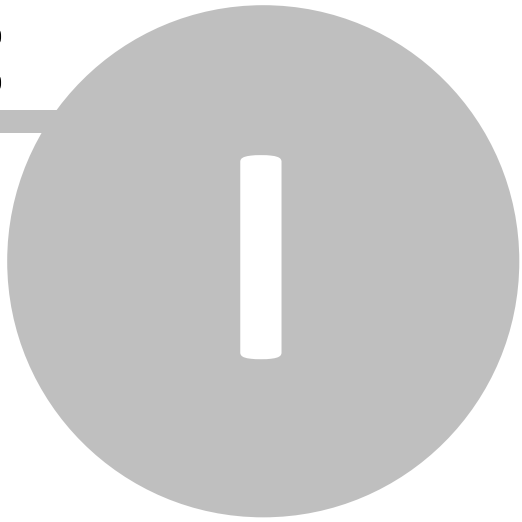
Exinda Topologies Guide

Exinda Firmware Version 6.1

Table of Contents

Part



1 Introduction

Exinda Topologies Guide

Exinda Firmware Version: 6.1

1.1 Using this Guide

Throughout the manual the following text styles are used to highlight important points:

- Useful features, hints and important issues are called "notes" and they are identified in a light blue background.

Note: This is a note.

- Practical examples are presented throughout the manual for deeper understanding of specific concepts. These are called "examples" and are identified with a light green background.

This is an example.

- Warnings that can cause damage to the device are included when necessary. These are indicated by the word "caution" and are highlighted in yellow.

Caution: This is a caution.

1.2 Further Reading

In addition to this Topologies Guide, the following additional user documentation is available:

- Exinda Quick Start Guides
- Exinda User Manual
- Exinda Command Line Interface (CLI) Reference Guide
- Exinda "How To" Guides

Please visit http://www.exinda.com for more information.

Part

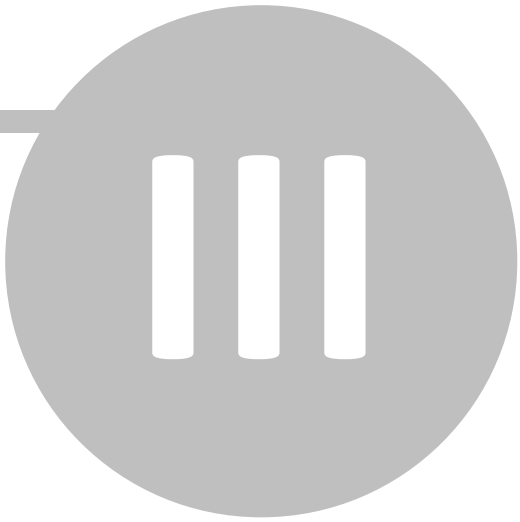
2 Platforms

The bridge and interface configuration differs between each Exinda platform. The table below summarizes the available bridges for each platform (without expansion cards installed).

Platform	Default Bridge (interfaces) / Bypass Support
1010	br0 (eth0 eth1) / no bypass br1 (eth2 eth3) / bypass
2000	br0 (eth0 eth1) / no bypass br1 (eth2 eth3) / bypass
2060	br1 (eth1 eth2) / bypass br3 (eth3 eth4) / bypass
4000	br0 (eth0 eth1) / no bypass br1 (eth2 eth3) / bypass
4060	br10 (eth10 eth11) / bypass
4061	br10 (eth10 eth11) / bypass
5000	br0 (eth2 eth3) / bypass br1 (eth4 eth5) / bypass br2 (eth6 eth7) / bypass
6000	br0 (eth1 eth2) / fiber br1 (eth3 eth4) / bypass br2 (eth5 eth6) / bypass
6010	br0 (eth2 eth3) / bypass br1 (eth4 eth5) / bypass
6060	br10 (eth10 eth11) / bypass
7000	br0 (eth2 eth3) / bypass br1 (eth4 eth5) / bypass
8060	br10 (eth10 eth11) / bypass
10060	br10 (eth10 eth11) / bypass

Table 1: List of platforms and supported bridges

Part

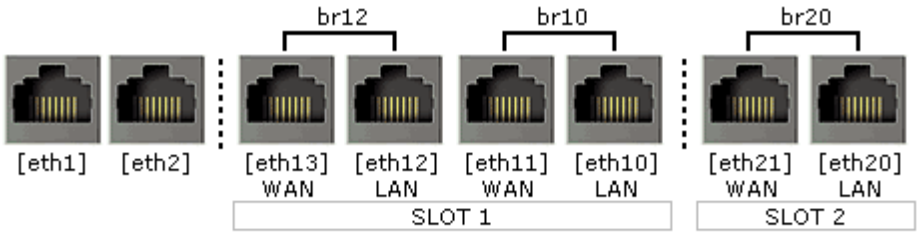


3 IP Modes

Exinda OS (ExOS) version 6 and later allows you to configure the appliances network interfaces to suit your network topology. To configure network interfaces, navigate to System | Network | IP Address on the Web User Interface, Advanced mode. Ensure that you understand the target network environment before changing settings on this page.

Note 1: interfaces that are not enslaved to a bridge may have roles assigned e.g. Cluster, Mirror or WCCP.

Note 2: the interface used to manage the appliance will depend on the network topology. In general any interface not assigned to a role may be used.



IP Settings

eth1	Role:	☐ Cluster ☐ Mirror ☐ WCCP
	Autoconf:	Static
	Addresses:	172.16.1.240 / 23
	Comment:	
eth2	Role:	☐ Cluster ☐ Mirror ☐ WCCP
	Autoconf:	Static
	Addresses:	/
	Comment:	
br10 ☑	Autoconf:	Static
	Addresses:	/
	Comment:	
br12 ☑	Autoconf:	Static
	Addresses:	/
	Comment:	
br20 ☑	Autoconf:	Static
	Addresses:	/
	Comment:	

Default Route: 172.16.1.254

Figure 1: IP settings configuration on the Web User Interface.

