CAPABILITIES REVIEW

Exinda Network Orchestrator

Aurea SMB Solutions

Exinda Network Orchestrator gives Network professionals and IT Executives the at a glance visibility and intelligent recommendations to track network performance in real time and quickly take action to ensure exceptional network quality to their users and critical business applications that have direct impact on achieving SLAs, application adoption, at an affordable price.

Exinda Network Orchestrator enables network professionals with

- Robust policy engine drives actions on objects, users, apps, time, locations and activities.
- Layer 7 visibility into applications natively identifying +2000 applications.
- Directory integration for granular control by user and group.
- Application acceleration using: Data compression, deduplication, TCP Spoofing, & byte caching
- Performance benchmarking for key applications.
- Recommendations based on pattern and trend analysis.
- Centralized configuration and policy management for a fleet of thousands of Exinda appliances across locations.

Real time Traffic Monitoring

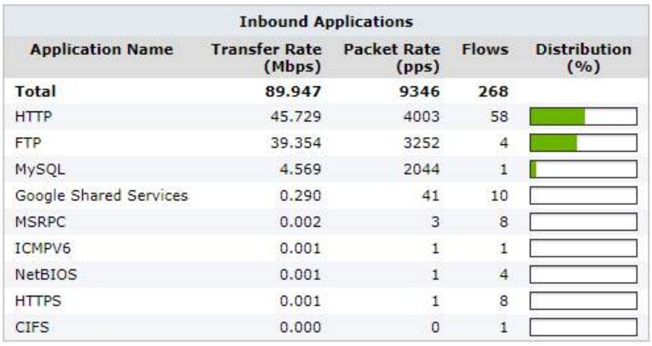
Exinda Network Orchestrator allows you to monitor your network, gaining full visibility into the applications users access, inbound traffic, outbound traffic and network throughput. This includes network interfaces, service levels, applications, network users, hosts, network conversations, subnets, virtual circuits and more, in real time. Easy to use graphs and charts will refresh every 1 second.

Application Monitoring

Applications in real time monitor show the top applications by throughput observed during the last 1 seconds. This report answers questions such as:

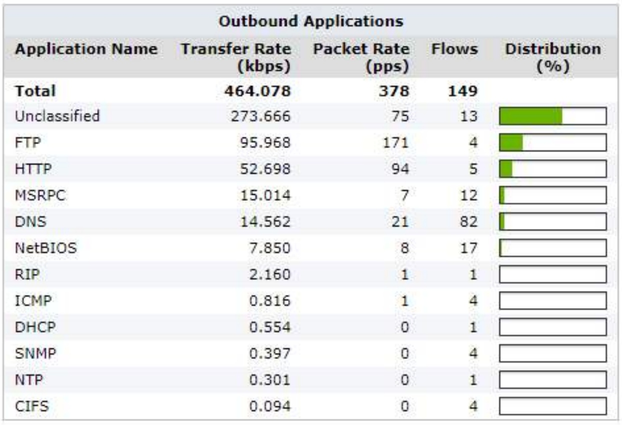
- My link is congested; which applications are on my network right now?
- How much bandwidth is BitTorrent using right now?

The Applications in Real Time monitor shows inbound application traffic separately from outbound application traffic. Traffic is sorted by transfer rate. The packet rate and a number of flows for each application in that 1 second period are also shown. The Distribution percentage shows the proportion of bandwidth consumption of each application relative to all applications.



Inbound Applications

Application Name	Transfer Rate (Mbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	**89.947**	**9346**	**268**	
HTTP	45.729	4003	58	
FTP	39.354	3252	4	
MySQL	4.569	2044	1	
Google Shared Services	0.290	41	10	
MSRPC	0.002	3	8	
ICMPV6	0.001	1	1	
NetBIOS	0.001	1	4	
HTTPS	0.001	1	8	
CIFS	0.000	0	1	



