Gateway AntiVirus

WatchGuard® Gateway AntiVirus

Technical Brief

WatchGuard® Technologies, Inc.
Published: March 2011

Malware Continues to Grow

New and ever-changing threats appear with alarming regularity, and no organization is immune from risk. In the early days of the Internet, Internet security was primarily about protecting your servers from bored teenagers who were writing malicious code to impress their friends. Today, threats have evolved and attacks are much more sophisticated. Organized criminals now write malware for financial gain. Polymorphic viruses mutate and look different with each infection – making them harder to detect by traditional signatures.

A few years ago, malware was primarily delivered via simple email attachments, but now infections are just as likely to spread from compromised web sites. Gartner reports that malware has been found on:

- 60% of the top 100 sites
- 75% of legitimate web sites
- 1% of Google search results

Many legitimate sites have been compromised, including well known names such as MSNBC, ZDNet, United Nations, Honda, MySpace, and Excite.com.

WatchGuard Gateway AntiVirus

Gateway AntiVirus (Gateway AV) is a fully integrated security subscription for WatchGuard® XTM appliances. It works in tandem with the application layer content inspection of the XTM to provide real-time protection against known viruses, trojans, worms, spyware, and rogueware. Gateway AV scans traffic on all major protocols (HTTP, HTTPS, FTP, TCP, UDP, SMTP, and POP3) using continually updated signatures and heuristics to detect and block all types of malware. Email traffic is scanned at the gateway to stop threats before they gain access to your servers and execute their dangerous payloads. Gateway AV provides safer web browsing by preventing the download and execution of malicious code.

Detection Methods

Gateway AV incorporates a highly rated scanning engine from industry-leader AVG Technologies. The Virus Bulletin, an independent test organization (www.virusbtn.com), ranks the AVG engine highly in both proactive and reactive virus detection tests. Reactive detection indicates response to known viruses, whereas proactive detection shows detection rates for new viruses in the first week of testing. The engine's efficiency at detecting infected files is guaranteed by using a combination of different detection levels.

Signature Techniques

Known virus detection: This is the simplest technique in which files are scanned for the presence of patterns or virus identifiers (a sequence of bytes characteristic for an exact virus). Based on this kind of detection, detailed analysis is performed to identify the exact infection. The WatchGuard XTM 1050, 8 Series, and 5 Series appliances use a 50 Mb database of all AVG known virus signatures. The XTM 2 Series and Firebox® e-Series appliances use a smaller dataset, which includes newer and high priority signatures, and viruses that are known to be active in the wild.

Model Family	Signature Set	Includes
Firebox X e-Series: (includes Edge, Core, Peak) XTM 2 Series	Reduced Set	250,000 signatures
WatchGuard XTM 1050 / 8 Series/5 Series	Full set	2.5 million signatures

Table 1: Signatures by product family

Generic detection: This is a more common method for the detection of known viruses and this is used to determine new variants of known viruses. If no known virus is identified, generic detection looks for sequences within the file typical for certain viruses. Such sequences usually don't change within the virus when it is modified, even if the behavior of the new variant is different. This method is effective especially in the detection of macro-viruses and script-viruses.

Heuristic Analysis (behavior analysis)

The last method for detecting viruses is heuristic analysis, which is used to detect viruses and dangerous code that signatures can't catch. During heuristic analysis, two methods are used:

- **Static heuristic analysis** looks for suspicious data constructions
- **Dynamic heuristic analysis - code emulation:** this means the file is started inside a protected environment. The file is analyzed for actions typical for viruses. An example being an application, which when run, looks for other executable files in order to modify them.

The engine also uses advanced file handling techniques to make sure that viruses don't slip by. Compressed and encoded files are decompressed for inspection, with wide compression support including .zip, .gzip, .tar, .jar, .rar, .chm, .lha, .pdf, XML/HTML container, OLE container (Microsoft Office documents),.cab, .arj, .ace, .bz2 (Bzip), and .swf.

Signature Updates

New signatures are typically provided each day. The signature database can be configured to check for updates hourly, ensuring timely, far-reaching coverage. A dashboard in WatchGuard System Manager and Web UI shows virus detection statistics and the latest status of the signature updates.

