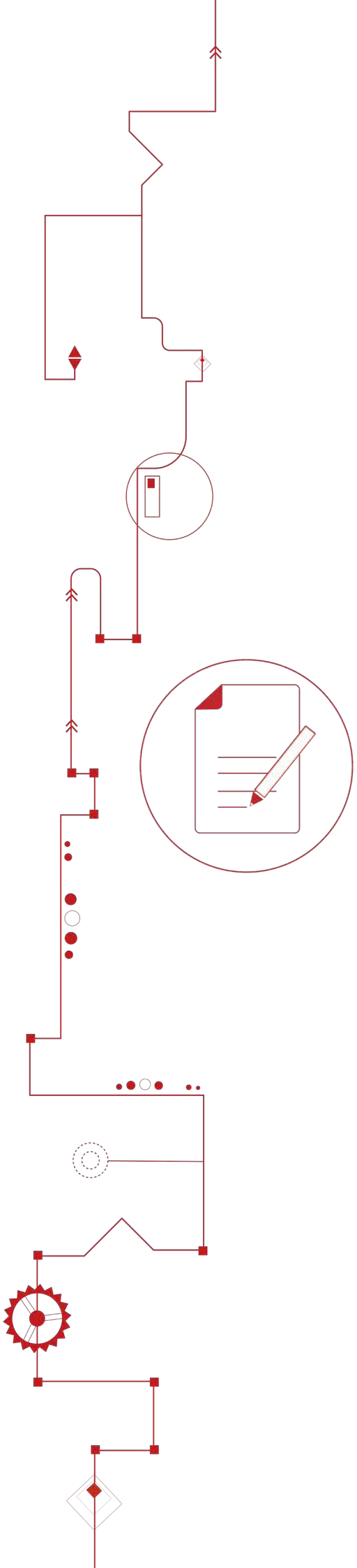
CUBRO
NETWORK VISIBILITY

EX400 ADVANCED OPTICAL BYPASS

APPLICATION NOTE

10.08.2021



CUBRO
NETWORK VISIBILITY

TABLE OF CONTENTS

Introduction

The EX400 Advanced Optical Bypass is a high-performance bypass switch with integrated network packet broker functionality. This allows aggregation, filtering, and load-balancing of network traffic to security, monitoring and management tools. The EX400 is based on an industry-leading programmable switch chip architecture plus an integrated optical relay to secure the availability of relevant services.

The Cubro Bypass Switch is deployed between network devices and in front of security tools, providing a reliable separation point between the network and security layers. The Bypass Switch provides comprehensive support of network and security tools without the risk of network interruptions.

Challenges

Modern networks are complex due to the high data rates. The complexity of the network causes additional blind spots. A Blind spot refers to network traffic that is not visible to network monitoring, security and analytics tools and can hide and obscure network performance and security threats.

As a result, troubleshooting is difficult because the root cause of the issue cannot be found easily. Inline appliances, which do not work accurately, can cause network downtime and network outages that may impact the experience of customers or employees. Additionally, it leads to losses in revenue and, in some cases, a bad reputation for the company.

Therefore, it is very important to have a reliable system which automatically isolates faulty services or tools that have a negative impact on the network itself.

Cubro Solution

The Cubro Bypass Switch provides a **fail-safe access** port for in-line active security appliances such as Intrusion Prevention Systems (IPS), Next-Generation Firewalls (NGFW) and more. The Bypass device is deployed between the network devices and before security tools, providing a reliable separation point between the network and security layers. Use of the Bypass Switch leads to comprehensive support of network and security tools without the risk of network interruptions.

