



Virtual Private Network (VPN) Security Monitoring Technical Brief

CounterStorm, Inc.
15 West 26th Street, 7th Floor
New York, NY 10010

212-206-1900
info@counterstorm.com
www.counterstorm.com

Executive Summary

While the popularity of VPNs continues to grow, the technology has also become a significant source of malware infections. The mobile and third party devices (unmanaged devices) of company employees are often unprotected and unpatched, and they are also exposed to the Internet, where worms and viruses can infect them at any time. Once the users of these unmanaged devices connect to the corporate network through a VPN, they may unwittingly release and propagate the malware they have picked up outside the corporate network. The types of malware typically introduced through VPNs include targeted and zero-day attacks.

To properly secure VPN access, companies first must recognize that network attacks are not always initiated from outside the corporate network, and that perimeter network defense technologies cannot protect them from attacks that originate on the network interior. To defend themselves against attacks initiated from the inside, companies must deploy specialized security devices at key points inside their networks. These internal network security devices must support a multifaceted network environment. They must adapt to future security threats as they arise. And they cannot rely on signature or patch based detection. New technologies are required to protect companies against threats to their interior networks, and to detect and block targeted and zero-day attacks.

Introduction

The virtual private network (VPN) has been adopted by many organizations looking to expand their networking capabilities while reducing their costs. The key feature of a VPN is its ability to use public networks like the Internet rather than private leased lines in order to allow remote users to access the corporate network.

In recent years, VPN has grown more and more popular as organizations seek to accommodate the increased mobility of their workers. Employees who travel or work remotely face a growing need to stay “plugged in” to the company network, and VPNs offer a convenient, cost-effective means of doing so.

VPN Security Issues

While the popularity of VPNs has grown, the technology has also become a significant source of malware infections. The mobile and third party devices (unmanaged devices) of company employees are often unprotected and unpatched. When these devices are exposed to the Internet, they may easily be infected by malicious worms and viruses. If the users then connect to the corporate network through a VPN, they may unwittingly release and propagate the malware they have picked up outside the corporate network. The types of malware introduced through VPN include targeted and zero-day attacks. Due to

their technological sophistication, these kinds of attacks are almost impossible to detect through traditional security products.

Furthermore, many large organizations have business partners whose respective networks are connected or peered to their own networks via a VPN tunnel. If these partner organizations do not have or enforce an identical (or stronger) security policy, they may become a logical point of approach for hackers who are looking to launch attacks.

VPN Security Needs

To properly secure VPN access, companies must recognize that network attacks are not always initiated from outside the corporate network, and that perimeter network defense technologies cannot protect them from attacks that originate on the network interior. To defend themselves against attacks that are initiated from the inside, companies must deploy specialized security devices at key points inside their networks.

Corporate networks are heterogeneous entities. Internal network security devices (INSDs) must, therefore, be able to support a multifaceted network environment and be able to function properly in unstable or unpredictable networks. They cannot rely on signature or patch based detection, since dangerous attack classes like zero-day and targeted attacks can usually evade these technologies. Finally, INSDs must be able to adapt to future security threats as they arise. Security threats are evolving constantly—and quickly. INSDs must be capable of evolving with them.

New technologies are required to protect companies against threats to their interior networks, and to detect and block targeted and zero-day attacks.

Limitations of Current Security Solutions

IDS/IPS

Since attacks that are introduced through VPNs enter through a trusted network (i.e. internally, rather than through the network perimeter), perimeter security devices—such as firewalls and intrusion-detection systems/intrusion-prevention systems (IDS/IPS)—cannot detect them. Furthermore, most IDS/IPS technologies do not support threat mitigation. If they detect suspicious network activity, these devices simply drop the offending traffic without providing feedback to the host (which may never know that it is infected and thus cannot follow the mitigation process). IDS/IPS devices are also unable to detect zero-day attacks, which exploit software vulnerabilities before fixes are readily available in the form of signatures and patches. Finally, they are powerless against targeted attacks, which use custom-created executables that are rarely detected by signature-based techniques.

NAC

One method for securing the network interior is to secure all end points that connect to it through the VPN: a device is allowed entry onto the network only if it passes network access control (NAC) verifications. However, as technologies evolve, almost all enterprise networks have become heterogeneous environments with a variety of hardware. A single corporate network may contain, for example, Windows- and Linux-based PCs, wireless PDAs, and portable computers. These devices cannot be fully protected by NAC solutions. NAC, which is designed to enforce corporate policy compliance, ensures that all company managed/supported devices have the latest software patches and signatures, the latest versions of anti-virus software, and perhaps a personal firewall. However, none of these security approaches can detect zero-day or targeted attacks, because they rely on signatures and patches which are not available at the time of the attack. Furthermore, networks will still be vulnerable even after patches and/or signatures are released as the security staff works to make sure they are deployed on all devices. This process can take anywhere from several hours to several days to accomplish, even under the best of circumstances.

