SearchNetworking.com

The ESSENTIAL GUIDE for Upgrading your Network

1 NETWORKING EVOLUTION AND ROADMAP PAGE 2

2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK PAGE 8

3 UPGRADING DISTRIBUTED NETWORKS PAGE 15

4 SECURING THE NEW NETWORK ARCHITECTURE PAGE 21

5 CASE STUDY: TOMORROW'S NETWORK—TODAY PAGE 29

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

CHAPTER 1

Networking Evolution and Roadmap

By David Greenfield

The network is on the move yet again. Running voice, videoconferencing and video surveillance across the network that also handles email, file transfers and critical business transactions is enabling organizations to reduce overall capital expenditures and improve their agility.

But none of that comes for free. A predictable infrastructure is needed for these new applications to work. Packet loss, delay and jitter must be rigorously inhibited if a pin drop is to be heard across a phone call. Those requirements are only going to become stiffer as application load and user expectations grow.

Availability is crucial. CEOs aren't particularly fond of having to reboot their phones. They don't want their surveillance systems to fail. And they most certainly aren't interested in hearing why their point-of-sale systems are offline or why a manufacturing plant has had to shut down. So before IT professionals can expect to deploy business-critical applications across their networks, they need to be sure that the network is business-critical ready. It's not just about having a huge pipe; it's about delivering a complete facility that supplies applications consistently, reliably and securely.

The art of impact assessments

Ensuring a properly designed infrastructure is the first step toward an effective deployment, be it of voice, video or any other application. Ultimately, though, any thorough impact assessment is more than just answering a checklist of questions. It relies on a deep understanding of the business problem that must be solved. Only then can the underlying technical requirements be determined.

Do regulatory requirements around data preservation need to be met? Are assurances around customer delivery metrics being promised, and must they be met? Or, even more simply, is that telephone being deployed sitting on the CEO's desk or the janitor's?

Answering questions such as these is fundamental to organizations' leveraging their infrastructure investment. If a business does not answer these questions, IT will find it very difficult to gauge the status of the current network, prioritize upgrades and evaluate whether improvements are meeting

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

IT and business needs. An impact assessment detailing business requirements and outlining a roadmap to transition to the architecture that will fulfil those requirements in several main areas is essential to success.

Physical plant

Complex, modern networks cannot run well without a solid underlying physical plant. Beefing up wiring, switches and routers can make a big difference in overall network performance.

Be certain to conduct a physical layer audit to ensure that all installed cabling is up to par. It's amazing how many stories of transient VoIP problems resolve into a question of bad cabling, a faulty splitter or a loose coupling. Take the time to be sure that the cabling plant meets specifications, and correct any errors before deploying those uber-applications.

While mobility is becoming a way of life for many users, most typical LANs are based on good old-fashioned Cat-5 or Cat-6 cabling. It's entirely probable that a network upgrade in three to five years may use wireless for more than guest Internet access; but today, the challenges of delivering quality of service, roaming between access points, security, voice quality and numerous other issues make wireless ill suited as the basis of many corporate networks. Networking professionals should ensure that wireless access is reliable and consistent in the places where it is deployed, but in most instances the wired network will be carrying the bulk of business-critical traffic.

Bandwidth: How much is enough?

Without the right amount of bandwidth in the network, real-time applications will grind to a halt. Finding what's right can be a challenge. One easy answer in the LAN environment is to roll out switched, 100 Mbps Ethernet to the desktop. Upgrading to 1 Gbps to the desktop is another option, but unless an organization moves huge files, such as engineering designs, most desktops won't be able to take advantage of the additional bandwidth.

Without the right amount of bandwidth in the network, real-time applications will grind to a halt.

The bigger challenge is providing enough bandwidth at key network junction points in the network, as well as over the WAN. Typically, there

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

is a mismatch between incoming demand and the outbound capacity. That can create bottlenecks where any number of links aggregate together, such as the switch at the front end of a server, or where the LAN meets the WAN.

Ensuring optimum performance on a minimal budget requires a good understanding … of the applications running over the network.

For these instances, ensuring optimum performance on a minimal budget requires a good understanding of the behavior of the applications running over the network. Understanding the application's latency, jitter and packet loss requirements, as well as its traffic patterns—such as whether flows are peer-to-peer, involve a server, or both—is critical for leveraging the capacity in your network topology.

Ultimately, 10 Gbps links may clear away any performance problems within the LAN, most notably to servers, especially those using virtualization. Today, however, 10 Gbps is still cost prohibitive for many organizations. For them, a more realistic option is sticking with 1 Gbps links and then distributing traffic across multiple servers using new technology such as application delivery controllers and, ultimately, grid or virtualized architectures.

WAN bandwidth must also be carefully considered. Businesses are global and mobile, making bandwidth use between locations skyrocket, and trends toward centralized applications and data center consolidation have created more of those congestion points where the LAN meets the WAN. Enterprises can work with carriers to negotiate the most cost-effective and appropriate WAN links. They can also implement WAN optimization and acceleration to use the WAN as efficiently as possible.

Predictable delivery

Invariably, someone in the organization will want to save a bit of money on the network upgrade by challenging the need for new switches with quality of service (QoS) for prioritizing traffic. He or she will point out that, even when VoIP is running on the network, the amount of bandwidth a VoIP session uses with a bulky wideband CODEC is a fraction of the speed of even a 10 Mbps link, let alone a 100 Mbps link.

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

Insist on QoS. While it may be true that voice doesn't require QoS under "normal" conditions, the network should not be designed for normal conditions. You must plan for peak conditions, such as a virus spreading across the network or a user deciding to back up a 100 GB file across the network. For those instances, the network staff must ensure that VoIP will take higher priority than Internet browsing.

While an issue for LANs, QoS becomes an even bigger issue in any location where there is a speed mismatch, such as on the access link from a customer premises to the Internet or the corporate WAN. With smaller bandwidth capacities, access links are notorious for places where delay-sensitive applications falter. Implemented properly, QoS prevents applications from hogging those links and ensures that priority traffic gets through.

Bandwidth consistency also must be considered in the context of network devices. The delay through a router can interrupt applications as well, and routers offer many queuing mechanisms for reducing transit times. Although routers may perform fine under normal conditions, however, it's the unusual or extreme conditions that IT needs to consider. When routers recalculate their routing tables in corporate WANs, for example, routing delays can result. Examining these "boundary conditions" will go a long way toward preparing your routing networking infrastructure for real-time applications.