Outbound Applications

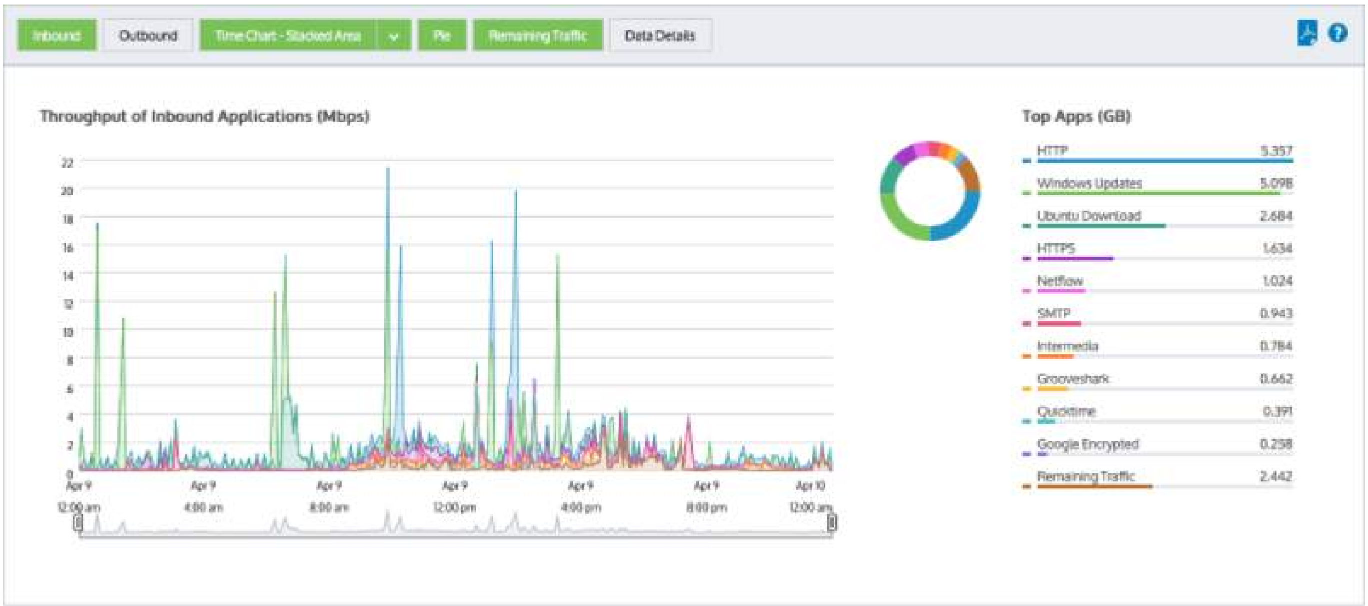
Application Name	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	**464.078**	**378**	**149**	
Unclassified	273.666	75	13	
FTP	95.968	171	4	
HTTP	52.698	94	5	
MSRPC	15.014	7	12	
DNS	14.562	21	82	
NetBIOS	7.850	8	17	
RIP	2.160	1	1	
ICMP	0.816	1	4	
DHCP	0.554	0	1	
SNMP	0.397	0	4	
NTP	0.301	0	1	
CIFS	0.094	0	4	

Application objects are used to classify traffic on the network and are made up of layer 7 signatures or TCP/UDP port numbers and port ranges. Application classification can be used to monitor traffic or to create application-specific policy. There are many (+2000) predefined applications on the appliance. You can add any applications that are not already in the list.

Applications can be created from various combinations of L7 signatures, TCP/UDP port numbers or ranges, and network objects.

Application Performance Metrics

Application Performance monitors generate reports that display information about application users, application performance, application bandwidth consumption, and the amount of reduction achieved (if applicable).



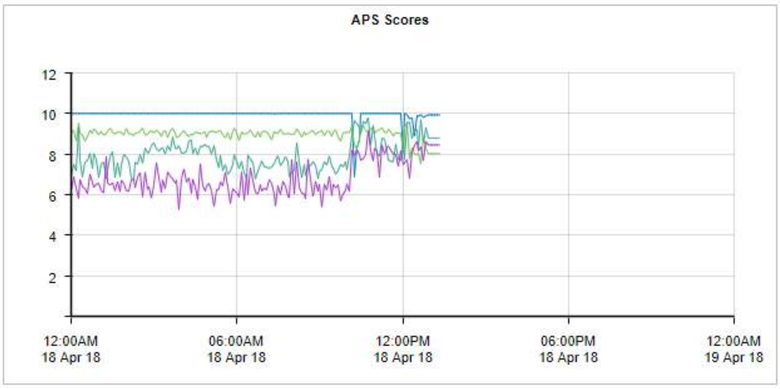
Top Apps (GB)

