the set of Firewall rules to determine whether the request should be allowed to pass through the Firewall. If the request is permitted to pass, then all subsequent data associated with this request (a "session") will also be allowed to pass, regardless of its direction.

For example, when you point your Web browser to a Web page on the Internet a request is sent out to the Internet for this page. When the request reaches the CAP the Firewall will identify the request type and origin—HTTP and a specific PC in your enterprise network, in this case. Unless you have configured access control to block requests of this type from this computer the Firewall will allow this request to pass out onto the Internet. When the Web page is returned from the Web server the Firewall will associate it with this session and allow it to pass, regardless of whether HTTP access from the Internet to the enterprise network is blocked or permitted.

The important thing to note here is that it is the ***origin of the request***, not subsequent responses to this request, that determines whether a session can be established or not.

You may choose from among three pre-defined security levels for the CAP: Minimum, Typical, and Maximum (the default setting). The table below summarizes the behavior of the CAP for each of the three security levels.

Security Level	**Requests Originating In the WAN**	**Requests originating in the LAN**
Maximum (Default)	***Blocked*:** No access to enterprise network from Internet, except as configured in the Local Servers, DMZ host and Remote Access screens	***Limited*:** Only commonly-used services, such as Web-browsing and e-mail, are permitted †
Typical	***Blocked*:** No access to the enterprise Network from the Internet, except As configured in the Local servers, DMZ host and Remote Access screens	***Unrestricted*:** All services are permitted, except as configured in the Access Control screen
Minimum	***Unrestricted*:** Permits full access from Internet to enterprise Network; all connection attempts permitted.	***Unrestricted*:** All services are permitted, except as configured in the Access Control screen

† These services include Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

Attention: Some applications (such as some Internet messengers and Peer-To-Peer client applications) tend to use these ports, if they can not connect with their own default ports. When applying this behavior, those applications will not be blocked outbound, even at Maximum

5.1.1 Configuring the Firewall Security Level

To configure the CAP’s security settings:

1. Choose from among the three pre-defined security levels described in the table above. *Typical Security* is the default setting.

2. Check the ’Block IP Fragments’ box in order to protect your enterprise network from a common type of hacker attack that could make use of fragmented data packets to sabotage your enterprise network. Note that VPN over IPSec and some UDP-based services make legitimate use of IP fragments. You will need to allow IP fragments to pass into the enterprise network in order to make use of these select services.

3. Click the ‘Apply’ button to save your changes.

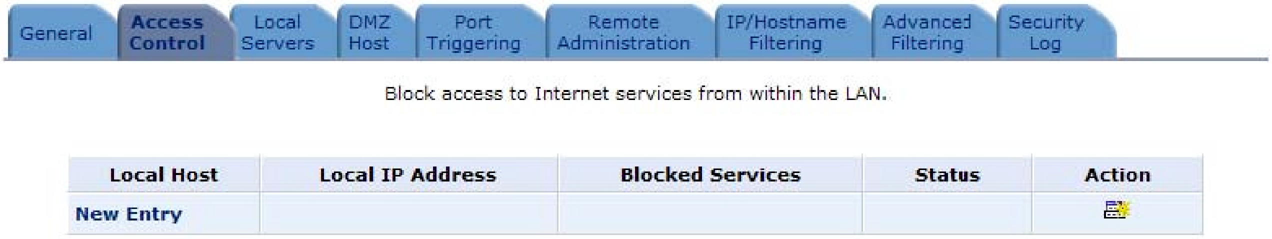
> Using the *Minimum Security* setting may expose the home network to significant security risks, and thus should only be used, when necessary, for short periods of time.

5.2 Adding Access Controls

You may want to block specific computers within the local enterprise network (or even the whole network) from accessing certain services on the Internet. For example, you may want to prohibit one computer from surfing the Web, another computer from transferring files using FTP, and the whole network from receiving incoming e-mail.

Access Controls work by placing restrictions on the types of requests that may pass from the enterprise network out to the Internet, and thus may block traffic flowing in both directions. In the e-mail example given above, you may prevent computers in the enterprise network from receiving *incoming* e-mail by blocking their *outgoing* requests to POP3 servers on the Internet.

Click the ’Access Control’ button to view a list of services that have been restricted.



Block access to Internet services from within the LAN.

Local Host	Local IP Address	Blocked Services	Status	Action
New Entry				✎

To add a new service or services to the Access Control table:

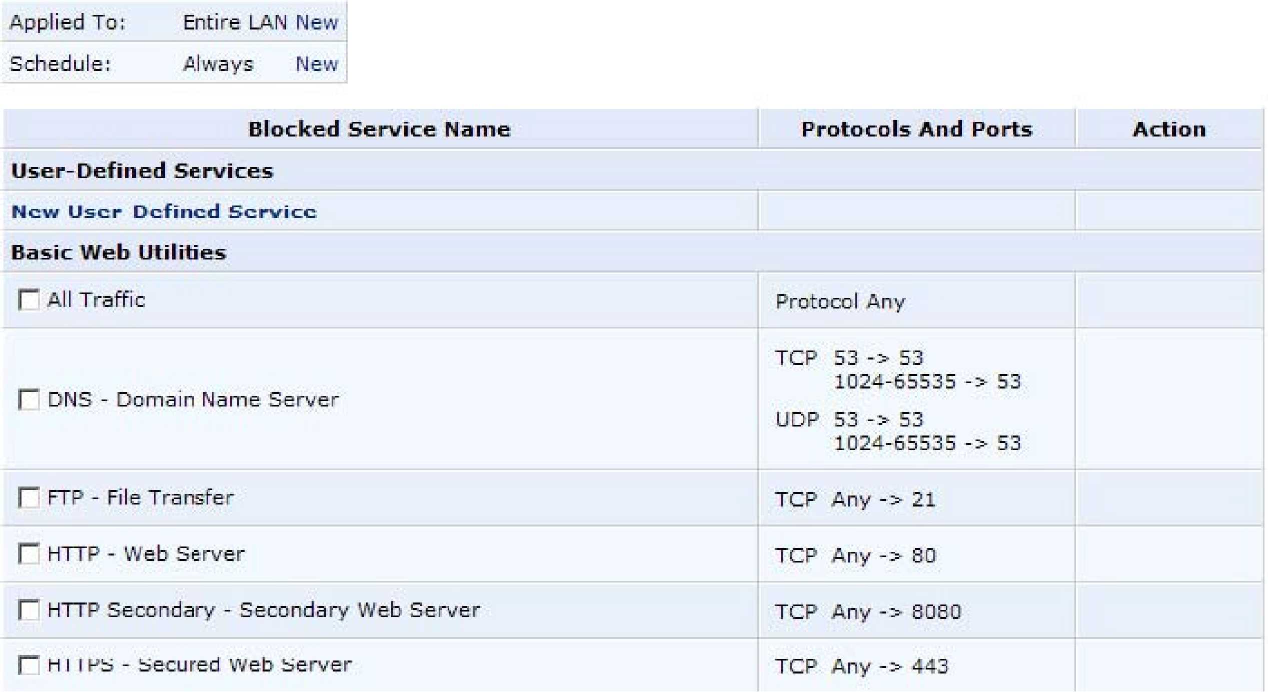
- Click the ’New Entry’ button. The ’Add Access Control Rule’ screen will appear.

- Select the service or services that you would like to block.

- Select the group of computers to which you would like to apply the access control rule. You can either select from a pre-defined list of groups by selecting one from the ’Applied To’ combo box, or create a new group by pressing the ’New’ link. To learn how to create groups to which you can apply rules, see the section 7.5 on ‘Network Objects’.

- Define the time period during which the access control rule will take effect. You can either select from a pre-defined list of schedules by selecting one from the ’Schedule’ combo box, or create a new schedule by pressing the ’New’ link. To learn how to create a new time schedule, see section 7.10.

- Click the ’OK’ button to save your changes and return to the ’Access Control’ screen.



Applied To:	Entire LAN	New
Schedule:	Always	New

Blocked Service Name	Protocols And Ports	Action
User-Defined Services		
New User Defined Service		
Basic Web Utilities		
☐ All Traffic	Protocol Any	
☐ DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
☐ FTP - File Transfer	TCP Any -> 21	
☐ HTTP - Web Server	TCP Any -> 80	
☐ HTTP Secondary - Secondary Web Server	TCP Any -> 8080	
☐ HTTPS - Secured Web Server	TCP Any -> 443	

You can **edit/change** the computer(s) prohibited from accessing a particular service by modifying the appropriate entry in the Access Control table.

To modify an entry in the Access Control table:

- Click the **Edit** button for the service. The ’Edit Service’ screen will appear.
- Select the network group to which you would like to apply the rule, and the schedule during which the rule will take effect.
- 3. Click the ’OK’ button to save your changes and return to the ’Access Control’ screen.

You can **disable an access control** and make the service available without having to remove the service from the Access Control table. This may be useful if you wish to make the service available only temporarily and expect that you will want to reinstate the restriction in the future.

To temporarily disable an access control

- Clear the check box next to the service name.

To reinstate the restriction at a later time

- Select the check box next to the service name.

To remove an access restriction from the Access Control table

- Click the **Remove** button for the service. The service will be removed from the Access Control table.

Note: When Web Filtering is enabled, HTTP services cannot be blocked by Access Control.

5.3 User-Defined Services

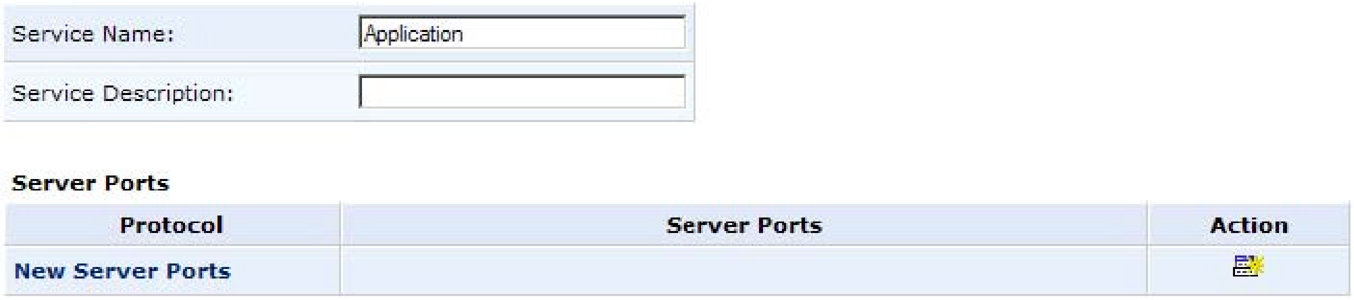
The tables that appear on the ’Add Access Control Rule’ and ’Add Local Servers’ screens are pre-configured to include most of the services that users may wish 80 to block or activate. Sometimes, however, the need arises to add a non-predefined service.

The CAP provides the ’User-Defined Services’ list for this purpose. This list appears at the top of the ’Add Access Control Rule’ and ’Add Local Servers’ screens. When a service is added to one list it automatically appears in the others. In this way, user-defined services never need to be entered twice.

To add a new service to the list:

1. Click the ’New User-Defined Service’ link. The ’Edit Service’ screen will appear.
2. Enter a name for the service.
3. Enter a description for the service.

4. Click the 'New Server Ports' link. The 'Edit Service Server Ports' screen will appear.



Service Name:	Application
Service Description:	

Server Ports

Protocol	Server Ports	Action
New Server Ports		✎

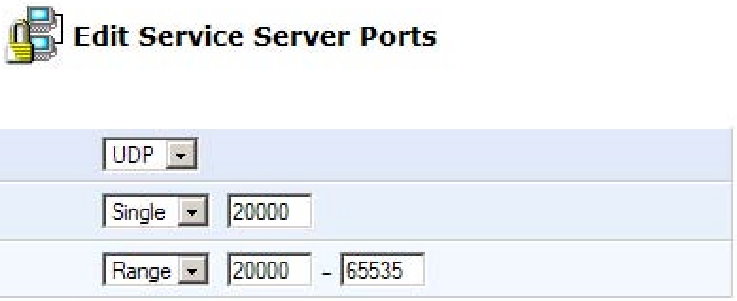
5. Choose a port type and enter a port range for this service to use as appropriate. Usually this information is available as part of the documentation that accompanies the program.

6. Click the 'OK' button to save your changes and return to the previous screen.

To modify a user-defined service already in the list:

1. Click the **Edit** button for the service. The 'Edit Service' screen will appear.

2. Modify the service name or port information as necessary.



Edit Service Server Ports

Protocol	UDP		
Source Ports:	Single	20000	
Destination Ports:	Range	20000	- 65535

3. Click the 'OK' button to save your changes and return to the previous screen.

To remove a service from the list:

1. Click the **Remove** button for the service. The service will be removed from the list.

5.4 Local Servers (Port Forwarding)

In its default state, the CAP blocks all *external* users from connecting to or communicating with your network, therefore your network is safe from hackers who may try to intrude on the network and damage it.

However, you may need to expose your network to the Internet in certain limited and controlled ways in order to enable some applications to work from the LAN (game, voice and chat applications, for example) and to establish servers in the enterprise network. The Local Servers feature supports both of these functions.

If you are familiar with networking terminology and concepts, you may have encountered this topic referred to as ”Port Forwarding”.

The Local Servers screen in the Management Console provides a list of the most commonly used applications that require special handling by the CAP. All you have to do is identify which of them you want to use, and provide the local IP address of the computer that will be using the service.

Soft-phone example:

For example, if you wanted to use the Net2Phone voice application on one of your PCs, you would simply select ‘Net2Phone’ from the list and enter the local IP address of that computer in the right-hand column.

All Net2Phone-related data arriving at the CAP from the Internet will henceforth be forwarded to the computer specified as the recipient of in-bound Net2Phone traffic.

Web Server example:

Similarly, if you want to grant Internet users access to servers inside your enterprise network, you must identify each service that you want to provide and the address of the computer that will provide it. For example, if you want to host a Web server inside the enterprise network you must select ‘HTTP - Web Server’ from the list and enter the local IP address of the computer that will host the Web server in the right-hand column. Then when an Internet user points her browser to the external IP address of the CAP, the product will forward the incoming HTTP request to the computer that is hosting the Web server.

Local Server with a ‘Forwarded Port’ – a port different than what was requested:

Additionally, Local Servers enable you to redirect traffic to a port different than the port it was designated. Lets say, that you have a web server running on your PC on port 8080 and you want to grant access to this server to anyone who accesses the CAP via HTTP. To accomplish this, do the following:

- Define a local server for the HTTP service, with the PC’s IP or hostname
- Specify 8080 in the ’Forwarded Port’ field

All incoming HTTP traffic will now be forward to the PC running the Web Server on port 8080.

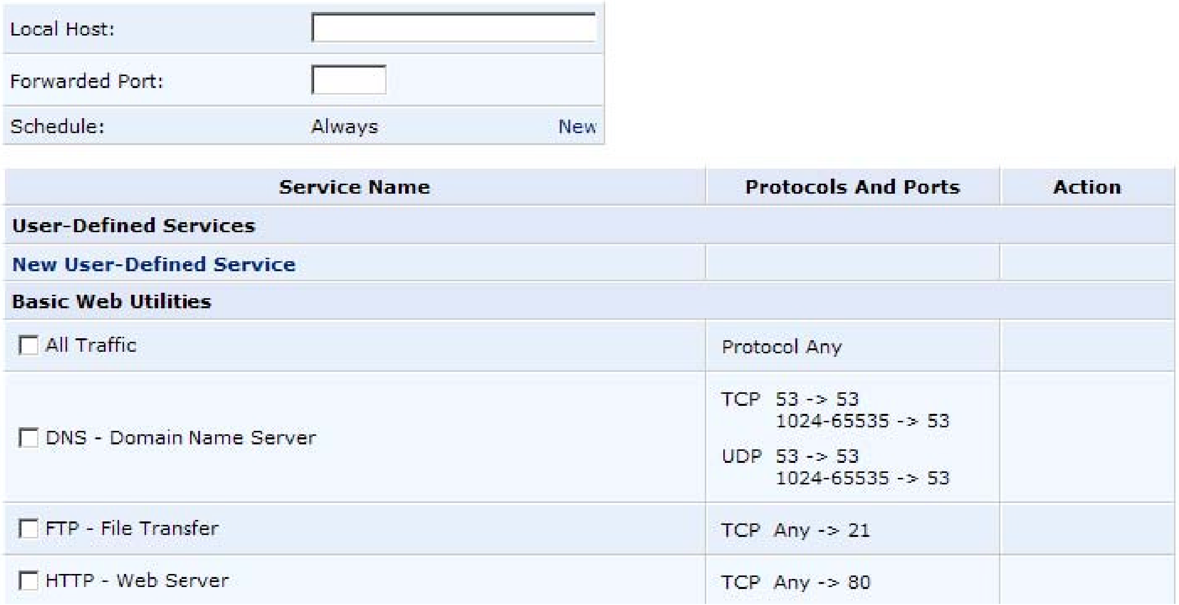
Note that if an Internet application that you wish to use or a service that you wish to provide is not already in the list, you can easily add it.

To add a new service to the list of active local servers:

1. Click the 'New Entry' button. The 'Add Local Servers' screen will appear.

2. Select the service that you would like to provide.

3. Enter the local IP address of the computer that will provide the service (the "server"). Note that only one LAN computer can be assigned to provide a specific service or application.



Local Host:	
Forwarded Port:	
Schedule:	Always New

Service Name	Protocols And Ports	Action
User-Defined Services		
New User-Defined Service		
Basic Web Utilities		
☐ All Traffic	Protocol Any	
☐ DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
☐ FTP - File Transfer	TCP Any -> 21	
☐ HTTP - Web Server	TCP Any -> 80	

4. Select a port to forward communications to (Note that this parameter is optional).

5. Define the time period during which the local server will be active. You can either select from a predefined list of schedules by selecting one from the 'Schedule' combo box, or create a new schedule by pressing the 'New' link.

6. Click the 'OK' button to save your changes and return to the 'Local Servers' screen.

To edit an entry in the Local Servers table so that a service can be provided by a different local computer:

1. Click the **Edit** button for the service. The 'Edit Service' screen will appear.

2. Enter the IP address of the computer that you would like to provide this service.

3. Click the 'OK' button to save your changes and return to the 'Local Servers' screen.

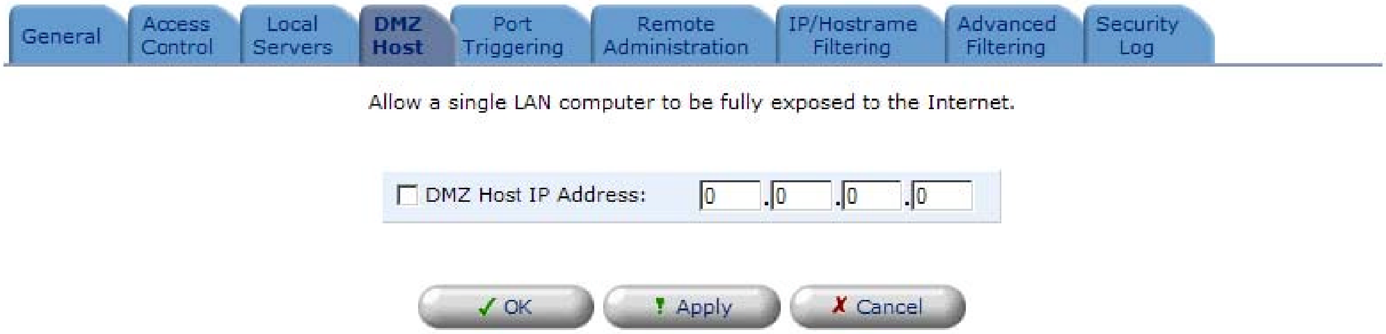
You may disable a service and make the service unavailable without having to remove the service from the Local Servers table. This may be useful if you wish to make the service unavailable only temporarily and expect that you will want to make it available again in the future.

5.5 Designating a Demilitarized (DMZ) Host

The ‘DMZ Host’ feature allows one local computer to be exposed to the Internet. Designate a DMZ host when:

- You wish to use a special-purpose Internet service, such as an on-line game or video-conferencing program, that is not present in the Local Servers list and for which no port range information is available.

- You are not concerned with security and wish to expose one computer to *all* services, without restriction.



Allow a single LAN computer to be fully exposed to the Internet.

□ DMZ Host IP Address: 0 .0 .0 .0

To designate a local computer as a DMZ Host:

1. Click the ’DMZ Host’ button. The ’DMZ Host’ screen will appear.

2. Enter the local IP address of the computer that you would like to designate as a DMZ host. Note that only one LAN computer may be a DMZ host at any time.

3. Click the ’OK’ button to save your changes and return to the ’DMZ Host’ screen.

You may disable the DMZ host so that it will not be fully exposed to the Internet, but keep its IP address recorded on the ’DMZ Host’ screen. This may be useful if you wish to disable the DMZ host but expect that you will want to enable it again in the future.

To disable the DMZ host so that it will not be fully exposed to the Internet:

- Clear the check-box next to the DMZ IP designation.

To enable the DMZ host:

- Select the check-box next to the DMZ IP designation

5.6 Port Triggering

Port triggering can be used for dynamic port forwarding configuration. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.

- The Firewalls blocks inbound traffic by default.
- The server replies to the CAP's IP, and the connection is not NATed back to your host.

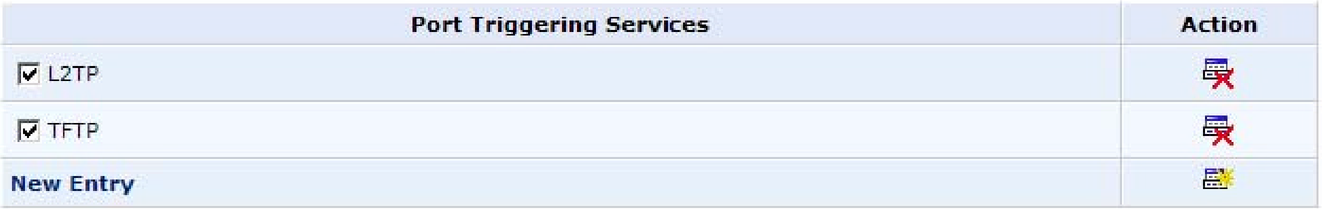
In order to solve this you need to define a Port Triggering entry, which allows inbound traffic on port 3333 TCP, only after a LAN host generated traffic to port 2222 TCP. This will result in accepting the inbound traffic from the gaming server, and sending it back to the LAN Host which originated the outgoing traffic to port 2222.

