

How To Guide

XRoads Networks

Edge Network Appliance How To Guide:
Firewall

Edge Network Appliance How To Guide: Firewall

@2009 XRoads Networks

22642 Lambert St, Suite 403

888-9-XROADS

Table of Contents

Firewall Overview

User/Device Management

Network Access Control

L7 Firewall Rules

L7 Firewall Control

L7 DoS/SYN Filtering

Site2Site Client Termination

PPTP Client Termination

Advanced Spyware & Web Filtering

Basic Web Domain & URL Filtering

Email Defense & Spam Filtering

Edge Configuration Series

Firewall Overview

The EdgeXOS appliance includes a fully stateful and hardened firewall. Our firewall meets the highest standards in terms of network security and the ability to block unwanted access to the internal network.

The firewall has been certified as being compliant with ICSA standards and has passed multiple tests to become PCI compliant for ecommerce networks.

The logo for XRoads Networks, featuring the text "XRoads Networks" in a white, sans-serif font against a dark blue background with a subtle wave pattern.[Home](#)[Interfaces](#)[Shaping](#)[NetBalancing](#)[Firewall](#)[Site2Site](#)[Tools](#)[Reporting](#)

Firewall Modules

The firewall components are designed to provide network administrators with a complete cloud security system, from a layer-7 stateful firewall to built-in web content filtering, and enhanced anti-spyware and anti-virus filtering, to remote access software to allow teleworkers to connect to the local network, the EdgeXOS platform is a complete security solution. The EdgeXOS firewall also includes enterprise class email and anti-spam filtering along with on and offsite backup solutions.

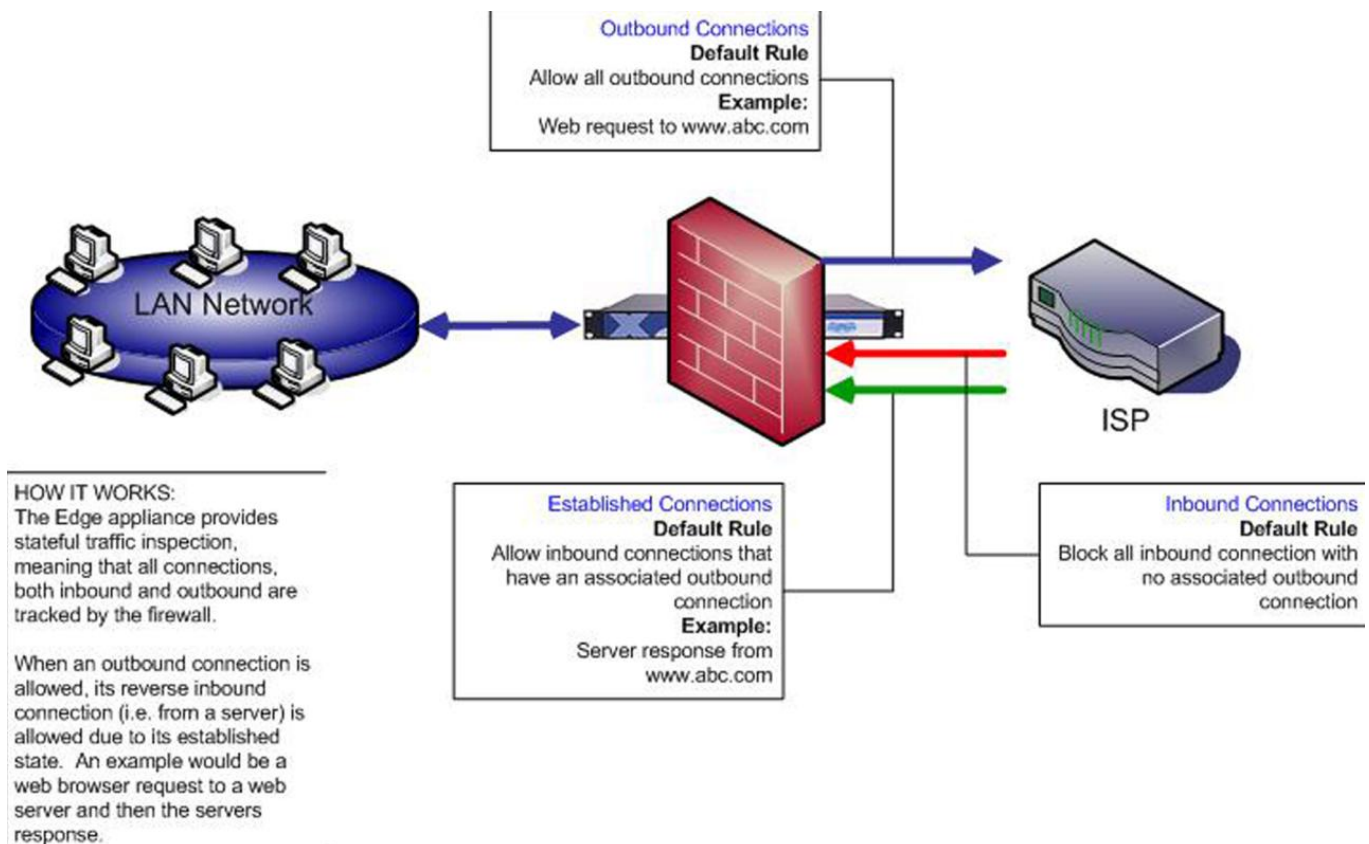
The EdgeXOS platform is able to achieve its industry leading security solution through strategic partnerships with companies like Webroot, Netsweeper, and McAfee.