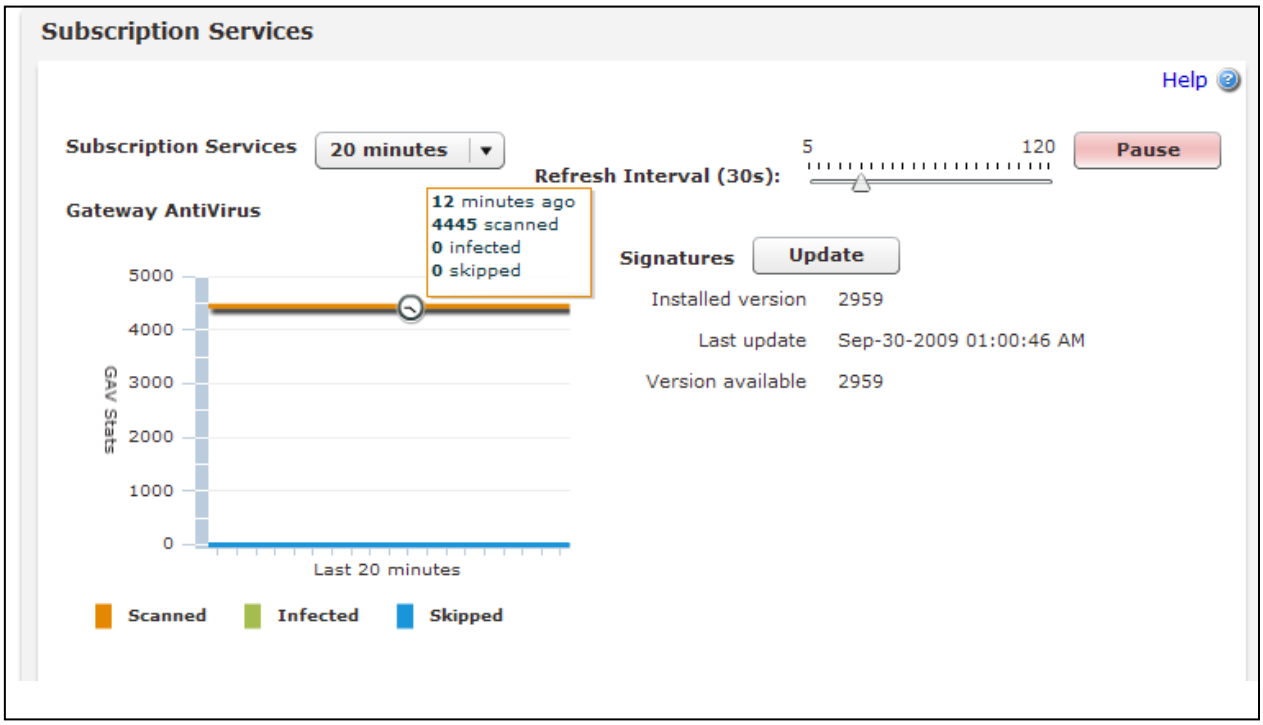

Figure 1: Gateway AV Signature Dashboard

Buffers for Optimized Performance

Scanning files at the gateway using all known signature and heuristic techniques could introduce unacceptable latency and delays into the network. Some "inline" solutions – such as those from SonicWall and Palo Alto Networks – scan every part of the file as it passes through the firewall, claiming no limits on file size or number of concurrent connections. But to keep the scanning lightweight they use very small signature sets (from 3,000 to 20,000 signatures) and only use pattern matching – no heuristic techniques. Such inline solutions often cannot perform file-handling operations, such as decomposing archives and OLE objects that require traversal over a file stream. There is no option to lock or quarantine files for further analysis.

WatchGuard Gateway AV takes an alternative approach and scans files in a buffer to provide a comprehensive combination of end user performance and security. The buffer allows for a much more comprehensive scan and a bigger signature set than inline solutions since it occurs in parallel to file streaming. Buffering ensures optimum user experience for HTTP scanning and file transfer. The engine scans a copy of the file in the buffer, but it continues to stream to the desktop while the file in the buffer is being scanned. When the file stream reaches the end of file or the scan limit, a small, last piece of data is kept "hostage" until the file has passed the scan. The file isn't available until that last piece is released. This may result in fragments or partial files getting to the desktop, but the full file is not delivered until it passes the AV scan. The malicious payload cannot be executed.

With this buffer approach only the beginning of very large files are scanned. The engine scans a number of bytes up to a threshold, which is configurable in the user interface. The engine can scan up to the first 30 Mb

of files for the XTM 1050, 8 Series, and 5 Series. This threshold size is different for each model as defined below since it depends on the available memory of the appliance (size in kilobytes).

Model	Minimum	Maximum	Default
Firebox X Edge e-Series:	250	1,024	250
Firebox X Core™ e-Series:	250	20,480	1,024
Firebox X Peak™ e-Series:	250	30,720	1,024
WatchGuard XTM 1050 / 8 Series / 5 Series	250	30,720	1,024
XTM 2 Series	250	5,120	512

Table 2: Scan limit size settings

The available memory in the appliance is fixed. Setting the scan limit to a lower setting like 250K would allow more files to be scanned at the same time and more connections, but the disadvantage is that potential viruses could be missed in the later parts of the file. Setting this limit to 30 Mb would ensure broader coverage of very large files, but it could result in scanning of fewer files at the same time.