5.6.1 Defining Port Triggering

This section describes how to define a port triggering entry. The entry values are relevant to the gaming example provided in the previous section.

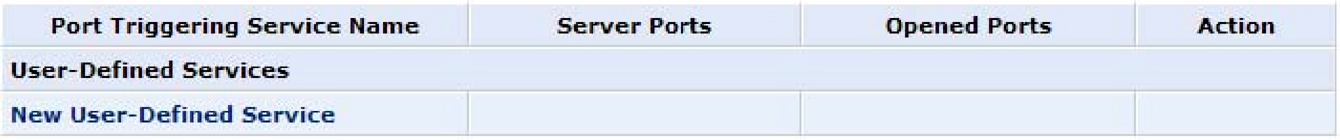
1. Click the 'Security' icon on the side-bar.

2. Click the 'Port Triggering' tab on the security screen, the 'Port Triggering' screen will appear. This screen will list all of the port triggering entries.



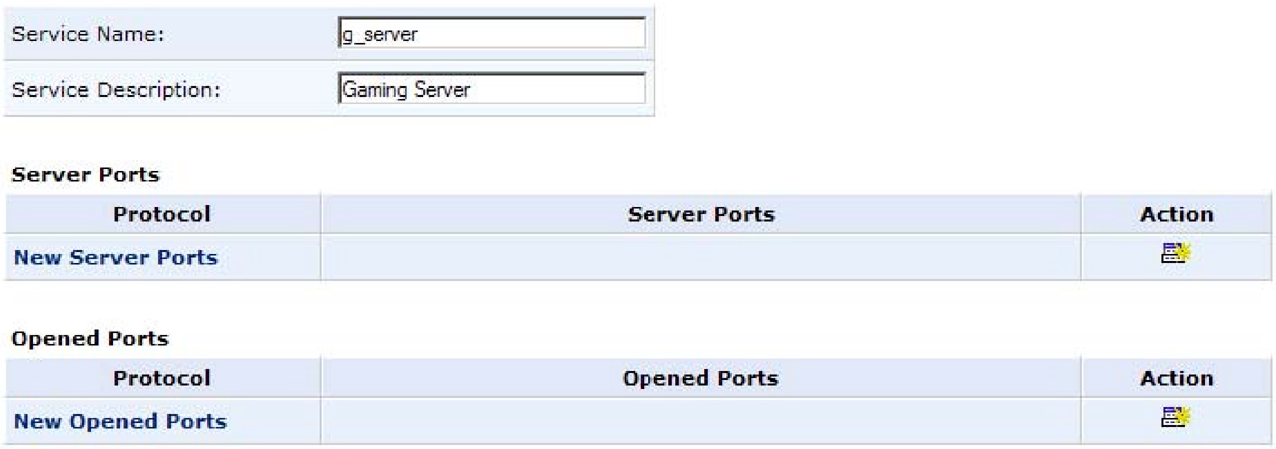
Port Triggering Services	Action
☑ L2TP	☒
☑ TFTP	☒
New Entry	

3. Click the 'New Entry' link to add an entry.



Port Triggering Service Name	Server Ports	Opened Ports	Action
User-Defined Services			
New User-Defined Service			

4. Click the ’New User-Defined Service’ link to add an entry.



Service Name:	g_server
Service Description:	Gaming Server

Server Ports

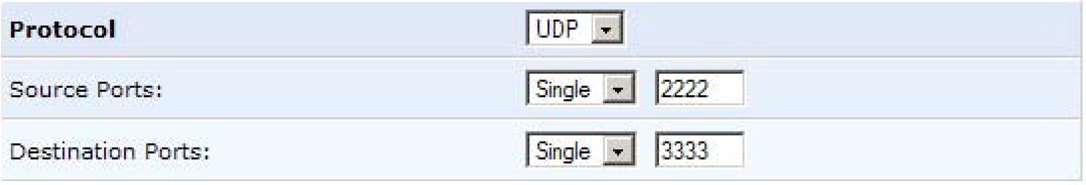
Protocol	Server Ports	Action
New Server Ports		✎

Opened Ports

Protocol	Opened Ports	Action
New Opened Ports		✎

5. Specify the following port triggering entries in the ‘New Server Ports’ and ‘New Opened Ports’ respectively.

- Server Ports: TCP ANY->2222
- Opened Ports: TCP ANY->3333



Protocol	UDP	
Source Ports:	Single	2222
Destination Ports:	Single	3333

6. Mark the ’Add Port Triggering Rule’ check-box next to your service description in the general ’Port Triggering’ screen to enable port redirection.

NOTE: There may be a few default port triggering rules listed when you first access the port triggering screen. Please note that disabling these rules may result in impaired gateway functionality.

5.7 Remote Management of the CAP

It is possible to access and control the CAP not only from within the local enterprise network, but also from the Internet. This allows your support staff or a Managed Service Provider to manage the system and view statistics remotely

Remote management access to the CAP is blocked by default to ensure the security of your local enterprise network, however, by modifying settings under ‘Security’, then ‘Remote Administration’, you can enable remote management for the following services:

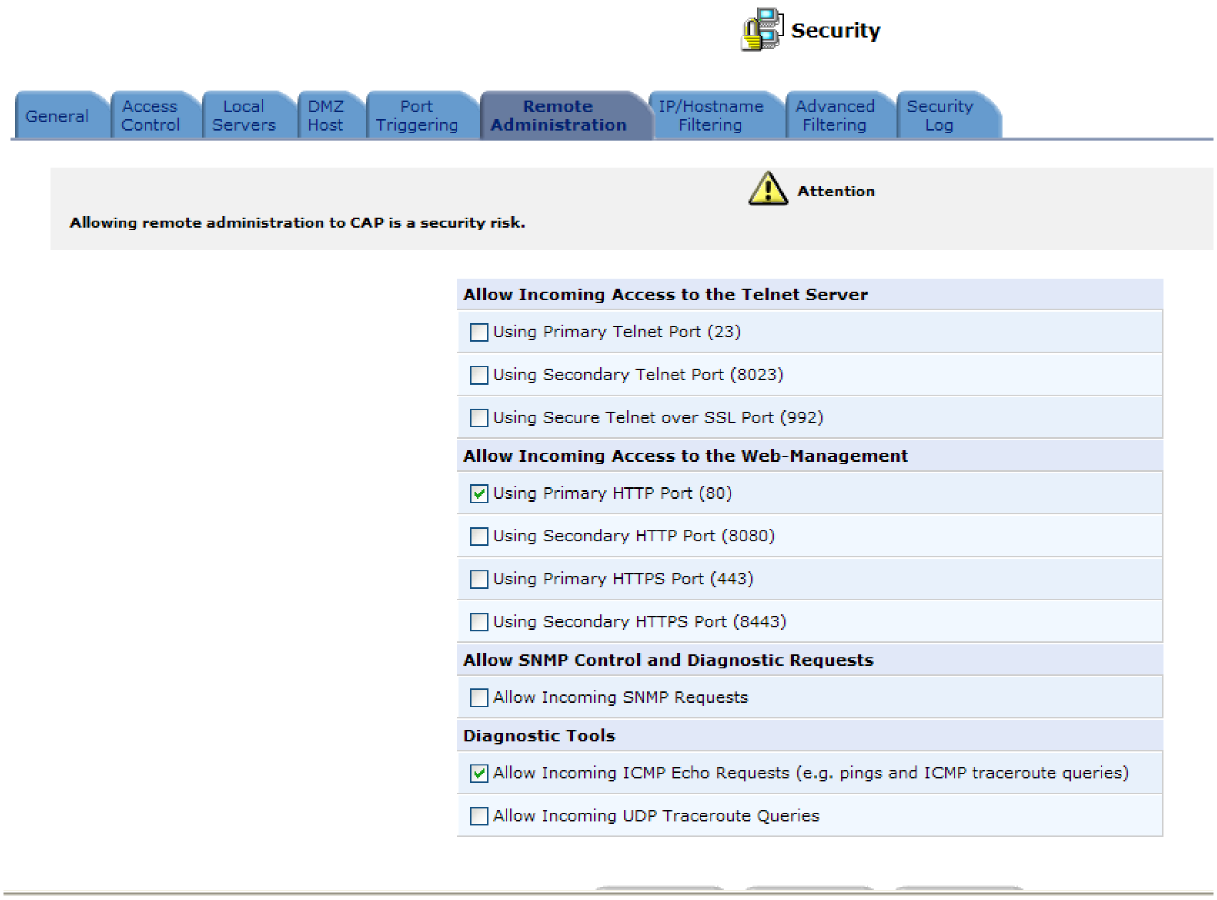
Telnet: Used to obtain a command-line and gain access to all system settings and parameters.

Web-Management/HTTP: Used to obtain access to the Management Console and gain access to all system settings and parameters.

Allow SNMP Control and Diagnostic Requests:

Used for granting access to incoming SNMP requests.

Diagnostic Tools: Used for troubleshooting and remote system management by your support staff or Managed Service Provider.



Attention

Allowing remote administration to CAP is a security risk.

Allow Incoming Access to the Telnet Server

□ Using Primary Telnet Port (23)

□ Using Secondary Telnet Port (8023)

□ Using Secure Telnet over SSL Port (992)

Allow Incoming Access to the Web-Management

☑ Using Primary HTTP Port (80)

□ Using Secondary HTTP Port (8080)

□ Using Primary HTTPS Port (443)

□ Using Secondary HTTPS Port (8443)

Allow SNMP Control and Diagnostic Requests

□ Allow Incoming SNMP Requests

Diagnostic Tools

☑ Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)

□ Allow Incoming UDP Traceroute Queries

To allow remote access to CAP services:

1. Click the ’Remote Administration’ button. The ’Remote Access Configuration’ screen will appear.

2. Select the services that you would like to make available to computers on the Internet. These services include:

Telnet: Grants command-line access to the CAP. While this service is password-protected, it is not considered a secured protocol. If a local server is configured to use port 23 select port 8023 to avoid conflicts.

Web-based Management: Grants access to password-protected Web-based management. If a local server is configured to use port 80 select port 8080 to avoid conflicts.

Allow SNMP Control and Diagnostic Requests; Grants access to incoming SNMP requests.

Diagnostic tools: Includes Ping and Traceroute (over UDP). These services may be used for troubleshooting and remote system management by the service provider.

3. Click the ’Apply’ button to save your changes and return to the ’Security’ settings screen.

Note: Encrypted remote administration is done using a secure SSL connection, requiring a SSL certificate. When accessing the CAP for the first time using encrypted remote administration, your web browser will prompt you with a warning regarding certificate authentication.

This is due to the fact that the CAP´s SSL certificate is self-generated. When encountering this message under these circumstances, ignore it and continue.

It is also possible to assign a user-defined certificate to the CAP.

5.8 IP-Hostname Filtering

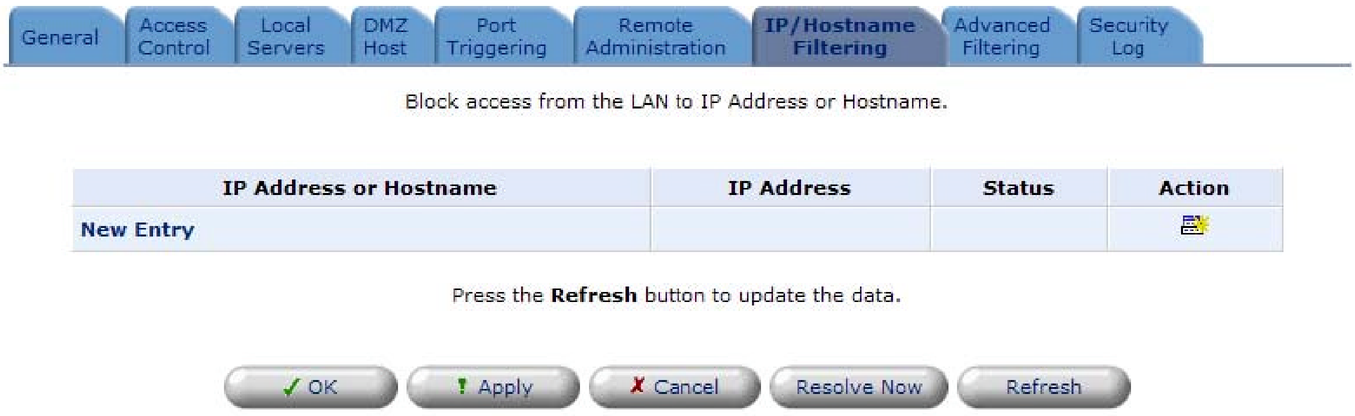
You may configure the CAP to block specific Internet Web sites so that they can not be accessed from computers in the local enterprise network. Restrictions can be applied to a comprehensive automatically updated list of sites to which access is not recommended.

To view the list of Web sites currently being blocked:

- Click the ’IP/Host-name Filtering’ tab

To add a new Web site to the list:

1. Click the ’New Entry’ button. The ’Restricted IP Address or Host-name’ screen will appear.

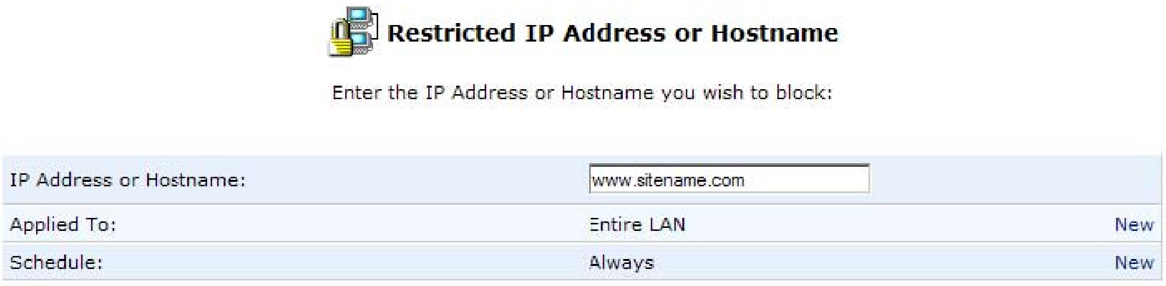


Block access from the LAN to IP Address or Hostname.

IP Address or Hostname	IP Address	Status	Action
New Entry			

Press the **Refresh** button to update the data.

2. Enter the web site address (IP or URL) that you would like to make inaccessible from your enterprise network (all web pages within the site will also be blocked). If the web site address has multiple IP addresses, the CAP will resolve all additional addresses and automatically add them to the restrictions list.



Restricted IP Address or Hostname

Enter the IP Address or Hostname you wish to block:

IP Address or Hostname:	www.sitename.com	
Applied To:	Entire LAN	New
Schedule:	Always	New

3. Select the group of computers to which you would like to apply the filtering rule. You can either select from a pre-defined list of groups by selecting one from the ’Applied To’ combo box, or create a new group by pressing the ’New’ link.

4. Define the time period during which the rule will take effect. You can either select from a pre-defined list of schedules by selecting one from the ’Schedule’ combo box, or create a new schedule by pressing the ’New’ link.

5. Click the ’OK’ button to add the web site to the list. You will be returned to the previous screen while the CAP attempts to find the site. You’ll see the ’Resolving. . . ‘ status indication appear in the Status column while the site is being located, indicating that the URL is being ’Resolved’ into one or more IP addresses.

6. If the site is successfully located then ’Resolved’ will appear in the status bar, otherwise ’Error’ will appear. Click the ’Refresh’ button to update the status if necessary.

If the CAP appears not to be able to resolve the address, do the following:

- Use a Web browser to verify that the Web site is available.

- If it is available, then you probably entered the Web site address incorrectly. Skip to ’To modify a Web site address currently in the list’ below.

- If the Web site is not available, return to the ’Restrictions List’ screen and click the ’Resolve Now’ button to verify that the Web site can be found and blocked by the CAP.

To modify a Web site address currently in the list:

1. Click the ’Edit’ button that appears in the Action column. The ’Restricted IP Address or Hostname’ screen will appear.

2. Modify the Web site address, group and schedule as necessary. If it is long and/or complicated you may want to use your browser’s Copy and Paste functions to copy the address from the address bar to the management console. <u>Be sure to omit the “http://” at the beginning and the “/” at the end of the address.</u>

3. Click the ’OK’ button to save your changes.

To ensure that all current IP addresses corresponding to Web sites in the list are blocked:

- Click the ’Resolve Now’ button. The CAP will check each of the Web site addresses in the list and ensure that all IP addresses at which this Web site can be found are included in the IP addresses column.

You may disable a restriction and make the Web site available again without having to remove the site from the ’Restrictions List’. This may be useful if you wish to make the Web site available only temporarily and expect that you will want to block it again in the future.

To temporarily disable a restriction:

- Clear the check box next to the restricted URL

To reinstate the restriction at a later time:

- Select the check box next to the URL

To remove a restriction:

- Click the ‘**Remove’** button. The restriction will be removed from the Restrictions List.

5.9 Security Log

The Security log displays a list of ***Firewall-related events***, including attempts to establish inbound and outbound connections, attempts to authenticate at an administrative interface (Web-based Management or Telnet terminal), Firewall configuration modifications, and system start-up.

To view the Security Log:

- Click the 'Security Log' button appearing on the 'Security'

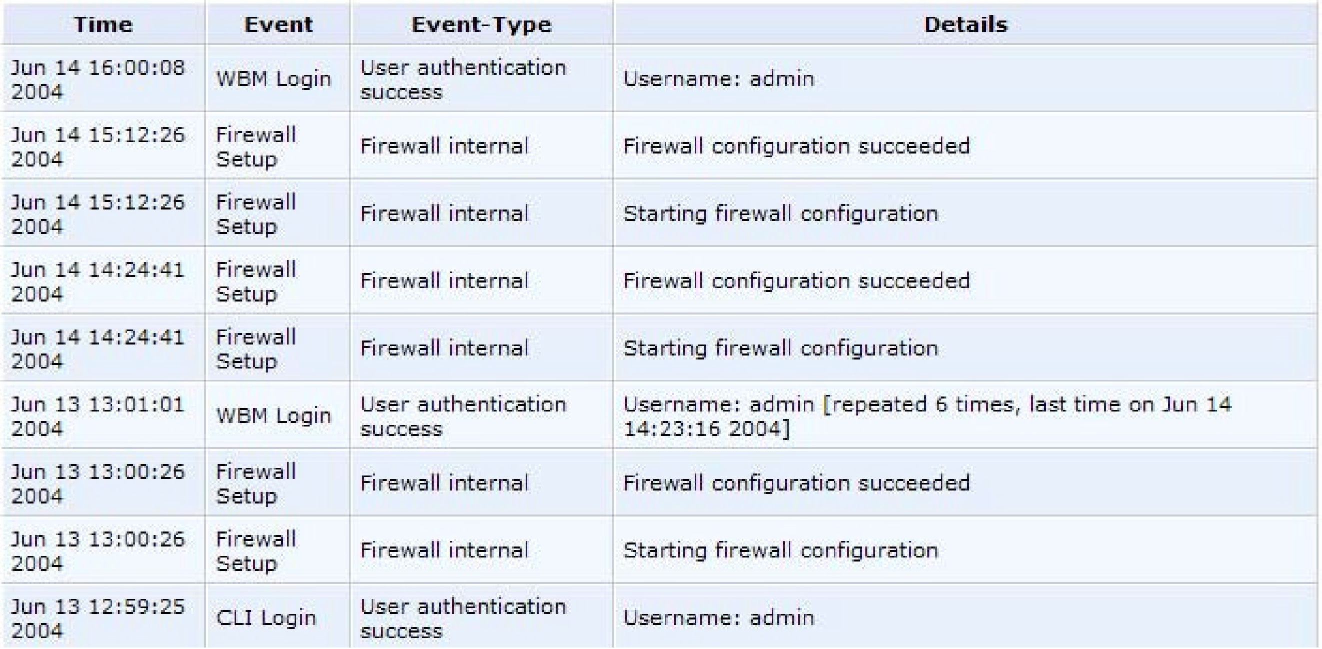
Time: The time the event occurred.

Event: Inbound Traffic: The event is a result of an incoming packet.
Outbound Traffic: The event is a result of outgoing packet
Firewall Setup: Configuration message

Event-Type: Textual description of the event (see full description below).

Blocked: Means that the packet was blocked. Message is colored with red.
Accepted: Means that the packet was accepted. Message is colored with green.

Details: More details about the packet or the event, Such as protocol, IP addresses, ports, etc.



