never designed to secure internal corporate assets. This approach is much like driving a nail with a screw driver—it's better than nothing, but you'll be more successful if you use a tool specifically designed for the job.

Solving the internal problem with traditional challenge and response solutions has the same drawbacks as moving perimeter solutions to internal networks. It's no wonder companies are finding current solutions to be less than effective and are rethinking protection strategies for their internal networks and critical assets.

Mark Bouchard, security program director at Meta Group, comments in his recent white paper on securing internal networks that despite significant investments in perimeter security, successful attacks continue to rise. He concludes that for security to be effective, additional perimeters will need to be established closer to the resources that are being protected. Perimeter-oriented security strategies, he notes, are no longer sufficient.

While this is a step in the right direction, security professionals and vendors may be able to create a better long-term strategy if they are willing to evaluate the effectiveness of their existing internal enterprise security and incorporate emerging innovative solutions that leverage the existing IPv4 protocols by attaching an identity at the packet level.

The Escalating Challenges of Securing Internal Networks

Corporate networks were fairly secure 30 years ago when applications ran on isolated systems using proprietary protocols. Corporate networks today are highly interconnected through TCP/IP, an inherently insecure and identity-blind protocol. User access options have also evolved dramatically over the years. You can no longer assume that insiders are "trusted" because this group often includes a mix of business partners, investors, consultants and customers. Even if you trust everyone on your internal network, the risk remains, since most vulnerabilities are a result of carelessness rather than intentional misuse. Thus, we face a wide variety of challenges around controlling access to and protecting internal network assets.

The proliferation of mobile devices connecting with corporate networks, IP telephony, and blended threats exploiting multiple avenues of attack are also changing the way security administrators deploy security inside their networks. The expanded use of wireless and wired IP-based

phone systems means that business or emergency services for hundreds or thousands of people could now be impacted by data network attacks. Hackers and identity thieves view handheld devices as prime targets because they offer a wide range of phone, Internet and data access functionality coupled with wireless connectivity to corporate networks.

Existing wireless security options are only minimally effective because they are largely disconnected from wired networks and applications. Until organizations can provide a secure means to access their private networks and applications from wireless devices, many are delaying deployment within the organization or outright banning these devices on their networks.

These issues are well known and sometimes frustratingly obvious, so why do they remain unsolved? One possible reason is that they are really just symptoms of a broader and less understood problem. As long as systems are allowed to connect before any strong application layer authentication can occur, TCP/IP will remain vulnerable to attack and misuse. Existing technology may reduce the risk, but it's clearly not enough to solve this problem. A solution will likely depend on new technology that is specifically designed to address this redefined problem without sacrificing interoperability with legacy applications, systems and networks. Either way, securing internal network assets will continue to be a struggle as long as the security community is given tools that address the symptoms rather than the underlying cause of ever-increasing internal threats.

What Isn't Working

IT organizations are in a difficult position, caught between the need for increased productivity and flexibility and secure access to critical assets. Because there are few options for securing internal corporate networks, many organizations have spent significant time and money deploying traditional, perimeter-based firewalls and IDSs to protect critical internal systems and applications. Increasing incidents of corporate breaches, however, leads to the conclusion that this approach does not work.

Firewalls, no matter how well they are implemented, aren't meant to stop everything. Effective deployment is a challenge that often involves incorporating a combination of a perimeter firewall with a Radius authentication server and tokens or smart cards for two-factor user authentication. While relatively effective at the perimeter, this solution is often considered complex, bandwidth-consuming, and too high a TCO for implementation inside corporate networks. In addition, most major corporations use DHCP and NAT, making the rule sets extremely complex if not impossible to maintain at the granular level needed to protect user access to applications. This is in addition to the cryptic rules that must be maintained on the Radius server. The network performance associated with such a setup,

especially for full stateful inspection firewalls, is generally considered unacceptable beyond the perimeter.

Worse yet, firewalls and IDS are identity-blind, operating on IP addresses that change frequently for most users and are easily spoofed by attackers. The identity-blind nature of IDS and the fact that legitimate users often act unpredictably cause excessive false positives and security event overload, forcing many organizations to use IDS sparingly and often only on the perimeter. This fact alone has prompted a thriving market for identity management and enterprise security event management in an attempt to provide better tools for security professionals to manage access rules and an overwhelming quantity of alerts. Unfortunately, because internal networks are comprised of many more systems, applications and protocols than are present at the perimeter, IDS and firewalls are too costly and complex to implement and manage across the enterprise.