These companies provide the databases and filtering capabilities that our solution utilize to provide our enhanced security offerings.

SPI Firewall Overview

The L7 (layer seven) stateful packet inspection firewall provides bi-directional session tracking to ensure that only those traffic flows which are allowed can actually pass-through the firewall.

The diagram below provides an example of how the stateful inspection works:



HOW IT WORKS:

The Edge appliance provides stateful traffic inspection, meaning that all connections, both inbound and outbound are tracked by the firewall.

In specific example above shows an outbound web request to www.abc.com. This request is allowed using the default rule which allows all outbound connectivity by default. When the corresponding response from the www.abc.com server is received by the firewall, the stateful engine determines that the packets from the www.abc.com server are in response to the outbound web request, and thus the firewall allows the inbound HTML packets to be forwarded to the internal client that made the web request.

Firewall Rule Creation

The firewall module is primarily controlled by creating firewall rules which either allow or deny traffic through the Edge appliance. The firewall rules can be applied to ALL or any individual network interfaces.

Rules are applied in ALPABETICAL ORDER based on the Group Name. Firewall rules are applied in a first to match method. In other words, the first rule to match the particular type of traffic will apply. If no rule matches, the default rules apply.

The screenshot displays the Firewall Rule Creation interface with the following configuration details:

- Edge Security:** SPI Firewall Rules
- Group Name:** WebFarm (with a note: <- Select A Firewall Group OR Create A New One ->)
- Inbound Interface:** WAN+
- Source Definition:** ANY (Source Network / Mask)
- Destination Definition:** ANY (Destination Network / Default: All LAN Addresses)
- Service:** ANY----->ANY (Specify A Service)
- Action:** ACCEPT
- Log:** (Matched Rule Logging) with a warning: WARNING: Use for temporary analysis only, can create system problems over time.
- Color:** - default - (Define a color for this rule, optional)
- Comments:** (Rule Description)

Buttons at the bottom: Reset, Add / Update, View Rules >>

NOTE: By default, all outbound access is allowed. By default, all inbound access is denied. Example: All inbound server traffic is denied by default, and all outbound LAN network traffic is allowed by default.

Create Or Select A Group Name

Select the group which this firewall rule will apply, or create a new group by entering the name in the field provided.

Group Name: <- Select A Firewall Group OR Create A New One ->

WebFarm
VPN
Sales
Engineering
Deny-Accounting
Accounting
AAA-Log
1-BlockPorts

(Source Address OR Select LAN - ANY)
(Source Network / Mask)

OR

NOTE: Rules are applied in ALPABETICAL ORDER based on the Group Name. Firewall rules are applied in a first to match method. In other words, the first rule to match the type of traffic will apply. If no rule matches, the default rules apply.

