Unified Threat Management from Check Point

The security you need. The simplicity you want

Contents

Introduction

Over the past couple years, the marquee threats of the past—denial-of-service attacks, viruses, worms—have been joined by an expanding array of newer culprits. The more recognizable ones include information leakage/theft, phishing, spam, spyware, and a growing number of targeted attacks.

One possible response to this onslaught is to progressively roll out a corresponding set of countermeasures in the form of independent, single-function solutions, also known as point products. However, this causes the solution to directly mirror the diversity and complexity of the problem. Not surprisingly, evidence indicates that such an approach is not sustainable. Associated costs, such as operating a growing collection of tools, would continue to rise unchecked at the same time that threats inevitably find their ways through the gaps of this type of patchwork defense. It is expensive, inefficient, and ultimately ineffective.

Enter unified threat management (UTM) products. The goal of UTM is to simplify the overall security solution despite the growing scope and rising complexity of the security problem. The most apparent aspect of this simplification is the physical consolidation of point products into a single appliance, hence the term unified threat management. Unfortunately, some UTM products have little else to offer. Their level of simplification—not to mention security effectiveness—is significantly limited due to the relative lack of effort spent on other important characteristics and capabilities, including quality of individual security mechanisms, functional integration, and management unification. Although the concept and promise of UTM makes sense, not all UTM products have the same capability to make good on that promise.

Furthermore, this white paper will explore drivers leading to the emergence of UTM products and the inadequacies that many of them exhibit. This will be followed by the introduction of a new solution from Check Point. UTM-1 tackles the challenges facing many other UTM products while complementing other elements of the comprehensive Check Point strategy for UTM and enterprise security.

Complexity of the security problem

The scope and complexity of the network security problem is driven by underlying trends related to threats, vulnerabilities, and the adoption of new technologies. To better understand these issues we will explore them in terms of the functional, logical, and physical coverage of network security, which need to be accounted for when establishing a comprehensive security solution.

Comprehensive functional coverage

Ongoing trends applicable to the threat landscape include the following:

- Falling time needed to generate new threats—among other factors, widespread availability of malware development toolkits has reduced the time between the announcement of a new vulnerability and the launch of a corresponding threat to days
- Rising diversity of threats—it is no longer just a battle against viruses and worms. Information-stealing spyware, rootkits, Trojans, and countless phishing schemes have now joined the fray

- More elusive threats—blended threats are now status quo. By taking advantage of multiple exploit mechanisms, payloads, and propagation techniques, blended threats increasingly elude organization defenses and cause damage. Targeted attacks present even bigger problems—ones that are "purpose-built" to account for the unique characteristics of a given computing environment and its defensive configuration

Providing an adequate level of protection depends on architecting a security solution that incorporates a wide range of functional capabilities For example, firewalls should be complemented with intrusion prevention systems, and purely preventive mechanisms should be supplemented with intrusion-detection or log-auditing features. Combine these capabilities with threat-specific countermeasures such as antivirus, anti-spyware, and anti-spam, and you get a sufficient blend of defenses. However, functional blending alone is not enough. This concept needs to be extended to account for the logical coverage of a comprehensive security solution, which, ideally, would be bundled with messaging security update and support services.

Comprehensive logical coverage

The following highlights from the vulnerability landscape can help us better understand logical coverage:

- There are already many vulnerabilities that require enterprise attention. Approximately 5,000 vulnerabilities were disclosed in 2007 alone. And this number only covers the most common products. Many of these vulnerabilities were targeted by new malware and other attacks

- Vulnerabilities affected more than networking and operating systems. During parts of 2007, Web applications made up anywhere from 58 to 61 percent of documented vulnerabilities

- The number of vulnerabilities will rise. Whatever benefit is gained from coding improvement is far exceeded by the rate at which organizations adopt emerging technologies, buy or build new applications, or implement new versions of existing software. The result is a growing population of new code-flaw vulnerabilities and weaknesses introduced through configuration errors

Thus, we can conclude that a comprehensive security solution requires more functional coverage than ever before. It is necessary to address the capabilities associated with vulnerability management, including vulnerability alerting services, asset inventory and management, vulnerability scanning, and patch, configuration, and other remediation management tools. Identifying and fixing vulnerabilities is an effective way to help secure an organization's computing environment.

