

# Protecting Endpoint Systems Using Host-Based Intrusion Prevention

---

# Table of Contents

---

## Executive Summary

---

SECTION 1: CHALLENGE **2**  
**Issues Surrounding Endpoint Security**

---

SECTION 2: OPPORTUNITY **2**  
**Requirements for Effective Host-Based Intrusion Prevention**

What Is CA HIPS?

Firewall

IDS/IPS

OS System Security

CA HIPS Policies

Rules and Rule Sets

Policy Deployment

The CA HIPS Client

---

SECTION 3: BENEFITS **11**  
**Business Benefits of Host-Based Intrusion Prevention**

**Business Benefits of Host-Based Intrusion Prevention in an Integrated Solution**

---

SECTION 4: CONCLUSIONS **13**

---

SECTION 5: REFERENCES **13**

---

ABOUT CA **Back Cover**

# Executive Summary

## Challenge

---

Traditional anti-virus and anti-spyware tools are fundamental to enterprise threat defense. However, these tools have limitations because, before a threat can be identified and stopped, the threat must be identified as malicious and new signatures must be distributed to endpoint computers. Anti-virus and anti-spyware must, therefore, be used together with a Host-Based Intrusion Prevention System (HIPS), in which behavior-based techniques are used to identify anomalous and potentially malicious behavior. These techniques enable HIPS to protect computers against threats even before new anti-virus and anti-spyware signatures are distributed.

## Opportunity

---

Effective, host-based intrusion prevention should include both intrusion detection and intrusion prevention. This means that network traffic is inspected for suspicious patterns that may indicate a network attack, and if suspicious activity is detected alerts can be generated and actions taken. A host-based firewall is also essential, to manage network traffic between the host and other computers and networks. Intrusion prevention should also include with some form of operating system security to protect files and system configurations and to restrict access to devices, such as USB storage drives.

## Benefits

---

CA HIPS blends stand-alone firewall and intrusion detection and prevention capabilities and provides centralized proactive threat protection to counter online threats. By using these technologies, CA HIPS can identify anomalous and potentially malicious behavior immediately, to help protect computers against zero-day and other attacks. HIPS techniques complement the signature-based approach that is used by anti-virus and anti-spyware applications. CA HIPS comes with a set of pre-defined policies that can be used as is. These policies can be supplemented by custom policies.

---

## SECTION 1: CHALLENGE

### Issues Surrounding Endpoint Security

A recent IDC study<sup>1</sup> found that the top three computer threats are viruses, spyware and unsolicited email, or spam. For this reason, traditional anti-virus and anti-spyware tools are fundamental to enterprise threat defense. However, these tools have limitations and should be complemented by other technology. For example, anti-spyware and anti-virus software detect and eliminate threats based on signatures, so, before a threat can be identified and stopped, other tools must identify the threat code as malicious, add the code to the signature list, and distribute the signature list to endpoint computers. The time between new signature creation and system update provides a brief opportunity for new, unidentified threats to infect endpoints in a zero-day attack.

What is needed is a Host-based Intrusion Prevention System (HIPS), which uses behavior-based techniques to identify anomalous and potentially malicious behavior, to protect computers against zero-day and other attacks.

---

## SECTION 2: OPPORTUNITY

### Requirements for Effective Host-Based Intrusion Prevention

To be effective, host-based intrusion prevention should include the following components:

- **IDS** An intrusion detection system (IDS) inspects inbound and outbound network traffic to identify suspicious patterns that may indicate a network attack. An IDS monitors host and server events and system logs from multiple sources for suspicious activity. An IDS can alert a system administrator to this type of suspicious activity, but it cannot deter or prevent the activity from taking place. An IDS deals with known threats and is primarily a reactive technology.
- **IPS** An intrusion prevention system (IPS) adds policies to an IDS to generate alerts and actions if suspicious activity is detected. The IPS policies use sets of rules to identify traffic, and also to make decisions about what happens when an anomalous event is detected. An IPS is a proactive technology and is used to protect the system from potential and unknown threats.
- **Firewall** A host-based firewall controls network traffic between the host and other computers and networks. As well as being able to inspect packet headers, a firewall must be able to perform stateful packet inspection, so that it can identify and permit only that traffic which matches known legitimate connection behavior.
- **Operating System Security** OS security includes protection against malicious or accidental access to specific files and folders, and system configurations such as the Windows Registry. It can also be very useful to be able to restrict access to devices, so that exploits cannot be introduced onto endpoint computers through devices such as USB storage drives.
- **Policy-Based Management** Policies are used to apply restrictions based on criteria such as user name, computer name, network address and time of day. The ability to use policy-based management is important for most enterprises, as all users do not need the same levels of threat protection. Computers in public locations, for example, must have more restrictive policies than those applied to trusted computers in secure offices.