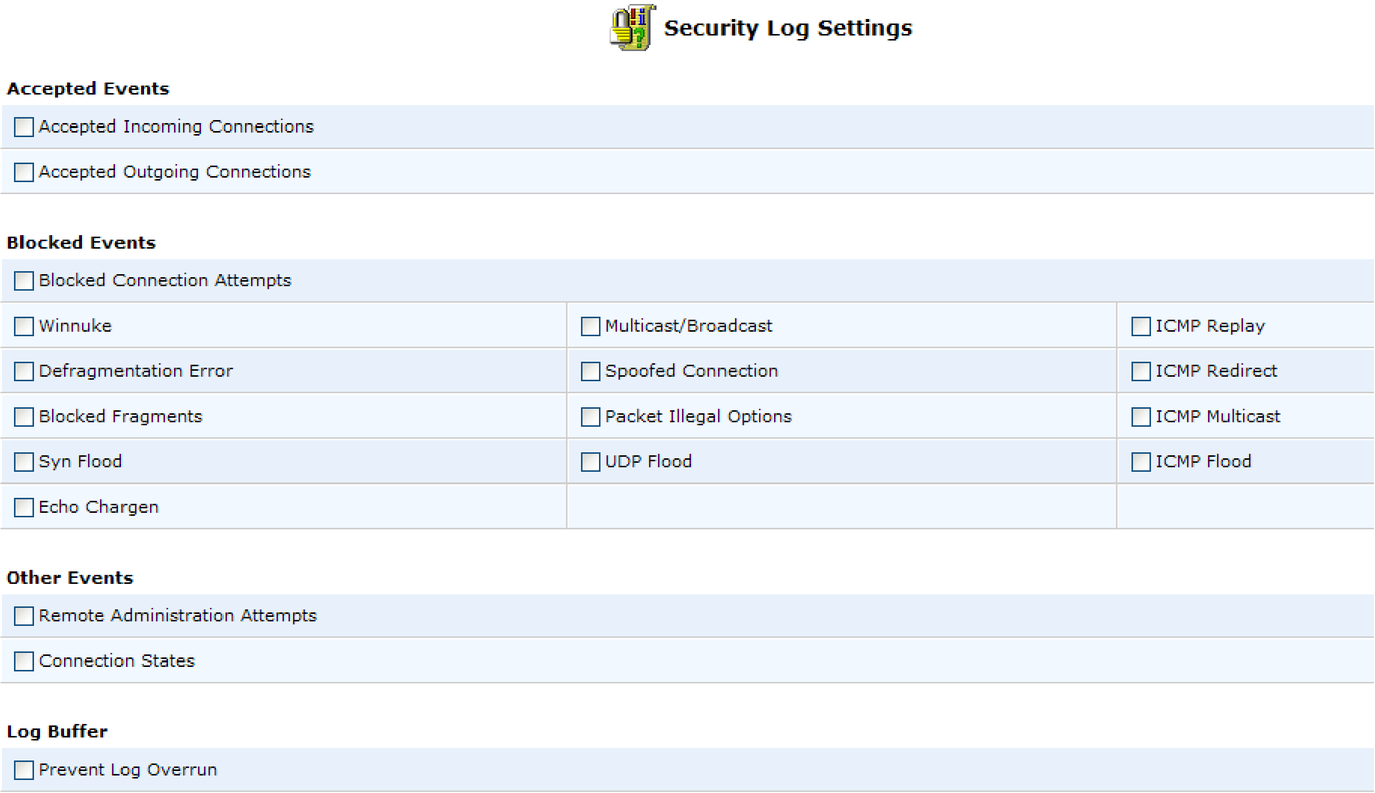
Time	Event	Event-Type	Details
Jun 14 16:00:08 2004	WBM Login	User authentication success	Username: admin
Jun 14 15:12:26 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 14 15:12:26 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 14 14:24:41 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 14 14:24:41 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 13 13:01:01 2004	WBM Login	User authentication success	Username: admin [repeated 6 times, last time on Jun 14 14:23:16 2004]
Jun 13 13:00:26 2004	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jun 13 13:00:26 2004	Firewall Setup	Firewall internal	Starting firewall configuration
Jun 13 12:59:25 2004	CLI Login	User authentication success	Username: admin

The following are the available Event-Types that can be recorded in the Firewall log:

1. Firewall internal
2. Firewall status changed
3. STP packet
4. Illegal packet options
5. Fragmented packet
6. WinNuke protection
7. ICMP replay
8. ICMP redirect protection
9. Packet invalid in connection
10. ICMP protection
11. Broadcast/Multicast protection
12. Spoofing protection
13. DMZ network packet
14. Trusted device
15. Default policy
16. Remote administration
17. Access control
18. Parental control
19. NAT out failed
20. DHCP request
21. DHCP response
22. DHCP relay agent
23. IGMP packet
24. Multicast IGMP connection
25. RIP packet
26. PPTP connection
27. Kerberos key management 1293
28. Kerberos 88
29. AUTH:113 request
30. Packet-Cable
31. IPV6 over IPV4
32. ARP
33. PPP Discover
34. PPP Session
35. 802.1Q
36. Outbound Auth1X
37. IP Version 6
38. CAP initiated traffic
39. Maximum security enabled service
40. SynCookies Protection
41. ICMP Flood Protection
42. UDP Flood Protection
43. Service
44. Rule
45. Fragmented packet, header too small
46. Fragmented packet, header too big
47. Fragmented packet, drop all
48. Fragmented packet, bad align
49. Fragmented packet, packet too big
50. Fragmented packet, packet exceeds
51. Fragmented packet, no memory
52. Fragmented packet, overlapped
53. De-fragmentation failed
54. Connection opened
55. Wildcard connection opened
56. Wildcard connection hooked
57. Connection closed
58. Echo/Chargen/Quote/Snork protection
59. First packet in connection is not a SYN packet
60. Error : No memory
61. NAT Error : connection pool is full. No connection created
62. NAT Error: No free NAT IP
63. NAT Error: Conflict Mapping already exists
64. Malformed packet -Failed parsing
65. Passive attack on ftp-server: Client attempted to open Server ports
66. FTP port request to 3rd party is forbidden (Possible bounce attack)
67. Firewall Rules were changed
68. User authentication

To view or change the Firewall Log settings:

1. Click the 'Settings' button that appears at the top of the 'Firewall Log' screen. The 'Security Log Settings' screen will appear.



Security Log Settings

Accepted Events

□ Accepted Incoming Connections

□ Accepted Outgoing Connections

Blocked Events

□ Blocked Connection Attempts

□ Winnuke	□ Multicast/Broadcast	□ ICMP Replay
□ Defragmentation Error	□ Spoofed Connection	□ ICMP Redirect
□ Blocked Fragments	□ Packet Illegal Options	□ ICMP Multicast
□ Syn Flood	□ UDP Flood	□ ICMP Flood
□ Echo Chargen		

Other Events

□ Remote Administration Attempts

□ Connection States

Log Buffer

□ Prevent Log Overrun

2. Select the types of activities for which you would a log entry generated:

- Accepted Incoming Connections: Logs a message for each successful attempt to establish an inbound connection to the enterprise network.

- Accepted Outgoing Connections: Logs a message for each successful attempt to establish an outgoing connection to the public network.

- Blocked Connection Attempts: Logs a message for each blocked attempt to establish an inbound connection to the enterprise network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options below it.

  Specify the blocked events that should be monitored. Use this to monitor specific event such as synflood. A log message will be generated if either the corresponding check-box is checked, or the "Blocked Connection Attempts" check-box is checked.

- Remote Administration Attempts: The log a message for each remote-administration connection attempt, whether successful or not.

- Connection States: Give extra information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application

Level Gateways (ALGs).

- Prevent Log Overrun: Stop logging Firewall activities when the memory allocated for the log is completely full.

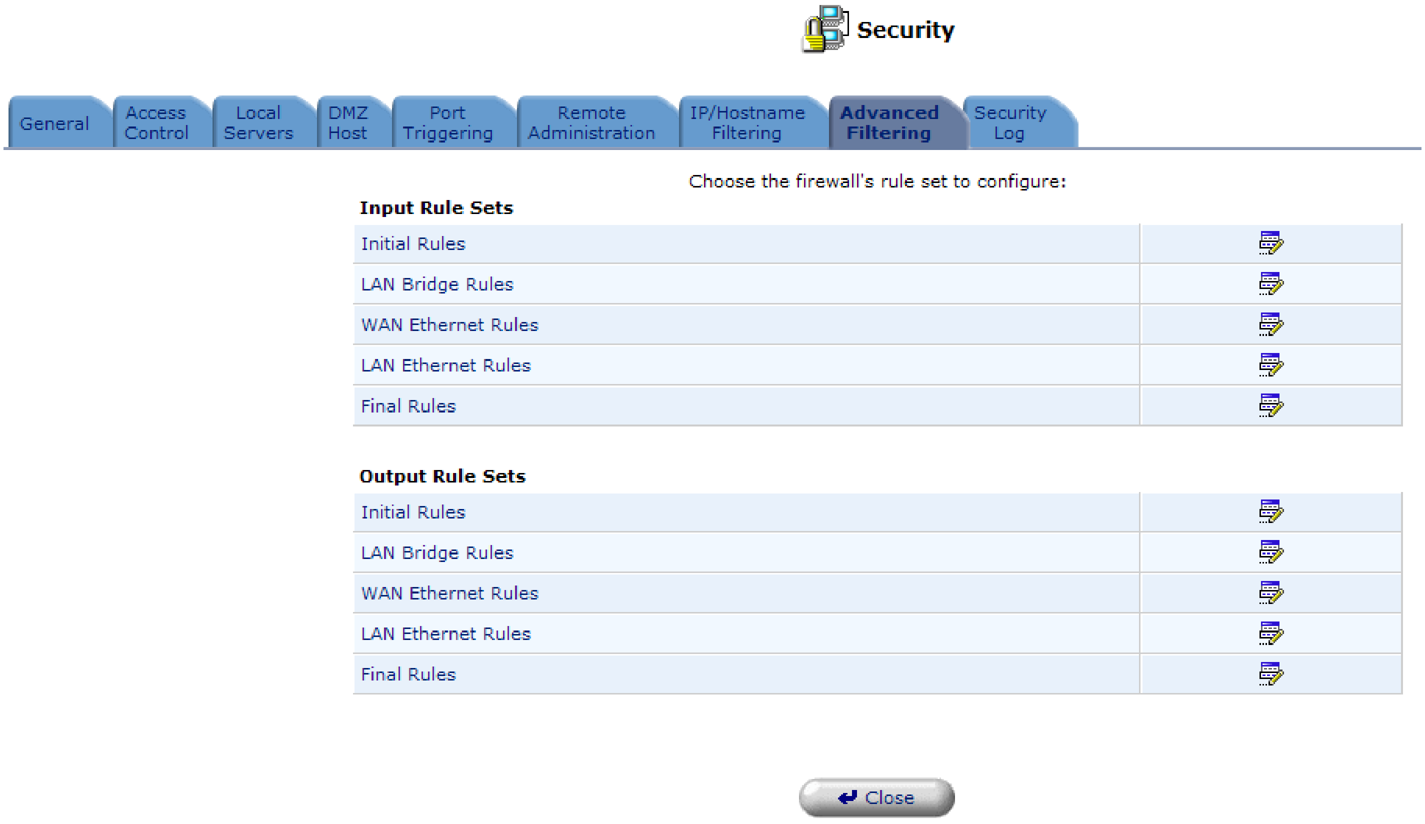
3. Click the 'OK' button to save your changes and return to the 'Firewall Log' screen.

5.10 Advanced Filtering

Advanced filtering is designed to allow comprehensive control over the Firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN network devices.

To access the Advanced Filtering screen:

- Press the 'Security' icon on the sidebar to display the security features
- Press the 'Advanced Filtering' button. The 'Advanced Filtering' screen will appear



Choose the firewall's rule set to configure:

Input Rule Sets

Initial Rules	✎
LAN Bridge Rules	✎
WAN Ethernet Rules	✎
LAN Ethernet Rules	✎
Final Rules	✎

Output Rule Sets

Initial Rules	✎
LAN Bridge Rules	✎
WAN Ethernet Rules	✎
LAN Ethernet Rules	✎
Final Rules	✎

You can configure two sets of rules, Input Rules and Output rules.

Each set of rules is comprised of three subsets:

- **Initial Rules**
- **Network Devices Rules**
- **Final Rules**

These subsets determine the sequencing by which the rules will be applied.

The following is a description of the set ordering for In-bound and Out-bound packets.

Inbound Packets – Input Rule Sets

- Initial rules
- All rules in the set of the network device the packet is on.
- 'Local Server' rules from the local server tab in the security screen.
- Rules to accept all the packets on a device for which the Firewall check box "Internet Connection Firewall" in the connection settings screen is unchecked.
- Remote administration rules from the remote administration tab.
- DMZ host rules from the DMZ tab.
- Final rules.

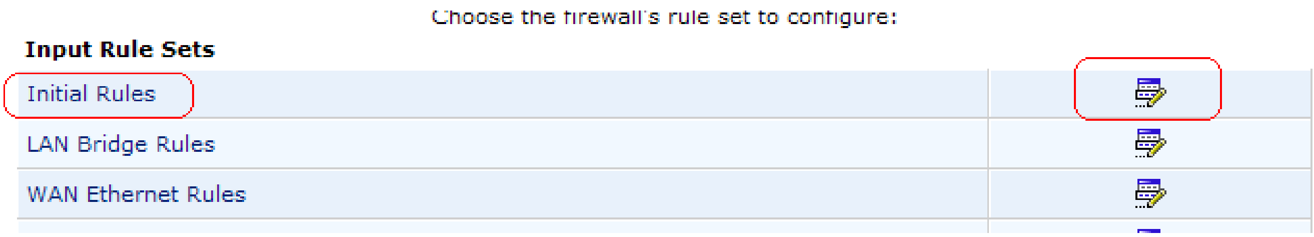
Outbound Packets – Output Rules Sets

- Initial rules.
- All rules in the set of the network device the packet is on.
- Rules to accept all the packets on a device for which the Firewall check box "Internet Connection Firewall" in the connection settings screen is unchecked.
- IP/hostname filtering rules and access control rules from the tabs in the security screen.
- Final rules.

There other numerous rules automatically inserted by the Firewall in order to provide improved security and block harmful attacks.

Defining Advanced Filtering rules:

- Press the 'Edit' button next to the rule title, or click on the title (such as 'Initial Rules') directly.

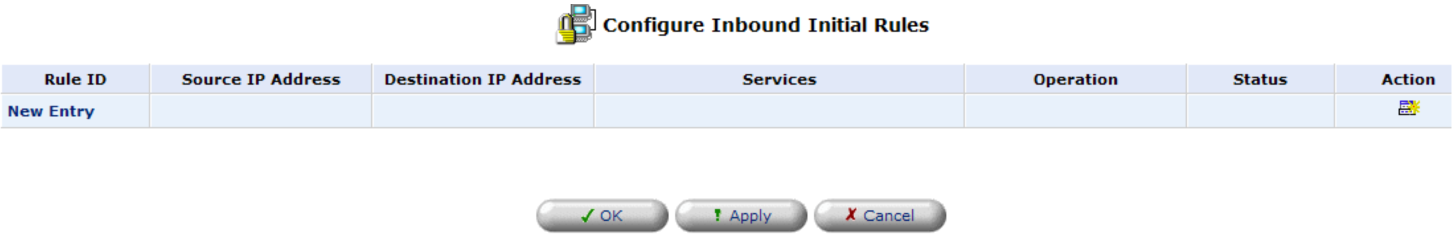


Choose the firewall's rule set to configure:

Input Rule Sets

Initial Rules	
LAN Bridge Rules	
WAN Ethernet Rules	

- The 'Configure Rules' screen will appear, displaying the entries currently constituting the rule subset you selected.



Configure Inbound Initial Rules

Rule ID	Source IP Address	Destination IP Address	Services	Operation	Status	Action
New Entry						

5.10.1 Adding an Advanced Filtering Rule

To add an advanced filtering rule, click on ‘New Entry’, then carefully define the following rule parameters:

1. **Matching:** To apply a Firewall rule, a match must be made between IP addresses or ranges and ports. Use the ’Source IP’ and ’Destination IP’ to define the coupling of source and destination traffic.

   Port matching will be defined when selecting services (see step 5). For example, if you select the FTP service, port 21 will be checked for matching traffic flow between the defined source and destination IP’s.

2. **Operation:** Where you define what action the rule will take, by selecting one of the following radio buttons:

   Drop: Deny access to packets that match the source and destination IP addresses and service ports defined in ’Matching’. No response is sent to the sending station.

   Reject: Reject s packets as Drop does, but also sends a response to the sending station.

   Accept: Allow access to packets that match the source and destination IP addresses and service ports defined in ’Matching’. The data transfer session will be handled using Stateful Packet Inspection (SPI).

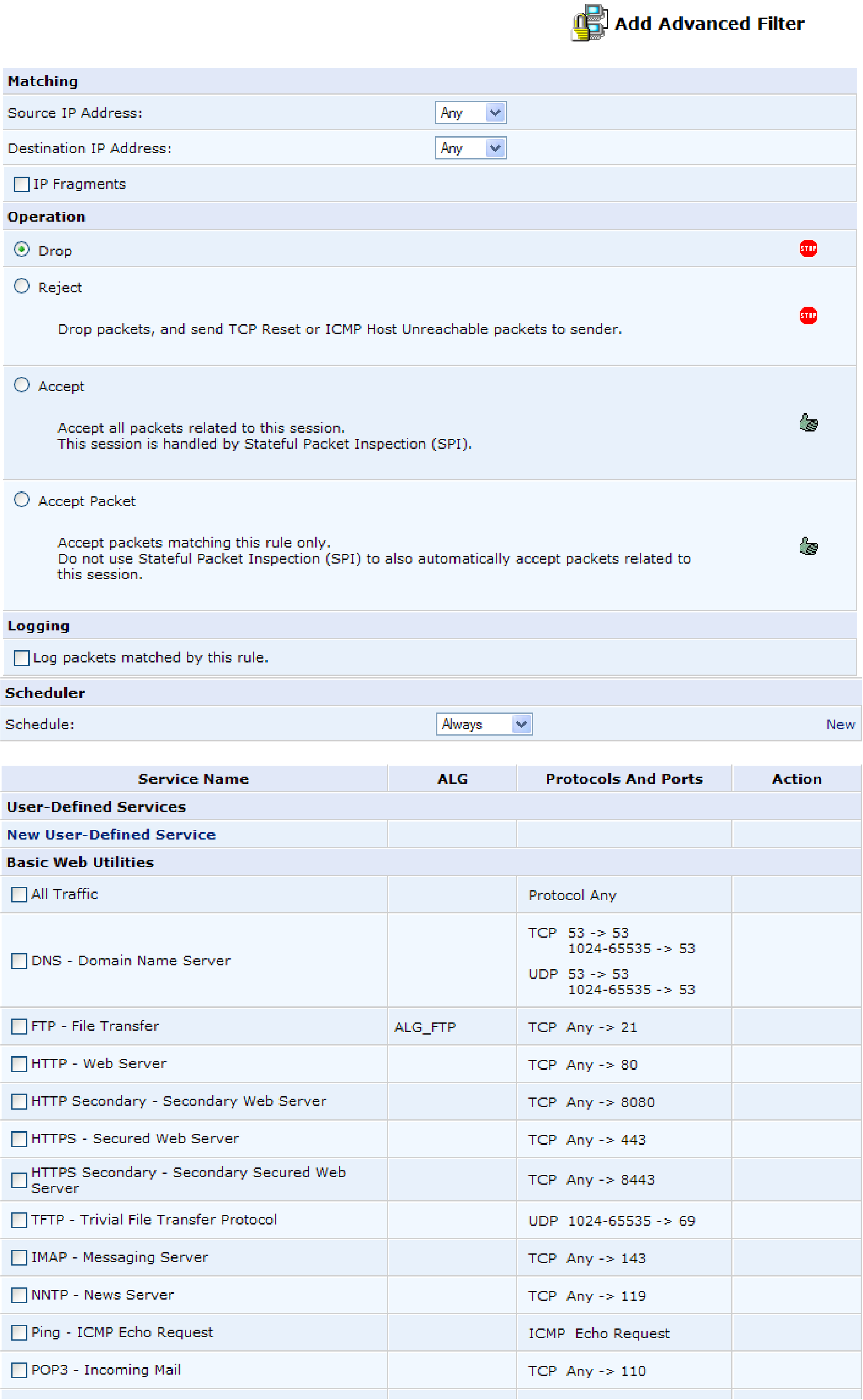
   Accept Packet: Allow access to packets that match the source and destination IP addresses and service ports defined in ’Matching’.

   The data transfer session **will not** be handled using Stateful Packet Inspection (SPI), meaning that other packets that match this rule will not be automatically allowed access. For example, this can be useful when creating rules that allow broadcasting.

3. **Logging:** Select this check-box to add entries relating to this rule to the security log.

4. **Scheduler:** Select or create a schedule for the rule. For information on how to configure Scheduler Rules refer to section 7.10.

5. **Services:** Select the services to which you would like to apply this rule. You can add user-defined services by clicking the ’New User-Defined Service’.



Add Advanced Filter

Matching

Source IP Address: Any

Destination IP Address: Any

□ IP Fragments

Operation

● Drop

○ Reject

Drop packets, and send TCP Reset or ICMP Host Unreachable packets to sender.

○ Accept

Accept all packets related to this session.
This session is handled by Stateful Packet Inspection (SPI).

○ Accept Packet

Accept packets matching this rule only.
Do not use Stateful Packet Inspection (SPI) to also automatically accept packets related to this session.

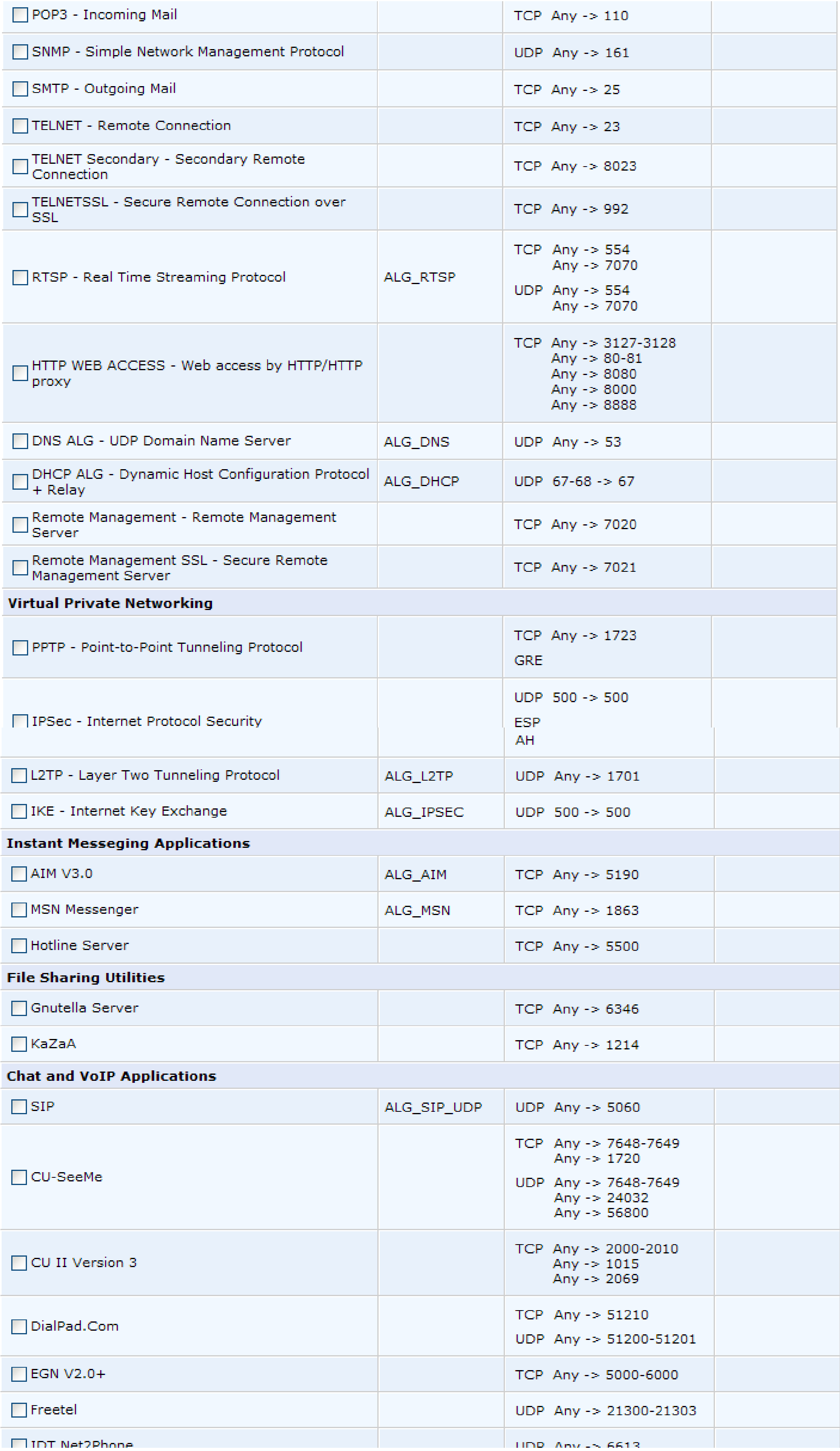
Logging

□ Log packets matched by this rule.

