SPAN and Mirror Port Monitoring

Exinda ExOS Version 6.3

Table of Contents

Part

1 Introduction

SPAN and Mirror Port Monitoring

Exinda Firmware Version: 6.3

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 How to Guide, the following relevant user documentation is available and should be read in conjunction with this guide:

- Exinda User Manual
- Exinda Topologies Guide

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

Part II

2 Overview

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

This topology is used when customers need to monitor only, without installing the Exinda in in-line mode. 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.

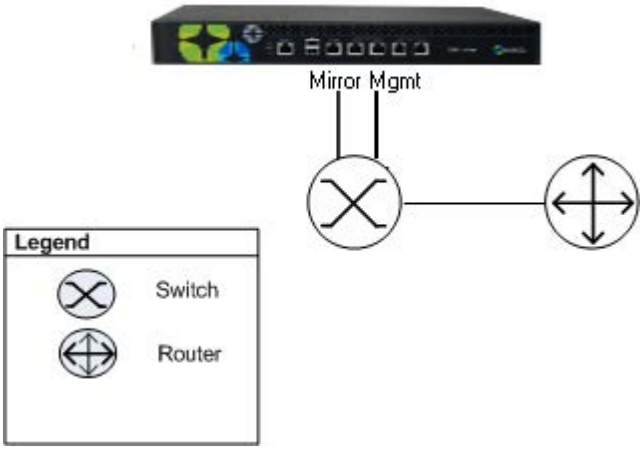
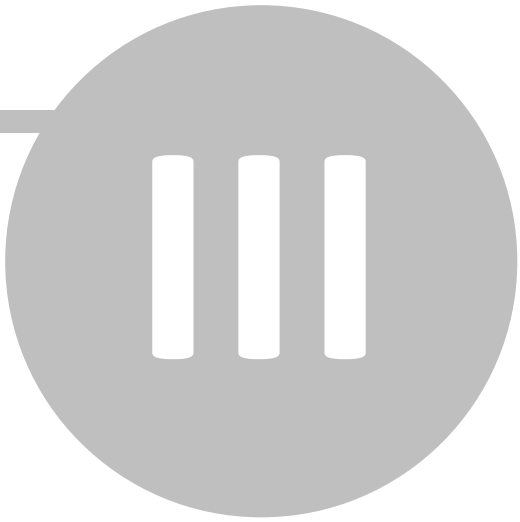


Figure 1: Topology diagram showing how to cable MGMT and Mirrorports for Mirror/SPAN port monitoring.

Part



3 Configuring Mirror Port Mode

To enable Mirror/SPAN port monitoring, you will first need to configure a switch port to mirror traffic to. Typically, the WAN port on the core switch is configured to mirror traffic to an unused port, which is cabled to the Exinda appliance. Alternatively, a network hub can be deployed in-path, and the Exinda appliance can be caballed directly to the hub (since a hub, by design, mirrors all traffic to all ports).

Any port not enslaved to a bridge or in use for another function (e.g. Cluster or WCCP) may be used to receive mirror port or SPAN port traffic.

3.1 Configure IP Settings

To enable Mirror/SPAN port monitoring, navigate to the System | Network | IP Address page on the Web UI, advanced mode.

Here, you will see all bridged and unbridged interfaces. Above each unbridged interface there are a number of checkbox's which show the Roles assigned to an interface. To use an interface as a Mirror port, check the Mirror box and then click on Apply Changes. The selected interface will now accept Mirror/SPAN traffic.

