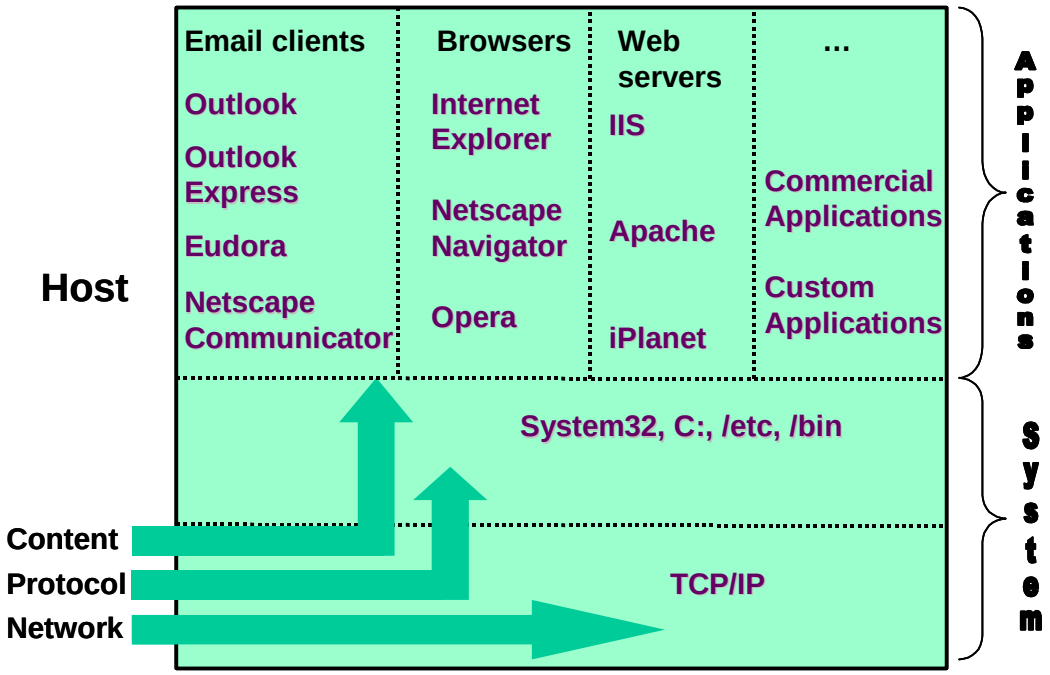
StormWatch™ Personal Firewall with Intrusion Prevention for Remote Corporate Users

Increasingly, organizations find users working remotely from corporate offices. Some of these users are mobile "Road Warriors", accessing corporate applications like email from hotel rooms, airports, or customer offices. Others are telecommuters working from home. Often, these users access the corporate network via the Internet instead of via dial-up modem. All of these users are exposed to probes or attacks from the Internet, and none are protected by the central corporate Firewall. Remote users whose computers are compromised provide attackers with a "Jumping Off Point" into the corporate network.

The introduction and growth of the centrally managed Personal Firewall (sometimes referred to as "Distributed Firewall") market demonstrates the desire of IT departments to reduce these risks. In order to meet customer needs, the following key features are typical of a number of personal firewall products available today:

- Port blocking
- Centralized security policy management
- Centralized reporting
- Intrusion detection (not offered by all products)
- Ability to control which applications can use the network (not offered by all products)

These features only address a subset of the risks facing remote users. Most Distributed Firewall features focus exclusively on network attacks such as attempts to connect to applications on the computer. However, many other risks are present from attacks via malicious content payloads such as email attachments or Javascript, or from protocol attacks like buffer overflow attacks on network applications.



