Cyberoam

Unified Threat Management

White Paper

The Unified Approach to Network Security: End of the Multiple Solutions Era

Lost in the Maze of Solutions

It's 1:00 p.m. in the afternoon and you receive a call from your office that your organization's network is down. As a system administrator, your job is to determine what happened, when it happened and how it happened and subsequently take steps to prevent future network outages. But at this precise moment, you visualize an array of appliances, neatly labeled Firewall, Gateway Antivirus, Anti-spam & Anti-Spyware, Intrusion Detection and Prevention, Content Filtering and VPN, all sitting in a row with cables worming in and out of them. Lost in this maze of networking, you look through various reports to figure out what has "actually happened." But there is light at the end of the tunnel enter Unified Threat Management (UTM) solutions.

This paper serves as an introduction to both traditional UTM and identity-based UTM, and discusses how a single appliance can provide all the benefits of multiple end-point security solutions.

Threat and Security: A Coexistence

Threat and security co-exist one would not survive without the other. But as threats continue to become more sophisticated, corporate security strategies begin to take precedence. To take a historical look at the security solution market, firewalls were introduced with the onset of large computer networks, which eventually led to desktop Antivirus solutions and gateway Antivirus, and most recently the advent of intrusion detection and prevention (IDP) solutions. Early solutions were mainly software specific, but dedicated hardware solutions coupled with software solutions and an underlying OS have also surfaced.

The evolution of security solutions has not been a logical progress, but rather one guided by necessity as advances in the security appliance market have primarily been goaded by increasing threat levels. Threats that started as viruses, have now graduated into sophisticated blended threats, which may consist of a mail-based Trojan that holds a backdoor open for a hacker to get in and ransack the network; a dissatisfied employee, who is out to 'get' the organization; or, more commonly, the average computer user who unwittingly falls prey to social engineering tactics.

In an effort to stay one step ahead, the security landscape is continuously working to learn the tricks of the hacker trade. But threats are very persistent and always present, so the moment the guard is down, threat triumphs. To address this challenge, small-to-medium organizations started deploying multiple end-point solutions, beginning with firewalls, and then implementing a variety of devices such as gateway Antivirus solutions, anti-spam and content filtering. Even now, organizations continue to layer their network with IDP and VPN solutions.

Multiple Solutions: One Threat Leads to Another

While it's clear that stacking appliances on top of each other may not be totally effective in addressing security challenges, blended threats cannot be tackled by just one security solution alone it's a 'Catch 22.' Blended threats leverage a myriad of tactics, and according to IDC, a leading global analyst group, perpetrators of malware have become more focused, gunning for quick and huge financial gains and are more apt to tap into an arsenal of attack measures to get into your network.

Security Threat	Type of Solution
Virus	Anti-virus
Trojan	Firewall, Anti-virus, IDP
Worm	Firewall, Anti-virus, IDP
Spam	Anti-spam
Spyware / Adware	Spyware Blocker
Unrestricted Surfing	Firewall, Content Filtering
Instant Messaging	Firewall, Content Filtering
OS Vulnerability	Firewall, Content Filtering, IDP
Rogue Intruders	Firewall, IDP
Hackers	Firewall, IDP
Internal Security Breech	Firewall, IDP
Remote Connectivity	VPN, Firewall, Anti-virus, IDP

As you can see, a single solution does not provide the necessary security coverage. But stacking 5-10 appliances on top of each other delivers operational challenges and could be a potential bottleneck.

Multiple Solutions Multiply the Problems

Multiple solutions are typically developed and managed by different vendors, which can pose a challenge when it comes to interoperability. For these single end-point solutions to be effective, every solution needs to be fine tuned by an expert and monitored within multiple network parameters. But many times these parameters are duplicated for different solutions, leading to redundancies, confusion and ultimately holes in the security infrastructure.

For example, if a blended threat is detected, multiple solutions will be configured separately to respond and could potentially fail to put up an integrated peripheral defense barrier. Each solution would be analyzing network traffic in its own way with its own set of native database signatures and policies to update all individually trying to provide "security." At the end of the day, this competition among appliances not only leads to ineffective security, but a costly drain on operational and IT resources.

Unified Threat Management Solution

Unified Threat Management (UTM) appliances are all-in-one security appliances for the small to medium business and branch office user market segments. They are fast replacing firewalls to offer comprehensive security to enterprises.

They carry firewall, VPN, gateway anti-virus, gateway anti-spam, intrusion detection and prevention, content filtering as basic features. The complete solutions offer bandwidth management and multiple link load balancing and gateway failover too.

A single UTM appliance makes it very easy to manage an organization's security strategy as it is one device to manage, providing one source of support that maintains the complete set of security features. UTM solutions are also a cost-effective investment, lowering the tax on resources and day-to-day costs to boost the bottom line.

UTM leverages a host of tightly integrated security solutions that work in tandem systematically to provide comprehensive network security. As there is a customized OS supporting the technology, the solutions work in unison and provide very high throughput. What makes UTM unique is its ability to bundle separate solutions that are designed to work together without competition. The solution's most important feature is its single, centralized platform that allows administrators to monitor and configure each of the solutions to reduce resource-draining redundancies.

However, most UTM appliances currently on the market focus only on IP address-based reporting and controls so we know where network activity is occurring, but we're still not sure who the actual user is. An employee or someone disguised as an employee? As internal and external threats continue to evolve, it's even more important to know who is accessing files and receiving malicious spam who is posing a threat to your network security?

Identity-Based UTM: The Solution for Today's Market

Over the course of the last few years, the security industry has seen major brand name organizations fall victim to massive data breaches. And it has become clear that in most cases, an insider was a party to these thefts. These internal threats grew in 2006, forcing more companies to monitor the information accessed and distributed by employees, and led to the Payment Card Industry's mandate of the Data Security Standard. Currently, traditional UTM devices do not have the ability to see who could be compromising an organization's network. But identity-based UTM appliances do.

Traditional UTM solutions are bound to TCP/IP protocol stack and only recognize the IP address of a machine on the network, not the actual user. But threats have become more sophisticated and rely on internal users to carry out their attacks, so monitoring the internal risks have begun to gain precedence creating a market demand for an identity-based UTM solution that connects to both the IP address and the user name or user group.

Now the decision to either allow or deny access to files, Internet sites and applications can be based on a user's access rights, determined by the user's or the user group's business needs.

A Wireless Scenario

The demand for identity-based UTM is clear when considering wireless and DHCP environments. The risks in wireless networks are equal to those of a wired network, but include risks introduced by new wireless protocols. In the wireless and DHCP environments, an identity-based UTM provides a second level of authentication to ensure the user identity is clearly established and information is not leaking out of the local network to an unauthorized user. If security is breached at a weak access point in the wireless network, an intruder will find that they are not allowed to access anything useful without proper authentication.

Identity-based UTM solutions are not only able to authenticate valid users, but are also powerful enough apply customized policies to either individual users or a group of users. Once anonymity is resolved, an organization can better enforce responsible user behavior, promoting user-centric network security versus just IP-address based security.

Conclusion

Many organizations find themselves stacking security appliances one on top of the other in an effort to address the daily challenges posed by emerging and known threats. However, if these solutions aren't apt to 'talk' to each other and work together, it can prove to be an ineffective security strategy leaving gaps in the infrastructure and wasting resources. While traditional UTM solutions solve the interoperability issue, organizations still need the granular visibility into the network that enables them to see who is accessing data, Internet sites and applications that cause increased internal risks. Identity-based UTM solutions address this market challenge, providing the interoperability and operational flexibility that organizations of all sizes demand.

