SOPHOS

The Expanding Network Perimeter

How to Protect it With Unified Threat Management

By **Angelo Comazzetto**, Senior Product Manager, Network Security

As the perimeter of networks continues to expand—to include the cloud, mobile devices and a new generation of virtual road warriors—authenticating users exclusively through a network gateway is no longer enough to keep your network protected. Unified threat management (UTM) integrates endpoint protection and management on the same gateway, simplifying set-up and troubleshooting. A UTM provides a unified view of security to actively reduce management costs and downtime. This whitepaper explains how integrated UTM solutions protect your network, your data and your endpoints, no matter where or how your users connect.

The expanding definition of the network

Networks continue to evolve. Your data no longer originates from the same building or the same set of users. Remote locations are now connected over the Internet, helping multiple users to share the same data and easing employee collaboration by removing borders. Wireless users are everywhere. And the rise of the cloud and the popularity of mobile devices redefine the network for a new generation of virtual users.

As an information security professional, how do you manage multiple vendor endpoints in different locations (internal, remote, mobile and cloud), authenticate them, enforce policies on a case-by-case basis, and still secure access to your network?

One solution is a modern UTM product.

What is UTM?

The term "unified threat management" (UTM) was first used by IDC Analyst Charles Kolodgy in 2003.[1] This new term reflected the consolidation of technologies which, up to that point in time, performed separate security functions. Firewall, intrusion detection and intrusion prevention (IDS/IDP), and gateway antivirus, were now combined in a single, integrated network security appliance.

According to the Gartner Magic Quadrant for Unified Threat Management:

> Gartner defines the UTM market as multifunction network security products used by small or midsize businesses (SMBs). Gartner defines midsize businesses as those with 100 to 1,000 employees, and with revenue ranging from $50 million to $1 billion. However, the majority of midsize businesses' annual revenue is in the range of $100 million to $500 million, with head count ranging from 20 to 1,000 employees. UTM products for this market need to provide the following functions as a minimum:
>
> - Standard network stateful firewall functions
> - Remote access and site-to-site virtual private network (VPN) support
> - Web security gateway functionality (anti-malware, URL and content filtering)
> - Network intrusion prevention focused on blocking attacks against unpatched Windows PCs and servers[2]

See why Gartner named Sophos a Leader in UTM. Read the full report:

Sophos.com/magicquadrant

1. For example, see Wikipedia, http://en.wikipedia.org/wiki/Unified_Threat_Management

2. Gartner, Inc., "Magic Quadrant for Unified Threat Management, " by Joe Pescatore and Greg Young, March 5, 2012. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

While historically attractive to SMBs, UTM is lately gaining traction with very large companies with hundreds of sites, where each site can have 1,000 or more employees.

UTM empowers network administrators and the teams they manage to work more efficiently and productively. It means not having to manage and update multiple point protection solutions from different vendors with varying GUIs, interfaces and management consoles.

UTM delivers everything a security professional requires—firewall, antivirus, web content and mail filtering, application control and networking functions like routing and load balancing—in a single appliance. It offers simple set-up, improved troubleshooting and a unified view of an organization's security policy, reducing management costs and downtime.

Integration means simplicity

UTM is all about simplifying security, management, gateways, endpoints and end-user needs. Ultimately, UTM simplifies the IT administrator's job.

Managing multiple point-only products increases complexity. Administrators must master multiple management environments, all with unique terminologies and feel. They must maintain many firmware and pattern updates, and correctly configure the solutions to work with each other in the right way to keep the entire security deployment functioning.

Additionally, multiple network security solutions increase troubleshooting complexity since there are many points where misconfiguration and errors can occur. And multiplying the number of places (nodes, links, endpoints) administrators need to inspect to find the problem. Financially, the deployment of multiple point products becomes even less attractive when you add the cost of subscription services for support, maintenance and updates.

A single UTM appliance means having to master just one management GUI, pay subscription fees to one company, and troubleshoot any issues through a common management console. Further, the applications on a UTM device work together and complement each other to take advantage of running on the same platform.

For example, a UTM appliance can first decrypt incoming road warrior VPN connections such as IPSec or SSL, and then filter that traffic through an intrusion protection system. This clearly has advantages over point products, which you have to install in the correct order and then configure with complex routing and traffic handling rules so that proper filters are applied in the correct sequence.

What sets UTM apart from its firewall and IDS/IDP predecessors is the fact that, with fewer network "boxes" (including individual interfaces, configurations and subscriptions), it's easier to secure, manage and troubleshoot.

UTM and the network's expanding perimeter

Information and the processing of data tend to grow exponentially. Moore's law tells us that the number of transistors that can be placed on an integrated circuit doubles approximately every two years. It's also an accepted truth in the information industry that the network's perimeter continues to expand.

Every network has a perimeter—a gateway to the Internet. These perimeters can improve the way your business gets things done and help you manage your Internet-based activities. But the addition of technologies can make managing your network harder, because every gateway on your extended network must still be protected. Every technology is vulnerable to manipulation and compromise. That's true of any device that connects two networks (e.g., firewall, router and switch) or could give access to the network.