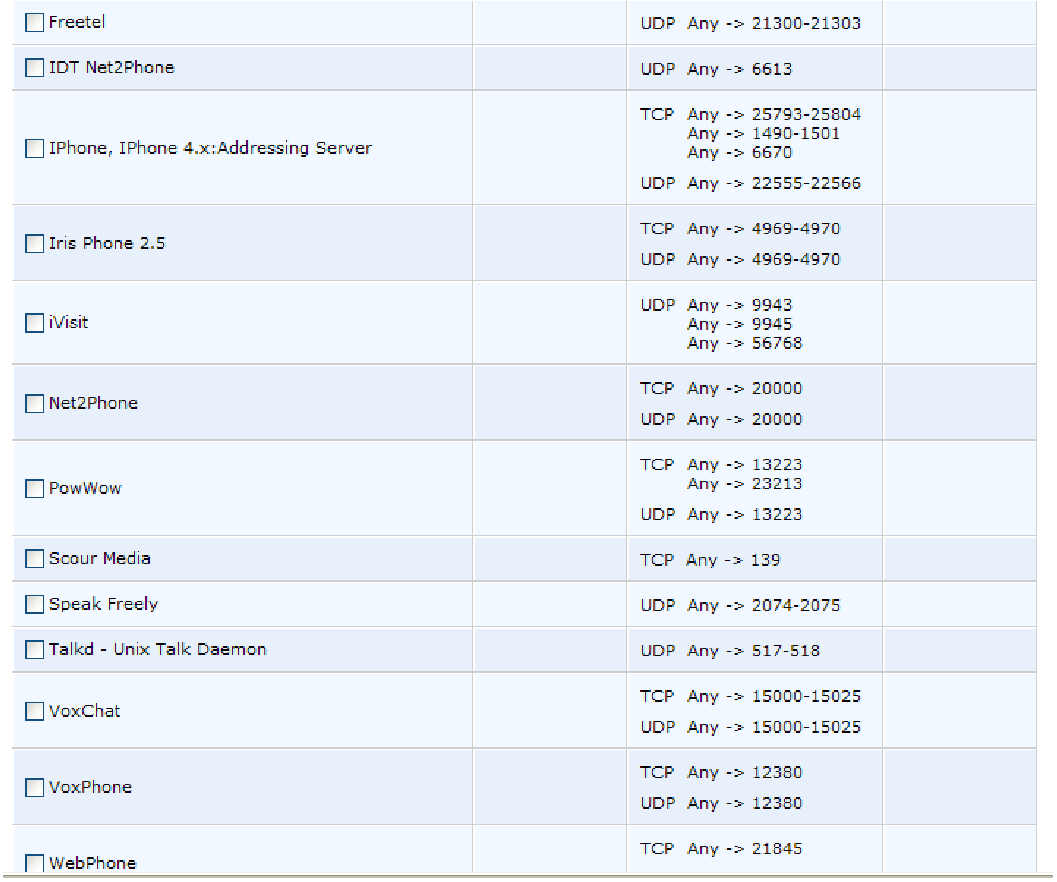
Scheduler

Schedule: Always New

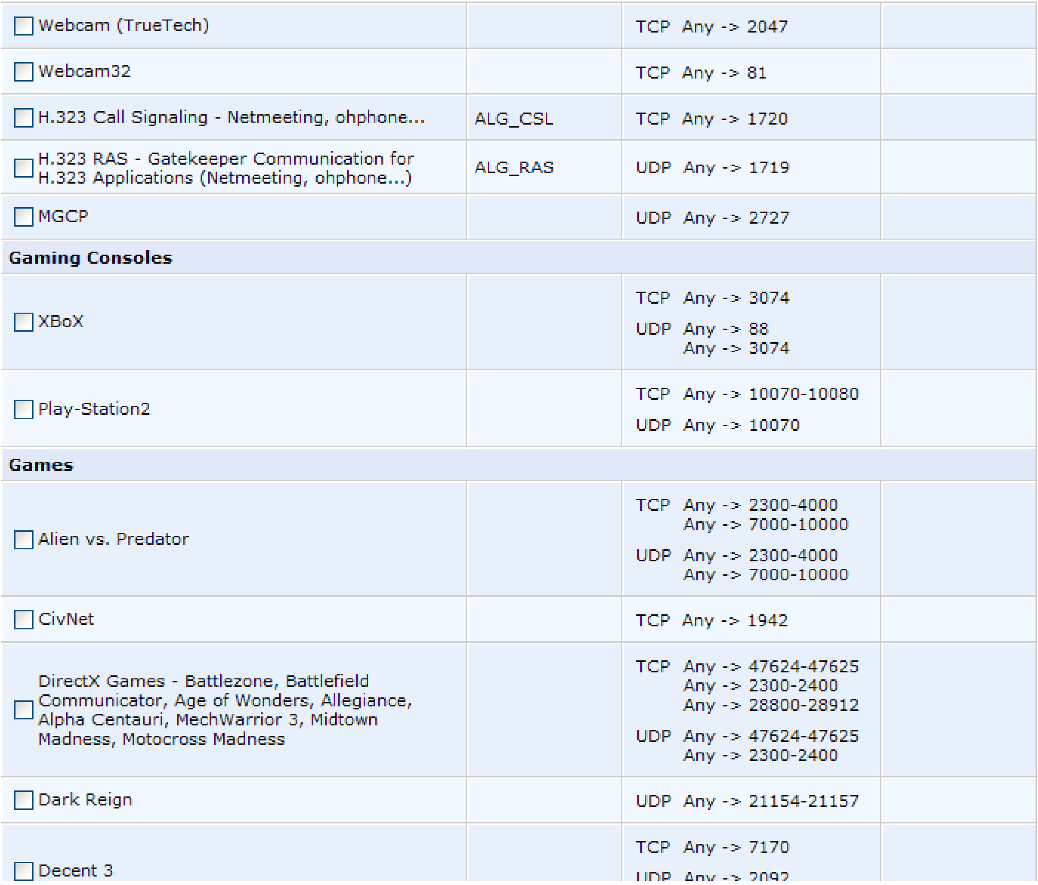
Service Name	ALG	Protocols And Ports	Action
User-Defined Services			
New User-Defined Service			
Basic Web Utilities			
□ All Traffic		Protocol Any	
□ DNS - Domain Name Server		TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
□ FTP - File Transfer	ALG_FTP	TCP Any -> 21	
□ HTTP - Web Server		TCP Any -> 80	
□ HTTP Secondary - Secondary Web Server		TCP Any -> 8080	
□ HTTPS - Secured Web Server		TCP Any -> 443	
□ HTTPS Secondary - Secondary Secured Web Server		TCP Any -> 8443	
□ TFTP - Trivial File Transfer Protocol		UDP 1024-65535 -> 69	
□ IMAP - Messaging Server		TCP Any -> 143	
□ NNTP - News Server		TCP Any -> 119	
□ Ping - ICMP Echo Request		ICMP Echo Request	
□ POP3 - Incoming Mail		TCP Any -> 110	



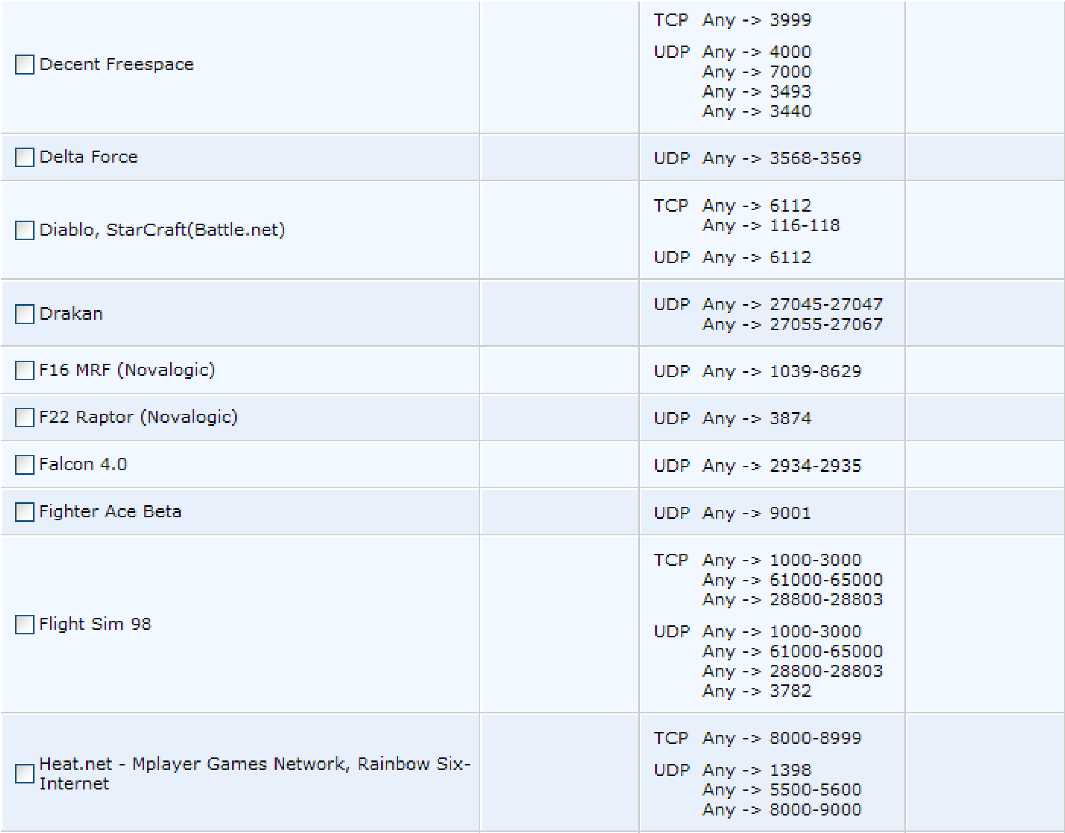
□ POP3 - Incoming Mail		TCP Any -> 110	
□ SNMP - Simple Network Management Protocol		UDP Any -> 161	
□ SMTP - Outgoing Mail		TCP Any -> 25	
□ TELNET - Remote Connection		TCP Any -> 23	
□ TELNET Secondary - Secondary Remote Connection		TCP Any -> 8023	
□ TELNETSSL - Secure Remote Connection over SSL		TCP Any -> 992	
□ RTSP - Real Time Streaming Protocol	ALG_RTSP	TCP Any -> 554 Any -> 7070 UDP Any -> 554 Any -> 7070	
□ HTTP WEB ACCESS - Web access by HTTP/HTTP proxy		TCP Any -> 3127-3128 Any -> 80-81 Any -> 8080 Any -> 8000 Any -> 8888	
□ DNS ALG - UDP Domain Name Server	ALG_DNS	UDP Any -> 53	
□ DHCP ALG - Dynamic Host Configuration Protocol + Relay	ALG_DHCP	UDP 67-68 -> 67	
□ Remote Management - Remote Management Server		TCP Any -> 7020	
□ Remote Management SSL - Secure Remote Management Server		TCP Any -> 7021	
Virtual Private Networking			
□ PPTP - Point-to-Point Tunneling Protocol		TCP Any -> 1723 GRE	
□ IPSec - Internet Protocol Security		UDP 500 -> 500 ESP AH	
□ L2TP - Layer Two Tunneling Protocol	ALG_L2TP	UDP Any -> 1701	
□ IKE - Internet Key Exchange	ALG_IPSEC	UDP 500 -> 500	
Instant Messeging Applications			
□ AIM V3.0	ALG_AIM	TCP Any -> 5190	
□ MSN Messenger	ALG_MSN	TCP Any -> 1863	
□ Hotline Server		TCP Any -> 5500	
File Sharing Utilities			
□ Gnutella Server		TCP Any -> 6346	
□ KaZaA		TCP Any -> 1214	
Chat and VoIP Applications			
□ SIP	ALG_SIP_UDP	UDP Any -> 5060	
□ CU-SeeMe		TCP Any -> 7648-7649 Any -> 1720 UDP Any -> 7648-7649 Any -> 24032 Any -> 56800	
□ CU II Version 3		TCP Any -> 2000-2010 Any -> 1015 Any -> 2069	
□ DialPad.Com		TCP Any -> 51210 UDP Any -> 51200-51201	
□ EGN V2.0+		TCP Any -> 5000-6000	
□ Freetel		UDP Any -> 21300-21303	
□ IDT Net2Phone		UDP Any -> 6613	

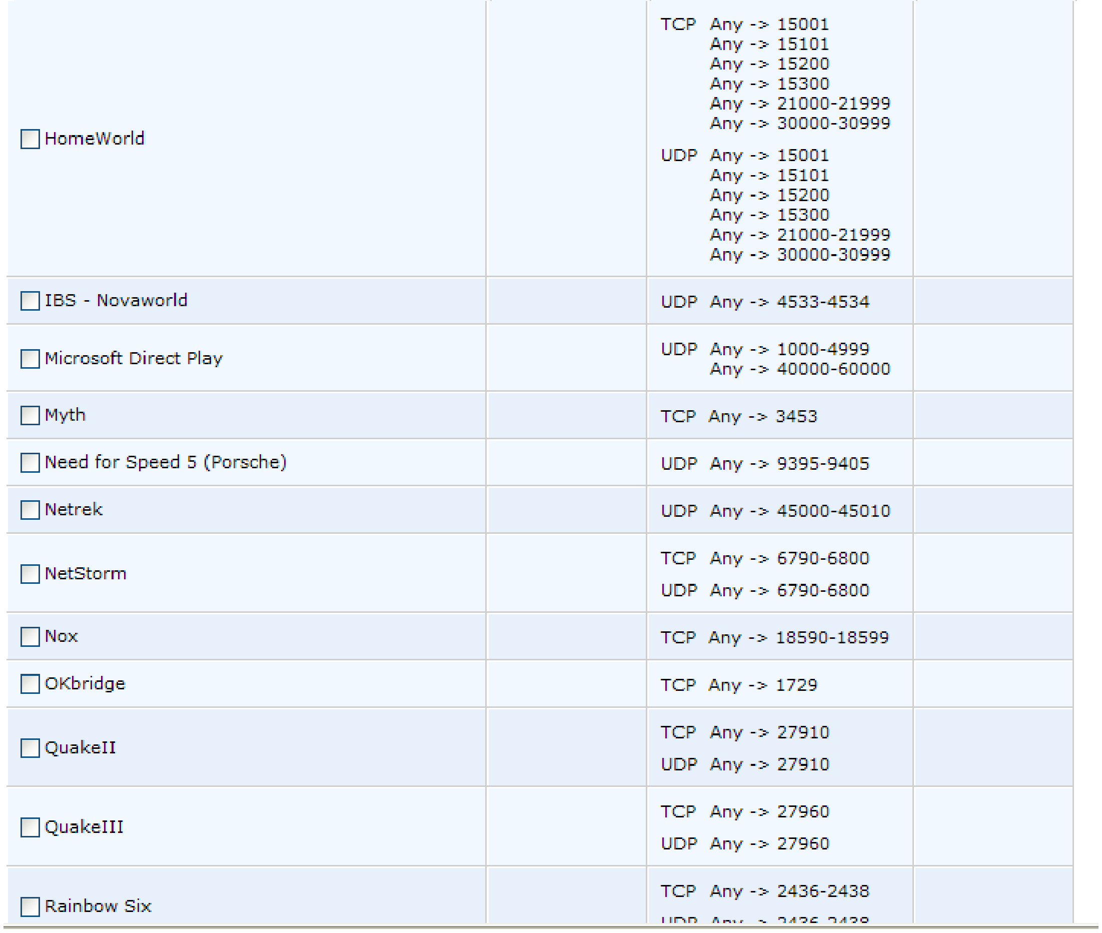


□ Freetel		UDP Any -> 21300-21303	
□ IDT Net2Phone		UDP Any -> 6613	
□ IPhone, IPhone 4.x:Addressing Server		TCP Any -> 25793-25804 Any -> 1490-1501 Any -> 6670 UDP Any -> 22555-22566	
□ Iris Phone 2.5		TCP Any -> 4969-4970 UDP Any -> 4969-4970	
□ iVisit		UDP Any -> 9943 Any -> 9945 Any -> 56768	
□ Net2Phone		TCP Any -> 20000 UDP Any -> 20000	
□ PowWow		TCP Any -> 13223 Any -> 23213 UDP Any -> 13223	
□ Scour Media		TCP Any -> 139	
□ Speak Freely		UDP Any -> 2074-2075	
□ Talkd - Unix Talk Daemon		UDP Any -> 517-518	
□ VoxChat		TCP Any -> 15000-15025 UDP Any -> 15000-15025	
□ VoxPhone		TCP Any -> 12380 UDP Any -> 12380	
□ WebPhone		TCP Any -> 21845	

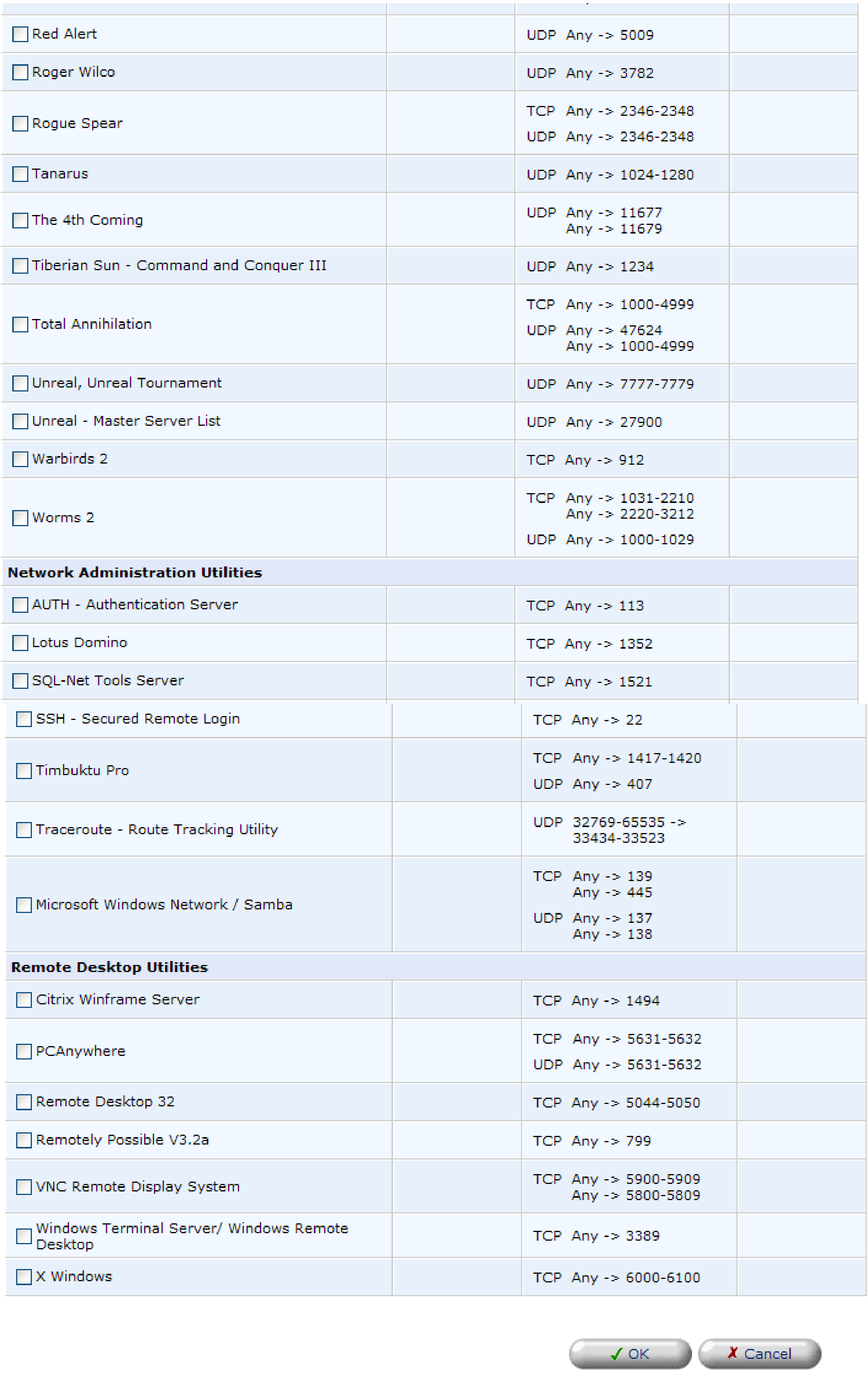


□ Webcam (TrueTech)		TCP Any -> 2047	
□ Webcam32		TCP Any -> 81	
□ H.323 Call Signaling - Netmeeting, ohphone...	ALG_CSL	TCP Any -> 1720	
□ H.323 RAS - Gatekeeper Communication for H.323 Applications (Netmeeting, ohphone...)	ALG_RAS	UDP Any -> 1719	
□ MGCP		UDP Any -> 2727	
Gaming Consoles			
□ XBoX		TCP Any -> 3074 UDP Any -> 88 Any -> 3074	
□ Play-Station2		TCP Any -> 10070-10080 UDP Any -> 10070	
Games			
□ Alien vs. Predator		TCP Any -> 2300-4000 Any -> 7000-10000 UDP Any -> 2300-4000 Any -> 7000-10000	
□ CivNet		TCP Any -> 1942	
□ DirectX Games - Battlezone, Battlefield Communicator, Age of Wonders, Allegiance, Alpha Centauri, MechWarrior 3, Midtown Madness, Motocross Madness		TCP Any -> 47624-47625 Any -> 2300-2400 Any -> 28800-28912 UDP Any -> 47624-47625 Any -> 2300-2400	
□ Dark Reign		UDP Any -> 21154-21157	
□ Decent 3		TCP Any -> 7170 UDP Any -> 2092	





