Realtime publishers
"Leading the Conversation"

The Essentials Series: Understanding & Responding to Network Threats

Managing Multi-Function Security Products

sponsored by
NOKIA

by Dan Sullivan

Copyright Statement

Managing Multi-Function Security Products

Consolidated, multi-function security products have matured over the past several years. These systems, known as unified threat management (UTM) systems, are a promising approach to improving the efficiency and manageability of security measures. This article examines several topics related to UTM:

- Characteristics of UTM systems
- Topics to consider when evaluating UTMs
- Benefits of a unified approach to security management
- Issues to consider with long-term use of a UTM system

We begin with a discussion of the types of security services provided by UTM systems.

Characteristics of UTM Systems

UTM systems consolidate several security functions in a single system. The functions provided in various UTM systems may vary but commonly include:

- Firewalls, which protect the perimeter of a network or different network segments by filtering network traffic. Firewalls may employ different levels of filtering, from relatively simple packet filtering in which decisions are made based on information available in a single packet, to stateful filters that use connection-level information, or application-level filters that take into account application-specific traffic patterns.
- Antivirus and anti-spyware systems that can detect binary patterns in files indicative of malicious software. Network-based antivirus and anti-spyware complement client-based anti-malware programs.
- Anti-spam filters, which detect and block unwanted, unsolicited email before it reaches email servers. Blocking spam on the network before it reaches the email infrastructure can significantly reduce the spam burden on email servers.

- Content filters block inappropriate content for business networks. For example, a content filter may block URLs to gambling, shopping, hate speech, or other content with no business purpose.
- Intrusion prevention systems (IPSs) monitor network traffic for distinctive patterns associated with attacks on servers or for traffic patterns well outside the norm for a particular network. In addition to detecting attacks, IPSs can take steps to shut down an attack without human intervention.
- Monitoring and reporting modules are another key element in UTM systems. These subsystems can provide broad information on the state of the network as reflected in the outputs of the countermeasures within the UTM system.

Different UTM systems may have a similar set of countermeasures but that does not mean they are indistinguishable from each other. Design decisions made when developing a UTM can yield varying results when the device is deployed.

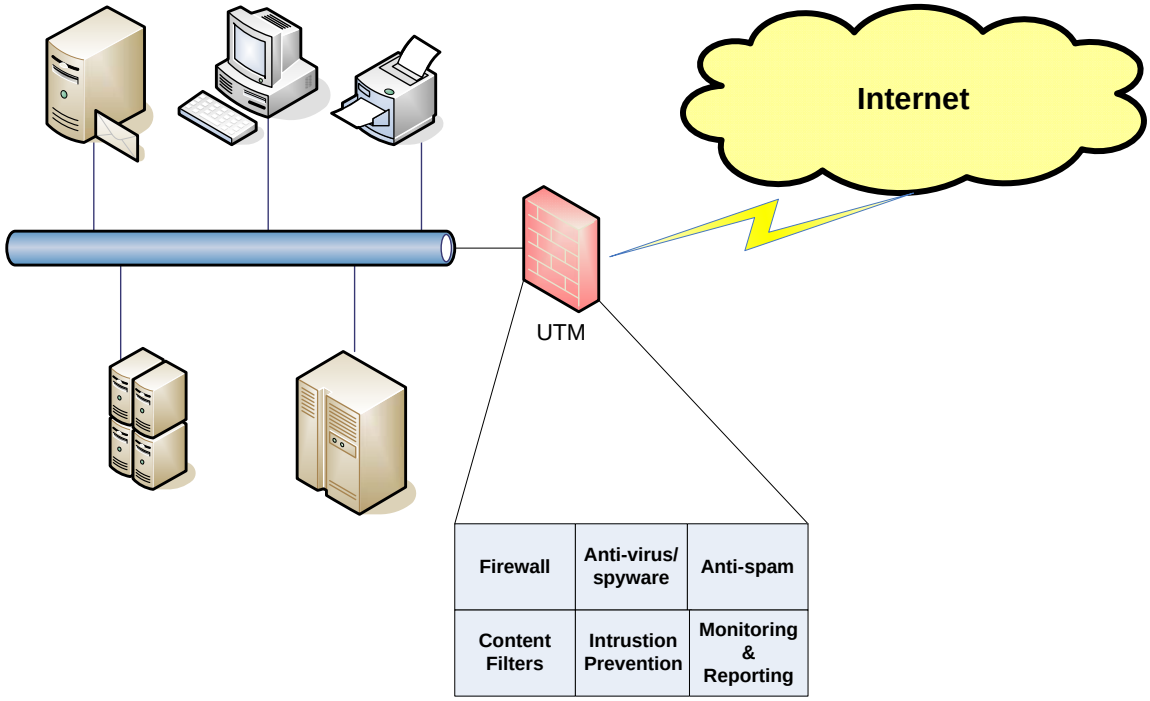

Figure 1: UTM systems provide multiple forms of protection to multiple types of devices on business networks.