Reliability

Reliability is a cornerstone of an enterprise-class network. In a network running VoIP, availability and reliability are complicated by having to protect the logical as well as physical facilities. Good design suggests running voice in its own virtual LAN (VLAN) to protect voice calls from the vagaries of data applications running on the rest of the network. However, doing so also allows for network architectures that may build redundancy in the switching fabric or routing core but still be unable to complete a voice call.

With smaller bandwidth capacities, access links are notorious for places where delay-sensitive applications falter.

Ensuring reliability starts with the physical network. Classic tiered-switching design provides an inherent

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

measure of failover. Should the distribution switch connecting a workgroup's access switch to the network's core switch fail, a second distribution switch is typically designed into the overall network plan to handle the load from the access switch. But such an approach consumes additional switch ports, the costs of which must be considered.

Simply segmenting voice traffic cannot protect a voice system nor can simply implementing a firewall secure the network from external attackers.

Router availability is a similar issue. Numerous options exist for individual router survivability and operation in the event of a failure. Alternatively, the networking team may consider redundant router designs as a more effective route.

Power supply and environmental factors within the writing closet must also be carefully considered. All devices will have to be backed up by sufficient power to meet the organization's needs during an outage. Again, the duration of power depends on the organization's objectives, but two to four hours is typical within the industry. If switches are to offer inline power, such as Power over Ethernet (PoE), the power requirements will be higher. This, in turn, means ensuring sufficient power delivery and cooling requirements for the wiring closet. It also means considering how to power end nodes during an outage.

As for logical failover, VLAN assignments must be done per node, not per application. While telephones may be easily assigned to a voice VLAN, softphones and unified communications (UC) clients are another matter. They are typically assigned to a data VLAN. Enterprises then need to route between VLANs if phones, softphones and UC clients are to communicate with one another.

Security

VLANs provide a small measure of security, but simply segmenting voice traffic cannot protect a voice system nor can simply implementing a firewall secure the network from external attackers. The distributed nature of modern networks, combined with the increased focus on applications and business data, makes network security less about locking down a network perimeter and more about controlling user access and behavior and ensur-

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

ing data safety in a dynamic and mobile environment.

Today, more attacks come from within the network than outside it. A survey last year by Deloitte showed that 83% of IT executives at technology, media and telecommunications companies were concerned about "employee misconduct involving information systems."

Protecting against these users requires rethinking today's security architecture. IT must assume that desktops have been compromised. Central to that protection architecture is the use of tools like network access control (NAC) and endpoint security products. Using these tools, centralized security systems can ensure that only authorized individuals are granted access to the network using approved devices and that those devices are using protocols, applications and processes defined by the enterprise.

IT can also implement data protection restrictions in the form of digital rights management (DRM). The combination of the endpoint security and DRM allows organizations to restrict access when data is editable on a user's machine and limit how it may be distributed across the network.

These measures are implemented in addition to security practices and systems that already exist in most organizations. Intrusion detection and prevention capabilities, for example, are needed for post-admission control, as are use of access control lists (ACLs) and internal firewalls to limit access to sensitive parts of the business.

Central to a data protection architecture is the use of tools like network access control (NAC) and endpoint security products.

Many companies have implemented Secure Sockets Layer (SSL) VPN for secure remote access for telecommuting and mobile workers.

Thought must also be given to how calls are placed to and from the PSTN. Today, that is normally done by purchasing local gateways but, increasingly, organizations are considering IP-based trunks supplied by an external service provider. This eliminates the cost of gateways while enabling calls to remain on the IP network end-to-end, improving call quality. At the same time, however, it exposes the network to external IP sessions and requires additional VoIP security. ■

David Greenfield is principal of STAnalytics, a global technology marketing consultancy where he advises enterprises on emerging technologies. He has spent the past 20 years analyzing network communications and most recently was the editor of *Network Computing*. His work has appeared in other leading technology publications, such as *PC Magazine*, *IT Architect*, *Data Communications* and *Red Herring*, and he has consulted to and assisted Fortune 500 enterprises in their technology acquisitions.

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

CHAPTER 2

Moving Toward the Application-Centric Network

By Robin Layland

The data center has continued to evolve and so have the requirements placed on the network. Not long ago, it was enough for the networking group to provide load balancing based on the TCP/IP address of applications, automatically notifying operations when a server was not responding and stopping network-based attacks such as denial of service (DoS). Today, much more is required. The network must be able to route traffic based on the information within the URL or even details within the application data. It is not enough to monitor an application; now, if a particular transaction within an application is not responding or is slow, the network must alert operations.

Security means going beyond stopping network-level DoS attacks to preventing application-level DoS attacks and actively protecting applications. The network must provide these functions to banks of specialized appliances such as firewalls and DNS appliances, not just servers. In addition, the network must help keep down the costs of provisioning the data center while providing this increased functionality.

Lastly, the network has to help with response time. The move to Web-based applications, with their richer and larger transactions, has negatively affected users' response time. The network is still the first place where management looks for help in solving response-time problems. The old answer of increasing the speed of the network is expensive and may not even help, given the way HTTP works.

Application delivery controllers emerge

A new class of networking products has emerged to address all these needs. They evolved from server load balancers (SLBs) and can be thought of as next-generation SLBs. A new name was needed to differentiate them from SLBs and, unfortunately, the market has given them several names. They go by application switch, application front ends, and application delivery controllers (ADCs), with ADC slowly becoming the most common term. Many of the vendors that provide SLBs have evolved their product lines to become ADCs, but that is not true for all the vendors that pro-

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

vide SLB solutions. In addition, a few new vendors have built new equipment to meet this challenge.

ADCs are different from SLBs in several ways, but all the new functionality is based on how deep they can efficiently look inside a message. SLBs always had deep packet inspection, and ADCs have taken it deeper. The easiest way to think of an ADC is that it can understand the application.

