bitdefender®

SECURITY FOR ISA SERVERS

INTERNET GATEWAYS - THE FIRST LINE OF DEFENSE

Organizations today provide shared Internet access to most employees, so Web-based proxy services can help to manage bandwidth utilization and consolidate traffic by caching the data locally. Web access for both personal and business related information greatly increases the amount of Internet traffic and in turn, exposure to threats. Therefore, company's deploying Internet Gateway solutions such as Microsoft® Internet Security and Acceleration (ISA) Server can see considerable gains in faster internet response times and basic firewall functionality that provides a first line of defense.

THE NEED FOR PROTECTING INTERNET ACCESS GATEWAYS

While company's deploying Internet Access Gateways do benefit from the additional firewall security, the protection they provide is limited because of static firewall rules and the lack of visibility into the packets that pass through the gateway. Therefore, protection against malicious code entering a company's network through unmonitored applications or due to the lack of content inspection can result in enormous amount of wasted time, money and IT resources when an infection strikes.

Web-based services may pose a security threats, including:

- Websites or downloaded files that are infected by malicious code
- Downloading infected email attachments from online mail services
- Downloading or uploading infected files by using FTP service
- Via an infection propagated through a mapped network drive

Gateways provide a central choke-point for Internet-based content and help an organization implement both inbound and outbound policy requirements for users within the network. In order to optimize the security and increase the survivability of an ISA server deployment – without impacting the performance and response times to business critical operations – additional solutions are needed to ensure your operational efficiency.

SECURING INTERNET GATEWAYS WITH BITDEFENDER

BitDefender Security for ISA Servers allows organizations to protect their Microsoft® ISA Servers to block specific types of websites, scan downloaded files and email attachments from web email services. Ensuring compliance to corporate security policies becomes easier and companies will be able to maintain control of sensitive data that would otherwise leak from inside of the organization.

BitDefender Security for ISA Servers scans inbound and outbound Web and FTP traffic and applies a set of scanning or filtering rules that are configurable through a Centralized Management Server.

KEY FEATURES AND BENEFITS

- *Award winning virus detection, cleaning and quarantine*
- *Minimize network downtime to increase operational efficiency*
- *Reduce security threats, resource costs and overhead, increase productivity*
- *Browser comforting technology for scanning and passing through large files in small blocks*
- *Easy to manage keyword based website and FTP blacklists or white lists for safe websites*
- *Scans file traffic ensuring real-time antimalware protection to minimize the risk of malware propagation throughout the network*
- *Integration with Microsoft's Firewall rules and Web caching through Microsoft's Virus Scanning Interface (ISAPI) to optimize and accelerate the scanning process*
- *Reports on virus activity, scanning statistics and Internet traffic volumes*
- *Configurable actions for various events triggering email alerts or executing other actions*
- *Supports high volumes with multiple ISA Servers configured as an array for load balancing*
- *Allows remote configuration from any computer in the organization through a centralized management console*

bitdefender

BITDEFENDER TECHNOLOGIES

All BitDefender solutions include B-HAVE, a patent-pending technology which analyzes the behavior of potentially malicious codes inside a virtual computer, eliminating false positives and significantly increasing detection rates for new and unknown malware.

AUTOMATIC UPDATES

BitDefender Security for ISA Servers offers intelligent updates once an hour with new virus definitions, ensuring your Microsoft® ISA Server deployment's security stays current with the very latest threat protection.

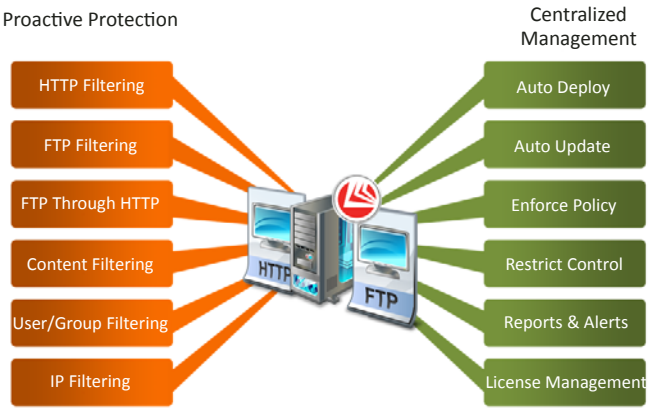
DEFENSE IN DEPTH

BitDefender Security for ISA Servers is just one element in a comprehensive suite of solutions providing end-to-end network protection from the gateway to the desktop. BitDefender's proactive, multi-platform products detect and stop viruses, spyware, adware and Trojan threats that can compromise your network integrity.

SYSTEM REQUIREMENTS

Software

- Windows Server 2003 with SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2
- Microsoft ISA Server 2000/2004/2006 Standard Edition
- Microsoft ISA Server 2004/2006 Enterprise Edition
- Internet Explorer version 6.0 or higher



BitDefender Security for ISA Servers provides award winning virus detection, management and reporting features to enable the sharing of information safely throughout an organization

MULTIPLE LEVELS OF SCANNING AND FILTERING

BitDefender's award-winning scan engines have been recognized by leading certification bodies, - including ICSA Labs, Virus Bulletin, and West Coast Labs - for their unmatched proactive antimalware protection. BitDefender provides scanning and filtering methodologies in multiple levels to detect malicious code to safeguard confidential information;

Web (HTTP) Traffic scanning engine detects viruses and malware in real-time when users are browsing websites, accessing web email services or other web based applications.

FTP Upload/Download scanning features detects viruses and malware in real-time whenever users are downloading or uploading files by using File Transfer Protocol (FTP).

Content Filtering - Content filtering allows for the detection of predefined information such as credit card or account information, report names, client databases, etc. from passing outside the company's control. The Content Filtering applies customizable restrictions based on website or FTP server addresses, keywords and content size.

Blacklists and White list for blocking websites based on keywords or listing known, safe websites.

Usage Polices enable flexible restrictions to be applied within the organization's network based on ranges of IP addresses, content types or protocols.

INBOUND AND OUTBOUND THREAT PROTECTION

- Award winning virus detection, cleaning and quarantine
- Integration with Microsoft's Firewall rules and Web caching through Microsoft's Virus Scanning Interface (ISAPI) to optimize and accelerate the scanning process
- Scans file and web content ensuring real-time protection to minimize the risk of malware propagation throughout the network
- Easy to manage keyword based website and FTP blacklists or white lists for safe websites

OPTIMIZATION, MANAGEMENT, AND REPORTING

- Reduces administration workload by enabling centralized notification management through the integration of BitDefender alerts with the ISA Server's Alerts Module
- Supports ISA Server deployments configured as an array for high volume traffic environments when used for load balancing
- Browser comforting technology for scanning and passing through large files in small blocks
- Reports on virus activity, scanning statistics and Internet traffic volumes
- Configurable actions for various events triggering email alerts or executing other actions
- Allows remote management and configuration via a centralized management console