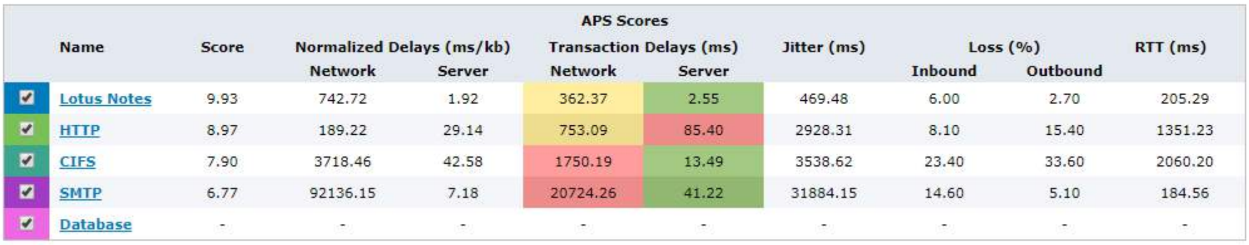
HTTP	5.357
Windows Updates	5.098
Ubuntu Download	2.684
HTTPS	1.634
Netflow	1.024
SMTP	0.943
Intermedia	0.784
Grooveshark	0.662
Quicktime	0.391
Google Encrypted	0.258
Remaining Traffic	2.442

The application performance metrics are used to generate an Application Performance Score (APS) that assess network performance and user experience when using business-critical applications regardless if they are natively detected by Exinda or you have defined them. These charts can answer questions such as:

- Are my important applications performing well from a network perspective for my network users?
- Has this been a persistent problem or is it getting worse?
- If an application is not performing well, what might be causing the problem?

These scores will use such metrics as Network delay, server delay, normalized network delay, normalized server delay, round-trip time, jitter, inbound loss, and outbound loss. Each metric that contributes to the score has a threshold value set. The threshold may be set manually or may have been determined automatically by the Exinda Appliance observing the traffic for the period of time to determine a baseline threshold value.





APS Scores

	Name	Score	Normalized Delays (ms/kb)		Transaction Delays (ms)		Jitter (ms)	Loss (%)		RTT (ms)
			Network	Server	Network	Server		Inbound	Outbound	
☑	Lotus Notes	9.93	742.72	1.92	362.37	2.55	469.48	6.00	2.70	205.29
☑	HTTP	8.97	189.22	29.14	753.09	85.40	2928.31	8.10	15.40	1351.23
☑	CIFS	7.90	3718.46	42.58	1750.19	13.49	3538.62	23.40	33.60	2060.20
☑	SMTP	6.77	92136.15	7.18	20724.26	41.22	31884.15	14.60	5.10	184.56
☑	Database	-	-	-	-	-	-	-	-	-

Data Caching (Edge Caching)

Provides acceleration of static web content such as HTML, GIF, JPEG, ZIP, RAR, ISO as well as dynamic content including Google Video, Vimeo. Enables single-sided caching of Internet-based content, including web objects, videos and software updates. Data Cache requires only one Exinda appliance and is also known as Edge Cache.

When web objects are downloaded from the Internet or across WAN links, Edge Cache stores them at the edge of the network. When subsequent requests come for the same material, the content is quickly delivered from Edge Cache, without the need to download the data again over the WAN. The result is the ability to experience LAN speeds of WAN objects, and provide users with a better network experience.

Through the upload of your trusted certificate, Exinda can also support HTTPS caching.

Policies are set up using the same simple policy creator to optimize your network and leverage Edge Caching where applicable.