A common example shows how new capabilities of ADCs allowed a company to handle explosive growth. Company A manages financial employee benefits for other companies and government agencies. Its business grew rapidly when it landed a large number of new contracts. All of its customers wanted it to begin the employee benefit at the same time—at the first of the year—but its existing server farm was not up to the task. Company A needed to quickly set up a large number of servers, both to handle different customers and also different sets of sub-applications for each customer, while meeting the security requirements that critical financial applications require. The application design also needed to maintain session persistence once a customer had logged onto a particular application on a server.

ADCs are different from SLBs in several ways, but all the new functionality is based on how deep they can efficiently look inside a message.

ADC Key Capabilities

THE KEY DIFFERENCES between ADCs and traditional load balancers are:

» Routing and load balancing are based on information within application data

» They take over functions that are done in the server to save server resources

» They accelerate application response time

» They provide application-level security

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

ADCs allowed Company A to set up complicated routing rules that looked within the application-level data along with providing cookie insertion. The security and acceleration features helped them meet their service goals for the customers. All this was provided without any modification to the company's original software design.

Application knowledge

SLBs can route a packet to a server based on the information in the TCP/IP header and, in the case of Web (HTTP) applications, based on the HTTP header. ADCs have taken that ability and expanded it to include any application header and any field in the application data. This has given application owners increased flexibility. An example of an e-commerce site demonstrates how this new ability is used. One person is browsing the site while another is starting the checkout process. If the site experiences a problem, such as slow response time due to high volume, the ADC can send the person checking out to a faster server, ensuring that he doesn't encounter errors. It could go even further and monitor how much people are spending, sending someone with a large dollar value to the faster server. The ADC gives the business the ability to create rules based on any information within the application data.

This flexibility comes with a price. ADCs are not magicians, and out of the box the ADC does not understand the business it is meant to support. It has the ability to implement rules to make the business run better, but only if it is told how to do so. In the previous e-commerce example, if the goal is to provide fast response time to the big spenders, a rule must be created telling the ADC where in the application data to look and what a big spender is. This means the person setting up the ADC has to understand the application and the business. This is knowledge that most networking professionals don't have.

Taking advantage of the flexibility of the ADC requires the networking department, which owns the ADC, to work closely with the company's business and application developers to create the rules. ADC vendors have helped by providing a large set of common rules based on research and

An ADC has the ability to implement rules to make the business run better, but only if it is told how to do so.

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

what they have learned from other customers. Many of these general rules can be used out of the box or with simple modifications to adapt them to the business's needs. Understanding the business is still a prerequisite for knowing whether the general rules are useful, however, and detailed knowledge of the business is needed to gain a competitive advantage. Creating the business-specific rules is the hardest part of taking advantage of the ADC.

Each set of virtual ADCs can have its own set of rules; a change to one group's rules does not affect another group's virtual ADC.

One solution is to allow each business unit to create its own set of rules. But this sometimes leads to another problem. ADCs generally support multiple applications and servers, cutting across business units. It is not cost-effective for each application or business unit to have its own ADC. Combining all the rules into one master set can cause problems, however. The resulting very large rule set can slow down the ADC, and when one business unit's rules cause trouble, it sometimes affects every business unit.

An emerging solution to this problem is virtualization. Virtualization allows an ADC to be logically partitioned into multiple virtual ADCs. This lets network management allocate a set of virtual ADCs to each business unit. Each set of virtual ADCs can have its own set of rules; a change to one group's rules does not affect another group's virtual ADC. Virtualization allows the network manager to restrict each group's ability to manage only its own virtual ADC and to define the management capabilities they access.

Server offload

Another major trend made possible with ADCs is offloading work from servers to the ADC. There are two primary drivers for this trend. First, the ADC can perform tasks more cost efficiently than servers. Second, moving the function to the ADC simplifies deployment by disconnecting the function from the server software and hardware.

The problem is that, in many cases, the server would need new hardware or software to efficiently perform the function, something not always possible and sometimes problematic, given the number of servers. Offload-

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

ing is used primarily for SSL processing and encryptions and for TCP/IP processing.

Acceleration

Moving applications to a Web interface creates several networking problems. First, Web applications send more data per transaction than traditional client/server applications, resulting in slower response time for users accessing them over the WAN. The second problem is the way HTTP works. HTTP breaks a transaction into multiple objects that are independently sent. A group of objects is often sent serially. This serial sending of objects can slow response time so that increasing the bandwidth doesn't help response time.

The ADC can't eliminate these problems, but it can help. The first way is by compressing the objects using the browser's built-in compression algorithm, gzip. The ADC can also cache objects. The first time the ADC sees an object, it stores that object. When a user asks for the object, the ADC can send the copy from its cache. This reduces response time by eliminating the time it takes to fetch the object from the server. It also has the added benefit of reducing the load on the server, providing another form of offloading. The ADC can take caching a step further by directing the user's browser to cache the object. When the user requests the object again, the ADC directs the client to use the object in its cache, saving the time it would take to resend the object.

Web applications send more data per transaction ... resulting in slower response time for users accessing them over the WAN.

The caching feature generally applies to static objects, but some vendors also apply the technique to dynamic objects. With static objects, the ADC must be told how long to keep the object, because even static objects can change. This is a case where individual application rules can be applied to guide the ADC. The rules are especially important for caching dynamic objects.

Application security

The ability to handle network DoS and distributed DoS attacks was one of the first security features added to SLBs. The load balancer was ideally situated to protect the data center from these attacks. The ADC has

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP
CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK
CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS
CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE
CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

expanded on that capability by taking on new security functions. Also, as the need grows for multiple intrusion detection and prevention systems and firewalls to protect the data center, the ADC takes over the role of balancing and routing traffic to the growing number of security appliances.

The ADC's role in security is based on its ability to perform deep packet inspection and understand applications. These abilities most commonly appear in the extension of the ability to stop DoS attacks at the application layer and in Web firewalls. As a general rule, the new security features apply only to Web-based applications.

An application DoS attack has the same characteristics as a network-level DoS attack: Servers are flooded with requests in an attempt to keep them so busy that they cannot process normal traffic. In a network DoS attack, this is done at the TCP level, generally using SYN requests. Application DoS attacks are more complicated. They flood the server with a legitimate request, such as an inquiry. They can use any legitimate request. Since the ADC understands application flows, it can recognize when the number of particular requests is outside the norm and eliminate the attacking requests before they reach the server, just as it would eliminate SYN requests in a network DoS attack.