□ Decent Freespace		TCP Any -> 3999 UDP Any -> 4000 Any -> 7000 Any -> 3493 Any -> 3440	
□ Delta Force		UDP Any -> 3568-3569	
□ Diablo, StarCraft(Battle.net)		TCP Any -> 6112 Any -> 116-118 UDP Any -> 6112	
□ Drakan		UDP Any -> 27045-27047 Any -> 27055-27067	
□ F16 MRF (Novalogic)		UDP Any -> 1039-8629	
□ F22 Raptor (Novalogic)		UDP Any -> 3874	
□ Falcon 4.0		UDP Any -> 2934-2935	
□ Fighter Ace Beta		UDP Any -> 9001	
□ Flight Sim 98		TCP Any -> 1000-3000 Any -> 61000-65000 Any -> 28800-28803 UDP Any -> 1000-3000 Any -> 61000-65000 Any -> 28800-28803 Any -> 3782	
□ Heat.net - Mplayer Games Network, Rainbow Six-Internet		TCP Any -> 8000-8999 UDP Any -> 1398 Any -> 5500-5600 Any -> 8000-9000	
□ HomeWorld		TCP Any -> 15001 Any -> 15101 Any -> 15200 Any -> 15300 Any -> 21000-21999 Any -> 30000-30999 UDP Any -> 15001 Any -> 15101 Any -> 15200 Any -> 15300 Any -> 21000-21999 Any -> 30000-30999	
□ IBS - Novaworld		UDP Any -> 4533-4534	
□ Microsoft Direct Play		UDP Any -> 1000-4999 Any -> 40000-60000	
□ Myth		TCP Any -> 3453	
□ Need for Speed 5 (Porsche)		UDP Any -> 9395-9405	
□ Netrek		UDP Any -> 45000-45010	
□ NetStorm		TCP Any -> 6790-6800 UDP Any -> 6790-6800	
□ Nox		TCP Any -> 18590-18599	
□ OKbridge		TCP Any -> 1729	
□ QuakeII		TCP Any -> 27910 UDP Any -> 27910	
□ QuakeIII		TCP Any -> 27960 UDP Any -> 27960	
□ Rainbow Six		TCP Any -> 2436-2438 UDP Any -> 2436-2438	



□ Red Alert		UDP Any -> 5009	
□ Roger Wilco		UDP Any -> 3782	
□ Rogue Spear		TCP Any -> 2346-2348 UDP Any -> 2346-2348	
□ Tanarus		UDP Any -> 1024-1280	
□ The 4th Coming		UDP Any -> 11677 Any -> 11679	
□ Tiberian Sun - Command and Conquer III		UDP Any -> 1234	
□ Total Annihilation		TCP Any -> 1000-4999 UDP Any -> 47624 Any -> 1000-4999	
□ Unreal, Unreal Tournament		UDP Any -> 7777-7779	
□ Unreal - Master Server List		UDP Any -> 27900	
□ Warbirds 2		TCP Any -> 912	
□ Worms 2		TCP Any -> 1031-2210 Any -> 2220-3212 UDP Any -> 1000-1029	
Network Administration Utilities			
□ AUTH - Authentication Server		TCP Any -> 113	
□ Lotus Domino		TCP Any -> 1352	
□ SQL-Net Tools Server		TCP Any -> 1521	
□ SSH - Secured Remote Login		TCP Any -> 22	
□ Timbuktu Pro		TCP Any -> 1417-1420 UDP Any -> 407	
□ Traceroute - Route Tracking Utility		UDP 32769-65535 -> 33434-33523	
□ Microsoft Windows Network / Samba		TCP Any -> 139 Any -> 445 UDP Any -> 137 Any -> 138	
Remote Desktop Utilities			
□ Citrix Winframe Server		TCP Any -> 1494	
□ PCAnywhere		TCP Any -> 5631-5632 UDP Any -> 5631-5632	
□ Remote Desktop 32		TCP Any -> 5044-5050	
□ Remotely Possible V3.2a		TCP Any -> 799	
□ VNC Remote Display System		TCP Any -> 5900-5909 Any -> 5800-5809	
□ Windows Terminal Server/ Windows Remote Desktop		TCP Any -> 3389	
□ X Windows		TCP Any -> 6000-6100	

5.11 Applying Corporate Security

The following set of instructions is designed to assist you in applying corporate security standards to your network. When implementing these instructions, it is important to execute the configuration steps in the exact order they are presented.

To apply corporate Firewall security standards perform the following:

Configure the CAP to permit only HTTPS as a means of remote administration:

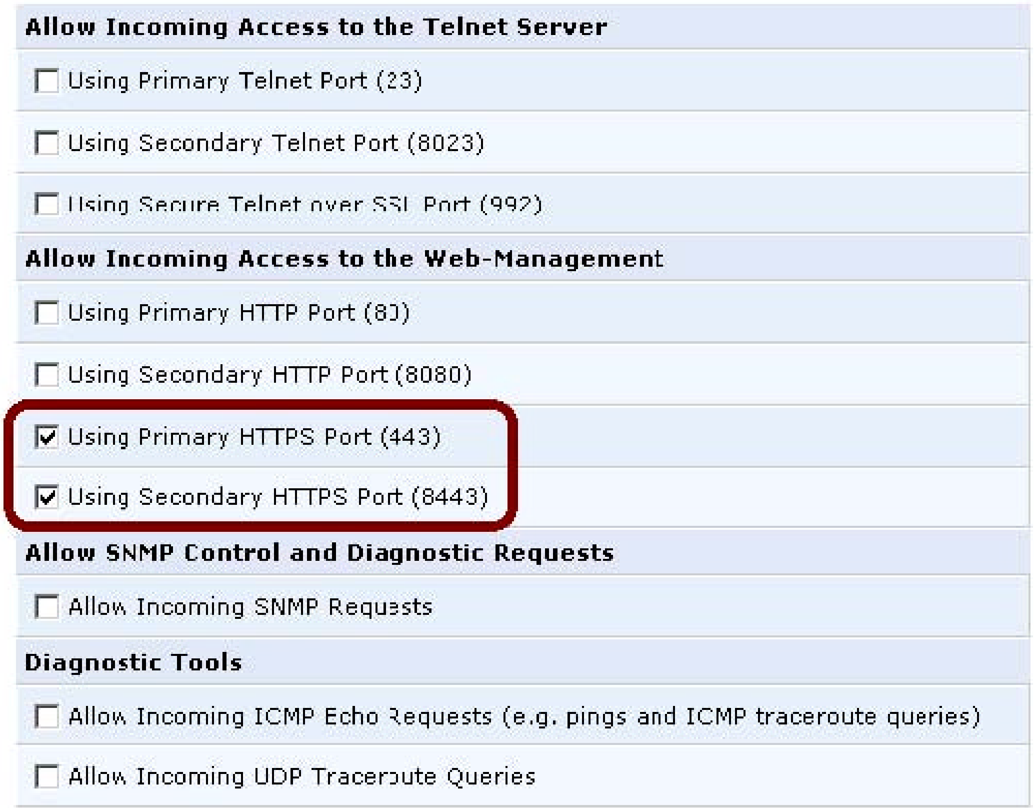
1. Click the ’Security’ icon on the side-bar.

2. Click the ’Remote Administration’ tab.

3. Enable the following check boxes:

- Using Primary HTTPS Port (443)
- Using Secondary HTTPS Port (8443)

4. Press the ’OK’ button.



Allow Incoming Access to the Telnet Server

□ Using Primary Telnet Port (23)

□ Using Secondary Telnet Port (8023)

□ Using Secure Telnet over SSL Port (992)

Allow Incoming Access to the Web-Management

□ Using Primary HTTP Port (80)

□ Using Secondary HTTP Port (8080)

☑ Using Primary HTTPS Port (443)

☑ Using Secondary HTTPS Port (8443)

Allow SNMP Control and Diagnostic Requests

□ Allow Incoming SNMP Requests

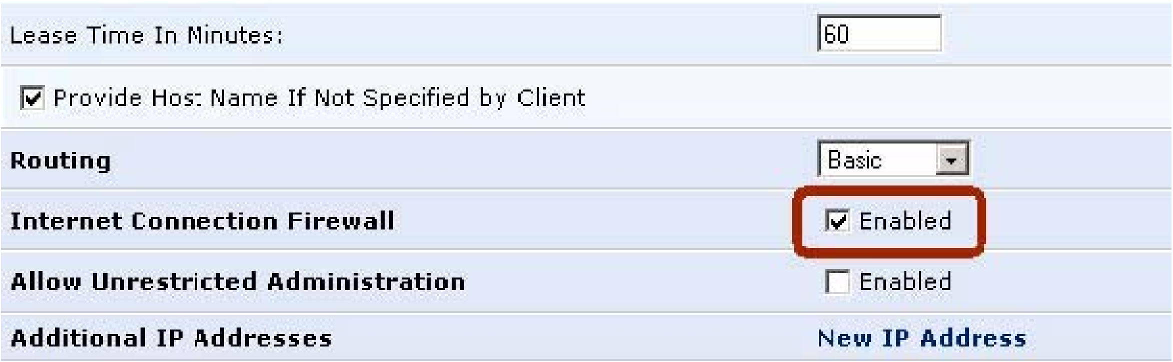
Diagnostic Tools

□ Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)

□ Allow Incoming UDP Traceroute Queries

Apply Firewall protection on the LAN:

1. Click the ’Network Connections’ icon on the side-bar.
2. Click the ’LAN Ethernet’ connection link.
3. Click the ’Settings’ button.
4. Enable the ’Internet Connection Firewall’ check box.
5. Press the ’OK’ button.



Lease Time In Minutes:	60
☑ Provide Host Name If Not Specified by Client	
Routing	Basic
Internet Connection Firewall	☑ Enabled
Allow Unrestricted Administration	□ Enabled
Additional IP Addresses	**New IP Address**

At this point you have set your Firewall to Corporate-Grade Security.

If you wish to allow additional LAN services, or other outbound services, refer to the ’Advanced Filtering’ section 5.10.

6

6.0 QoS Traffic Management Capabilities

One of the major capabilities of the CAP is the ability to guarantee both In-bound and Out-bound Quality of Service for business critical network traffic passing through the CAP.

Every network environment has it's own unique requirements as to which types of applications are absolutely critical to their business, therefore, the QoS capabilities within the CAP have been designed to be extremely flexible to meet each network administrator's unique QoS desires.

An example of how a network would benefit greatly by implementing the CAP's QoS functionality, might be a company desiring to best utilize an existing T1 (1.544Mb/s) WAN link, that is currently supporting the following:

- Time-sensitive data applications (such as Point-of-Sale or Citrix)
- Time-sensitive voice applications (such as an IP-Centrex based VoIP network)
- Dozens of other less business critical and/or time-critical applications (such as recreational Web browsing, gaming, music downloads, etc.).

If this company typically experiences WAN congestion, leading to excessive delays in the delivery of these time-sensitive applications, typically, adding more bandwidth to try and solve the problem doesn't always guaranteed a fix.

Implementing the CAP, a QoS-aware, enterprise class, bandwidth management solution, can guarantee the delivery of business critical traffic both in and out of the enterprise WAN link and solve this problem.

6.1 Configuring QoS in the CAP

In order to configure QoS traffic management parameters in the CAP you must first:

- Understand which applications you need to prioritize through the CAP

- Know how much total bandwidth is available on the entire WAN link

- If implementing VoIP, be able to define how many calls of each type of codec you need to concurrently support

- Know which applications are business critical, and need be allocated guaranteed amounts of the available WAN bandwidth

- Define which of the business critical applications are the most time-sensitive, and will require higher prioritization than others

This section is documented as a configuration example, to show the relationship between the screens as clearly as possible

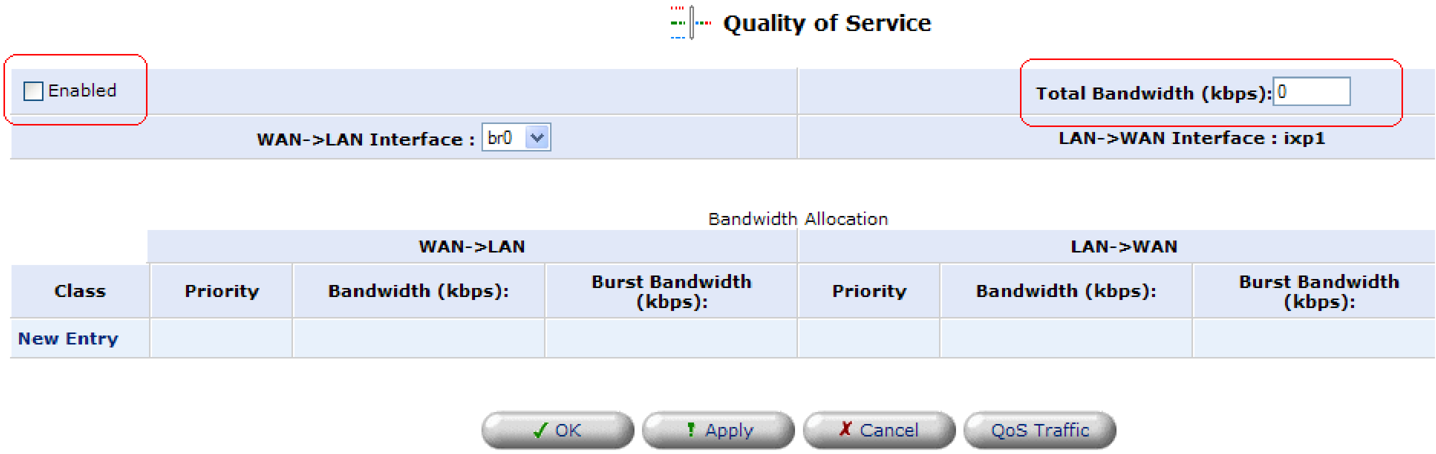
The example configuration below is based on the following requirements:

- Total of 1.536 Mbps WAN bandwidth available
- 6 * G.711 SIP signaled VoIP calls need to be supported with highest priority
- 256 Kbps required for Citrix, and require the 2nd highest priority behind VoIP
- All other traffic to share remaining bandwidth as "best effort"

(Note: You'll also need to have a defined plan such as shown in this example for your own specific network environment and requirements)

To input the configuration supporting the above requirements:

Start by selecting the 'Quality of Service' icon on the left side of the screen. This will launch the main QoS screen.



Quality of Service

☐ Enabled

Total Bandwidth (kbps): 0

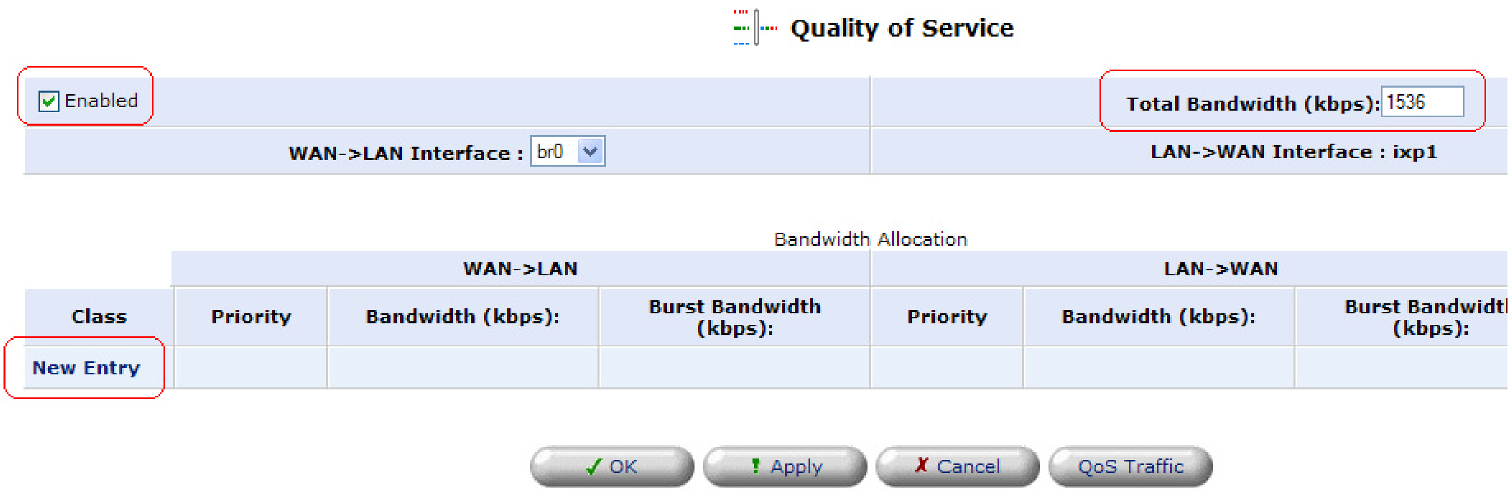
WAN->LAN Interface : br0

LAN->WAN Interface : ixp1

Bandwidth Allocation

	WAN->LAN			LAN->WAN		
Class	Priority	Bandwidth (kbps):	Burst Bandwidth (kbps):	Priority	Bandwidth (kbps):	Burst Bandwidth (kbps):
New Entry						

Click on the ‘Enabled’ box to activate QoS on the CAP, then define the total amount of bandwidth that is available in the “Total Bandwidth’ box. This value is entered in kbps, therefore, a T1 would be entered at ‘1536’ (and a 384Kbps link would be ‘384’).



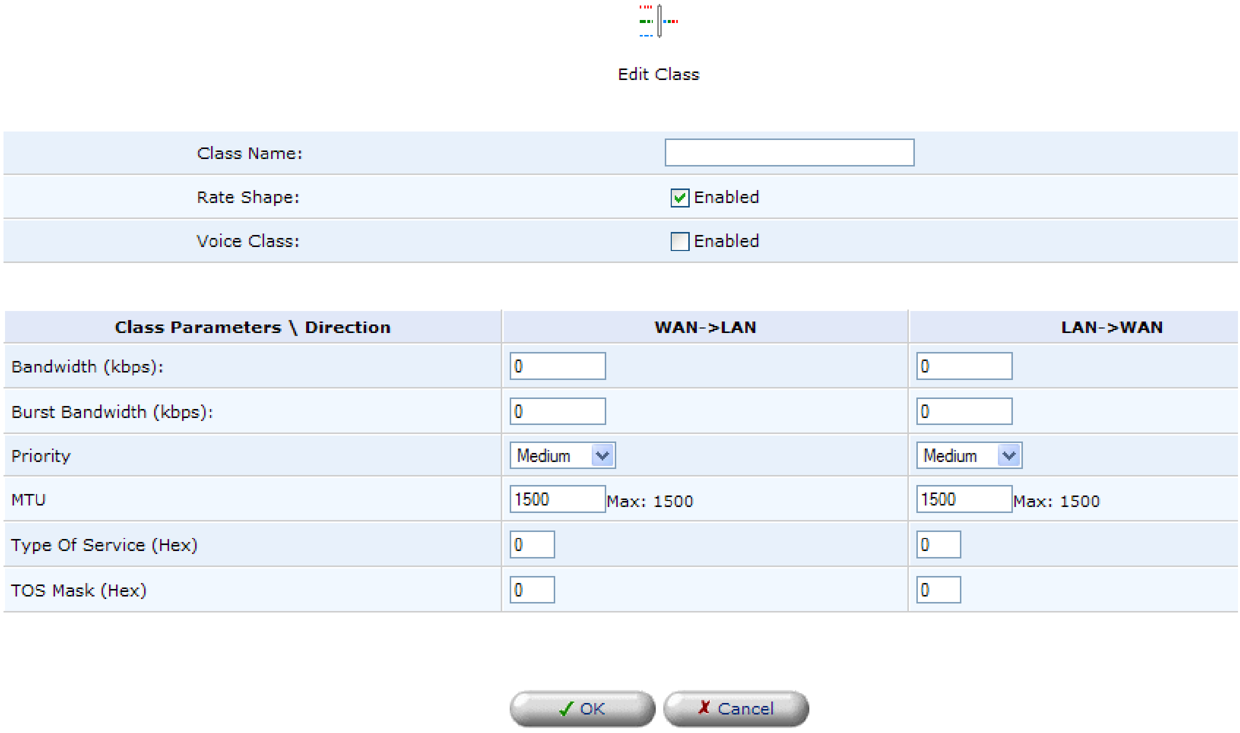
Quality of Service

☑ Enabled	Total Bandwidth (kbps): 1536
WAN->LAN Interface : br0	LAN->WAN Interface : ixp1

Bandwidth Allocation

	WAN->LAN			LAN->WAN		
Class	Priority	Bandwidth (kbps):	Burst Bandwidth (kbps):	Priority	Bandwidth (kbps):	Burst Bandwidt (kbps):
New Entry						

Next, click on ‘New Entry’, to take you to the Class definition screen. You will create a ‘New Entry’ for each class you need to support in the CAP, including a ‘Default’ class to catch all other traffic that is not being prioritized by QoS.