---

<sup>1</sup> Source: IDC, "Worldwide Secure Content Management 2006-2010 Forecast Update and 2005 Vendor Shares: "The Convergence of Secure Content and Threat Management," #203550, September, 2006

- **Simple Deployment Tools** If multiple computers are installed across several physical locations, it is important to be able to rapidly deploy host-based protection by using automated methods. It must also be simple to deploy software updates across the network and to identify any computers that have not been updated.

### What Is CA HIPS?

CA HIPS is a combined IDS, IPS and firewall. CA HIPS, therefore, blends stand-alone firewall and intrusion detection and prevention capabilities and provides centralized proactive threat protection to counter online threats. By using these technologies, CA HIPS can identify anomalous and potentially malicious behavior immediately, to help protect against zero-day and other attacks.

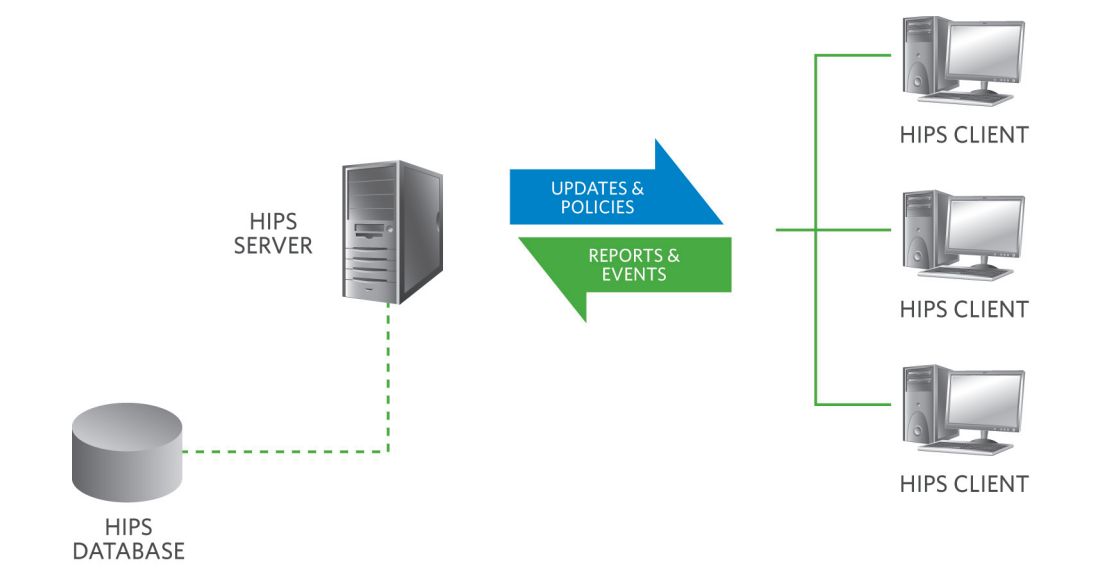
CA HIPS is an endpoint protection tool that you configure and manage from a central management server. The client “phones home” to the server to receive updates, on a schedule that you define. The client connects to a main server but for resilience can be configured to contact alternate servers if the main server is not available. Policies are managed from the server and stored in a database, before deployment to client computers. When the client is not connected to the network, client protection is defined by the policy which was most recently downloaded from the server.

Figure A shows the main CA HIPS components.

FIGURE A

CA HIPS is a client protection tool managed from a central server.

### CA HIPS SERVER AND CLIENT COMPONENTS



The HIPS server controls the CA HIPS software in your environment. You use the web console on the HIPS server to perform the following tasks:

- Create and distribute policies and rules to all of the HIPS clients in your organization. HIPS policies control how clients respond to threats. You create and manage policies from the server, and then deploy them by replacing the current read-only policies that are stored on the server with your new or updated policies. By using a schedule that you can configure, HIPS clients regularly check the server for updated policies and download updates as required.
- Collect and store events recorded on each client. The HIPS server collects and records events from each client. HIPS clients send low and medium events to the server at regular intervals. High-priority events are sent to the server immediately.
- Specify which components of the HIPS client are installed on each client computer. You use the web console on the HIPS server to create an installation package for the HIPS client software. You can create customized installations for particular types of users. For example, if you do not want certain users to know CA HIPS is installed, you can use the server console to create a custom HIPS client that does not have a user interface and use the silent install option.
- Control whether users of a client computer can change any of their local CA HIPS software settings. When you create the HIPS client package, you can restrict what client settings users can change.
- The HIPS server uses a relational database to store event data that is collected from CA HIPS clients, and also user, group and computer information. When you first install CA HIPS, you can configure the server to use a built-in SQL database. Alternatively, you can use an external SQL server to store the CA HIPS data.
- The CA HIPS application provides several important levels of protection, including firewall, intrusion detection and prevention, and OS system security.