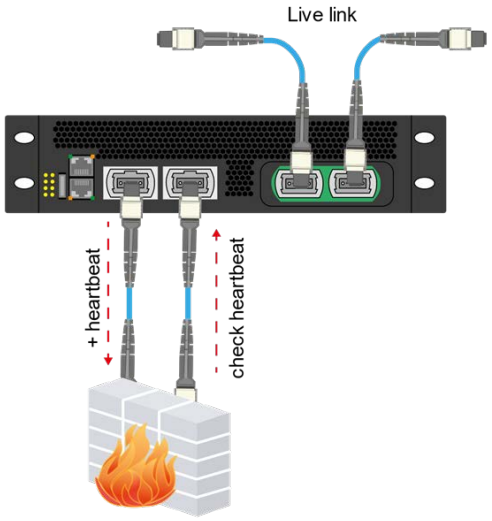
Benefits

- Self-generating heartbeat packets
- Keeps network traffic flowing when the in-line appliance fails.
- Allows the in-line appliance to be removed or serviced without impacting network traffic. For example, an IPS can be taken offline for upgrades, maintenance or troubleshooting.
- The in-line appliance can be moved from one network segment to another without impacting network traffic.
- Different bypass options to match your specific inline security devices.
- Flexible Deployments
- Fast “switching” Route Bypass (Software instead of Hardware based)
- In-line filtering of network traffic based on L2 to L4 criteria
- Supports link ratios from 1 to 100Gbit/s
- Easy to use WebUI
- Customizable trigger options

Possible Use Cases

1. Link Scenario

Bypass a single appliance of a normal 100Gbit/s link in any environment.

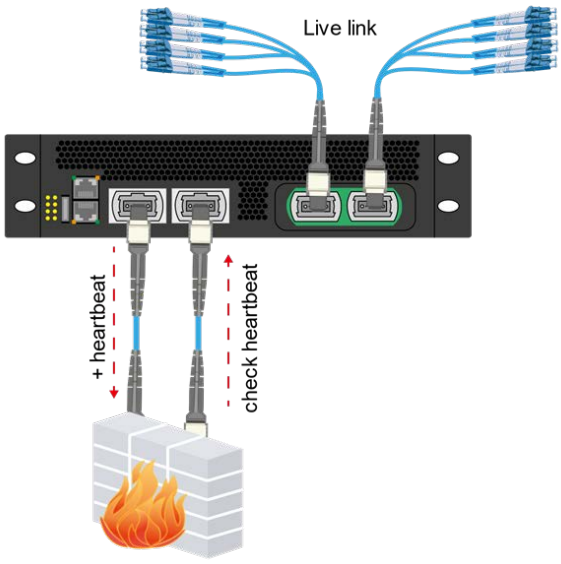


2. Quad Link - Single Appliance Scenario

Bypass a single appliance of four (4) normal 25/10G links in any environment.

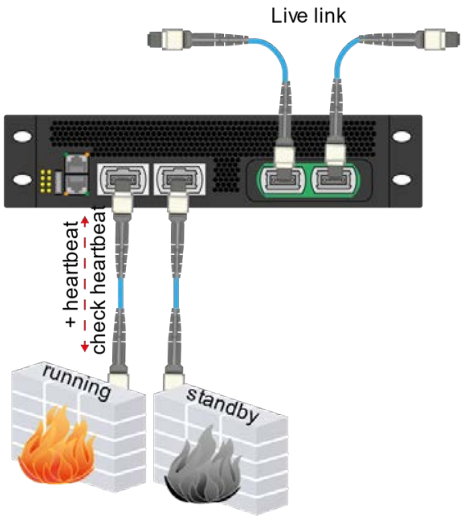
The Cubro Bypass uses VLAN tagging & filtering to keep track of where the data packets are coming from and where to send them.

Each link has its own dedicated route bypass allowing the user to bypass any link at any time without impacting the other links.



3. Single Link - Hot/standby Scenario

Bypass two inline appliance of four (4) normal 25/10G links in any environment. All data will be sent to the primary appliance as long as it is fully functional. If the Bypass detects any issue, it will bypass it and send the data to the backup appliance which takes over the job of the primary one. If both appliances fail, both will be bypassed.

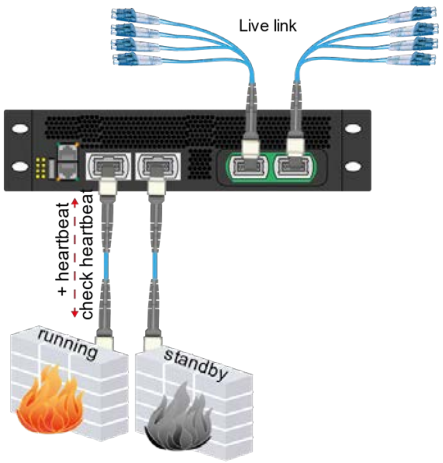


The Cubro Bypass uses VLAN tagging & filtering to keep track of where the data packets are coming from and where to send them.

