A MANAGER'S GUIDE TO UNIFIED THREAT MANAGEMENT AND NEXT-GENERATION FIREWALLS

Key factors to justify and evaluate UTM and NGFW systems

This guide is intended to help executives and managers evaluate UTM systems by answering the following questions:

- Why invest in unified threat management?
- What is the difference between UTM and next-generation firewalls (NGFW)?
- Which security technologies should be included?
- What is important about ease of management?
- How can UTM systems protect employees at remote offices?
- What flexibility and future-proofing should be considered?

THINKING ABOUT UNIFIED THREAT MANAGEMENT

Unified threat management systems are one of the most widely used tools in the information security arsenal. Industry analysts at Frost & Sullivan estimate that more than 1.5 million UTM systems will be purchased in 2014 alone.[1]

The concept of unified threat management is very appealing: multiple critical security technologies, integrated on a single platform, provided by a single vendor.

But the process of evaluating UTM options is not simple. You may wonder: Is a UTM solution right for my organization? What security features are most important? What other issues need to be considered, such as ease of management and support for remote users?

SOPHOS

TechTarget Custom Media

[1] "Analysis of the Global Unified Threat Management (UTM) Market," Frost & Sullivan, Nov. 28, 2012

SMBs Suffering Data Breaches

55% of SMBs

Had at least one data breach

53% of SMBs

Had more than one data breach

31% of Data Breaches

Experienced by companies with 100 or fewer employees

WHY INVEST IN UNIFIED THREAT MANAGEMENT?

Experts agree that organizations of all sizes need to implement a "defense in depth" strategy to protect IT systems and data with multiple security technologies.

That's because enterprises face an unprecedented range of threats. Attacks come from cybercriminals intent on extracting confidential information about customers and employees, from state-sponsored hackers targeting intellectual property, from political activists trying to disrupt business operations, and from crooked or terminated employees seeking financial gain or revenge.

These parties may employ viruses and Trojans carried in email attachments, "drive-by downloads" from compromised websites, SQL injection and other attacks on Web applications, social engineering techniques to entice employees to reveal account information and passwords, and eavesdropping on wireless communications. Today, many use advanced persistent threats and "blended" attacks combining several of these techniques.

Small and medium-sized organizations are not immune: A Ponemon Institute survey of businesses with annual revenues of $10 million or less found that more than half (55%) had suffered a data breach and 53% had experienced more than one, while a Verizon study found that 31% of data breaches were experienced by companies with 100 or fewer employees.[2] And these figures are probably understated, because many small and medium-sized organizations are not able to detect breaches.

To address this wide range of security threats, IT organizations often implement and manage multiple security technologies. One approach is to select and deploy several products from different vendors. However, this requires installing and integrating multiple products, learning dissimilar management consoles, and managing updates and upgrades from several vendors.

The alternative is to deploy a UTM system: a selection of integrated security technologies, implemented on a single hardware or cloud platform, with one management interface.

The technical advantages UTM systems have over the integrate-it-yourself approach include:

- Simplified deployment, with dramatically fewer installation and configuration steps.
- Easier management, because there is only one management console and one update process.
- Faster troubleshooting, since there are fewer opportunities for conflicts between modules and there's no finger-pointing with one vendor providing support.
- Integrated reporting, with information from multiple security technologies in one place, in a consistent format, with useful correlations between different kinds of data.

These technical advantages produce concrete business benefits:

- Lower implementation costs
- Less demand on overworked IT staff
- Fewer security vulnerabilities
- Faster reaction to attacks
- Lower administrative costs (licensing, billing and support are from one source)

[2] See HSB press release: "Survey Shows Small Businesses Have Big Data Breach Exposure" (survey conducted by the Ponemon Institute); "2013 Data Breach Investigations Report," Verizon

The value of these benefits is reflected in the growing demand for UTM systems: According to the Frost & Sullivan study cited earlier, the worldwide UTM market is expanding at 17% annually, and in 2014 is expected to reach more than 1.5 million units and $2.1 billion in revenue.

WHICH SECURITY TECHNOLOGIES SHOULD BE INCLUDED?

Every enterprise needs to determine what security technologies are most important, based on a combination of:

- The type of attacker it is most likely to encounter: cybercriminals, state-sponsored hackers, "hacktivists" or insiders.
- The types of techniques these attackers are most likely to use, such as viruses and Trojans; targeted attacks using social engineering methods; denial of service; SQL injection, cross-site scripting and other attacks on Web applications; interception of emails and wireless communications; and abuse of privileges by insiders.
- The data and devices they need to protect—for example, information about credit card accounts and finances, health records, intellectual property and system passwords, on servers, laptops, tablets and smartphones.
- The consequences of attacks and breaches, including lost revenue and employee productivity, damaged reputation, regulatory fines and breach notification costs, and a lessened competitive position.

The IT staff also needs to consider the propensity of employees to open doors for some of these attacks by engaging in risky behaviors, such as clicking on links in emails from unknown sources, surfing to suspicious websites and using insecure public wireless access points.

