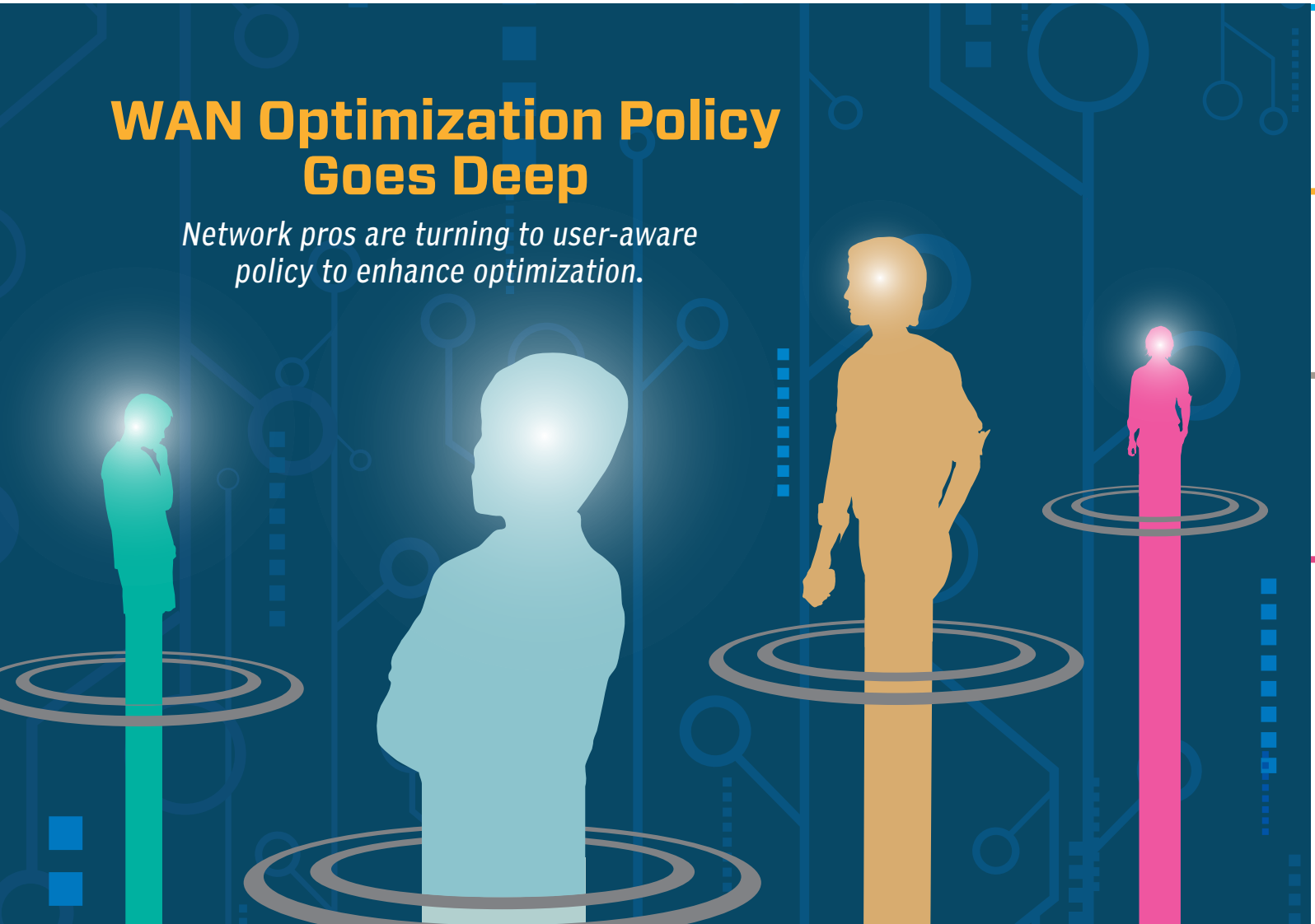
Network Evolution

JUNE 2013 \ VOL. 4 \ NO. 3



WAN Optimization Policy Goes Deep

Network pros are turning to user-aware policy to enhance optimization.