Web Firewalls Enhance ADC Security

ADCS HAVE ALSO leveraged their understanding of applications with the addition of Web firewalls. Examples of this type of protection offered by Web firewalls include:

- » Ensuring that the application receives only valid inputs
- » Ensuring that buffer overruns don't reach the application
- » Handling command and SQL injection attacks
- » Stopping cross-scripting attacks
- » Preventing cookie tampering and problems resulting from applications improperly handling errors

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

XML

In the future, Web firewall functionality will be expanded to include XML transactions by incorporating an XML firewall. An XML firewall ensures that XML data within the application data is not exploited, patching the holes left by the application much as a Web firewall does at the HTTP level. One simple example of the role an XML firewall plays is when XML data includes a payment. The XML firewall would make sure that no unauthorized person tampered with the amount, such as changing a small payment to a large payment. This is increasingly needed as application-to-application processing removes people from the process.

A more controversial area is the role that the ADC will play in XML translation. Translation is needed between two applications that use XML when they have defined the same field differently—they both use XML but with a different dialect. This problem is generally solved by adding middleware to one of the applications and letting the middleware perform the translation. This translation role is a function some within the ADC community are proposing for ADCs. One of the primary reasons is to leverage the application rules the ADC already has.

Functionality of ADCs has grown significantly from the original load balancer, with the focus shifting deeper into the message, understanding the application and expanding its role to include security and application acceleration. The next few years will see these new abilities become standard and more fully developed.

In the future, Web firewall functionality will be expanded to include XML transactions by incorporating an XML firewall.

The challenge will be to make it easier to manage the increasing number of ADCs required to run a data center and provide the application intelligence they need. This will be accomplished by allowing applications groups—the people who understand the applications and have the detailed knowledge to fully utilize ADC capabilities—to have a greater role in configuring the ADC. Virtualization is the key technology for allowing the network group to maintain control over the ADC while giving the business unit the control it needs to customize the ADC for its business. ■

Robin Layland is president of Layland Consulting. As an industry analyst and consultant, Robin has covered all aspects of networking from both the business and technical sides and has published more than 100 articles in leading trade journals, including *Network World*, *Business Communication Review*, *Network Magazine* and *Data Communications*. Prior to his current role, Robin spent a combined 15 years at American Express and Travelers Insurance in a wide range of jobs, including network architect, technical support, management, programming, performance analysis and capacity planning.

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP
CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK
CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS
CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE
CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

CHAPTER 3

Upgrading Distributed Networks

By Robin Layland

At a major enterprise, executive IT management has already made the decision to consolidate local file servers in branch offices to the data center. Consolidation makes sense—it will save money, provide a more secure environment and make maintenance easier. The problems, however, begin to rear their heads early in the project. The branch offices consolidated first begin complaining because the time it takes to download files is affecting their productivity. The consolidation project is saved by implementing a new branch office technology: application acceleration. With an application acceleration appliance, download times are reduced to acceptable levels and the project is back on track.

Branch offices are important to the business. They need the same quality IT services as corporate headquarters and can't be treated as second-class locations. When branch offices lose connectivity, there is an immediate impact on the overall business. The fear is that providing excellent service to branch offices can also create a money pit. It is not just server consolidation that has made managing distributed networks more difficult. The move to Web browser-based applications has increased the size of each transaction. If that were not enough, the HTTP protocol has some inefficiency built into it that can make it slower than older client/server applications.

Server consolidation

The growth of server-based applications has done wonders for productivity and provides important functionality to the people in distributed locations. File servers allow users to quickly retrieve important business data. Email servers such as Microsoft's Exchange provide fast and efficient email service. Having these and other servers in branch offices has made good response time, and thus productivity, the norm.

But the growth of servers and applications in the branch office has a dark side. Maintenance and problem resolution are expensive. It takes the IT staff extra time and expensive tools to remotely diagnose problems. The remoteness leads to frustration for both the branch office workers and the IT

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

staff. Remote servers waste resources if they are running at low utilization, which is a common occurrence. Backup and recovery takes longer and uses expensive WAN resources when the server is remote. The security of the server is also challenging and makes it harder to meet many of the regulatory requirements of providing data protection.

All these reasons have led to the desire to move remote servers to the data center. The IT staff is located there and can react quickly when a problem arises. Backing up or restoring a server is faster when it is at the data center. It is easier to apply best practices and ensure that the data on the server is secure in the data center. With all servers at the data center, the IT staff can take advantage of server virtualization technologies, such as VMWare, to combine several servers into one.

It doesn't matter whether it is called server consolidation or data center consolidation—the concept solves many problems. However, moving servers to the data center is not the perfect solution. The workers in branch offices frequently see poor response time that negatively affects productivity and morale. Consolidation can also affect the budget, because servers residing in the data center and transmitting all data to branch offices require significant WAN resources.

The question is: How does a good infrastructure design become a better infrastructure design? The answer is incorporation of new technologies that allow an enterprise to capture all the benefits of server consolidation while solving its problems. In this case, the solution at hand goes by two names: WAN optimization and application acceleration. Both names refer to virtually identical technological solutions. If a vendor wants to emphasize WAN bandwidth savings and resulting cost savings, it focuses on WAN optimization. If the vendor wants to highlight improvement in response time and productivity, it focuses on application acceleration.

Application acceleration and WAN optimization

Acceleration applies many techniques to solve the twin problems of poor branch office response time and the extra bandwidth required. The techniques can be grouped into two general categories. The first are "generic" techniques. Generic techniques apply to all the data going to the branch office, no matter the protocol. The benefit is that the technique helps CAD/CAM, file and Web traffic equally.

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP
CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK
CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS
CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE
CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

The primary generic techniques include TCP/IP protocol optimization, bandwidth management and shaping, quality of service (QoS), and compression. Some of these optimization techniques have been around for a while; the biggest recent improvements are in the area of compression.

Older compression techniques generally reduced the amount of data sent by two to three times, while newer techniques, called dictionary compression or de-duping, can reduce bandwidth requirements by 10 to 50 times. Applying these newer compression algorithms means that

How Dictionary Compression Works

IN DICTIONARY COMPRESSION, also known as de-duping, the accelerator learns patterns from the data flowing through it and stores them in a large cache, located both in memory and on a disk drive. The patterns are generally 100 characters long. Accelerators are located at the data center and the branch office, and they both learn the same patterns from the data. The first time the data passes the accelerator, it can only apply older compression techniques; the real advantage comes when it sees the pattern the second time. When the pattern shows up again—this can be in any data, including data totally unrelated to the first instance—the accelerator substitutes the entire pattern with a reference number. The reference number refers to the pattern it has stored, and because the accelerator on the other end has learned the same pattern, it can easily rebuild the message.

