

The
ESSENTIAL GUIDE
for
Upgrading
your **Network**

.....
1 NETWORKING EVOLUTION
AND ROADMAP

.....
2 MOVING TOWARD THE
APPLICATION-CENTRIC NETWORK

.....
3 UPGRADING
DISTRIBUTED NETWORKS

.....
> 4 SECURING THE NEW
NETWORK ARCHITECTURE

.....
5 CASE STUDY:
TOMORROW'S NETWORK—TODAY

CHAPTER 4

Securing the New Network Architecture

By Lisa Phifer

In years past, companies relied on network edge security to establish a perimeter separating trusted insiders from everyone else. However, the distributed and dynamic nature of modern networks, combined with targeted threats against applications and data, is changing that focus. Today, network security is more about controlling individual user access to services and data, and auditing their behavior to ensure compliance with policies and regulations.

For example, when IDC surveyed enterprises about pressing security challenges for 2007, growing attack sophistication, lack of employee adherence to security policy, and increasing complexity of security solutions and network traffic were top concerns. Moreover, the larger the enterprise, the greater the risk posed by internal sources. Insider abuse of network access and email surpassed virus infection as the most reported incident in this year's Computer Secu-

rity Institute Computer Crime and Security Survey.

In short, today's threat landscape has fundamentally altered what constitutes an effective defense or timely response. Businesses must inspect not only network protocols but the valuable and sensitive information those messages carry. Stopping insider misuse and abuse requires more granular measures like endpoint security, identity-based network access controls and network behavior analysis. Best practices developed for perimeter security still apply, but they must now be deployed more pervasively and become an integral part of the network itself.

Unified threat management

Most purpose-built perimeter firewalls have now morphed into multi-function unified threat management (UTM) appliances. These malleable all-in-one network security platforms can deliver firewall, intrusion prevention and antivirus services from a single, integrated box. Many can also provide further security services, from anti-spyware and VPN capabilities to spam and Web filtering.

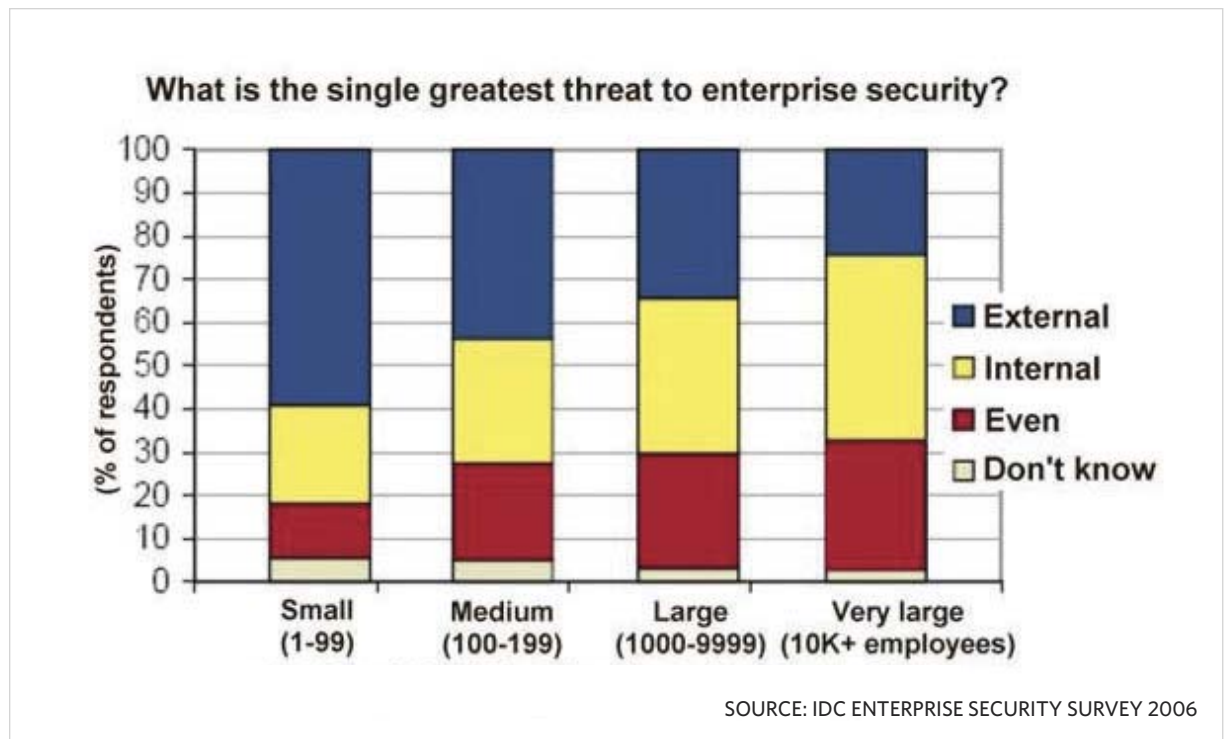
According to IDC, UTM is the fastest growing segment of the security appliance market. Worldwide sales are projected to exceed \$3 billion