WAN is the new black. No, really.

EDITOR'S DESK | RIVKA GEWIRTZ LITTLE

The New WAN: Virtualization, User-Aware Optimization, and More

IN ALL THE hubbub about software-defined networking (SDN) and network programmability, it's easy to lose focus on traditional wide area networking technologies. Yet WAN innovation is plentiful these days, with radical developments in the way we architect and manage networks.

This innovation will be driven, in part, by SDN and network virtualization. New technology will enable a sort of WAN-on-demand where service providers and enterprises can automatically spin up virtual networks to interconnect data centers, campuses and remote offices. Soon these long-distance virtual segments will be able to cross network domains to enable granular routing across hybrid clouds.

But it's not just SDN driving the new WAN. WAN optimization itself is now being optimized. In this issue of The Network Evolution, we learn that WAN optimization and application acceleration can be improved by technology that lets admins prioritize applications and data according to user identity, location, time of day and other factors. With that, enterprises can better serve diverse branch offices and a wide range of remote workers who are accessing core applications on many different types of devices.

Beyond WAN optimization, we're seeing innovation in the way enterprises are building their WANs. In this issue, we learn about Ethernet-dedicated Internet (Ethernet DIA), which provides Internet connectivity over an Ethernet fiber optic connection with bandwidths ranging from 1 Mbps to 10 Gbps. Enterprises are turning to Ethernet DIA services to enable hybrid-cloud computing, handle bandwidth-intensive applications and to bolster their business continuity and disaster recovery strategies. Dedicated Ethernet is one of many examples of how enterprises are looking to service providers for WAN services that offer them on-premises style management capabilities in an external network.

Users will have to closely investigate the choices and travel what could be a bumpy road.

Yet, all of this is not to say that emerging technologies will completely displace legacy networks and the way we run them. As Marc Goodman writes in the new Voice of the Evolution blog: "With all of the potential problems that could occur with SDN implementation, you'd better take a really deep breath before diving in." With any new technology there are as many unanswered questions as there are potential advances, he points out. To enjoy the range of recent innovations, users will have to closely investigate the choices and travel what could be a bumpy road. ■

Rivka Gewirtz Little

Executive Editor, Networking Media Group

Diving into SDN WAN? Take a Deep Breath

With all of the potential problems that could occur with SDN implementation, you'd better take a really deep breath before diving in.

When I was a kid, my friends and I used to swim in a neighbor's pool every day in summer, and we would compete to see who could hold their breath the longest under water. I was pretty good, but in the back of my mind, I was always concerned about making it to the surface before my air ran out.

When I think about new technologies like software defined networking (SDN) that have the potential to cause sweeping new network advances, I think back to inhaling as much air as I could before immersing my head. With all of the potential problems that could occur with SDN implementation, you'd better take a really deep breath before diving in.

The promise of SDN WAN

When SDN first began to dominate conversation in the networking market, most thought of it as a data center technology. The idea was to decouple the control plane from the underlying physical network and then use a centralized controller to manage the entire data center network as one. This centralized controller would offer the ability to program specific flows between nodes and eventually enable network

virtualization where software network instances could be spun up on demand.

But soon SDN research turned to the WAN. After all, why not use the same architecture to manage the networks between geographically dispersed data centers and offices? We could even have the ability to spin up virtual networks over long distances that could cross network domains.

Going further, SDN could improve WAN performance and flexibility. WAN optimization vendor Silver Peak envisions enterprises and cloud operators using hypervisors to allow non-networking employees to directly manipulate and provision networking infrastructure to support their applications. For example, an employee from marketing, sales or finance could adapt network, storage and compute resources through a simple user interface to support a replication process.