Edit Class

Class Name:	
Rate Shape:	☑ Enabled
Voice Class:	□ Enabled

Class Parameters \ Direction	WAN->LAN	LAN->WAN
Bandwidth (kbps):	0	0
Burst Bandwidth (kbps):	0	0
Priority	Medium	Medium
MTU	1500 Max: 1500	1500 Max: 1500
Type Of Service (Hex)	0	0
TOS Mask (Hex)	0	0

Define the ‘Default’ class:

- Give it a Class Name. ‘Default’ would probably be best for this class, but you can call it whatever name makes the most sense to you.

- Leave ‘Rate Shape’ enabled. This will ensure that the CAP will be authorized to slow down bursty data traffic as required to support time sensitive traffic such as the VoIP.

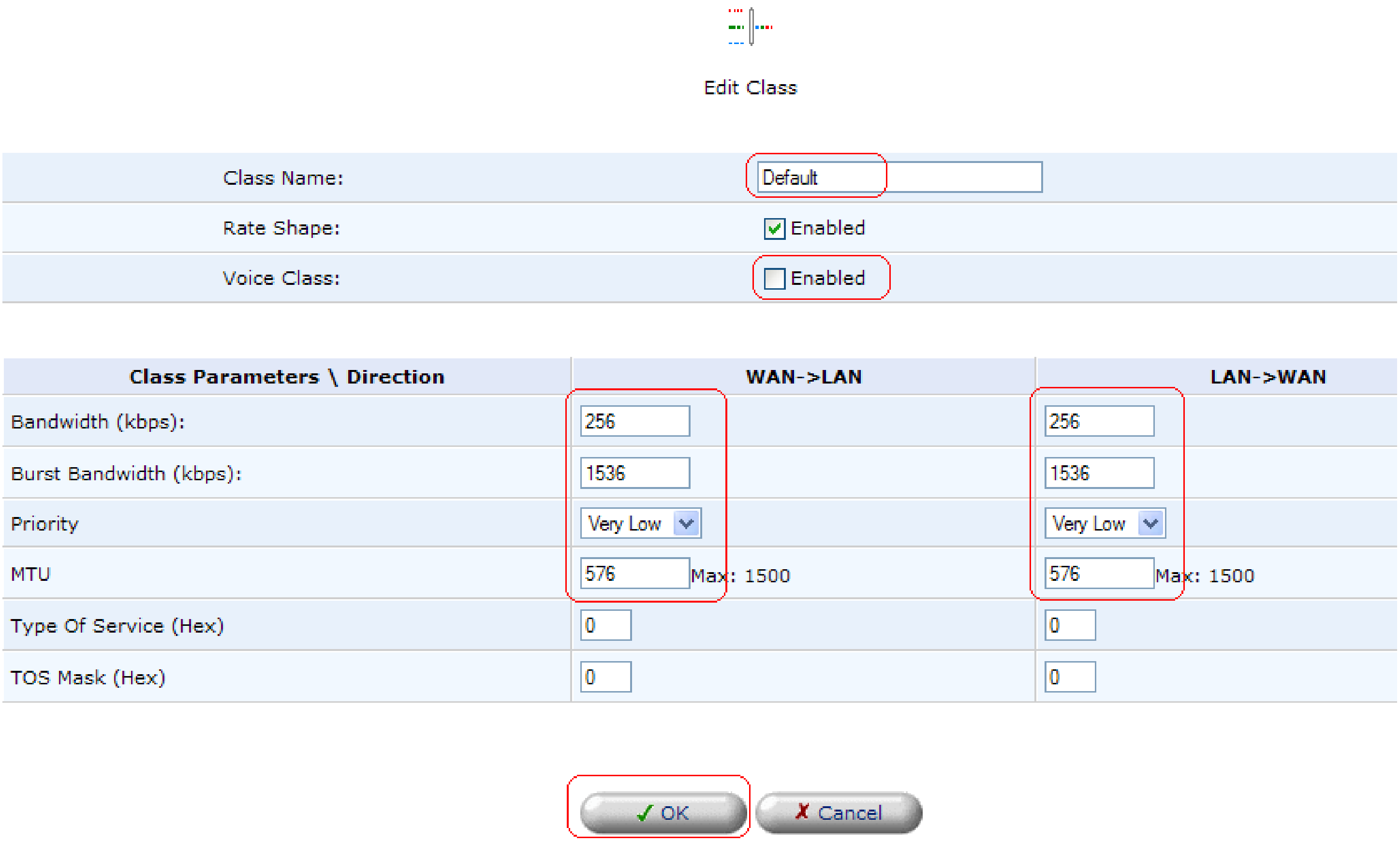
- If you will be supporting a VoIP class, you should also limit the MTU of this class to 576 Bytes, to ensure that voice traffic has the shortest queuing times, while providing for the least amount of data re-transmissions in the best effort/’Default’ class.

- Don’t click the ‘Voice Class’ box, as this is not a voice class (more on this later)

- Set the guaranteed ‘Bandwidth (kbps)’ to 256

- Set the ‘Burst Bandwidth (kbps)’ to the maximum link bandwidth, which is 1536. If other, higher priority traffic is not using their allocated bandwidth, other lower priority traffic such as this ‘Default’ class can use it

- Set the ‘Priority’ at the lowest priority setting (ie. Very Low = lowest of the 5 classes)



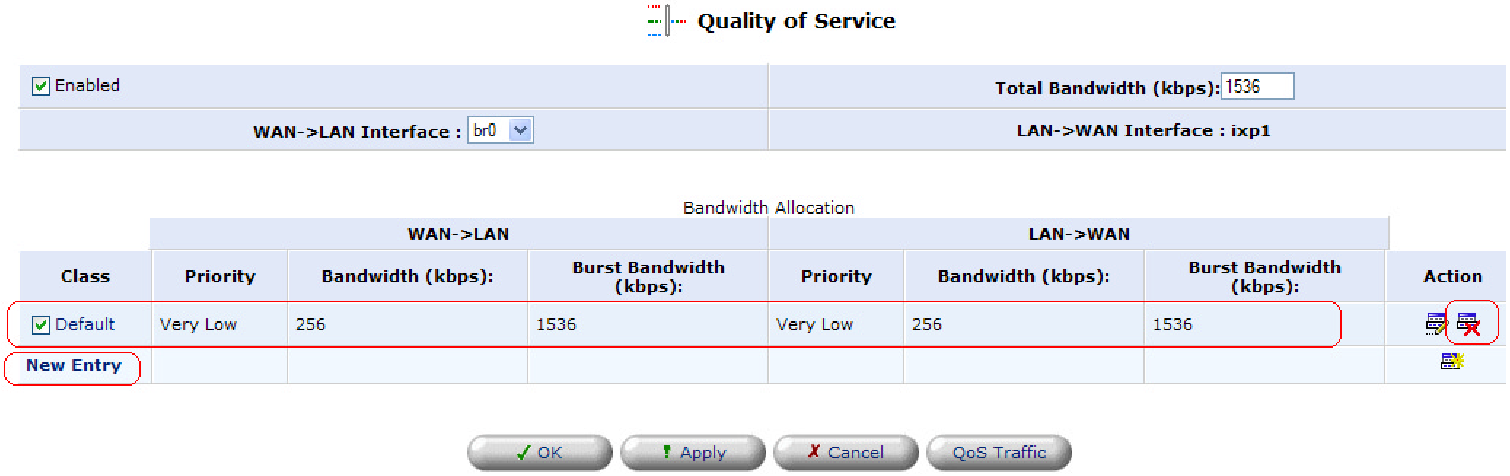
Edit Class

Class Name:	Default
Rate Shape:	☑ Enabled
Voice Class:	□ Enabled

Class Parameters \ Direction	WAN->LAN	LAN->WAN
Bandwidth (kbps):	256	256
Burst Bandwidth (kbps):	1536	1536
Priority	Very Low	Very Low
MTU	576 Max: 1500	576 Max: 1500
Type Of Service (Hex)	0	0
TOS Mask (Hex)	0	0

- Click ‘OK’ to accept these settings for the ‘Default’ class

- You now have a ‘Default’ class defined on the CAP. If you made a mistake, you can either completely delete the class by clicking the ‘delete icon’ to the right of the new ‘Default’ class, or click on the class itself or ‘edit button’ to edit it. Next, click on ‘New Entry” again to define your Citrix class.



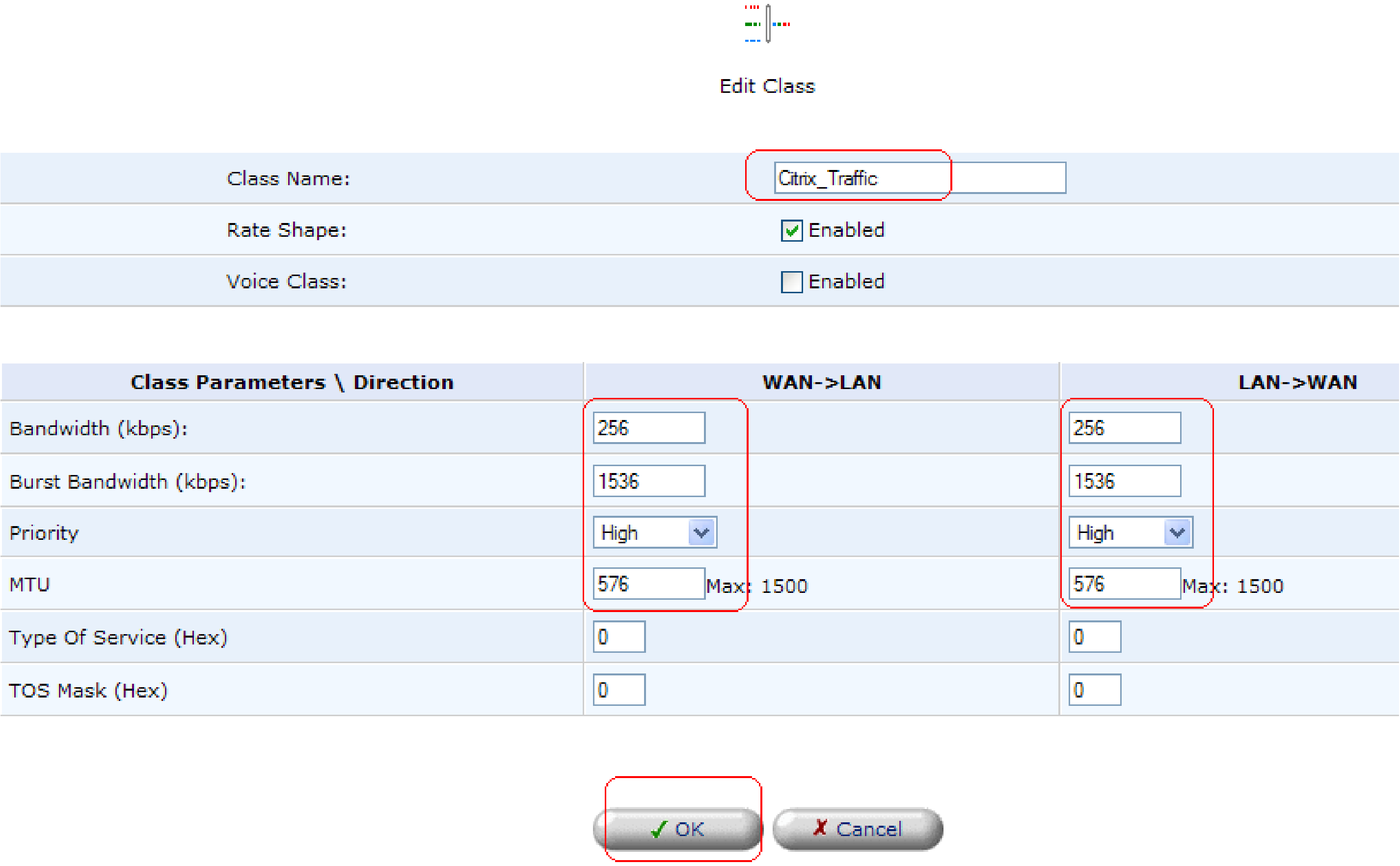
Quality of Service

☑ Enabled	Total Bandwidth (kbps): 1536
WAN->LAN Interface : br0	LAN->WAN Interface : ixp1

Bandwidth Allocation

	WAN->LAN			LAN->WAN			
Class	Priority	Bandwidth (kbps):	Burst Bandwidth (kbps):	Priority	Bandwidth (kbps):	Burst Bandwidth (kbps):	Action
☑ Default	Very Low	256	1536	Very Low	256	1536	
New Entry							

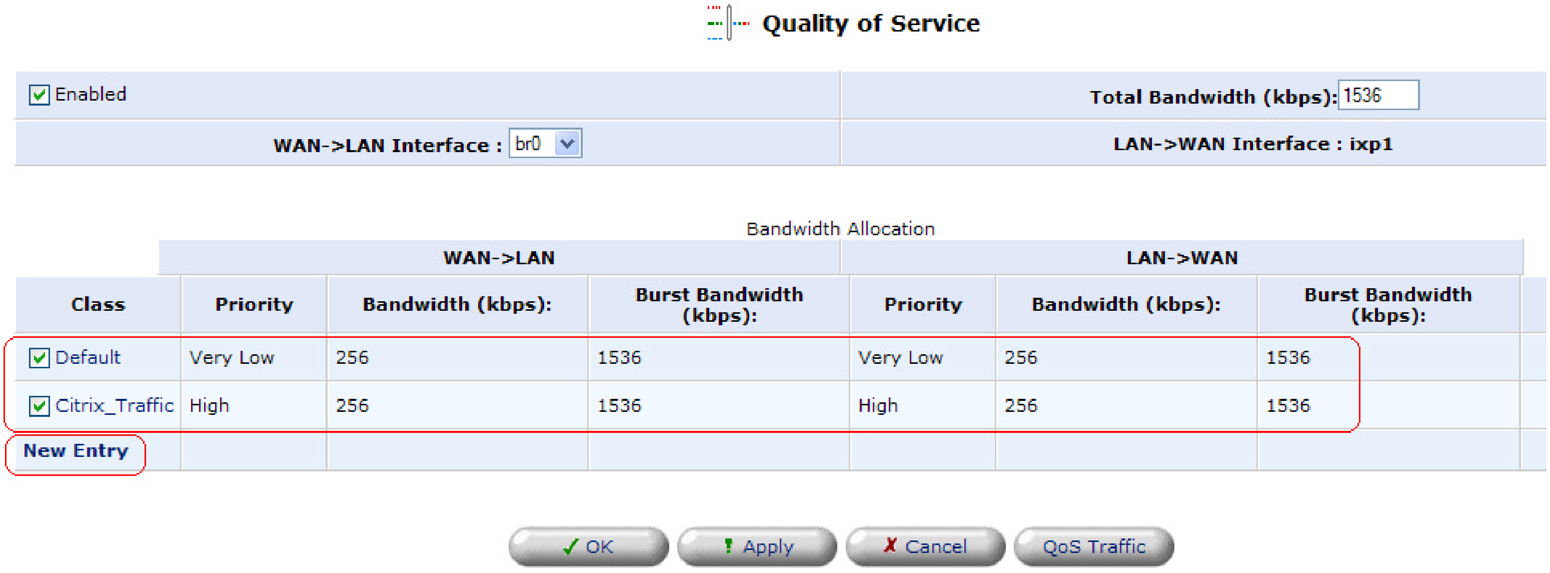
Define your ‘Citrix Traffic’ class, using the same principles as you did for the ‘Default’ class above, except increase the ‘Priority’ to ‘High’, and setting the Guaranteed ‘Bandwidth’ to 256 (kbps), as required in our planning. Click on ‘OK’.



Edit Class

Class Name:	Citrix_Traffic
Rate Shape:	☑ Enabled
Voice Class:	□ Enabled

Class Parameters \ Direction	WAN->LAN	LAN->WAN
Bandwidth (kbps):	256	256
Burst Bandwidth (kbps):	1536	1536
Priority	High	High
MTU	576 Max: 1500	576 Max: 1500
Type Of Service (Hex)	0	0
TOS Mask (Hex)	0	0



Quality of Service

☑ Enabled	Total Bandwidth (kbps): 1536
WAN->LAN Interface : br0	LAN->WAN Interface : ixp1

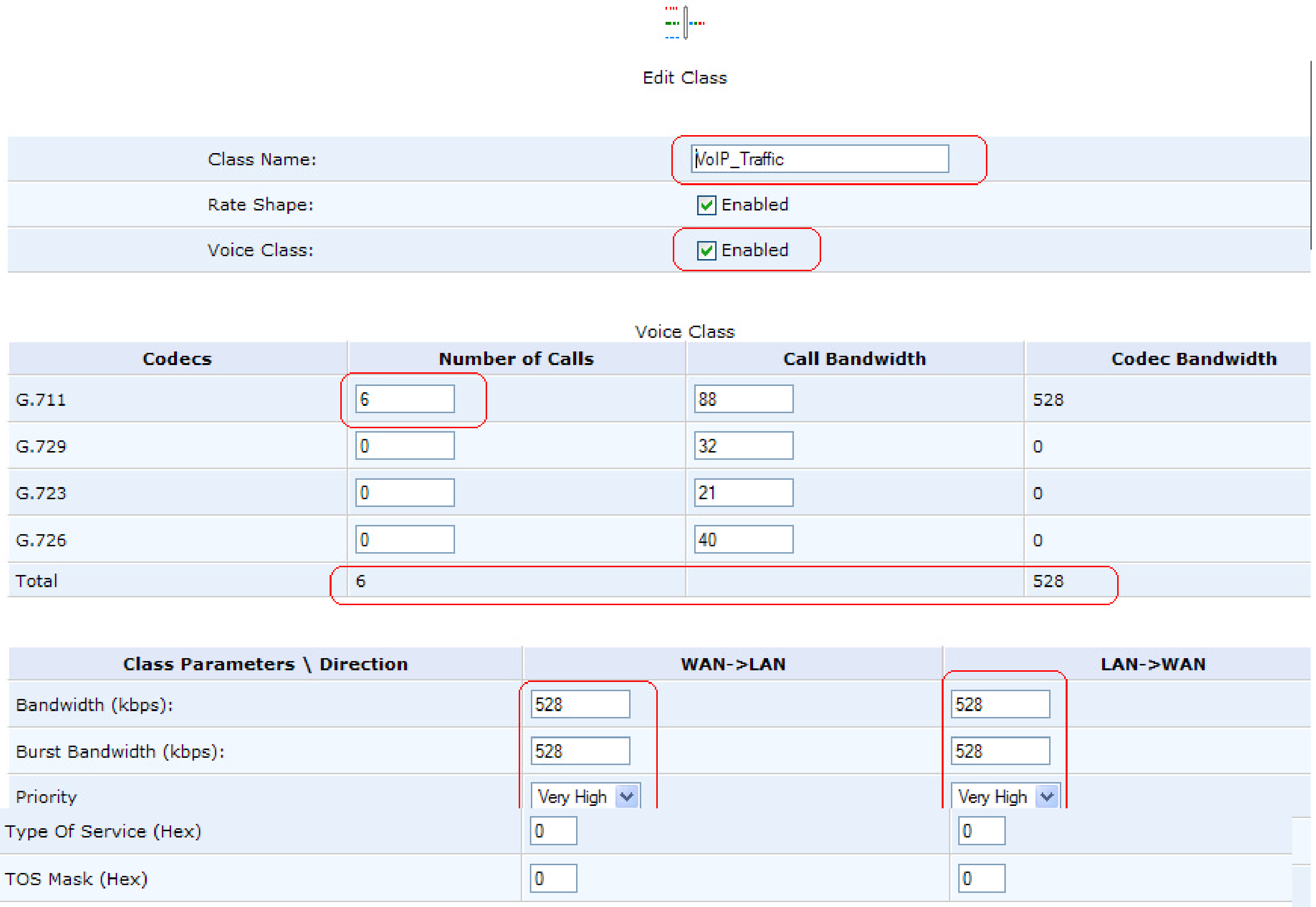
Bandwidth Allocation

	WAN->LAN			LAN->WAN		
Class	Priority	Bandwidth (kbps):	Burst Bandwidth (kbps):	Priority	Bandwidth (kbps):	Burst Bandwidth (kbps):
☑ Default	Very Low	256	1536	Very Low	256	1536
☑ Citrix_Traffic	High	256	1536	High	256	1536
New Entry						

Click on ‘New Entry’ once more to create your ‘VoIP Traffic’ class.

Define your ‘VoIP’ class:

- Enter a ‘Class Name’ – ie. ‘VoIP_Traffic’ or whatever you prefer.
- Select ‘Voice Class’ - This tells the CAP to open up a larger set of parameters that are specific to VoIP traffic, allowing you to provide fine detail in the VoIP class.



Edit Class

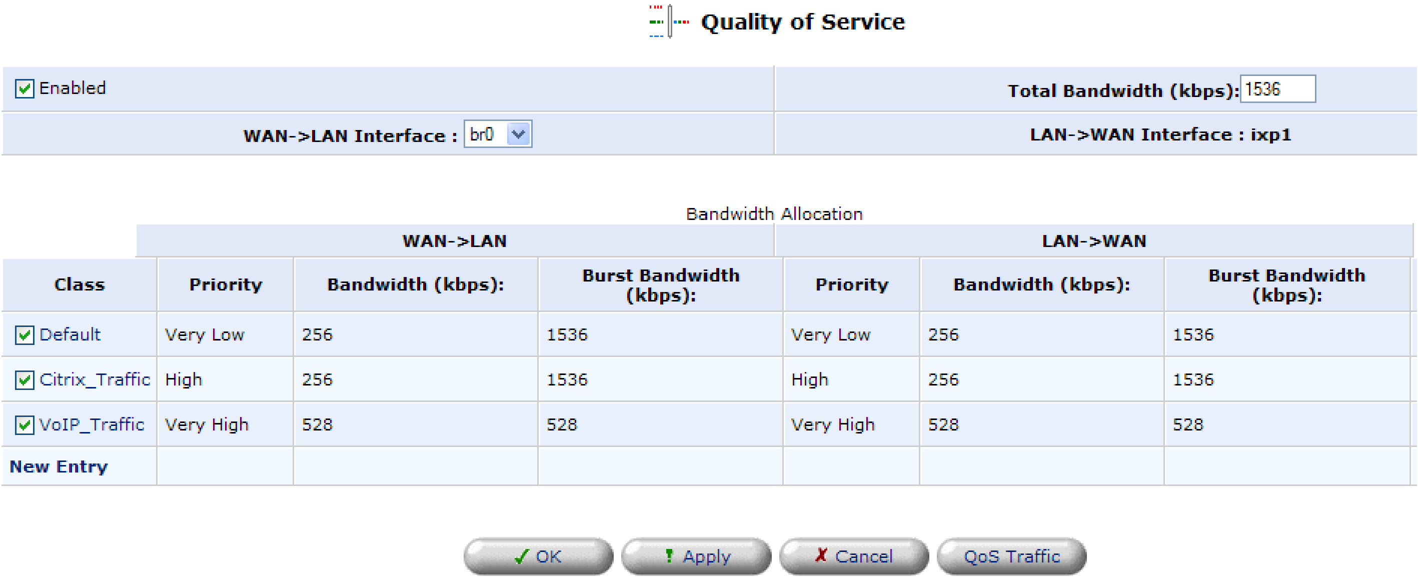
Class Name:	VoIP_Traffic
Rate Shape:	☑ Enabled
Voice Class:	☑ Enabled

Voice Class

Codecs	Number of Calls	Call Bandwidth	Codec Bandwidth
G.711	6	88	528
G.729	0	32	0
G.723	0	21	0
G.726	0	40	0
Total	6		528

Class Parameters \ Direction	WAN->LAN	LAN->WAN
Bandwidth (kbps):	528	528
Burst Bandwidth (kbps):	528	528
Priority	Very High	Very High
Type Of Service (Hex)	0	0
TOS Mask (Hex)	0	0

Summary of all 3 classes we've defined.