The variety of threats—and abetting behaviors by employees—means that many enterprises must include a wide range of security technologies in their UTM system.

UTM vs. NGFW:
What's the Difference?

Most industry analysts define next-generation firewalls (NGFWs) as firewalls enhanced with intrusion prevention and application intelligence, and unified threat management (UTM) systems as products that include those features plus additional technologies such as email security, URL filtering, wireless security, Web application firewalls and virtual private networks. In this view, UTM systems include NGFWs as components. (For example, see the definitions of NGFWs and UTMs in the Gartner IT Glossary.)

However, many use the terms interchangeably, and some UTM vendors label their high-end offerings NGFWs.

In any case, we don't need to get wrapped up in semantics here: If you use the term "next-generation firewalls" in the broader sense, the ideas discussed in this paper apply to them as well as to UTMs.

Below is a breakdown of security technologies that should be considered. While this seems like a long list, all of the items are available in advanced UTM systems. And it is not necessary to deploy all technologies at once. With most UTM systems, organizations can implement the defenses they need at the moment and “turn on” others when the need arises.

Also, as we will discuss in the next section, one of the great advantages of the UTM approach is that many security technologies can be installed, configured and managed together, with far less effort than when technologies are deployed separately.

Security Technologies That Should Be Considered on UTM Systems, by Category

Network Protection

- Stateful firewall
- Network Address Translation
- Intrusion prevention system
- Flood-protection (DoS, DDoS, port scan blocking)
- Two-factor authentication
- Remote access and site-to-site VPN

Next-Generation Firewall Protection

- Application visibility and control
- Advanced threat protection
- Quality of service and bandwidth control

Web Protection

- URL filtering
- Spyware protection
- Antivirus scanning of Web traffic
- HTTPS scanning

Email Protection

- Antispam detection
- Quarantine of suspect messages
- Antivirus scanning of email attachments
- Email encryption and data loss prevention

Web Server Protection

- Web application firewall and reverse proxy
- Antivirus scanning for Web uploads and downloads
- Form hardening
- URL hardening
- Cookie protection

Wireless Protection

- Scanning of wireless as well as wired traffic
- WPA and WPA2 encryption
- Separate wireless zones for guest access
- Flexible hotspot authentication

Endpoint Protection

- Antivirus scanning on the endpoint
- Device control to prevent the connection of risky devices (e.g., USB sticks) and networking connections (e.g., Bluetooth)
- Endpoint data loss prevention
- Web protection for traveling users

CLICK HERE FOR...

More information on these technologies and their uses can be found in the **Sophos Network Protection and UTM Buyers Guide.**

WHAT IS IMPORTANT ABOUT EASE OF MANAGEMENT?

Staffing is a major concern in every IT organization. Everyone is being asked to do more with fewer people, and finding professionals with advanced skills is a challenge. Small and medium-sized businesses especially cannot afford to employ an entire team of security specialists.

These pressures are a major reason why UTM systems are popular. Compared with an integrate-it-yourself approach, UTM systems dramatically reduce the time required to evaluate, install, manage and update multiple security technologies. In most cases, they also reduce the learning curve, skill requirements and training needs. In fact, by reducing the workload, UTM systems often allow organizations to implement additional security defenses that would not have been feasible otherwise.

However, organizations should not take ease of management for granted or assume that all UTM systems are strong in that area. While some were developed with integrated management in mind, others are the result of vendors bolting together security products with different configuration processes and management consoles. Still others started as complex, highly tunable firewalls for large enterprises but were later "dumbed down" for smaller organizations. These UTM systems may be strong on functionality, but they require more knowledge and effort to operate.

When evaluating ease of management, organizations should consider the following factors:

1. Simple deployment. Factors that simplify deployment include:

- Features that work out of the box.
- Simple configuration processes with few steps.
- Identical features and configuration rules on systems of all sizes and all form factors (appliance, virtual appliance, software on server, and hosted in the cloud).
- Units that provide plug-and-play connection of remote offices without local IT staff.
- Parameter or configuration settings that can be recognized by multiple security technologies or modules.

An example of how integration simplifies deployment would be activating a Web content filter and having the change immediately recognized by the firewall. Without this integration, the administrator would need to first activate the Web content filter, then change packet filtering rules on the firewall, and then explicitly allow the retrieval of threat updates for the content filter.

2. Ongoing management. Capabilities that reduce the effort of ongoing management include:

- A single console to manage and track all security technologies on all the UTM systems in the enterprise.
- A single method to apply all types of malware and threat signatures to all locations.
- Automatic one-click updates of firmware and attack patterns.

Advanced management capabilities include system clustering and load sharing, as well as failover and fault tolerance. Such features improve performance and protect business continuity in the event of hardware or software failures.

3. Management by systems administrators instead of security specialists. Features that allow UTM systems to be managed by systems and network administrators include:

- Intuitive management consoles and user interfaces.
- Intelligent default configurations.
- Tight integration among security technologies, so configuration changes in one area do not conflict with settings in another.