Meanwhile application delivery vendor F5 sees SDN being used to manage Layer 7 networking services and to ensure security, acceleration, optimization and routing in the WAN.

Lots of Potential, But Even More Unanswered Questions

All of this is exciting, but the problems along the way will be plentiful.

For example, WAN disruptions could occur when adding a new software layer to create a virtual network that is independent from your physical network. Consider the potential management challenges that could arise from no longer configuring each WAN hardware device, but instead programming them all with centrally

managed software in a controller. It sounds great, but will this actually ease network management or make it more difficult? What's more, can one controller handle an entire WAN? If not, how will we manage an environment that must have multiple controllers? Will there be a controller of controllers?

Then there is the problem that multiple SDN architectures are emerging and it's increasingly difficult to know where to invest.

It's hard to feel confident in spending money on SDN-compatible network devices.

While the Open Networking Foundation is developing the OpenFlow protocol and the OpenDaylight consortium is expected to work on northbound application standards, some vendors in the meantime are developing proprietary strategies.

That can be a real problem when it comes to the WAN. What if an enterprise has deployed one SDN solution but later needs to integrate its WAN with a cloud provider that is using a different SDN variant? With all this uncertainty, it's hard to feel confident in spending money on SDN-compatible network devices.

I'm not saying SDN won't eventually be worth the investment. I simply think it's a good idea to take a deep breath before you take the plunge and evaluate how SDN might impact your business in the near and long-term. Will it allow you to break the surface victorious, or leave you gasping for air? ■

WAN Optimization Policy

WAN Optimization Policy Goes Deep

BY DAVID GEER

→ IT teams are setting WAN optimization policy that takes into account user, location and application type.

THE BRANCH OFFICE used to be uncomplicated. It housed small groups of workers—sales people, for example—who all worked on similar tasks and accessed a small group of applications. That simplicity is a thing of the past.

Now branch offices often house a diverse set of workers who need access to everything from virtual desktop to basic email, delivered on a wide array of devices. The sheer number of applications sent between remote offices, their headquarters and data centers, can strain the

WAN, even surpassing the limits of MPLS technologies.

So network managers and administrators are responding by applying application acceleration and WAN optimization policy that takes into account user identity and role, as well as location and even time of day.

This kind of granular policy setting can be accomplished with next-generation firewalls that are often attached to WAN optimization appliances.

Implementing WAN Optimization: In-Band or Out-Of-Band?

Before network managers move into setting user-based policy, they must first determine where a next-generation firewall or WAN optimization appliance would live in the network, as well as which kinds of applications actually need to be optimized or accelerated.

"You can put a WAN optimizer in-line with the network, such as behind the border router or firewall, and then it processes all traffic (either optimizing or bypassing optimization)," said Mike Fratto, senior analyst for enterprise networking at Current Analysis.

Engineers can also place the WAN accelerator out-of-band, where it is not in-line with network traffic. This lets the IT team decide which applications to send to the WAN optimizer to be optimized. "They would do this primarily because some traffic does not benefit from WAN optimization," Fratto said.

Real-time voice and video, for example, wouldn't need to be optimized since this

traffic is already compressed and doesn't repeat. Other examples include encrypted traffic, which is not predictable, and back-up data, which tends to be uniquely ordered.

"The decision to send to the WAN optimizer is made not about the user but based on the type of traffic. This is a common deployment option particularly in data centers or larger remote offices," said Fratto.

Once engineers decide which applications to optimize, things can get more complex. The next step is policy setting by identity, location, time of day or application type—and this can vary by the type of technology deployed for optimization.

"When we had the MPLS issue, we flipped over to our VPNs and realized we could still run. Our transactions were just a little slow"'

—Bryan Nash,
CIO, McHenry Savings Bank

A Bank Dumps MPLS for WAN-Optimized VPN

McHenry Savings Bank faced slow connections on its point-to-point MPLS network, which meant sluggish check image transactions and failed offsite backup replication.