Some topologies may require you to configure a specific failover mode for a bridge. To configure the failover mode of a bridge, navigate to System | Network | NIC's.

Use the form below to configure bypass state and failover settings.

Note: ***Take care when making changes here as this appliance may become unreachable.***

Bridge	Status	Running Mode	Enable Failover	On Failover
br10	Active	Active	☑	Bypass
br12	Active	Active	☑	Bypass
br20	Active	Active	☑	Bypass

Figure 2: bridge bypass state and failover mode

Part

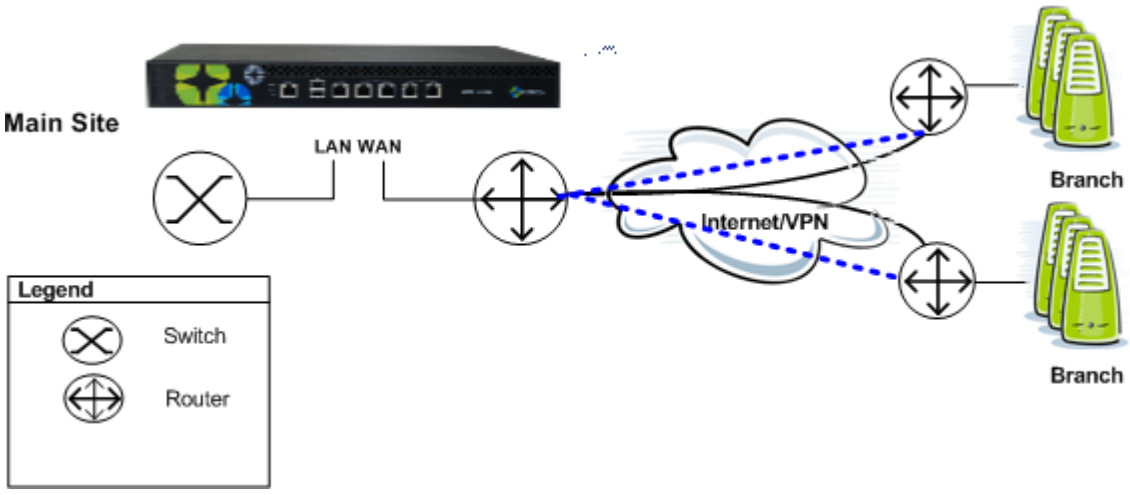
4 Main Site Internet Link Topology

Main site with Internet link and potentially branch offices as well. Applications are hosted in the Main Site where branch offices connect to via the Internet.

All platforms support this topology.

4.1 Reason for this Topology

This topology is used when customers need to monitor and control Internet and branch traffic to and from the main site. The Exinda can guarantee performance of critical applications such as voice, VPN and extranet; monitor Internet usage and control P2P applications.



4.2 Installation

The Exinda should be plugged in-line between the switch and router or firewall. If you have a VPN refer to "Topologies with VPNs".

1. Connect the WAN port to your router/firewall using a crossover cable.
2. Connect the LAN port into the LAN switch.

It is recommended that you use a bypass capable bridge, which will provide ethernet bypass in the event of hardware failure (refer to Table 1). The bridge in use also needs to be enabled on the IP Address configuration page (Figure 1)

4.3 Capabilities

In this topology, the Exinda appliance can:

- Monitor all traffic utilization and all applications to/from the Internet. You can distinguish between business relevant traffic and traffic used for recreational purposes.
- Monitor usage of Internet and VPN branch traffic. e.g. How much of the link is being used by each branch network?
- Control all traffic traversing the link. Allocate some bandwidth to VPN branch offices and respective priorities for Internet applications.

4.4 Limitations

- With this topology, it is not possible to monitor and control branch traffic and their respective Internet links as each branch has direct access to the Internet.
- Application Acceleration is not possible with a single appliance.

4.5 Suggestions

- Disable direct access to the Internet for branch offices. Route all Internet traffic via the main site if possible.
- Use an Exinda appliance at each branch office to monitor and control traffic and increase WAN capacity with Exinda's Application Acceleration.

Part V

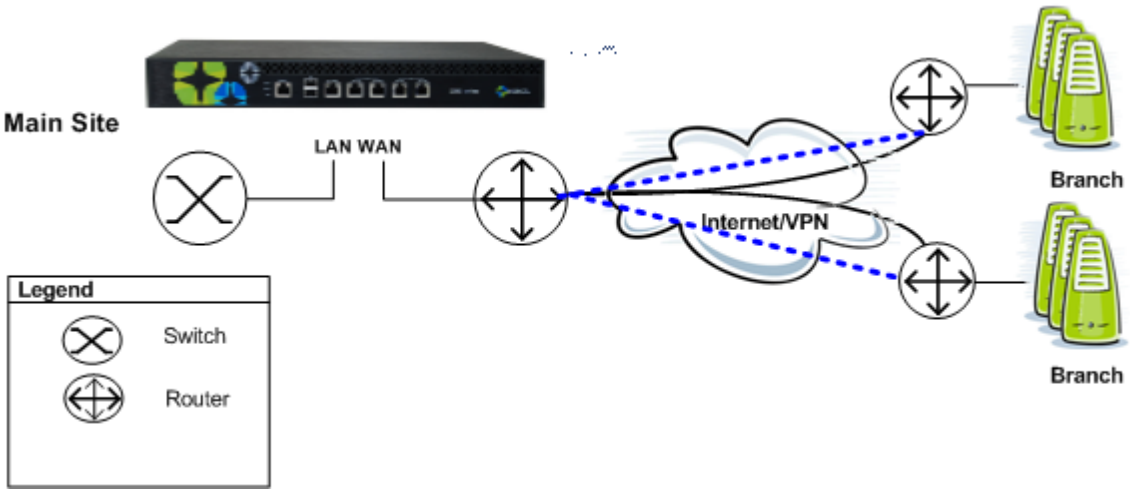
5 Main Site WAN Link Topology

Single site with Internet link and separate WAN link to branch offices.

