APPLICATION NOTE

Ixia and FireEye High Availability Solution

Summary

In networking, high availability refers to a system or component that is continuously operational for an uninterrupted amount of time. Usually, “availability” is measured relative to 100% operational, or “never failing.” A widely-held standard of availability is known as "five 9s": 99.999% availability (a difficult and nearly unobtainable end result).

A FireEye customer needed a networking solution that encompassed the following requirements:

- **Elimination of single points of failure**. The customer needed additional system redundancy so that the failure of an appliance does not mean failure of the entire network.
- **Reliable crossover**. In multi-appliance deployments, the crossover point itself tends to become a single point of failure. The customer needed a high availability architecture that provides reliable crossover.
- **Detection of failures as they occur**. The customer needed to eliminate downtime as maintenance activities take place.

FireEye and Ixia In-line Security Architecture

In order to meet FireEye requirements, Ixia employed elements of its network visibility architecture to monitor traffic across the network—in combination with the FireEye Threat Prevention Platform. The combined FireEye Ixia in-line security architecture consisted of a Ixia iBypass HD active fail-open switch, two Ixia xBalancers in a high availability configuration (responsible for aggregating and de-aggregating traffic flows), and two FireEye NX Series appliances that enable organizations to prevent, detect, and respond to network-based zero-day exploit attempts, web drive-by downloads, and advanced malware that routinely bypass conventional signature-reliant defenses.

The Ixia iBypass HD active fail-open switch enables the entire in-line security architecture to be deployed to the current IAP configuration without introducing a single point of failure to the current network architecture. This appliance is designed to fail the link open in the event of a failure that would otherwise impede the flow of traffic through the switch or in-line security architecture.

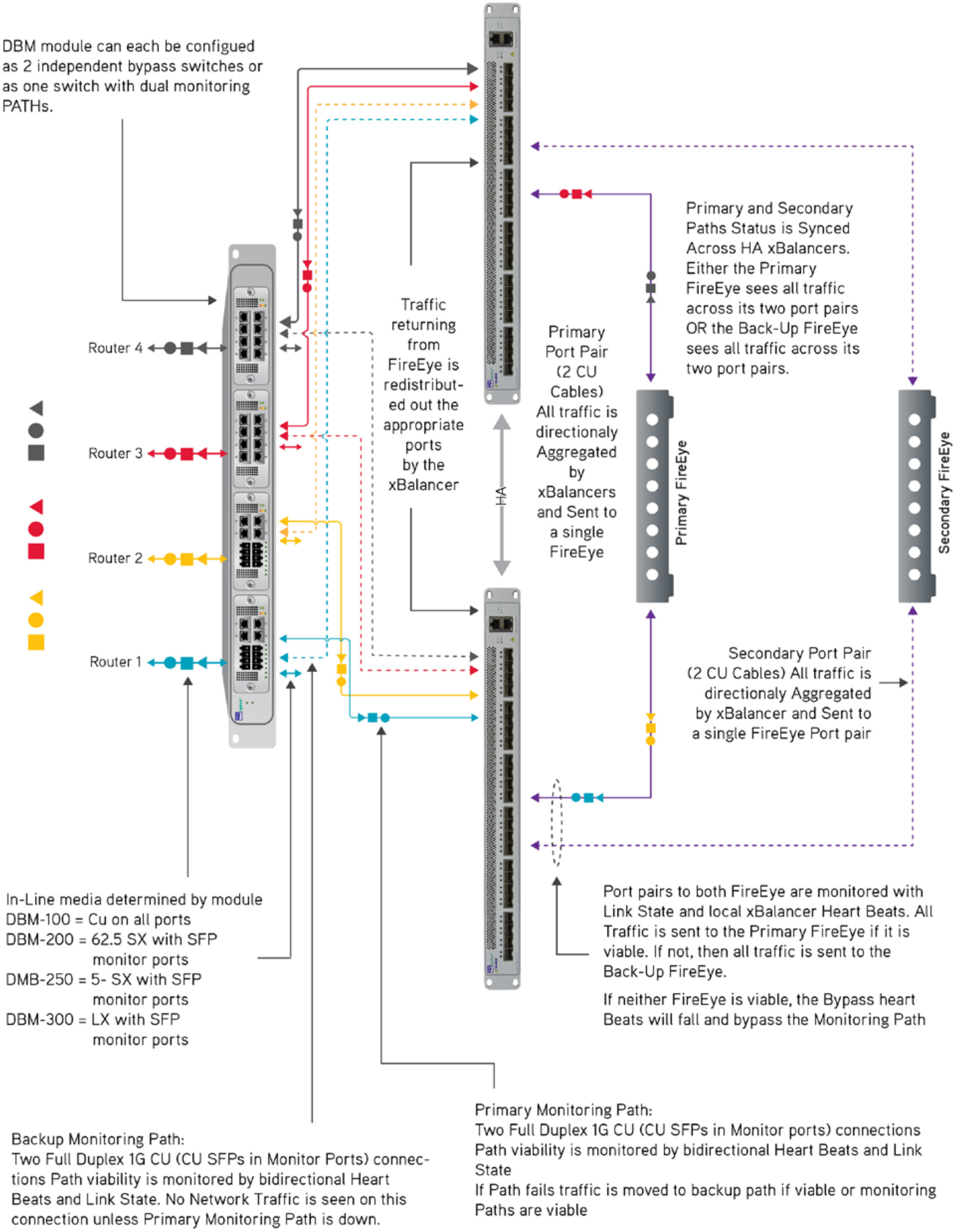
The xBalancers provide two methods by which to manage traffic, aggregation, and de-aggregation within the in-line security architecture: using MAC addresses or Q-in-Q tunneling. The Q-in-Q tunneling method for managing the traffic traversing the in-line security architecture is used due to the dynamic nature of how the MAC addresses are handled across the interfaces within the current IAP’s HSRP configuration. This Q-in-Q tunneling method allows for the in-line security architecture to encapsulate the traffic for effective management in, through, and out of the in-line security architecture. Enterprise service providers throughout the world commonly use this form of traffic management today to transparently manage traffic traversing carrier grade links, without impacting the performance or operation of the currently employed routing methodology.

