PATTON TECH NOTES

IP Filtering for Patton RAS Products

RAS Filtering: Applications and Functionality

Security PLUS Service Differentiation

Did you know you can use IP filtering to boost your revenues? Patton's Remote Access Server (RAS) provides IP Filtering as a standard on-board feature. Most often, people think of filtering as a mechanism for implementing security functions — and it is. However, you can also use filters to offer differentiated services to your dial-up users, charging higher rates for premium services. Consider three examples:

1) Low-cost email only service – configure filters which allow these dial-in users to access to your e-mail server while blocking all access to all other destinations
2) Full Internet access service – configure filters that allow these dial-in users to access your web server as well as your e-mail server.
3) Privatized service – configure filters allow access to specified private e-mail, web, or proxy servers, while blocking all access to all other destinations.

Functionality

The filtering software in Patton's RAS examines packets traversing user interfaces only (i.e. packets exchanged between dial-in users and the RAS device). Packets traversing other RAS interfaces (ethernet links and WAN links) are not examined for filtering.

An IP Filter comprises a set of configurable of parameters, defined by the RAS operator. Once defined, the parameter set tells the RAS whether to accept or reject an IP packet, depending on the values of certain fields in the IP, TCP, and UDP protocol headers.

Patton's IP Filtering mechanism has the following characteristics:

- Provides up to twenty (20) separately configurable filters.
- Each filter may be shared by an unlimited number of users.
- Up to 10 filters may be applied to each user connection.

Procedure: Configuring Filters for Patton RAS

Defining a Filter is a three-step procedure:

1) **Create the Filter Name and Filter ID**

2) **Define the Filter Parameters**

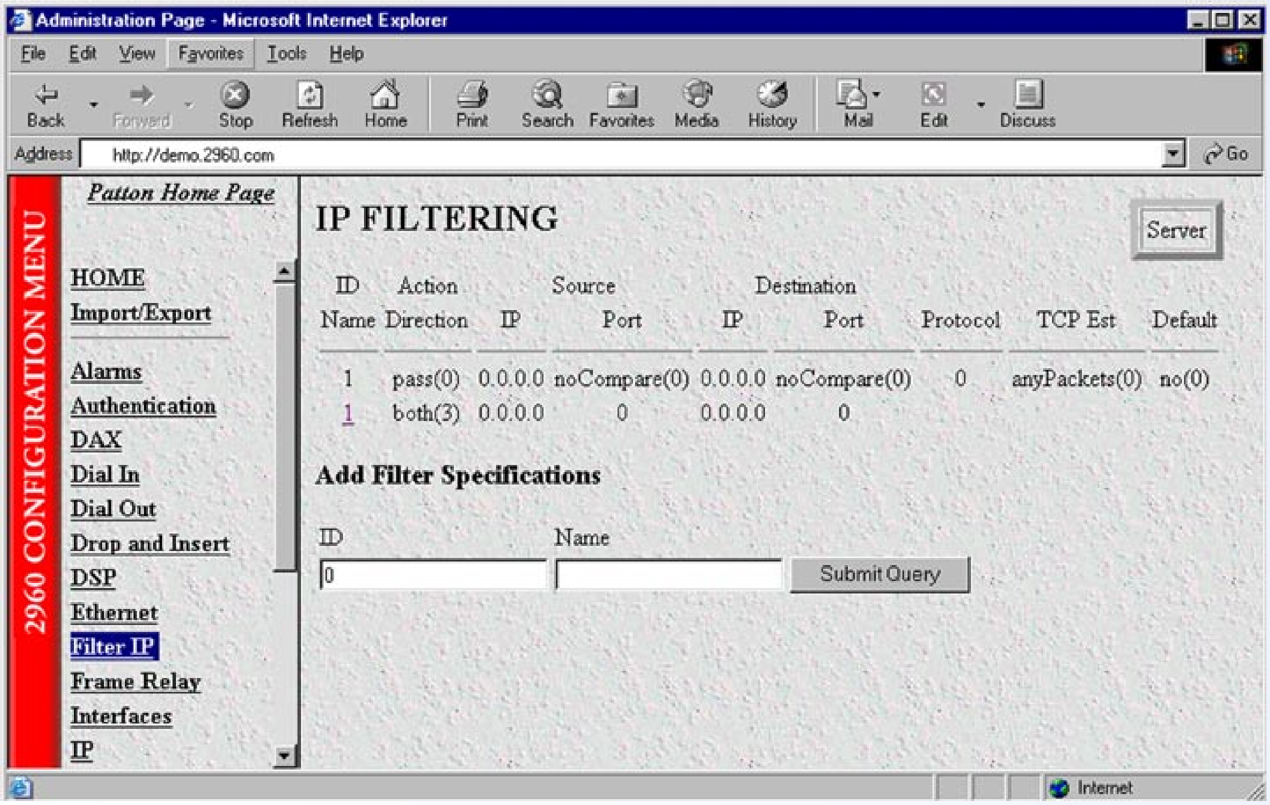
3) **Apply the filter to a user connection**