All platforms support this topology.

5.1 Reason for this Topology

This topology is used when customers need to monitor and control Internet and WAN traffic in the main site and WAN traffic from branch offices. The Exinda can guarantee traffic for the WAN and treat applications and users from different branch offices with different priorities.



5.2 Installation

The Exinda should be plugged in-line between the switch and router or firewall. If you have a VPN refer to "Topologies with VPNs".

1. Connect the WAN port to your router/firewall using a crossover cable.
2. Connect the LAN port into the LAN switch.

It's recommended that you use a bypass capable bridge, which will provide ethernet bypass in the event of hardware failure (refer to Table 1). The bridge in use needs to be enabled on the IP Address configuration page (refer to Figure 1).

5.3 Capabilities

In this topology, the Exinda appliance can:

- Monitor all traffic utilization and all applications to the Internet. You can distinguish between business relevant traffic and traffic used for recreational purposes.
- Monitor usage of Internet and WAN traffic. E.g. How much of the link is being used by the Internet and each branch office?
- Monitor and control individual applications and users from each branch office.
- Control all traffic traversing the link. Allocate bandwidth to WAN and Internet applications.

5.4 Limitations

- Application Acceleration is not possible with a single appliance.
- If a branch office connects to Internet directly, the branch link cannot to be monitored and controlled.

Part VI

6 Distributed Branch Topology

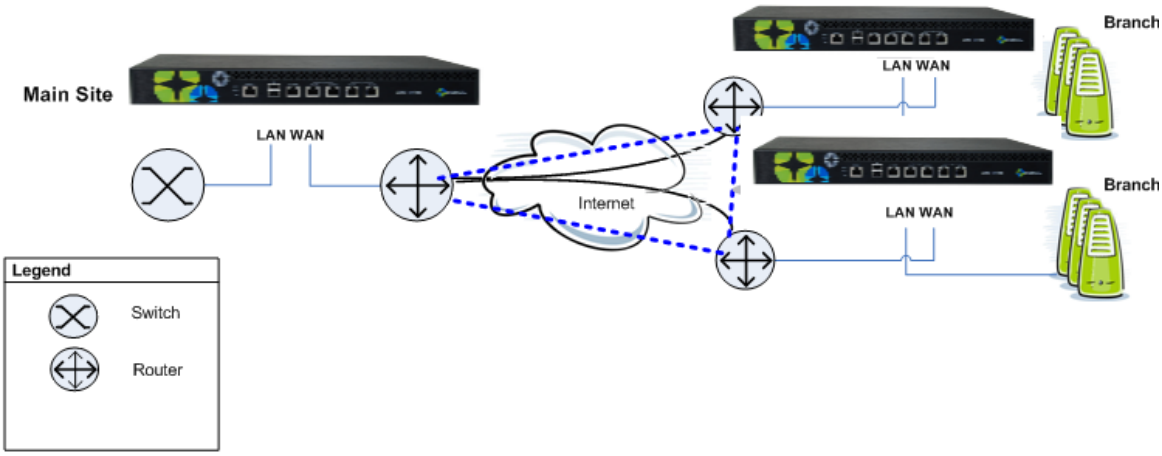
A distributed topology of Exinda appliances offers the most flexible control. Such topology is also required for customers using Exinda's Application Acceleration technology.

All platforms support this topology.

Note: Application Acceleration is possible with this topology. An acceleration license is required for Application Acceleration to be enabled. An acceleration license is not available on the 1010 platform.

6.1 Reason for this Topology

This topology is used to monitor and control all nodes in a distributed branch office environment. As both WAN and Internet can be accessed directly from each office, an Exinda is used to monitor and manage the performance of each branch office.



6.2 Installation

An Exinda is required at all branch offices connecting to the WAN. The Exinda will need to be installed in in-line mode at each office.

It's recommended that you use a bypass enabled bridge (refer to Table 1), which will provide ethernet bypass in the event of hardware failure. The bridge in use needs to be enabled on the IP Address configuration page (refer to Figure 1).

6.3 Capabilities

In this topology, the Exinda appliance can:

- Monitor and control all traffic to/from the Internet and WAN.
- Accelerate traffic between all WAN sites.
- Monitor distribution of application traffic between all sites.
- Prioritize and manage application performance in a fully meshed environment.
- Control or block P2P and recreational applications site-wide.

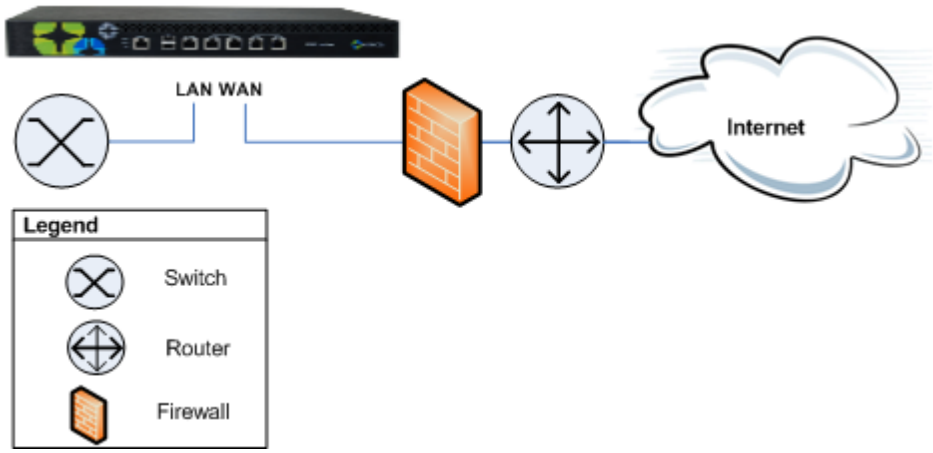
6.4 Limitations

None - this is the most flexible topology.