### Firewall

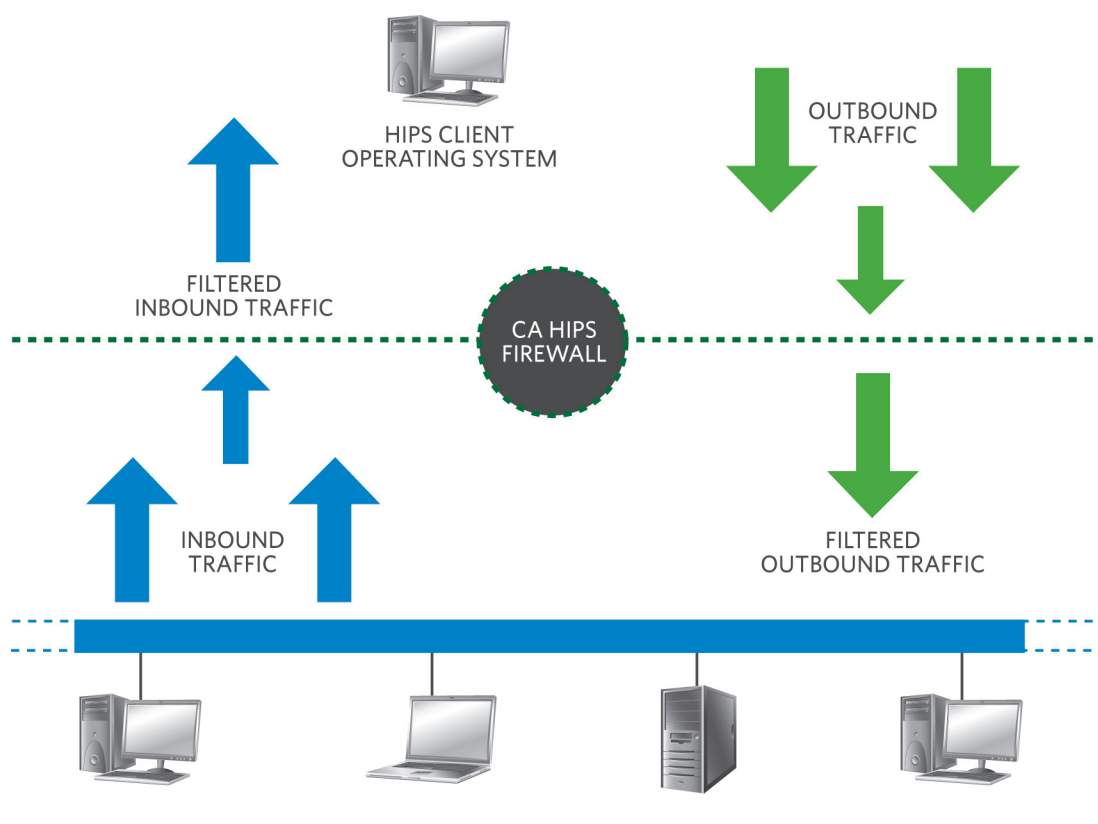
The HIPS firewall uses predefined rules to filter network activity, or uses rules that you configure yourself, to allow or block traffic. The HIPS firewall is a stateful packet inspection firewall, which replaces the built-in firewall on Windows XP and Windows Server 2003 computers.

Figure B shows the CA HIPS firewall operation.

**FIGURE B**

The CA HIPS firewall inspects inbound and outbound traffic.

**CA HIPS FIREWALL**



*SNORT rules define patterns and behaviors that identify potentially malicious traffic on your network. They are tested and certified by the Sourcefire Vulnerability Research Team.*

**IDS/IPS**

IDS and IPS are combined in one module of CA HIPS. The CA HIPS IDS/IPS module examines network packets for known attack patterns, as well as for attacks that are documented in the HIPS database. CA uses a combination of SNORT rules, as well as information from the CA Research team, when preparing the information to distribute to HIPS servers.