by 2009. Why have UTM appliances grown so popular, so quickly?

- Network-borne threats now blend attack techniques to evade legacy defenses. For example, spyware—especially Trojans and root-kits—are dangerous and hard to remove. Most are delivered by unwanted email or malicious websites. Once implanted, they “phone home” over back-channels that pass through lax perimeter firewalls. Network-based IPS, antivirus, anti-spam, and Web filtering can stop spyware before it reaches the desktop.
- Smaller businesses are easily overwhelmed by the cost and complexity

of deploying multiple independent best-of-breed security systems. Larger enterprises are better able to manage those systems, but adding a new cluster to address every new threat adds network latency, reduces reliability, and increases capital and operating expense. UTM makes it possible to combine security services in ways that make the most sense for each business and location.

UTM is not a product but a contemporary approach to battle sophisticated network-borne threats with fewer moving parts. For many businesses, the question is not whether to apply



UTM, but when, where and how to consolidate security services. Successful UTM deployment requires careful planning. Start by considering where security services could be consolidated throughout your network, and the benefits and impacts of doing so.

Where consolidating everything on one platform is impractical, plan to distribute security services across multiple UTM appliances or UTM chassis blades. Apply UTM at internal trust boundaries in a layered defense to distribute workload and enforce policies with increasing granularity. For example, coarse network/intrusion prevention filters might be applied at the outer perimeter, backed by detailed email inspection as messages enter a server pool.

Finally, although UTM may lead to retirement of older systems, it does not require displacement of best-of-breed solutions that are meeting business needs. The more granular the corporate policy is, the more likely it is that at least some best-of-breed depth will be required to complement UTM breadth.

Application firewalls

As network firewalls grew robust, attackers adjusted their tactics. Today's most dangerous threats are aimed at specific application protocol vulnera-

bilities, coding flaws and configuration errors. According to CSI, one in five companies even experience attacks that target specific groups or individuals. Application firewalls can

Although UTM may lead to retirement of older systems, it does not require displacement of best-of-breed solutions meeting business needs.

help defeat these more tightly focused attacks.

Many UTM firewalls use deep packet inspection and/or proxy techniques to examine message content for malicious URLs, viruses and spyware, but they are still general-purpose devices. On the other hand, an application firewall is a highly specialized system designed to protect and defend a single business application.

For example, Web application firewalls examine HTTP/HTTPS/SOAP/XML requests and responses, looking for attacks against Web servers and their applications. VoIP application firewalls filter and proxy SIP/SIPS/RTCP/RTP streams, mapping calls to registered users and defending call managers and PBXs from VoIP hacks.

