

## Exinda Optimizer and Layer 7 Classification

### Introduction

Traditionally, applications could be identified by the TCP/UDP port number they use. For example, HTTP uses TCP port 80 and SMTP uses TCP port 25. This made it easy to monitor and control traffic as packets traversing a network could be blocked, optimized and accounted by simply referring to their TCP/UDP port number. However, these days, making such assumptions based on port numbers alone doesn't suffice. For example, unwanted and sometimes malicious applications can work over TCP port 80, and appear to be HTTP. Some applications allocate ports dynamically and even randomly port swap so there is no way of knowing what they are based purely on port number.

Exinda Optimizer uses layer 7 packet inspection to analyse the contents (payload) of the packet in order to classify it. This allows users to both monitor and optimize traffic that masks as other traffic (e.g. peer-to-peer using port 80) and also determine what certain traffic is that runs over unknown ports (e.g. http over TCP port 12345). There is also support for applications that dynamically swap ports such as passive FTP and h.323.

### How does Exinda Layer 7 Classification Work?

Exinda Optimizer monitors traffic flows and keeps track of their status. As part of this monitoring process, Exinda Optimizer looks at packet header information (such as IP address and port numbers). A typical packet may look like the example in Figure 1, below.



*Figure 1: An example packet diagram.*

To gain specific information about the type of traffic contained within a packet, Exinda Optimizer must look in the packet payload (layer 7). Each application uses different signatures and protocols to communicate, and with knowledge of these signatures and protocols, Exinda Optimizer can use the layer 7 information to identify what application the traffic is.

Exinda Optimizer can also extract information from the packet payload to provide extra optimization options. For example, users can manage the bandwidth of Citrix ICA traffic based on the priority of the Citrix traffic as specified in the payload. High priority Citrix traffic can be guaranteed more bandwidth while low priority Citrix traffic (such as printing) can be restricted to use less bandwidth. This level of optimization can only be achieved using layer 7 packet inspection.

Exinda's layer 7 packet inspection engine works extremely fast as Exinda uses advanced algorithms and checks to ensure only relevant data is inspected, and inspected quickly. This ensures that no latency is introduced into the network.

### Layer 7 Monitoring

Exinda Optimizer implements and performs layer 7 monitoring automatically. There are 3 situations where Exinda Optimizer will examine layer 7 data in order to correctly identify and classify traffic flows, viz

- Traffic that systematically allocates ports for data transfer (e.g. passive FTP)
- Traffic using a non-standard port number (e.g. HTTP on a high port)
- Traffic using a port number it wouldn't normally use (e.g. KaZaa using TCP port 80)

Figure 2 shows how the Exinda Optimizer displays a passive FTP connection that is actually running over high ports (not the standard FTP data port 20). It has been successfully classified

and monitored as FTP even though it is using random high ports assigned by the FTP control channel.

Inbound Conversations				Outbound Conversations			
Source	Destination	Service	Rate (kbps)	Source	Destination	Service	Rate (kbps)
216.49.88.143	172.14.1.144	ftp	203.674	172.14.1.144	216.49.88.143	ftp	7.398

Figure 2: Real-time monitoring of an FTP data stream.

The same occurs for malicious or unwanted traffic that pretends to be legitimate traffic. Applications such as KaZaa can run over HTTP's port 80. Exinda Optimizer will detect this and correctly display it as KaZaa (or Fast Track – the KaZaa protocol) as shown in Figure 3, below.

Top 30 Inbound Applications LAN ← WAN

Application Name	Packets	Data (MB)	Throughput (Kbps)		
			Min	Avg	Max
<a href="#">http</a>	43954	49.781	0.03	<b>8.93</b>	228.35
<a href="#">https</a>	8078	4.301	0.03	<b>4.96</b>	56.47
<a href="#">smtp</a>	4498	2.698	0.03	<b>6.99</b>	226.80
<a href="#">fastrack</a> ←	1246	1.761	0.35	<b>28.64</b>	220.80

Figure 3: Traffic correctly identified as Fast Track (KaZaa).