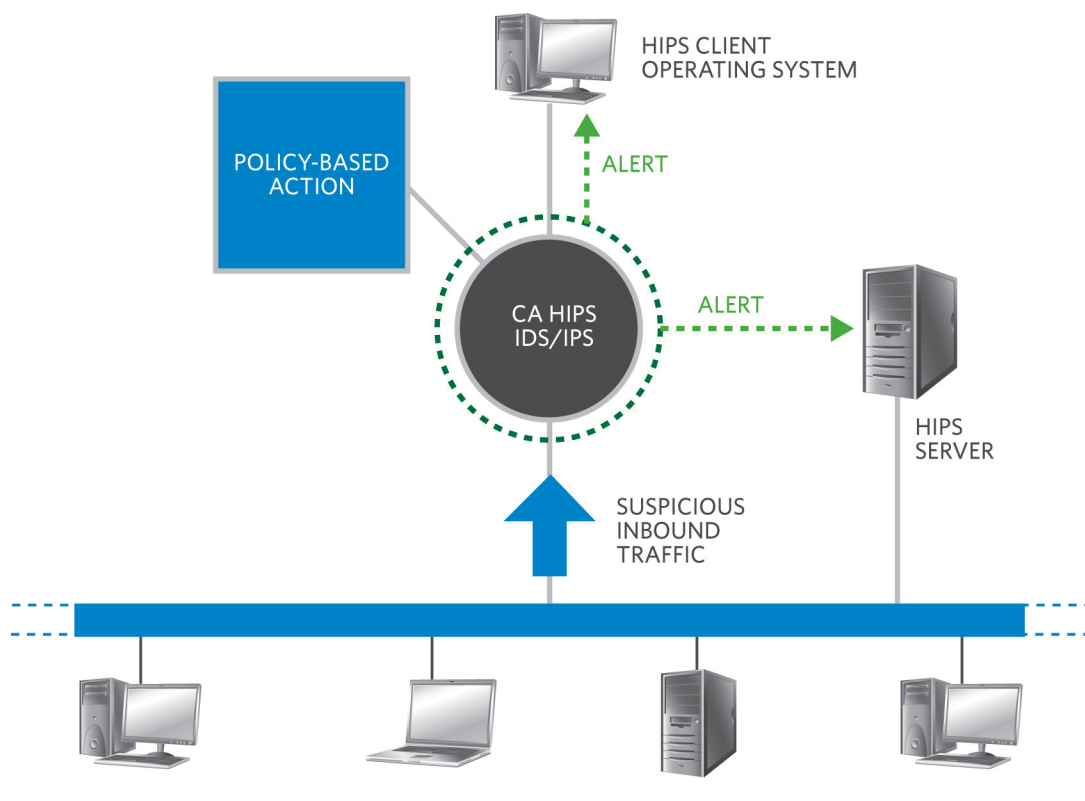
Based on the HIPS policy that is in force on the client, and through the implementation of IDS/IPS rules, the HIPS server issues a warning and can block an action if necessary. This activity on the endpoint is captured and reported back to the server by the Event Manager.

Figure C shows the IDS/IPS service in operation.

#### FIGURE C

CA HIPS has a combined IDS/IPS module.

#### CA HIPS IDS/IP



#### OS System Security

The CA HIPS OS system security service provides a base level of security, and protects operating system resources from unwanted or suspicious changes. The operating system can be monitored for changes, including:

- Reading and modifying files and the registry
- Spawning applications
- Loading DLLs
- Accessing OLE/COM objects
- Modifying system services
- Attempting to acquire system privileges
- Accessing computer devices, such as USB storage devices, CD-ROM and DVD drives, and infrared ports

### CA HIPS Policies

A policy is set of rules that state what a client is allowed or not allowed to do, by determining acceptable networking, application and device use. Policies are downloaded to HIPS clients from the HIPS server. You can use or modify the default policies or import policies from other systems. Policies are built by using re-usable component objects that are then used in rules and rule sets. The rule sets are used to create HIPS policies. This architecture makes it easy to define policies for specific work environments, manage groups of policies, and update and maintain those policies. Updating any object automatically updates all rules, rule sets and policies that use that object. For example, if you have several policies that are configured to run during the working week and your business changes its hours of operation from 9:00 a.m. – 5:00 p.m. Monday to Friday to 7:00 a.m. – 6:00 p.m. Monday to Friday, you simply update the relevant Time Frame object, and every policy that uses rules that reference that object will be updated for the new time period.