The FireEye NX was positioned in-line in this security architecture to provide analytics and real-time defensive capability. A single FireEye NX appliance is effectively in-line at any given point in time for the traffic traversing the in-line security architecture. Should any failure be experienced on a single FireEye NX, the xBalancer will have the traffic redistributed to the secondary appliance, effectively removing the device with the failure from operation. Both appliances are configured to use the Q-in-Q tunneling feature on their interfaces, a newly released feature introduced in the FEOS version 7.4. This feature allows for the monitoring interfaces on the FireEye NX appliances to perform analytics and real-time defensive actions on Q-in-Q tunneled traffic.

Demonstration Scenarios

A single Ixia XM2 traffic generator was connected to the iBypass HD, via 8 physical multi-mode fiber (gigabit) ports, to simulate the client (4 ports) and server (4 ports) side connectivity across the four WAN links as in the production environment. The Ixia XM2 simulates fully formed HTTP sessions traversing the in-line security architecture, as it would within the production environment. The traffic being sent from the XM2 is completely stateful, meaning it won't be different from any real HTTP traffic. A sustained traffic volume of 600 Mbps, for a thirty-minute, timeframe was used for each test scenario.

Various emulated failure scenarios were tested using the set-up shown on the next page: single power supply failures on all appliances, dual power supply failures on all appliances, and link failures to the FireEye NX appliances.



DBM module can each be configued as 2 independent bypass switches or as one switch with dual monitoring PATHs.

Traffic returning from FireEye is redistributed out the appropriate ports by the xBalancer

Primary Port Pair (2 CU Cables) All traffic is directionaly Aggregated by xBalancers and Sent to a single FireEye

Primary and Secondary Paths Status is Synced Across HA xBalancers. Either the Primary FireEye sees all traffic across its two port pairs OR the Back-Up FireEye sees all traffic across its two port pairs.

Secondary Port Pair (2 CU Cables) All traffic is directionaly Aggregated by xBalancer and Sent to a single FireEye Port pair

Port pairs to both FireEye are monitored with Link State and local xBalancer Heart Beats. All Traffic is sent to the Primary FireEye if it is viable. If not, then all traffic is sent to the Back-Up FireEye.

If neither FireEye is viable, the Bypass heart Beats will fall and bypass the Monitoring Path

In-Line media determined by module
DBM-100 = Cu on all ports
DBM-200 = 62.5 SX with SFP monitor ports
DMB-250 = 5- SX with SFP monitor ports
DBM-300 = LX with SFP monitor ports

Primary Monitoring Path:
Two Full Duplex 1G CU (CU SFPs in Monitor ports) connections Path viability is monitored by bidirectional Heart Beats and Link State
If Path fails traffic is moved to backup path if viable or monitoring Paths are viable

Backup Monitoring Path:
Two Full Duplex 1G CU (CU SFPs in Monitor Ports) connections Path viability is monitored by bidirectional Heart Beats and Link State. No Network Traffic is seen on this connection unless Primary Monitoring Path is down.

Scope of the Demonstration

With this configuration, Ixia used an IxLoad simulating HTTP traffic though the FireEye and Ixia appliances, and monitored traffic during 14 various failover conditions. To emulate real world scenarios we added two emulated subnets behind an emulated router for each port. We used a total of eight ports for the test, with four ports running the HTTP client traffic and four ports acting as the servers. Each scenario was run for 30 minutes, with reports being created from the results of each test. We were able to successfully show that traffic fully recovered after each failover with minimal impact to the traffic flow.

FireEye and Ixia Demonstrate High Availability

Ixia demonstrated that the FireEye Ixia in-line security architecture doesn’t introduce a single point of failure along the network’s current Internet access points, and effectively managed traffic within the architecture regardless of the current use of the HSRP configuration.

The Ixia solution was deployed as a two-tier design that detected the overall availability of the FireEye Threat Prevention Platforms. The iBypass served as a network focal point that transparently redirected traffic to the security complex that was fronted by a pair of xBalancer appliances. Each DBM module of the iBypass has the ability to detect the availability of a primary monitor path, defer to a secondary path, or bypass the entire complex in the event of an overall failure. Two of the modules used one xBalancer as a primary path while the other two used the second xBalancer. This method assured constant active-active use of the packet broker tier in a normal uptime situation. However, if either xBalancer failed or was brought down for maintenance, the iBypass has the inherent capability to shift traffic flows to the remaining xBalancer. Moreover, if the entire xBalancer tier became unavailable, then the iBypass would maintain general network connectivity by forwarding around the security complex altogether.

Likewise, the xBalancer tier maintained awareness of the FireEye appliances. Both xBalancer appliances were configured to prefer the same FireEye appliance. This guaranteed that regardless of which of the four network paths traffic was flowing, the same FireEye would be able to inspect all aspects of the conversation. If the primary FireEye appliance failed, then both xBalancers would switch in tandem to use the secondary FireEye appliance, again assuring that all flows were inspected by a common device. Flow management within the xBalancer is achieved by leveraging VLAN tagging to denote the original ingress circuit and returning each packet to the same circuit from which it originated.

This solution eliminates single point of failures, allows for maintenance or software upgrades to be performed, and provides the ability to test new versions of software. These factors are crucial to operations staff to help minimize downtime with a fully redundant architecture.