



CA Host-Based Intrusion Prevention System r8

CA Host-Based Intrusion Prevention System (CA HIPS) blends stand-alone firewall and intrusion detection and prevention capabilities to provide centralized proactive threat protection to counter online threats. This combination offers superior security access control, policy enforcement, easy intrusion prevention management and deployment from a central location via a single console with an intuitive user interface. It also extends the endpoint protection of the CA Threat Manager r8.1 solution composed of the CA Anti-Virus r8.1 and CA Anti-Spyware r8.1 offerings and complements the gateway protection offered by CA Secure Content Manager r8.

Key Features at a Glance

- Three Threat Protection Technologies in One
- Behavior-based Real-time Threat Protection
- Enterprise-focused Threat Management Solution
- Centralized Policy Management
- Comprehensive Event Management

Supported Environments

Client Computer (Win32)

- Windows 2000 SP3 or Higher
- Windows 2003
- Windows XP Professional

Management Server

- Java 1.5x
- Windows 2000 SP 4
- Windows 2003 (32-Bit) 5.2
- Windows XP (32-Bit) SP1 and SP2

Today's Malware Challenges

The sophistication of new threats and the damage they cause are increasing at the same time that more and more employees and partners are working remotely. To counterattack today's threats, traditional anti-virus and anti-spyware solutions are no longer sufficient to protect stand-alone systems against targeted application-level attacks.

To effectively manage today's threats and security challenges, organizations also require an enterprise-ready, combined stand-alone firewall with a host-based intrusion detection and prevention (IDS/IPS) solution. This solution provides protection by proactively identifying and preventing the malicious behavior characteristic of malware. It assists both

IT administrators and end users by detecting, filtering, and managing applications and system resources.

Comprehensive CA HIPS Solution Benefits

CA HIPS is an innovative combination of a stand-alone firewall and a comprehensive host-based intrusion detection and prevention system. By adding CA HIPS, you enhance your endpoint protection through centralized access control and policy enforcement. The IPS capabilities allow organizations to automatically react to threats and block malicious traffic while the IDS features block known threats. Both provide alerts based on the priorities defined by the system administrator via the Event Manager.

Fewer Threat Infections Means Reduced Costs. CA HIPS reduces the risk of downtime by preventing malware, spyware, adware and rogue software from gaining access to the network via the endpoint. By reducing or eliminating the remediation expenses and help desk costs associated with successful malware attacks, CA HIPS helps improve cost and operational efficiencies.

Protection from Zero-Day Attacks Helps Ensure Service Continuity. CA HIPS provides proactive, host-based security against zero-day attacks. System administrators can use key functionality within CA HIPS to learn system behavior and then create or edit existing policies to detect anomalies. This feature helps keep your critical IT assets up and running by protecting resources and processes in absence of signature updates. This also helps the system administrator customize environments based on business requirements.

Expands and Complements your Existing Threat Management Products to Offer Multilayered Threat Protection. Adding CA HIPS to your existing endpoint threat defenses will help you prevent known and unknown threats such as malware, spyware, adware and rogue software from penetrating your network. When combined with your existing anti-virus and anti-spyware products (such as CA Anti-Virus or CA Anti-Spyware) you gain the added capability to detect and remove threats that may happen to evade detection.

Distinctive Features and Functionalities

Three Threat Protection Technologies in One. CA HIPS blends stand-alone firewall and intrusion detection and prevention capabilities to provide centralized proactive threat protection to counter online threats. This combination offers superior access control, policy enforcement, easy intrusion prevention

management and deployment from a central location via a single, intuitive user interface to enhance your endpoint protection.

Behavior-based Real-time Protection from Known and Unknown Threats. System administrators can use key functionality within CA HIPS to learn system behavior and then create or edit existing policies to detect anomalies based on behavior and prevent potentially malicious activity. This feature helps ensure service continuity and helps keep your critical IT assets up and running by protecting resources and processes. This also helps the system administrator customize environments based on business requirements.

Enterprise-focused Threat Management Solution. IT professionals and network administrators can now protect against security breaches and ensure service continuity by determining what traffic is appropriate, what applications can communicate and even what behaviors and access rights on individual systems will be allowed or blocked. Centralized management functions allow for efficient and effective logging of all relevant events

to help with compliance, reporting and investigations

Centralized Policy Management. CA HIPS offers excellent centrally-managed policy creation, deployment and maintenance to make ongoing administration of security policy across the enterprise easy and flexible.

CA HIPS makes it easy to set policies to apply rules for:

- Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory User Groups (users, administrators)
- Computer Groups (laptops, servers, devices)
- Firewall, IDS and IPS Rules and File Protection
- Security Levels

The system administrator can determine the level of access and control applied to the system, to groups of users or to an individual user. Even better, the system administrator can set up a policy that applies to specific users when they are in specific roles or locations.

