

Configuring Policies and Filter Rules in the Exinda Optimizer

Introduction

Policies and filter rules allow users to apply actions to specific traffic on their network. Users are able to configure traffic to discard, allocate bandwidth, compress and/or ToS/DiffServ tag. This document will explain how to create and implement policies to effectively optimize the traffic on an example network.

What are Policies and Filter Rules?

Policies are created inside virtual circuits (refer to the “Configuring Circuits and Virtual Circuits in the Exinda Optimizer” application note for further information) and describe a set of actions to take for any matching traffic. Filter rules are created inside policies and are used to define the traffic that should match that policy. An example of policies and filter rules are shown below.

1. DISCARD (i.e. block)	All traffic to John’s PC (192.168.100.22)
	All ping traffic (ICMP)
2. Restrict Bandwidth to 100kbps and allow to Burst to 400kbps	All email (POP and SMTP)
3. Restrict Bandwidth to 500kpbs between 8am and 6pm	All web (HTTP and HTTPS)
	All FTP
4. Guarantee 1000kpbs of Bandwidth and Compress	All Citrix traffic to/from Citrix Server
5. Restrict Bandwidth to 200kpbs and allow to Burst to 500kbps	All other traffic

The policies are shown in bold and describe an action (i.e. Restrict Bandwidth to 100kbps) and the filter rules appear under each policy. Any traffic that passes through the Optimizer will be applied to each policy’s filter rules, in numerical order, until a match occurs. When a match occurs, that policy will be applied to the matching traffic.

For example, if a HTTP packet passes through the Optimizer, it would be first be inspected by policy 1, where no match occurs. It then moves onto policy 2, where also no match occurs. When it is compared to policy 3, however, the HTTP packet matches and the resulting policy is applied (Restrict Bandwidth to 500kpbs between 8am and 6pm) and optimization ceases.



Notice how Policy 5 consists of an “All other traffic” rule. This rule is used to “catch” any traffic that has not been matched by any previous policies and provides a way of controlling any other or unknown traffic on the network. If there was another policy after policy 5, it would never be reached since policy 5 catches all traffic. If there was no “catch-all” rule, then any traffic that is unmatched will behave as it otherwise would on the network, and as such, would make it impossible to guarantee bandwidth for any other traffic.

Figure 1, below, shows the setup screen for policies and filter rules. The top half of the screen allows users to configure what action should be taken if a packet matches the filter rules, which are defined in the bottom half of the screen.

Add/Edit Optimization Rules

TIP: To delete a line entry simply blank out the drop down lists on that line. ?

Rule Num: **Allocate Bandwidth** **Guaranteed Bandwidth:** kbps
Name: **Maximum Bandwidth:** kbps
Schedule: ALWAYS **Priority:** 1 (high)
Action: Optimize **Enable Compression** **DiffServ Type:** TOS
 Mark Packets **TOS Type:** Normal-Service
Code Point: (0-63)

Client	Direction	Server	Traffic Type
<input type="button" value="v"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="button" value="v"/>	<input type="button" value="v"/>
<input type="button" value="v"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="button" value="v"/>	<input type="button" value="v"/>
<input type="button" value="v"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="button" value="v"/>	<input type="button" value="v"/>
<input type="button" value="v"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="button" value="v"/>	<input type="button" value="v"/>
<input type="button" value="v"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="button" value="v"/>	<input type="button" value="v"/>

Figure 1: Policy and filter rule setup screen.

The following describes each component of this setup screen for configuring policies.

- **Rule Num:** A number given to this policy. Since policies are applied in order, rule numbering is important and should be carefully considered.
- **Name:** A name given to the policy to make it easier to recognize.
- **Schedule:** Select what time of the day this policy should be active. Custom schedules can be defined by selecting "Scheduling Rules" from the left-hand side menu.
- **Action:** Select what this policy should do to matching traffic. Choices are Optimize, Discard (block) or Ignore (allow to pass though Optimizer without matching). Selecting 'Optimize' activates the 3 choices on the right-hand side.
- **Allocate Bandwidth:** Select this if you want to manage the bandwidth for any matching traffic.
 - **Guaranteed Bandwidth:** Enter how much bandwidth any matching traffic should be guaranteed (in kbps).
 - **Maximum Bandwidth:** Enter the maximum bandwidth any matching traffic is entitled to (enter 'ALL' to specify the maximum possible bandwidth).
 - **Priority:** Select a priority to use if this policy is competing with another policy for left-over or unused bandwidth. Policies with higher priorities will have first access to any left-over or unused bandwidth.