For example, if a PowerPoint presentation is attached to an email, the first time it is sent to the branch office there is some data reduction. When the file is sent back to the data center with a few changes, the accelerator can use its pattern database to remove all the parts that haven't changed and send only reference numbers to those parts along with the changes. The result is that a file that was 5 MB can be reduced to a few kilobytes.

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

despite the large bandwidth requirements for server consolidation, the overall utilization of a WAN link could be less than it was before consolidation. Response time is also improved because the overall amount of data that needs to be sent is decreased and because the smaller compressed packets are automatically combined into larger packets, reducing the number of packets sent.

Accelerators can do wonders, but they don't help with certain types of traffic.

The second group of techniques that accelerators apply to improve response time and solve the problems of consolidation are "protocol specific." Many protocols, including Microsoft's Common Internet File System (CIFS) and HTTP, are not very efficient. This inefficiency is unnoticed in a LAN environment because of the speed of the LAN and the short distances traveled. Over the slower WAN, however, protocol inefficiencies can affect response time. Accelerators understand the protocols and apply techniques that overcome their shortcomings. For example, Microsoft file servers can experience close to LAN-like service with the combination of generic techniques and CIFS-specific acceleration.

Accelerators can do wonders, but they don't help with certain types of traffic. Video, such as training films, is not helped much by accelerators because video is already highly compressed. Voice traffic can actually suffer because there is little an accelerator can do, and trying to accelerate it can actually slow it down. It is best to have the accelerator recognize voice traffic and pass it directly through at a high priority.

Acceleration architectural challenges

Acceleration can do wonders for response time and significantly reduce bandwidth requirements, but several issues must be addressed for a successful implementation. The first is a good understanding of which applications are using the WAN.

Gone are the days when identifying traffic by port number was enough. Knowing that Web applications are using port 80, for example, tells you little. Web-based applications using the same port number can include those that are mission critical along with those that are time wasters. Accelerating all Web applications may mean that music-sharing applications

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

run faster. Before applying acceleration, the network group needs to implement application monitoring tools that report on the applications that are using the network, not just the ports that are being used. This information will allow the accelerator to accelerate business applications before non-critical applications. It is also important because, in many cases, network managers will not be aware of all the applications using the network.

The next issue is what to do about encrypted traffic. The movement of applications to Web interfaces has made it easier to encrypt the traffic using SSL. There are many good reasons to use encryption, but it is impossible to apply many of the acceleration and optimization techniques, such as dictionary compression, to encrypted traffic. If business critical traffic, or a significant amount of overall traffic, is encrypted, then an accelerator that can de-encrypt traffic, accelerate it and then re-encrypt is needed. There are accelerators that can perform this function, but not all do it equally well.

Keeping the Branch Connected

FAST APPLICATION RESPONSE time is meaningless if branch connectivity to the data center is lost in the event of an outage or disaster. Providing backup connectivity has always been difficult and expensive. Even if two service providers are in the area, their actual infrastructure often follows the same route out of the building and may be subject to the same backhoe accidents or other disasters.

A new alternative is wireless connectivity from cellular vendors. The connectivity many mobile workers use to get a broadband connection can also be used to connect a branch office. Branch office routers are available that integrate this option directly into the router. The biggest advantage of this option is that the cellular last-mile infrastructure is completely separate from landline facilities. The speeds are not as high as normal landline connection, but wireless can provide significant bandwidth that allows the office to continue working.

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

Securing the accelerator is also necessary because of the new capabilities of dictionary compression techniques and file caching. The dictionary compression file has a copy of all the patterns that have passed through the appliance. With file caching, a copy of the file is stored on the appliance. If someone hacks into the accelerator or runs out the door with it, then it is possible that the sensitive data could be compromised, and traffic could even be recreated from the stored patterns. This is not likely, because the patterns are short and nothing in the accelerator relates one pattern to another, making it very difficult to reconstruct a file. The solution is to encrypt both the cache and the compression files. This feature is available from many acceleration vendors, but not all of them.

Another architectural issue is transparency. This issue has two layers. The first is how the traffic is packaged when it is sent between the two accelerators. The most common way is to create a tunnel between the two accelerators with all the accelerated traffic having a new TCP/IP header added to the packet. The transparency issue is that any monitoring or security device between the two accelerators will no longer see the traffic as coming from the client or server. This loss of visibility causes problems for monitoring and security equipment. The solution is to move all the monitoring or security devices before the accelerator. Some of the acceleration vendors do not create tunnels between the accelerators and thus do not have this problem.

When any monitoring or security device that performs deep packet inspection looks into the packet, what it will see is nothing like what the client or server sent.

A larger transparency issue is created by the accelerators. Accelerators significantly change the traffic by compressing it and combining multiple packets into one larger packet. When any monitoring or security device that performs deep packet inspection looks into the packet, what it will see is nothing like what the client or server sent. Because compressing packets is inherent in the acceleration and optimization process, the only solution is to place all security and monitoring devices before the accelerator. ■

Robin Layland is president of Layland Consulting. As an industry analyst and consultant, Robin has covered all aspects of networking from both the business and technical sides and has published more than 100 articles in leading trade journals, including *Network World*, *Business Communication Review*, *Network Magazine* and *Data Communications*. Prior to his current role, Robin spent a combined 15 years at American Express and Travelers Insurance in a wide range of jobs, including network architect, technical support, management, programming, performance analysis and capacity planning.