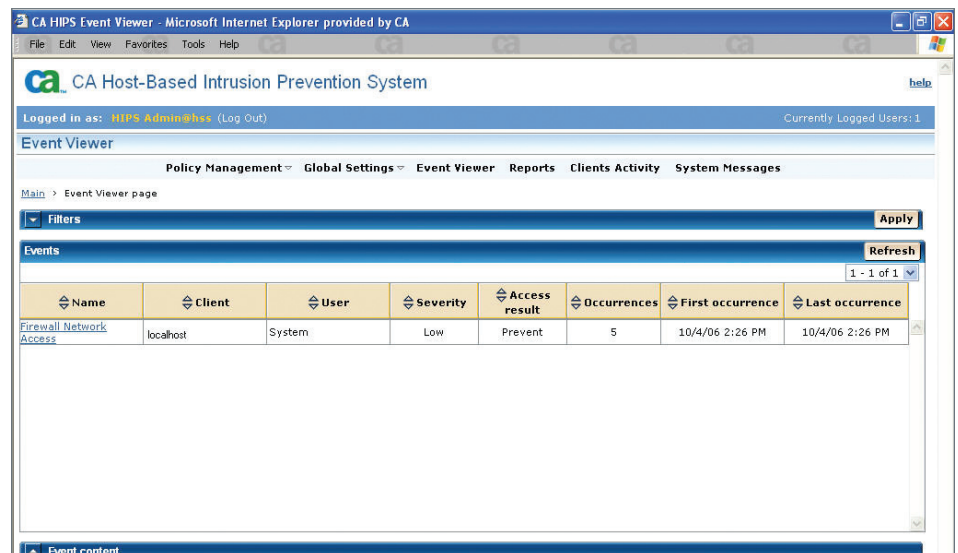


Figure 1. The CA HIPS Event Viewer

Comprehensive Event Management. The CA HIPS server collects and records the events that occur on each client. To help administrators make sense of the high volume of events, CA HIPS provides primary criteria the system administrator can use to filter the events. For example, the system administrator can display a list of the last events uploaded to the server, or examine a specific event for more information using the additional filtering criteria on the convenient drop-down menu.

Policy-based Client User Interface. CA HIPS provides an intuitive client user interface for end users. Depending on the policies set by the system administrator, end users can see and modify CA HIPS defensive measures and block new attacks to the desktops if necessary. This feature is set centrally by the administrator and can be turned on or off at the administrator's discretion.

Graphical Technical and Business Threat Reports. CA HIPS provides the ability to track incidents and look for patterns. Graphical reports are designed make it easy for administrators to collate, analyze, understand and present their information. CA HIPS provides several preconfigured reports that allow administrators to display their information graphically in tables, pie charts or bar charts.

Broad Language Support. Global English at general availability. French, Italian, German, Spanish, Brazilian Portuguese and Simplified Chinese shortly after general availability.

For more information,
call 1-800-875-9659 or
visit ca.com/threatmgmt

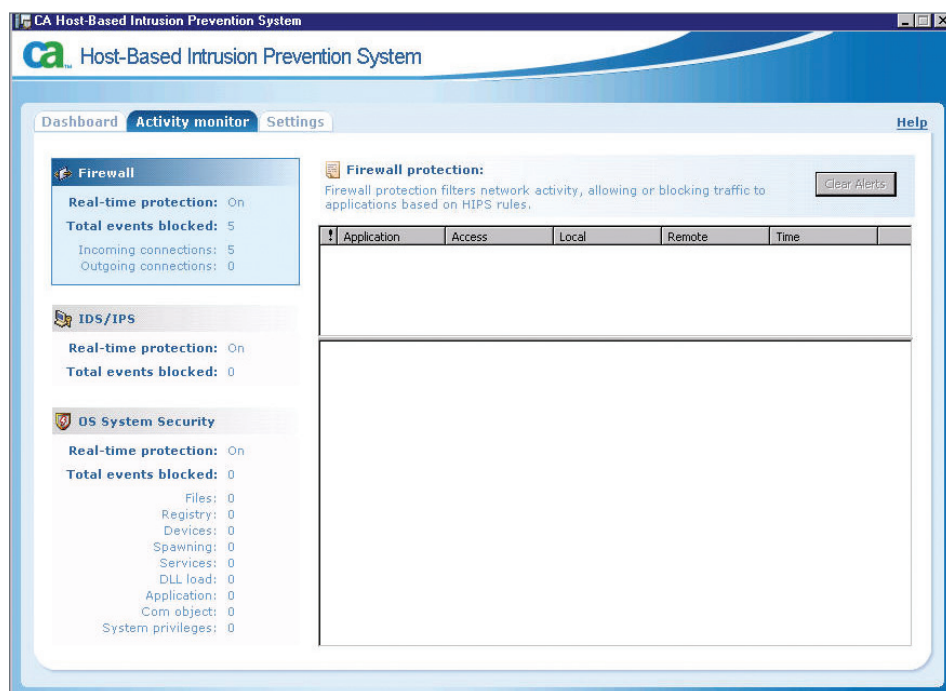


Figure 2. The CA HIPS Client Interface