STEP ONE: Create the Filter Name and Filter ID

To define a new filter:

1) From the RAS Administration page, select **Filter IP** to open the **IP Filtering** screen (shown below).
2) Enter a **Filter ID** number (must be an integer between 1 and 20)
3) Enter a **Filter Name**
4) Click on the Submit Query button to submit the request.

The **Filter ID** and **Filter Name** must not previously exist in the **IP FILTERING** list.


Administration Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Print Search Favorites Media History Mail Edit Discuss
Address http://demo.2960.com
Go
2960 CONFIGURATION MENU
Patton Home Page
HOME
Import/Export
Alarms
Authentication
DAX
Dial In
Dial Out
Drop and Insert
DSP
Ethernet
Filter IP
Frame Relay
Interfaces
IP
Server
Internet

IP FILTERING

ID	Action	Source		Destination				
Name	Direction	IP	Port	IP	Port	Protocol	TCP Est	Default
1	pass(0)	0.0.0.0	noCompare(0)	0.0.0.0	noCompare(0)	0	anyPackets(0)	no(0)
1	both(3)	0.0.0.0	0	0.0.0.0	0			

Add Filter Specifications

ID: 0
Name:
Submit Query

***NOTE:* There are two ways to delete a filter:**

i) Using the `IP Filtering` **screen y**ou may delete an existing filter as follows:

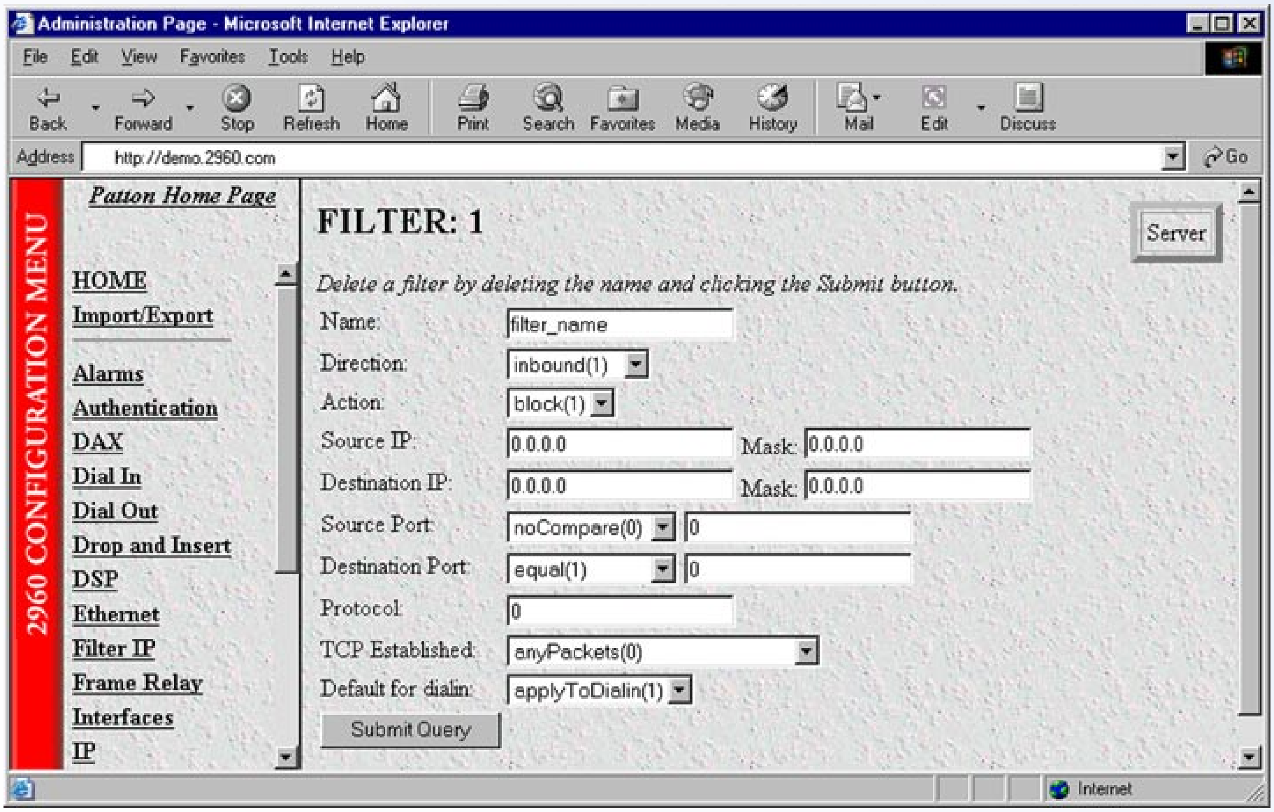
1. Under “Add Filter Specifications,” enter the Filter ID number for the exisitng filter leaving the **Filter Name** blank.
2. Click on the Submit Query button to delete the filter.

ii) Using the **filter parameters window y**ou may delete an existing filter as follows:

1. Delete the **Filter Name**.
2. Click on the Submit button to delete the filter.

STEP TWO: Define the Filter Parameters

a) Once you have created the filter name and number in the **IP FILTERING** list, click on the name of the filter to display the filter parameters window (shown below).


Administration Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Print Search Favorites Media History Mail Edit Discuss
Address http://demo.2960.com
Go
2960 CONFIGURATION MENU
Patton Home Page
HOME
Import/Export
Alarms
Authentication
DAX
Dial In
Dial Out
Drop and Insert
DSP
Ethernet
Filter IP
Frame Relay
Interfaces
IP
Server
Internet

FILTER: 1

Delete a filter by deleting the name and clicking the Submit button.

Name:	filter_name		
Direction:	inbound(1)		
Action:	block(1)		
Source IP:	0.0.0.0	Mask:	0.0.0.0
Destination IP:	0.0.0.0	Mask:	0.0.0.0
Source Port:	noCompare(0)	0	
Destination Port:	equal(1)	0	
Protocol:	0		
TCP Established:	anyPackets(0)		
Default for dialin:	applyToDialin(1)		

Submit Query

b) Defining Filter Parameters (Part 1)

First, we will define values for three of the filter parameters: **Direction**, **Action**, and **Default for Dial-In.**

Direction: The value of this parameter defines whether the RAS will apply the filter to packets transmitted, packets received, or both.

`Inactive(0)` RAS will **not** apply the filter to any packets

`Inbound(1)` packets are sent **to** the RAS from the dial-in user.

`Outbound(2)` packets are sent **from** the RAS to the dial-in user.

`Both(3)` RAS will apply the filter to **both** inbound and outbound packets.

Action: The value of this parameter defines whether the RAS should forward or discard a packet that matches the filtering criteria.