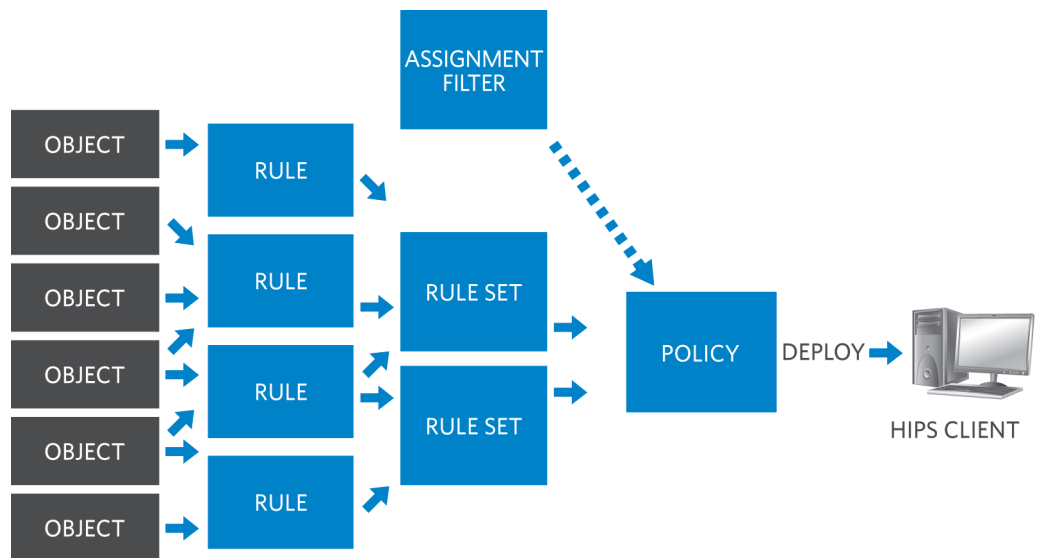
CA HIPS enables you to define highly granular policies. You might have a group of users who spend time in your headquarters location, work part-time in a remote office and who also travel to customer locations. In this case, you could define three policies; HQ, Remote and Traveling. Each of these policies would have a specific set of rules relevant to the location. For example, when traveling to a customer site, the user would use the Traveling policy, with rules for accessing networks by using a VPN or by using wireless links.

Figure D shows how objects are used to create HIPS policies.

FIGURE D

CA HIPS uses objects and rules to create flexible and effective policies.

### OBJECTS, RULES, RULESETS AND POLICIES



CA HIPS uses common settings and several types of objects:

- **Application Objects** CA HIPS includes an application repository, which holds application objects for any application or DLL file that you want to use in a rule. You define application objects by filename, path or Message Digest 5 (MD5) hash, which creates a specific identify and means that you can easily distinguish between updated versions if required. Application objects can be grouped by using application groups, so that, for example, all trusted applications can be referenced in a policy. The default CA HIPS application repository includes predefined objects and groups for common applications.

You can use application repository rules to automatically enroll applications in the repository and add them to specific application groups. This makes it easy to set up a new CA HIPS environment, because most common applications do not need to be manually added to the repository. When an application tries to use a network resource that is monitored by CA HIPS, the client checks the application repository to see if the application is already enrolled. If the application is enrolled, it is processed according to any rules and policies previously associated with the application. If the application is unknown, it is processed in the following way:

1. The HIPS client searches a database of known applications. This database includes a list of application information supplied by CA HIPS, updates to the list from the CA Research team, and applications added by CA HIPS administrators. The HIPS server distributes the database to HIPS clients.
  2. If an application is found in the database, it is enrolled and assigned to an application group according to the application repository rules.
  3. If the unknown application does not match any of the application repository rules, it is enrolled in the application repository, but not assigned to any groups, and the most-restrictive (default) security policy is assigned to it. This means you can allow a user to continue to run an application, whilst keeping it in a restricted environment where the application is not permitted to make changes to core services or install malicious code.
- **Firewall Objects** If you want to control the type of traffic that is allowed to access a HIPS client, you use the firewall objects. There are firewall objects for Protocols, which define a protocol, port number and traffic access direction, and IP addresses, which define IPv4 or IPv6 addresses or subnet masks. You then use firewall objects in a firewall rule. For example, if you want to block all TCP traffic on port 80 to a particular IP address on your network, you:
    1. Create a protocol firewall object that specifies the TCP protocol and port 80.
    2. Create an IP address firewall object that specifies the IP address you want to block from receiving traffic.
    3. Create a firewall rule that uses both of these objects.
  - **OS System Security Objects** If you want to control access to operating system resources on a HIPS client, you use one of the OS system security objects; File, Registry, OLE/COM, Services or Devices. You then use OS system security objects in an OS system security rule. For example, if you want to block access to the print spooler service on a client, you must:
    1. Create an OS system security services rule object that specifies the print spooler service.
    2. Create an OS system security rule by using this object.