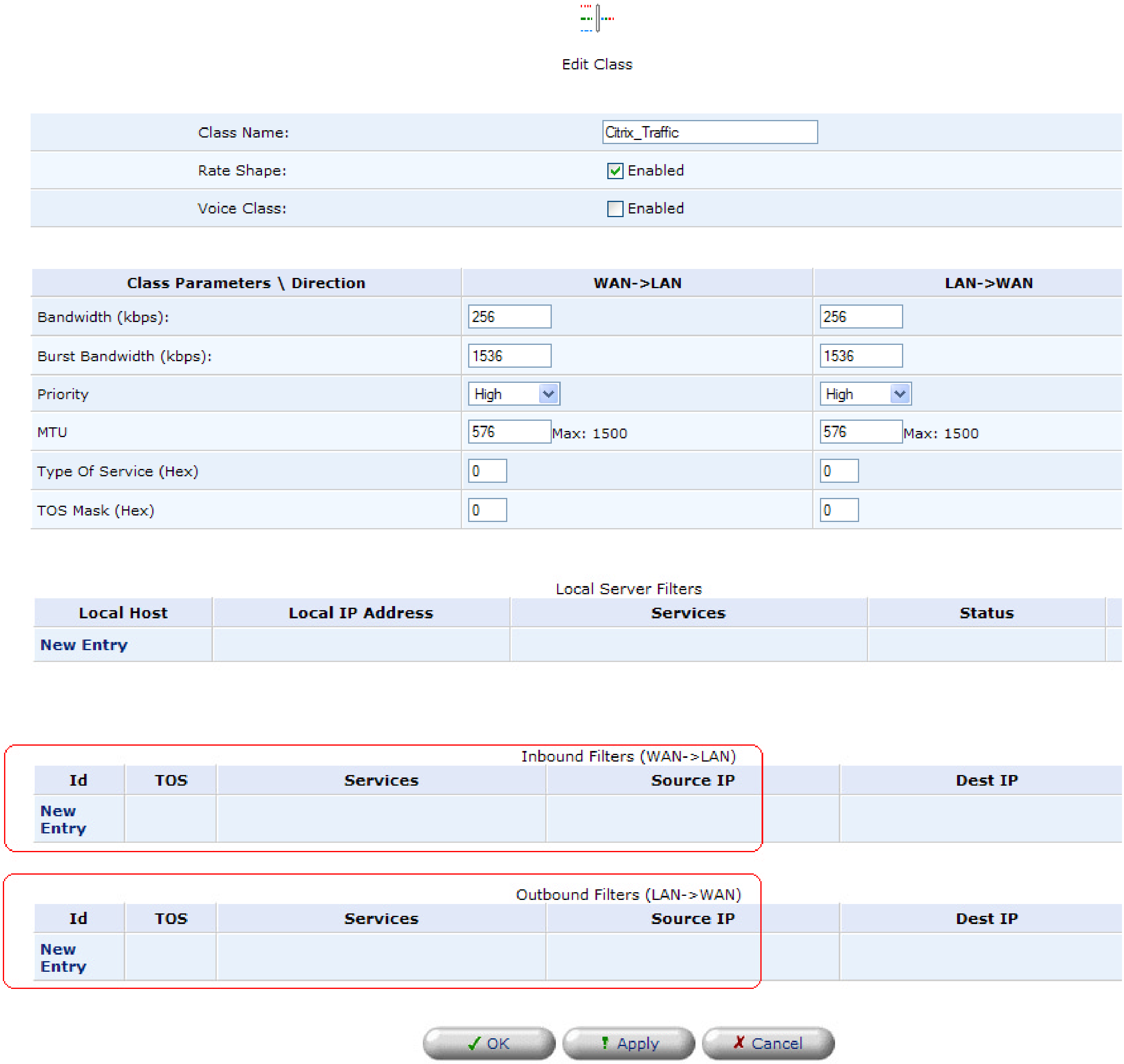
Quality of Service

☑ Enabled	Total Bandwidth (kbps): 1536
WAN->LAN Interface : br0	LAN->WAN Interface : ixp1

Bandwidth Allocation

	WAN->LAN			LAN->WAN		
Class	Priority	Bandwidth (kbps):	Burst Bandwidth (kbps):	Priority	Bandwidth (kbps):	Burst Bandwidth (kbps):
☑ Default	Very Low	256	1536	Very Low	256	1536
☑ Citrix_Traffic	High	256	1536	High	256	1536
☑ VoIP_Traffic	Very High	528	528	Very High	528	528
New Entry						

Next, you need to define what specific traffic is in your two non-Default classes. Click on the 'Citrix_Traffic' class to begin. At the bottom of the screen, you'll notice that you can now see items to click on to allow you to define this class' traffic further.



Edit Class

Class Name:	Citrix_Traffic
Rate Shape:	☑ Enabled
Voice Class:	□ Enabled

Class Parameters \ Direction	WAN->LAN	LAN->WAN
Bandwidth (kbps):	256	256
Burst Bandwidth (kbps):	1536	1536
Priority	High	High
MTU	576 Max: 1500	576 Max: 1500
Type Of Service (Hex)	0	0
TOS Mask (Hex)	0	0

Local Server Filters

Local Host	Local IP Address	Services	Status
New Entry			

Inbound Filters (WAN->LAN)

Id	TOS	Services	Source IP	Dest IP
New Entry				

Outbound Filters (LAN->WAN)

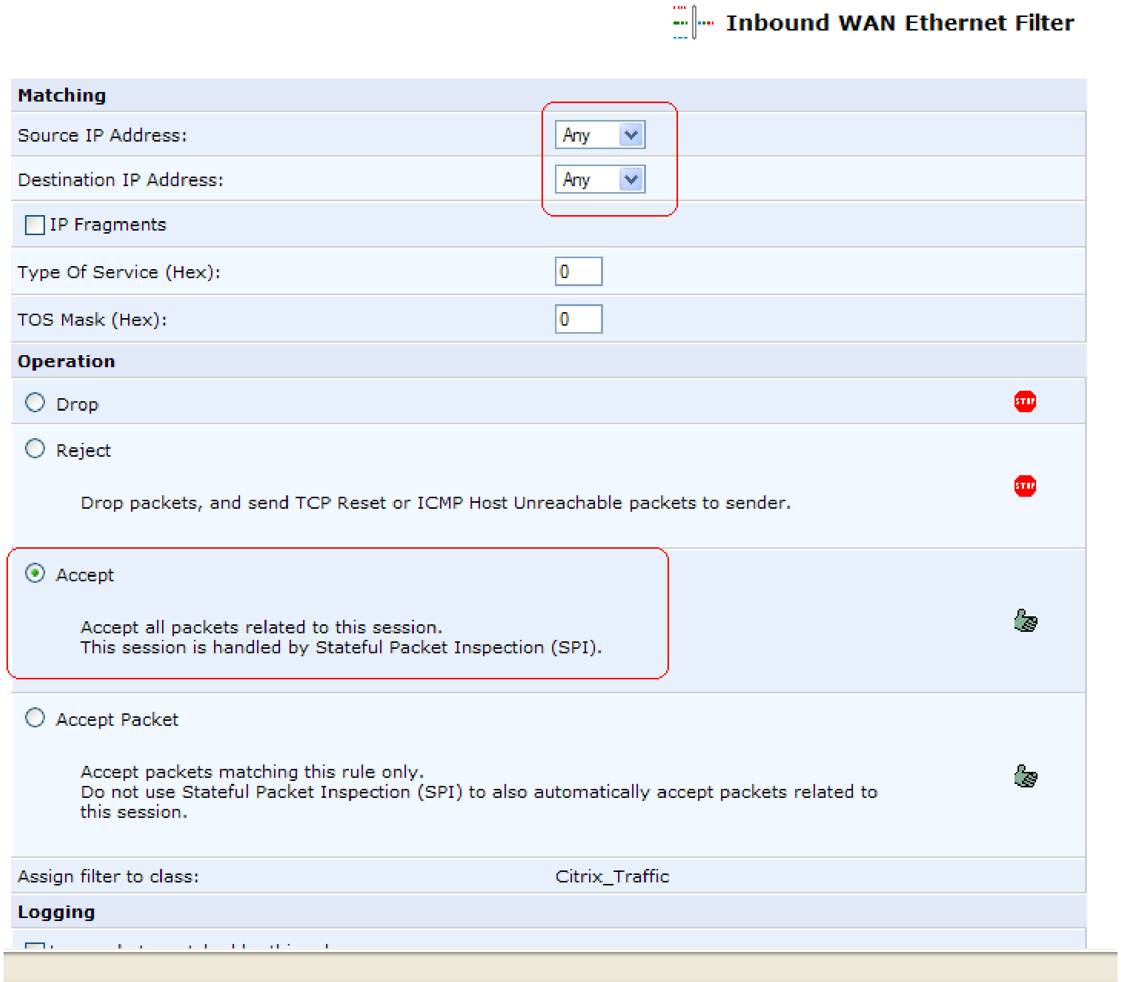
Id	TOS	Services	Source IP	Dest IP
New Entry				

Click on ‘New Entry’ in the ‘Inbound Filters (WAN → LAN) area. You can specify the Source IP and Destination IP to be ANY, SINGLE, or RANGE. For this example, we’ll leave these as ANY, but you can define this to meet your filtering requirements.

Note: You can filter traffic applicable to the class based upon TOS settings already existing on incoming traffic. You can define how many bits to match, and what the bits should have in them, to be applicable to this class of traffic. Also, if you not only specify the TOS marking requirements, but also specify additional data application information below this in the filter, it results in an AND’ing of the two (or more). What this means is that the incoming traffic MUST match BOTH the TOS requirements and the application protocol, to be traffic applicable to this class filter.

Select ‘Accept’, as we will be accepting this traffic in this class. Then, either scroll down until you find ‘Citrix Winframe Server’, or on your web browser, do an ‘Edit/Find on this page’ for ‘Citrix’, to locate the box to check to make this a Citrix class.

Note: If a particular class needs to support more than one application, just make the class name something common to all the traffic types. Then click on all of the appropriate boxes in the filter selection area (see filter area on the next page) to combine all of them into one single class definition.



Inbound WAN Ethernet Filter

Matching

Source IP Address:	Any
Destination IP Address:	Any
□ IP Fragments	
Type Of Service (Hex):	0
TOS Mask (Hex):	0

Operation

○ Drop

○ Reject

Drop packets, and send TCP Reset or ICMP Host Unreachable packets to sender.

● Accept

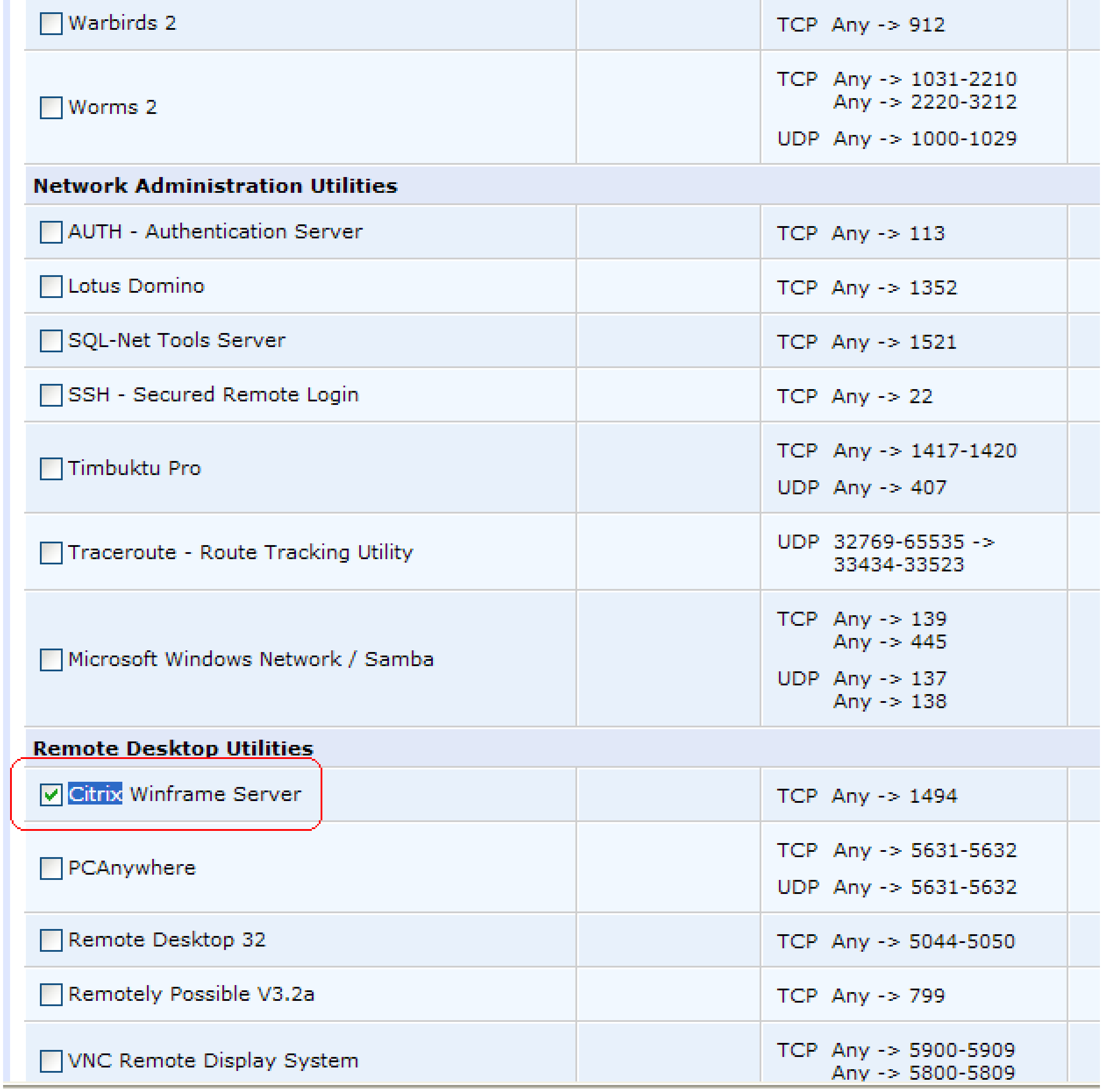
Accept all packets related to this session.
This session is handled by Stateful Packet Inspection (SPI).

○ Accept Packet

Accept packets matching this rule only.
Do not use Stateful Packet Inspection (SPI) to also automatically accept packets related to this session.

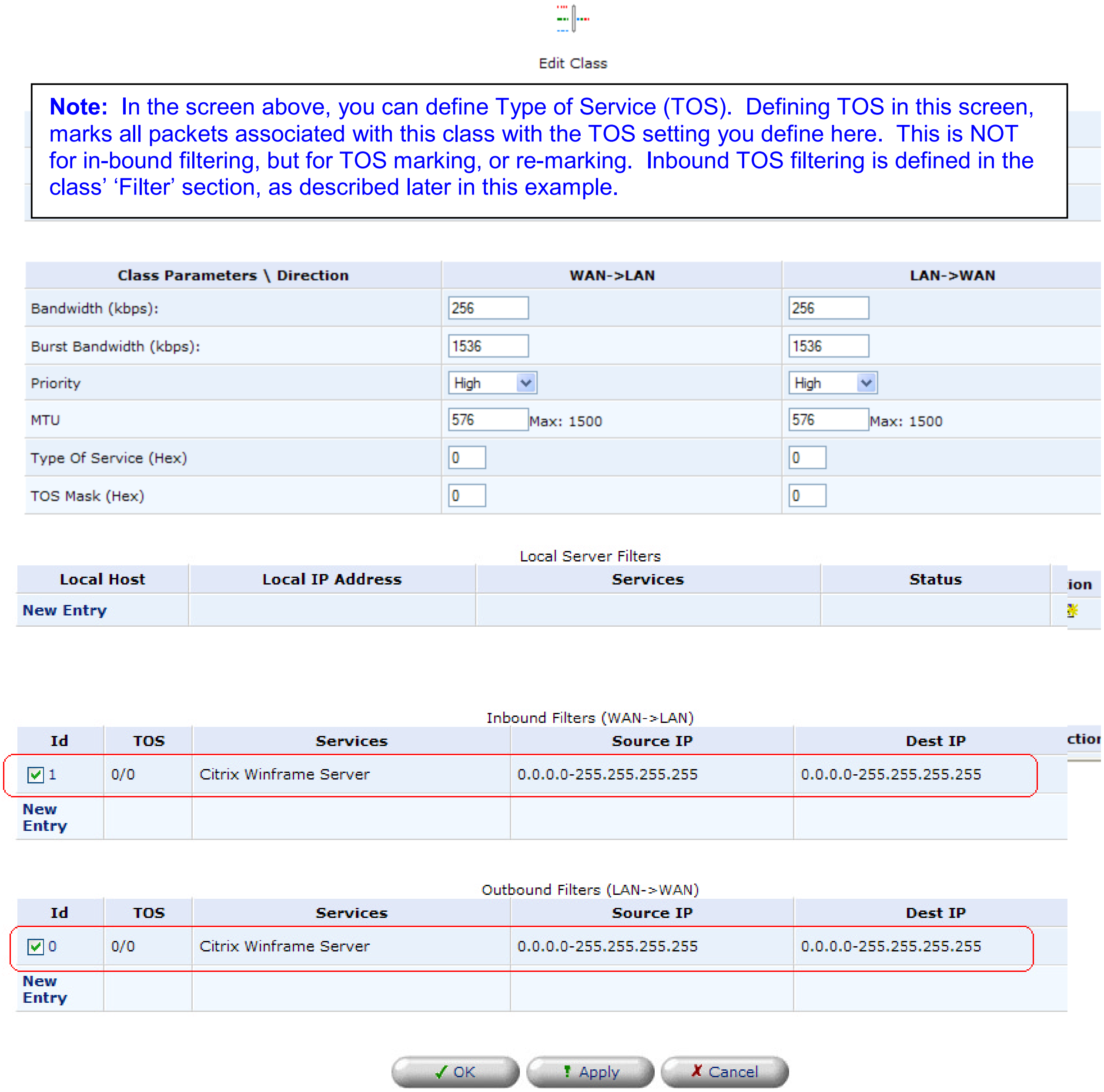
Assign filter to class: Citrix_Traffic

Logging



□ Warbirds 2		TCP Any -> 912	
□ Worms 2		TCP Any -> 1031-2210 Any -> 2220-3212 UDP Any -> 1000-1029	
Network Administration Utilities			
□ AUTH - Authentication Server		TCP Any -> 113	
□ Lotus Domino		TCP Any -> 1352	
□ SQL-Net Tools Server		TCP Any -> 1521	
□ SSH - Secured Remote Login		TCP Any -> 22	
□ Timbuktu Pro		TCP Any -> 1417-1420 UDP Any -> 407	
□ Traceroute - Route Tracking Utility		UDP 32769-65535 -> 33434-33523	
□ Microsoft Windows Network / Samba		TCP Any -> 139 Any -> 445 UDP Any -> 137 Any -> 138	
Remote Desktop Utilities			
☑ Citrix Winframe Server		TCP Any -> 1494	
□ PCAnywhere		TCP Any -> 5631-5632 UDP Any -> 5631-5632	
□ Remote Desktop 32		TCP Any -> 5044-5050	
□ Remotely Possible V3.2a		TCP Any -> 799	
□ VNC Remote Display System		TCP Any -> 5900-5909 Any -> 5800-5809	

Click OK. Then do the same for your 'Outbound Filters (LAN → WAN), if required. Returning back to your 'Citrix_Traffic' screen will show the following.



Note: In the screen above, you can define Type of Service (TOS). Defining TOS in this screen, marks all packets associated with this class with the TOS setting you define here. This is NOT for in-bound filtering, but for TOS marking, or re-marking. Inbound TOS filtering is defined in the class' 'Filter' section, as described later in this example.