4. Quad Link - Hot/standby Scenario

Bypass two inline appliance of a normal 100Gbit/s link in any environment. All data will be sent to the primary appliance as long as it is fully functional.

If the Bypass detects any issue, it will bypass it and send the data to the backup appliance which takes over the job of the primary one. If both appliances fail, both will be bypassed.



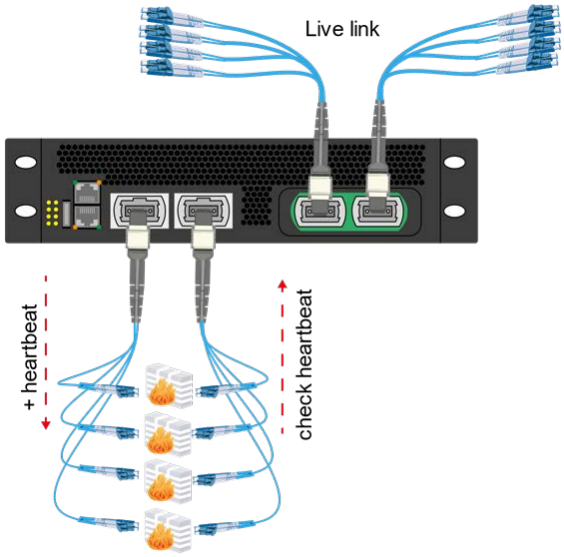
The Cubro Bypass uses VLAN tagging & filtering to keep track of where the data packets are coming from and where to send them.

Each link has its own dedicated route bypass allowing the user to bypass any link at any time without impacting the other links.

5. Quad Link Scenario

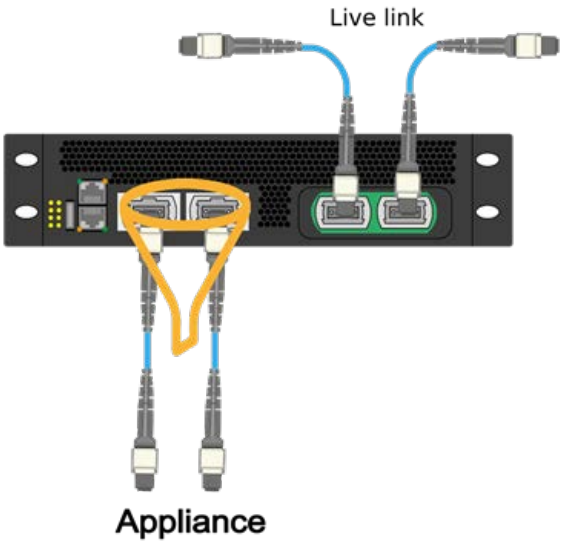
Bypass up to four (4) inline appliance of four normal 25/10G links in any environment.

The links and the corresponding appliances are totally independent of each other. Each link has its own dedicated route bypass allowing the user to bypass any link at any time without impacting the other links.



6. Traffic Filtering

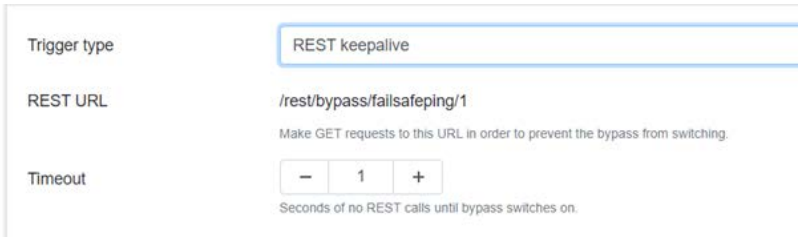
The EX400 supports more than 2000 L4 filters and can therefore act as a four (4) port 100 Gbit NPB with a built-in Bypass Module. The filters can easily be configured via the WEB UI.



Possible Bypass Triggers

1. REST Keepalive

Execute the REST URL from any remote service to reset the timeout. If the timeout is exceeded, the “Route Bypass” will be triggered.