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 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 Security 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 multifunction 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

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS

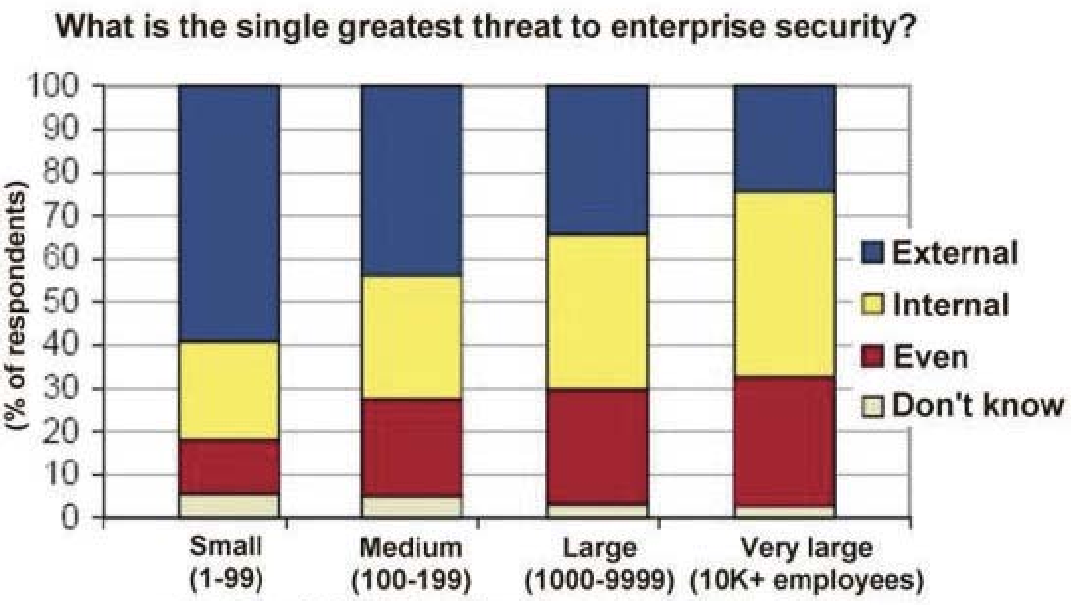
CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

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



SOURCE: IDC ENTERPRISE SECURITY SURVEY 2006

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

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 vulnerabilities, coding flaws and configuration errors. According to CSI, one in five companies even experience attacks that target specific groups or individuals. Application firewalls can help defeat these more tightly focused attacks.

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

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.

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

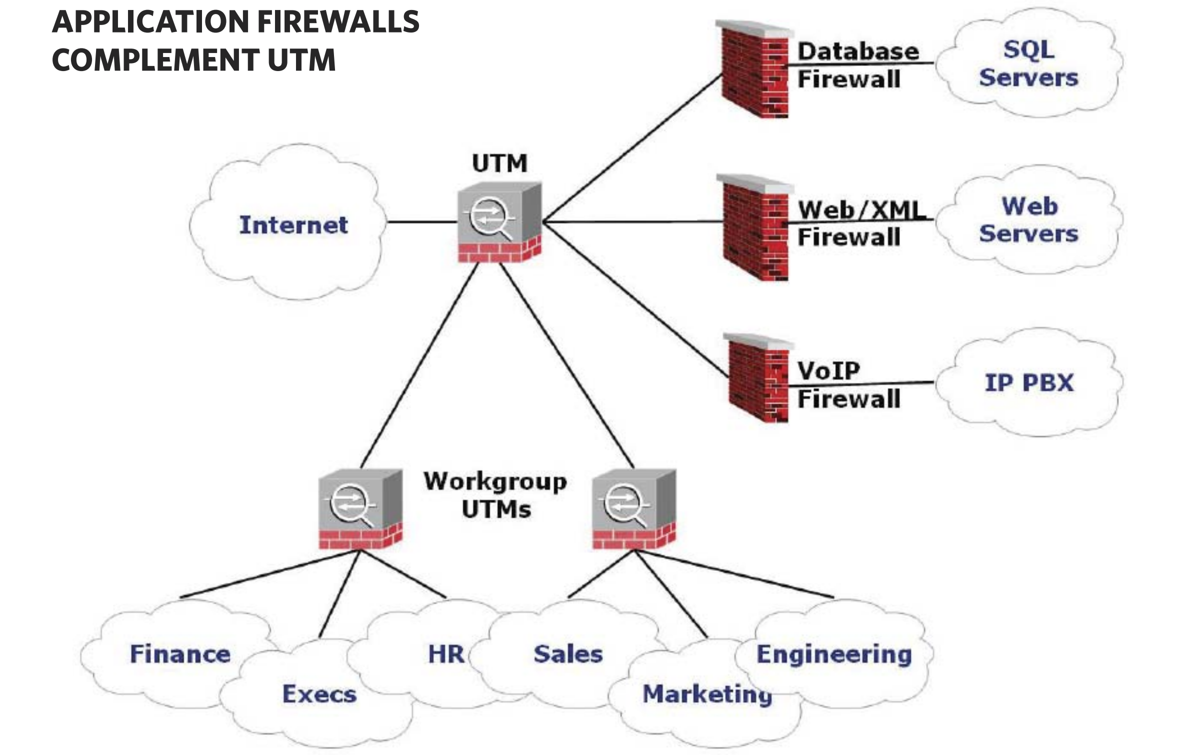
Application firewalls do not replace UTM firewalls; they are deployed behind established trust boundaries, complementing broader defenses with a more detailed layer of security. Application firewalls can be helpful wherever network defenses do not sufficiently protect high-value, high-threat, mission-critical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

APPLICATION FIREWALLS COMPLEMENT UTM



CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP
CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK
CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS
CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE
CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

