UTM

SECURITY MADE SIMPLE

Unified threat management offers small businesses ways to manage many security functions without a large budget or extra manpower.

Small business networks are as much at risk from cybercrime as large enterprises. Consider that Panda Security recently published its "International Barometer of Security," and of the 1,500 small- and medium-size business (SMB) respondents, a staggering 46 percent have been infected by an Internet threat this year.

It's obvious that small businesses need a simplified, yet effective and comprehensive, network security approach. It should be one that they can afford to maintain but which is also easy to operate.

First entering the marketplace in 2004, the unified threat management (UTM) solution was developed to fill this vital need. Available as hardware or software, UTM packs multiple security and protection functions into a single soluton.

Unified threat management simplifies the security management workload through centralization and simplification of the technology tools necessary to provide adequate protection for a business' data assets. And these tools can help maintain IT security overhead and budget for most small businesses.

Smaller Companies Face Threats

Why small businesses are failing to provide adequate network and data protection is no mystery. Obviously, network security costs money. And that can be in short supply, especially during tough economic times. As WatchGuard Technologies' director of product management Tim Helming says, "Every dollar is precious."

There has always been a perceived tradeoff between having effective network security and the cost it involves. "When we look at small companies, we see they are getting hit by the general attacks," says Ashok Madanahalli, head of appliances and product management at Check Point Software. "However, they want the same protection as the banks and large enterprises."

But small businesses do not have multimillion-dollar budgets or enterprise-level IT resources to deliver this protection. In fact, the lack of security expertise and tight budgets related to tough economic conditions means small firms are hard pressed to secure their systems.

There is also more going on than simple concern over cost issues. "There is a failure to realize the nature of the threats out there," says Matt Dieckman, product manager for Secure Remote Access solutions at SonicWALL. "Ignorance is not the right word; it's more like, 'I'm a small guy. Why would someone come after me when they can go after the big fish?'"

Although small businesses may feel they are not under direct threat, it comes as a shock to find that they are actually prime targets. "Hackers don't care whether you are big or small," Dieckman says. "They are just looking for the least secured network. And often, those can be found in small businesses."

The idea that small businesses do not see themselves as prime targets is echoed by Jeff Wilson, principal analyst for network security at Infonetics. "When we look at network threats, we see two broad types: first, the specific targeted attack which most SMB's don't have to worry about," Wilson says.

However, the major threat facing any small company's network comes from the massive wave of generalized attacks through the web and e-mail, according to Wilson. "This is the major threat to small-business networks."

Bill McGee, Cisco System's manager of security solutions, agrees. "The focused attack is usually aimed at the big networks," he points out. "But even the smallest company is vulnerable to web and application-type threats."

Increasing Number of Threats

One leading security monitor has reported that web-based malware infection doubled during the second quarter of 2010. In fact, it topped the 1 million threshold for the first time with 1.3 million sites recorded as infected.

This is double what was reported for the year's first quarter, demonstrating the exponentially growing nature of the threat. But it's not just the growing numbers of attacks causing concern.

Even companies that have deployed a firewall are finding they are not effectively protected from the increasingly sophisticated array of web-based threats. Once a piece of malicious code has made it past the firewall, what happens then?

"We can talk about firewalling, but there is a general need for layer protection," says Check Point's Madanahalli. "This is where antivirus, antispam and malware security quickly enters the conversation."

"For instance, with Facebook, a user only needs to click on a link they think is going to take them to a video," says SonicWALL's Dieckman. "But it's very simple to hide

>>>

46%

[OF SURVEYED] SMBs INFECTED BY INTERNET SECURITY THREATS IN 2010[1]

[1]Source: Panda Security, International Barometer of Security (U.S. Edition), August 2010

Different UTM Flavors

Unified threat management can be delivered in a few different ways, via a physical appliance, a virtual appliance and/or software installed on a server at the edge of the network. Each method has its advantages and disadvantages.

Physical UTM Appliance

This is normally a proprietary piece of hardware installed at the edge of the network. In addition to easier installation and management, it offers a number of advantages including: validated hardware, simple upgrades, enhanced integration and more.

Virtual UTM Appliance

These rely on virtualization technology to operate. That means a virtual server must be set up on the network to run the virtual UTM appliance. In most cases, administrators will set up a VMware ESX server on standard server hardware to run the virtual UTM appliance as a guest operating system on the virtual server.

UTM Software

This is installed onto the server and then configured as services running on the server. This alternate approach to delivering UTM to the enterprise offers a few advantages including: integration, improved management, lower costs and more.

malicious code behind a video URL that downloads onto your network."

Chris Rodriguez, research analyst at Frost & Sullivan, is succinct in his view: "The key threat to small business networks comes from social networks and all the media that small business users are clicking. What's more, many small business owners may not be aware of the potential of this threat."

The issue is not just protecting the perimeter or gateway anymore. "Companies need to think beyond the simple firewall concept," says WatchGuard's Helming. "They need to look for a product that helps them define and enforce their business' relationship to the Internet in holistic terms."

Clearly, there is a major threat to small businesses and their networks. But how can they deploy effective protection in depth, that falls within their budgets and they can easily manage? One answer is with unified threat management.