Part

7 Topologies with Firewalls

Firewall topologies can vary significantly. Typically customers will place the Exinda between the switch and internal interface of the firewall. This ensures that the Exinda can see all hosts on the LAN.

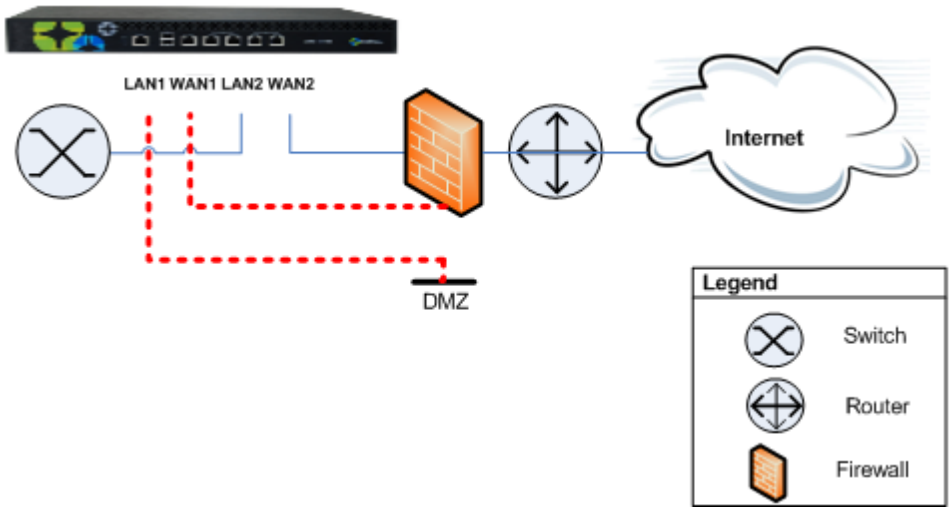


All platforms support this topology.

Note: Placing the Exinda appliance between the router and external interface of the firewall will only monitor applications and IP addresses present on the external interface of the firewall. So if your firewall performs Network Address Translation (NAT), you will only see the firewall's external IP address as the source address of the monitored flows, rather than their internal addresses.

7.1 DMZ

The Exinda appliance can be deployed in-path of a DMZ, allowing for Monitoring, Optimization and Application Acceleration of traffic to/from the DMZ.



Note: You will need to define a Network Object called DMZ and mark it as "Internal", so that the Exinda appliance can ignore all traffic between the local LAN and the DMZ.

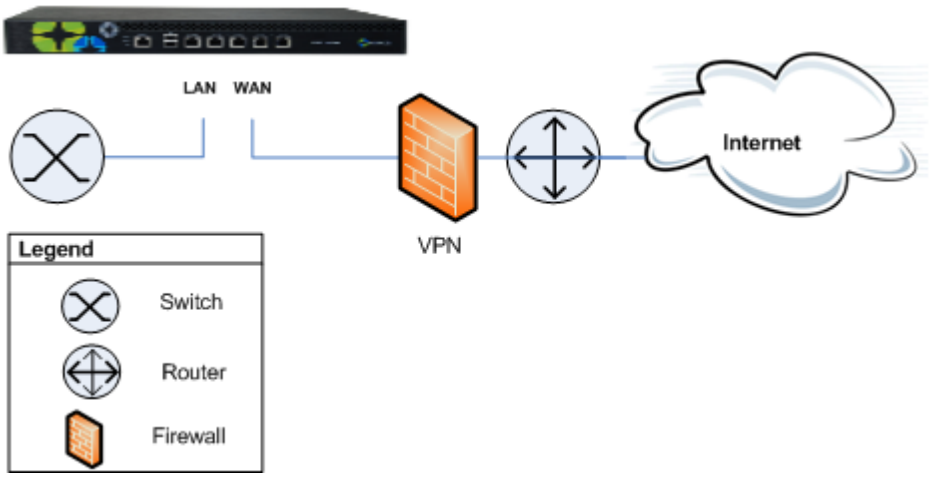
7.2 Installation

1. Enable the appropriate bridges on the IP Address configuration page (refer to Figure 1).
2. Connect Exinda WAN2 into your router/firewall using a crossover cable.
3. Connect Exinda LAN2 into the LAN switch.
4. Connect Exinda LAN1 into the DMZ switch or host.
5. Connect Exinda WAN1 in the DMZ interface of the firewall using a crossover cable.

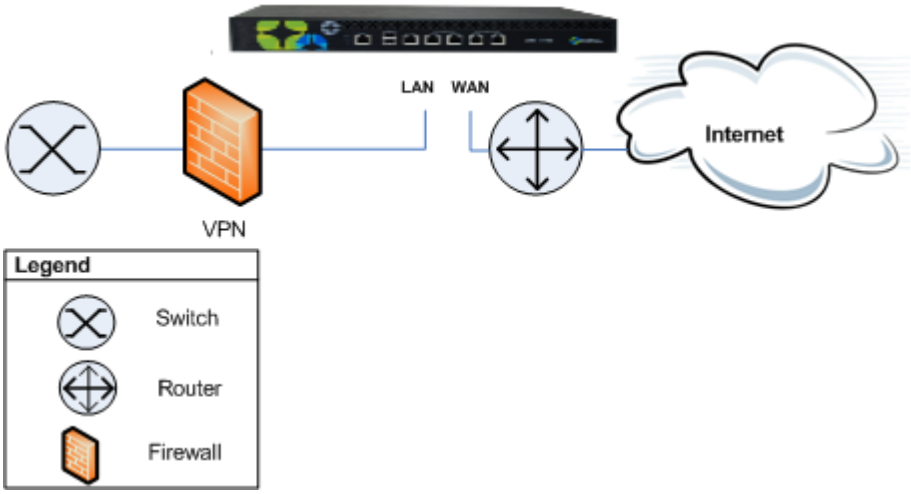
Part

8 Topologies with VPNs

Scenario 1: Typically customers will place the Exinda between their internal LAN switch and VPN terminator. This allows for monitoring and optimization of traffic before it gets encrypted and transported across the VPN tunnel.



