

## How to Define Generic IPS Patterns for Content Filtering

<https://campus.barracuda.com/doc/41115742/>

Barracuda Networks recommends using the [Intrusion Prevention System \(IPS\)](#) instead of the legacy generic IPS patterns.

Generic IPS Patterns do not work in combination with Application Control.

To block Internet worms and exploit attacks, configure a content filter. The Barracuda NG Firewall provides a set of predefined content filters that can be referenced by the firewall rule set. Network connection types (for example, SMTP) that are specified in the service or [Service Object](#) of firewall rules are checked for patterns that are configured in the content filters. Detected network attacks are logged in the <fw>\_Content log file for later review. The source and destination address and the associated network interfaces or firewall rule actions are stored in the corresponding filter log (for example, [sqlslammer]).

Filter Group	Filters	Description
HTTP	google chrome download HTTP,google chrome DOS HTTP,ViewW...	
SMTP	Sobig SMTP,prescan SMTP,from comment SMTP	
DNS	bind NXt DNS,bind tsig DNS-TCP,bind tsig DNS-UDP,bind NXt D...	
MS-SQLRS	SQLSlammer MS-SQLRS	
MS-RPC	MS05-039 WINRPC445,korgo RPC,sasser RPC,spybot.ap WINRP...	
Phion ALL	google chrome download HTTP,google chrome DOS HTTP,rdesk...	
SPYBOT	spybot.ap SPYBOT	
NBSESSION	MSNETBIOS MS04031 NBSESSION	
SIP	Asterisk SQL injection SIP,Notify Spoofing SIP,ekiga negative lengt...	
HTTP-TDMCAT	Tomcat Webdav Disclosure HTTP	
RDP	rdesktop RDP	
SocialWeb	SocialWooMe,Social-Webshots,SocialVKontakte,Social-twtkr,Soc...	Container to add...

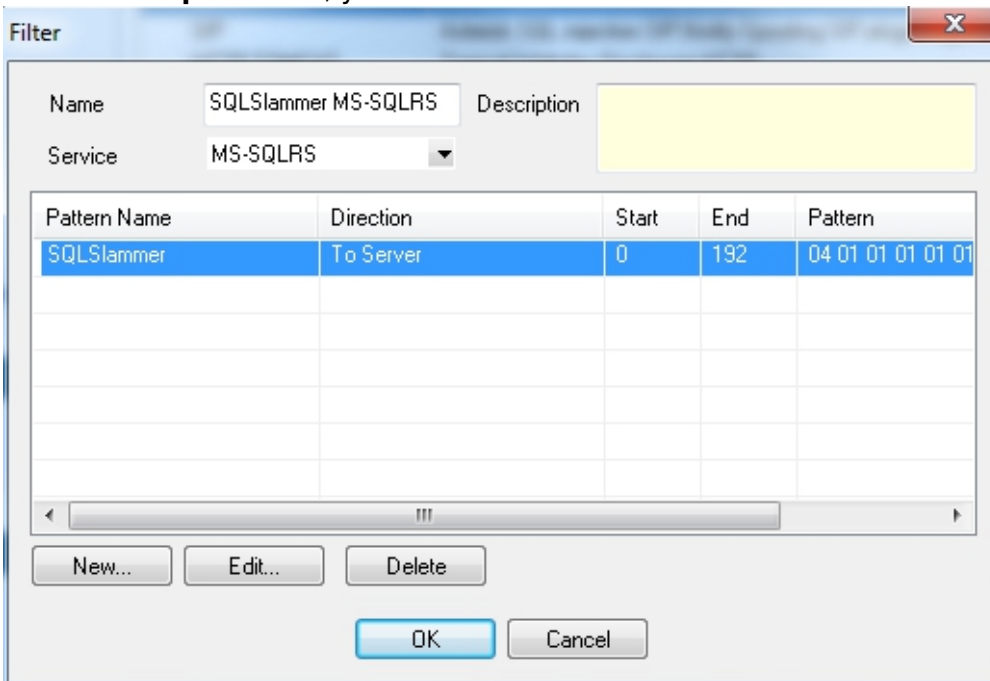
Filter Name	Service	Patterns	Description
Nimda HTTP	HTTP	attack1,attack2,attack3,attack4,atta...	
.htr cai browsing HTTP	HTTP	htr qet,htr post,HTR GET,HTR POST	

You can edit existing filters or add new filters. You can also create filter groups.

### In this article:

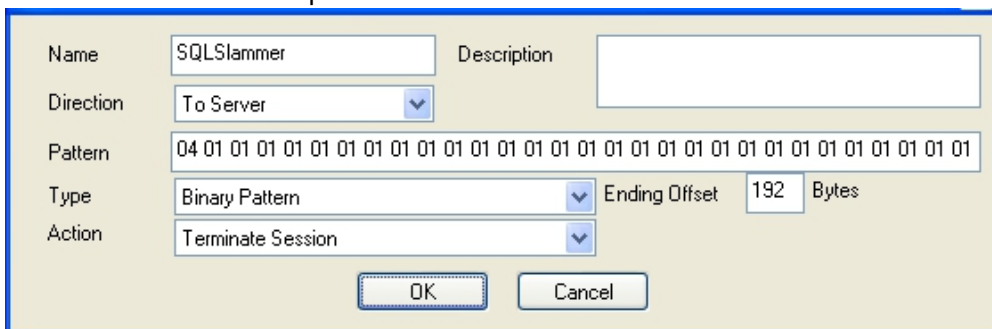
## Configure a Filter

1. Open the **Forwarding Rules** page (**CONFIG > Full Config > Virtual Servers > your virtual server > Firewall**).
2. In the left navigation pane, click on **Generic IPS Patterns**.
3. Create a new filter or select an existing filter to edit:
  - To create a new filter, right-click the lower table and select **New**.
  - To edit an existing filter, double-click its name in the lower table.
4. Enter or edit the descriptive **Name** for the filter.
5. From the **Service** list, select the service to be filtered.
6. In the **Description** field, you can enter additional information about the filter.