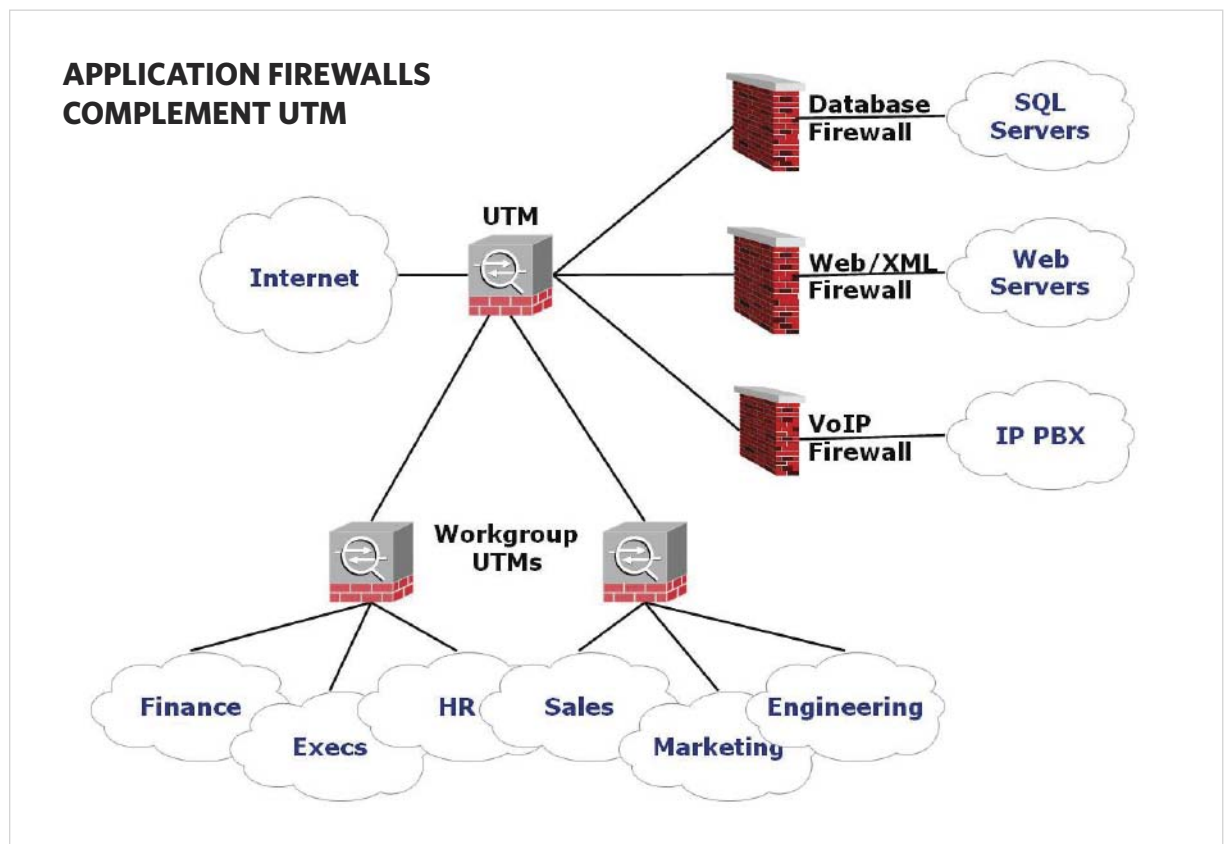
Application firewalls do not replace UTM firewalls; they are deployed behind established trust boundaries, complementing broader defenses with a more detailed layer of security. Application firewalls can be helpful wherever network defenses do not sufficiently protect high-value, high-threat, mission-critical applications.

SSL VPNs

In a perimeter defense, virtual private networks (VPNs) can securely

connect branch offices and trusted laptops to corporate networks—in effect, treating them as trusted insiders. But B2B partnerships and mobile workforces have blurred those trust boundaries. For employees using home PCs and suppliers that deserve limited access, those old remote-access VPN clients are insufficient and impractical.

According to Forrester Research, SSL-based VPNs have become the technology of choice for remote ac-



cess, used by 44% of North American enterprises. Why? SSL VPNs leverage Web browsers to avoid client software installation. By using embedded browser capabilities to authenticate, encrypt and verify traffic, SSL VPNs can deliver secure access with less hassle.

Early SSL VPNs were limited to applications with browser-based interfaces. Today's SSL VPNs offer multiple access methods, ranging from Web portals to bi-directional network tunnels. Common applications like webmail and file access can be reached through any browser, but many other applications require client-side processing. To accomplish that, an ActiveX or Java agent is pushed to the browser at connect time and "dissolves" at logoff. But more challenging applications (e.g., VoIP) require permanently installed SSL VPN agents.

Using SSL VPNs, businesses can extend at least basic access to unmanaged devices, such as home PCs, public kiosks and consultant laptops. Because those endpoints could be unprotected or compromised, however, most SSL VPNs offer two further capabilities:

- **Endpoint scans:** SSL VPNs may use dissolvable agents to examine device state, such as determining

whether antivirus software is current and running.

- **Granular controls:** Based on scan results and authenticated user identity, SSL VPNs can restrict users to specific authorized resources and actions.