Scenario 2: There are scenarios where the Exinda can only plug in between the VPN terminator and the router. In this scenario only encrypted tunnel traffic will be seen by the Exinda appliance. Typically traffic of the GRE or ESP protocol will be present.



All platforms support this topology.

8.1 Installation

Scenario 1:

1. Connect the Exinda WAN port into the internal interface of the VPN terminator using a crossover cable.
2. Connect the Exinda LAN port into the LAN switch.

Scenario 2:

1. Connect the Exinda WAN port into the internal interface of the router.
2. Connect the Exinda LAN port into the external interface of the VPN terminator using a crossover cable.
3. Connect an Exinda unbridged interface (e.g. eth1 on a 4060) into the LAN switch and configure an address to manage the appliance (refer to Figure 1)

8.2 Capabilities

In VPN scenario 2, the Exinda appliance can:

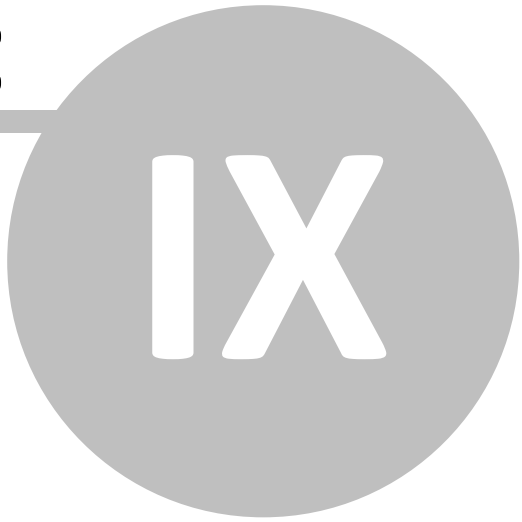
- Monitor and control any unencrypted traffic to the WAN and Internet.
- Monitor and prioritize the encrypted traffic between other VPN terminator sites. Only a single IP address will be visible per site.

8.3 Limitations

In VPN scenario 2 the Exinda appliance cannot:

- Monitor and prioritize the encrypted traffic by application, internal hosts and servers.

Part



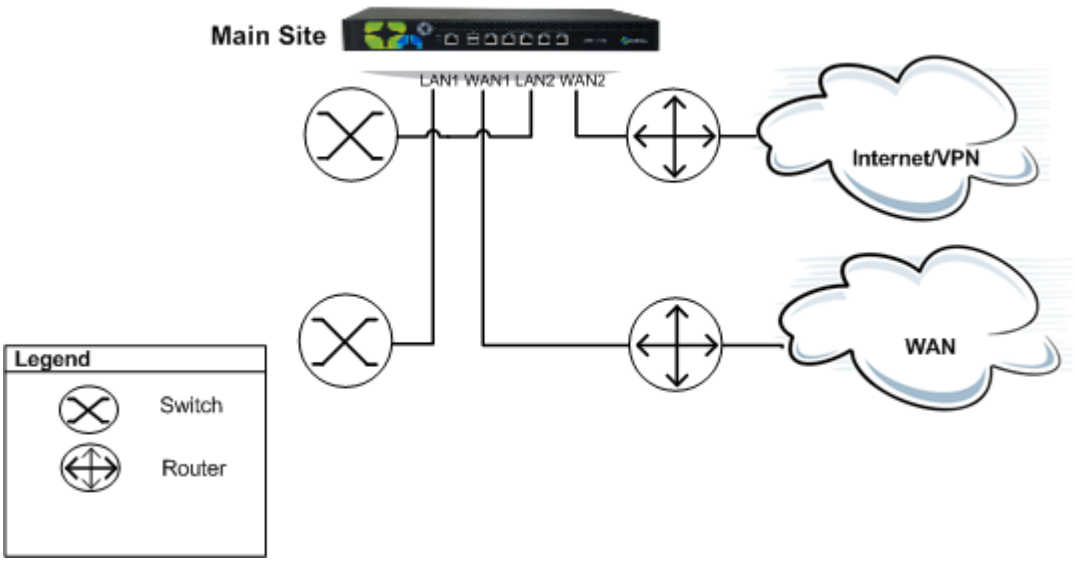
9 Multiple Link Topology

Exinda appliances can support multiple bridges, allowing users to connect multiple links through the appliance.

All platforms support this topology, however, some platforms only have a single bypass enabled bridge (refer to Table 1), which will provide ethernet bypass in the event of hardware failure.

9.1 Reason for this Topology

This topology is used when customers need to monitor and control Internet traffic to and from the main site as well as WAN traffic through a single Exinda appliance.



9.2 Installation

The Exinda should be plugged in-line between the switch and router or firewall.

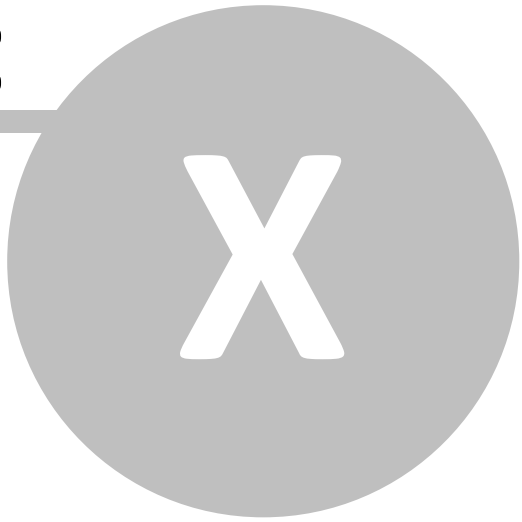
1. Connect the Exinda WAN1 port into your WAN router/firewall using a crossover cable.