In addition, a comprehensive security solution requires complete logical coverage. Threats and vulnerabilities will need to be addressed at all network and application layers. Protection is necessary not only for network- and system-level components, but also for applications and data. Logical coverage is necessary to counter the prevailing trend of exploits happening at higher network and application layers. Hackers have pursued this approach because it enables them to elude lower-level network-layer countermeasures that organizations have deployed so far.

Enterprises must recognize that blended defenses entail more than implementing countermeasures that account for all security functions. With many of these capabilities—especially those focused on access control and threat detection—

it is necessary to address each logical network and application layer. In practice, a single device like a multi-layer firewall could do it, as could separate application- or technology-specific firewalls. While adding full logical coverage is necessary, it will not be sufficient in and of itself for network security.

Comprehensive physical coverage

The third dimension of network security, physical coverage, concerns increased user mobility, proliferation of remote offices, and greater interconnectivity and integration among organizations and their customers, partners, and other third parties. The primary issue is introducing more threat points with access to the organization network. These threat points also cause the data and resources requiring protection to be more highly distributed. As a result, organizations should no longer rely so heavily on countermeasures deployed primarily from their main Internet connections.

It is now necessary for organizations to provide comprehensive physical coverage. Main locations, branch offices, and even individual endpoints must be accounted for. Countermeasures need to be implemented at established boundaries, in closer proximity to important information resources, and at choke points on internal networks. It is important to consider the countermeasures needed at each location. Ideally, they should be multi-functional and multi-layered.

Sprawl of the typical security solution

The problems associated with the information security problem should not be taken lightly. The trends for threats, vulnerabilities, and technology adoption dictate architecting a solution that provides comprehensive functional, logical, and physical coverage. In doing so, coordination of processes, procedures, and tools will be necessary. And comprehensive security means reducing the sprawl of security solutions that has cropped up over time.

Individual aspects of the security problem and the products introduced to address them emerged over many years. Firewalls and antivirus led to virtual private networking. Denial-of-service attacks and worms drove the need for intrusion prevention and vulnerability management systems. Soon came instant messaging, P2P file sharing, and a dramatic rise in spam. Now we are dealing with information leakage, phishing, and spyware.

Largely, it has been unavoidable that organizations would wind up with a security infrastructure composed of numerous, disparate, disconnected countermea- sures. In recent years, organizations have come to understand that a patchwork approach is not only unsustainable, but it leads to disadvantages that include:

- High capital costs—each security issue requires a separate, expensive IT project
- Runaway operating expenses—all security products and systems must be operated and maintained individually, but still coordinated in some fashion
- Incomplete and/or ineffective coverage—organizations will forgo a product with unique capabilities if it overlaps significantly with its installed base, leaving network security gaps. And since products are configured separately, conflicting or incomplete rule sets can occur due to false assumptions about which products treat which threats

As a result, most organizations now realize that when they build a comprehensive security solution they must emphasize simplicity in the infrastructure and its management.

Unified threat management—a fundamentally simpler approach

Unified threat management involves combining multiple functional and logical security capabilities in a single product. UTM directly targets the enterprise need for simplicity, but it is not designed to tackle every security issue. Instead, it takes on a significant number of security issues that can be addressed with a compatible set of network technologies including firewall, VPN, antivirus, and intrusion prevention. It does not eliminate the need for other countermeasures.

UTM can also lower costs and improve security not just as a result of physical consolidation, but because of integration and unification of underlying security services and how they are managed. In reality, many UTM products fall short because they exhibit one or more deficiencies, such as:

- Not using best-of-breed security components
- Not supporting a core capability like antivirus
- Little or no integration of individual security capabilities such as sharing security information and event management data, which would increase overall security effectiveness
- Insufficient performance or capacity of system resources to support operation of all services under normal and extreme conditions—i.e., during attacks or heavy network traffic
- Little or no unification of management capabilities in terms of policy development, event handling, logging, and reporting

For example, some UTM products utilize only best-of-breed security from market-leading solution providers. However, they completely lack integration, requiring the customer to purchase and operate a separate management application for each security function. Others may provide better management, but lack the quality of individual security components.

Check Point UTM-1—simplicity without compromise

UTM-1 is a Check Point appliance that provides extensive functional and logical network-based threat management and security coverage. It does so without exhibiting the shortcomings of other UTM offerings. UTM-1 delivers proven, tightly integrated security to achieve an ideal blend of simplicity and high levels of security effectiveness.