"It worked perfectly in the test environment, but as soon as we came into production, with all the tellers signing on and all the VoIP going through, it killed the MPLS vendor's head-end router," said Bryan Nash, McHenry's CIO.

But when McHenry Savings Bank switched over to the new MPLS network, it maintained its backup connections over Dell SonicWALL firewall VPNs, using service from three ISPs. "When we had the MPLS issue, we flipped over to our VPNs and realized we could still run. Our transactions were just a little slow," said Nash.

The McHenry IT team ultimately gave up its MPLS and discovered it could mesh its entire network through the Dell SonicWALL firewall.

The only sticking point was latency that affected the check image capture application data stream. "Our images were taking forever to come across," said Nash. The bank must record a front and back image for every check and every ticket that goes with each check. The latency was unacceptable.

The McHenry IT team ultimately gave up its MPLS and discovered it could mesh its entire network through the Dell SonicWALL firewall.

"Since we had such a cost reduction by getting rid of the MPLS, we decided to look at putting in WAN accelerators to speed check image captures," Nash said. Nash contacted Dell SonicWALL about its new WXA WAN accelerators, asking for a product evaluation.

"They shipped me out three WXA WAN accelerators," said Nash. "We popped them in and my branches came back and said, 'I don't know what you did, but everything is just flowing really fast'."

The WAN accelerators also resolved an issue McHenry Savings Bank had been having with its offsite backup replications. The bank had been using the Data Domain backup product, which EMC acquired. "EMC applied a firmware upgrade and suddenly we could not get our replications to complete. While EMC was working on the issue, the McHenry IT team added the same WAN accelerators for a trial run. "When we did the WAN accelerator testing, it fixed our backups. Now our backups

are completing in less than two hours every night," said Nash.

WAN Optimization Policy That Starts With a Next-Generation Firewall

The Dell SonicWALL strategy applies application and bandwidth prioritization policy that can be based on employee and application hierarchies at branch offices.

To accomplish this, the Dell SonicWALL Next-Generation Firewall starts by fingerprinting applications as they pass through using Deep Packet Inspection (DPI) technology.

"We have 4,000 application use cases in 28 categories, representing over 1,700 individual applications in an application signature database," said Matthew Dieckman, SonicWALL tech director. The Next-Generation Firewall ties the application signature database to user identities through single sign-on technology.

The technology enables McHenry Savings' WAN administrator to look at program categories such as IM, for example, and applications that run between IM clients, such as FTP transfers. "The Application Control in the Next-Generation Firewall allows the administrator to control applications at the group level," said Dieckman. So the administrator can decide whether to allow IM use on a per-user basis depending on real business need, and whether those allowed to use IM can also facilitate FTP transfers between IM clients, for example.

The Next Generation Firewall passes application traffic that the bank permits and that the WAN accelerators can accelerate

on to those WXA devices. "The WXAs don't care; it's however you present the traffic to them. That's one of the nice things about it. It's all driven by policy," said Nash.

Going further, the bank's WAN administrator can also use bandwidth prioritization policies to limit access to sites, such as Facebook, that unnecessarily eat capacity. At the same time, however, "the administrator can also determine that marketing employees need access to Facebook," said Dieckman. "You can be very granular about what you want to accelerate," he said.

WAN Optimization-As-A-Service Tackles Slow Citrix and SharePoint

IT solutions provider Tavant Technologies ran into latency problems running Citrix for remote customer locations and SharePoint/Windows File Sharing between its offices in Bangalore, Delhi and Santa Clara.

Specifically, Tavant was experiencing Citrix log-on and screen refresh latency issues during peak times and the company was having challenges pulling up HR-related files from SharePoint across the WAN.

The solution to these problems was to use a WAN Optimization-as-a-Service solution that allowed the company to enforce optimization policy that takes into account user identity, time and location.

