Maintaining High Availability with Datacom DURAStream™ Bypass Switches

Overview

In-line security tools, such as Intrusion Protection Systems (IPS) and Deep Packet Inspection (DPI) provide critical services, but can be a source of unplanned downtime or performance degradation when they fail or become overloaded.

Datacom's DURAStream™ bypass switches provide a reliable, consistent fail-safe method of connecting in-line network tools – which minimizes the risk of these potential issues by diverting network traffic away from failed inline devices. In addition, network administrators can also manually remove inline devices from active service for maintenance and troubleshooting, while still ensuring connectivity of the link.

Links in which inline tools are deployed are typically connecting a firewall and a router. The bypass switch is placed directly into the link. It has a pair of "Appliance ports" to which the inline tool is then connected. Transparent to the network, the traffic passes into the bypass switch in both directions, also passing through the in tool, which inspects the traffic and may take proactive action (e.g. blocking certain attempts at entry or suspect payloads, and alerting a security administrator.)

Inline tools can fail in a number of ways. Some failure modes, such as a loss of power or hardware failure, are easy to detect, but a significant amount of time can pass before network protocols can converge and restore connectivity. Other problems, such as congestion or system overload, are more difficult to detect, and will frequently fail to trigger network based remediation techniques.

Bypass switches are designed to address both classes of problems. Furthermore, failures can be dealt with rapidly and automatically using a combination of detection and remediation techniques.

Failure detection: Heartbeat Mode

Heartbeat mode is used to detect failures of inline devices that impact operations or data flows caused by software problems, oversubscription, or hardware failures that leave the network link physically intact. The bypass switch injects heartbeat frames into the data stream and measures the time taken for these frames to pass through the attached tool. If the frames fail to arrive within the configured threshold, then the device is determined to be unavailable or overloaded. It will switch to bypass mode

and redirect traffic around the failed or degraded device. While operating in bypass mode, it continues to generate heartbeat frames. Thus, it is able to restore the system to normal operation once the inline device is returned to service.

In addition to active bypass, the bypass switch is designed to fail closed (i.e. “fail to wire”) if it loses power. In such an event, traffic on the link is automatically passed through the bypass switch. This ensures fail-safe operation and minimizes the impact of a failure of the bypass switch device itself. It should be noted that this is a physical operation. An extremely brief interruption of link will occur in a fiber bypass switch (milliseconds) on power down or power up.

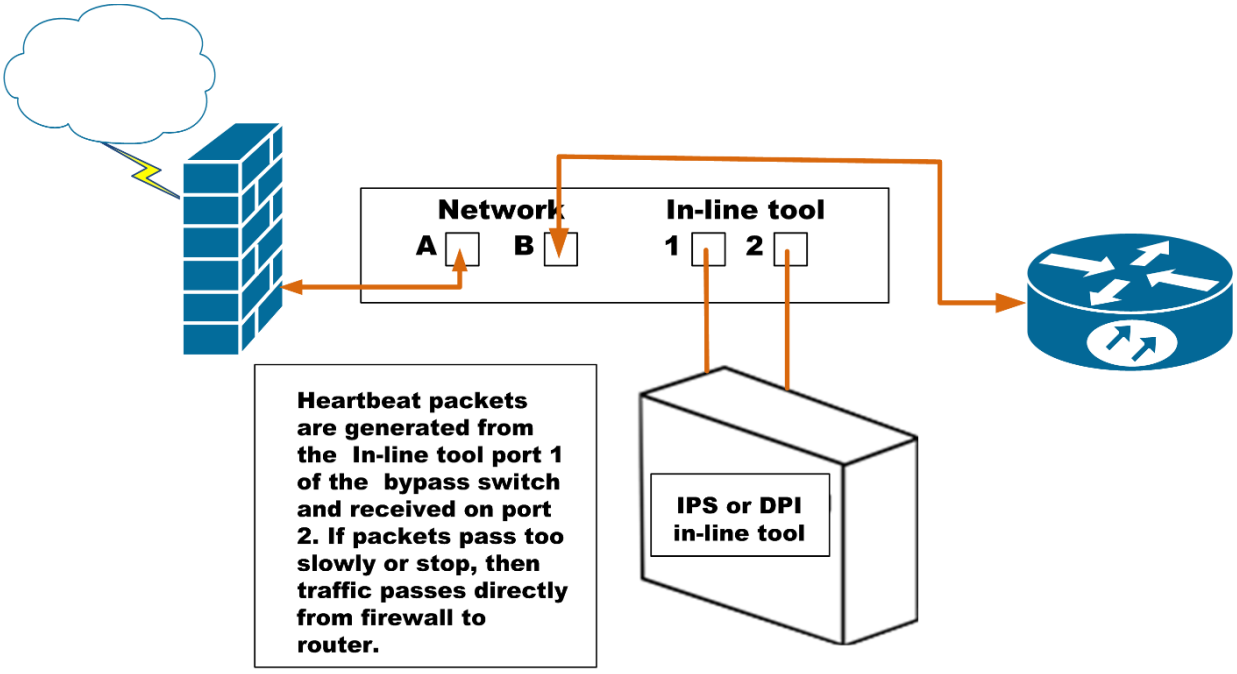

Figure 1: DURAstream DS-1404 functionality with one tool

Consistent Failover for Varying Device Types:

Some in-line tools have a feature allowing them to fail closed in the event of power loss or a catastrophic hardware failure Performance degradation and system overloads do not trigger a bypass mechanism in the bypass systems that are integrated into the tools. They provide only power fault tolerance. Additionally, each system behaves somewhat differently, increasing operational complexities. By deploying DURAStream Bypass Switches, network administrators can simplify operational procedures and provide greater consistency.