Dynamic Policies

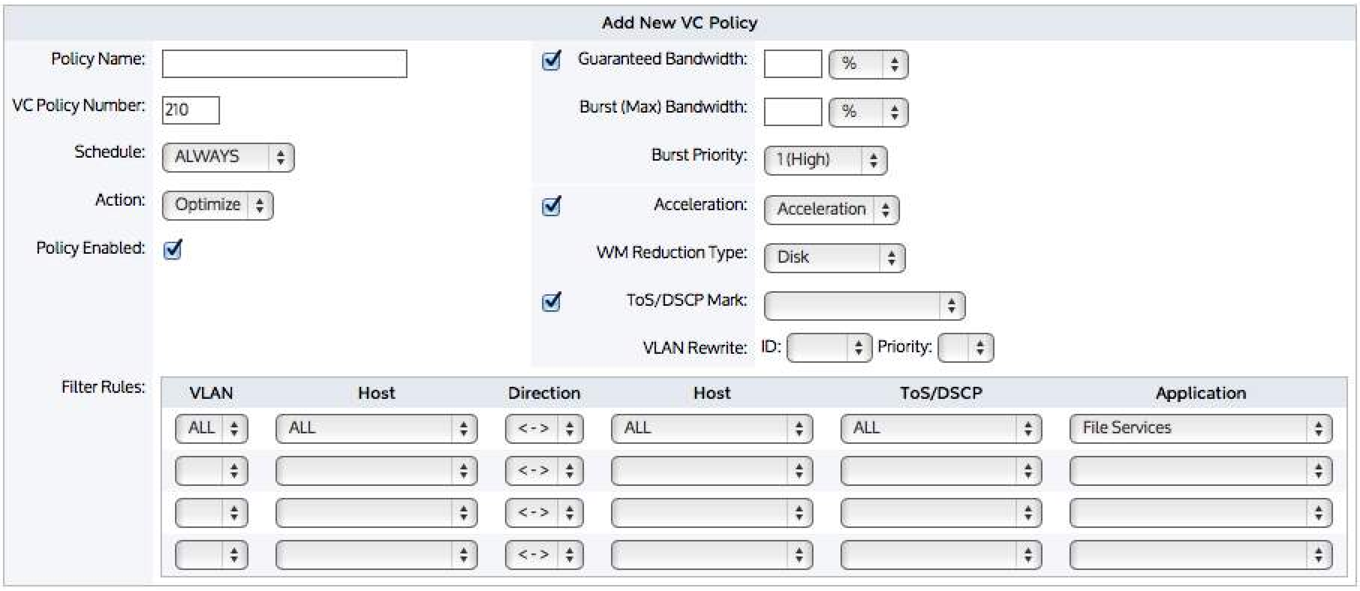
Policies define what actions to perform on specific targeted traffic. Policies can be applied and grouped into “virtual circuits”. The policies can specify whether:

- to optimize the traffic by bandwidth shaping, acceleration, or marking the packets.
- to block the traffic by discarding the packets.
- to monitor the traffic by ignoring the packets.
- or to redirect the traffic to a specific URL.

The policy managed traffic can then be filtered by:

- Application or application group
- Hosts or subnets and users, groups of users (from AD)
- Hosts or subnets that are communicating with other specific hosts or subnets
- VLAN
- ToS/DSCP markings

You can apply any combination of these filters and schedule them. For example, the policy could be targeted to traffic between a particular branch and headquarters, which has particular ToS markings on a particular VLAN during work hours. Furthermore, you can also add more than one filter.



Add New VC Policy

Policy Name:

VC Policy Number: 210

Schedule: ALWAYS

Action: Optimize

Policy Enabled: ☑

☑ Guaranteed Bandwidth: %

Burst (Max) Bandwidth: %

Burst Priority: 1 (High)

☑ Acceleration: Acceleration

WM Reduction Type: Disk

☑ ToS/DSCP Mark:

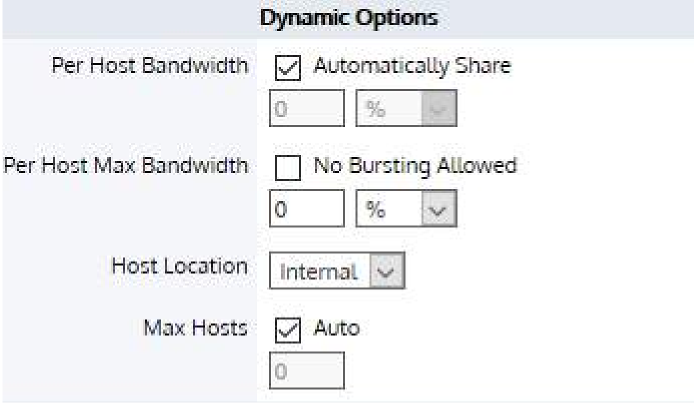
VLAN Rewrite: ID: Priority:

Filter Rules:

VLAN	Host	Direction	Host	ToS/DSCP	Application
ALL	ALL	<->	ALL	ALL	File Services
		<->			
		<->			
		<->			

Virtual circuits are created within circuits in the policy tree and are used to logically divide or partition the circuit. The virtual circuit defines what traffic will be processed in this partition and how much bandwidth it is allowed. The virtual circuit can enforce fair sharing amongst the network hosts. Traffic is evaluated against the defined filters of the virtual circuit. Traffic that does not fall within the virtual circuit is evaluated by the next virtual circuit and so on. Each virtual circuit will have it's own set of policy rules.

Allocation of bandwidth can be dynamically applied within virtual circuits and the policies they hold.

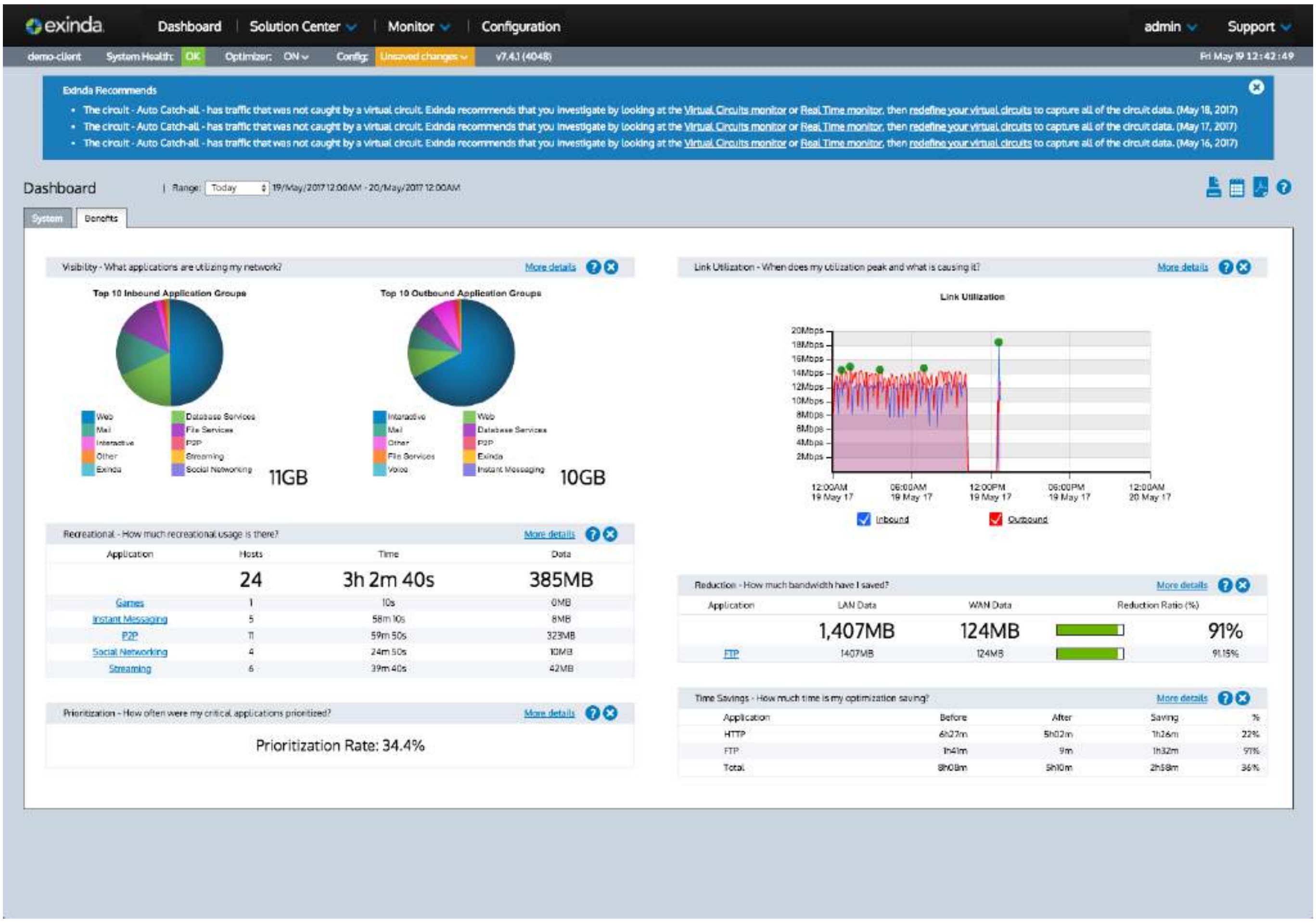


Dynamic Options

Per Host Bandwidth	☑ Automatically Share 0 %
Per Host Max Bandwidth	□ No Bursting Allowed 0 %
Host Location	Internal
Max Hosts	☑ Auto 0

Recommendation Engine

The Exinda appliance analyzes the traffic and makes recommendations based on what it learned about your traffic. These recommendations appear in blue at the top of the dashboard.



demo-client System Health: OK Optimizer: ON Config: Unsaved changes v7.4.1 (4048) Fri May 19 12:42:49

Exinda Recommends

- The circuit - Auto Catch-all - has traffic that was not caught by a virtual circuit. Exinda recommends that you investigate by looking at the Virtual Circuits monitor or Real Time monitor, then redefine your virtual circuits to capture all of the circuit data. (May 18, 2017)
- The circuit - Auto Catch-all - has traffic that was not caught by a virtual circuit. Exinda recommends that you investigate by looking at the Virtual Circuits monitor or Real Time monitor, then redefine your virtual circuits to capture all of the circuit data. (May 17, 2017)
