Important Notice

Cyberoam Technologies Pvt. Ltd. has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Cyberoam Technologies Pvt. Ltd. assumes no responsibility for any errors that may appear in this document. Cyberoam Technologies Pvt. Ltd. reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER’S LICENSE

Use of this product and document is subject to acceptance of the terms and conditions of Cyberoam End User License Agreement (EULA) and Warranty Policy for Cyberoam UTM Appliances.


RESTRICTED RIGHTS

Copyright 1999 - 2015 Cyberoam Technologies Pvt. Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Cyberoam Technologies Pvt. Ltd.

Corporate Headquarters

Cyberoam House,
Saigulshan Complex, Opp. Sanskruti,
Beside White House, Panchwati Cross Road,
Ahmedabad - 380006, GUJARAT, INDIA.
Tel: +91-79-66216666
Fax: +91-79-26407640
Web site: www.cyberoam.com
Contents

Preface ................................................................................................................................. 4
Technical Support .................................................................................................................. 5
Introduction .......................................................................................................................... 6
Appliance Administrative Interfaces ..................................................................................... 7
  Web Admin Console .......................................................................................................... 7
  Command Line Interface (CLI) Console ........................................................................... 8
  Cyberoam Central Console (CCC) .................................................................................... 8
Web Admin Console ............................................................................................................. 9
  Web Admin Language ....................................................................................................... 9
  Supported Browsers ......................................................................................................... 10
  Login procedure .............................................................................................................. 11
  Log out procedure ........................................................................................................... 12
  Menus and Pages ............................................................................................................. 13
  Page .................................................................................................................................. 15
  Icon bar ............................................................................................................................. 16
  List Navigation Controls ................................................................................................. 17
  Tool Tips ........................................................................................................................... 17
  Status Bar ......................................................................................................................... 17
  Common Operations ......................................................................................................... 18
IPS ....................................................................................................................................... 20
Cyberoam IPS ....................................................................................................................... 21
  Policy ................................................................................................................................. 22
  Policy ................................................................................................................................. 23
  Custom Signature ............................................................................................................ 27
Preface

The Appliances use Layer 8 technology to help organizations maintain a state of readiness against today's blended threats and offer real-time protection.

Unified Threat Management Appliances offer identity-based comprehensive security to organizations against blended threats - worms, viruses, malware, data loss, identity theft; threats over applications viz. Instant Messengers; threats over secure protocols viz. HTTPS; and more. They also offer wireless security (WLAN) and 3G wireless broadband. Analog modem support can be used as either Active or Backup WAN connection for business continuity.

The Appliance integrates features like stateful inspection firewall, VPN, Gateway Anti-Virus and Anti-Spyware, Gateway Anti-Spam, Intrusion Prevention System, Content & Application Filtering, Data Leakage Prevention, IM Management and Control, Layer 7 visibility, Web Application Firewall, Bandwidth Management, Multiple Link Management and Comprehensive Reporting over a single platform.

The Appliance has enhanced security by adding an 8th layer (User Identity) to the protocol stack. Advanced inspection provides L8 user-identity and L7 application detail in classifying traffic, enabling Administrators to apply access and bandwidth policies far beyond the controls that traditional UTMs support. It thus offers security to organizations across layer 2 - layer 8, without compromising productivity and connectivity.

The Appliance accelerates unified security by enabling single-point control of all its security features through a Web 2.0-based GUI. An extensible architecture and an 'IPv6 Ready' Gold logo provide Appliance the readiness to deliver on future security requirements.

The Appliances provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection.

Layer 8 Security:
The Appliance’s features are built around its patent pending Layer 8 technology. The Layer 8 technology implements the human layer of networking by allowing organizations control traffic based on users instead of mere IP Addresses. Layer 8 technology keeps organizations a step ahead of conventional security solutions by providing full business flexibility and security in any environment including WI-FI and DHCP.
Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
Cyberoam House,
Saigulshan Complex, Opp. Sanskruti,
Beside White House, Panchwati Cross Road,
Ahmedabad - 380006, GUJARAT, INDIA.
Tel: +91-79-66216666
Fax: +91-79-26407640
Web site: www.cyberoam.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-66216565
Email: support@cyberoam.com
Web site: www.cyberoam.com

Visit www.cyberoam.com for the regional and latest contact information.
Introduction

Welcome to Cyberoam’s – IPS Implementation guide.