Topics to Consider When Evaluating UTMs

Assuming UTMs under consideration meet the basic functionality requirements, other key considerations center on operational issues. These fall into several broad categories.

IPS Functionality

The first consideration is what services are needed and where are they needed. For example, IPSs are especially important on network segments with servers supporting critical applications, while anti-spam filtering is needed on paths of incoming email traffic. Concerns about insider abuse may lead to deploying IPSs on internal segments hosting databases while leaving content filtering for other deployed UTM appliances.

Performance

Performance is another issue to consider when combining services on a single appliance. It is especially important to understand dependencies between modules deployed on the same device. For example, will the firewall continue to function if the antivirus module is over taxed? How will the performance of other modules degrade if the firewall is countering a Denial of Service (DoS) attack? Performance problems can also arise as normal business traffic increases. Under these conditions, it is best to understand how the UTM device will scale and if a consolidated system is really the answer.

Load Balancing

One way to deal with increased traffic is to distribute the workload over multiple devices. This setup raises questions of the best way to balance the load across appliances, such as running multiple devices with the same applications or specializing devices to run only some security modules. The optimal configuration will depend on the particular traffic patterns and architecture of one's network, so flexibility with regard to deployment strategies can be a distinguishing feature among UTM devices.

Another question to consider during UTM evaluations is whether products have a modular hardware infrastructure that distributes processing power among the countermeasures to achieve the best overall performance. For example, can some of the security services be offloaded from the CPU to other elements so that cycles on the core processor can be freed for computational-intense services such as AV or IPS?

Maintenance Operations

Evaluators should also consider maintenance operations when evaluating UTMs; in particular, will maintenance to one module affect other modules? For example, could a maintenance patch to the antivirus module adversely affect the IPS? Also, changes to configurations could alter the way other network services are delivered, resulting in additional calls to the service desk. For example, applying more restrictive intrusion prevention rules could unintentionally block legitimate operations. How readily can the impact of changes be assessed and, if necessary, corrected?

As these topics demonstrate, a simple checklist evaluation of products is insufficient when it comes to assessing UTM products. Many of the factors that determine the success or failure of a deployment have to do with specific business requirements, the particular network architecture in which the device operates, and the type and volume of network traffic found in the environment.

Benefits of a Unified Approach to Threat Management

Properly evaluated and deployed, a UTM system can yield multiple benefits to an organization's security. UTMs offer consolidated reporting on the state of a network and associated infrastructure. One of the challenges with deploying multiple point systems to address specific security functions is that the reporting is not coordinated and the data is not normalized. Normalizing data from multiple sources is a difficult challenge; a generalized solution that works in a broad range of environments is still some time off. Management dashboards, however, can provide a single point of access to information collected from multiple security systems. By filtering, summarizing, and reporting on multiple sources of data, dashboards can reduce time required to analyze threat information and take appropriate action.

One of the greatest benefits of UTMs is that they can be deployed in smaller remote locations that would otherwise be held back by a lack of specialized security staff. UTMs can be centrally managed, so costs are minimized while still providing a significant set of security measures to remote offices.

Another benefit is that security controls can be selected as needed. Antivirus and intrusion prevention, for example, can be deployed at vulnerable points throughout the network while firewalls may be deployed only at the perimeter. This ability to control what modules are running and to deploy multiple UTM appliances or servers throughout the network ensures administrators will be able to scale the system with appropriate hardware configurations.

The result of benefits of consolidated reporting, selected security controls, and the ability to scale to the organization's needs have a direct impact on business. Systems administrators work more efficiently with consolidated reporting mechanisms that reduce the time and effort required to cull key information from potentially large volumes of raw data.

Summary

UTM systems offer a unique opportunity to mitigate multiple risks that exist today while gathering information to maintain an awareness of emerging and evolving threats and changes in networking patterns. here are two significant benefits of these systems. First, well-designed UTMs are easy to use—they offer reports and management dashboards that enable systems administrators to identify and address problems efficiently. Second, UTMs can be deployed to scale to the changing needs of growing networks, including demands for remote network management. These benefits, in turn, support the activities needed to maintain a governance framework necessary for compliance and to protect the integrity of business operations. Selecting the proper UTM, though, requires attention to a number of details, such as:

- Understanding the security services needed and their locations
- UTM performance
- Maintenance and management, especially with regard to remote locations

With a proper evaluation criteria based on these factors rather than a high-level checklist, customers can select the best solution for their requirements.