Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Is your virtual environment protected from bots?

SOLUTION DESCRIPTION

Check Point Security Gateway Virtual Edition (VE) with Anti-Bot Software Blade protects virtual environments from bots and malware

Anti-Bot for Virtual Environments

Security Gateway Virtual Edition provides bots and malware protections for virtual data centers

THE CHALLENGE

A bot is a malicious, stealthy software that invades your virtual network and allows criminals to remotely control your virtual servers. Cybercriminals can remotely execute illegal activities such as stealing data, spreading spam, distributing malware and participating in Denial of Service (DOS) attacks without your knowledge. Bots play a key role in targeted attacks also known as Advanced Persistent Threats (APTs). A multi-layered integrated threat prevention solution is needed to protect not only your physical servers but also your virtual servers from such threats.

OUR SOLUTION

Check Point Security Gateway Virtual Edition with integrated Anti-Bot Software blade, provides a comprehensive security solution to protect virtual environments. It detects bot-infected virtual machines and prevents bot damages by blocking Command and Control (C&C) communications. Security Gateway Virtual Edition plug-&-play operation streamlines deployment, and full support for live migration of VMs means zero downtime. Also, as new VMs are brought online, they are immediately protected by automatic security policy enforcement.

CHECK POINT ANTI-BOT SOFTWARE BLADE OVERVIEW

The Check Point Anti-Bot Software Blade discovers bot outbreaks, detects APT attacks and stops bot damage. Using a continually updated list of C&C addresses from ThreatCloud™, the largest real-time security threat knowledgebase from the cloud, the Anti-Bot Software Blade detects stealthy bots before they can do damage. Once a bot is detected, the Check Point Anti-Bot Software Blade blocks remote communication between the infected machine and the C&C server, rendering the bot useless to the Cybercriminal and protecting the Virtual environment from potential bot damage.

PROTECTION FROM BOTS INSIDE THE VIRTUAL ZONE

The Anti-Bot for virtual environment solution is powered by ThreatCloud™ which feeds the security gateway with up-to-the-second security intelligence with over 250 million addresses analyzed for bot discovery, over 4.5 million malware signatures and over 300,000 malware infested websites.

FEATURES

First Integrated Anti-Bot Solution for Virtual Networks

- Post-infection detection by discovering bots and stopping their damage
- Fully virtualized security gateway
- Enforce security for dynamic virtual environments
- Inter-VM traffic inspection
- Easy to deploy security for virtualized environments
- Unified management for physical and virtual environments
- Management, reporting and policy unified with Antivirus

POWERED BY ThreatCloud™

ThreatCloud is the first collaborative network to fight cybercrime that feeds security gateway software blades with real-time security intelligence

- 250 million addresses analyzed for bot discovery
- 4.5 million malware signatures
- 300,000 malicious websites

SOLUTION BENEFITS

- Discovers bots that are infiltrated into your virtual environment
- Stops APT Attacks
- Automatically protects new VMs
- Prevents damage such as stolen data
- Ensures VM security by inspecting all inter-VM traffic with granular firewall policies and integrated best-in-class intrusion prevention
- Provides continuous protection during live migration of VMs from one host to another
- Unified management for both physical and virtual environment

softwareblades™

Anti-Bot for Virtual Environments

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

FULLY VIRTUALIZED SECURITY GATEWAY

Security Gateway VE provides comprehensive security based on the Software Blade Architecture, protecting both inter-VM traffic and external networks and assets. In addition to seamless hypervisor-layer security, VE also provides the flexibility to be deployed as a Layer 2 or Layer 3 default gateway.

Security Gateway VE simplifies security deployments by consolidating proven security functions within a single solution streamlining deployment and administration. Virtual machines are protected from external threats as well as from each other with best-in-class integrated firewall, Anti-Bot, IPS, DLP, application control, identity awareness, VPN, anti-virus, anti-spam, URL filtering, web security and mobile access. Where separation of servers and data is required for compliance, VE protects segregated applications and information from one another without the need for physical security appliances.

