1.0 Document Purpose

This User Guide is designed to assist customers using the Nuvox FireWall service to access and use the various administration, configuration and reporting capabilities of their FireWall using the MyFireWall Portal.

2.0 NuVox Firewall Overview

The Nuvox Firewall service is designed to assist customers in protecting their network-based resources. Based on technologies from Cisco, the world's leader of networking equipment and top provider of security solutions, the Nuvox Firewall can be a key component to any company's overall security strategy. Configured according to the customer's desired Security Policy, the Firewall provides packet filtering features for blocking malicious traffic from entering the customer's network from the Internet. And, at the same time, necessary communication is allowed from inside the network so employee's can continue to get their job done - uninterrupted and securely.

In addition to providing numerous security features, reporting features are available for each Firewall customer through their own individual Web Portal.

The NuVox Firewall basic services include the following features:

- Customized packet filtering
- Stateful packet inspection
- Network address translation
- Internal network services
- Basic & enhanced reporting
- MyFireWall administration portal

Additional enhanced services, such as intrusion detection and web browsing filtering, can be purchased for each FireWall installation based on the customer's own unique needs.

Customized packet filtering
The FireWall implements packet filtering abilities to help protect the customer's network as defined by the customer's unique FireWall Security Policy. By default, all traffic that originates from the Internet is prohibited from entering the customer's internal network. At the same time, all traffic originating from inside the network is allowed out to the Internet (except for any exceptions as noted by the customer's FireWall Security Policy). By default, the customer's FireWall Security Policy blocks any traffic associated with Windows NetBIOS traffic from leaving the local network.

Stateful packet inspection
Providing "stateful" packet inspection capabilities allow for the NuVox FireWall to "keep track" of each network session that starts from within the customer's internal network, ensuring that not only is the connection allowed out to the Internet, but that also the reply is allowed back in.

Other stateful packet inspection features include the ability of the FireWall to defend against Denial-of-Service (DoS) attacks such as "SYN floods" where an attacker may attempt to overwhelm a network, or individual system, by sending a tremendous amount of specific packets at one time.

Network address translation
Using 'network address translation' (NAT) can be seen as providing an additional 'virtual' layer of protection for customer networks by using the FireWall service to further segregate the internal network from the Internet. With NAT, computers within the client's network can use 'private' IP addresses – these addresses are not directly accessible by the Internet, effectively hiding all of the customers' internal hosts from Internet-based attackers.

If a customer does have an internal system such as a mail or web server that needs to be directly accessible from the Internet, specific NAT rules can be written to allow the required traffic, and only the required traffic, to pass through the FireWall.

Internal network services
Not only can the FireWall help protect a customer's network, but it can also be used to provide basic network infrastructure services such as DHCP (Dynamic Host Configuration Protocol) to internal computers. In this case, the NuVox FireWall could be configured to act as a DHCP server, offloading DHCP administration responsibilities from the customer. The FireWall operating as a DHCP server could also be leveraged to provide business continuity through its configuration as a second source of DHCP addresses for internal systems.

Basic & enhanced reporting features
Basic "built-in" reports are available for each FireWall customer to monitor various aspects of their network activity, such as the top Internet destinations for internal users.

MyFireWall administration portal
To be able to make changes to their own FireWall configuration, customers can make changes through their MyFireWall web portal. This collection of dynamic web pages allows for the customer to not only makes changes to their Security Policy, but also allows users to run and view reports for their own FireWall.

3.0 FireWall Security Policy

Each customer's unique FireWall configuration is stored in their own FireWall Security Policy. Configured based on the individual needs of each customer, the FireWall Security Policy includes specific settings which control the following:

- Port Filtering
- Address Translations
- Website Filtering (if purchased)

**** NOTE ** Currently, to make changes to your Firewall's Security Policy, you must contact the Nuvox Customer Repair Center at (800) 600-5050. In the near future, customers will be able to make their own changes to their Firewall Security Policy through their customized MyFireWall web portal.**

Port Filtering
Port filtering is used by each FireWall to block Internet-based traffic from entering the customer's internal network, while allowing all communication from inside the customer network out to the Internet. The only exception to this rule is that Windows NetBIOS ports are blocked from leaving the internal network for security purposes.

Address Translations
If an internal system needs to be accessible from the Internet, a network address translation rule can be created to allow for the required connectivity. For example, if the customer hosts their own mail server on their internal network, a special NAT rule must be written to allow Internet-based traffic to pass through to the mail server on the specific port, or 'channel', associated with Email traffic.

Website Filtering
If the Website Filtering service has been purchased, customers will be allowed to configure their website filtering options through the web portal. Based on technologies from Websense, the leading provider in web content filtering software, the FireWall has the ability to block a wide-range of website categories which include sites that may contain questionable or illegal material.

