Security Tool Chaining in a DMZ with Big Monitoring Fabric Inline

Enabling Network Visibility & Dynamic Threat Mitigation

Securing enterprise networks and online assets is of paramount importance for any modern IT organization. The ever increasing reliance on the network for critical business functions has, in parallel, resulted in an explosion of cyber threats. This presents significant and sometimes conflicting challenges for network and security teams. They need to design and maintain a high-performance, resilient and always-on network, while ensuring that it is compliant and secure against intrusions and other threats.

A common network security design to achieve these goals involves separating the network into trusted and untrusted zones, and deploying security and network monitoring tools in a DMZ environment (between the two zones). By virtue of being inline, security tools can assess every packet that traverses between trusted and untrusted zones) and, actively prevent or block intrusions.

In this document we discuss how Big Monitoring Fabric (Inline Mode) can be deployed in a highly available (HA) configuration to **enable visibility and threat mitigation** in the DMZ and addresses the challenges faced by traditional solutions while offering lower-cost and SDN-centric operational simplicity.

Tool Deployment in a DMZ – Traditional Approach

Traditionally, security teams have used two approaches to deploying multiple inline security/analytics tools in the DMZ production network:

Approach 1: Placing the security tools sequentially inline between the production nodes as shown in Figure 1. There are several challenges with this approach:

- If a particular tools goes down it impacts network connectivity for all end nodes in the trusted zone
- Production traffic is potentially dropped due to bandwidth mismatch between production ports (typically 10/40G) and tools supporting lower bandwidth (e.g. 1G)
- All traffic is sent to the tools, rather than only sending the traffic needed by the tool
- For any tool modification (add/remove/upgrade), maintenance window has to be scheduled which again, involves impacting network connectivity.

Approach 2: Configuring complex WCCP Based Routing or Policy Based Routing (PBR) for traffic steering. While on the surface, this approach seems agile, it adds its own set of challenges:

- WCCP is complex and does not support tool chaining
- Complex PBR rules are error-prone as it interferes with other routing

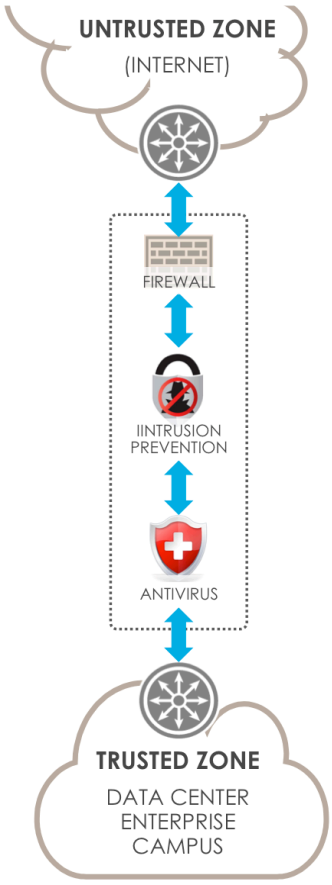

Figure 1: Traditional Security Tool Deployment in DMZ

decisions made on the router or switch. Managing addition, removal or downtime of these tools can get tricky if the PBR rules are not set properly.

- Tools need to be connected to the expensive edge router ports. This puts additional burden on the relatively complex (and expensive) enterprise edge routers that also act as a security services management point

Key Operational Considerations

The discussion above highlights the key requirements in managing inline security tools in a DMZ, as well as associated challenges presented by the traditional deployment designs. In summary:

1. Network administrators, in their pursuit to ensure stable network connectivity, are generally reluctant to modify networking infrastructure or policies as and when required by security or other tool administrators.
2. Traffic needs to be programmatically chained through relevant tools based on certain policies, tool constraints etc. with making extensive network configuration changes.
3. HA design is a key consideration when deploying inline tools, such that network traffic is appropriately handled in case of network or tool failures.