For example, when Sue logs in from a business center PC, she might have read-only access to her mailbox and nothing more. In addition to limiting access, the SSL VPN would stop Sue from leaving behind cookies or temp files. But when connecting from her company laptop, she can write to databases and save files to her encrypted laptop.

Endpoint security

Devices used for remote access are not the only endpoints that can and should be protected. Antivirus became standard issue on corporate desktops and laptops long ago. As Internet connectivity grew, host-resident (personal) firewalls became popular enough to be included in operating systems.

Today, those measures are just a starting point. To stop more diverse and hostile threats, desktop security vendors have assembled advanced defenses into endpoint security suites. Like UTM, these tightly integrated bundles combine firewall, antivirus,

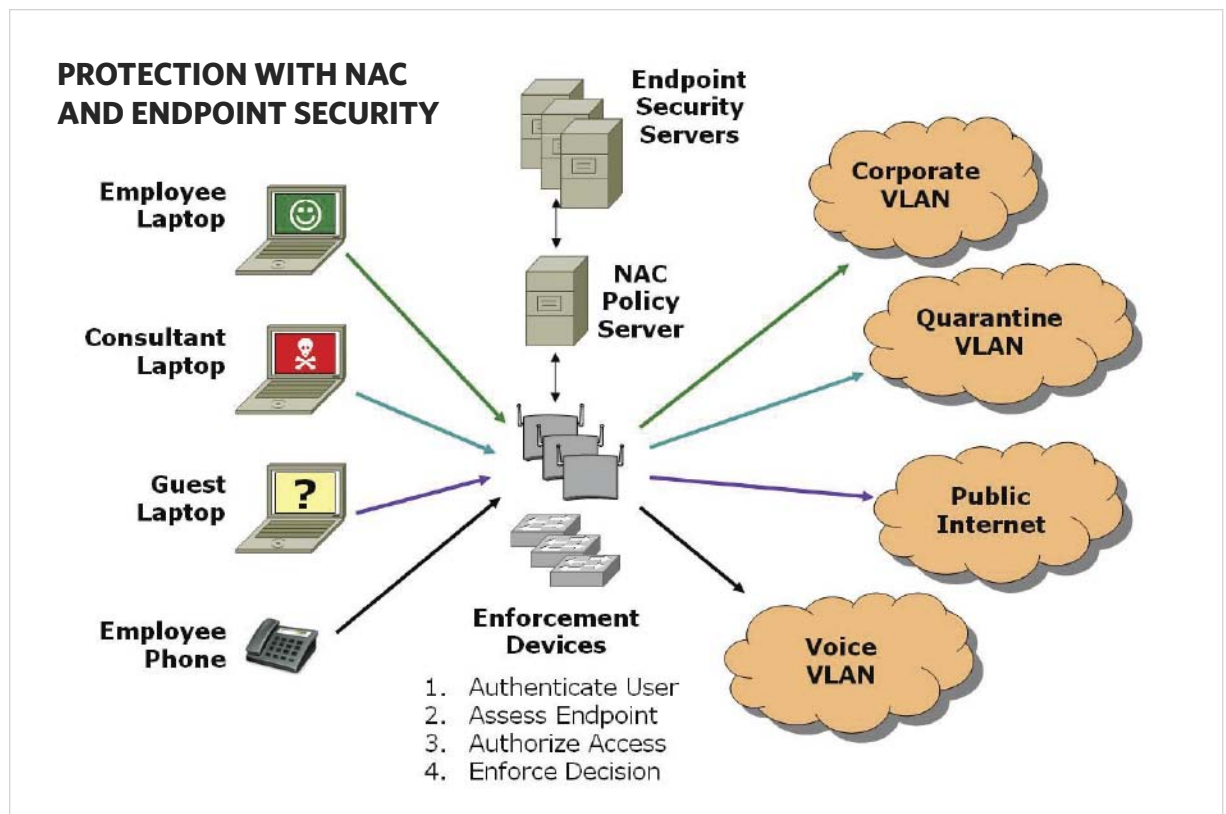
anti-spyware, anti-spam and intrusion prevention services. Unlike UTM, endpoint security suites are programs that run on each host. Enterprise-class endpoint security suites go further by using an IT server to centrally install and maintain those clients.