For example, customers may choose to block potentially harmful categories such as 'Adult Material' or 'Hacking' or want to block websites associated with employee productivity issues such as 'Games' or 'Job Search'.

Access a complete list of Websense categories at http://www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php.

4.0 Using the MyFireWall Portal

The MyFireWall portal allows FireWall customers to access various aspects of their FireWall installation. The customer's own unique portal can be used to configure various aspects of the FireWall's features while also providing customers with the ability to view reports on their network activity.

Accessing the NuVox Customer Portal

To access your own customized Web Portal for your company, login with your web browser at http://my.nuvox.net. Numerous account management tools are available through the Customer Portal page, including the ability to sign up for online billing and open trouble tickets for assistance you with all of your NuVox services.

For more information on using the NuVox Customer Portal, consult the 'MyNuVox Portal User Guide' at http://my.nuvox.net/files/mynuvox_portal_userguide.pdf.

Accessing FireWall Features through the NuVox Customer Portal

Once logged in to your company's web portal, you can access your Firewall's feature-set by using the "My NuVox Navigator" tool which appears as a drop-down menu in the upper right-hand corner of the screen (Figure 4.1).

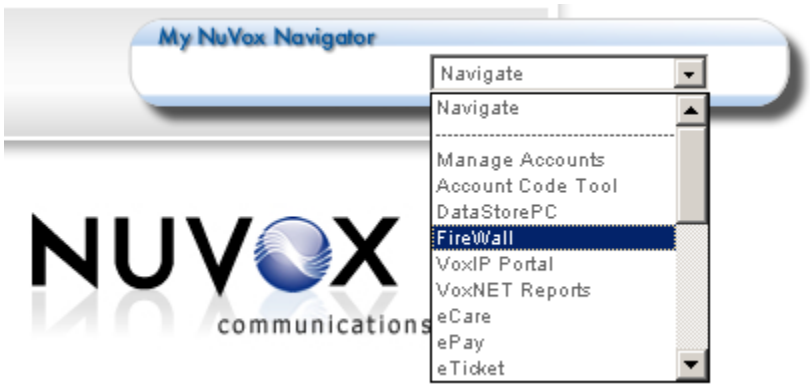

Figure 4.1 My NuVox Navigator

To access your Firewall features, click on the My NuVox Navigator drop-down menu and select **'Firewall'**. You should now be brought to the **'MyFireWall'** section of your web portal (Figure 4.2).

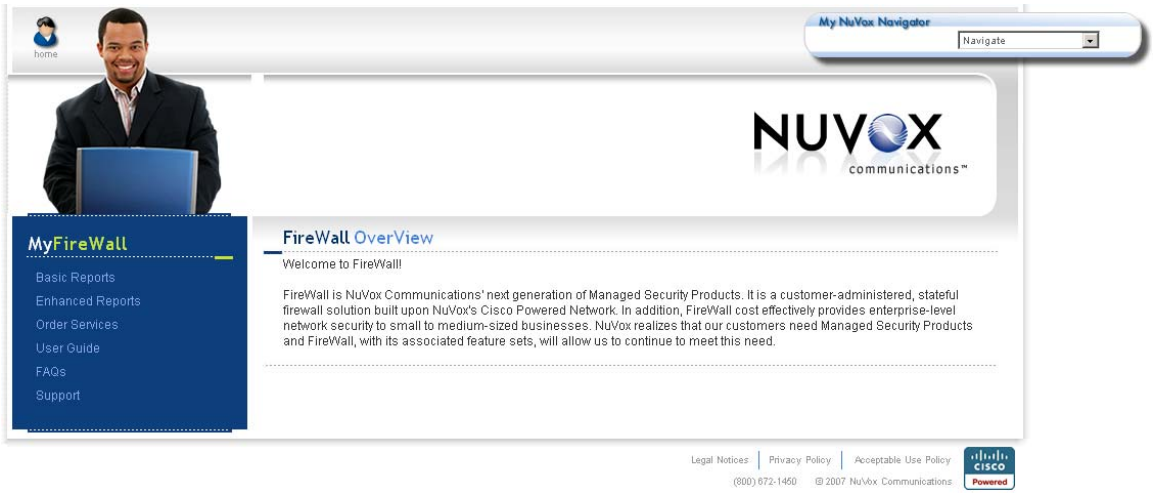

Figure 4.2 MyFireWall Web Portal

From the MyFireWall page, you can currently view Basic Reports associated with your FireWall service and order additional services. Enhanced Reports are also available for customers that have purchased the additional features with enhanced reporting capabilities, such as Intrusion Detection or Website Filtering.

5.0 Basic Reports

Each Nuvox FireWall includes the ability for customers to view a set of reports, known as 'Basic Reports', used to view various activity and security aspects of their Internet connectivity. Each report can be generated by 'Last 7 Days', 'Last 30 Days' and 'Last Calendar Month'.