Cyberoam is an Identity-based UTM Appliance. Cyberoam’s solution is purpose-built to meet the security needs of corporates, government organizations, and educational institutions.

Cyberoam’s perfect blend of best-of-breed solutions includes user based Firewall, Content filtering, Anti Virus, Anti Spam, (Intrusion Prevention System) IPS, and VPN – IPSec and SSL.

Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server and others hosted in DMZ, which are visible to the external world and still have firewall protection.

Cyberoam is a real time IPS that protects your network from known and unknown attacks by worms and viruses, hackers and other Internet risks.

Cyberoam appliance at the perimeter of your network analyzes all traffic and prevents attacks from reaching your network. Whether it is a worm, a suspicious web request, a hacker targeting your mail server or any other attack - it simply does not get through.

Note

All the screen shots are taken from NG series of Appliances. The feature and functionalities however remains unchanged across all Cyberoam Appliances.

Note

The Intrusion Prevention System module is a subscription module that needs to be subscribed before use. Check the features of the module by subscribing to the free trial subscription of the module. (See System > Maintenance > Licensing)
Appliance Administrative Interfaces

Appliance can be accessed and administered through:

1. Web Admin Console
2. Command Line Interface Console
3. Cyberoam Central Console

Administrative Access An administrator can connect and access the Appliance through HTTP, HTTPS, telnet, or SSH services. Depending on the Administrator login account profile used for access, an administrator can access number of Administrative Interfaces and Web Admin Console configuration pages.

Appliance is shipped with two administrator accounts and four administrator profiles.

<table>
<thead>
<tr>
<th>Administrator Type</th>
<th>Login Credentials</th>
<th>Console Access</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Administrator</td>
<td>admin/admin</td>
<td>Web Admin Console</td>
<td>Full privileges for both the consoles. It provides read-write permission for all the configuration performed through either of the consoles.</td>
</tr>
<tr>
<td>Default</td>
<td>cyberoam/cyber</td>
<td>Web Admin console only</td>
<td>Full privileges. It provides read-write permission for all the configuration pages of Web Admin console.</td>
</tr>
</tbody>
</table>

Note
We recommend that you change the password of both the users immediately on deployment.

Web Admin Console

Web Admin Console is a web-based application that an Administrator can use to configure, monitor, and manage the Appliance.

You can connect to and access Web Admin Console of the Appliance using HTTP or a HTTPS connection from any management computer using web browser:

1. HTTP login: http://<LAN IP Address of the Appliance>
2. HTTPS login: https://<LAN IP Address of the Appliance>

For more details, refer section Web Admin Console.
Command Line Interface (CLI) Console

Appliance CLI console provides a collection of tools to administer, monitor and control certain Appliance component. The Appliance can be accessed remotely using the following connections:

1. **Remote login Utility – TELNET login**
   
   To access Appliance from command prompt using remote login utility – Telnet, use command `TELNET <LAN IP Address of the Appliance>`. Use default password “admin”.

2. **SSH Client (Serial Console)**
   
   SSH client securely connects to the Appliance and performs command-line operations. CLI console of the Appliance can be accessed via any of the SSH client using LAN IP Address of the Appliance and providing Administrator credentials for authentication.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start SSH client and create new Connection with the following parameters:</td>
</tr>
<tr>
<td>Host – &lt;LAN IP Address of the Appliance&gt;</td>
</tr>
<tr>
<td>Username – admin</td>
</tr>
<tr>
<td>Password – admin</td>
</tr>
</tbody>
</table>

Use CLI console for troubleshooting and diagnose network problems in details. For more details, refer version specific Console Guide available on [http://docs.cyberoam.com/](http://docs.cyberoam.com/).

Cyberoam Central Console (CCC)

Distributed Cyberoam Appliances can be centrally managed using a single Cyberoam Central Console (CCC) Appliance, enabling high levels of security for Managed Security Service Provider (MSSPs) and large enterprises. To monitor and manage Cyberoam using CCC Appliance you must:

1. **Configure CCC Appliance in Cyberoam**

2. **Integrate Cyberoam Appliance with CCC using: Auto Discovery or Manually**

   Once you have added the Appliances and organized them into groups, you can configure single Appliance or groups of Appliances.

   For more information, please refer CCC Administrator Guide.
Web Admin Console

CyberoamOS uses a Web 2.0 based easy-to-use graphical interface termed as Web Admin Console to configure and manage the Appliance.