- The circuit - Auto Catch-all - has traffic that was not caught by a virtual circuit. Exinda recommends that you investigate by looking at the Virtual Circuits monitor or Real Time monitor, then redefine your virtual circuits to capture all of the circuit data. (May 16, 2017)

Dashboard | Range: Today 19/May/2017 12:00AM - 20/May/2017 12:00AM

Visibility - What applications are utilizing my network? More details

Link Utilization - When does my utilization peak and what is causing it? More details

Recreational - How much recreational usage is there? More details

Application	Hosts	Time	Data
	24	3h 2m 40s	385MB
Games	1	10s	0MB
Instant Messaging	5	58m 10s	8MB
P2P	11	59m 50s	323MB
Social Networking	4	24m 50s	10MB
Streaming	6	39m 40s	42MB

Prioritization - How often were my critical applications prioritized? More details

Prioritization Rate: 34.4%

Reduction - How much bandwidth have I saved? More details

Application	LAN Data	WAN Data	Reduction Ratio (%)
	1,407MB	124MB	91%
FTP	1407MB	124MB	91.15%

Time Savings - How much time is my optimization saving? More details

Application	Before	After	Saving	%
HTTP	6h27m	5h02m	1h26m	22%
FTP	1h41m	9m	1h32m	91%
Total	8h08m	5h10m	2h58m	36%

The following are examples of the kinds of recommendations that the Exinda may make:

„The applications „app-name-1" and „app-name-2" are appearing in the top 10 for the first time in the preceding seven days. Exinda recommends that you create a policy to control or protect this traffic."

Every night, the Exinda appliance looks at the top ten applications by data volume and determines if any of the applications are new to the top ten. That is, when looking at the data for the day, have any of the top ten applications not been in the daily top ten for the seven preceding days.

„The circuit „circuit-name" has traffic that was not caught by a virtual circuit. Exinda recommends that you investigate by looking at the Virtual Circuits monitor or Real Time monitor, then redefine your virtual circuits to capture all of the circuit data."