Source Definition

Use the source definition to define where the traffic is coming from, or select ANY.

When defining a source, the first step is to select the appropriate Inbound interface (i.e. the interface in which the traffic arrives to the Edge appliance). Then enter the IP address or network address to be applied and select the appropriate subnet mask, or select SINGLE HOST to specify only a single host match.

Source Definition: (Source Address OR Select LAN - ANY)

ANY (Source Network / Mask)

OR

--- Select Source --- (Select a pre-defined source)

64.12.15.20 / SINGLE HOST
10.100.30.5 / SINGLE HOST
LAN / LAN

(Destination Network / Default All LAN Addresses)

NOTE: The WAN+ selection specifies all WAN interfaces.

Destination Definition

Use the destination definition to define where the traffic is going to, or select ANY.

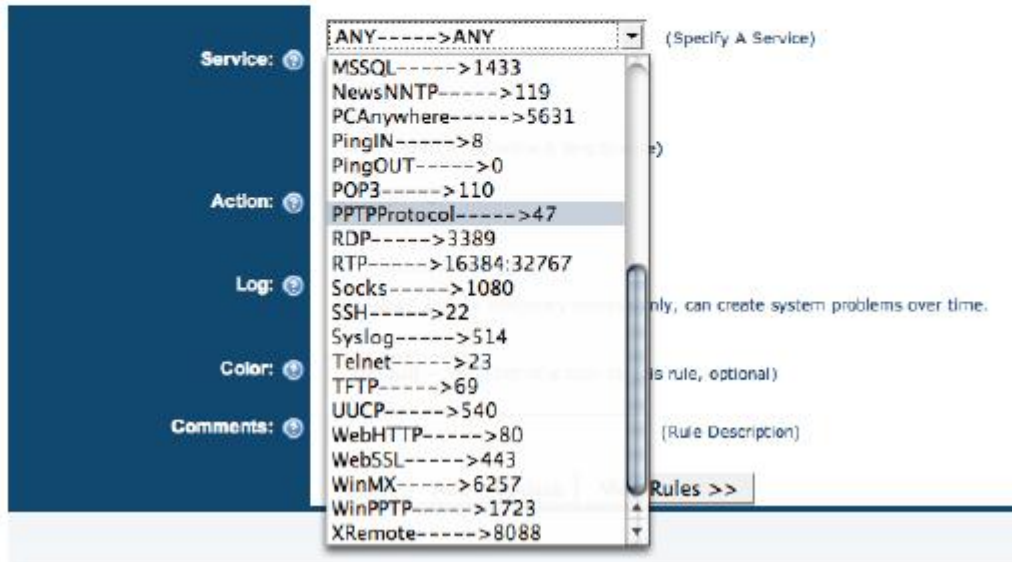
Enter the destination IP address or network address to be applied and select the subnet mask, or select SINGLE HOST to specify only a single host. When specifying a network, make sure to enter the correct network address, i.e. xxx.xxx.xxx.0 for a 255.255.255.0 subnet mask. See the "Network Address Table" section in this HowTo-Guide for more information.

The screenshot shows a configuration window with a dark blue sidebar on the left containing the labels "Destination Definition:" and "Service:". The main area is white and contains the following elements:

- A text input field for a destination address, currently empty, with the placeholder text "(Destination Address OR Select LAN - ANY)".
- A dropdown menu currently set to "ANY", with the tooltip text "(Destination Network / Default All LAN Addresses)".
- The text "OR" centered below the dropdown.
- A dropdown menu currently set to "--- Select Destination ---", with the tooltip text "(Select a pre-defined destination)".
- A list of pre-defined destinations: "78.12.51.2 / SINGLE HOST", "10.20.0.0 / 24", "10.50.0.0 / 24", and "LAN / LAN". The tooltip text "(Specify A Service)" is positioned to the right of this list.
- A "New Service" button with the tooltip text "(Define A New Service)".