71 Second Avenue, Waltham, MA 02451
Tel: 781-209-3200 Fax: 781-209-3199
E-mail:info@okena.com

www.okena.com

6905 Rockledge Drive, Suite 600
Bethesda, MD 20817
301-896-9388

When resources are protected by traditional personal firewalls, the protection usually "stops" at the network – once an attack compromises an application, the host is completely vulnerable. If a personal firewall actually allows a service to execute, the software providing the service must be up-to-date and configured properly. Once the application is accessed over the network, the personal firewall cannot protect the application. And the personal firewall cannot control application usage of the network beyond simple port/IP address control. Other standard personal firewall disadvantages include:

- Intrusions masquerading as authorized applications might bypass personal firewall security. As an example, Foundstone's "Firehole" attack can allow other applications to impersonate Internet Explorer to make "authorized" connections[1].
- A vast majority of security events generated by Personal Firewalls are unremarkable and not part of any malicious intent; this can make it difficult for companies to judge the effectiveness of the personal firewall[2].
- A personal firewall does nothing to protect client applications that use the network. For example, a recent Internet Explorer hole allows a basic HTML attack to compromise the operating system[3]. Other examples include the ability of users to download potentially infected files via Instant Messenger, and e-mail snooping via embedded HTML in the message body[4].

The recent NIMDA attack illustrates the "Blended Threat" risk. The NIMDA worm was a multifaceted attack that used multiple avenues of attack: HTTP, email, and shared folders. Systems that were protected at the network level from HTTP attacks were often vulnerable via email, or due to vulnerable web browsers. Since the StormWatch Distributed Firewall includes an Intrusion Prevention capability, it is able to control attack propagation and damage even after it has entered a system. StormWatch stopped NIMDA, even after it entered a system, because NIMDA's activity was beyond the scope of "normal behavior" – the attack executed buffer overflows in applications and tried to email itself to other targets. Even though StormWatch does not contain attack signatures, and even though NIMDA was an attack that had never been seen before, it stopped the malicious attempts that the attack used to try to cause damage.

The StormWatch Distributed Firewall Prevents all Classes of Attack

The OKENA StormWatch Distributed Firewall satisfies the basic requirements for a Personal/Distributed Firewall, blocking network-based attacks against remote users. It also goes beyond these traditional features by preventing damage from protocol and malicious content attacks. In addition, the StormWatch Distributed Firewall offers the following advantages over personal firewall products from other vendors:

- ***Active Content Sandbox*** protects web browsers from subversion via mobile code like Java, Javascript, and ActiveX

---

[1] Firehole can be found at http://keir.net/firehole.html. TooLeaky can be found at http://tooleaky.zensoft.com.

[2] "Study: Constant security fixes overwhelming IT managers," ComputerWorld, 30 November 2001, http://www.computerworld.com/itresources/rcstory/0,4167,STO66215_KEY73,00.html

[3] CERT Advisory CA-2001-36, "Microsoft Internet Explorer Does Not Respect Content-Disposition and Content-Type MIME Headers", 16 December 2001, http://www.cert.org/advisories/CA-2001-36.html

[4] "Privacy group warns of e-mail wiretap", CNN.com, 5 February 2001, http://www.cnn.com/2001/TECH/internet/02/05/email.wiretap.idg/

- ***Email Worm Detection*** bocks email worm attacks like NIMDA or GONER
- ***Application Masquerade Prevention*** protects against "Application Hijacking" (via DLL control hook as done by the "Firehole" and "Tooleaky" attacks)
- ***Application Policy Control*** allows prevention of risky user behavior within applications, such as downloading files via Instant Messenger
- ***Buffer Overflow Protection*** protects against known and unknown buffer overflow attacks against network applications
- ***Application Execution Control*** allows central specification of which applications can run, which can use the network, and which cannot
- ***Location-Aware Protection*** allows normal network use – such as file sharing – in the office, while preventing risky network use when at a remote location
- ***Zero-Update™ Intrusion Detection*** detects and blocks attacks without the need for signatures. Since signatures are not required to prevent intrusions – and unlike other Intrusion Detection products – there is no "Window of Exposure" when an attack is circulating but the vendor has not yet created signatures. There is also no administrative burden associated with installing signatures and keeping them current.