- **Enable Compression:** Select this if you want any matching traffic to be compressed. Another Exinda appliance will be required at this traffic's destination in order to decompress it. Compression can be used in conjunction with bandwidth management.
- **Mark Packets:** Select this if you want any matching traffic to be marked by the Optimizer for further QoS processing by another device on the line (refer to the "Exinda Optimizer and the IP ToS/DiffServ Field" application note for further information regarding TOS or DSCP marking).
 - **DiffServ Type:** There are 2 marking options; TOS and Code Point.
 - **TOS Type:** If TOS was selected, above, then select the relevant TOS type here.
 - **Code Point:** If Code Point was selected, above, then enter the relevant Code Point value here (must be a number between 0 and 63).

Client, Server, Direction and Traffic Type are used to define filter rules for the policy.

- Client and Server entries are simply made by selecting a network object. Network objects are groups of one or more subnets and can be configured by clicking the link on the left-hand side menu. Select ALL to match all traffic on any client or server.
- Direction simply specifies which direction traffic should be travelling in between the client and server network objects. Options are either direction or both directions.
- Traffic Type represents the type of traffic that should be matched (i.e. http, smtp, etc). Custom Traffic Types can be configured by selecting the link on the left-hand side menu. Select 'All traffic' to match any traffic regardless of Traffic Type.



Many filter rules can be created within each policy. If additional filter rules are required, save the policy, then edit it, and an additional 5 filter rules will become available.

Exinda Optimizer uses a fair bandwidth allocation system within policies. For example, if a particular policy limits http traffic to a certain bandwidth, and there are many simultaneous http connections, then each http connection will receive a fair (proportional) allocation of bandwidth (i.e. no one http connection will hog the bandwidth).

A Simple Example

Consider the network shown in Figure 2, below.

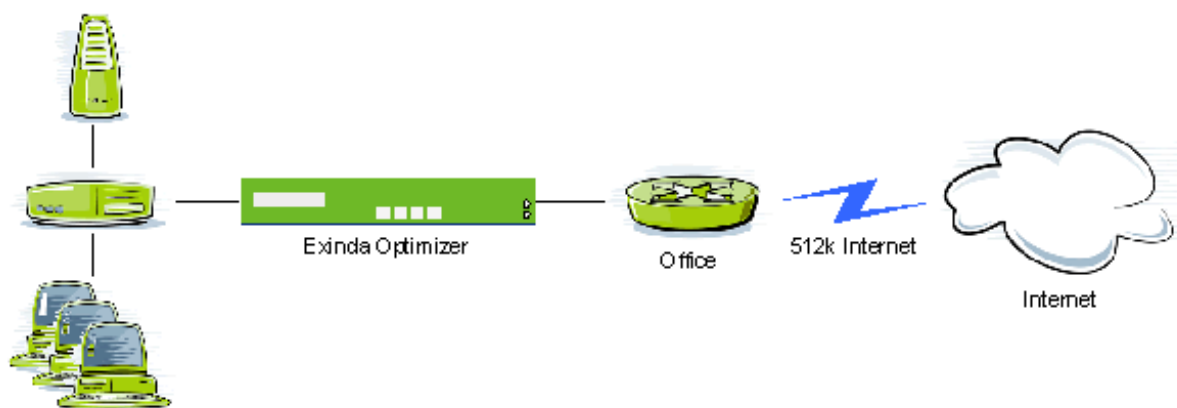


Figure 2: An Exinda Optimizer in a network.

This diagram represents a simple connection to the Internet and the Exinda Optimizer is to be setup according to the specification on the following page.

10. Guarantee 300kbps, Restrict to 512kbps (Burst with Priority 1)
Web (HTTP)
Web (HTTPS)
20. Guarantee 50kbps, Restrict to 512kbps (Burst with Priority 10)
Email (SMTP)
Email (POP)
30. Guarantee 100kbps, Restrict to 512kbps (Burst with Priority 5)
All other traffic

Figure 3, below, shows the main Optimizer setup screen. Click the 'Add New Policy' link to enter the policy setup screen.

Figure 3: Optimizer setup page with no policies defined.

Figure 4, below, shows the policy setup screen for the last (catch-all) policy in this example. The relevant entries have been made to allocate bandwidth and the specified filter rules match all traffic as required by the specification.