`Pass(0)` The RAS will forward any packet that matches the filter criteria. When one or more pass filters are defined, the RAS will discard (block) any packet that does not match at least one pass filter.

`Block(1)` The RAS will drop any packet that matches the block filter criteria.

Block filters take precedence and are examined first. If a packet matches any block filters the RAS will discard the packet. Pass filters are examined next. If any PASS filters are defined, the packet must match at least one or the RAS will discard the packet.

For example, suppose both a block filter and a pass filter are assigned to a user.

Case 1: If a packet does **NOT match** the pass filter (fail) **and**
does **NOT match** the block filter (pass),
discard (block) the packet.

Case 2: If a packet does **NOT match** the pass filter (fail) **and**
matches the block filter (fail),
discard (block) the packet.

Case 3: If a packet **match**es the pass filter (pass) **and**
does **NOT match** the block filter (pass),
forward (pass) the packet.

Case 4: If a packet **match**es the pass filter (pass), **and**
matches the block filter (fail)
discard (block) the packet.

Default for Dial-In: The value of this parameter defines whether the RAS will use the filter as the default filter as described in the following value definitions.

`ApplyToDialin(1)` The filter will be applied to all dial-in user connections **unless** another filter is assigned to the user via RADIUS or the static user identification table.

`no(0)` The filter will only be applied to dial-in user connections to which it has been assigned (via RADIUS or the static user identification table).

NOTE: Assigning a RADIUS filter or a Static User filter to a user disables all default filters for that user.

2b) Defining the Remaining Filter Parameters

We will define values for one or more of the remaining fields depending on the filter's desired function (e.g. block access to a web server, allow access to a mail server, etc.).

For example, we might use **Source IP and Mask,** and **Destination IP and Mask** to limit a user's access to specific hosts or networks. These parameters may also be used in combination with the **Source Port** and **Destination Port** parameters to enable or disable access to specific application services on specified host(s)

Source Port and **Destination Port** specify TCP or UDP port numbers. For example, we might use these parameters to open up the entire World Wide Web to a guest account while also preventing them from accessing an e-mail server.

The **Protocol** parameter controls user access to features and functions defined in the IP protocol. For example, we might prevent a user from performing traceroute and ping by selecting 1 for ICMP. For the list of protocol numbers as currently defined by the Internet Assigned Numbers Authority (IANA), please see *Appendix A* at the end of this document.

STEP THREE: Applying the filter to a user connection

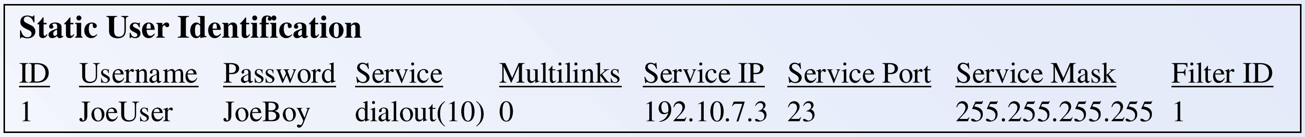
Patton's RAS uses three methods to apply filters to user connections, depending on how the user authenticates.

1) Default Filters

Up to 10 default filters may be assigned to every dial-in user as described in *b) Defining Filter Parameters (Part 1)* above.

2) Static User Identification

Single Filter per User. No more than one filter may be assigned to users who authenticate by means of Static User Identification. The RAS authenticates Static Users by means of the locally resident Static User table, shown below.



Static User Identification

ID	Username	Password	Service	Multilinks	Service IP	Service Port	Service Mask	Filter ID
1	JoeUser	JoeBoy	dialout(10)	0	192.10.7.3	23	255.255.255.255	1

Looking at the the table above, notice the **Filter ID** column heading. This field allows one entry only. The **Static User Identification** table limits each user defined in the table to no more than one **Filter ID**.

To assign a filter to a static user, we will use the **`Static User Identification`** table at the bottom of the RAS **`Authentication`** screen as follows: click on the username to bring up the **STATIC USER** screen, then enterthe **Filter ID** number in the **Filter ID** field to assign a filter to the user.