Every night, the Exinda appliance looks at the traffic and determines whether traffic is showing up in any Auto Catch-all virtual circuits. It then reports traffic in the Auto-Catch-all virtual circuit if > 1% of the traffic of your entire appliance is caught in the single Auto Catch-all virtual circuit.

Central Management

The Exinda Management Center (EMC) provides complete management insight and configuration control of your Exinda Network Orchestrator appliances from one central console. All applications, devices, users, and activities across all network locations are managed from a central location giving IT Administrators the ability to manage network policies and manage appliance configuration across the entire organization.

You can configure Exinda Appliances and monitor network usage directly from the appliance. However, once you have more than a few appliances to manage, it can become difficult to manage them individually and maintain standard configurations when needed.

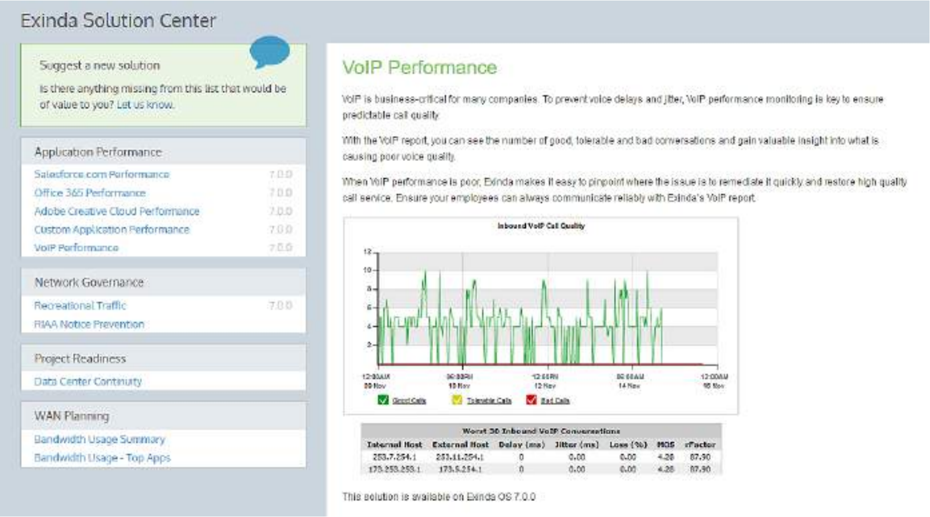
The Exinda Management Center solves the management gap by enabling policy configuration on multiple appliances.

In-depth Reporting & Solution Center

The Exinda Solution Center provides a series of predefined monitors you can run to generate network performance reports for applications like FTP, SSH, Salesforce.com, Office365 VoIP and many more.

- The generated reports answer questions, such as:
- How is salesforce.com performing for network users?
- How are critical applications performing on the network?
- How can I best mitigate data center disasters?

Each solution description indicates which Exinda OS version is required to run the solution, shown both in the solution list and in each solution description. You may need to upgrade your Exinda OS version to take advantage of the desired solutions. Some solutions may not yet be available and are shown as 'Coming soon'.



Exinda Solution Center

Suggest a new solution

Is there anything missing from this list that would be of value to you? Let us know.

Application Performance

Salesforce.com Performance	7.0.0
Office 365 Performance	7.0.0
Adobe Creative Cloud Performance	7.0.0
Custom Application Performance	7.0.0
VoIP Performance	7.0.0

Network Governance

Recreational Traffic	7.0.0
RIAA Notice Prevention	

Project Readiness

Data Center Continuity

WAN Planning

Bandwidth Usage Summary

Bandwidth Usage - Top Apps

VoIP Performance

VoIP is business-critical for many companies. To prevent voice delays and jitter, VoIP performance monitoring is key to ensure predictable call quality.

With the VoIP report, you can see the number of good, tolerable and bad conversations and gain valuable insight into what is causing poor voice quality.

When VoIP performance is poor, Exinda makes it easy to pinpoint where the issue is to remediate it quickly and restore high quality call service. Ensure your employees can always communicate reliably with Exinda's VoIP report.