Stronger forms of authentication such as tokens and smart cards work well in certain circumstances, but have their own cost, complexity and effectiveness issues. They are often perceived as remote access solutions because implementation and management issues make them impractical for controlling access all the way down to the application.

Despite their weaknesses, most corporations continue to rely on passwords as their key method for protecting systems and data on internal networks. Passwords, however, are easily compromised, and their limits as an authentication mechanism are well understood. In addition, passwords authorize access at the application layer only, and as an audit mechanism, they can't be trusted to prove compliance.

IPv6 and IPsec were designed specifically to solve the lack of privacy and weak authentication in IPv4, but deployment has been significantly slower than anticipated. While IPv6 with IPsec is probably the best solution technically, the deployment challenges and costs have prevented widespread adoption. One of the key challenges has been the lack of interoperability between legacy infrastructure and IPv6.

While there are a variety of options to transition from IPv4 to IPv6, many security professionals report that a gradual transition is painful and often impossible. Most large enterprises have a mix of old and new infrastructure and few can justify the cost, downtime, or resources necessary to upgrade or replace their entire infrastructure to support IPv6 at once. The only remaining option is to do what many enterprises have done and restrict implementation of this technology to small, extremely high-risk segments of their network, leaving them to secure the balance of their internal assets some other way.

Identification for Deeper Authentication

While it sounds obvious, knowing who is on your network can be your greatest advantage in the quest to secure corporate networks, systems and applications. Traditionally equated with authentication, identifying who should be on your network is the cornerstone of the increasingly important identity management movement.

There is, however, a weakness in traditional "challenge-response" authentication. Authentication is the act of introducing, verifying and registering an identity, but only when someone logs into a system or connects to a domain-controlled network. Once logged on, a user can access almost any system or application on a network with little or no challenge. Even if the application requires passwords, which are easily compromised, there's rarely any link to the authentication credentials. This emphasizes the disconnect between network or port level access control and application access. In addition to the inherent security weaknesses in TCP/IP, determining who users are and where they can go at the packet level on a private network is a real challenge.

Unlike authentication credentials, a true user identity must stay with that user from system logon to port-, or network-level access, to application access. Not only does this provide coherent authentication and identification of users across networks, but it provides the means to truly audit where users go without trying to correlate changing IP addresses across time and network boundaries. By attaching an identity to every session at the packet level, security administrators can prevent unwanted access and unauthorized use and manipulation of corporate assets and data.


Consider the following analogy to explain the distinction between authentication and identification. Imagine entering a public building complex. You walk into the main office building, for example, and present your credentials—driver's license, passport or ID card—to the security guard. This is authentication. Once your credentials are verified, you are given a visitor's badge that is encoded to allow access to only those buildings, offices or elevators that you are authorized to enter. The visitor's badge allows other people, guards and sometimes electronic devices to control and monitor your access throughout the complex. The visitor's badge acts as an identity that stays with you wherever you go in the building complex and can provide an audit trail of your access.

Protecting Internal Networks by Enforcing Identity at the Packet Level

The need to create secure private networks is more pressing than ever. Traditional methods cannot accommodate this demand coherently across system-, port-, network-, and application-level access. Fortunately, innovative solutions are emerging that leverage the existing IPv4 protocols by attaching an identity at the packet level that can't be spoofed, hijacked or stolen, ensuring that critical assets such as customer and financial information is secure.

Because network-layer protocols persist as communications traverse networks and applications, enforcing a digital identity at the network layer can tightly control and audit how data is allowed to be passed between systems. In effect, the end result is an identity-based firewall that no longer relies on transient and unreliable credentials like source IP address. Such a strategy goes well beyond perimeter firewall-level controls by actually providing strong user authentication that is maintained at the TCP/IP level and can easily be extended to applications and systems. Essentially, you have perimeter firewalls for public-facing networks and identity-based firewalls for private networks, finally providing security professionals with a tool built specifically for protecting private network assets.

Such a strategy provides proactive protection of critical internal networks, systems, applications and data from unauthorized users, including hackers, password thieves or "accidental tourists" by stopping them before they can connect. And, since the identity stays with the packet regardless of its path through the network, it provides robust audit, reporting and user monitoring capability.

Security professionals have done their best with perimeter security technologies that are ill-suited to secure internal networks. They are beginning to encourage integration and collaboration between networking and security teams in order to find a solution that doesn't negatively impact business. Identifying known users and controlling their access to private network resources through network identity enforcement is proactive and effective and involves significantly lower TCO. It exploits the one advantage a good guy has over a bad guy on an internal network—you know who should be there. 

Dave Shay is founder, CTO and VP of Engineering of Trusted Network Technologies.