The greatest malware threats today come from the inadvertent download of malicious files while web browsing. An engine that uses heuristics is more likely to capture new and emerging threats. Users are unlikely to accidentally download files that are greater than 30 Mb in size. Even if they download suspect files, the first 30 Mb of the file is scanned. Any virus would have to be hidden outside the first 30 Mb of the file to avoid detection.

Options When a Virus Is Discovered

Gateway AV provides several options for actions to take when a virus is detected. Suspect email, for example, can be flagged to go into quarantine, where administrators can restrict access or allow users to review quarantined files through automatic email alerts. The complete set of actions that can be taken when a virus is detected in an email include:

- **Lock:** lock the message content
- **Allow:** allow the email
- **Remove:** remove message parts
- **Quarantine:** quarantine the email
- **Drop:** drop the connection immediately
- **Block:** drop the connection and Autoblock the source

Autoblock adds the offending site to the blocked sender's list, disabling all future communication from that IP address. The Allow, Drop, and Block options are also available for viruses that are detected in HTTP scanning.

Any virus detection events can be logged to the WatchGuard log server for subsequent reporting and analysis. Possible alarms on detecting a virus include SNMP traps, email notifications, and pop-up windows.

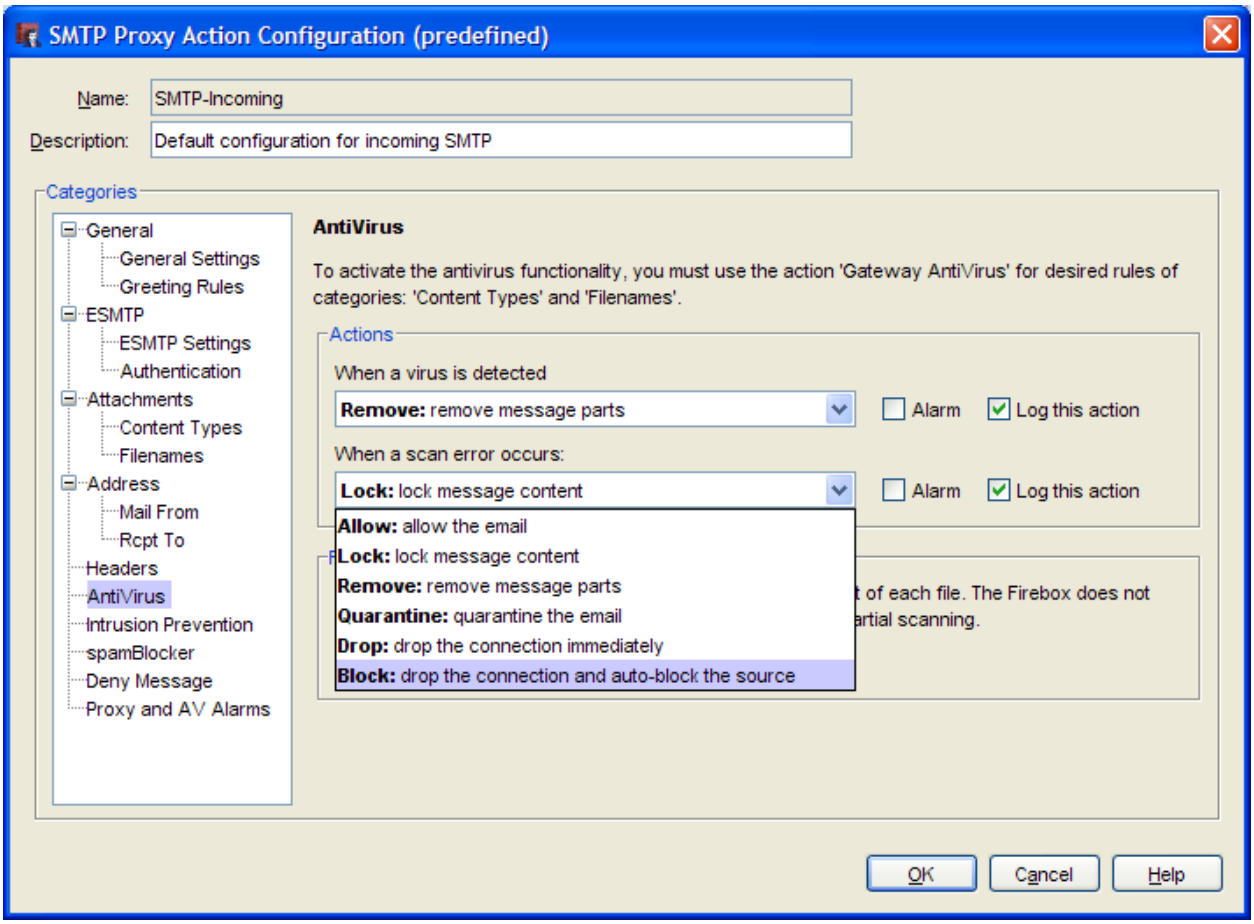

Figure 2: **Actions when a virus is detected or a scan error occurs**

Virus Outbreak Detection

The WatchGuard anti-spam solution also provides another layer of protection against viruses using CommTouch Recurrent Pattern Detection (RPD) technology. Subscribers to the spamBlocker service get the added benefit that email outbreaks around the world are monitored to detect outbreaks of mass distributed viruses.