Products that require command-line syntax for configuration or use obscure security jargon often need to be managed by security specialists. Another red flag is management screens with different screen layouts or processes to manage different modules of the system, which is evidence that modules have been bolted together rather than designed for consistent management.

4. Extensive reporting with local storage. UTM systems are easiest to manage (and forensic analysis is easiest to perform) when they include a wide variety of standard reports, and when log data and reports are stored locally on each system. Some UTM systems have few standard reports or charge extra for them, while other UTM products include low-end appliances with no hard disk and therefore no local storage for log and report data.

5. Freedom from reliance on end users. Some UTM systems minimize reliance on end users for configuration and support tasks with features such as plug-and-play appliances for remote sites and self-service portals where end users can view and manage their own quarantined emails.

Sophos UTM systems (and their Astaro predecessors) have long been noted for outstanding ease of management. For example, noting that basic setup and configuration could be accomplished in 10 to 15 minutes, a recent independent review awarded the Sophos UTM 220 model five out of five stars for ease of use.[3]

HOW CAN UTM SYSTEMS PROTECT EMPLOYEES AT REMOTE OFFICES?

One of the major challenges facing IT departments today is protecting workers and data at remote offices. The following help address this challenge while minimizing management effort:

- Remote office UTM devices that require no initial configuration and can be managed centrally with no support from remote employees.
- UTM systems that direct all wired and wireless network traffic from remote sites through the full UTM scanning process, to ensure that all emails and Web traffic are tested for threats.
- VPN clients for mobile and home workers that protect network traffic without any action by the user.

An example of an advanced feature for protecting data at remote offices is controlled wireless access for guests and contractors, which limits these users' access to restricted network segments for fixed time periods.[4]

WHAT FLEXIBILITY AND FUTURE-PROOFING SHOULD BE CONSIDERED?

Organizations need to select UTM systems that fit their immediate requirements. But because threats—and businesses—are evolving so quickly, they should also look for systems that are future-proof, in the sense of having capabilities that might be needed at a later date.

The most certain way to ensure that security technologies and management tools will be available in the future is to pick a UTM system that offers them today. While it may seem like vendors can always add new technologies to their product lines, there are often technical and business reasons why they never do.

Organizations also should look for a choice of deployment platforms. This allows them to choose the best platform for each location and type of office, and to evolve from one platform to another as the organization grows or its needs change. Platforms include:

- Software that can be installed on servers in the data center.
- Software that is available on cloud-based servers such as those hosted by Amazon.
- Traditional UTM (hardware) appliances with pre-integrated hardware and software.
- Virtual appliances (integrated software suites that can be deployed in virtual environments provided by VMware, Microsoft, Citrix and KVM).

Finally, to provide flexibility, organizations should look for a product line that ranges from small, economical boxes for small offices to systems that can handle millions of concurrent connections and gigabits of traffic per second for large offices. To simplify management, they should all provide a consistent set of features and be manageable from the same central console.

[3] Review of Sophos UTM 220, SC Magazine, March 1, 2013
[4] "5 Tips for Securing Your Wireless Network," Sophos

SUMMARY: WHAT DO YOU NEED FOR UNIFIED THREAT MANAGEMENT?

By integrating multiple security technologies, UTM systems can provide simplified deployment, easier management, reduced need for specialized personnel, and faster troubleshooting compared with an integrate-it-yourself approach to network security.

These characteristics ultimately lead to business benefits such as:

- Cost savings
- Fewer security vulnerabilities
- Faster reactions to attacks
- Fewer demands on IT staffs

Some of the key factors we have discussed are summarized in the table below.

10 Recommendations
A Unified Threat Management System Should:

1. Include all of the key technologies required by the business, such as network protection, next-generation firewall protection, Web protection, email protection, Web server protection, wireless protection and endpoint protection.
2. Provide specific security features the business requires, and offer free trials so they can be evaluated.
3. Be easy to deploy and configure.
4. Be easy to manage.
5. Be manageable by systems or network administrators rather than security specialists.
6. Protect workers and data at remote offices economically.
7. Be easy to set up and manage in remote offices without local support.
8. Run on a wide choice of deployment platforms, including appliance, virtual appliance, software on commodity servers, and hosted in the cloud.
9. Scale from economical boxes for small offices to high-performance systems for very large offices.
10. Provide identical features on systems of all sizes and form factors, to simplify management and scaling.

More information on

UTM requirements and Sophos offerings:

CLICK HERE TO... Request a free trial

Learn more about Sophos UTM ...BY CLICKING HERE

CLICK HERE TO... Compare UTM vendors

SOPHOS

SOPHOS

From network to endpoint to server security, our products are to be easy to install, configure and maintain. Whether your business has 5 or 5,000 employees, or even more spread across multiple offices, you'll know everyone is secure with Sophos.

Read more at www.sophos.com/products.