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,

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

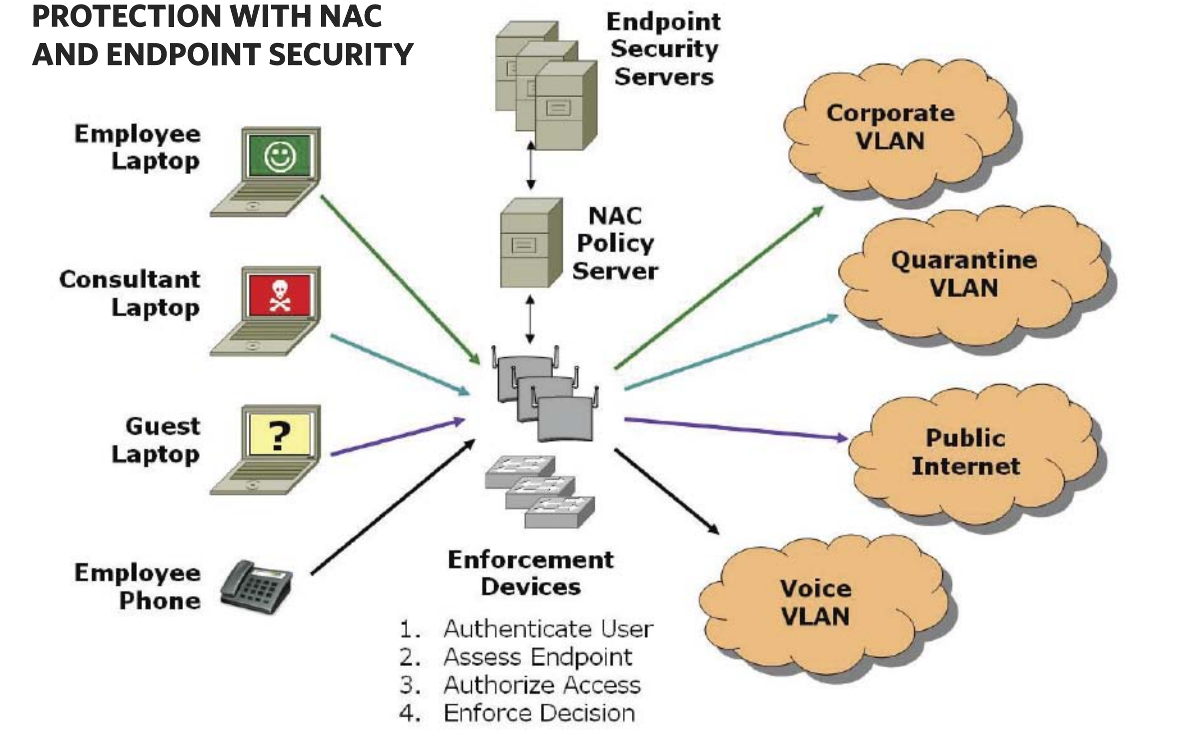
anti-spyware, anti-spam and intrusion prevention services. Unlike UTM, endpoint security suites are programs that run on each host. Enterprise-class endpoint security suites go further by using an IT server to centrally install and maintain those clients.

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

PROTECTION WITH NAC AND ENDPOINT SECURITY



CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

patches and signature updates. When defenses impede usability, workers disable or reconfigure them. Even endpoint security software can be corrupted, accidentally or intentionally, and stealthy rootkits can mask symptoms.

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

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 Internet-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.

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

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 interaction 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 patches have not yet been deployed.

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

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.

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

CHAPTER 5

Case Study: Tomorrow's Network—Today

By Andrew Hickey

Newer and faster applications, increased need for bandwidth, and additional users are in store for almost any enterprise network, forcing companies to re-evaluate network resources and redefine their model for a secure, resilient, application-aware, global network. Achieving that network sometimes requires new technology and new equipment, as well as new skills for networking professionals.

In the following examples, you'll see how two companies upgraded their networks in strategic areas to improve workflow and processes while at the same time keeping in mind the business cases for their upgrades. From data center and server consolidation and bandwidth upgrades to WAN optimization and VoIP preparations, these companies looked to new technologies and tools to get the most out of their critical enterprise networks. There may have been some hiccups along the way, but these companies addressed challenges with an eye to the future, knowing that the hurdles they overcome today will help their networks stand up to tomorrow's business challenges.

Application acceleration cements consolidation project

What started as a simple application rollout for Ozinga Bros. Inc., a concrete manufacturer in the Great Lakes region, led to a much more intensive project in the long run, resulting in data center and server consolidation and a jump into the application acceleration arena.

Ozinga, which operates 21 sites across its distributed network, owns and operates 500 trucks that are vital to its operations. Trucks need maintenance, but with siloed data centers and server farms, there was no single point of reference to track that maintenance. Some branches used software. Others used a chalk board with scribblings to indicate that trucks were up to date with repairs and other work.

The company always had a wide area network (WAN) in place, but was lacking the tools to tie all 21 locations together cohesively. Tom Allen, Ozinga's IT director, said the company needed a method that would allow truck mechanics to communicate with one another and a place to keep

CHAPTER 1 NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2 MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3 UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4 SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5 CASE STUDY: TOMORROW'S NETWORK—TODAY

an inventory of maintenance records and other pertinent information.

The first step was data center consolidation. The company, which had data centers scattered throughout its 21 locations, moved to a single data center in a central location. Along with it, the company also consolidated its Citrix server, putting that in the same central spot. In each branch location, the company rolled out client terminals for mechanics to access the maintenance software over the WAN.

The maintenance software, called TMT, is necessary for several reasons: It saves Ozinga money because it avoids overstocking of parts; it ensures that the fleet of trucks is well maintained, avoiding unexpected repair costs; and it can save money in liability because Ozinga will have a record of the trucks' maintenance to make sure that everything is up to date.

To ease into the data center consolidation project, Allen said, the company moved slowly and added one application at a time. That allowed them to monitor each application's performance on the IT side and to gauge user perception. Ozinga also added and upgraded WAN monitoring tools, which Allen called "a very important step forward" for the consolidation project.

Despite all the planning, when the TMT software was rolled out over the WAN, mechanics began experiencing problems immediately.

"We thought this would work great, and it didn't," Allen said. Mechanics encountered performance problems and freezing with the maintenance application.

To try to quell the problems, each site attempted its own fix. One site added bandwidth. Another tried using quality of service. But nothing worked. Consultants were called in for a second opinion but could find nothing wrong. Still, the application was plagued with jitter and freezes and deemed worthless by the mechanics whose lives it was supposed to make easier.

"Basically," Allen said, "it came down to this. It was a million-dollar rollout of this application that came to a halt because the mechanics said it was unusable."

Allen said he lost a lot of sleep racking his brain about the problem. His colleague, Alex Kropiewnicki, said he "turned to prayer."

The issue sparked dozens of meetings, and several potential solutions were discussed. One suggestion was to move everything to a Multiprotocol Label Switching (MPLS) network, but

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

Allen said that option was quickly dismissed because of the cost involved. Running MPLS to 21 sites would have added thousands of dollars a month to a budget that was already stretched too thin for comfort.

"Fortunately, we never got to that," he said, adding that Ozinga wanted to keep the WAN running with relatively inexpensive connections strung together with VPNs, an architecture that in the past had provided adequate performance.