The company invested in cloud-based WAN Optimization-as-a-Service provider Aryaka, connecting customers into its WAN with varying access levels for prioritization and optimization. Tavant Technologies' logical WAN topology connects

multiple locations, including a primary data center in Santa Clara, a backup data center in Sacramento and offices in the U.S. and Bangalore. Each node of the Tavant ring network is connected directly to a node of the Aryaka ring network. Aryaka offers a combination of MPLS, VPLS and point-to-point links.

During peak times when customers are checking in software program code, they need priority access. "Policies set up in the Aryaka system give those users priority access on Citrix in terms of available bandwidth," said Sonal Puri, vice president of sales, marketing and alliances at Aryaka.

During peak times when customers are checking in software program code, they need priority access.

The log-in time is quicker when compared with a normal network connection and also the screen refresh time is much faster, said Anaand Papaiah, director of information systems at Tavant Technologies. The latency in the normal connect time is around three seconds, according to Papaiah, but Tavant customers see a real-time screen changeover on Citrix using Aryaka.

Tavant is also able to use Aryaka's technology to address latency in the SharePoint applications, which had become quite pressing. Tavant Technologies' CTO experienced challenges pulling up HR files in Excel from SharePoint across the WAN. "The CTO was in the Santa Clara office opening the Excel file from our SharePoint server, which is in Bangalore. It used to take at least 10 to 20 minutes" said Papaiah.

Using Aryaka's WAN Optimization-as-a-Service and Application Delivery-as-a-Service solutions, Tavant also set bandwidth policies based upon user, location, conditions and the application to speed SharePoint file sharing.

Applying Aryaka's acceleration proxies with its own controls and policies enables quicker refresh in SharePoint and removes some of the chattiness among the network protocols that can slow SharePoint down.

"Aryaka optimized the TCP stack to ensure that data flows smoothly. File transfers that took 10 to 20 minutes [were brought] down to about a minute by opening up the entire pipe and pushing the data through," said Puri. Likewise, Tavant created specific policy to address latency in sensitive applications, such as multimedia using TCP optimization in addition to acceleration proxies.

In User-Based WAN Optimization, Challenges Are Many

Success stories of granular WAN optimization policy setting are becoming more common, but plenty of challenges remain. In, fact most companies are still "optimizing all traffic ... for all users," Fratto said. These companies hold back from setting user-based quality policies because they haven't gone through the difficult process of breaking down roles and defining policies. What's more, doing so adds significant administrative overhead, as well as maintenance. Finally, administrators find it difficult to discern where to enforce role-based policy since many users of an application tend to need similar quality.

"Organizations are much more compelled to create user-based policies based on security needs. And if they have gone through that process, they are much more likely to have the roles already defined and can add quality policies on top," said Fratto. ■

Ethernet-Dedicated Internet

What is Ethernet-Dedicated Internet?

BY SALLY JOHNSON

→ Ethernet-dedicated Internet provides the strong upstream and downstream speeds required for hosting a Web presence, which is attracting many enterprises.

Ethernet-dedicated Internet

Access is a continuous, high-bandwidth method for enterprises to connect their local area networks (LANs) with the public Internet and streamline the performance of their wide area network (WAN).

Ethernet-dedicated Internet Access (Ethernet DIA) is also called dedicated Ethernet, dedicated Internet, business Ethernet or enterprise Ethernet. No matter

what you choose to call it, Ethernet DIA is an alternative to legacy technologies—such as T1 lines, frame relay and ATM—that typically rely on bonding multiple T1 lines or fractional T3 lines. These legacy WAN links cannot handle escalating bandwidth requirements for cloud computing, business continuity, business process automation, software-as-a-service (SaaS) and other applications.

Traditionally, enterprises relied on T1 access to the Internet. But as bandwidth requirements began doubling every year, many enterprises outgrew T1 and there was no logical way to grow or expand this type of Internet access.