The Big Switch Approach: Big Monitoring Fabric Inline – A Programmable SDN Switching Fabric

Big Monitoring Fabric Inline enables pervasive security in the DMZ and addresses the challenges faced by traditional solutions while offering lower-cost and SDN-centric operational simplicity. Big Monitoring Fabric Inline consists of a Big Monitoring Fabric Controller and open Ethernet switches deployed in High availability configuration. The inline security tools directly connect (optionally via link aggregation) to these Ethernet switches.

Leveraging the Big Monitoring Fabric controller as the central point of management, Big Monitoring Fabric Inline configures policies that create paths through the inline tools. The solution supports load balancing across multiple instances of the same tool as well as chaining of a set of tools on a per-policy basis. As a result, Big Monitoring Fabric Inline addresses the key operational challenges associated with deploying security tools in the DMZ:

A. Decoupling Security & Networking Infrastructure Management using SDN

Big Monitoring Fabric Inline addresses the problems with the traditional approaches by enabling network and security admins to easily deploy and manage multiple inline security or analytics tools in their production network. As shown in Figure 2, these inline/active Big Monitoring Fabric switches are managed by same pair of controllers used for managing the Big Monitoring Fabric (Out of Band).

This architecture allows for a clean separation of roles between network and security admins within the production network: tools and the rules governing which traffic flows through those tools are typically managed by the security team whereas the networking equipment and associated management is handled by the networking team.

B. Optimal Tool Utilization, Load Balancing & Service Chaining

Big Monitoring Fabric Inline supports chaining of multiple tools as well for traffic coming in as well as exiting the DMZ. Tools can be selectively chosen for incoming vs. outgoing traffic flows – **symmetric vs. asymmetric**. For oversubscribed situations, traffic flows can be load balanced across multiple lower bandwidth tools. For better tool utilization, administrators can selectively send only requisite traffic to the tools. Additionally, once a decision has been made with respect to a particular flow, the tools can programmatically (using REST APIs) off-load decision

enforcement (drop or pass through) to the Big Monitoring Fabric Inline fabric switches. For more efficient tool usage, Big Monitoring Fabric Inline also enables tool sharing across different chains.

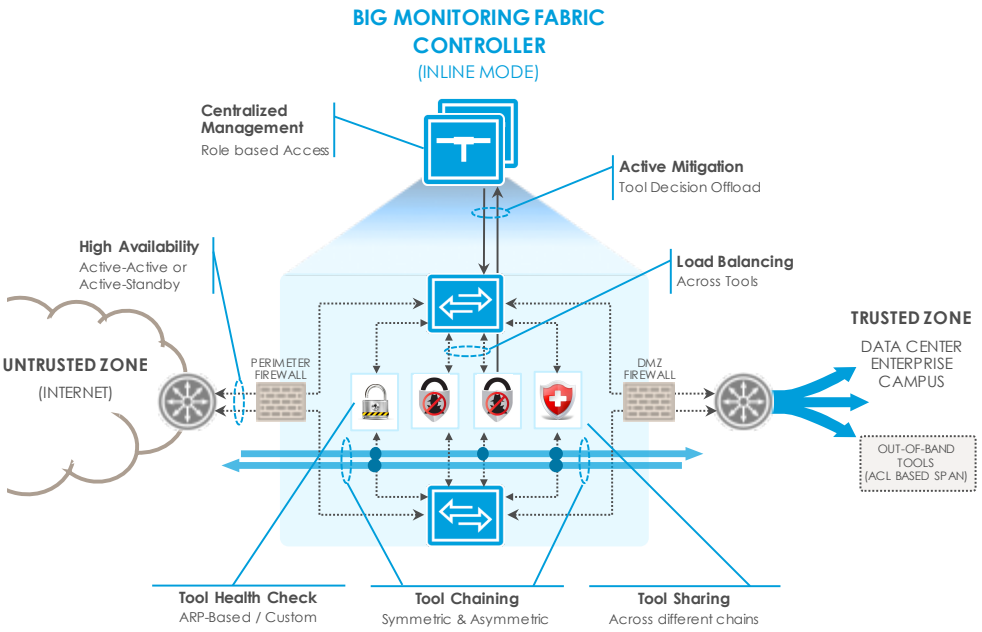

Figure 2: Security Tool Deployment in a DMZ with Big Monitoring Fabric Inline

C. Resilient Fabric Design Enables HA Deployment

Another key deployment consideration has to do with handling any eventual inline tool failures. The Big Monitoring Fabric Inline supports ARP-based as well as custom health checks to identify tool failures. Different organizations implement different HA architectures, strategies and associated operating models. In short though, it boils down to two key considerations:

- Production Network High Availability (HA) and,
- Tool Redundancy

With Big Monitoring Fabric Inline, the recommended deployment architecture addresses both these requirments.

- **Production Network High Availability:** As shown in the above Figure 2, pair of Big Monitoring Fabric Inline switches (active-active or active-standby) is typically deployed in DMZ where untrusted traffic enters the WAN router, gets inspected through the multiple security tools attached to the Big Monitoring Fabric fabric switches, and then enters the trusted internal network. This provides switch redundancy, link redundancy (inline switch to tool, production switch to inline switch), controller redundancy as well as tool redundancy.
- **Tool Redundancy**: It is also typical for tools in a DMZ to be deployed in pairs for load balancing as well as resiliency requirements. Using Big Monitoring Fabric Inline deployment as shown in Figure 2, a pair of security tools is connected to each of the two Big Monitoring Fabric switches. The tools can be deployed in **Active-Active** or **Active-Standby** mode.

Big Monitoring Fabric Inline: A Secure Alternative to Hardware Bypass Switches

Traditional Network Packet Broker (NPB) solutions that support inline tool chaining or load balancing functionality, sometimes also support hardware bypass. In case of hardware bypass switch, if a switch fails all security tools are either skipped (Fail Open) or all traffic is black holed (Fail Close). Thus rendering the organization defenseless as all untrusted traffic goes uninspected in one case or dealing with a connectivity issue in the other. Even in the scenarios where redundant hardware bypass switches are deployed, manual intervention is required to failover.

Deploying redundant pair of SDN controlled Open Ethernet switches is more secure as compared to proprietary hardware bypass switch. These switches use the same ASICs as the highly reliable switches used in most large-scale production networks and have been production-tested for reliability characteristics.

Tool Failure Scenario: Big Monitoring Fabric supports both Fail Open and Fail Close deployment designs or modes. If one of the mandatory tools fails, Big Monitoring Fabric Inline switch will bring down the failed side of the production links forcing the production traffic to steer to other switch where all security tools are up.

Big Monitoring Fabric Inline also provides an option to configure periodic data path heart-beat per tool instance. By default, if the heart-beat fails for any instance of any tool, admin is alerted. There is also an option to treat failed tool as down if the health check fails. It also provides an ability to disable the tool instance via the REST APIs.

Conclusion

Big Monitoring Fabric (Inline Mode) can be deployed in a highly available (HA) configuration to enable pervasive security in the DMZ and addresses the challenges faced by traditional solutions while offering lower-cost and SDN-centric operational simplicity.

The solution is designed to ensure maximum resilience against network or tool failures and satisfy the high availability (HA) requirements of security and network administrators. Using the centralized and programmable SDN controller based design not only enables multi-team operational workflows, it also enables optimal tool utilization through automated feedback loops. When combined with the functionality supported by Big Monitoring Fabric (Out of Band Mode), network and security administrators can finally gain pervasive visibility into their IT infrastructure.

ABOUT BIG SWITCH

Big Switch Networks is the market leader in bringing hyperscale data center networking technologies to a broader audience. The company is taking three key hyperscale technologies—OEM/ODM bare metal and open Ethernet switch hardware, sophisticated SDN control software, and core-and-pod data center designs—and leveraging them in fit-for-purpose products designed for use in enterprises, cloud providers and service providers. For additional information, email info@bigswitch.com, follow @bigswitch or visit www.bigswitch.com.