Deploying UTM

UTM is a network security solution that has added to the functionality of traditional firewalls. In addition to a firewall, a UTM may include all or a combination of the following:

- Intrusion Prevention System (IPS)
- Data Leakage Protection (DLP)
- Antivirus
- Antispam
- Content filtering
- Virtual Private Network (VPN) capability for remote access
- Load balancing
- Simplified management reporting

Since UTMs first appeared on the market, they have experienced dramatic growth in response to the small business need for simplified, cost-effective network security. The UTM market clocked $1.7 billion in 2009, according to Frost & Sullivan's World Unified Threat Management Products Market Report released earlier this year. Market forecasts predict steady growth through 2011.

The primary value proposition for UTM appliances is that with one low-cost appliance, a network can be protected from a wide range of sophisticated threats. And it also requires only one deployment while being easier to use and manage than specific point solutions.

Small Business Network Protection

The traditional or point approach to network security called for having a separate appliance to perform each security function: one box for the firewall, one for antivirus, one for load balancing and so on. Many large companies and organizations handle security that way. However, they have the resources and budget to do so.

"With point solutions, you could have five different suppliers, five different products, five different management and support issues and five different security solutions which may not work well together," Madanahalli says. "This can be a real headache for any business, but impractical in a small-company scenario."

On the other hand, a UTM only requires one installation to perform multiple security functions and this provides several distinct advantages. "A UTM removes the need for multiple appliances," Dieckman says. "This reduces costs, and it is easier to manage because it is a simplified solution."

Frost & Sullivan's Rodriguez says there's an obvious business case to be made for taking the UTM approach. Small businesses can provide cost-effective solutions that address most of the key threats to which their networks are exposed. Meanwhile, costs are dramatically reduced because instead of five or more appliances to buy, deploy, manage and support, there is now only one.

A business need not fear that this simplified solution comes at the expense of delivering inferior network protection. Still, dealing with the quality of network security provided by UTMs requires more than deploying a box at the network gateway.

"There are the brains behind the box," Dieckman says. "The research and monitoring resources that are actively searching for emerging threats on the web are critical to maintaining effective network security."

But, some may wonder, do small businesses really need enterprise-class protection? "Many security professionals and vendors believe in providing best-of-breed protection, and there certainly is a need for that kind of protection," Rodriguez says. "However, most small businesses really need 'good enough' as opposed to 'best,' and that message has not been fully embraced by most small businesses." There is a bal-

ancing act between delivering necessary, effective protection, without increasing cost and complexity to a level where small businesses feel they are in a better place, assuming the business risk themselves.

Today, most users expect fast Internet access. Speed is crucial for many business applications, and a firm's employees (and customers) can easily become disgruntled with anything slowing down web transactions. But there's no need to worry about performance relative to deploying a UTM solution, WatchGuard's Helming says: "Bandwidth has become more available, and today's businesses demand security without sacrificing speed."

WatchGuard is not the only company to have dramatically improved performance. For example, SonicWALL's entry-level UTM has increased speed three-fold over the previous model.

UTM Solutions

The small business UTM space is dominated by some familiar names in network security: Check Point Software, Cisco Systems, Fortinet, SonicWALL, WatchGuard Technologies and others.

Check Point offers the Safe@Office and UTM-1 Edge appliances as entry-level UTM network protection appliances, which are suitable for small- to midsize businesses and remote workers. Starting at just less than $600 for UTM-1 Edge and $250 for Safe@Office appliances, small businesses can quickly and simply install best-in-class network protection, including a firewall, IPS and antimalware — with wired and wireless options.

Fortinet offers enterprise-class UTM protection that's ideal for remote and small offices, as well as retail installations. Its entry-level appliance is the FortiGate 30B, starting at around $250 (also comes in a Wi-Fi version) and providing simplified management control and configuration features. Fortinet UTM appliances also provide data loss prevention (DLP) and identity-based policies using the new FortiOS 4.0 operating system, which delivers protection from Web 2.0 threats that may elude other security solutions.

Cisco offers the SA 520 Series Security Appliance for businesses with fewer than 100 users and combines a firewall with VPN functionality and optional e-mail and web protection. The SA-520 delivers enhanced remote-access protection using optional VeriSign Identity Protection with two-factor authentication and onetime-use password access control. Pricing starts at around $420 for the basic appliance without optional protection modules.

SonicWALL's TZ 100 Series network security appliance delivers a powerful stateful packet inspection firewall, including real-time scanning which delivers effective and comprehensive network protection without affecting traffic throughput. Ideal for small businesses and remote workers, the TZ 100 provides antivirus, antispyware, IPS and content filtering with an SSL VPN for remote access as well as an IPSec VPN for site-to-site connection. It's three times faster than previous SonicWALL UTM appliances in this range, with an entry price of less than $275.

WatchGuard offers the XTM 2 Series, combining firewall and VPN functionality. A Wi-Fi version is available as well, featuring dual-band 802.11n for faster speed. VoIP support is included together with full HTTPS content inspection and a flexible management interface using a web-based, intuitive graphical user interface, complete with real-time monitoring and reporting as standard features.◊

Look to CDW to leverage the right threat prevention solution for your IT environment.

Small Business Sans Security

Many small business owners believe that larger corporations are far more susceptible to security threats than they are.

However, in reality, it's the other way around. Hacker attacks, spyware and viruses can be devastating to small businesses. Still, many small businesses are running without adequate security.

Check out these facts from Panda Security's annual International Barometer of Security in small- and medium-sized businesses:

- **46%** of SMBs have become victims of cybercrime
- **31%** have no antispamware
- **23%** have no antispyware
- **15%** have no firewall
- **13%** have no security protection at all

Source: Panda Security, International Barometer of Security (U.S. Edition), August 2010