A relatively new alternative, Ethernet DIA is delivered over a single Ethernet fiber optic connection and boasts bandwidth ranging from 1 Mbps to 10 Gbps. It provides the strong upstream and downstream speeds required for hosting a Web presence, which is the primary reason enterprises are buying it.

Even though this is still a new market, Ethernet DIA is taking off quickly. "An estimated 15% of enterprises are using Ethernet for dedicated Internet access today," said Nav Chander, research manager of telecom services and networks, IDC.

■ ***Who's Offering Ethernet DIA?*** More than 40 service providers in the U.S. offer Ethernet DIA, including "all of the big cable companies—Comcast Business, Time Warner Cable, Cox Communications, Charter, Optimum Light Path," Chander said. "These providers are now in direct competition with Verizon, and to a lesser extent AT&T, Level 3, and Century Link."

■ ***Advantages of Using Ethernet DIA Over Other WAN Technologies?*** At a basic level, Ethernet DIA is the same technology that enterprises use in their LANs, so the technology can use what enterprises already have implemented on their LANs and extend it to the WAN.

"By using a single technology, Ethernet, it sets aside much of the complexity of networking and enables the use of Ethernet at all sites—both on LAN and WAN. When its all Ethernet, it scales extremely well—from 1 Mbps to 10 Gbps," said Mike Tighe, executive director of data services at Comcast Business.

Ethernet DIA is an affordable alternative to multiprotocol label switching (MPLS). MPLS, traditionally used in high-performance telecom networks to direct data from one network node to the next based on short path labels, is a Layer 3 technology and much more complex than Ethernet.

Ethernet DIA's advantage over MPLS virtual private networks (VPN) is the policy control and management that customers have access to, according to Chander.

"Ethernet is a Layer 2 protocol, often used for data center applications or storage, because it works reliably and handles distances well. Since MPLS VPN services are often more complex to configure and change, many enterprises outsource it," Chander added.

Overall, it's much more difficult for enterprises to figure out how to transition from Ethernet on LAN to an IP-based WAN. "For enterprises with a very large global network, this is more efficient. But other enterprises prefer Ethernet throughout because they're comfortable with the

technology and it scales nicely from a Metro perspective," Tighe said.

■ ***What Are Enterprises Using Ethernet DIA For?*** Enterprises are turning to Ethernet DIA services for capacity up to 10 Gbps to support cloud computing and other bandwidth-intensive applications, as well as leveraging it as part of their business continuity and disaster recovery strategies.

"Ethernet is a key part of connecting to the on-demand or cloud virtualization world, where many enterprises want to offload their work to cloud-like managed providers such as Amazon Web Services," said Chander.

Ethernet DIA also helps enterprises handle massive amounts of data. "Facebook, for example, adds 7 terabytes of storage every month. Enterprises need to be able to share increasing amounts of data and transfer it. Many kinds of WAN technologies can transfer large amounts of data across cities, countries, and globally," Chander said. "Data center networking using Ethernet-dedicated services is one of the most economical ways to achieve that."

And enterprises are incorporating Ethernet into their business continuity and disaster recovery strategies. "After Superstorm Sandy, many enterprises realized that if their data center is close to the coast they need a strategy to back up that data as well as a way to reconstitute things if their primary data center goes down," Tighe said. "Enterprises view Ethernet as a fast and robust way to link data centers together, but it's also an ideal way to back up data." ■

WAN Security Options

Should Your Network Hardware Provider Be Your WAN Security Vendor?

BY PAUL KORZENIOWSKI

→ Network hardware providers and third-party vendors have very different WAN security offerings. How do you choose?

BEST-OF-BREED OR INTEGRATED solution? For years, IT departments have struggled to answer that question. Network vendors, such as Cisco and Juniper Networks, have carved out leading positions in WAN security, but along the way, dozens of third-party providers have emerged, offering features that often outdo the incumbents. Now IT pros must weigh the pros and cons in each type of provider, taking into consideration factors that range from cost to ease of management. What's more, they've got to keep an eye on the

emergence of virtual network security appliances and new programmable network architectures.

