



XROADS NETWORKS

Network Appliance How To Guide: EdgeWALL

How To Guide

EDGE NETWORK APPLIANCE

How To Guide EdgeWALL

© XRoads Networks
17165 Von Karman • Suite 112
888-9-XROADS

Table of Contents

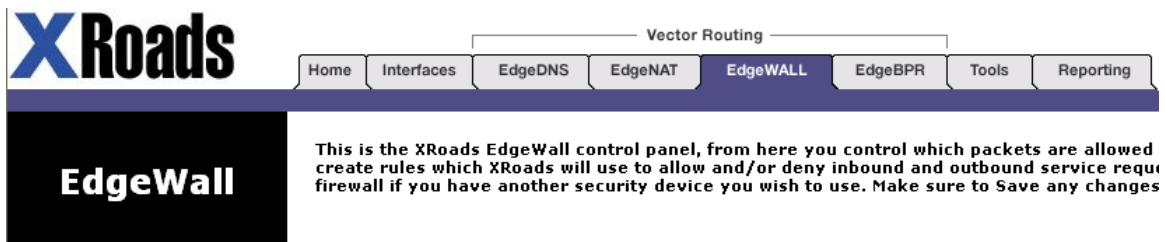
EdgeWALL Overview	3
C O M P O N E N T S	
SPI Firewall Overview	4
Firewall Rule Creation	5
Firewall Rule Listing	7
Firewall Logging	8
DoS Protection	9
Vulnerability Scanning	10
IPSEC VPN Client/Server Preview	12
Application Filtering Preview	13
Ref A: Correct Subnetting	14

Edge Configuration Series

EdgeWALL Overview

The Edge 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 EdgeWALL firewall has been certified as being compliant with ICSA standards.



EdgeWALL Menu

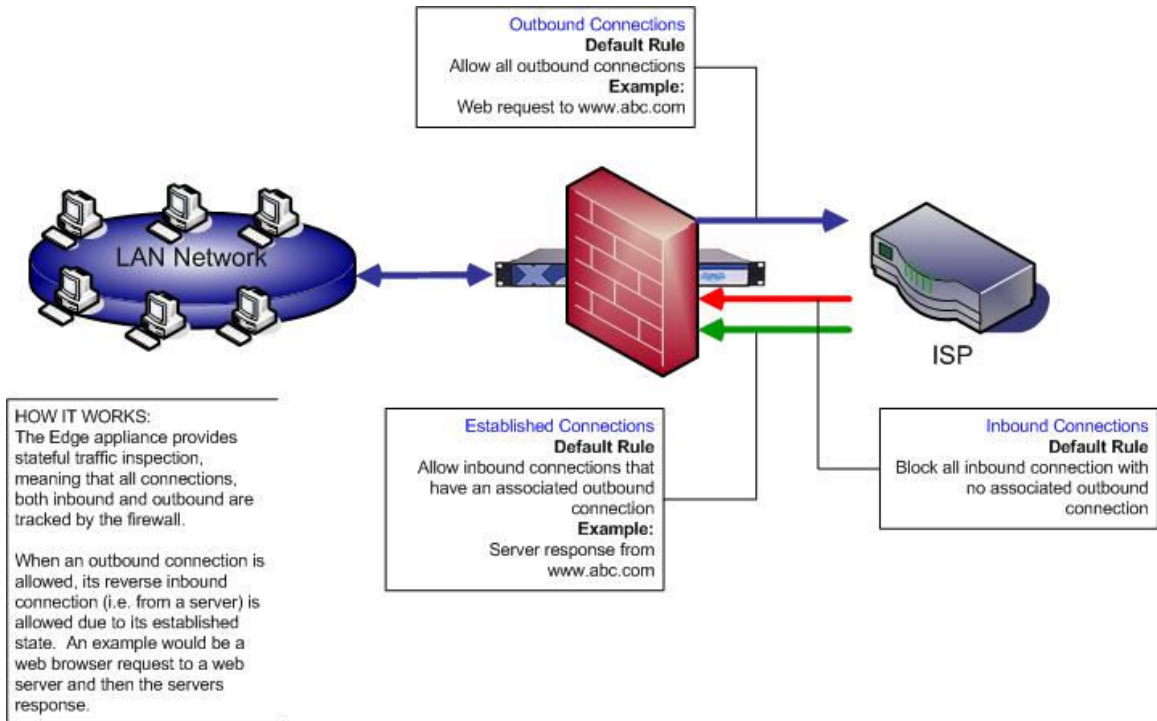
The following menu provides a quick overview of the capabilities of the EdgeWALL module and its features.