Figure 4: Policy and filter rule setup for the last policy.

Figure 5, below, shows the completed optimizer setup page.

Optimizer Policies									
Add New Circuit ?									
Circuit	Virtual Circuit	Policy #	Schedule	Client	Direction	Server	Traffic Type	Edit	Delete
10. Internet (512 kbps)								Edit	Delete
10.10. Internet (512 kbps)								Edit	Delete
		10	ALWAYS	Fast (300 - 512 kbps, priority 1)				Edit	Delete
				ALL	◀▶	ALL	http (tcp, port 80)		
				ALL	◀▶	ALL	https (tcp, port 443)		
		20	ALWAYS	Slow (50 - 512 kbps, priority 10)				Edit	Delete
				ALL	◀▶	ALL	smtp (tcp, port 25)		
				ALL	◀▶	ALL	pop3 (tcp, port 110)		
		30	ALWAYS	General (100 - 512 kbps, priority 5)				Edit	Delete
				ALL	◀▶	ALL	All traffic		
Add New Policy									
Add New Virtual Circuit									

Figure 5: The completed policy setup.

In order to view these policies, click on the “Allocated Bandwidth in Policies” link at the bottom of the optimizer setup page. This will present a graphical representation of the allocated bandwidth and also makes it easier to visualize policies.

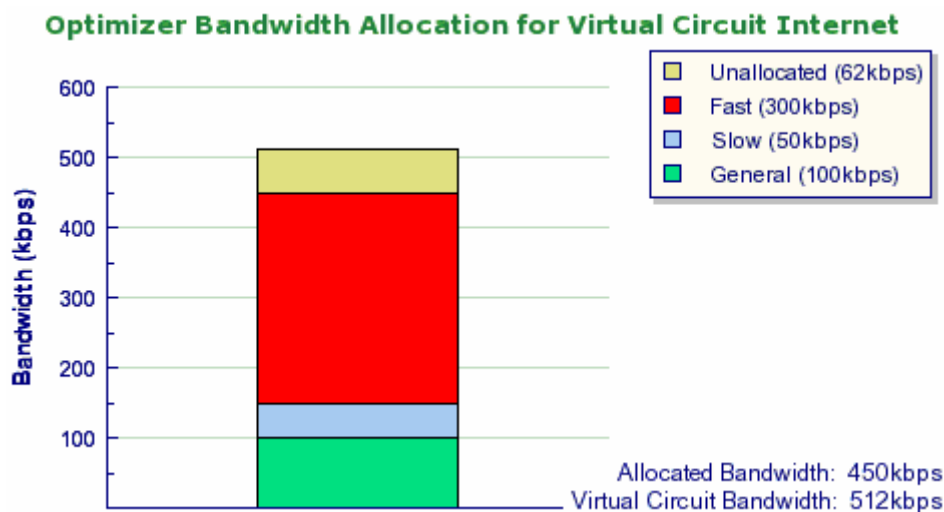


Figure 6: Bandwidth allocation graph.

Figure 6, above, shows the bandwidth allocation graph for the example policies. Notice how there is 62kbps of unallocated bandwidth. This spare bandwidth will be used by any policy wanting more than it’s guaranteed bandwidth. If multiple policies are competing for this bandwidth, then the policy with the highest priority will receive it first.



The bandwidth allocation graphs can also be viewed as a pie chart. The ‘Visualise Policies’ page has a number of options for viewing policies including bandwidth allocation over days of the week; useful when schedules are being used.

The above setup can also be achieved using the CLI (command line interface) “conf” command. This is useful if a large number of devices need to be configured (using copy and paste).

The following text shows the input required to perform this setup using the "conf" command (refer to the "Exinda Optimizer CLI Reference Guide" for further information).