- **IDS/IPS Objects** If you want to filter traffic against known attack patterns, you use an IDS/IPS object in an IDS/IPS rule. IDS/IPS objects specify an IP address or range of addresses. For example, if you want to create IDS/IPS rules to monitor or block traffic from the 172.16.0.0 - 172.16.0.255 range of IP addresses, you:
  1. Create an IDS/IPS object specifying the 172.16.0.0 - 172.16.0.255 address range.
  2. Create an IDS/IPS rule using this object.

**COMMON SETTINGS** There are several common settings that can apply to one or more types of policy. For example, you can use time frame objects to control when a rule is active, and the same object can be applied to multiple rules so that you do not need to specify an active time for each rule individually. Other global settings include port scanning detection, so that client computers detect, block and report on external attempts to scan for open ports, and then send details of these events to the HIPS server.

### Rules and Rule Sets

Rules allow or deny individual actions and are created by using HIPS objects. Individual rules are grouped into rule sets, and the rule sets are applied to policies and deployed to HIPS clients. Predefined rules and rule groups are updated regularly and automatically downloaded to the HIPS server to provide protection against new threats. There are several types of rules, including:

- **Application Repository** Controls specific application behaviors and how applications that are not currently defined in the application repository are processed by CA HIPS.
- **Firewall** Controls network access to and from computers, by restricting access to protocols, ports and IP addresses.
- **Firewall Zone** Defines network interfaces, IP addresses or protocols as safe or dangerous.
- **OS System Security** Controls access to the operating system of the computer.
- **OS System Security Guard** Enables or disables types of rules for certain applications or groups of applications, such as specifying that only file and registry access is monitored for particular application groups. These guards protect core services, including areas such as the Registry and system configurations.
- **IDS/IPS** Controls intrusion detection and intrusion prevention. The CA HIPS server includes a set of predefined IDS/IPS rules. These IDS/IPS rules are divided into rule groups according to the type of threat that they protect against. For example, IDS/IPS rules that protect against distributed denial-of-service attacks are included in an IDS/IPS rule group called `ddos.rules`. CA uses SNORT rules and information from the CA Research team to build the IDS/IPS rules list. You can also add your own IDS/IPS rules.

CA HIPS has a learning mode that you can use to import application repository objects, and several types of rules, to the HIPS server from an existing example computer. This means you can make best use of previously created policies and rules, and then customize the CA HIPS environment without needing to manually add application objects and rules.

### Policy Deployment

The CA HIPS software uses policies to determine when and how to apply rules and rule sets to the HIPS client computers. Setting policies on the server and passing policies to the client, makes for consistency across clients. Clients poll the server to download policy updates by using a configurable time interval. This minimizes the administrative overhead that is required for policy distribution.

CA HIPS includes several example policies that you can use or modify. Alternatively, you can create your own policies. For example, if you want to block TCP/IP traffic on port 80 between 9 a.m. and 5 p.m. and for a particular group of computers, you:

1. Create a firewall protocol object for outbound TCP port 80.
2. Create a time frame object for the hours of 9 a.m. to 5 .pm.
3. Create a firewall rule that uses the TCP/IP port 80 firewall object and the time frame object.
4. Add the rule to a firewall rule set.
5. Create a policy that includes the rule set, which has an assignment filter for the group of computers that must be controlled.
6. Deploy the policy.

Assignment filters control how a policy is applied. There are several assignment filter options, including:

- **Server Status** This controls how a policy is applied, based on whether the client can successfully communicate with the HIPS server. For example, you might want to apply a restrictive policy that only takes effect after the client has unsuccessfully tried to connect to a server a specific number of times. This ensures that clients are protected even if they have not been able to obtain an update from the server.
- **Security Level** This controls how a policy is applied, based on configurable criteria that you define on the HIPS server. For example, you could set a highly restrictive policy to apply only when the server security level has been set to “red”.
- **Subnet** This enables you to apply a policy to a specific subnet or subnets on your network. Subnets are defined as part of the configuration of your organizational structure on the HIPS server. You could use this to define a set of rules for a remote site that does not have dedicated IT resources.
- **Users** This enables you to apply a policy to a specific user or user group on your network. Users are defined as part of the configuration of your organizational structure on the HIPS server, and you can configure the HIPS server to automatically query an Active Directory server for user and group information.
- **Computers** This enables you to apply a policy to a specific computer, or group of computers, on your network. Computers are defined as part of the configuration of your organizational structure on the HIPS server, and you can configure the HIPS server to automatically query an Active Directory server for computer information.