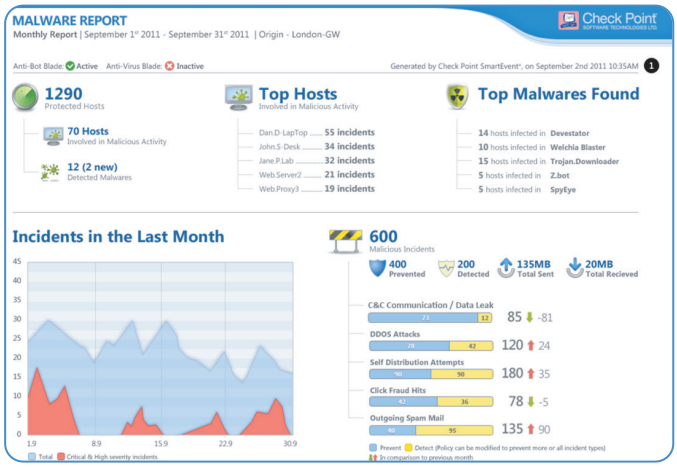
ThreatSpect™ BOT DISCOVERY ENGINE

Bots are stealthy, often hiding in your computer or virtual server undetectable by common antivirus programs. The Check Point Anti-Bot Software Blade detects bot-infected machines with its ThreatSpect™ engine, a unique multi-layer discovery technology with up-to-the-minute updates feeds from ThreatCloud. ThreatSpect correlates information for accurate bot detection.

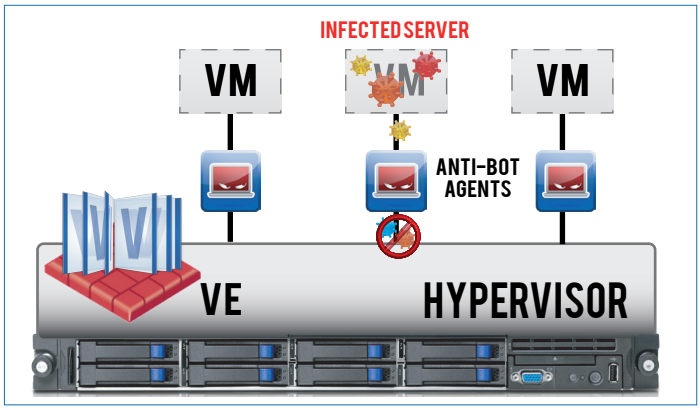
- Remote operator addresses including IP, DNS and URLs
- Detect unique botnet communication patterns
- Detect attack behavior such as spam or clickfraud

UNIFIED MALWARE AND BOT PROTECTION

Anti-Bot Software Blade is unified with the Antivirus Software Blade to give both pre-and post-infection protection to organizations and provide multi-layered threat prevention. Administrators can manage unified policies and reports all in a single user interface.



View the "big malware picture" with integrated threat reports.



Bots traffic to Command & Control center is blocked by Anti-Bot Software Blade

ENFORCE SECURITY FOR DYNAMIC VIRTUAL ENVIRONMENTS

Virtual machine protection is continuous during live migration of virtual machines from one host to another and when new virtual machines are added. Full support for VMware VMotion and full-term Dynamic Resource Scheduler (DRS) allows the security policy to be enforced while maintaining open connec tions. This also ensures zero down time when virtual machines are moved from host to host for maintenance and dynamic resource allocation.

Virtual machines are so easy to create that it sometimes leads to VM sprawl. Security Gateway VE alleviates this concern by ensuring that newly added virtual machines are segregated from existing VMs with automatic security policy enforcement.

UNIFIED MANAGEMENT FOR PHYSICAL AND VIRTUAL ENVIRONMENTS

Security management is simplified with unified administration of physical and virtual environments including clear separation of administrative functions between virtualization and security administrators.

Security Gateway Virtual Edition is managed from the same Security Management or Multi-Domain Management (MDM) as all other physical Check Point security gateways and appliances. This enables you to deploy a single pane of glass to ensure consistent security at all gateways, while minimizing the expense of separate management consoles.

Check Point SmartDashboard GUI – Unified management for physical and virtual gateways

Traffic logging, reporting and full virtualization auditing solutions tailored for the virtual infrastructure enable users to accelerate and achieve compliance, with dedicated reports that are mapped to relevant requirements within the PCI, SOX, HIPAA, COBIT and ISO 17799 regulations and standards.

Check Point Security Management and MDM can also be deployed on virtual machines.