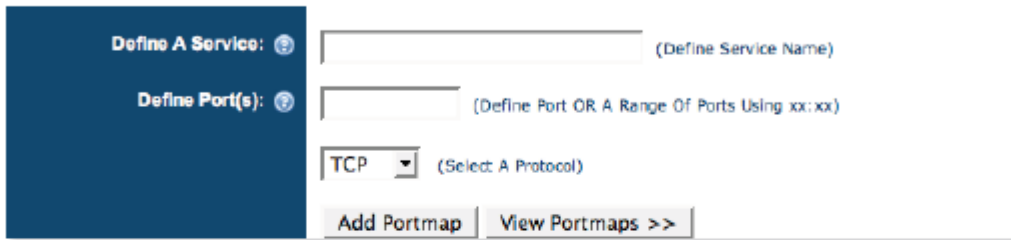
Select Or Create A New Service

Once the source and destination have been defined the next step is to determine the type of traffic to match. The default is to match ANY traffic that matches the source and destination traffic. There is a list of pre-defined traffic types, however new traffic types can easily be created clicking the "New Service" button.



New Service Creation

In order to create a new service (if needed) enter the name of the service and the port(s) used by the service. Then select the protocol to apply to the service. There are default rules created for PPTP and L2TP so generally these are not required.



Define A Service: (Define Service Name)

Define Port(s): (Define Port OR A Range Of Ports Using xx:xx)

TCP (Select A Protocol)

Select An Action

Finally, after entering the characteristics required to match a specific rule, the next step is to determine the action that should be taken when a match occurs. This action is either to ACCEPT or DROP the traffic. This action occurs immediately without any further rule testing.



Action: ACCEPT (Matched Rule Logging)

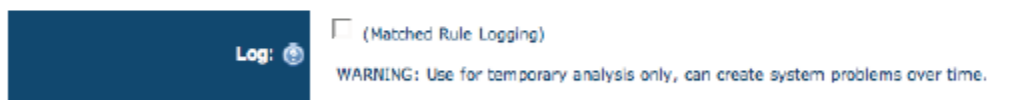
Log:

WARNING: Use for temporary analysis only, can create system problems over time.

NOTE: The DROP action is a complete dump of the packet, no response is provided. Also, when a packet matches a DROP rule, no other

Enable Logging

Selecting the logging button will cause any matched packets to be logged to the firewall logging system, see below. This allows for the viewing of traffic usage and troubleshooting of connections.



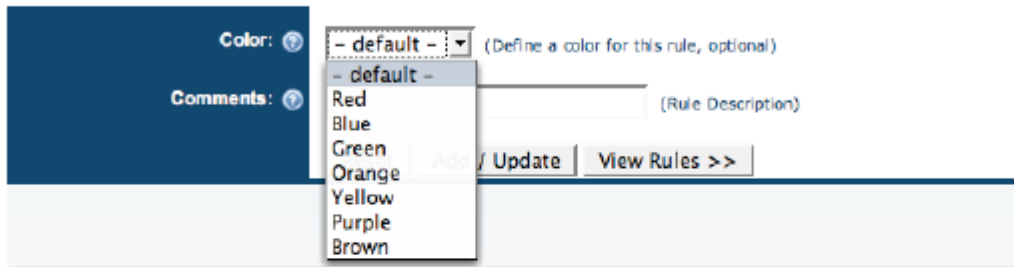
Log: (Matched Rule Logging)

WARNING: Use for temporary analysis only, can create system problems over time.

WARNING: Be very careful when enabling logging, this is similar to debugging, and can create a heavy load on the route processor and potentially slow traffic.

Color Coding

Selecting the color you wish to associate with this rule. Default colors are green for allow and red for deny.



The screenshot shows a user interface for configuring a rule. On the left, there is a dark blue sidebar with two sections: "Color:" and "Comments:", each with a circular icon containing a question mark. The "Color:" section is active, and a dropdown menu is open, displaying a list of color options: "- default -", Red, Blue, Green, Orange, Yellow, Purple, and Brown. The dropdown menu is positioned over a text input field that currently contains "- default -" and is followed by the text "(Define a color for this rule, optional)". Below the dropdown menu, there is a text input field for "(Rule Description)", a button labeled "Add / Update", and a button labeled "View Rules >>".