### The CA HIPS Client

If the client has been installed with the user interface (optional, at the administrator’s discretion), you can use the interface to display information about the CA HIPS software that is installed on the computer, such as the list of blocked events in the local alert history. As an administrator, you can control whether users can configure some of the client settings.

Figure E shows the client interface, on an endpoint computer without interface restrictions.

FIGURE E

The CA HIPS client can include a detailed user interface.

CA HIPS CLIENT INTERFACE



The dashboard page shows an overview of the client software and policy versions, together with a summary of the events that have been blocked. The activity monitor page gives detailed event information. The settings page enables the user to change aspects of the client configuration, if the user has permission to do so.

## SECTION 3: BENEFITS

### Business Benefits of Host-Based Intrusion Prevention

CA HIPS includes a range of features that are designed to protect client computers from network-related threats and include:

- **Combined Threat Protection Technologies** CA HIPS combines a stand-alone firewall, IDS and IPS technologies and OS security guards. This combination can protect computers against a wide range of attacks. By using a combination of these technologies, you can reduce your support and implementation costs.
- **Behavior-Based Real-Time Threat Protection** By using the learning mode tool, you can use CA HIPS to define the system behavior that is normal or acceptable for your networks. You can then use HIPS policies to detect activity which falls outside your expected behavior patterns. This technology works in the absence of signature-based updates to protect data against zero-day and other previously unknown attacks. By modifying these policies you can customize your CA HIPS environment to fit your business requirements.
- **Enterprise-Focused Threat Management** You can decide what network traffic should be allowed in or out of a client computer, and the applications that are allowed to access the network. You can also select the type of application behavior and access rights that are allowed or blocked. Centralized management functions provide efficient and effective logging of all relevant events to help with compliance, reporting and investigations.

- **Centralized Policy Management** HIPS policies, and the deployment and maintenance of HIPS client software, is centrally-managed from the HIPS server, and provides simple and flexible administration of security policy. As a system manager, you have the option to:
  - Import policy from another system.
  - Use the CA HIPS default policy.
  - Modify an existing policy for a specific instance.
- From the server console, you can assign policies and configure settings for all computers and users, for groups of computers and users, or for an individual computer or user. You can customize policy by location, role and access method. This flexibility means you can easily configure a policy that applies to specific users in specific work situations.
- **Comprehensive Event Management** The HIPS server collects details of all events that occur on HIPS clients. As an example, you can use event filters to view recent events, or events by particular HIPS module, such as firewall module, IDS/IPS module, or OS system security module. The event viewer makes it easy to investigate and identify possible attack patterns or system anomalies.
- **Policy-Based Client User Interface** As an administrator, you can customize the client user interface. The options range from a full view of all policy and rules, through event tracking and client connection information, to a locked down interface, where the user is not aware of the software or the installation process. This makes it simple to customize the client for your users, according to their needs and technical competency.
- **Graphical Technical and Business Threat Reports** CA HIPS reports help you to track incidents and look for patterns. There is a range of preconfigured reports, such as the top 10 intrusions and recent blocked applications, which can be customized as required (by using filters). Clear reporting helps your organization to comply with legal and other requirements.
- **Deployment Tools** You first build and configure a client installation package, by using the server console, then you can deploy the HIPS client from disk, flash drive, network share, or by using msi-based software deployment tools, such as CA Unicenter® Software Delivery and Microsoft Systems Management Server (SMS). When creating the client from the server you can define a set of policies that are transferred to all clients during the installation process. This means it is easy to create different types of client installations, for different types of users or work styles.
- **Supported Environments** CA HIPS is a Windows application that supports the following Windows versions for the client:
  - Windows 2000 Professional with SP3 or SP4
  - Windows 2000 Server with SP3 or SP4
  - Windows 2000 Advanced Server with SP3 or SP4
  - Windows XP Professional with SP1 or SP2 (32 bit edition only)
  - Windows 2003 Server Standard without SP or with SP1 (32 bit edition only)
  - Windows 2003 Server Enterprise Edition without SP or with SP1 (32 bit edition only)

The following Windows versions are supported for the management server:

- Windows 2000 Professional with SP4
  - Windows 2000 Server with SP4
  - Windows 2000 Advanced Server with SP4
  - Windows XP Professional with SP2 (32 bit edition only)
  - Windows 2003 Server Standard with SP1 (32 bit edition only)
  - Windows 2003 Server Enterprise Edition with SP1 (32 bit edition only)
- **Language Support** CA HIPS supports Global English, French, Italian, German, Spanish, Brazilian Portuguese and Simplified Chinese. If your business is multi-lingual or global, you can select the best language for your users.