You can access the Appliance for HTTP and HTTPS web browser-based administration from any of the interfaces. Appliance when connected and powered up for the first time, it will have a following default Web Admin Console Access configuration for HTTP and HTTPS services.

<table>
<thead>
<tr>
<th>Services</th>
<th>Interface/Zones</th>
<th>Default Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>LAN, WAN</td>
<td>TCP Port 80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>WAN</td>
<td>TCP Port 443</td>
</tr>
</tbody>
</table>

The administrator can update the default ports for HTTP and HTTPS services from **System > Administration > Settings**.

Web Admin Language

The Web Admin Console supports multiple languages, but by default appears in English. To cater to its non-English customers, apart from English, Chinese-Simplified, Chinese-Traditional, Hindi, Japanese and French languages are also supported. Administrator can choose the preferred GUI language at the time of logging on.

Listed elements of Web Admin Console will be displayed in the configured language:

- Dashboard Doclet contents
- Navigation menu
- Screen elements including field & button labels and tips
- Error messages
**Supported Browsers**

You can connect to the Web Admin Console of the Appliance using HTTP or a secure HTTPS connection from any management computer using one of the following web browsers:

The minimum screen resolution for the management computer is 1024 X 768 and 32-bit true xx-color.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Explorer</td>
<td>Version 8+</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Version 3+</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>All versions</td>
</tr>
<tr>
<td>Safari</td>
<td>5.1.2(7534.52.7)+</td>
</tr>
<tr>
<td>Opera</td>
<td>15.0.1147.141+</td>
</tr>
</tbody>
</table>

The Administrator can also specify the description for firewall rule, various policies, services and various custom categories in any of the supported languages.

All the configuration done using Web Admin Console takes effect immediately. To assist you in configuring the Appliance, the Appliance includes a detailed context-sensitive online help.
Login procedure

The log on procedure authenticates the user and creates a session with the Appliance until the user logs-off.

To get to the login window, open the browser and type the LAN IP Address of Cyberoam in the browser’s URL box. A dialog box appears prompting you to enter username and password.

![Login Screen](image_url)

Screen – Login Screen

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter user login name. If you are logging on for the first time after installation, use the default username.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify user account password. Dots are the placeholders in the password field. If you are logging on for the first time after installation with the default username, use the default password.</td>
</tr>
<tr>
<td>Language</td>
<td>Select the language. The available options are Chinese-Simplified, Chinese-Traditional, English, French, and Hindi. Default – English</td>
</tr>
<tr>
<td>Log on to</td>
<td>To administer Cyberoam, select ‘Web Admin Console’. To view logs and reports, select “Reports”. To login into your account, select “My Account”.</td>
</tr>
<tr>
<td>Login button</td>
<td>Click to log on the Web Admin Console.</td>
</tr>
</tbody>
</table>

Table – Login Screen

The Dashboard appears as soon as you log on to the Web Admin Console. It provides a quick and fast overview of all the important parameters of your Appliance.
Log out procedure

To avoid un-authorized users from accessing Cyberoam, log off after you have finished working. This will end the session and exit from Cyberoam.

To log off from the Appliance, click the **Logout** button located at the top right of any of the Web Admin Console pages.
Menus and Pages

The Navigation bar on the leftmost side provides access to various configuration pages. This menu consists of sub-menus and tabs. On clicking the menu item in the navigation bar, related management functions are displayed as submenu items in the navigation bar itself. On clicking submenu item, all the associated tabs are displayed as the horizontal menu bar on the top of the page. To view a page associated with the tab, click the required tab.

The left navigation bar expands and contracts dynamically when clicked on without navigating to a submenu. When you click on a top-level heading in the left navigation bar, it automatically expands that heading and contracts the heading for the page you are currently on, but it does not navigate away from the current page. To navigate to a new page, first click on the heading, and then click on the submenu you want navigate to. On hovering the cursor upon the up-scroll icon or the down-scroll icon, automatically scrolls the navigation bar up or down respectively.