UTM-1 provides extensive functional and logical coverage

UTM-1 appliances examine hundreds of predefined applications, protocols, and services out-of-the-box, ensuring that the vast majority of programs are threat-free entering or exiting the network. This includes common and emerging applications that are difficult to secure, such as Voice over IP (VoIP), instant messaging, and P2P file sharing. Overall, UTM-1 goes well beyond typical UTM products in terms of the scope of security coverage that it provides. Specific capabilities include:

Multi-layer, stateful firewall

Based on FireWall-1®—the industry's most proven firewall for more than 10 years—UTM-1 provides robust traffic inspection and access control for network-layer protocols and services and a growing list of applications—an essential UTM capability—because threats continue to exploit application-layer vulnerabilities.

Intrusion prevention

UTM-1 includes a number of mechanisms for identifying and responding to threats directed at any network or application layer. Among these are a vast collection of signatures and heuristics that can address both known and unknown threats. Backed by an expert threat and vulnerability research team, UTM-1 can receive timely updates via Check Point SmartDefense™ Services, which ensure protection from even the latest, emerging threats.

Antivirus

Gateway-based antivirus effectively complements desktop antivirus. For UTM-1, an ICSA-certified antivirus engine provides it with the capability to scan email (POP3 and SMTP), file transfers (FTP), and Web (HTTP) traffic in real time for possible threats hidden inside legitimate content.

Messaging security and anti-spam

Messaging security and anti-spam, including the Check Point six dimensions of comprehensive security, provide a solution that offers six protections for enterprise messaging infrastructure: IP reputation-based anti-spam, pattern-based anti-spam, administrator-defined block/allow lists, email antivirus, Zero-Hour malware detection, and email intrusion prevention. This multi-dimension approach protects the email infrastructure, provides highly accurate spam protection, and protects organizations from a wide variety of virus and malware threats within email.

Anti-spyware

UTM-1 includes two anti-spyware-specific features: SmartDefense-supplied signatures, which enable the gateway to stop spyware communications, and a Web filtering engine that can block access to known spyware sites.

Web application firewall

Web Intelligence™, an optional component of UTM-1, is a Web application firewall that protects against attacks such as cross-site scripting, directory traversal, and SQL injection. By incorporating the patent-pending Malicious Code Protector™, it also detects and blocks buffer overflow attacks and malicious executables that target Web servers. Uncommon among UTM products, these capabilities enable organizations to implement a Web application firewall without purchasing a separate solution.

One-Click VPNs

Secure site-to-site and remote access VPN communications can be established in just One Click with UTM-1. By establishing security parameters and identifying community endpoints, VPNs can be enabled automatically among all associated gateways or between a gateway and remote users. New endpoints added to the community inherit the same properties and are automatically configured for VPN communications. In addition to out-of-the-box support for IPSec tunnels, SSL-based access can be implemented—without separate hardware—by licensing the Check Point SSL Network Extender™ plugin.

Web filtering

UTM-1 can control access to specific Web sites with built-in Web filtering. The UTM-1 Web classification database is among the largest and most accurate in the industry, maximizing the value proposition of Web filtering. Benefits include enhanced employee productivity, reduced corporate liability, increased network bandwidth, and lowered malware exposure.

Integrated endpoint security

An optional module of UTM-1, Check Point Endpoint Security On Demand™ helps ensure that unmanaged computers—even those outside the control of the IT department—do not introduce threats into the corporate environment. It inspects unmanaged computers for malicious software and enforces policies for up-to-date antivirus, presence of a personal firewall, and so on prior to granting network access.

UTM-1 Total Security value proposition

According to the IDC study "Is UTM a Threat to Routers? We Think So!," the advantages of UTM appliances over routers "are numerous." It goes on to state, "UTM devices are the choice for many organizations because of their convenience, ease of installation, affordability, security, and centralized management capabilities."

In keeping with the spirit of that study, the Check Point family of UTM-1 Total Security appliances offer a compelling valued-added proposition with all-inclusive, turnkey solutions that deliver everything you need to secure your network in a simple, cost-effective way. Each solution includes the proven security features you need along with complete security updates, hardware warranty, and reduced support costs for up to three years. Based on the same Check Point technologies that secure the Fortune 500, UTM-1 appliances provide uncompromising security with streamlined deployment and administration.