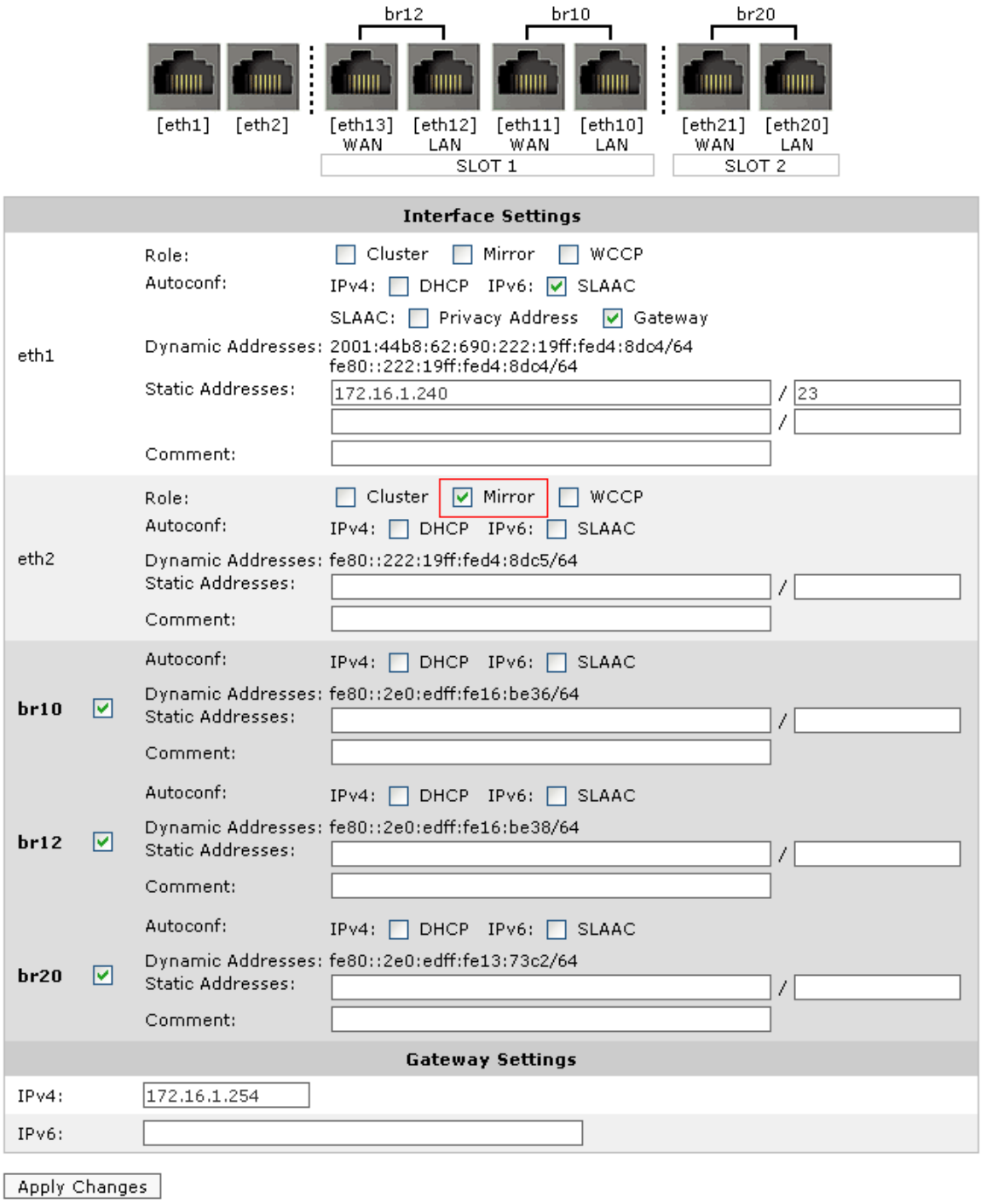


Figure 2: Web UI form showing where to enable Mirror/SPAN port monitoring.

The following commands can be executed from the CLI in order to enable or disable Mirror/ SPAN port monitoring on an interface.

```
> en
# con t
(config) # mirror interface <inf>
```

```
(config) # no mirror interface <inf>
```

3.2 Configure Network Objects

In order for the Exinda appliance to determine traffic direction, all internal subnets need to be defined as internal Network Objects.

Navigate to the Objects | Network Objects page and ensure all internal subnets are defined as internal Network Objects.

The Exinda appliance will determine packet direction based on the following rules:

Rule	Result
Packet's source IP matches an Internal Network Object AND Packet's destination IP DOES NOT match an Internal Network Object	Packet is monitored and classified as outbound.
Packet's source IP DOES NOT match an Internal Network Object AND Packet's destination IP matches an Internal Network Object	Packet is monitored and classified as inbound.
Packet's source IP matches an Internal Network Object AND Packet's destination IP matches an Internal Network Object	Packet is not monitored.
Packet's source IP DOES NOT match an Internal Network Object AND Packet's destination IP DOES NOT match an Internal Network Object	Packet is not monitored.

Table 2: Packet processing rules for Mirror/SPAN traffic received on the Exinda appliance.

Note: The "Ignore Internal-to-Internal" setting has no effect in Mirror/SPAN port monitoring mode.

Part IV

4 Monitoring Traffic

Once Mirror/SPAN monitoring is enabled and the appropriate Internal Network Objects have been defined, the Exinda appliance will monitor traffic received on the Mirror/SPAN receiving port as if it were in-line.

The only exception is the Interface Reports will be blank, because the Exinda appliance has no concept of packet direction at the Interface level.