7. Configure the patterns for the filter:
  - To edit an existing pattern, select it from the table and click **Edit**.
  - To create a new pattern, click **New**.

The **Pattern** window opens.



8. You can edit the following pattern settings:

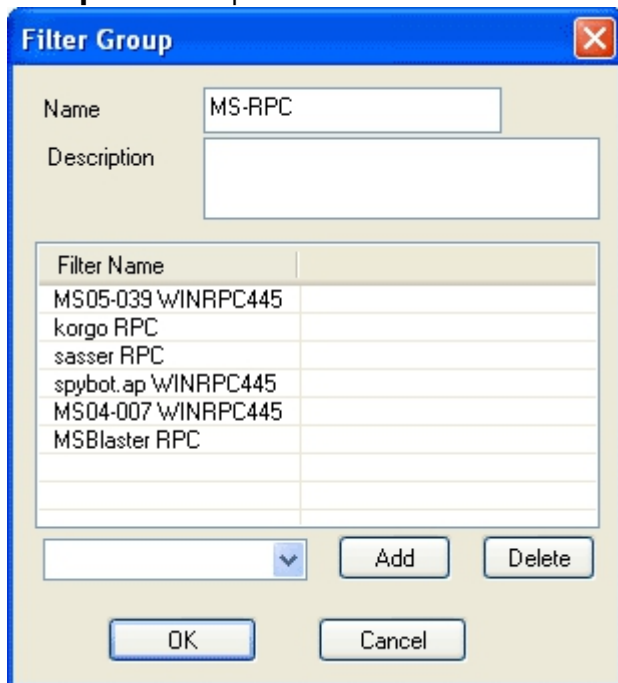
Setting	Description
---------	-------------

<b>Name</b>	The pattern name.		
<b>Direction</b>	Which direction of traffic/stream is affected. You can select one of the following directions: <ul style="list-style-type: none"> <li>◦ <b>To Server</b> - Incoming traffic/stream.</li> <li>◦ <b>To Client</b> - Outgoing traffic/stream.</li> </ul>		
<b>Description</b>	Any additional information about the pattern.		
<b>Pattern</b>	The search pattern for the object that the stream is scanned for.		
<b>Type</b>	The pattern type. You can select any of the following pattern types:	<b>Binary Pattern</b>	List of hexadecimal digit pairs separated with a space. The above screenshot of the <b>Pattern</b> window displays an example for a binary pattern (SQL slammer).
		<b>ASCII Pattern + Wildcards(*,?,[ ])</b>	* - represents a variable number of characters including an empty string (space)
			? - matches exactly one character.
			[...] - matches only the characters that are enclosed within the brackets.
<p>Example pattern: [123]?attack*##  Match on the following:  200attacking##  321attacker##  1stattack##  Mismatch on the following:  500attackers##  1million attackers##  123ata#</p> <p>The patterns are detected at any offset in the traffic flow unless the sequence of matching characters exceeds the boundary that is specified by the <b>Ending Offset</b> setting.</p>			
<b>Action</b>	Enables a reporting only mode for individual patterns. You can select one of the following actions: <ul style="list-style-type: none"> <li>◦ <b>Terminate Session</b> - Causes session termination when the pattern matches.</li> <li>◦ <b>Create Log Entry</b> - Triggers log entry generation only.</li> </ul>		
<b>Ending Offset</b>	The number of bytes from the connection start that are scanned to find the pattern.		

9. Click **OK**.

## Configure a Filter Group

1. Open the **Forwarding Rules** page (**CONFIG > Full Config > Virtual Servers > your virtual server > Firewall**).
2. In the left navigation pane click on **Generic IPS Patterns**.
3. Click **Lock**.
4. Create a new group or select an existing group to edit:
  - To create a new filter, right-click the upper table and select **New**.
  - To edit an existing group, double-click its name in the upper table. The **Filter Group** window opens:



Filter Name	
MS05-039 \WINRPC445	
korgo RPC	
sasser RPC	
spybot.ap \WINRPC445	
MS04-007 \WINRPC445	
MSBlaster RPC	

5. You can edit the following group settings:
  - **Name** - The group name.
  - **Description** - Any additional information about the filter group.
  - **Filter Name** - Table that lists each filter that is included in the group. You can add or delete filters.
    - To add a filter, select it from the filter list and click **Add**.
    - To delete a filter, select it and click the **Delete**.
6. Click **OK**.

## Referencing within the Corresponding Rules

When a pattern for content filtering was successfully applied to a service, the service, when selected in context with a firewall rule, will now automatically apply this pattern to the rule.

## Figures

1. ct\_filter.png
2. gen\_filter\_new.png
3. gen\_pattern.png
4. f\_group.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.