3) RADIUS Authentication

Multiple Filters per User. Up to 10 filters may be assigned to each user who authenticates by means of Remote Authentication Dial In User Service (RADIUS). Detailed procedures for the RADIUS management interface are beyond the scope of this Tech Note. However, to assign multiple filters to a user, we will log in to the management interface for our RADIUS server and edit the user profile to associate one or more RAS filter definitions with the user. You may enter either the RAS **Filter ID** or **Filter Name** for the RADIUS **`Filter-Id`** attribute (attribute 11). A RADIUS user profile with associated filters is shown below:

```
User1  Password = “user1”
   Framed-Protocol = PPP
   Filter-Id = ”15”
   Filter-Id = ”permit_smtp”
```

When a RADIUS user dials in, the the RAS will communicate with the RADIUS server to learn which filters (if any) should be applied to packets associated with that call.

NOTE: You may assign any filter to both static users and RADIUS users simultaneously.

EXAMPLE: Private E-Mail and Web Service

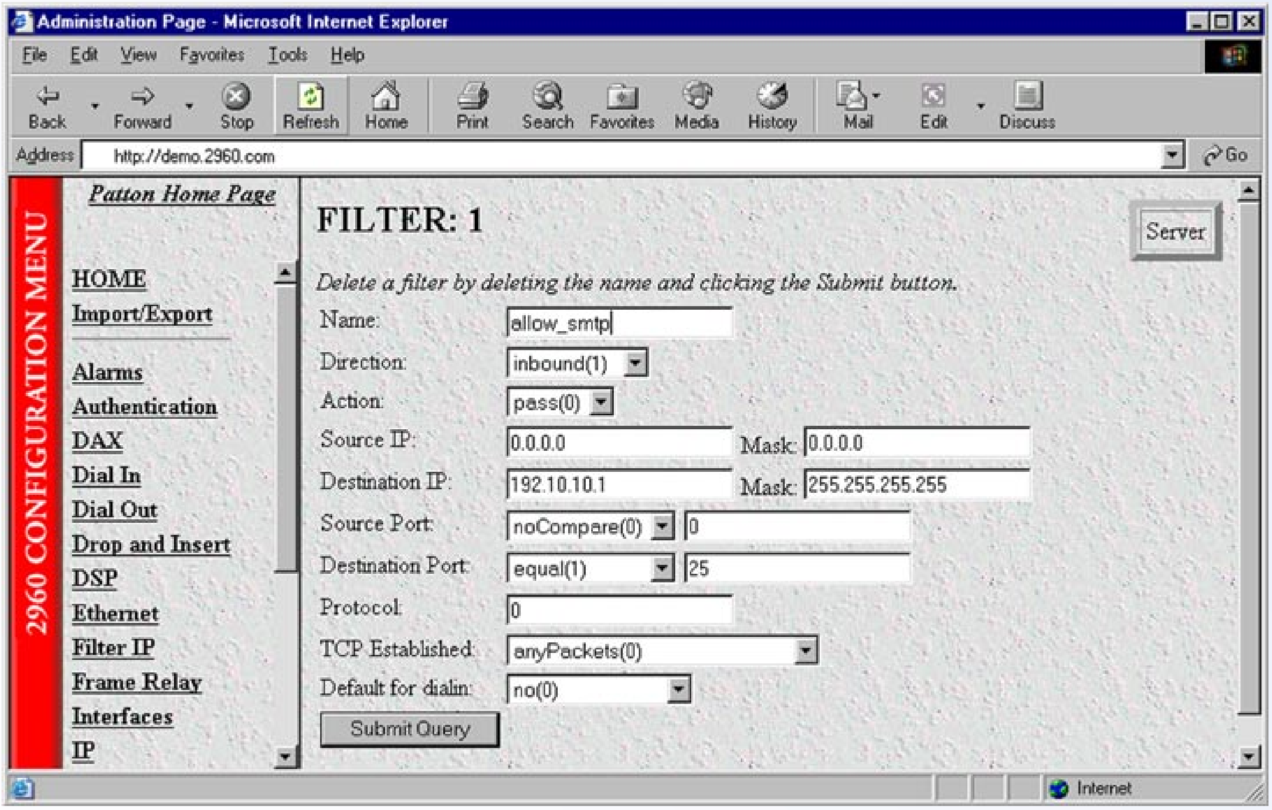
Suppose we are setting up a filtering scheme for private service to a customer. For e-mail, the customer accounts will only be able to access their own private mail server (www.privatemail.com) and webserver (www.privateweb.com). Access to all other destinations will be blocked.