Accessing Basic Reports

1. To access these reports, click on the **'Basic Reports'** link underneath the **'MyFireWall'** heading.

Running Basic Reports

To run a Basic Report:

2. Select the report you wish to view by title.

In this example, we will select **'Total Bandwidth Usage'**.

3. Choose the time period on which you wish to report on.

In this example, we will select **'Last 7 Days'**.

4. As your report data is generated, a swirling icon will be displayed next to the **'MyFireWall'** heading.

Once your report has been generated, you should see the data displayed in a table such as seen in Figure 5.1 below.

Total Bandwidth Usage

The Total Bandwidth Usage Report measures your bandwidth utilization over the course of the reporting period for the following areas:

- Web Traffic
- Mail Traffic
- FTP Traffic
- DNS Traffic
- Telnet Traffic
- Other Traffic

This report can give you a quick look at where your bandwidth is being used.

Visual Graph of Report

PROTOCOL	USAGE	% OF USAGE
DNS	1505526	0.33
Web	359432298	79.68
FTP	2844	0
Telnet	0	0
Mail	66640309	14.77
Other	23511991	5.21

Figure 5.1 Sample Usage Report – Total Bandwidth Usage by 'Last 7 days'

If you'd like to view a graph of the available data, click on the **'Visual Graph of Report'** link just above the table. Once selected, a graphical representation of your network data will be displayed as seen in Figure 5.2.

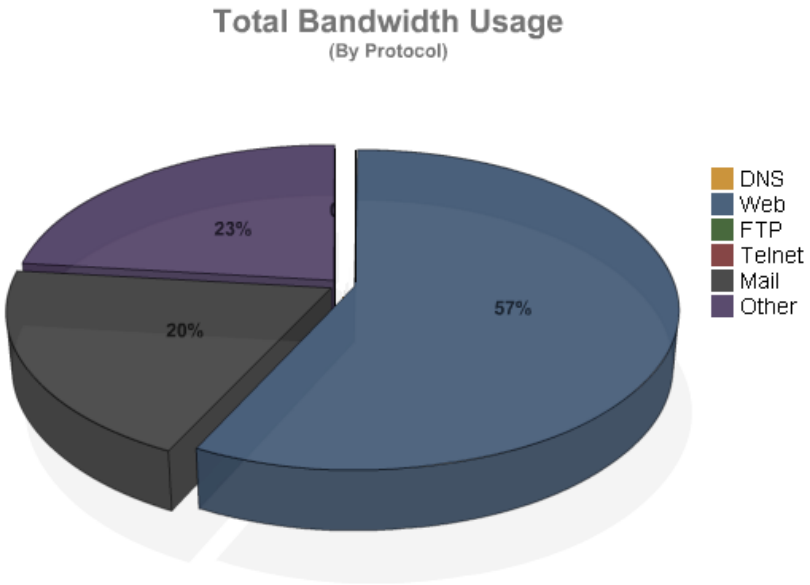

Figure 5.2 Sample Graphical Report – Total Bandwidth Usage (By Protocol)

Available Basic Reports
The following are Basic Reports available for each Firewall customer:

Total Bandwidth Usage
This report displays the amount of network traffic, or bandwidth, sorted by the following protocols:
- Web Traffic (web browsing traffic)
- Mail Traffic (Email traffic)
- FTP Traffic (file transfer traffic using FTP)
- DNS Traffic (name resolution traffic)
- Telnet Traffic (Telnet traffic for remote management of devices)
- Other Traffic

Top 10 Mail Servers
This report sorts the top 10 destinations for Email traffic from your network.

Top 10 Websites
This report lists the top 10 destinations for web browsing by users on your network.

Top 10 Users
This report shows the top 10 users based on the amount of Internet usage (by bandwidth).

Top 10 Users - Destinations
This report further shows the top 10 users based on the amount of their Internet usage (by bytes transferred), along with further details on their "most visited" destinations on the Internet.

6.0 Enhanced Reports

With each additional add-on product to the Firewall service (such as Website Filtering or Intrusion Detection capabilities), Enhanced Reports are available for customers with these extra features enabled. Following is a list of some of the Enhanced Reports that are available for the NuVox FireWall:

Top Attacks
This report lists the Top 10 Attacks attempted against the FireWall that were blocked.

Top 10 Attacked Hosts

This report lists the Top 10 hosts on the customer's network that were attacked from the Internet.

Top External Attackers
This report lists the Top 10 hosts detected as launching attacks against the FireWall's protected network.

Top Blocked Category Attempts
This report lists the Top 10 blocked sites that internal users are attempting to access.

7.0 Additional Assistance

For additional help with your NuVox FireWall service, please contact the Nuvox Customer Repair Center at (800) 600-5050.