Why University of Kentucky Chose Cisco as a WAN Security Vendor

The University of Kentucky operates a WAN that provides access to 28,000 students and 12,000 staff and faculty members. The university relies mainly on Cisco routers and switches to move information from place to place, so when the network was deployed years ago, the IT team opted for Cisco firewalls.

One reason for that choice was that the integrated approach required less training. Typically, network vendors offer solutions that work with a common user interface and set of commands. "Our techs are more efficient because they only have to learn how to use one interface in order to control our network equipment and security solutions," said Doyle Friskney, CTO at the University of Kentucky.

In the old days, layering firewalls and antimalware on top of switches and routers seemed quite natural. "Network devices provided clear demarcations between internal and external communications and were a good place to install needed security checks," explained Pete Lindstrom Principal at Spire Security, an industry analyst firm. As the network equipment vendors added security tools to their product lines, they found ready-made customers, like the University of Kentucky.

Using integrated tools can also simplify the process of troubleshooting a complicated network. "Networks are becoming

more complex, so businesses need solutions that mask the underlying complexity," stated Kevin Beaver, principal information security consultant at Principle Logic, LLC, a consulting firm. As businesses extend their networks to more locations and support more devices, it has become difficult for support personnel to bounce among a number of different applications to pinpoint problems. In many cases, networking vendors have consolidated that information and can present support staff with the root cause analysis for any network or security problem.

Going with one vendor for integrated technology can also be less expensive than choosing a best-of-breed option.

By opting for one vendor, support requirements in this troubleshooting process diminish. IT teams only need to call one vendor to solve problems when they arise; they avoid the finger-pointing that sometimes occurs in multi-vendor environments.

"Customers develop a level of comfort when they work with a supplier for a long time," noted Principle Logic's Beaver. For instance, Cisco has built up a formidable presence in the enterprise, developed a robust channel to support its solutions, and has trained numerous network engineers. As a result, enterprises feel comfortable using its equipment and have little trouble finding individuals to operate its solutions.

Finally, going with one vendor for integrated technology can also be less expensive than choosing a best-of-breed option. When WAN network equipment and security solutions are bundled, suppliers often offer enterprises a discount.

That's a crucial factor since IT teams have so much trouble convincing C-level execs to fund security solutions. In many instances, management is reluctant to fork over the dough needed for security solutions because their payback is not always clear. "IT departments can wrap a few thousand dollars for security products into a multi-million dollar network equipment purchase," explained Spire Security's Lindstrom.

The Downside of Choosing a Network Hardware Vendor For WAN Security

Network hardware vendors might seem like the simpler choice for WAN security, but there are drawbacks. Most notable, security is not their bailiwick, so their products may not be as robust as those from specialists, such as CheckPoint, Fortinet, Palo Alto Networks and Sourcefire.

These third-party companies understand that the hardened perimeters enterprises have built are becoming weaker. Rather than attacking companies at the network level, hackers have now focused on application level attacks, such as exploiting flaws in programming languages and inserting bogus code into corporate applications and databases.

"Typically, the networking vendors offer generic security solutions rather than bleeding edge technology," stated Principle Logic's Beaver. If a business needs to solve a specific, uncommon security challenge, the security specialists usually emerge as the better option.

What's more, the network vendors can be slow to respond to new market drivers

while start-ups are more flexible. For example two years ago, Cisco outlined its new SecureX, architecture, which is designed to help companies establish granular corporate security policies. Rather than focusing on network connections, SecureX examines content traveling over a network and uses that information to enforce corporate security policies. But users viewed the project as overly complicated, and it remains largely a work-in-progress.