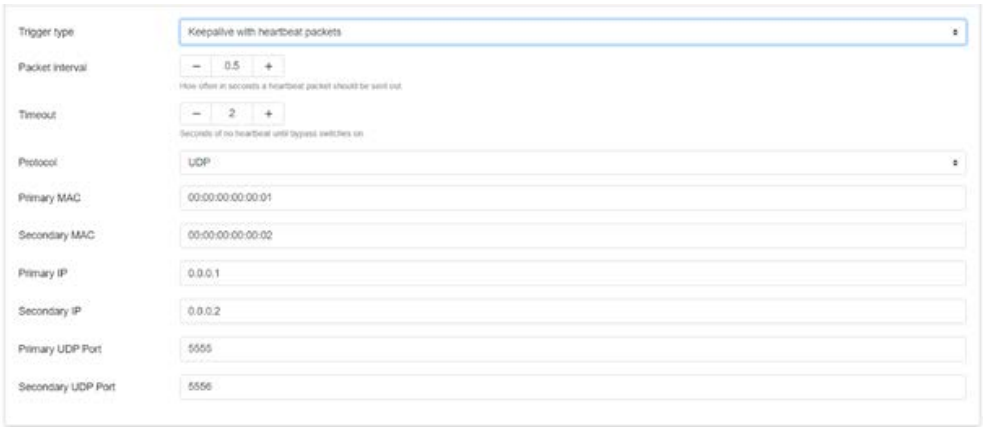


In the case of the Quad Link scenario, there will be up to four (4) different REST URLs available, to control each of the individual route bypasses.

2. Keepalive with Heartbeat packets

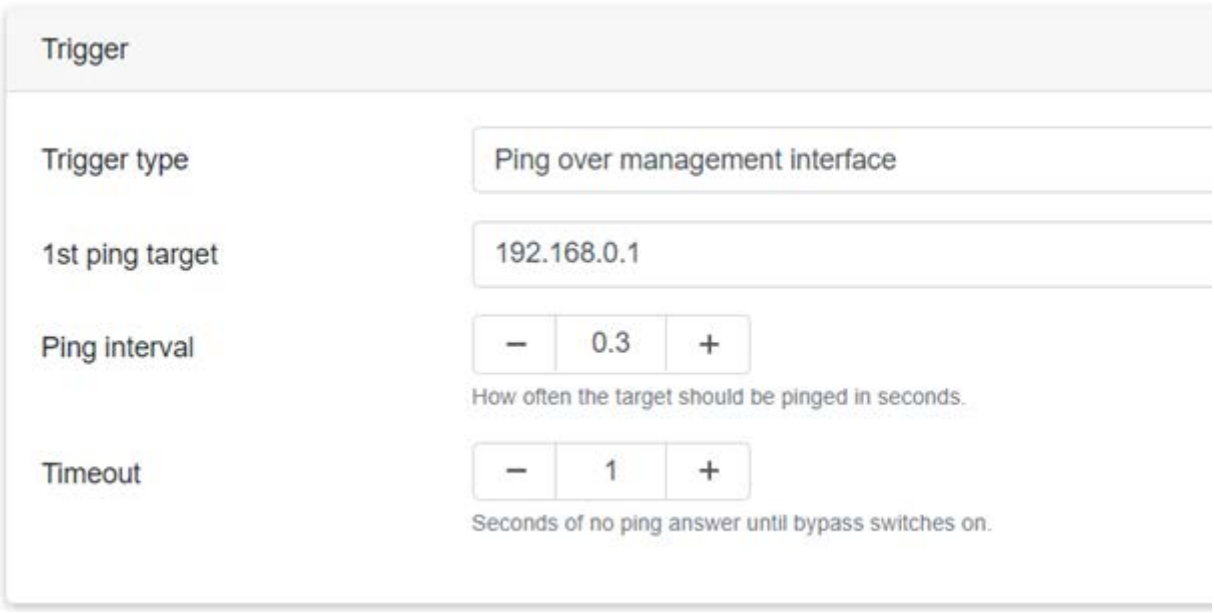
The Bypass adds so called “heartbeat packets” to the inline traffic, monitoring the service of the inline tool/appliance. In the event there are no heartbeat packets detected within the defined timeout range, the Route Bypass will be triggered. In the Quad Link scenario, each individual appliance will be monitored with its own heartbeat packet stream.

The heartbeat packet can either be UDP or ICMP type.



3. Ping over management interface

The Bypass is pinging a target device. In the event the ping fails, the “Route Bypass” will be triggered.



In the case of the Quad Link scenario, it is required to enter four (4) target IP addresses, to control each of the individual route bypasses.