Security must be a primary concern when designing an optimum network. Even a single unsecured perimeter device could compromise your corporate network. A complete network security solution reduces the likelihood of an unauthorized intrusion by offering formal authentication, authorization, confidentiality, availability and integrity measures. These measures typically include encryption, certification, directory, network and other security components.

UTM serves as the traffic cop, enforcing perimeter security by inspecting packets and sessions to determine if they should be allowed on the protected network or dropped entirely. In effect, firewalls—especially second-generation ones—have become a single point of network access, analyzing and controlling traffic using firewall scripts that define application, address and user parameters. In turn these scripts help protect the connectivity paths to external networks and data centers.

Identifying devices that provide access to the network can help improve your network's overall security. You should consider each perimeter device as a part of the perimeter of the network. This includes network hardware devices, servers and all client endpoints, along with any devices that can be dynamically added in the future—for example, VPN clients. Once you have identified the area of your physical and virtual perimeter, it's easier to establish uniform authentication policies for every device and user.

See the evolution of network security over time.

Download our infographic

Protecting mobile users

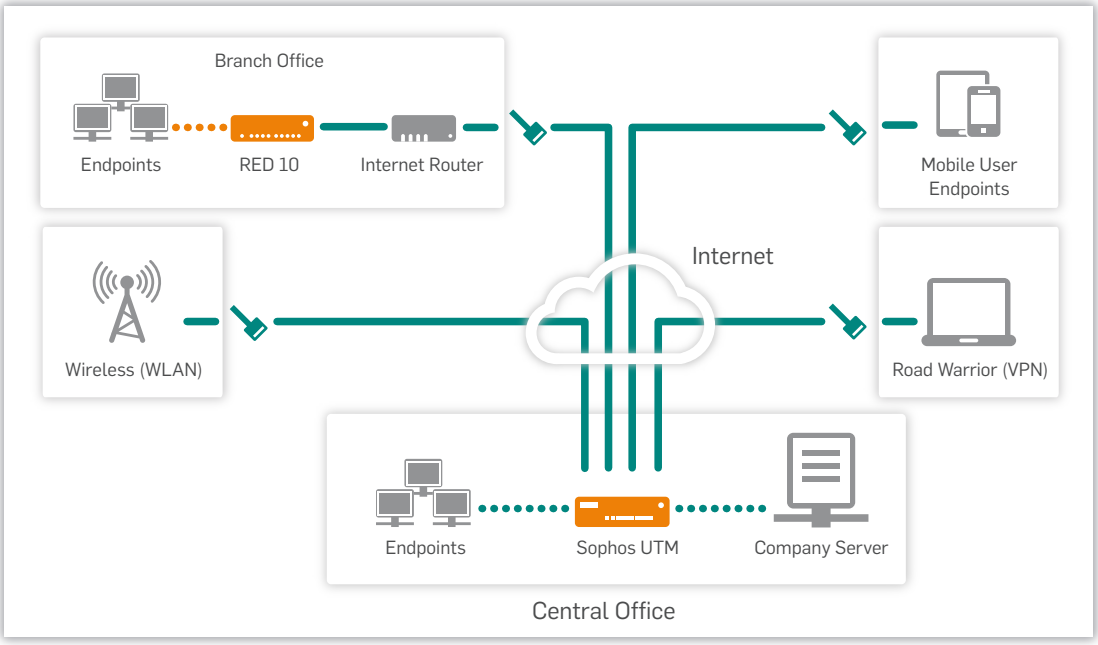
Users are getting more mobile every day. But they still need access to critical information that resides within the company network. Whether they are connecting from their home office, a mobile hot spot, a remote office, or a wireless PC on the company campus, they need as much protection as users sitting at their desk in the workplace.

Dedicated VPN and wireless products are often very complex to set up, requiring IT security know-how even for the smallest remote offices. As a result, IT specialists have to travel to remote locations and spend time setting up or updating VPNs and the equipment that supports them. It means buying managed VPN/MPLS services or leasing expensive lines to achieve a secure and stable connection back to the central office.

Wireless users and solutions pose similar challenges. You could buy consumer-grade products, but they are cumbersome to configure and lack central management. Or you could purchase a professional solution that requires five days of training before you send a single byte across your new wireless network.

With plug-and-play UTM products, you get antivirus protection, web content filtering, intrusion prevention/detection and much more. You can easily extend unified protection from a UTM appliance to remote offices and WLANs, without the trouble of integration planning and complex configuration requiring deep IT security knowledge.

Deployment scenario of Sophos UTM



You can easily extend UTM protection to remote offices, mobile devices, WLANs and road warriors.

Moving to the cloud

The expanding network perimeter has influenced the development of technologies that secure it. Perhaps the best example of this trend is "the cloud." As defined by the National Institute of Standards and Technologies:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[3]

As your organization moves data and processes to cloud service providers, a UTM solution can provide a secure gateway that's entirely under your control. For example, the Sophos UTM Security Gateway can support Amazon Machine Images (AMIs) running in the Amazon Elastic Computing Cloud (EC2).