Networking vendors have had a checkered past in being successful in overcoming these bumps in the road. Several years ago, Cisco developed its own distributed denial of service (DDoS) security solution, the Anomaly Guard and Anomaly Detector Modules. However, the company phased out the products at the end of 2010 and recently began embedding Arbor Networks' DDoS technology directly into Cisco routers instead.

The Upside of Choosing a Third-Party WAN Security Vendor

Temple University, which has more than 35,000 students enrolled in 17 colleges on nine campuses, had no choice but to work with a separate network security vendor since its wired and wireless network provider Avaya Inc. never entered the security market. So the university went to Check-Point for its firewalls.

"We like having software based security solutions rather than hardware based systems," said Seth Shestack, Associate Director of Information Security at Temple University.

When customers choose a best-of-breed

provider, they can avoid getting locked into a one-vendor environment in their overall network technology. For example, many of Cisco's solutions work only with its own devices, so companies can find it difficult to integrate new network technologies as they emerge.

What's more, with equipment from third-party vendors, customers can integrate security into a greater network management strategy. For instance Riverbed and MacAfee recently teamed up, allowing enterprises to buy a one-box solution that includes the McAfee Firewall running on a Riverbed Steelhead WAN optimization appliance. This kind of approach can improve both the WAN optimization and firewall functions by sharing information between the two.

With SDN, network security can become almost completely driven by virtual appliances, and it can be granularly programmed.

Watch out WAN Security Vendors: Enter SDN

Sofware-defined networking may further weaken the networking vendors' hold on the WAN security market. SDN shifts the of focus maximizing performance and securing underlying hardware to creating software-driven, programmable networks that enable a whole new kind of security strategy.

With SDN, network security can become almost completely driven by virtual appliances, and it can be granularly programmed. In some cases, engineers will use SDN controllers to direct specific applications or traffic flows to certain firewalls,

offering varying levels of security depending on the application or traffic.

SDN is still in the very early stages. The University of Kentucky, for example, plans to deploy an SDN supporting only a few hundred users in the next three months to begin with, according to Friskney.

But the SDN movement will pick up and it will present significant challenges to traditional vendors. To date, these vendors' value has largely come from their ability to maximize the hardware that enterprises rely on to move information from place to place with security features.

With this new approach, software becomes more important and hardware could eventually become commoditized. In that case, enterprises could lose even further ground in the battle for the WAN security customer. ■

RIVKA GEWIRTZ LITTLE is the executive editor for TechTarget's Networking Media Group. She and the Network Media Group recently launched SearchSDN.com, a new site on software defined networking and network programmability.

MARC GOODMAN is a marketing consultant with over 30 years' experience as a marketing professional in the technology industry. He has a successful history of building leading brands for emerging companies, managing corporate and product marketing strategy, and working in the trenches on tactical program implementations.

PAUL KORZENIOWSKI is a freelance writer who specializes in data center issues.

DAVID GEER writes about security and enterprise technology for international trade and business publications.

SALLY JOHNSON is the feature writer for TechTarget's Networking Media Group. She writes about networking, data centers, cloud computing and network management topics for SearchNetworking.com and SearchEnterpriseWAN.com.

TechTarget

Network Evolution
is a SearchNetworking.com e-publication.

Kate Gerwig, *Editorial Director*
Rivka Gewirtz Little, *Executive Editor*
Kara Gattine, *Senior Managing Editor*
Shamus McGillicuddy, *Director of News and Features*
Chuck Moozakis, *Site Editor*
Sally Johnson, *Feature Writer*
Rachel Shuster, *Associate Managing Editor*
Linda Koury, *Director of Online Design*
Neva Maniscalco, *Graphic Designer*

FOR SALES INQUIRIES, PLEASE CONTACT:
Doug Olender, *Vice President/Group Publisher*
dolender@techtarget.com

WEBSITE Visit us
E-MAIL Contact us
TWITTER Follow us

TechTarget, 275 Grove Street, Newton, MA 02466

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.