NBAD/NBA

Most network behavioral anomaly detection/network behavior analysis (NBAD/NBA) systems use network flow data to track pre-defined parameters for establishing a baseline of normal network behavior. Once they have modeled ordinary, or “good,” behavior, they then look for deviations from that baseline in order to detect anomalies.

NBAD/NBA is primarily an investigative or decision support technology. While it may be able to detect certain zero-day and mass attacks, NBAD/NBA alone is not reliable enough to enable automated security responses. NBAD/NBA technologies require stable network systems whose definition of what constitutes good behavior remains consistent throughout time. Whenever network traffic patterns vary, however, good behavior cannot be as effectively modeled, and NBAD/NBA systems will suffer high false positive rates.ⁱ The VPN network environment is highly dynamic, with managed and unmanaged devices regularly accessing and leaving the network and causing significant changes in traffic patterns. VPN network behavior is therefore unpredictable—and unstable—by its very nature, and hence NBAD/NBA devices are vulnerable to high false positives when monitoring VPN networks.

Targeted attacks, which can be introduced into the corporate network through VPNs, present another problem for NBAD/NBA devices. The targeted attacker spends a lot of time probing the victim's network. This type of attacker is discrete; he or she does not bombard the victim with portscans, but rather sends

ⁱ Gartner Research, Paul E. Proctor, ID Number: G00134030, *Use Network Behavior Analysis for Better Visibility Into Security and Operations Events*.

occasional packets, each from a different source address each with a specific purpose in mind. These probe packets will blend in with the normal scanning that occurs on a typical network, making them indistinguishable from background scans and rendering NBAD/NBA-like device useless.

CounterStorm

CounterStorm, Inc. provides accurate and immediate internal network security defense against targeted attacks and zero-day wormstorms. CounterStorm's internal network security offering, CounterStorm-1, employs revolutionary technology to accurately identify and automatically stop internal, targeted, and zero-day attacks within seconds. CounterStorm-1 uses a unique combination of behavioral attack recognition, anomaly detection, and dynamic honeypot methods to search for non-standard traffic profiles without the use of signatures. Evidence from these engines is then dynamically correlated in real-time to enable the accurate and immediate containment of all malicious network activities. CounterStorm-1 also adjusts to future threats—including slow and stealthy attacks—that other solutions fail to detect.

CounterStorm-1 provides:

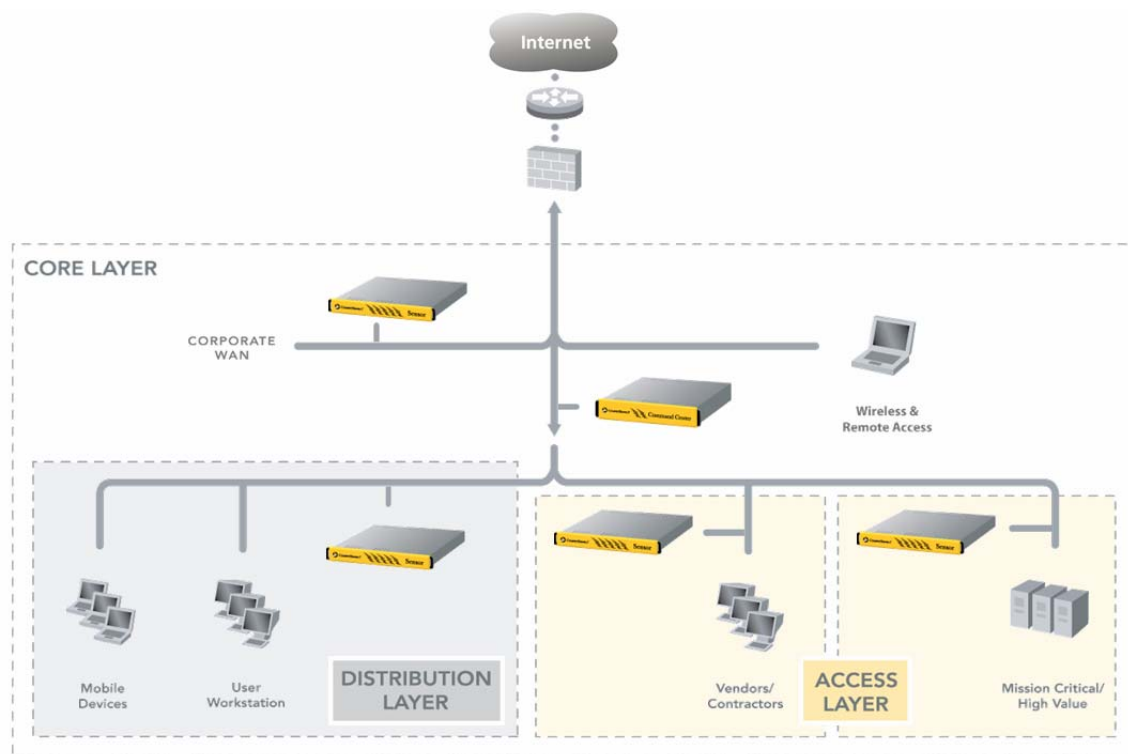
- Immediate and accurate internal network security: CounterStorm-1 maintains an extremely low incidence of false positives, whether functioning in a predictable or an unpredictable environment.
- Actionable visibility: CounterStorm-1 provides network security administrators extreme visibility into the network's security information, allowing them to see beyond layer 3 boundaries. CounterStorm also enables its users to drill down on all security events to the packet level.
- Support for heterogeneous network environments: Today's attacks have an extremely high velocity—whole networks can be infected in minutes. CounterStorm-1 detects and stops attacks within seconds in both heterogeneous and homogeneous environments.
- Flexible Response: CounterStorm-1 provides several response modes for dealing with malicious activities: Automatic Response, Emergency Response, and Manual Response. In each mode, CounterStorm-1 immediately and accurately identifies the infected remote device, obtains the user's access information, and integrates with the VPN terminator. It then either terminates the user's active session, or allows the network security administrator to optionally disable the account in order to prevent repeated logons. CounterStorm-1 also enables the network security administrator to reconfigure the device remotely and guide it into a remediation VLAN.