SPI Firewall Overview

The SPI (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.

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.

Edge Security: ?	SPI Firewall Rules
Group Name: ?	<input type="text" value="v"/> <- Select A Firewall Group OR Create A New One -> <input type="text"/>
Inbound Interface: ?	WAN+ <input type="text" value="v"/>
Source Definition: ?	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> (Source Address OR Select LAN - ANY) ANY <input type="text" value="v"/> (Source Network / Mask)
Destination: ?	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> (Destination Address OR Select LAN - ANY) ANY <input type="text" value="v"/> (Destination Network / Default All LAN Addresses)
Service: ?	ANY → ANY <input type="text" value="v"/> (Specify A Service) OR <input type="button" value="New Service"/> (Define A New Service)
Action: ?	ACCEPT <input type="text" value="v"/>
Log: ?	<input type="checkbox"/> (Matched Rule Logging) WARNING: Use for temporary analysis only, can create system problems over time.
	<input type="button" value="Reset"/> <input type="button" value="Add / Update"/> <input type="button" value="View Rules >>"/>

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.

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.



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


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.

NOTE: The WAN+ selection specifies all WAN interfaces.

Inbound Interface:  WAN+ 

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

ANY  (Source Network / Mask)

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 specify 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 HowToGuide for more information.

Destination:  . . . (Destination Address OR Select LAN - ANY)

ANY  (Destination Network / Default All LAN Addresses)

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.

Service: (Specify A Service)
OR
 (Define A New Service)

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)
TCP
UDP
PPTP
L2TP
ICMP

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.


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

Action:

Enable Logging

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.

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.

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	
1	<input type="radio"/>	Alpha	 ANY	ANY	 192.168.168.10/27	 TCP 80 - Web HTTP	DROP	Off
2	<input type="radio"/>	Alpha	 LAN	ANY	ANY	 TCP 50:51 - ESP/AH	DROP	Off
3	<input type="radio"/>	OtherRules	 ANY	 4.2.2.0/24	ANY	 UDP 53 - DNS	 ACCEPT	Off
4	<input type="radio"/>	Outbound	 LAN	ANY	ANY	 TCP 5190 - AOL	 ACCEPT	On
5	<input type="radio"/>	WebServers	 ANY	ANY	 192.168.168.0/27	 ANY ANY - ANY	 ACCEPT	Off

Firewall Logging

This page displays the log output produced when the Logging button is selected when creating a firewall rule. 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).

Logs are listed in order by time.

Search (Returned Lines <500 Max>) (Criteria - src address, port, other)

Time	Packet
Fri Aug 14:30:08 2	IN=lan OUT= MAC=00:90:fb:04:85:1c:00:50:ba:b0: Source Addr=192.168.168.252 Destination Addr=192.168.168.254 Length=48 TOS=0x00 ID=7947 DF Protocol=TCP Source Port=3952 Destination Port=23 SYN
Fri Aug 14:30:05 2	IN=lan OUT= MAC=00:90:fb:04:85:1c:00:50:ba:b0: Source Addr=192.168.168.252 Destination Addr=192.168.168.254 Length=48 TOS=0x00 ID=7946 DF Protocol=TCP Source Port=3952 Destination Port=23 SYN
Fri Aug 14:30:04 2	IN=lan OUT= MAC=00:90:fb:04:85:1c:00:50:ba:b0: Source Addr=192.168.168.252 Destination Addr=192.168.168.254 Length=48 TOS=0x00 ID=7945 DF Protocol=TCP Source Port=3952 Destination Port=23 SYN

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.

Edge Security: ?

SPI DoS/SYN Filters

Enabled Disabled (Deny ICMP Fragments)

(Limit [per second] Echo Responses - Default '10')

(Limit [per second] SYN Requests - Default '10')

(Limit [per second] SYN,ACK,FIN,RST Flags Set - Default '10')

DoS Rules

- Deny IP Fragments will block IP packets that have been broken up in an attempt to fool the firewall and allow certain types of network connections.
- Limits the number of ICMP packets that the firewall will allow.
- Limits the number of connection initialization requests that the firewall will allow. This may need to be increased for highly active networks.
- Limits the ability for a hacker to scan the firewall for vulnerabilities.

Vulnerability Scanning

The EdgeWALL firewall module includes the ability to perform virus detection for well-known network based viruses within the local area network. The scanner identifies network based viruses by checking the port status of nodes on the LAN.

NOTE: To receive automated email alerts when a network virus is detected, create an Alert Notification, under the Reporting tab with the appropriate alert level checked.