Why should companies apply such defenses within the network and at the desktop? UTM stops malware before it spreads, reducing bandwidth consumption and cleanup cost. Endpoint security hardens desktops against insider attack and protects

mobile laptops connected to public networks. Many endpoint security suites go beyond network threats—for example, identity theft protection on home PCs or black-listing risky applications on corporate endpoints. Together, UTM and endpoint security are more effective than either could be alone.

Network access control

Endpoint security is effective only when enforced. Without IT oversight, users fail to keep up with software



patches and signature updates. When defenses impede usability, workers disable or reconfigure them. Even endpoint security software can be corrupted, accidentally or intention-

NAC is the model to which enterprises should aspire, but few have attempted full-blown implementation.

ally, and stealthy rootkits can mask symptoms.

Network access control (NAC) has emerged as a promising approach to enforce endpoint security and deliver appropriate access to each user. NAC takes a page from the SSL VPN playbook by treating everyone—on-site contractors, Wi-Fi visitors, off-site employees—as potentially untrustworthy and unsafe. NAC authorizes resource access based on the combination of authenticated user identity, endpoint security state, and policy. NAC makes and enforces access decisions at network connect time and/or by periodic reassessment thereafter.

The potential benefits of NAC are many. Laptops that leave the enterprise and return infected can be quarantined for remediation. Visitors with “clean machines” can be given Inter-

net-only access. Not only can policy be enforced on managed endpoints, but NAC can help document compliance for all network usage.

NAC is being promoted as the model to which enterprises should aspire, but few have attempted full-blown implementation. Some companies are waiting for a winner to emerge from the chief contenders: Cisco’s Network Admission Control, Microsoft’s Network Access Protection, and the Trusted Computing Group’s Trusted Network Connect. Others have been put off by the network upgrades and endpoint agents needed to enforce access decisions. Some have deployed NAC appliances—tactical overlay devices that scan endpoints and control what users can reach without relying on (or cooperating with) network infrastructure or endpoint security servers.

Many analysts believe that NAC will become an accepted best practice. Others find NAC architectures overly complex and believe that NAC appliances suffice. Still others argue that endpoint software, rather than the network, should enforce access decisions. Only time will tell which approach will prevail. All seem to agree, however, that network access must be more tightly controlled, reflecting identity and endpoint state.

Network security monitoring

Controlling network access is half the battle—the rest is keeping a watchful eye on any threat or high-risk traffic that slips past those defenses or originates inside the network.

Network intrusion detection systems (IDS) complement perimeter firewalls by passively observing traffic and alerting administrators to attacks. IDS have largely given way to intrusion prevention systems (IPS)—active systems that not only detect, but prevent, intrusions. UTM appliances are one way to deploy IPS; best-of-breed IPS systems are another. IPS can also be applied to wireless environments using either embedded wireless LAN controller capabilities or by deploying overlay wireless IPS servers and sensors.

Intrusion prevention compares monitored traffic to signatures and protocol rules. When violations are spotted, IPS can take policy-based action to break the connection or quarantine the source. However, IPS focuses on traffic at trust boundaries: behind the firewall, or behind the VPN concentrator, at the point where wireless hosts connect.

Today, companies must also be concerned about activity inside the network, between systems within the same trust groups. Atypical interac-

tion between servers and hosts can be evidence of attack, even when permissible protocols are used. To address this, a new class of security product has emerged: network behavior analysis (NBA). This uses flow observation to spot traffic spikes, unexpected activity and policy violations. NBA can profile relationships, flag anomalies, and spot zero-day attacks for which IPS signatures and endpoint security

Atypical interaction between servers and hosts can be evidence of attack, even when permissible protocols are used.

patches have not yet been deployed.

Finally, in large networks, security has grown so complex that administrators can no longer effectively analyze logs and alerts and flow records without assistance. Security information management (SIM) products can gather, aggregate and correlate security data from network devices, application servers, databases, firewalls, VPN concentrators, NAC appliances, endpoint security servers, and so on. Like NBA, SIM is a relatively new field that larger enterprises should watch. ■

Lisa A. Phifer is Vice President of Core Competence Inc. She has been involved in the design, implementation and evaluation of data communications, internetworking, security and network management products for more than 25 years and has advised companies large and small regarding security needs, product assessment and the use of emerging technologies and best practices. Lisa is a well-known industry author and speaker, especially in the areas of network security and wireless technologies.