Rule Comments

A descriptive comment is generally helpful when a number of rules are used. The description can assist with quick editing of the rules table.



The screenshot shows a user interface for configuring a rule. On the left, there is a dark blue sidebar with a section labeled "Comments:" with a circular icon containing a question mark. To the right of the sidebar is a text input field for "(Rule Description)".

Firewall Rule Listing

When you have completed the creation of your firewall rules, you can view these rules by clicking on the "View Rules" button. This is also the default view prior to adding new rules.

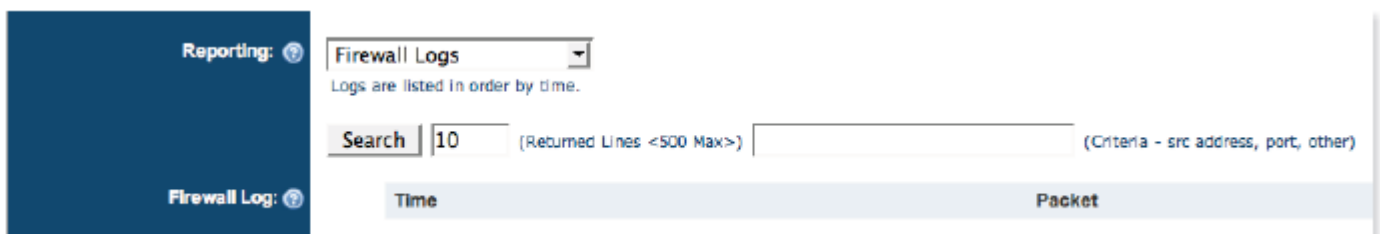
This page displays the current rule set added to the firewall by the administrator. It does not show the default rules used for administrative access to the Edge appliance, or the default ALLOW and DENY rules (see the Firewall Rule Creation section for more information on the default rules).



Select	Group	Inbound	Src Net	Dst Net	Service	Action	Log	Comments
<input type="checkbox"/>	1-BlockPorts	LAN	ANY	ANY	BitTorrent	DROP	Off	
<input type="checkbox"/>	AAA-Log	WANx	ANY	ANY	DNS	ACCEPT	On	Log DNS DDoS
<input type="checkbox"/>	Accounting	LAN	10.100.30.5	78.12.51.2	WebSSL	ACCEPT	Off	Payroll Server
<input type="checkbox"/>	Deny-Accounting	LAN	ANY	ANY	ANY ANY	DROP	Off	

Firewall Logging

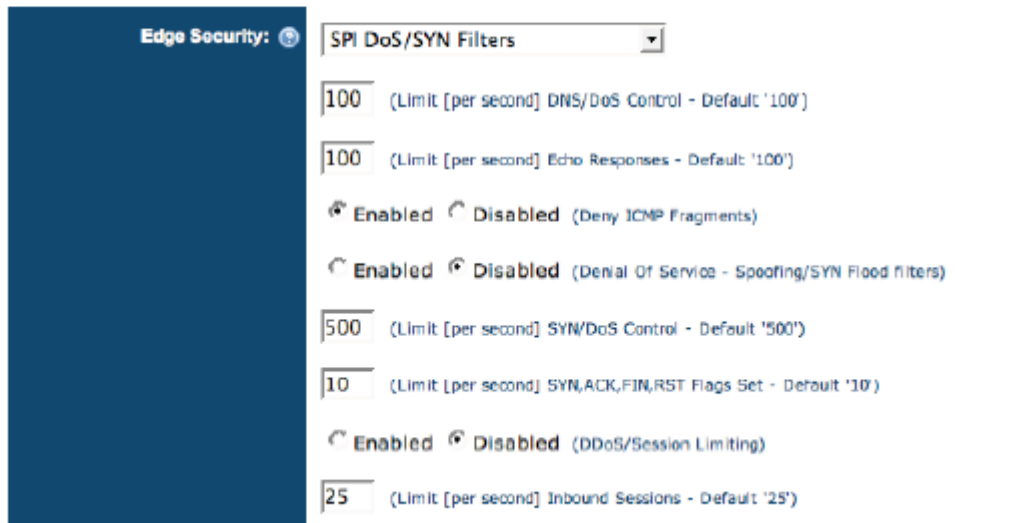
All firewall logging is now located under the reporting tab. When logging is enabled, all packets which match the firewall rule will be logged here. The output here displays the actual header information captured from packets that match the log rules (see the Firewall Rule Creation -> Enable Logging section for more information).