The navigation menu includes following modules:

- System – System administration and configuration, firmware maintenance, backup - restore
- Objects – Configuration of various policies for hosts, services, schedules and file type
- Networks – Network specific configuration viz., Interface speed, MTU and MSS settings, Gateway, DDNS
• Identity – Configuration and management of User and user groups
• Firewall – Firewall Rule Management
• VPN – VPN and SSL VPN access configuration
• IPS – IPS policies and signature
• Web Filter – Web filtering categories and policies configuration
• Application Filter – Application filtering categories and policies configuration
• WAF – Web Application Filtering policies configuration. Available in all the models except CR15iNG and CR15wiNG.
• IM – IM controls
• QoS – Policy management viz., surfing quota, QoS, access time, data transfer
• Anti Virus – Antivirus filtering policies configuration
• Anti Spam – Anti Spam filtering policies configuration
• Traffic Discovery – Traffic monitoring
• Logs & Reports – Logs and reports configuration

Note

Use F1 key for page-specific help.
Use F10 key to return to Dashboard.

Each section in this guide shows the menu path to the configuration page. For example, to reach the Zone page, choose the Network menu, then choose Interface sub-menu from the navigation bar, and then choose Zone tab. Guide mentions this path as Network > Interface > Zone.
A typical page looks as shown in the below given image:
Icon bar

The Icon bar on the upper rightmost corner of every page provides access to several commonly used functions like:

1. **Dashboard** – Click to view the Dashboard
2. **Wizard** – Opens a Network Configuration Wizard for a step-by-step configuration of the network parameters like IP Address, subnet mask and default gateway for your Appliance.
3. **Report** – Opens a Reports page for viewing various usage reports. Integrated Logging and Reporting solution - iView, to offer wide spectrum of 1000+ unique user identity-based reporting across applications and protocols and provide in-depth network visibility to help organizations take corrective and preventive measures.

   This feature is not available for CR15xxxx series of Appliances.

4. **Console** – Provides immediate access to CLI by initiating a telnet connection with CLI without closing Web Admin console.
5. **Logout** – Click to log off from the Web Admin Console.
6. **More Options** – Provides options for further assistance. The available options are as follows:
   - **Support** – Opens the customer login page for creating a Technical Support Ticket. It is fast, easy and puts your case right into the Technical Support queue.
   - **About Product** – Opens the Appliance registration information page.
   - **Help** – Opens the context-sensitive help page.
   - **Reset Dashboard** – Resets the Dashboard to factory default settings.
   - **Lock** – Locks the Web Admin Console. Web Admin Console is automatically locked if the Appliance is in inactive state for more than 3 minutes. To unlock the Web Admin Console you need to re-login. By default, Lock functionality is disabled. Enable Admin Session Lock from **System > Administration > Settings**.
   - **Reboot Appliance** – Reboots the Appliance.
   - **Shutdown Appliance** – Shuts down the Appliance.
List Navigation Controls

The Web Admin Console pages display information in the form of lists that are spread across the multiple pages. Page Navigation Control Bar on the upper right top corner of the list provides navigation buttons for moving through the list of pages with a large number of entries. It also includes an option to specify the number entries/records displayed per page.

Tool Tips

To view the additional configuration information use tool tip. Tool tip is provided for many configurable fields. Move the pointer over the icon 🔄 to view the brief configuration summary.

Status Bar

The Status bar at the bottom of the page displays the action status.

Status: ✅ Country Host 'Sydney_Office' has been added successfully.

Status: ⚠️ User could not be registered. User or User group with the same name already exists, choose a different name.
Common Operations

Adding an Entity

You can add a new entity like policy, group, user, rule, ir host by clicking the Add button available on most of the configuration pages. Clicking this button either opens a new page or a pop-up window.

Editing an Entity

All the editable entities are hyperlinked. You can edit any entity by clicking either the hyperlink or the Edit icon under the Manage column.

Deleting an Entity

You can delete an entity by selecting the checkbox and clicking the Delete button or Delete icon.

To delete multiple entities, select individual entity and click the Delete button.

To delete all the entities, select in the heading column and click the Delete button.
Sorting Lists

To organize a list spread over multiple pages, sort the list in ascending or descending order of a column attribute. You can sort a list by clicking a column heading.

- Ascending Order icon in a column heading indicates that the list is sorted in ascending order of the column attribute.
- Descending Order icon in a column heading indicates that the list is sorted descending order of the column attribute.

Filtering Lists

To search specific information within the long list spread over multiple pages, filter the lists. Filtering criteria vary depending on a column data and can be a number or an IP address or part of an address, or any text string combination.

To create filter, click the Filter icon in a column heading. When a filter is applied to a column, the Filter icon changes to .