2. Connect the Exinda LAN1 port into the LAN switch.

3. Connect the Exinda WAN2 port into your Internet router/firewall using a crossover cable.

4. Connect the Exinda LAN2 port into the LAN switch.

Part



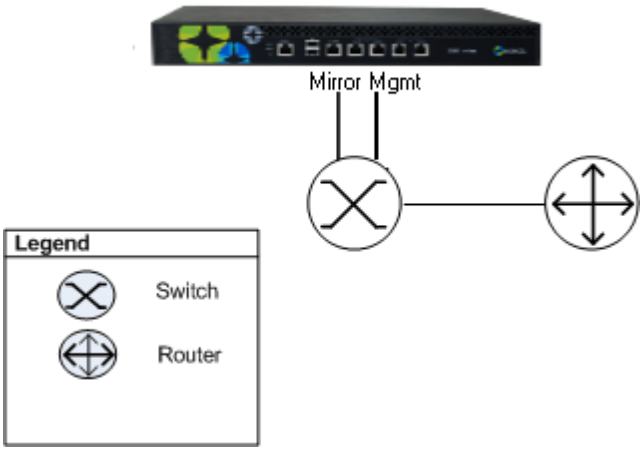
10 Out of Path - Monitor

The Exinda appliance can operate out-of-path for monitoring (e.g. ON-LAN mode) with any hub or switch (that supports port mirroring or SPAN ports).

All platforms support this topology.

10.1 Reason for this Topology

This topology is used when customers need to monitor only, without installing the Exinda in-line. The Exinda will monitor and report on all applications presented on the SPAN/mirror port. This is regularly used to perform network audits as it provides great flexibility in restricted and complex network environments.



10.2 Installation

1. From the the IP Address configuration page (Figure 1) assign a Mirror interface. Choose a second interface to manage the appliance and set an address on this interface.

2. Connect the second (management) interface on the Exinda into the switch.

3. Setup port mirroring from the port that is connected to the router, port X, to be mirrored onto port Y (span or mirror port) on the switch/router.

4. Connect the Exinda Mirror interface into switch port Y.

Note: All internal subnets must be correctly defined as "Internal" Network Objects on the Exinda appliance so that the appliance can correctly monitor and report on the mirrored data.

10.3 Capabilities

The Exinda appliance in mirror mode can:

- Be deployed out-of-path.
- Work with any SPAN ports, mirrored switched ports or hubs connecting to multiple hosts.

10.4 Limitations

- Interface and PPS Reports will not be available.
- Optimization (QoS and Application Acceleration) cannot be performed in this mode.

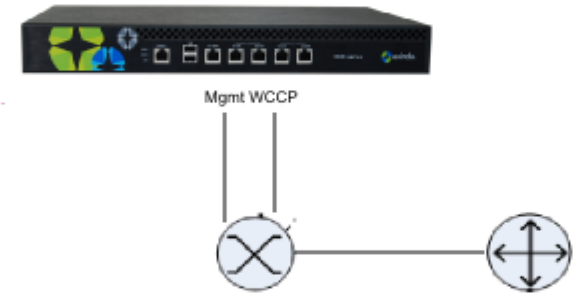
10.5 Suggestions

- Be cautious when using SPAN and port mirror - mirrored traffic should not be presented back to the switch. This would create a “switch loop” and may interrupt the operation of the switch.
- Setup “Network Objects” to define the subnets you wish to monitor as all the traffic is incoming to a single port.

Part

11 Out of Path - Acceleration

This features enables an Exinda to accelerate in an out-of-path topology. The router must support WCCP to use this topology.



11.1 Installation

1. From the the IP Address configuration page (Figure 1) assign a WCCP interface and set an address on this interface. Choose a second interface to manage the appliance and also set an address on this interface.
2. Connect the second (management) interface on the Exinda into the switch.
3. Configure WCCP on both the Exinda and the router. Refer to the WCCP Howto Guide for details.
4. Connect the WCCP interface on the Exinda into the switch.

11.2 Capabilities

The Exinda appliance in WCCP mode can:

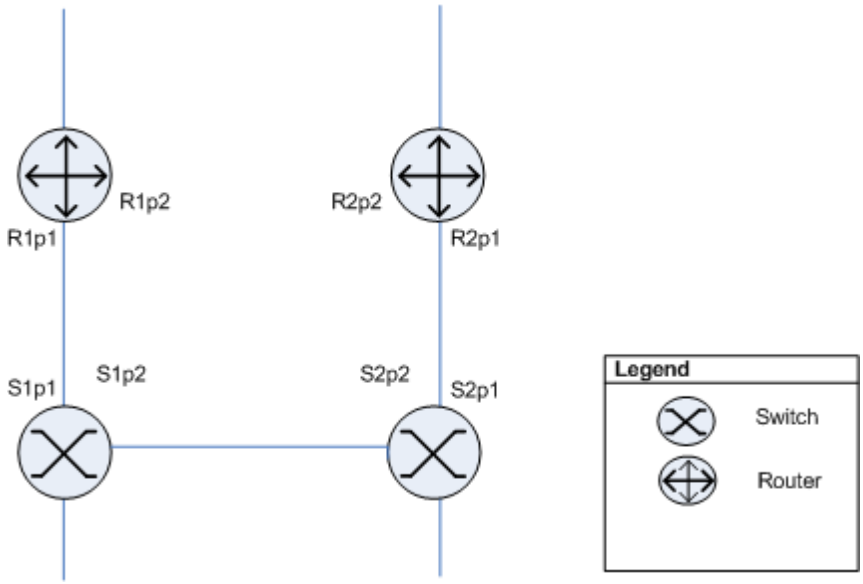
- accelerate TCP based applications out-of-path
- monitor TCP based applications