Like most peer-to-peer applications, KaZaa uses a file sharing protocol as a means of sharing data. KaZaa uses the Fast Track protocol (also used by iMesh and Grokster), however, several other major protocols exist, such as gnutella (used by Morpheus, BearShear and Shareaza), Direct Connect and Bit Torrent. All these protocols are supported by Exinda Optimizer.

Figure 4, below, shows a HTTP session that was connected to a web server using a high port. This traffic was detected and successfully classified as HTTP even though the web server did not use the standard HTTP port (TCP port 80).

Inbound Conversations				Outbound Conversations			
Source	Destination	Service	Rate (kbps)	Source	Destination	Service	Rate (kbps)
210.50.5.29	172.14.1.89	http	9.518	172.14.1.89	203.166.110.169	http	1.710
206.65.183.125	172.14.1.89	http	1.102	172.14.1.89	203.111.102.15	http	1.072
203.166.110.169	172.14.1.89	http	0.669	172.14.1.89	216.73.85.29	http	0.676
203.111.102.15	172.14.1.89	http	0.402	172.14.1.89	210.50.5.29	http	0.160

Figure 4: Real-time monitoring of a HTTP session over high-ports.

The layer 7 signatures used for packet inspection are stored in an internal database and are setup automatically by the Exinda Optimizer. From time-to-time, signatures change and new protocols evolve, so the internal signature database may become outdated. Exinda will ensure the latest layer 7 signatures are included with every firmware update and recommend users make sure their Exinda Optimizer is kept up-to-date.

### Layer 7 Optimization

Optimization policies can be setup to manage traffic based on layer 7 information. At this stage, this includes matching peer-to-peer signatures and identifying Citrix priority tags. In order to match this traffic, a 'Traffic Type' entry must be setup for each type of traffic to be matched. Figure 5 shows how to setup a traffic type using peer-to-peer signatures. Note that the 'P2P Type' option must be selected from the drop-down list.

### Add Traffic Type

?

Name	<input type="text"/>		
Protocol	ALL	ICMP Type:	All ICMP
Service	P2P Type →	P2P Type:	P2P-Fasttrack
		ICA (Citrix) Priority:	ALL
DiffServ	ALL	TOS:	Normal-Service
		Code Point:	<input type="text"/> (0 - 63)
Search Term	<input type="text"/>		
Save		Cancel	

Figure 5: Setting up a Traffic Type using peer-to-peer signatures.

Figure 6, below shows how to setup a traffic type based on Citrix priority tags. Note that the ICA service must be selected in order to enable this option.

### Add Traffic Type

?

Name	<input type="text"/>		
Protocol	ALL	ICMP Type:	All ICMP
Service	ica (port 1494) →	P2P Type:	P2P-Fasttrack
		ICA (Citrix) Priority:	0 (High)
DiffServ	ALL	TOS:	Normal-Service
		Code Point:	<input type="text"/> (0 - 63)
Search Term	<input type="text"/>		
Save		Cancel	

Figure 6: Setting up a Traffic Type to use ICA priority tags.

Once the appropriate Traffic Types have been created, they can be used in the Optimizer to control that traffic (e.g. manage bandwidth). Figure 7, below, shows a policy that controls peer-to-peer traffic by restricting the bandwidth it consumes to 5kbps.

### Optimizer Policies

?

[Add New Circuit](#)

Circuit	Virtual Circuit	Policy #	Schedule	Client	Direction	Server	Traffic Type	Edit	Delete
<b>10. Internet (512 kbps)</b>								Edit	Delete
<b>10.10. Internet (512 kbps)</b>								Edit	Delete
		<b>10</b>	ALWAYS	<b>Choke P2P (5 kbps)</b>				Edit	Delete
				ALL	↔	ALL	P2P-Gnutella		
				ALL	↔	ALL	P2P-BitTorrent		
				ALL	↔	ALL	P2P-Fasttrack		

Figure 7: Using layer 7 Traffic Types in the Optimizer.



Exinda strongly recommends that any traffic matched using a layer 7 traffic type is never discarded (blocked), but rather slowed down. During the packet inspection process, traffic can be falsely classified on very rare occasions. Nevertheless, if legitimate traffic is falsely matched as peer-to-peer, it should not be blocked.

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](mailto: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.

No part of this document may be reproduced, photocopied or transmitted without the express written consent of Exinda Networks.

### 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.