Removing all video from the WAN was considered, because video applications are notorious bandwidth hogs. Ozinga had been using video for years to monitor concrete production.

"We had the same issue with jitter and packet loss," Allen said. The company determined that it had plenty of bandwidth for both video and the new truck maintenance applications to coexist in harmony.

Someone suggested WAN acceleration, but Allen and his crew were skeptical because most attempts to alleviate the problem had already failed. "We didn't have high hopes for it," he said.

Ultimately, the company tried it, using Citrix's WANScaler application accelerators. Application performance improved, and jitter, latency and congestion disappeared. The mechanics picked up on the change right away, Allen said. Once the 30-day product trial ended, the phone started to ring—with mechanics calling to ask what happened—because the application's performance had reverted to its old, slow ways. Ozinga was able to extend the trial until it could install accelerators at each location.

Having that application taken care of and out of the way, Allen said, let his team return its focus to its larger network upgrade projects.

"We're on a trend to continue to consolidate and move more applications into the central data center," he said. "We still have some applications distributed, like the mechanics' software used to be, but we're moving a lot of that."

3M prepares the network for VoIP

Accommodating roughly 300 locations in 80 countries, 3M Corp. is responsible for a lot of traffic flowing into and out of its network. And with a strong Web presence and increasing use of internal Web-based applications, the amount of internal and external traffic traversing the network has been increasing by several orders of magnitude.

According to Murray Butler, senior network analyst with 3M, that boost in traffic prompted networking pros

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

at the company to take a step back and re-examine the network to determine what types of strategic upgrades would aid in helping the traffic flow better and more reliably, while also keeping costs as reasonable as possible.

"Our big upgrade recently has been egress bandwidth," Butler said, adding that his team had to allow for more traffic to come in and go out. "There really just seemed to be a general increase in Web traffic coming in and going out."

Internal applications, which are mostly Web-based, included site-to-site applications, enterprise planning tools and other demand-side applications. That requires funneling a lot of traffic from external sites into the same pipes.

Using a centralized architecture, 3M attempts to provide most of its branch office server needs from a single location, Butler said. The company has whittled down the number of servers to avoid redundant purchases and equipment, ultimately cutting costs, and it has built Web-based applications and must allow them to be accessed from almost anywhere through a secure SSL connection.

"Traffic has just increased over time, and that made our current lines a bit over-utilized in some places," he said. "We have to make sure we have good baselines."

The bandwidth upgrade, while necessary to account for current traffic increases, also has an eye to the future, Butler said, as 3M continues to examine its plans for VoIP. While VoIP has been much contemplated, he said, the method of deployment has been an "ongoing debate."

Things can get tricky, because each business unit within 3M is fairly autonomous but still needs to use the company's centralized architecture for access to business-critical applications.

"VoIP is one facet of that," Butler said. "How can we do that and make it a generalized offering? How can we make it scale up and down? I need things to scale up and down."

Many VoIP vendors 3M has talked to offer ideas about how to scale up, he said, but scaling down—accommodating not only offices with 1,000 users but offices with fewer than 10—is a puzzle. At the same time, he said, 3M must determine how to manage VoIP centrally for consistency and supportability across the entire network.

Butler said he knows the benefits of a VoIP deployment, namely cost savings both on the back end and with connectivity, but figuring out the best

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

way to utilize it while upgrading the network to support it is the key challenge.

Working voice into the existing data lines will reduce provider infrastructure while also reducing 3M's need to utilize that additional infrastructure, something Butler called a "win-win."

Still, Butler said, there are a few nagging problems before VoIP can be given the green light. First, where will QoS play? "If I can do it and I can do QoS, I could have a very nice way of managing communications from here," he said.

Butler is talking to vendors to find a solution that fits the company's unique need to scale both up and down. From there, he plans to get the back end up and running—converting the standard phone system 3M is using now to the existing data lines is a good starting point, he said, before cutting over to VoIP. Then 3M would have to get VoIP to the desktop, deploying Power over Ethernet for every endpoint.

But still the big question is: "Do you want to mix the data and voice network or not?" Butler said. "I vacillate on that one daily. There are a number of steps to it, all to get it the way we want it. It's a tall mountain

Looking beyond VoIP to UC

THE BUSINESS GOAL for VoIP, said Murray Butler of 3M, is simple: It gives users portable, accessible and constant availability. Currently, many users have a cell phone, a desk phone, a BlackBerry and a PC or laptop. VoIP, coupled with unified communications (UC) tools, has the potential to break down those siloes of communication.

"It gives them one point of reference, one phone number," he said. "It gives them one point of presence."

And wrapping a UC model with capabilities like IM, chat, video and Web conferencing can add a great deal of flexibility, Butler said.

"I want my salesperson to be able to give a client a nice, elegant business card with just one phone number on it," he said. "But to get to that level, planning, projects, infrastructure and amazing amounts of scale are required for each level. We're starting with baby steps."

CHAPTER 1
NETWORKING EVOLUTION AND ROADMAP

CHAPTER 2
MOVING TOWARD THE APPLICATION-CENTRIC NETWORK

CHAPTER 3
UPGRADING DISTRIBUTED NETWORKS

CHAPTER 4
SECURING THE NEW NETWORK ARCHITECTURE

CHAPTER 5
CASE STUDY: TOMORROW'S NETWORK—TODAY

to climb."

And if bandwidth upgrades and VoIP conundrums aren't enough to keep the network staff busy, 3M has a few other upgrade tricks up its sleeve, Butler said, including changing and updating the streaming media and caching proxies and testing out WAN optimization tools in the lab.

"It's a new thing, something we have to make valuable and attractive before we deploy it," Butler said of WAN optimization. "We do it somewhat with Web application proxies and caching."

Also, he said, a lot of the tools 3M has bought can already handle the application load without the benefits of optimization, such as updated router cards that can handle the line speed.

Butler said his view of the network is that it is a tool that offers easy and ubiquitous access for users. He wants to fulfill the "expectation of dial-tone" and craft the network so it just works.

"My own personal view of IT is … IT is an enablement to help the business function better, quicker and faster," he said. "Network improvements facilitate that. As we're improving the network, we're improving its availability and stability for the users. It just makes life easier for IT and for the users." ■