Time	Packet
------	--------

DoS Protection

DoS (Denial of Service) is a technique used by some hackers to attempt to block connectivity to and from a network. The Edge appliance provides protection against this type of attack by limiting the number of packets allowed that match certain characteristics generally found in these types of attacks.



DoS Rules

- DNS/DoS controls how many DNS requests are allowed per second. These are inbound requests to the Edge appliance.
- Echo Responses controls how many ICMP responses are allowed per second. There are inbound requests to the Edge appliance.
- Deny IP Fragments: When enabled will block IP packets that have been broken up in an attempt to fool the firewall and allow certain types of network connections.
- DoS SYN Flood: When enabled all inbound SYN requests are monitored. If the limit is met it will block requests until the level of requests falls below the set limits.

DDoS Session Limiting

- When enabled new inbound sessions are blocked when requests exceed the given limit. DDoS filtering is based on a per device basis so it provide very good distributed denial of service attack control.

Site2Site Client Termination

If you have remote users that wish to access the local network from their home or on the road, the Site2Site software client enables any Windows-compatible computer to connect back to the EdgeXOS appliance.

The client is small and installs in seconds. The configuration is simple and only requires the IP address of the EdgeXOS appliance (two can be provided for failover) and the port which is being used for client connections. This information can be obtained by the EdgeXOS administrator. Additional step-by-step installation instructions for the client are provided in our Platform Notes section. The client includes 3DES encryption protection using standard SSL tunneling technology, which is an improvement over IPSec based VPNs as they do not have any issues going through hotel firewalls, etc.

To get started simply download the client from the link on the configuration page.

Edge Security: ? Site2Site Client Termination ▼

Download the latest Site2Site client from here: [Site2Site Client Download](#)

Enabled Disabled (Enables Site2Site Client Termination)

Enabled Disabled (Direct Client-to-Client Communications)

Enabled Disabled (Force Default Gateway)

. . .0 Site2Site Client Network (Examples: 192.168.1.0 or 10.10.0.0)

Site2Site Clients: ? Server Port (Default XRLogin Port 1104)

(Enter the network and port to be used by Site2Site server)

(DNS Address - Optional)

(Secondary DNS Address - Optional)

(WINS Address - Optional)

[Manage User via Firewall->User/Device Management](#)

Site2Site Configuration Details

In order for a remote client to connect they must first be defined within the User/Device Management tool. This tool includes an authentication field which is used as the remote users password.

If “client-to-client” communication is enabled then two remote users will be able to share network information and potentially connect to each others shared resources.

If the “force default gateway” option is used, then all of the remote users traffic will go through the EdgeXOS appliance, i.e. the user will not be able to surf the Internet locally.

When defining the client network make sure that it is not part of any local network, including the local LAN IP addresses, this network **MUST** be separate from any other networks used by the EdgeXOS appliance.

The EdgeXOS administrator can use any port they wish for client connections, however keep in mind that many ISPs will block high ports so it is typically recommended to use ports under 1200.

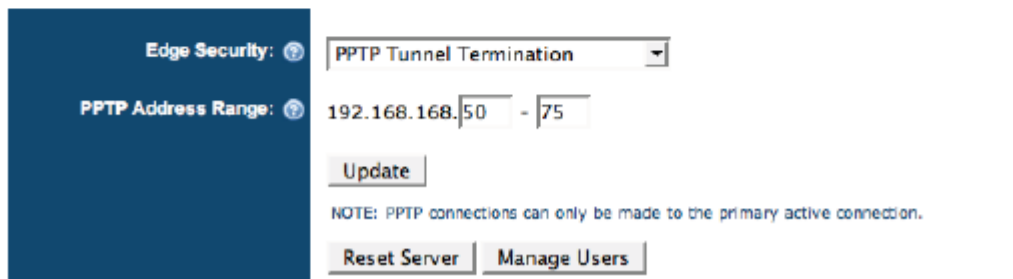
Finally, if you have local resources which should be passed to the remote clients they can be passed using the DNS and WINS fields.