StormWatch Distributed Firewall Features

The following features, performance benchmarks, and product attributes can be compared to those offered by other personal firewall products to determine the level of adherence to your specific security requirements.

Basic Security Features:

Inbound and Outbound port blocking: The Distributed Firewall policies in StormWatch control all aspects of network traffic including all inbound and outbound connections. StormWatch also controls traffic based on protocol, port, and communicating host address.

Protection from fragmented packet attacks: The StormWatch Distributed Firewall protects against a wide range of layer 3 attacks, including packet fragments.

Protection from attacks using "Evasion" techniques: The StormWatch Distributed Firewall is immune from methods commonly used to evade Intrusion Detection Systems[5].

Intrusion Detection and Prevention: Known and unknown attacks are detected and automatically blocked at the agent. Because the StormWatch Distributed Firewall contains an intrusion prevention system that uses behavioral policies to enforce appropriate system behavior, no Intrusion Detection signatures are needed. Other Intrusion Detection products release new signatures to detect and block new attacks. Unfortunately, these updates are often released infrequently, resulting in a considerable time period where the computer is vulnerable because no signature is yet available. Since the StormWatch Intrusion Detection and Prevention does not rely on signatures, the protection provided by the firewall is not dependent on how rapidly new signature updates are made available. This not only gives StormWatch a higher level of protection, but also results in a "Zero Update" architecture, where no signature updates need be managed.

Configurable IDS rules: The StormWatch Distributed Firewall focuses on preventing, rather than detecting intrusions, and the behavioral policies that make up the system are customizable by the administrator.

---

[5] "IDS Evasion with Unicode", Eric Hacker, Bugtraq security mailing list, 3 January 2001, http://www.securityfocus.com/infocus/1232

***Application Execution Protection*:** The StormWatch Distributed Firewall can control which applications are allowed to execute, and which are not.

Location-Aware Protection: The StormWatch Distributed Firewall allows normal network use – for example, sharing files between computers – while in the office, but prevents these risky activities when the computer is in a remote location.

Advanced Security Features:

"Sandbox" protection for Web Browsers and Email clients: The StormWatch Distributed Firewall prevents content-based attacks against web browsers and other end-user network applications. Users are protected against malicious content while they surf, read email, or chat on-line.

Email Worm Prevention: The StormWatch Distributed Firewall detects attempts to send mass email containing potentially malicious attachments, the heart of the email worm threat. Not only does it block these attempts by strictly controlling access to resources like the Microsoft Outlook address book, but it also reports malicious email attachments to the central manager, which updates a system-wide Global Quarantine List. This quarantine list is deployed to all agents, resulting in agents being "inoculated" even if they have never been attacked by that particular worm.

Protection against both known and unknown Buffer Overflow attacks: The StormWatch Distributed Firewall detects and blocks buffer overflow attacks against any application running on the computer. Because the detection is based on how applications execute code, and not on analysis of packet contents, it will block both known buffer overflow attacks as well as unknown ones. Even attacks that use IDS evasion techniques will be blocked.

Application Masquerade Prevention: One of the latest attack techniques against Personal Firewall products is where a malicious application attempts to masquerade as a trusted application, via a mechanism such as DLL Injection[6]. Since this allows the malicious program code to appear to be running "inside" the trusted application, the firewall will be fooled into thinking that the malicious code is part of the trusted program. Thus, the malicious application will be able to bypass the firewall controls, for example to access the network. The StormWatch Distributed Firewall detects and blocks all DLL Injection attacks, protecting not only against unauthorized network access, but against password theft attacks as well.

Configurable Instant Messaging controls: The StormWatch Distributed Firewall offers ***Application Policy Control***, which gives companies the ability to control, with a high level of specificity, which aspects of the Instant Messenger application are used within their organizations. StormWatch can allow text messaging, for example, but explicitly forbid the transfer of files through the Instant Messenger system, while continuing to allow file transfers via other mechanisms such as browser or FTP.