11.3 Suggestions

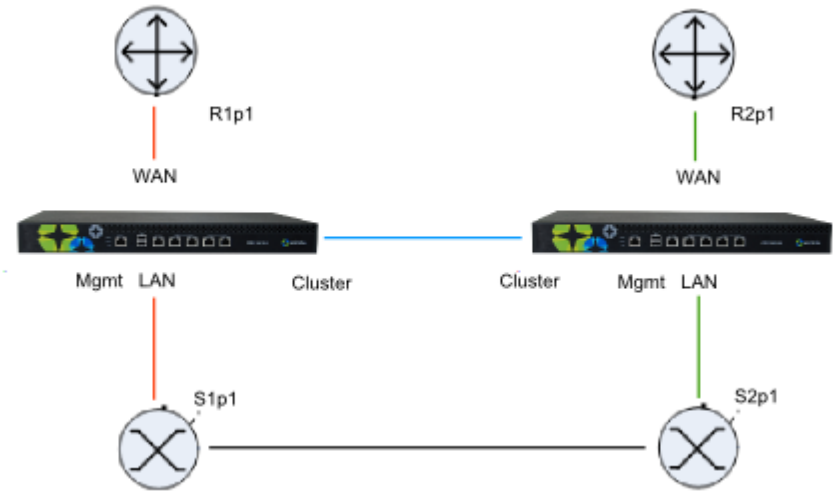
Part XII

12 Cluster/High Availability Topology 1

The clustering feature allows two Exinda appliances to be connected in a redundant topology.



With the Exinda appliances installed the above topology will appear as below:



The two appliances are directly connected to each other. Both appliances will capture the same data. The appliance that receives the data directly will forward the traffic to the other appliance which will monitor it the same way. However, the copied traffic will not be forwarded onto the LAN.

Exinda's Clustering/HA framework is also responsible for automatically synchronizing configuration settings between the two appliances.

All platforms support this topology.

Note: Clustering and High Availability currently only works with x700 (non Application Acceleration) licenses.

12.1 Installation

1. On each Exinda, assign an interface for cluster internal use and an interface to manage the appliance (refer to Figure 1).
2. Connect the cluster interfaces on each Exinda with a crossover cable.
3. Power up Exinda 1. After 1 minute power up Exinda 2.
4. Connect Exinda 1 LAN into switch 1 (S1p1).
5. Connect Exinda 1 WAN into router 1 (R1p1).
6. Connect Exinda 2 LAN into switch 2 (S2p1).
7. Connect Exinda 2 WAN into router 2 (R2p1).
8. Connect Exinda 1 management interface into switch 2 (S2p2)
9. Connect Exinda 2 management interface into switch 1 (S1p2)

12.2 Capabilities

- Monitoring of both links.
- Optimization of both links.
- Redundancy of Exinda appliances.

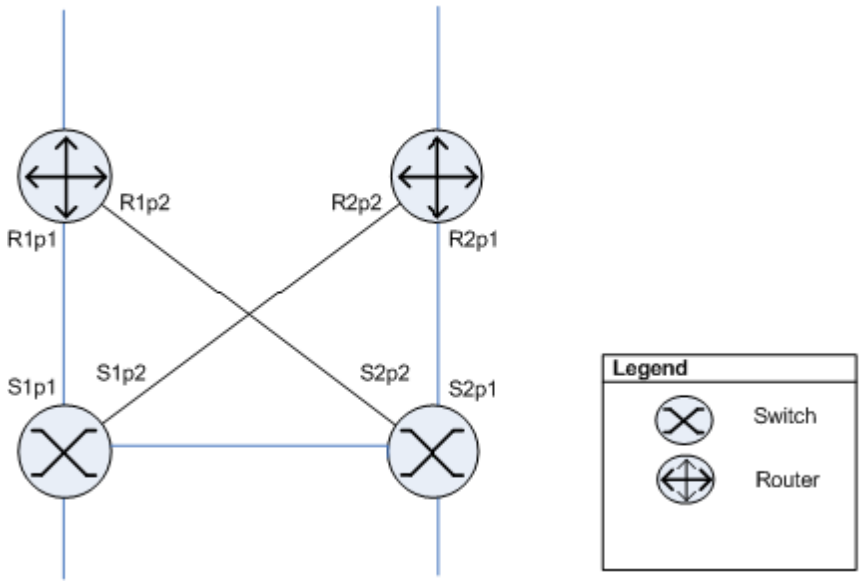
12.3 Suggestions

For further information on clustering and high availability, refer to the “Clustering (HA) - How To Guide”, available at http://www.exinda.com.

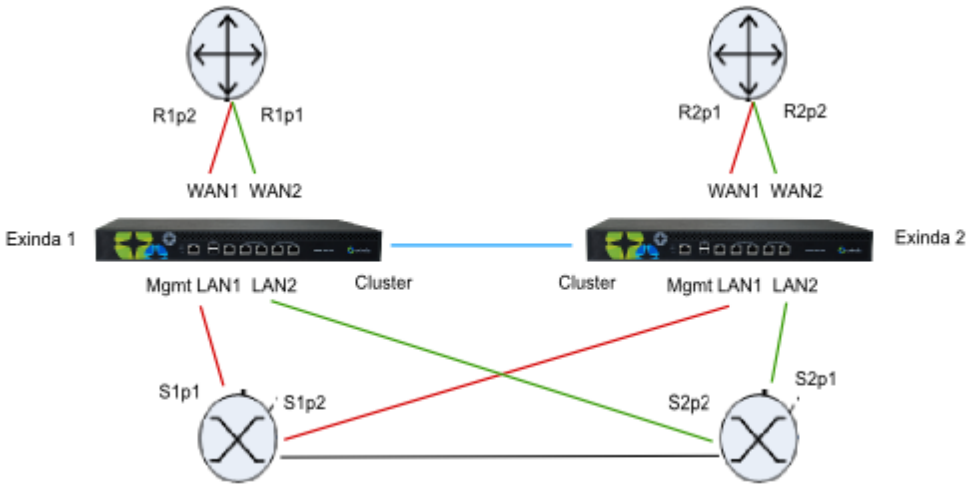
Part XIII

13 Cluster/High Availability Topology 2

Similar to the previous topology but in this case the routers are configured for load balancing. Both links in this topology act as fail-over and load balancing.