The screenshot shows the 'Edge Security' configuration page for 'SPI Vulnerability Scanning'. The page is divided into several sections on the left with a dark blue background and white text, each with a question mark icon:

- Edge Security:** A dropdown menu is set to 'SPI Vulnerability Scanning'.
- Scan Interval:** A dropdown menu is set to 'Once A Week'. Below it is an 'Immediate' button and an empty text input field. A note says: '(Optionally, enter a single valid address to scan)'. Below that, a note says: 'Clicking Immediate will scan either the entire LAN or the address above against all of the scan rules.'
- Add Port:** An empty text input field with a note: '(Enter the port(s) to scan, example: 80 or 80,25,22 or 25-80)'
- Protocol:** A dropdown menu is set to 'TCP' with a note: '(Select the protocol to use when scanning)'
- Description:** An empty text input field with a note: '(Enter a description for this type of scan)'

At the bottom of the configuration area are three buttons: 'Add / Update', 'View Report', and 'View Port Listing >>'.

Enabling the Scanner

The scanner is disabled by default and must be enabled to begin network scans. The scans can be performed on an hourly, daily, weekly and monthly basis.

This screenshot shows a close-up of the 'Scan Interval' configuration. On the left, a dark blue vertical bar contains the text 'Scan Interval: ?'. To the right, there are two radio buttons: 'Scanning Enabled' (which is unselected) and 'Scanning Disabled' (which is selected). A note next to the radio buttons says: '(Enabling will turn on automated LAN network scanning)'. Below the radio buttons is a dropdown menu set to 'Once A Week' with a note: '(How often to conduct LAN network scans)'.

Immediate Scan

The administrator may perform an immediate scan at any time by entering the IP address of a specific host to scan and then clicking the "Immediate" button. This will launch an immediate scan to the specified host and produce a report, which can be viewed by clicking the "View Report" button.

This screenshot shows a close-up of the 'Immediate Scan' configuration. On the left, a dark blue vertical bar is partially visible. To the right, there is an 'Immediate' button and an empty text input field. A note next to the input field says: '(Optionally, enter a single valid address to scan)'. Below the input field, a note says: 'Clicking Immediate will scan either the entire LAN or the address above against all of the scan rules.'

Create a Scan Rule

To add a specific network port to scan, simply enter the port(s) to be scanned, the protocol type (from the drop-down) and the description that should be provided when a scan has a positive response. There is no limit to the number of rules which can be created, however the more rules, the longer the scan will take to complete.

Add Port: ?	<input type="text"/>	(Enter the port(s) to scan, example: 80 or 80,25,22 or 25-80)
Protocol: ?	TCP ▼	(Select the protocol to use when scanning)
Description: ?	<input type="text"/>	(Enter a description for this type of scan)

View Scan Rules

The following list is a short example of some of the well-known viruses in the scanning database. This list can be updated manually by uploading the latest scan rules, available via the XRoads Networks website, when under an annual support contract.

NOTE: The virus definition list can be updated automatically via a central global management server (GMS) with the proper annual contract services.

Select	Description	Protocol	Port(s) To Scan
<input type="radio"/>	Potential Ripper virus detected on this host.	TCP	2023
<input type="radio"/>	Potential Sokets de Trois v1 /Bubbel virus detected on this host.	TCP	5001
<input type="radio"/>	Potential Blade Runner virus detected on this host.	TCP	5400,5401,5402
<input type="radio"/>	Potential Net Monitor virus detected on this host.	TCP	7300,7301,7306,7307,7308

IPSEC VPN Client/Server Preview

The VPN (virtual private network) module is either a built in option on the appliance purchased or can be added as a licensed feature. The VPN module allows for the setup of an IPSEC (standard IP based tunnel protocol) encrypted tunnel between two locations.

The Edge VPN is 100% compliant with other IPSEC VPN's, and has been tested with SonicWall, Netscreen, ZyXEL, Cisco, and others. Unlike many other VPN devices the Edge VPN is fully redundant, meaning that it can failover in the case of a network failure. This failover capability not only includes point-to-point failover, but also includes WAN to WAN failover.

By design, our VPN policies are extremely easy to configure. For this reason, some of the extensive features of other VPN devices have been left out in order to simplify the configuration process.

The screen below provides an overview of the tunnel configuration. For detailed configuration information, refer to the HowToGuide VPN.