Configuring Column Settings

By default on every page all columnar information is displayed but on certain pages where a large number of columnar information is available, all the columns cannot be displayed. It is also possible that some content may not be of use to everyone. Using column settings, you can configure to display only those numbers of columns that are important to you.

To configure column settings, click Select Column Settings and select the checkbox against the columns you want to display and clear the checkbox against the columns which you do not want to display. All the default columns are greyed and not selectable.
IPS

An IPS is a type of security management system that gathers and analyzes information from a network to identify possible security breaches, which include both intrusions - attacks from outside the organization and misuse - attacks from within the organization.

IPS detects and/or prevents malicious activity such as Denial of Service attacks, port-scans or even attempts to crack into computers by monitoring network traffic.

To detect such activity, IPS uses signatures. Whenever a matching traffic pattern to the signature is found, the IPS triggers an alarm and blocks the traffic from reaching its destination.

Standard IPS allows defining a global policy that can be applied to source-destination networks-hosts/ports combination. This global policy can be modified or tuned as per requirement but cannot be tailored per network or per host.

As global policy is a general policy for all, standard IPSs generate a high amount of false positives and this makes it difficult to pinpoint the host generating malicious traffic or vice versa.

Fine-tuning of the global policy means to disable a set of signatures for all the networks-hosts. However, this may not be a fit-for-all policy and hence might reduce false positives for one network while increase for another. Chances are that sometimes it may not even detect certain obvious malicious activity.
Cyberoam IPS

Cyberoam IPS is a real time Intrusion Prevention System (IPS) that protects your network from known and unknown attacks by worms and viruses, hackers and other Internet risks.

Cyberoam appliance at the perimeter of your network analyzes entire traffic and prevents attacks from reaching your network. Whether it is a worm, a suspicious web request, a hacker targeting your mail server or any other attack - it simply does not get through.

IPS consists of a signature engine with a predefined database of signatures and uses signatures to identify malicious activity on the network. Predefined signatures cannot be modified.

As per your network requirements, the Appliance allows you to define multiple policies instead of one global policy, to decrease packet latency and reduce false positives.

The IPS policy allows you to view predefined signatures and customize the intrusion prevention configuration at the category as well as individual signature level. Categories are signatures grouped together based on the application and protocol vulnerabilities.

The Appliance, instead of providing only a single policy (global) for managing multiple networks/hosts, allows you to define multiple policies per network/host. Defining multiple policies instead of a single global policy helps in decreasing packet latency and reducing false positives.

To enable Intrusion Detection and Prevention, apply IPS Policy from Firewall Rule. You can create rules to apply:
- A single policy for all the users/networks
- different policies for different users/networks or hosts

As Firewall Rules control all traffic passing through the Appliance and decide whether to allow or drop the connection, the IPS rule will be applied to only that traffic/packet which passes through the Firewall.

- Policy
- Custom Signature
Policy

The IPS consists of a signature engine with a predefined set of signatures. Signatures are the patterns that are known to be harmful. IPS compares the traffic with these signatures and responds at a high rate of speed if it finds a match. Signatures included within the Appliance cannot be modified.

Category

Signatures are organized in categories such as DNS, Finger, P2P, DDoS, and others. These signature categories are listed in the policy. You can configure these categories to change the prevention and/or detection settings. To perform Intrusion Prevention and Detection, you need to enable IPS services for each category. Hence, you will be able to configure attack threats for an individual signature only if an IPS service for the category is “Enabled”.

Each IPS Policy contains a set of signatures that the Appliance searches for, and logs, blocks and allows to:

- Enable or disable a category from IPS protection.
- Enable or disable an individual signature in a category to define the IPS protection based on your network environment.
- Define an action to be taken when the matching traffic pattern is found. The Appliance can either detect or drop the connection. In either of the case, the Appliance generates the log and alerts the Network Administrator.

IPS provides six actions for managing attack threats: (action if signature matches)

- **Allow Packet** – The Appliance allows the packet to its intended destination.
- **Disable** – Disables the signature, if it detects any traffic that matches with it,
- **Drop Packet** – The Appliance drops the packets, if detects any traffic that matches the signature.
- **Drop Session** – The Appliance drops the entire session, if detects any traffic that matches the signature.
- **Reset** – The Appliance resets entire session, if detects any traffic that matches the signature.
- **Bypass Session** – The Appliance allows all the session packets, if detects any traffic that matches the signature.