With Exinda appliances installed the above topology will appear as below:



In this topology both Exinda appliances are connected to both routers. As with the Cluster/ High Availability Topology 1 case, direct traffic reaching one appliance is copied to the second appliance for monitoring and optimization, but is not forwarded on.

Platforms that support this topology include the 4060[1], 4061[1], 5000, 6010, 6060[1], 7000 and 10060[1].

Note: Clustering and High Availability currently only works with x700 (non Application Acceleration) licenses.

[1] Network expansion modules are required.

13.1 Installation

1. On each Exinda, assign an interface for cluster internal use and an interface for managing the appliance (refer to Figure 1).
2. Connect the cluster interfaces on each Exinda with a crossover cable.
3. Power up Exinda 1. After 1 minute power up Exinda 2.
4. Connect Exinda 1 LAN2 into switch 1 (S1p2).
5. Connect Exinda 1 WAN2 into router 1 (R2p2).
6. Connect Exinda 1 LAN1 into switch 1 (S1p1).
7. Connect Exinda 1 WAN2 into router 1 (R1p1).
8. Connect Exinda 2 LAN2 into switch 2 (S2p1).
9. Connect Exinda 2 WAN2 into router 2 (R2p1).
10. Connect Exinda 2 LAN1 into switch 2 (S2p2).
11. Connect Exinda 2 WAN1 into router 2 (R1p2).
12. Connect Exinda 1 MGMT into switch 2.
13. Connect Exinda 2 MGMT into switch 1.

13.2 Capabilities

- Monitoring of both links.
- Optimization of both links.
- Redundancy of Exinda appliances.

13.3 Suggestions

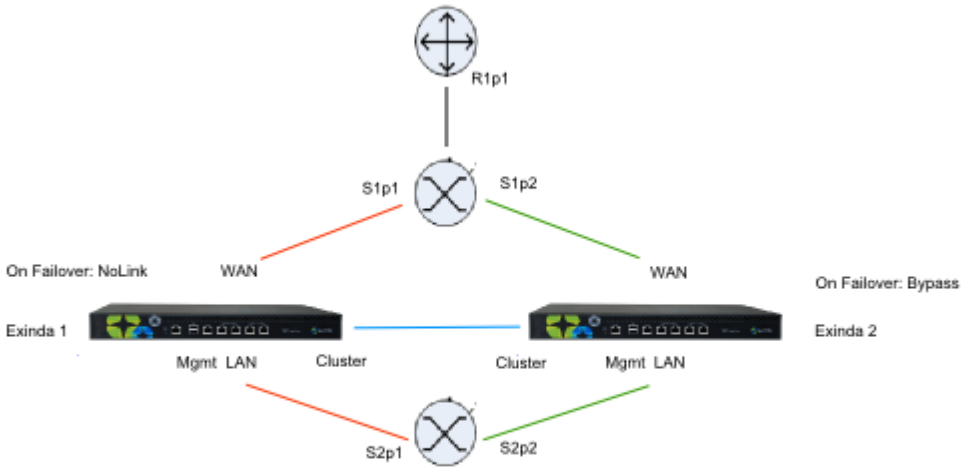
For further information on clustering and high availability, refer to the “Clustering (HA) - How To Guide”, available at http://www.exinda.com.

Part XIV

14 Cluster/High Availability Topology 3

When Router Redundancy is not present but you would still like to configure the Exinda solution in High Availability mode, use the configuration below.

With Exinda appliances installed the above topology will appear as below:



In this topology, both Exinda appliances are connected via a WAN switch. As with the Cluster/ High Availability Topology 1 case, direct traffic reaching one appliance is copied to the second appliance for monitoring, but is not forwarded.

Note: Your WAN switch and LAN switch must support the Spanning Tree Protocol (STP) Configure STP with S2p1 higher priority then S2p2. If the link at S2p1 goes down (e.g. Exinda 1 loses power) then the switch will enable S2p2. Exinda1 should configure NoLink as the bridge failover option, Exinda 2 should configure Bypass.
Active Path: S2p1 to S1p1
Standby Path: S2p2 to S1p2

All platforms support this topology.

Note: Clustering and High Availability currently only works with x700 (non Application Acceleration) licenses.

14.1 Installation

1. On each Exinda, assign an interface for cluster internal use and an interface for managing the appliance (refer to Figure 1).
2. Connect the cluster interfaces on each Exinda with a crossover cable.
3. Power up Exinda 1. After 1 minute power up Exinda 2.
4. Connect Exinda 1 LAN into switch 1 (S1p1).
5. Connect Exinda 1 WAN into switch 2 (S2p1).
6. Connect Exinda 2 LAN into switch 1 (S1p2).
7. Connect Exinda 2 WAN into switch 2 (S2p2).
8. Connect the management interface of Exinda 1 into switch 1.
9. Connect the management interface of Exinda 2 into switch 1.
10. On Exinda 1, select "NoLink" for the LAN/WAN bridge failover mode (refer to Figure 2).
11. On Exinda 2, select "Bypass" for the LAN/WAN bridge failover mode (refer to Figure 2).

Note: S2p2 should have the highest STP priority.

14.2 Capabilities

- Monitoring data available on both Exinda appliances.
- Optimization available via Exinda 1 or Exinda 2.
- Redundancy of Exinda appliances.

14.3 Suggestions

For further information on clustering and high availability, refer to the “Clustering (HA) - How To Guide”, available at http://www.exinda.com.

Index