PPTP Setup

This point-to-point VPN (virtual private network) module was developed to terminate remote end-users, teleworkers. It is built-in to all new Microsoft operating systems and is thus easy to configure, inexpensive, and easy to use.

Please reference the PPTP HowToGuide for full instructions on setting up a PPTP connection.

Configuration on the appliance requires the setup of an IP range for these remote users, and the setup of user accounts under the User Management section under the Shaping tab (see the Shaping HowToGuide for details on setting up user accounts).



The screenshot displays a configuration panel for PPTP. On the left, a dark blue sidebar contains two sections: 'Edge Security' and 'PPTP Address Range', each with a help icon. The main area is white and contains a dropdown menu set to 'PPTP Tunnel Termination'. Below this is an IP address range field showing '192.168.168.50 - 75'. An 'Update' button is positioned below the range field. A note states: 'NOTE: PPTP connections can only be made to the primary active connection.' At the bottom, there are two buttons: 'Reset Server' and 'Manage Users'.

Edge Security: ?	PPTP Tunnel Termination
PPTP Address Range: ?	192.168.168.50 - 75
	Update
	NOTE: PPTP connections can only be made to the primary active connection.
	Reset Server Manage Users

Advanced Spyware & Web Filtering

The EdgeXOS appliance can be used as a complete Web Threat Protection appliance by simply enabling the advanced spyware and web filtering module. This module does require additional licensing however when enabled it provides some of the most advanced Internet protection in the industry, including zero hour spyware and virus filtering. Real-time URL and web filtering with built-in phishing protection. Detailed usage reporting, including allowed and denied sites, top sites accessed and many others. With per user licensing network administrators can create different user groups which can have different privileges based on their group definition.

The screenshot shows a configuration page for 'Advanced Spyware & Web Content Filtering'. On the left, there is a dark blue sidebar with 'Edge Security: ?' and 'Threat Protection: ?' labels. The main content area has a dropdown menu set to 'Advanced Spyware & Web Content Filtering'. Below this, there are three radio button options, all with 'Disabled' selected: 'Enabled Disabled (Activate web threat protection engine)', 'Enabled Disabled (Engine Accelerator - Note: Some sites could have problems)', and 'Enabled Disabled (Secure HTTPS traffic)'. A link '(Click here to activate your account.)' is provided. There are three input fields: the first is for '(Enter the provided Webroot server URL)', the second for '(Enter the registered license key)', and the third for '(Enter the registered passcode)'. A 'START SERVICE MANAGER' button with a gear icon is present, with a note '(Click here to start managing this service)'. An 'Update' button is at the bottom. The 'Technology Partner:' section features the Webroot logo, which consists of a purple key icon inside a circle followed by the word 'webroot' in purple lowercase letters.

To enable this feature simply click the link to active the spyware account, additional licensing may be required.

Once activated and enabled, simply use the “SERVICE MANAGER” to control website access and view usage information in real-time. This service establishes a real-time connection to our partners portal for instant site updates and real-time spyware and virus filtering thus the service manager is used to control that functionality.

The acceleration engine provides for faster web downloads and optimizes the web threat protection to enhance the end-user experience.

For more information please review the Platform Notes for the Spyware & Web Filtering module.

Basic Web Domain & URL Filtering

This module provides global domain and URL filtering and is included with the purchase of our annual platform maintenance agreement. This module cannot be used in conjunction with the Spyware & Web Filtering module. To get started simply click on the “activate your account” link to obtain the account ID and login information.

The screenshot shows a configuration page for "Basic Web Domain & URL Filtering" under the "Edge Security" section. The page includes several radio button options for enabling or disabling features, a dropdown menu for clearing cache frequency, a text input for a filter redirect site, and three text inputs for Netsweeper account details. At the bottom, there is a "START SERVICE MANAGER" button and four action buttons: "Update", "Flush Cache", "Rules Database", and "User Bypass".