Worst 30 Inbound VoIP Conversations

Internal Host	External Host	Delay (ms)	Jitter (ms)	Loss (%)	MOS	rFactor
253.7.254.1	253.11.254.1	0	0.00	0.00	4.28	87.90
173.253.253.1	173.5.254.1	0	0.00	0.00	4.28	87.90

This solution is available on Exinda OS 7.0.0

In addition to the Solution Center, PDF reports can be generated and downloaded on demand or generated and emailed at scheduled intervals. The content of the PDF reports can be configured in two ways:

- exploring the data in the monitor screens and requesting a report
- going to the Report page to configure the details of the PDF report

The following PDF report generation scenarios are supported:

- Explore the data in the monitor screens and generate an ad hoc PDF report of what is shown on the screen.
- Explore the data in the monitor screens and schedule a PDF report to be generated using the configuration and filters shown on the screen.
- Configure a PDF report using the Report page .
- Configure a PDF report using the Report page and request an on-demand generation of the PDF report.

In depth reporting is available to analyze based on traffic direction and granularity over time. The data and interactive time graphs can be used to view:

- Traffic in real time
- Traffic by network interfaces, applications, network users, hosts, conversations, subnets and virtual circuits and more.

SSL Common Name Policies

Exinda Network Orchestrator provides the ability to monitor traffic even if it is encrypted with SSL. Https traffic will identify from the SSL certificate the common name or organization name which is in most cases domain/website name. This information is then used to define the traffic as an application and then use it in the policies.

Https traffic is nearly standard for basic security even for internal network traffic, and most applications out of the network require it. This leaves large swaths of network traffic that without visibility, cannot be properly managed. Exinda Network Orchestrator allows Network Engineers to categorize and identify the https traffic via the SSL certificate and create policies based on the common name identified to get full management of all your traffic.

Exinda Network Orchestrator - Capabilities Cheat Sheet

Real Time Traffic Monitoring

Exinda Network Orchestrator allows you to monitor your network, gaining full visibility into the applications users access, inbound traffic, outbound traffic and network throughput.

Application Monitoring

Applications in the real time monitor show inbound application traffic separately from outbound application traffic. Traffic is sorted by transfer rate. The packet rate and a number of flows for each application in that period are also shown. There are many (+2000) predefined applications on the appliance. You can add any applications that are not already in the list.

Application Performance Metrics

Application Performance monitors generate reports that display information about application users, application performance, application bandwidth consumption, and the amount of reduction achieved (if applicable). The application performance metrics are used to generate an Application Performance Score (APS) that assess network performance and user experience when using business-critical applications regardless if they are natively detected by Exinda or you have defined them.

Data Caching (Edge Caching)

Provides acceleration of static web content such as HTML, GIF, JPEG, ZIP, RAR, ISO as well as dynamic content including YouTube, Google Video, Vimeo. Enables single-sided caching of Internet-based content, including web objects, videos and software updates. Data Cache requires only one Exinda appliance and is also known as Edge Cache.

Dynamic Policies

Policies define what actions to perform on specific targeted traffic. Policies can be applied and grouped into “virtual circuits”. The policies can specify whether to optimize the traffic by bandwidth shaping, acceleration, or marking the packets. They can also block the traffic by discarding the packets, monitor the traffic by ignoring the packets and redirect the traffic to a specific URL.

Recommendation Engine

The Exinda appliance analyzes the traffic and makes recommendations based on what it learned about your traffic. These recommendations appear in blue at the top of the dashboard.

Central Management

The Exinda Management Center (EMC) provides complete management insight and configuration control of your Exinda Network Orchestrator appliances from one central console. All applications, devices, users, and activities across all network locations are managed from a central location.

In depth Reporting & Solution Center

The Exinda Solution Center provides a series of predefined monitors you can run to generate network performance reports for applications like FTP, SSH, Salesforce.com, Office365 VoIP and many more. In depth reporting is available to analyze based on traffic direction and granularity over time. The data and interactive time graphs can be used to view traffic in real time, traffic by network interfaces, applications, network users, hosts, conversations, subnets and virtual circuits and more.

SSL Common Name Policies

Exinda Network Orchestrator provides the ability to monitor traffic even if it is encrypted with SSL. Https traffic will identify from the SSL certificate the common name or organization name which is in most cases domain/website name. This information is then used to define the traffic as an application and then use it in the policies.