The DURAStream Bypass Switch itself has power fault tolerance, in addition to being able to provide protection for tools that perform too slowly, lose link, or completely lose power. This functionality exists regardless of the type or brand of in-line tool being used.

High Availability:

High Availability is a well-known networking strategy, which uses interconnected equipment to provide redundancy (and sometimes increased bandwidth,) thereby reducing the risk of a single point of failure. Often used with firewall pairs or interconnected network core switches, it is also highly beneficial on single links by using two in-line tools.

The DURAstream can automatically take an inline tool off line if it fails or underperforms, and also allows Network Administrators to manually force bypass mode, thus preserving data flow on the link while tasks such as hardware or firmware upgrades are performed on the tool. This raises a dilemma: inline tools are typically used on mission critical links at the Ingress-Egress points of a network. Bypass switches that support two inline tools, such as the DURAstream DS-1406, will automatically switch traffic to the Passive (backup) tool, if the Active (primary) tools fails or is forced off line manually.

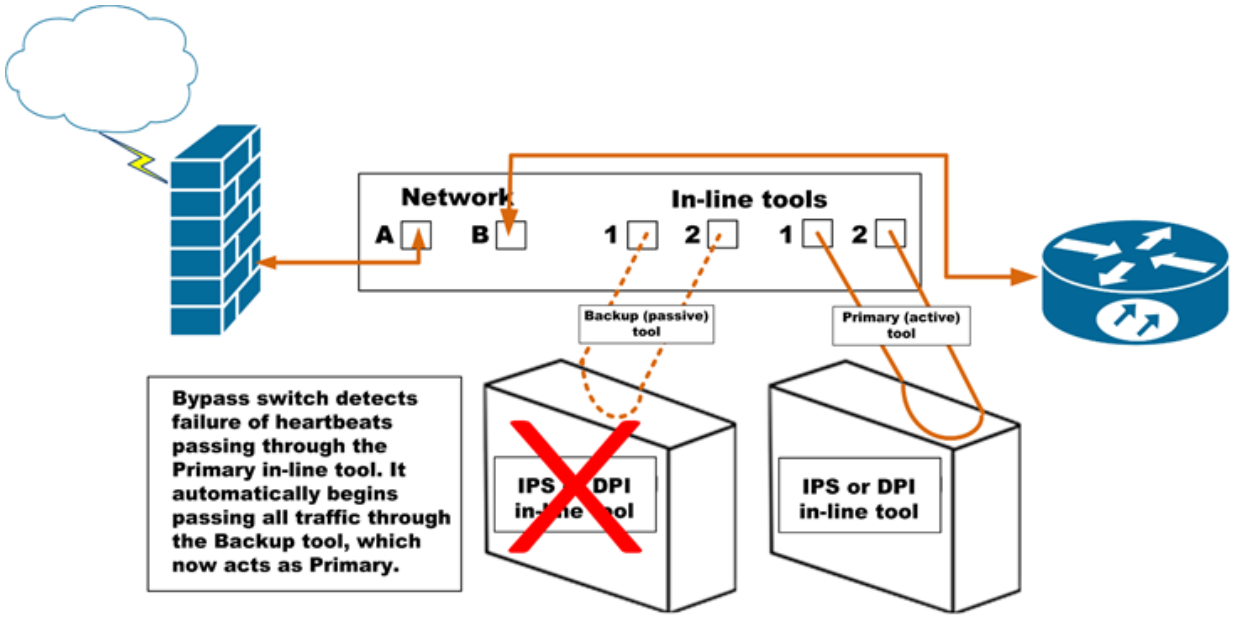

Figure 2: DURAstream DS-1406 High Availability functionality with two tools

High Availability for Dual Links:

Links pairs that require protection by inline tools are most frequently the connections between routers and firewalls. Dynamic load balancing, in which both links carry data simultaneously and automatically re-route the data if one link fails, is a common deployment for such firewall installations. Use of a dual bypass switch, such as the DURAstream DS-2408, allows both links to be deployed and protected by a single in-line tool which has a passive backup tool, or deployed in scenarios where two tools are used simultaneously to protect two active load balanced links. Datacom's LINKprotect feature will automatically re-route traffic to either link if the other link in that pair fails. This allows many types of protection, including but not limited to the following:

1) Either of the links fails, and the active inline tool continues to protect all traffic from the active link
2) Either of the tools fails, and the traffic from both active links continues to be protected by the remaining tool
3) One of the links AND one of the tools fails, and traffic on the remaining active link is protected by the remaining tool

A more detailed document – entitled "Supplemental Bypass Information" - shows a matrix of possible failure scenarios, and outlines how the DS-2408 provides protection for all such failures, and is available on request by emailing support@datacomsystems.com or contacting your Account Manager.

Summary:

Inline tools perform a crucial security function that must remain active and engaged at all times**.** Use of a bypass switch with a High Availability function, which supports two tools, is a useful way to ensure protection at all times, Active-Passive or dynamically load balanced link pairs provide increased bandwidth and greatly reduce risk from potential single points of failure on the network. Protecting such link pairs, while also ensuring that the network continues to run smoothly and be protected if one link fails, is easily accomplished with use of a Datacom Systems DURAstream dual bypass switch.