This process effectively removes any infected devices from the enterprise network, eliminating the risk of further worm propagation or data theft. With the help of a remediation VLAN, infected devices can be isolated from the network, yet remain accessible for cleaning and patching by IT staff or the user.

- Adaptation to future threats: CounterStorm-1 employs proprietary machine learning techniques and will adjust to future security threats as they manifest themselves.
- Mitigation support: Through the establishment of a remediation VLAN, CounterStorm-1 can inform end user issues of the status of their machines, thereby enabling them to fix the devices on their own. This reduces IT support work without blocking other users, and it helps end users remain compliant with corporate policy.

Deployment

CounterStorm-1 is designed for ease of use in installation, maintenance, and day-to-day operation.



CounterStorm-1 can be deployed in high-values areas in order to fortify an organization's defense systems, and in high-risk areas in order to stop attacks in seconds. When it is deployed at the network segment where the VPN concentrator is located, CounterStorm-1 can immediately and accurately identify the infected remote device, disconnect the users' active sessions and/or

optionally disable the accounts to prevent repeated logons, and guide the infected remote device into a remediation VLAN. Organizations can also deploy CounterStorm-1 at core network distribution layers in order to provide comprehensive, enterprise-wide network protection.

Conclusion

VPNs have become a significant source of malware infections. Remote access users often work from unmanaged devices that are unprotected and unpatched. As these devices are exposed to the Internet, they often unwittingly pick up malware, and then introduce that malware into the corporate network when they connect to it through a VPN tunnel. The types of malware typically introduced through VPNs include targeted and zero-day attacks.

Moreover, many large organizations have business partners whose respective networks are connected or peered to their own networks via a VPN tunnel. If these partner organizations do not have or enforce an identical (or stronger) security policy, they often become a logical point of approach for hackers who are looking to launch targeted and zero-day attacks. Due to their technological sophistication, targeted and zero-day attacks are almost impossible to detect through traditional security products.

To protect VPNs against internal and targeted attacks, as well as zero-day wormstorms, businesses need to acknowledge—and prepare for—risks to their internal network security. They need to deploy effective adaptive internal network security devices that can support unpredictable heterogeneous network environments while quickly and accurately detecting and quarantining attacks. Internal network security devices must provide threat mitigation support and be able to adjust to future threats including slow and stealthy attacks. Furthermore, in order to protect networks against targeted and zero-day attacks, these devices cannot rely on signatures to identify and block attacks.

CounterStorm-1 provides its users unparalleled accuracy and protection against internal threats, zero-day wormstorms, and targeted attacks, with no time consuming false positives. It detects and quarantines attacks in seconds in both heterogeneous and homogeneous network environments without relying on signatures, and it equips its users with flexible response methods in order to neutralize malicious activities. When used in conjunction with a remediation VLAN, CounterStorm-1 can inform end user issues of the status of their machines, thereby enabling them to fix the devices on their own. CounterStorm-1 is also self learning, adjusting to future security threats as they manifest themselves. Finally, CounterStorm-1 provides network security administrators actionable visibility into the network's security information, allowing them to see beyond layer 3 boundaries and enabling them to drill down on all security events down to the packet level. CounterStorm-1 is a proven security technology, and it has detected targeted, zero-day, and known attacks in Fortune 1000 companies.



To learn more about CounterStorm, please visit <http://www.counterstorm.com>.