The EC2 from Amazon allows you to run virtual machines within a scalable, reliable cloud infrastructure, without worrying about cabling or the need to ship appliances or rack-mount hardware. Users launch the UTM Gateway within the EC2 and in minutes can have a secure, scalable gateway solution of any size ready to support your business.

In production, users access EC2 and Sophos UTM Gateway to connect branch offices via Sophos RED (Remote Ethernet Device). Users retain a robust central point for VPN connections, and centrally manage Sophos wireless access points plugged into deployed RED devices.

Additionally, Sophos offers support for the Amazon Virtual Private Cloud (VPC) service that allows you to host and run your server infrastructure in a secure, scalable cloud. Our VPC connector gives you a permanent, encrypted connection to your VPC resources directly from the Security Gateway. Rather than configure technical hardware VPNs with BGP (border gateway patrol) capability by hand, our VPC Connector lets you download a single file from Amazon and upload it into your local gateway, which then builds the connection to your VPC automatically.

Sophos also offers a virtual appliance pre-installed and pre-configured for VMware environments. The first unified threat management product certified as VMware Ready, it allows secure and easy deployment of an all-in-one security solution within a virtual environment.

3. National Institute of Standards and Technology: http://www.nist.gov/itl/cloud/index.cfm

The limits of gateway-only network perimeter security

While large deployments of endpoint products have become easier to manage, by and large they remain dependent on the endpoints' operating systems and capabilities. However, security gateways are largely independent from the endpoint as well as the operating systems. Working transparently for the client and offloading all the workload from the endpoint to a central machine, gateways can also protect the network infrastructure to a degree an endpoint cannot.

Even with all these perceived advantages, there are drawbacks to gateway-only network perimeter security, including:

No control over data flow and leakage to portable USB devices. A big drawback of gateway-only security is it can't effectively control data downloaded to portable devices or transferred to other computers or the Internet via wireless connections, including Bluetooth or 3G USB flash drives.

Inability to protect mobile endpoints. Mobile endpoints like laptops or tablet computers lack important protections like antivirus, web filtering, firewall or application control when not communicating through the gateway (when at a hot spot, for example). Most of them only have minimal antivirus protection installed, which is managed through a different system.

Many gateway vendors are beginning to integrate endpoint clients into their gateway. But this integration is very loose. In most cases the gateway GUI acts exclusively as a launch point to a separate console for managing the endpoints. As a result you have to configure different policies for endpoints and gateways. With almost no integration between gateway and endpoint protection, you end up with inefficiencies in scale, poor productivity, and gaps in security.

Integrated gateway and endpoint network perimeter security

To this point, combining UTM and endpoint protection into a single platform has meant less functionality and less integration. In many cases, you'll only get antivirus on the endpoint. And integration means a link to another vendor's product.

No longer. By integrating endpoint protection and its management into the gateway, a modern UTM extends the network perimeter to the endpoint and the cloud. So your network and data remain safe from threats no matter where people work, what device they use, or where they connect.

The Sophos UTM gives you the capability to:

- Easily configure and monitor protection with a browser-based interface, but without deep technical knowledge
- Deploy a solution that integrates firewall and intrusion prevention with web control, email security and endpoint protection
- Protect your endpoints against threats and data loss while managing them from within your UTM appliance
- Secure branch offices quickly with integrated VPN technology and our plug-and-protect Sophos RED (Remote Ethernet Device)
- Provide complete UTM security for wireless networks and clients through dedicated wireless access points
- Deploy policies for web protection, firewall or application control. Policies only have to be configured once at the gateway and then synchronized with all endpoints, rather than configured separately for each one
- Always keep endpoints connected to the gateway without requiring directory services or VPN connections to headquarters

Sophos UTM means complete security for your business

Sophos UTM 9 gives you complete security within a single modular appliance. Without the complexity of multiple point solutions, it simplifies your IT management tasks, keeps you safe from viruses, spam and hackers, and keeps your employees working.

Full spectrum of security applications including firewall, VPN, IPS, email security, web filtering, antivirus, anti-spam, secure wireless connections, application control and endpoint security.

Connect branch offices and mobile users in minutes through our plug-and-protect VPN and wireless extensions.

Centrally manage antivirus and device control on all your endpoints and keep them up to date wherever they are (coming soon).

Integrated management of log data and spam quarantine makes external servers redundant.

All features available on all appliances means even your smallest location receives the same protection as your central office.

An open architecture that integrates features into a hardened Linux OS on standard Intel-compatible server systems, without the need for proprietary hardware chips.

Choose a hardware, software or virtual appliance. Each provides an identical feature set, including active/active clustering, WAN link balancing and Active Directory integration.

Easily configure and run our products without deep technical knowledge through our intuitive browser-based GUI—no command line interface or client software required.

Sophos UTM 9 helps you keep up with your network's changing and always-expanding perimeter.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

A Sophos Whitepaper 4.12v1.dNA

SOPHOS