Edge Security: [?](#)

Basic Web Domain & URL Filtering [v](#)

Enabled Disabled (Activate web content filtering engine)

Enabled Disabled (Enable Netsweeper site lookup and caching)

Enabled Disabled (Dedicate memory for web filtering)

Allowed Denied (Default rule setting) [v](#) (How often to clear domains in cache)

http:// (Filter Redirect Site)
Default: siteblock.xroadsnetworks.com

[\(Click here to activate your account.\)](#)

(Enter the provided Netsweeper server URL)

(Enter the Netsweeper ACCOUNT identifier)

(Enter the Netsweeper LOGIN / PASSWORD)

START SERVICE MANAGER (Click here to start managing this service)

Netsweeper Filtering: [?](#)

This service provides real-time URL filtering by connecting to our partners portal and obtaining instant allow and deny status based on the URL requested. The redirect site is can be customized to point to any domain the EdgeXOS administrator selects, example: www.google.com, etc. The default is our own siteblock.xroadsnetworks.com web page which provides a simple default block page.

The “SERVICE MANAGER” can be used to view real-time usage statistics and configure specific URL categories be allowed or denied. This functionality is similar to the Spyware & Web Filtering module except that “basic” filtering does not include spyware or virus filtering and does not provide per user control.

The filtering engine works in three stages, the first stage checks the local “Rules Database”. This database is controlled by the EdgeXOS administrator and can be used to quickly block specific sites. The second stage checks the local URL cache to determine if the site has been checked recently, if it has been then the cached response will be provided up until the defined cache clearing time has been met for that specific domain (the default is five days). The third stage is performed if the first two do not match any domains, this third stage makes an automated scan of the website to determine if the site should be allowed or blocked based on the defined categories using the service manager. If it is determined that the site should be blocked it will be blocked immediately.

It is important to note that sites which have no status i.e. it has not yet been checked or are not in the URL cache, and which should be blocked, may be initially allowed when the first request to the site is made. This is because the site is being scanned and that scan may take several moments. For this reason, there is an option to allow or deny all sites by default. For organizations where end-users should only go to a small number of sites, the deny default may be the best option; the default is to allow by default and simply log the traffic. All site requests, whether allowed or denied are logged.

Please review the Platform Notes for more details on the Netsweeper portal controls.

Email Defense & Spam Filtering

The EdgeXOS can also perform spam filtering services by leveraging our partners real-time spam filtering portal. This service provides for granular spam filtering not available through other spam filtering solutions, including zero hour virus scanning, and detailed email reporting.

The process for setting up the spam filtering is simple, just click the “activate your account” link, this will require additional per mailbox licensing. If the mail server is located on the LAN side of the EdgeXOS appliance, it will automatically scan email for spam, however if the mail server is located offsite, then a modification to the customers MX rules will be necessary. The XRoads Network support team can assist with this configuration in either scenario.

To configure the spam filtering rules click on the “SERVICE MANAGER” to open access to our partners portal. Through this portal all real-time spam controls can be accessed. These are the settings which are used for all mail either going through the EdgeXOS appliance or being redirected by the MX records.

Please review the Platform Notes for more details on the Email Defense & Spam Filtering portal controls.

The screenshot shows a configuration page for 'Email Defense & Spam Filtering' within the 'Edge Security' section. The page includes a sidebar with 'Edge Security' and 'Email Defense' headers. The main content area features a dropdown menu set to 'Email Defense & Spam Filtering', a status section with 'Enabled' and 'Disabled' radio buttons (the 'Disabled' option is selected), and a link to activate the account. Below this are three input fields for MXLogic servers, account identifier, and password, each with a descriptive placeholder. At the bottom, there is a 'START SERVICE MANAGER' button with a gear icon and an 'Update' button.

Edge Security: ?

Email Defense: ?

Email Defense & Spam Filtering

Enabled Disabled (Activate email anti-spam & virus protection engine)

[\(Click here to activate your account.\)](#)

(Enter the provided MXLogic servers, separated by ',')

(Enter the MXLogic ACCOUNT identifier)

(Enter the MXLogic PASSWORD)

START SERVICE MANAGER (Click here to start managing this service)

Update