In packet-based actions, the Appliance checks each packet before taking the action while for session-based action, only the first packet is checked and the action is taken. In case of Reset, the TCP reset packet is sent to the originator. In all the cases, the Appliance generates a log and alerts the Network Administrator.

To save resources and avoid latency, set action as “Bypass Session” as in this, if the initial packets match the signature then the rest of the session packets will not be scanned at all.

To avoid getting a high number of Alerts and to save resources, set action as “Drop session” as in this, if the Appliance identifies an attack in the initial packets then it will terminate the entire session instead of scanning all the session packets.
Policy

The IPS Policy page displays a list of all the pre-defined and custom IPS policies and you can sort the list based on policy name. The page provides options to add a new policy, configure the handling of signatures by category or on a signature-by-signature basis, or delete the policy. Create and deploy IPS policies to block malicious or suspicious traffic and increase security and productivity.

The Appliance provides following pre-defined policies. You can directly use policies 1 to 6 without any modifications while policies 7 to 10 can either be used directly or can be modified as per your requirements:

- DMZ TO LAN
- DMZ TO WAN
- LAN TO DMZ
- LAN TO WAN
- WAN TO DMZ
- WAN TO LAN
- generalpolicy
- lan2wans strict policy
- lan2wan general policy
- dmzpolicy

- **Enable/Disable Individual Signature** – Click the Edit icon in the Manage column against the IPS Policy in which the signature matching is to be enabled or disabled. Search the signature category or click on the Category name under which the signature is included. Change the action for the required signature.

Manage Policies

To manage IPS Policies, go to **IPS > Policy**.

![Table - Manage IPS Policies screen elements](image-url)

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays name of the IPS Policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays IPS Policy description.</td>
</tr>
</tbody>
</table>
Creating IPS Policy

To add policies, go to **IPS > Policy**. Click the Add Button to configure a new policy. The IPS Policy Parameters are given below.

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name to identify the IPS Policy.</td>
</tr>
<tr>
<td>Template</td>
<td>Select the IPS Policy to be used as a template from the available list.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the IPS Policy description.</td>
</tr>
</tbody>
</table>

Table – Add IPS Policy screen elements

IPS Policy Rules

Once the policy is created, policy rules can be added to take appropriate action for signatures in the policy. Define a rule to configure the action to be taken when a matching traffic pattern is found. If the rules are already added, they are displayed along with their details like signature filtering criteria, action. You can add, update, or delete the rules.
<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Provide a name for IPS Policy Rule.</td>
</tr>
</tbody>
</table>

**Signature Criteria**

<table>
<thead>
<tr>
<th>Default</th>
<th>Select the signature criteria as “Default” to get a list of default signatures and take action on them.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Signature</td>
<td>Select the signature criteria as “Custom Signature” to get a list of custom signatures and take action on them.</td>
</tr>
<tr>
<td>Category</td>
<td>Select the IPS signature category from the list of available categories.</td>
</tr>
<tr>
<td>Severity</td>
<td>Select the type of severity from the available options</td>
</tr>
<tr>
<td><strong>Available Options:</strong></td>
<td></td>
</tr>
<tr>
<td>Select All</td>
<td></td>
</tr>
<tr>
<td>1 – Critical</td>
<td></td>
</tr>
<tr>
<td>2 – Major</td>
<td></td>
</tr>
<tr>
<td>3 – Moderate</td>
<td></td>
</tr>
<tr>
<td>4 – Minor</td>
<td></td>
</tr>
<tr>
<td>5 - Warning</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platform</th>
<th>Select the platform from the available options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available Options:</strong></td>
<td></td>
</tr>
<tr>
<td>Select All</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>Unix</td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td></td>
</tr>
<tr>
<td>Solaris</td>
<td></td>
</tr>
<tr>
<td>BSD</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

| Target          | Select the target from the available options |
### Available Options:
- Select All
- Client
- Server