- The IP address for www.privatemail.com is: 192.10.10.1
- The IP address for www.privateweb.com is: 192.10.10.2

We will define three filters using the parameter values shown below:

Filter Name	`allow_smtp`	`allow_pop3`	`web_server`
Direction	`inbound`	`inbound`	`inbound`
Action	`pass`	`pass`	`pass`
Source IP & Mask	N/A	N/A	N/A
Destination IP & Mask	192.10.10.1 255.255.255.255	192.10.10.1 255.255.255.255	192.10.10.2 255.255.255.255
Source Port	`nocompare(0)`	`nocompare(0)`	
Destination Port	`equal 25` (SMTP)	`equal 110` (POP3)	`equal 80` (HTTP)
Protocol	`0`	`0`	
Function	Allow user to send email	Allow user to receive email	Allow user to access web services

The completed **filter parameters** window for allow_smtp is shown below as a sample.



Administration Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Print Search Favorites Media History Mail Edit Discuss
Address http://demo.2960.com
Go
2960 CONFIGURATION MENU
Patton Home Page
HOME
Import/Export
Alarms
Authentication
DAX
Dial In
Dial Out
Drop and Insert
DSP
Ethernet
Filter IP
Frame Relay
Interfaces
IP
Server
Internet

FILTER: 1

Delete a filter by deleting the name and clicking the Submit button.

Name: allow_smtp
Direction: inbound(1)
Action: pass(0)
Source IP: 0.0.0.0 Mask: 0.0.0.0
Destination IP: 192.10.10.1 Mask: 255.255.255.255
Source Port: noCompare(0) 0
Destination Port: equal(1) 25
Protocol: 0
TCP Established: anyPackets(0)
Default for dialin: no(0)

Submit Query

Suppose a service provider implements the above filters for the private customer accounts, then discovers the users are unable to reach the web server (192.10.10.2) or the mail server (192.10.10.1). As it turns out, the users are using ***URL*** www.privateweb.com rather than the ***IP address*** 192.10.10.2 to reach the private web server.

The set of two filters above allows access to the correct IP addresses for the two servers, but it also prevents users from accessing any domain name server (DNS). Without access to DNS, users cannot resolve the domain names (e.g. www.privateweb.com) to the IP addresses (e.g. 192.10.10.2) and therefore cannot reach the servers. For users to reach the domain name server, a pass filter must be created allowing access to DNS.

The parameter values for the third filter are shown in the following table:

Filter Name	`DNS`
Direction	`inbound(1)`
Action	`pass(0)`
Source IP & Mask	
Destination IP & Mask	192.10.10.1 255.255.255.255
Source Port	
Destination Port	`equal 53`
Protocol	
Function	Allow access to the Domain Name Server for name-to-address translation service. Without this filter, users could NOT access the mail and web server using domain names, but only by using IP addresses.

For a comprehensive discussion of IP Filtering for Patton RAS products please visit http://www.patton.com/manuals/AccessServer_Admin-D_lo-res.pdf and read ***Chapter 12 Filter IP*** in ***Access Server Administrator's Reference Guide.***

Appendix A:
Internet Assigned Numbers Authority (IANA) Port Numbers

For the most recent information on TCP and UDP PORT NUMBERS please visit http://www.iana.org/assignments/port-numbers