Interface Masters
TECHNOLOGIES
Innovative Network Solutions

BLUE COAT

Maximizing Your Network Performance with Blue Coat and Interface Masters

Overview

A key challenge in today's fast growing inter-networking world is to create cost-effective solutions that provide greater visibility into network traffic while ensuring maximum network uptime. There are numerous tools available in the market that specialize in controlling the flow of traffic, providing functionality ranging from prioritizing application traffic, monitoring network efficiency and assuring quality of service for critical business applications. These inline tools allow administrators to shape network traffic for optimal security and efficiency. A combined solution of Blue Coat's PacketShaper 12000 and Interface Masters' Niagara 2299 Intelligent Active bypass technology networks can provide maximum efficiency and uptime.

Blue Coat PacketShaper 12000 Feature

The PacketShaper helps enterprises to control bandwidth cost, deliver a superior user experience and align network resources with business priorities. The system is able to prioritize application specific items, providing QoS and contain recreational traffic to any specified level. Supporting more than nine hundred applications and tens' millions of websites with its cloud-connected, real-time classification engine, the PacketShaper gives administrators the tools necessary to quickly identify and diagnose issues while placing priority applications, such as Salesforce or WebEx, over recreational traffic such as YouTube or Facebook.

Interface Masters' Intelligent Active Bypass Feature

Interface Masters' offers a diverse selection of Intelligent Active bypass switches to protect critical network links from costly downtime due to power outage, software or hardware failure or link-loss of inline networking or security devices. The Interface Masters Intelligent Active bypass solutions protect one or multiple 10/100, 1G, 10G and/or 40G network links that are being monitored by an inline appliance and support flexible media configuration options including multi-mode fiber, single-mode fiber, and copper. In addition, these interfaces can be mixed and matched to support datacenter environments where the network requires fiber connection, but the inline tool requires copper connection. In this case, the conversion is done on the bypass saving cost while maximizing space.

Solution

In networking, a common network topology consists of a router on one side which enables communication from the internal LAN and a switch or router on the other which creates a channel of communication to and from the WAN side. Depending on the network, this is usually a single connection.

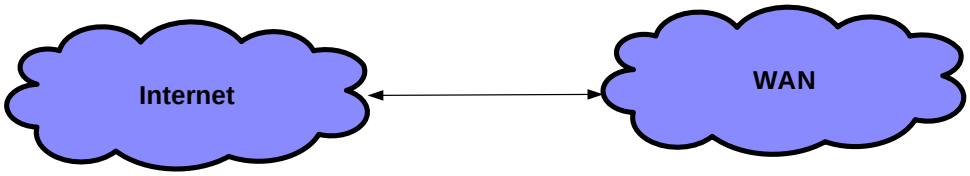

Figure 1: Common Network

When an inline tool is introduced into the network, it is generally placed between the Internet connection and WAN connection. This deployment scenario will enable all bi-directional traffic on the network link to be monitored and managed in real-time. A bypass is placed in front of the inline appliance and will direct the flow of traffic to the appliance when it is healthy and bypass the appliance when the appliance fails or goes down. When the appliance comes back up, the bypass will instantly redirect the network traffic back to the appliance for inline monitoring and shaping.

In order to install an Intelligent Active bypass unit to protect a network being monitored by an inline device, the Internet and WAN end points need to be connected directly to the bypass unit on two dedicated ports called Network Port 1 (or N1) and Network Port 2 (or N2) which are the top two ports on any bypass segment. The bottom two ports on the same bypass segment, Appliance Port 1 (or A1) and Appliance Port 2 (or A2) need to connect directly to the PacketShaper. When the bypass is in an inline state, the traffic will traverse through to the PacketShaper, where the information will be processed according to the rules specified on the system. In order to determine whether the PacketShaper is in good health, heartbeats are generated from A1 and A2 and sent to the PacketShaper. Should heartbeats not be received, bypass will be initiated, and once the heartbeats are received again, indicating the health of the system has returned, the bypass will once again go back to inline mode. See below diagram for Inline Mode and Bypass Mode diagrams (Figure 2 and Figure 3 respectively).