No compromises

The scope of security coverage provided by UTM-1 is impressive. However, it is important to realize that no compromises have been made integrating these capabilities. The following points prove every effort has been made to maximize the benefits of UTM-1:

1. Each security capability included in UTM-1 has a track record of superior effectiveness, consistent with the Check Point history of providing innovative, best-in-class security

2. There are UTM-1 appliances to meet the performance needs of every size of organization. Performance ranges from 400 Mbps firewall and 100 Mbps VPN throughput up to 4.5 Gpbs firewall and 1.1 Gbps VPN throughput.

3. Management functionality is robust, integrated, and easy to use. With its setup wizard, initial deployment and configuration can be accomplished in less than 10 minutes. Once set up, UTM-1 appliances can be centrally managed from Check Point SmartCenter™. As an optional, embedded component of UTM-1, organizations can implement SmartCenter without deploying a separate,

dedicated system to manage UTM-1 appliances. Specific capabilities of SmartCenter include:

- SmartDashboard™, which enables centralized, cross-functional configuration of security policies. Sites and gateways can be managed individually or simultaneously, reducing administrative burden and ensuring consistency across the network
- Version control for all security objects and policies to support quick roll-back and applicable audit requirements
- SmartView Monitor™ and SmartViewTracker™, which provide comprehensive logging, real-time monitoring, and in-depth, customizable reporting, offering valuable insight into real-time security issues as well as the ability to track trends and developments

4. UTM-1 is reliable by design. As a purpose-built solution, sufficient resources have been designed into it. In addition, with several models to choose from, customers can pick the UTM-1 appliance with the performance and capacity that matches their needs. And UTM-1 supports clustering and back up network connections.

5. Updates via optional SmartDefense Services—which provide ongoing, automatic updates to defenses, policies, and other security elements—ensure that UTM-1 security engines can counter emerging threats. Other optional modules enable organizations to build systems that fit their requirements and to make modifications as their needs change.

Check Point appliances solutions—physical coverage and the bigger picture

Physical coverage is a critical objective of a comprehensive security strategy. So realize that UTM-1 alone may not be enough to secure your perimeter. Check Point also offers UTM-1 Edge™ appliances with lower throughput for smaller enterprises and branch offices at a more cost-effective price point. In addition, VPN-1 UTM is a Check Point software option that can be installed on your choice of hardware for the high-performance, high-capacity requirements typical of larger enterprises. Beyond the need for a UTM solution, if an even higher-performance solution is required, Check Point also offers its OpenChoice offering of IT security appliances, providing customers with the greatest choice for deploying our award-winning security solutions. Customers can deploy Check Point software on open servers, Check Point appliances, Check Point Integrated Appliance Solutions, or dedicated appliance platforms from partners such as Crossbeam and Nokia. All Check Point appliances are built around a unified security architecture, enabling organizations to perform all aspects of security management via a single, unified console. This offers customers the flexibility to deploy a complete security solution on their choice of hardware platform. See the Check Point Appliance Ecosystem: OpenChoice brochure for more information.

Conclusion

For most organizations, the complexity of information-security infrastructure has risen in lockstep with the growing diversity and complexity of computing systems and their arrayed threats. The result has been spiraling costs with diminishing returns of effectiveness. Unified threat management products can help address this situation by simultaneously simplifying network security and lowering associated costs, while strengthening organization defenses. However, many UTM products focus solely on physical consolidation and fail to fully deliver these benefits. In contrast, organizations will not be shortchanged with UTM-1. Purpose-built as a UTM solution, UTM-1 combines an unmatched range of best-of-breed security components, multi-level integration, and unification with its management capabilities for fundamentally simpler network security.

About Check Point Software Technologies

Check Point Software Technologies Ltd. (www.checkpoint.com) is the leader in securing the Internet. Check Point offers total security solutions featuring a unified gateway, single endpoint agent, and single management architecture, customized to fit customers' dynamic business needs. We are unique in this offering as a result of our leadership and innovation in the enterprise firewall, personal firewall/endpoint, data security, and VPN markets. The pure focus of Check Point is on information security. Through its NGX platform, Check Point delivers a unified security architecture to protect business communications and resources, including corporate networks and applications, remote employees, branch offices, and partner extranets. The company also offers market-leading endpoint and data security solutions with Check Point Endpoint Security products, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point award-winning ZoneAlarm solutions protect millions of consumer PCs from hackers, spyware, and identity theft. Check Point solutions are sold, integrated, and serviced by a network of Check Point partners around the world, and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters

3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: **http://www.checkpoint.com**

Check Point®
SOFTWARE TECHNOLOGIES LTD.