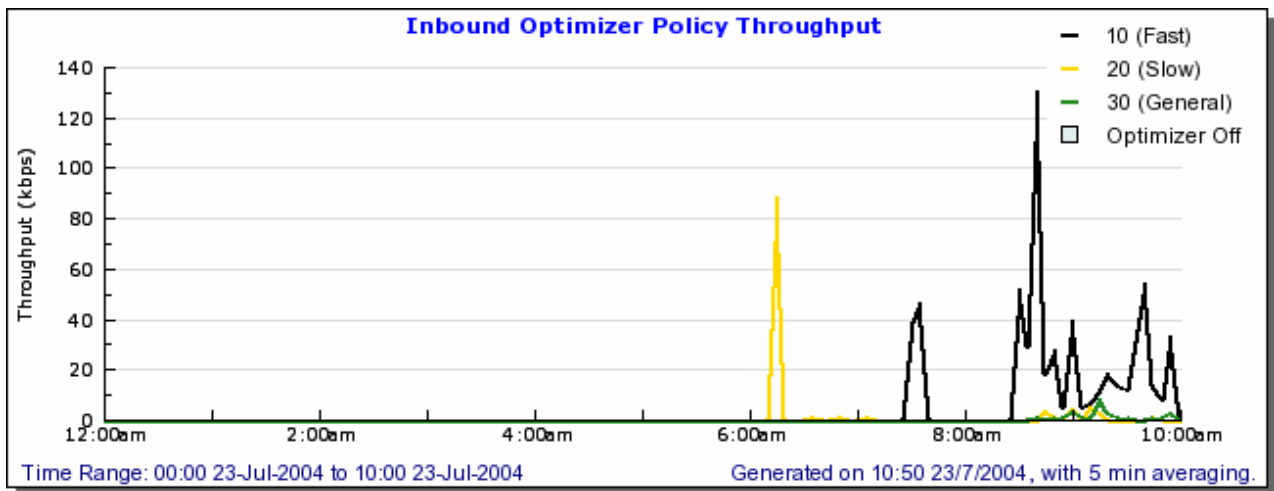
```

optimizer
circuit 10 "Internet" 512 512
vcircuit 10 "Internet" 512 "ALL"
  policy 10 "Fast"
    schedule 0
    minbw 300
    maxbw ALL
    priority 1
    action OPTIMIZE
    filter ALL any ALL "https (tcp, port 443)"
    filter ALL any ALL "https (tcp, port 443)"

  policy 20 "Slow"
    schedule 0
    minbw 50
    maxbw ALL
    priority 10
    action OPTIMIZE
    filter ALL any ALL "smtp (tcp, port 25)"
    filter ALL any ALL "pop3 (tcp, port 110)"

  policy 30 "General"
    schedule 0
    minbw 100
    maxbw ALL
    priority 5
    action OPTIMIZE
    filter ALL any ALL "All traffic"
  
```

Users have the ability to monitor optimizer policies by viewing the information on the Monitor, Optimizer page (accessible under the 'Monitor' tab). This page contains policy utilization graphs for both inbound and outbound traffic, as well as statistics and real-time utilization data as shown in Figure 6, below.



Inbound Optimizer Throughput Statistics



Rule Number and Name	Plot	Guaranteed BW	Maximum BW	Average Rate	Current Rate	Current Utilization
10 - Fast	<input checked="" type="checkbox"/>	300 kbps	2000 kbps	9.00 kbps	52.13 kbps	17.38%
20 - Slow	<input checked="" type="checkbox"/>	50 kbps	2000 kbps	0.00 kbps	0.05 kbps	0.10%
30 - General	<input checked="" type="checkbox"/>	100 kbps	2000 kbps	15.00 kbps	0.42 kbps	0.42%

Figure 6: Real-time optimizer policy utilization and statistics.

Policies and filter rules, when used properly in conjunction with circuits and virtual circuits, can provide a total WAN optimization solution. Exinda recommends assessing your network (using Exinda Optimizer's monitor) and carefully planning optimization strategies and policies before implementing them.

For any further information, please contact Exinda Networks.

Exinda Networks Pty Ltd
Level 1, 235 Queen Street
Melbourne, VIC 3000, Australia
Phone: +61 (3) 9670 0714
Fax: +61 (3) 9670 0719
Email: info@exinda.com
Web: <http://www.exinda.com>

Recommended Reading

- "Configuring Policies and Filter Rules in the Exinda Optimizer"
- "Configuring Circuits and Virtual Circuits in the Exinda Optimizer"

Copyright

Copyright ©2005 Exinda Networks. All rights reserved.

Warranty

The information in this guide is supplied without warranty of any kind and is subject to change without notice. Exinda Networks will not be liable for any damages of any kind arising from the supply of this guide, regardless of the form of action, whether in contract, tort, strict liability or otherwise.

Trademarks

All rights reserved. Exinda Networks and Exinda Optimizer are either registered trademarks or trademarks of Exinda Networks Pty Ltd.

All other trademarks, trade names, service marks and images mentioned and/or used herein belong to their respective owners.