***Operating System Lock-Down*:** The StormWatch Distributed Firewall hardens the Windows Operating System, preventing attacks from modifying critical OS binary files or

[6] *PWDUMP2* from the Bindview Razor security team (http://razor.bindview.com/tools/desc/pwdump2_readme.html) steals passwords from Windows NT and Windows 2000 computers. For a discussion of DLL injection attacks to bypass Personal Firewall protection, see http://keir.net/firehole.html.

configuration settings. Since this capability does not require the use of cryptographic analysis of file system contents, it adds virtually no performance impact to the system.

Audit log consolidation: The StormWatch Distributed Firewall provides detailed logging of attacks. It can also collect Windows Event Log and Security Log entries such as bad logons.

Open and Customizable: Application security measures are controlled by policies. The policies are comprised of a set of rules that specify how applications may access network, file system, registry, or COM system components. While the StormWatch Distributed Firewall provides default policies for Distributed Firewall and desktop application protection, all these policies are customizable, and administrators can easily define new policies through the browser-based GUI.

Management Features

Central Management of Agents: Policies for the StormWatch Distributed Firewall are defined centrally and automatically pushed out to the agents, residing on servers and desktops requiring protection.

"Manage from anywhere solution" for administrators: The StormWatch Distributed Firewall management is HTTP/HTTPS-based, so all management can be handled from any location using a standard web browser.

Works in a DHCP environment: Agents are not identified by IP address, which will typically change often in DHCP environments. Rather, each agent is assigned a globally unique identifier (GUID) that does not rely on IP address. Therefore, all central management functions such as grouping, policy assignment or modification, or agent update will reach the intended agents, even if those agent's address change.

Central Alerting: All agent events are sent to the management console, where alerts are centrally generated.

Configurable Alerting: Alerts are report to central console; all client events report to the StormWatch management console, which in turn generates alerts to a central customer console. All events generated by client agents can be configured to alert via email, pager, SNMP trap, flat log file, or via a custom programmatic interface.

Secure Communications between agents and management console: Agent updates are automatically pulled from the management console with every event report. If agents are disconnected for a period of time, all policy enforcement will continue to be performed locally. When the agent is "reconnected," new policies and updates will automatically be installed. All communications between the management console and agents is performed via SSL.

Remote installation and automatic configuration: The initial agent software may be deployed via HTTP, SMS, or other corporate software distribution mechanism. All further policy and software updates are done automatically through the agent polling mechanism.

End user isolated from security policies: The user does not have direct access to the StormWatch agent, and cannot change policy locally. The StormWatch agent enforces a centrally defined policy that is cached locally on the agent. This policy cannot be viewed or modified by the client user.

Optional notification of end-user when under attack: All security events are stored locally on the client, as well as sent to the central management console. The client can optionally be notified of policy violations via a waving flag in the Windows taskbar.

Reduced logging and no false-positives: Because he StormWatch Distributed Firewall is a customizable behavior-based policy system there are no false positives. Policies may be easily adapted to specific computing environments.

For further information, please contact OKENA at info@okena.com, visit our website at www.okena.com, or call 781.209.3200.

OKENA StormWatch provides uncompromising intrusion prevention for enterprise environments. StormWatch prevents intrusions from executing and offers security without signatures. StormWatch agents, residing on critical servers and desktops, go beyond standard personal firewall products by invoking OKENA's proprietary INCORE architecture to provide safe access to required resources. INCORE (INtercept COrrelate Rules Engine) intercepts an application's resource requests to the operating system, correlates the behavior within its rules engine, and makes a real-time allow/deny decision according to the customer's application security policy. StormWatch's ability to proactively repel new attacks directly on the servers and desktops to be protected makes it a central component to a customer's security policy. StormWatch is an entirely new stand-alone layer of defense, one that does not burden IT departments with the continual management of signature updates.