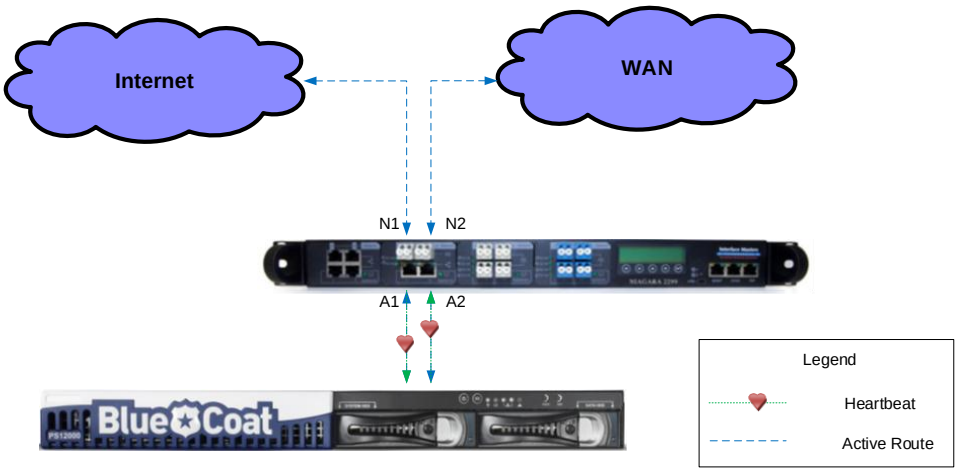

Figure 2: Inline Mode

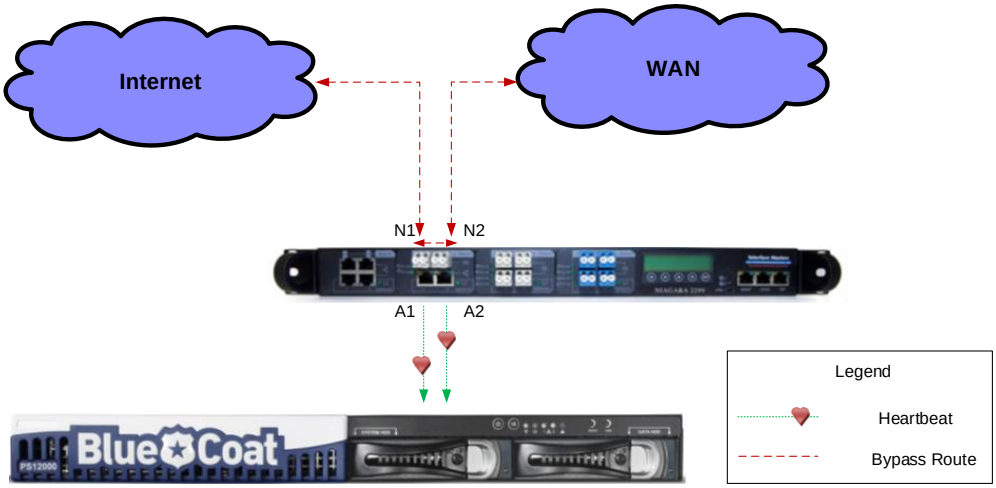

Figure 3: Bypass Mode

One of the advantages of the Intelligent Active bypass is its plug-and-play capability and highly customizable heartbeat functionality. The programmability of the heartbeat enables administrators to have full control over heartbeat configuration and optimize heartbeat parameters include the timeout/delay to deem a heartbeat packet lost, the type of heartbeat packets required, and the heartbeat packet parameters such as IP, MAC and/or TCP port information.

When the connections are in place, the bypass offers two levels of security. As mentioned previously, when the bypass is operational, the unit will generate heartbeats that are sent on the appliance port and expected to be received back on the adjacent appliance port. This will constantly monitor the PacketShaper to determine if it is in a healthy state. When the heartbeat is not received in the timeout defined, the traffic will bypass the PacketShaper ensuring network uptime. When the tool is healthy enough to process the heartbeats, the flow of traffic will traverse through the PacketShaper again. In the event that the bypass loses power, a second level of protection called Passive bypass will ensure that the traffic will continue to flow even in an unpowered state. Passive bypass is managed by hardware bypass logic that will continuously monitor the bypass and once power is lost will ensure that traffic continues to flow.

Another major advantage that separates Active bypass from any internal bypass or passive bypass solution is the ability to proactively disconnect the PacketShaper from the network for maintenance or upgrade with no downtime. When a PacketShaper is disconnected from the bypass for any type of service, troubleshooting, or even a replacement, the Active bypass will instantly transition to bypass mode, ensuring the network link is maintained and continues to flow. When the original PacketShaper appliance or a new PacketShaper appliance is detected via the continuous flow of the heartbeat

mechanism, the bypass will instantly switch to active mode, seamlessly rerouting all network traffic back inline to the PacketShaper appliance.

Conclusion

In a world that is increasingly more interactive, mobile and content-driven, the Blue Coat PacketShaper helps enterprises to control bandwidth cost, deliver a superior user experience and align network resources with business priorities. The Interface Masters External Intelligent Active bypass adds critical layers of protection to the network ensuring maximum uptime. Together, the Blue Coat PacketShaper and the Interface Masters Intelligent Active Bypass provide the ideal solution to effectively manage any network, regardless of complexity, size and speed.

About Bluecoat

Blue Coat empowers enterprises to safely and securely choose the best applications, services, devices, data sources, and content the world has to offer, so they can create, communicate, collaborate, innovate, execute, compete and win in their markets. Blue Coat has a long history of protecting organizations, their data and their employees and is the trusted brand to 15,000 customers worldwide, including 86 percent of the Fortune® Global 500. With a robust portfolio of intellectual property anchored by more than 200 patents and patents pending, the company continues to drive innovations that assure business continuity, agility and governance. For more information please contact insidesales@bluecoat.com or visit www.bluecoat.com

About Interface Masters Technologies

Interface Masters Technologies is a leading vendor in the high speed network visibility market based in the heart of the Silicon Valley. Flagship product lines include Network Packet Brokers, specialized 10G internal server adapter cards, switches, external intelligent Network TAP and Bypass and failover systems that increase network monitoring capabilities, network reliability and inline appliance availability. Company Headquarters are located in San Jose, CA with satellite offices in Hong Kong and Europe. For more information please contact sales@interfacemasters.com or visit www.interfacemasters.com