The screenshot displays a configuration page for an IPSEC VPN tunnel. The interface is organized into sections on the left with a dark blue background and white text, and a white configuration area on the right. Each section includes a question mark icon for help. The configuration area contains various input fields, dropdown menus, and radio buttons. At the bottom, there are two buttons: 'Add/Update' and 'View Tunnels >>'. A small note at the very bottom states: '- RSA public and private keys will be auto-generated if 'RSA Key' is selected. -'

Edge Security:

Connection Name: (Used to define this tunnel)

Shared Secret RSA Key (Select VPN key type)

3DES / MD-5 3DES / SHA-1 (Select encryption and algorithm type)

Shared Secret Key:
(When using 'Shared Secret' enter a key value here, or leave blank to auto-generate)
NOTE: This key must match the remote tunnel definition.

Dynamic Tunnel: Disable Enable Remote ID (When using clients which do not have static IP addresses)

VPN Interface: (Select the outbound interface)

Tunnel Local Network: . . . (Enter the LAN network to tunnel)
 (Local network mask)

Remote VPN Device: . . . (Enter the WAN address of the remote device)

Remote VPN Network: . . . (Enter the network address of the remote network)
 (Remote VPN network mask)

Remote Probe Address: . . . (This is the remote devices LAN address, it is used for the VPN heartbeat)

Failover VPN: (Used to define the failover VPN tunnel, defaults to the Connection Name above)

VPN Hub/Client: Client Side Hub Side (Select the VPN tunnel type)

- RSA public and private keys will be auto-generated if 'RSA Key' is selected. -

Application Filtering Preview

The Application Filtering module is either a built in option on the appliance purchased or can be added as a licensed feature. The functionality of the Application Filtering is to filter and/or block unwanted content from being accessed by internal users.

The content which can be blocked includes, P2P, Chat, Instant Messaging, Spyware, File Download services, and various other web sites and multi-media applications.

The filtering works by intercepting DNS requests made by internal clients and providing either the appropriate response, or based on the filtering rules, respond with a local host address which essentially blocks the application/web browser from being able to access the selected content.

There are various controls which can be placed on the Application Filtering feature, including the ability to match a device to an actual user name, or setting up a by-pass list for the filter.

The screen below provides an overview of the initial Application Filtering setup. For detailed configuration information, refer to the HowToGuide Application Filtering.

The screenshot shows a configuration interface for Application Filtering. On the left is a dark blue sidebar with three sections: 'Edge Security: ?' (with a question mark icon), 'Application Filtering: ?' (with a question mark icon), and 'Categories: ?' (with a question mark icon). The main content area is white and contains the following elements:

- A dropdown menu labeled 'Application Filtering Control' with a downward arrow.
- Two radio buttons: 'Enabled' (selected) and 'Disabled', followed by a link '(Application Filtering Services)'.
- A text input field containing 'http://www.google.com' with a blue link '(Filter Redirect Site - default 127.0.0.1)' to its right. Below the input is the text 'Example: www.abc.com'.
- A heading '(Check to enable the various filtering/throttling categories)'.
- A grid of 15 checkboxes arranged in 5 rows and 3 columns:
 - Row 1: Adult, News, Chat (throttle)
 - Row 2: Illegal/Vice, Pornography, P2P (throttle)
 - Row 3: Forums/Blogs, Search Engines, General (throttle)
 - Row 4: Entertainment, Webmail, Games (throttle)
 - Row 5: Job Search, Downloads, MultiMedia (throttle)
- At the bottom, two buttons: 'Update' and 'View Latest DNS Requests'.

Reference A: Correct Subnetting

Subnetting is the act of taking a larger network and breaking it down into smaller networks. Example: Taking a full Class C network 255.255.255.0 (/24, slash 24), and breaking it down into four separate networks. Each subnet'd network would consist of 64 addresses and have a 255.255.255.192 subnet mask (/26, slash 26). The first network would be xxx.xxx.xxx.0-xxx.xxx.xxx.64, the next would be xxx.xxx.xxx.65-xxx.xxx.xxx.128, etc, etc.

WARNING: Assigning the correct subnet with an IP address is 100% necessary in order for the interface to properly communicate with the rest of the network. An incorrect subnet is the fastest way to produce strange and hard to identify (except by looking at the subnet mask) problems.

The method used by engineers to figure out a subnet mask involves using network address bits to determine the correct masked bits. The masked bits are used by the network device to determine what range its interface can communicate, and when it can not, to forward all requests to the default gateway.

To avoid having to learn the somewhat complicated and often time consuming method for converting decimal to binary and back again, use the following table as a quick reference for all of your subnetting needs.

Quick Subnetting Reference Guide			
Subnet	Slash Notation	Available Addresses	Usable Addresses
255.255.255.0	/24	256	254
255.255.255.128	/25	128	126
255.255.255.192	/26	64	62
255.255.255.224	/27	32	30
255.255.255.240	/28	16	14
255.255.255.248	/29	8	6
255.255.255.252	/30	4	2