### List of Matching Signature

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select All</strong></td>
<td>Select the option “Select All” to choose all the signatures listed for the selected criteria. Based on the selected Signature Criteria the signatures are made available.</td>
</tr>
<tr>
<td><strong>Select Individual Signature</strong></td>
<td>Select option “Select Individual Signature” to customize the choice of Signature list for the selected criteria. Based on the selected Signature Criteria the signatures are made available.</td>
</tr>
<tr>
<td><strong>Search</strong></td>
<td>Specify the Signature Name in the textbox to search for a Signature. This option is available, only if option “Select Individual Signature” is selected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Displays the signature name.</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Displays the signature category.</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Displays the signature severity.</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Displays the signature platform.</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>Displays the signature target.</td>
</tr>
<tr>
<td><strong>Recommended Action</strong></td>
<td>Displays the recommended signature action.</td>
</tr>
</tbody>
</table>

### Action

Select an action to be taken from the available options:

**Available Options:**
- **Recommended** - This action means that you want the CyberoamOS to handle this alert level according to its best-fit recommendations.
- **Allow Packet** – Allows the packet to its intended destination.
- **Drop Packet** – Drops packets if it detects any traffic that matches the signature.
- **Disable** – Disables the signature, if it detects any traffic that matches the signature.
- **Drop Session** – Drops the entire session if detects any traffic that matches the signature.
- **Reset** – Resets entire session if detects any traffic that matches the signature.
- **Bypass Session** – Allows all the session packets if detects any traffic that matches the signature.

**Table – Add IPS Policy Rules screen elements**
Custom Signature

Custom Signatures provide the flexibility to customize IPSs for diverse network environments. Predefined signatures included in the Appliance cover common attacks while Custom Signatures protect your network from uncommon attacks that are due to the use of a proprietary server, custom protocol, or specialized application in the corporate network.

The Custom Signature page displays a list of all the custom signatures. The page provides options to add a new signature, update the parameters of existing signature, or delete the signature.

You can also create Custom Signature for a proprietary server, custom protocol, or specialized applications used in the corporate network and protect your network.

To create and manage Custom IPS Signatures, go to **IPS > Custom Signature > Custom Signature**.

Manage Custom Signatures

To manage Custom IPS Signatures, go to **IPS > Custom Signature**.

![Screen – Manage Custom Signatures](image)

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the Custom Signature.</td>
</tr>
</tbody>
</table>

Table – Manage Custom Signatures screen elements

Custom Signature Parameters

To add Custom IPS Signatures, go to **IPS > Custom Signature**.

![Screen – Add Custom Signature](image)
<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name to identify the Custom Signature.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the signature Protocol from the list.</td>
</tr>
<tr>
<td>Custom Rule</td>
<td>Specify the signature definition.</td>
</tr>
<tr>
<td></td>
<td>Signature definition must begin with a keyword followed by the value enclosed between the double quotes and must end with semicolon (;)</td>
</tr>
<tr>
<td></td>
<td>Format: Keyword: &quot;value&quot;;</td>
</tr>
<tr>
<td></td>
<td>For example, content: &quot;USER JOHN&quot;;</td>
</tr>
<tr>
<td></td>
<td>If traffic with the content USER JOHN is detected, action defined in the policy will be taken.</td>
</tr>
<tr>
<td></td>
<td>Refer to Appendix B – IPS - Custom Signature Syntax for more details on creating signature.</td>
</tr>
<tr>
<td>Severity</td>
<td>Select the level of severity from the available options.</td>
</tr>
<tr>
<td></td>
<td>Available Options:</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Major</td>
</tr>
<tr>
<td></td>
<td>• Moderate</td>
</tr>
<tr>
<td></td>
<td>• Minor</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td>Action</td>
<td>Specify action to be taken on the selected policy when matching pattern is found.</td>
</tr>
<tr>
<td></td>
<td>Available Actions:</td>
</tr>
<tr>
<td></td>
<td>• Allow Packet – Appliance checks each packet before taking action.</td>
</tr>
<tr>
<td></td>
<td>• Drop Packet – Appliance does not check each packet before taking action.</td>
</tr>
<tr>
<td></td>
<td>• Drop Session – Entire session is terminated instead of scanning all the session packets to save resources and avoid getting high number of alerts.</td>
</tr>
<tr>
<td></td>
<td>• Reset – TCP reset packet is sent to the originator.</td>
</tr>
<tr>
<td></td>
<td>• Bypass Session – Only initial packets are matched to save resources and avoid latency.</td>
</tr>
<tr>
<td></td>
<td>In all the cases, the Appliance generates the log and alerts the Network Administrator.</td>
</tr>
</tbody>
</table>

*Table – Add Custom Signature screen elements*