Edit Class

Class Parameters \ Direction	WAN->LAN	LAN->WAN
Bandwidth (kbps):	256	256
Burst Bandwidth (kbps):	1536	1536
Priority	High	High
MTU	576 Max: 1500	576 Max: 1500
Type Of Service (Hex)	0	0
TOS Mask (Hex)	0	0

Local Server Filters

Local Host	Local IP Address	Services	Status	ion
New Entry				

Inbound Filters (WAN->LAN)

Id	TOS	Services	Source IP	Dest IP	ctior
☑ 1	0/0	Citrix Winframe Server	0.0.0.0-255.255.255.255	0.0.0.0-255.255.255.255	
New Entry					

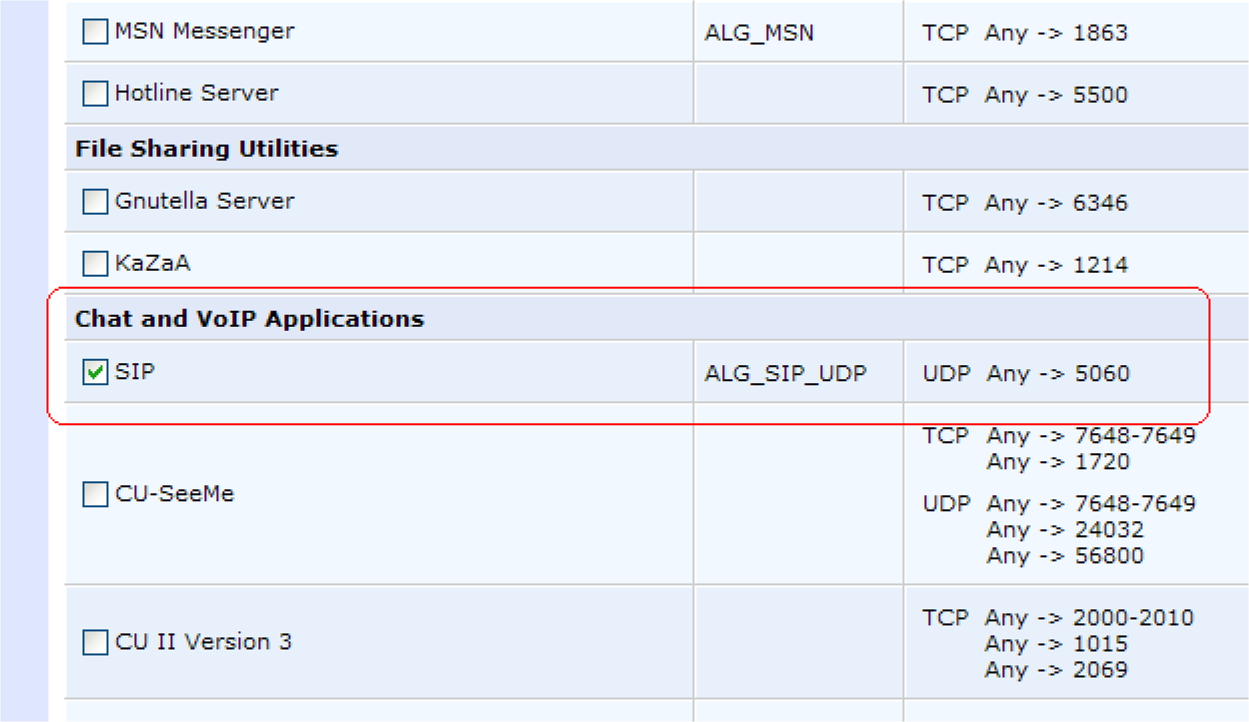
Outbound Filters (LAN->WAN)

Id	TOS	Services	Source IP	Dest IP
☑ 0	0/0	Citrix Winframe Server	0.0.0.0-255.255.255.255	0.0.0.0-255.255.255.255
New Entry				

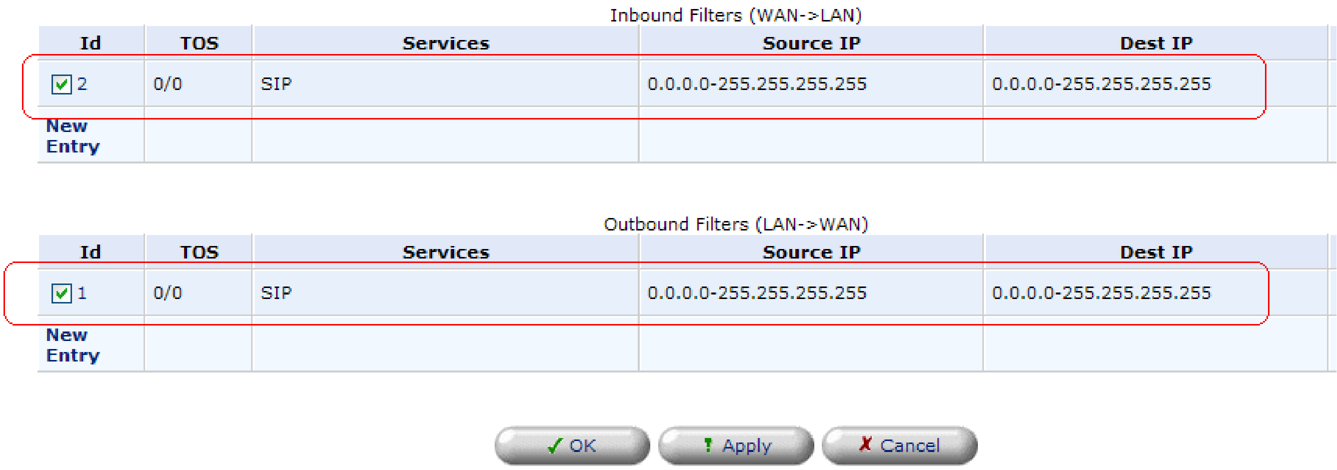
- Click ‘Apply’ then ‘OK’ to save and exit from this screen.

When you hit ‘OK’, you are returned to the QoS screen.

Click on your ‘VoIP_Traffic” class to define the SIP traffic specific to this class. The principle is exactly the same as the ‘Citrix_Traffic” class, except this time, we’ll specify the application is ‘SIP’. The ALG’s in the CAP, include a SIP ALG, therefore, the CAP is intelligent enough to know that when a SIP call is initiated, there will be RTP and RTCP associated with it. Therefore, you do not have to check any boxes other than ‘SIP’. The screen below shows the ‘SIP’ ALG selection.



□ MSN Messenger	ALG_MSN	TCP Any -> 1863
□ Hotline Server		TCP Any -> 5500
File Sharing Utilities		
□ Gnutella Server		TCP Any -> 6346
□ KaZaA		TCP Any -> 1214
Chat and VoIP Applications		
☑ SIP	ALG_SIP_UDP	UDP Any -> 5060
□ CU-SeeMe		TCP Any -> 7648-7649 Any -> 1720 UDP Any -> 7648-7649 Any -> 24032 Any -> 56800
□ CU II Version 3		TCP Any -> 2000-2010 Any -> 1015 Any -> 2069



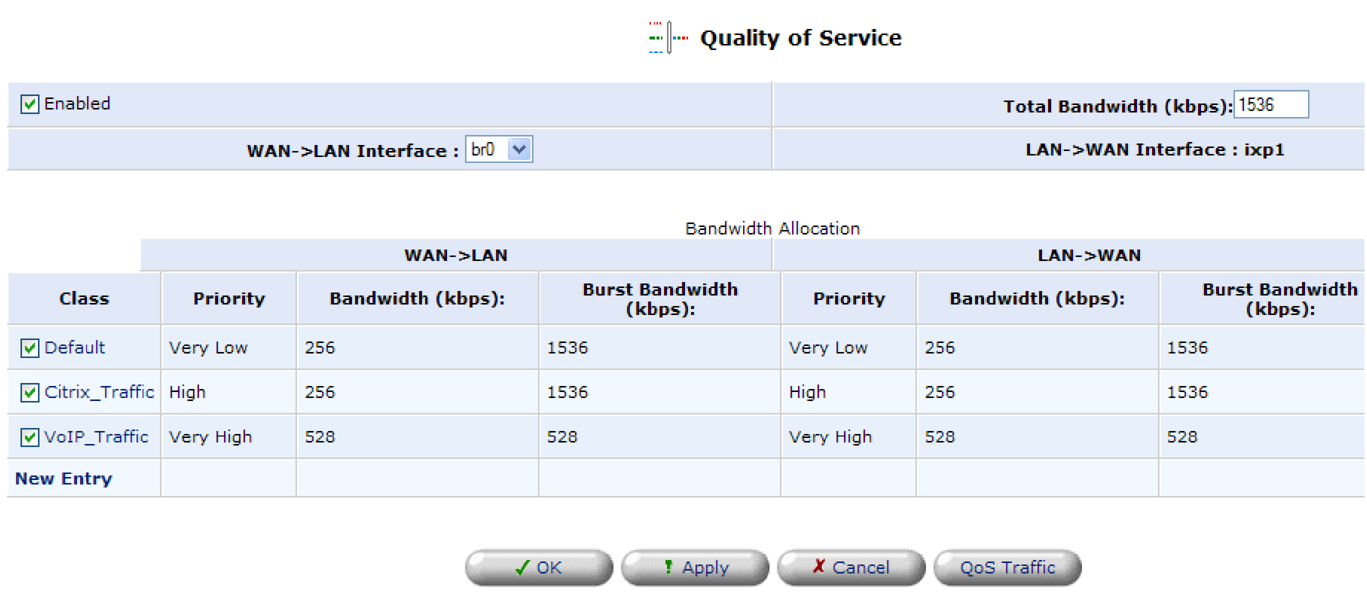
Inbound Filters (WAN->LAN)

Id	TOS	Services	Source IP	Dest IP
☑ 2	0/0	SIP	0.0.0.0-255.255.255.255	0.0.0.0-255.255.255.255
New Entry				

Outbound Filters (LAN->WAN)

Id	TOS	Services	Source IP	Dest IP
☑ 1	0/0	SIP	0.0.0.0-255.255.255.255	0.0.0.0-255.255.255.255
New Entry				

QoS has been defined for all 3 classes. Click ‘Apply’. Click on ‘QoS Traffic’ to see statistics on the QoS traffic classes.



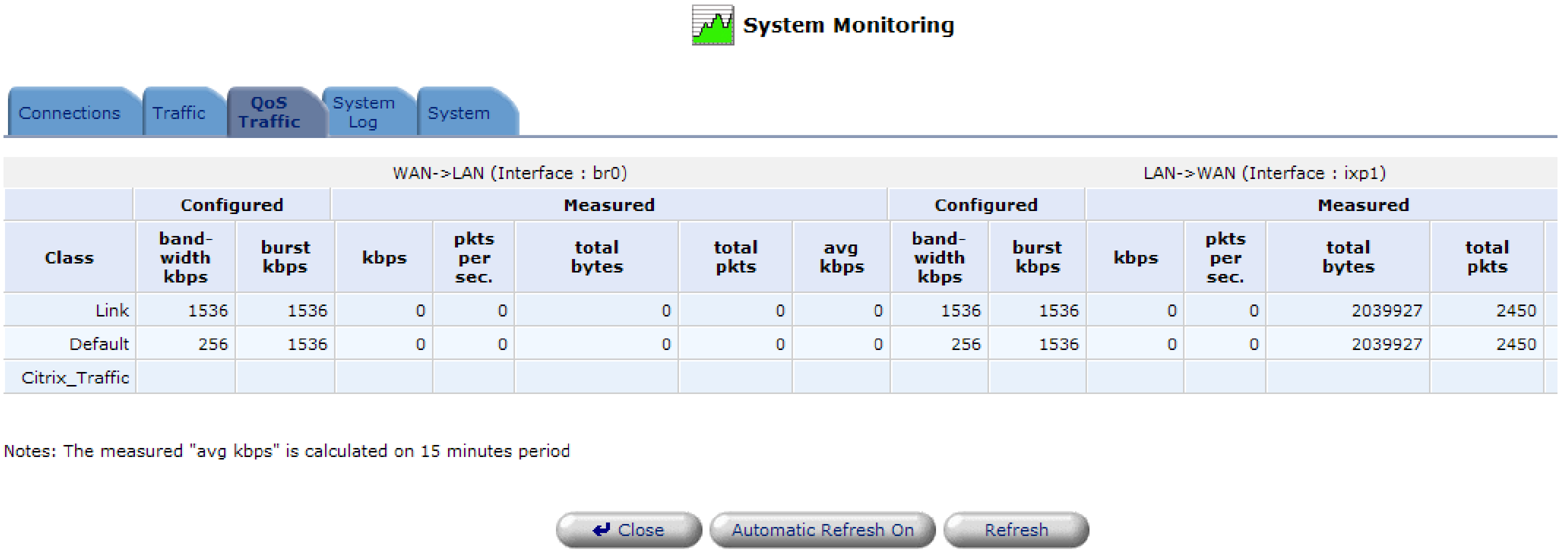
Quality of Service

☑ Enabled	Total Bandwidth (kbps): 1536
WAN->LAN Interface : br0	LAN->WAN Interface : ixp1

Bandwidth Allocation

	WAN->LAN			LAN->WAN		
Class	**Priority**	**Bandwidth (kbps):**	**Burst Bandwidth (kbps):**	**Priority**	**Bandwidth (kbps):**	**Burst Bandwidth (kbps):**
☑ Default	Very Low	256	1536	Very Low	256	1536
☑ Citrix_Traffic	High	256	1536	High	256	1536
☑ VoIP_Traffic	Very High	528	528	Very High	528	528
New Entry						

QoS traffic monitoring. If you click on ‘Automatic Refresh’, it will update statistics on this screen about every 15 seconds.



System Monitoring

	WAN->LAN (Interface : br0)							LAN->WAN (Interface : ixp1)					
	Configured		**Measured**					**Configured**		**Measured**			
Class	**band-width kbps**	**burst kbps**	**kbps**	**pkts per sec.**	**total bytes**	**total pkts**	**avg kbps**	**band-width kbps**	**burst kbps**	**kbps**	**pkts per sec.**	**total bytes**	**total pkts**
Link	1536	1536	0	0	0	0	0	1536	1536	0	0	2039927	2450
Default	256	1536	0	0	0	0	0	256	1536	0	0	2039927	2450
Citrix_Traffic													

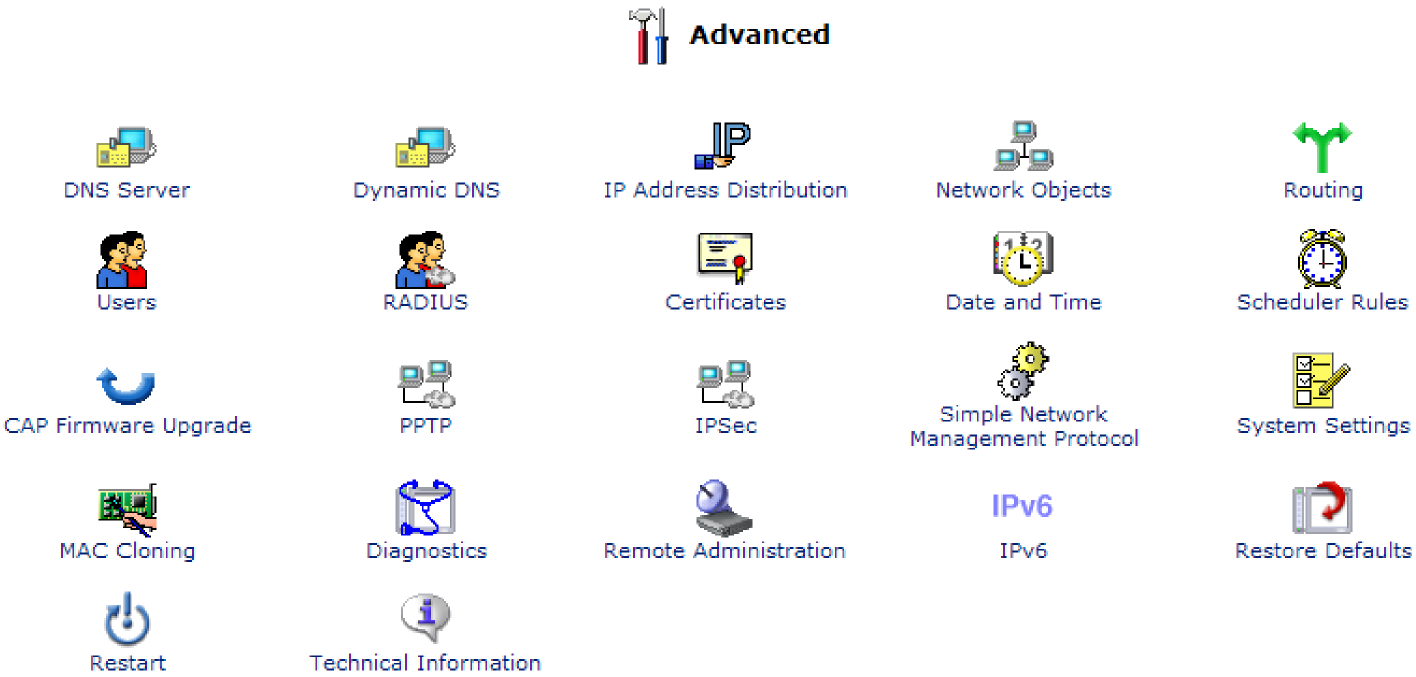
Notes: The measured "avg kbps" is calculated on 15 minutes period

7

7.0 Advanced

Note: The 'Advanced' section of the Management Console consolidates a number of previously described services into an easy to browse section of the management interface, as well as is the location for other new services such as User Administration, Defining Network Objects, Firmware Review and Upgrade, SNMP service definitions, etc.

To get to these services, click on 'Advanced' in the side-bar. The following services are available under this section:



7.1 System Settings

The System Settings button allows you to configure various system and management parameters.

Use this section to configure the following:

1. Specify the gateway’s host name. The host name is the gateway’s URL address.

2. Specify your network’s local domain.

7.1.1 Management Console Settings

Use this section to configure the following:

Automatic Refresh of System Monitoring Web Pages:

– Select this checkbox to enable the automatic refresh of system monitoring web pages.

Warn User Before Network Configuration Changes:

– Select this checkbox to activate user warnings before network configuration changes take effect.

7.1.2 Management Application Ports Settings

This section allows you to configure the following management application ports.

1. **Primary/secondary HTTP ports**
2. **Primary/secondary HTTPS ports**
3. **Primary/secondary Telnet ports**
4. **Secure Telnet over SSL ports**

7.1.3 System Logging Settings

Use this section to configure the following:

1. System Log buffer size

2. Remote system notify level

- None
- Error
- Warning
- Information

7.1.4 Security Logging Settings

Use this section to configure the following:

1. Security Log buffer size

2. Remote system notify level

- None
- Error
- Warning
- Information

7.1.5 Outgoing Mail Server Settings

Use this section to configure the following:

1. Enter the hostname of your outgoing (SMTP) server in the ’Server’ field.

2. Each email requires a ’from’ address and some outgoing servers refuse to forward email without a valid ’from’ address for anti-spam considerations. Enter a ’from’ email address in the ’From Email Address’ field.

3. If your outgoing email server requires authentication check the ’Server Requires Authentication’ checkbox and enter your user name and password in the ’User Name’ and ’Password’ fields respectively.

7.2 Managing the DNS Server

Domain Name System (DNS) provides a service that translates domain names into IP addresses and vice versa.

The CAP’s DNS server is an auto-learning DNS, which means that when a new computer is connected to the network the DNS server learns its name and automatically adds it to the DNS table. Other network users may immediately communicate with this computer using either its name or its IP address.

In addition, your gateway’s DNS:

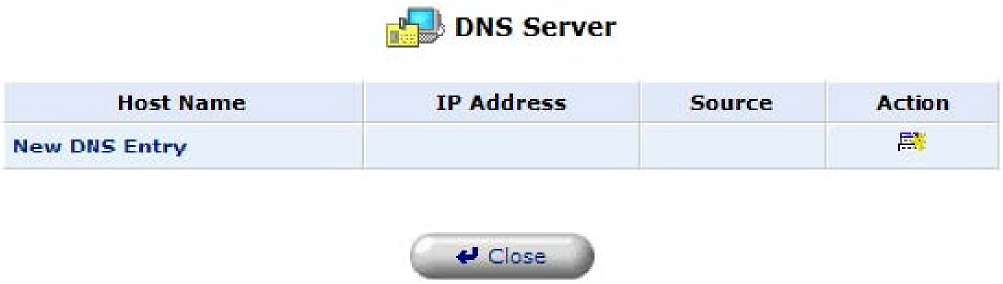
- Shares a common database of domain names and IP addresses with the DHCP server.
- Supports multiple subnets within the LAN simultaneously.
- Automatically appends a domain name to un-qualified names.
- Allows new domain names to be added to the database using the CAP’s Web-based Management.
- Permits a computer to have multiple host names.
- Permits a host name to have multiple IP’s (needed if a host has multiple network cards).

The DNS server does not require configuration. However, you may wish to view the list of computers known by the DNS, edit the host name or IP address of a computer on the list, or manually add a new computer to the list.

7.2.1 Viewing and Modifying the DNS Table

To view the list of computers stored in the DNS table:

1. Click the ’DNS Server’ icon in the ’Advanced’ screen of the Management Console. The DNS table will be displayed.



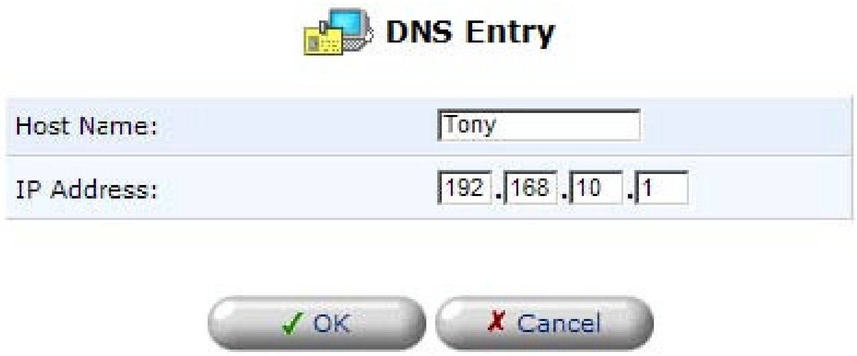
Host Name	IP Address	Source	Action
New DNS Entry			✎

To add a new entry to the list:

1. Click the 'New DNS Entry' button. The 'DNS Entry' screen will appear.

2. Enter the computer's host name and IP address.

3. Click the 'OK' button to save your changes.



DNS Entry

Host Name: Tony

IP Address: 192 . 168 . 10 . 1

To edit the host name or IP address of an entry:

1. Click the 'Edit' button that appears in the Action column. The 'DNS Entry' screen will appear.

2. If the host was manually added to the DNS Table then you may modify its host name and/or IP address, otherwise you may only modify its host name.

3. Click the 'OK' button to save your changes.

To remove a host from the DNS table:

1. Click the 'Delete' button that appears in the Action column. The entry will be removed from the table.