The chart below shows the number of viruses detected for WatchGuard customers over a 90-day period in 2009.

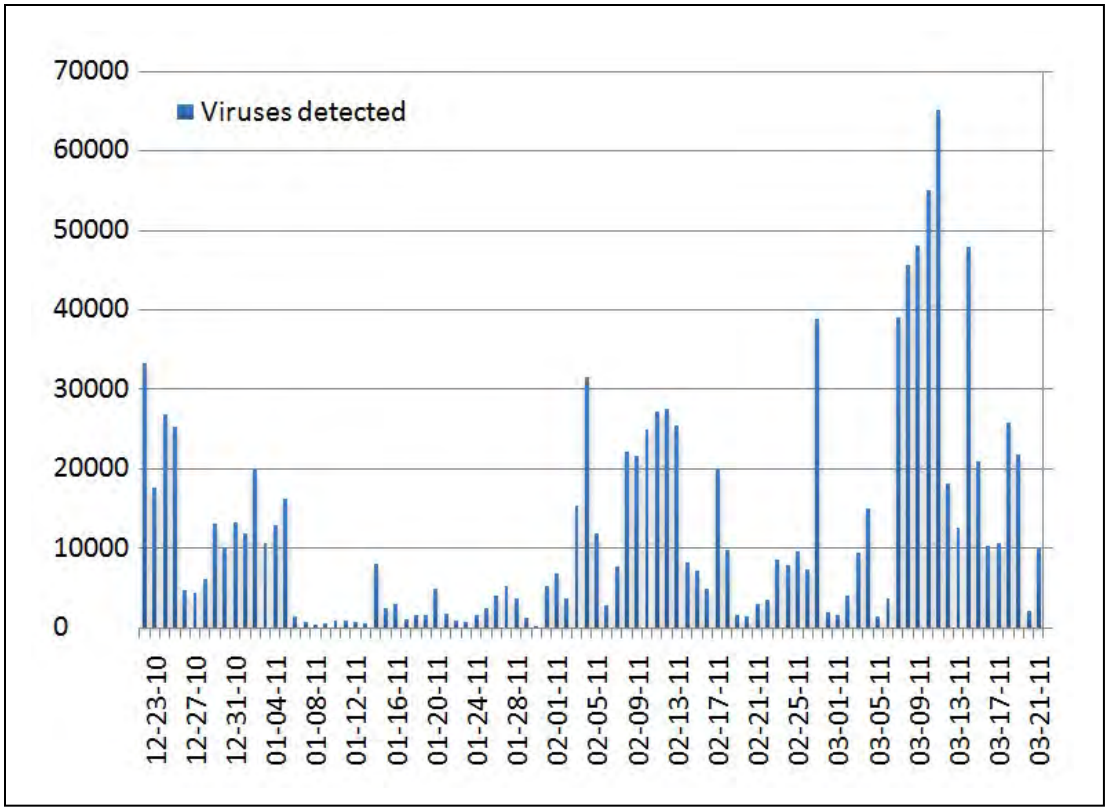

Figure 3: Number of viruses detected in email for WatchGuard customers, Dec 2010 – Mar 2011

Cost-Effective Solutions

WatchGuard Gateway AV is an easy to manage cost-effective solution that provides another layer of security to complement existing server and desktop antivirus solutions. A single subscription to Gateway AV provides network-wide protection for all users configured behind the WatchGuard XTM firewall. There are no per-user charges.

You can also purchase Gateway AV bundled with our suite of powerful security subscriptions for even greater savings.

- **WatchGuard Security Bundle** includes your choice of WatchGuard XTM appliance, and subscriptions to Gateway AV, Application Control, Reputation Enabled Defense, Intrusion Prevention Service, spamBlocker, WebBlocker, and LiveSecurity® Service – a comprehensive support and maintenance program.

- **WatchGuard Security Software Suite** is for customers who already have a WatchGuard XTM appliance and want to turn it into a comprehensive threat management solution. The Suite includes Gateway AV, Application Control, Reputation Enabled Defense, Intrusion Prevention Service, spamBlocker, and WebBlocker, as well as LiveSecurity Service for support and

maintenance. Firebox X e-Series customers can purchase a Software Suite that includes Gateway AV, Intrusion Prevention Service, spamBlocker, WebBlocker, and LiveSecurity Service.

For more information about WatchGuard Gateway AntiVirus, or any of our other network security products, visit www.watchguard.com, or contact your reseller.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.