---

## Business Benefits of Host-Based Intrusion Prevention in an Integrated Solution

One product or technique cannot protect a computer against every possible threat. Multiple layers of defense are required, with specific technologies that are used to combat specific threat types. A combination of products working together is needed to protect the endpoint. CA HIPS is designed to work with other CA Threat Management Solutions to offer comprehensive threat protection. CA HIPS can also add value to third-party threat management products.

**THE CA THREAT MANAGEMENT SOLUTIONS** includes solutions for both the endpoint systems (desktop, server, laptop, and other network access point) and gateway:

- **CA Anti-Virus** Standalone virus protection for endpoint systems.
- **CA Anti-Spyware** Standalone spyware protection for endpoint systems.
- **CA Threat Manager** Integrated anti-virus and anti-spyware protection for endpoint systems. The CA Threat Manager components detect and remove malware threats that evade detection or that previously infected the endpoint.
- **CA Secure Content Manager** Anti-virus protection for the gateway. SMTP and HTTP filtering for incoming Web threats, messaging threats or spam, and content filtering of outgoing email traffic.

According to Gartner, “there are several drivers for HIPS deployments, and prioritizing which is more important will help to narrow the list of solutions. In surveys at conferences and in conversations with clients, the primary driver cited is the need to proactively shield desktops and servers from attacks on known vulnerabilities until patches can be applied. For proactive shielding until systems can be patched, solutions capable of deep packet inspection (DPI) are generally better-suited. A secondary driver tends to be protection from “zero day” and targeted attacks in which the vulnerability hasn’t yet been disclosed. For robust protection from zero-day and targeted attacks, execution-level solutions (see Table A) are generally better-suited. If the organization wants both, this narrows the list to HIPS vendors that provide multiple styles of protection in a single client.”

**TABLE A**

Gartner defines Nine Styles of Host-Based Intrusion Prevention<sup>1</sup>.

**“THE NINE STYLES OF HOST-BASED INTRUSION PREVENTION” BY GARTNER**

|                      | ALLOW<br>KNOWN GOOD<br>(BLOCK ALL ELSE)         | BLOCK<br>KNOWN BAD<br>(ALLOW ALL ELSE)          | UNKNOWN  |
|----------------------|---|---|--|
| EXECUTION<br>LEVEL   | <b>7</b><br>APPLICATION<br>CONTROL              | <b>8</b><br>RESOURCE<br>SHIELDING               | <b>9</b><br>BEHAVIORAL<br>CONTAINMENT<br><small>PASSIVE → ACTIVE</small> |
| APPLICATION<br>LEVEL | <b>4</b><br>APPLICATION AND<br>SYSTEM HARDENING | <b>5</b><br>ANTI-VIRUS                          | <b>6</b><br>APPLICATION<br>INSPECTION                                    |
| NETWORK<br>LEVEL     | <b>1</b><br>HOST<br>FIREWALL                    | <b>2</b><br>ATTACK-FACING<br>NETWORK INSPECTION | <b>3</b><br>VULNERABLE-FACING<br>NETWORK INSPECTION                      |

CA HIPS alone or in combination with other CA Threat Management Solutions covers each of the nine types. For type 5, CA HIPS provides both IDS and IPS rules to identify a virus but it relies on the advanced capability of anti-virus products (CA Anti-Virus or CA Threat Manager) to deal with the virus and restore the system to health. Further, CA Secure Content Manager (CA SCM) provides additional application level protection, including URL filtering.

<sup>1</sup> Source: Gartner, “Best Practices for Implementing Host-Based Intrusion Prevention Systems,” # G00144668, Neil McDonald, November 2006.

---

**SECTION 4: CONCLUSIONS**

CA Host-Based Intrusion Prevention System uses behavior-based techniques to identify threats, and complements the signature-based approach that is used by anti-virus and anti-spyware applications. CA HIPS works with other CA Threat Management Solutions providing a complete suite of threat management tools.

---

**SECTION 5: REFERENCES**

“CA Security Advisor”  
<http://www3.ca.com/securityadvisor/>

---

“SNORT”  
<http://www.snort.org/>

---

To learn more about the CA Host-Based Intrusion Prevention System (CA HIPS) architecture and technical approach, visit [CA HIPS Product Page](#).

CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies complex IT management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

TB05HIPSP01E MP317620807

---

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

