Interface Masters
TECHNOLOGIES
Innovative Network Solutions

Network Security Migration Strategies

Introduction

This paper is offered with the assumptions that the reader is familiar with networking, data security, in-line acceleration tools and passive monitoring tools, but may not be as familiar with TAPS, Bypass Switches and Aggregation and Filtering Switches.

The goal of this document is to provide an introduction and illustrate some use cases for TAPS, Bypass Switches and Network Packet Broker (NPB) focused on how they are complimentary pieces in any network security and data monitoring application. This paper is not an authoritative and detailed description of all the features and capabilities of these tools, but will introduce some valuable concepts to the reader.

The following examples are provided:

- Using TAPS and Bypass switches to add IDS/IPS functionality to a network
- Using Network Packet Broker such as Interface Masters PacketMaster™ to connect multiple tools into a network
- Retaining use of existing data security and network monitoring equipment when migrating to a higher speed network

TAP/Bypass with IDS/IPS

In general, Intrusion Detection Systems and Intrusion Protection Systems are similar and in some cases are the same tools. They can be configured in a passive manner to be an IDS or in an active manner to be an IPS. When first deploying this technology, it is prudent to activate the tool in passive mode (as an IDS). In this way, detailed configurations can be tested before being deployed and the effect on live traffic can be considered before actually changing traffic.

It is possible to attach an IDS appliance to a SPAN port on a network switch and mirror all the network traffic to the IDS through the SPAN port. Figure 1 illustrates a connection like this. However, there are limitations to SPAN ports. Most important, since a SPAN port is unidirectional and the network traffic is bi-directional, the aggregate traffic could be twice as much as the SPAN port connection. Also, in times of congestion, the switch may not be able to mirror 100% of the network traffic to the SPAN Port. In both cases the result is unacceptable because some packets may not make it to the monitoring appliance.

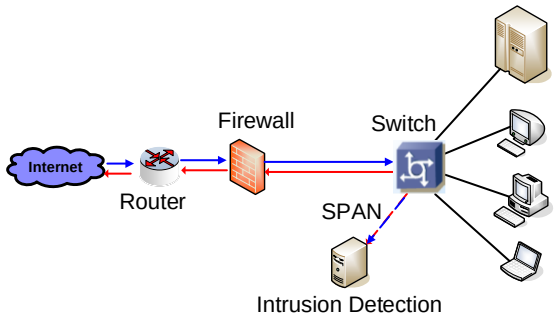

Figure 1: IDS on a SPAN Port

Therefore, it is better to attach passive inspection tools to the network using a TAP. A network TAP takes a copy of the network traffic and provides it to the monitoring appliance without modifying the network traffic. Figure 2 demonstrates this principle.

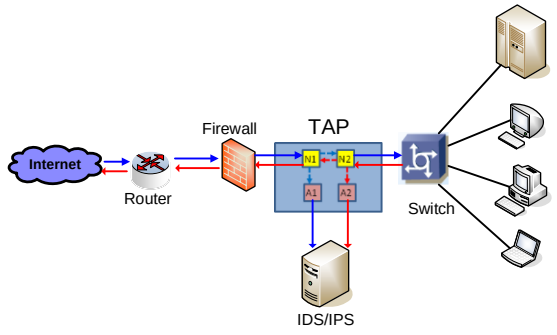

Figure 2: Network TAP Connected to IDS

Traffic flows from Network input 1 (N1) to Network output 2 (N2) and from N2 to N1 without modifying the traffic. The TAP also takes a copy of the traffic from both directions and provides it to the monitoring appliance (Appliance ports 1 (A1) and 2 (A2) in figure 2). In the event of a power failure of a failure of the monitoring tool, Interface Masters TAPS will continue to forward traffic on network ports 1 and 2. The monitoring tool (IDS) can not affect the network.

Interface Masters provides 2 types of TAP systems that can fit in this case:

- Passive TAP: Niagara 3201PT
- Aggregation TAP: Niagara 3212

The difference between the 2 TAP systems is described in The Interface Masters TAPs application notes.

Intrusion Prevention Systems are connected to the network "in-line"; meaning that they have the ability to modify the traffic before forwarding it along. If an appliance is directly connected to the network and it fails, due to a power outage or software crash, it will take the network down. Similarly, when the appliance requires a software or firmware upgrade, it can take the network down during the process. In most networks, this is unacceptable. The solution for this need is a Bypass Switch.

The function of a Bypass Switch is to allow an appliance to be connected "in-line" while also protecting the network in the event that the appliance fails. Interface Masters Bypass Switches (figure 3) support this requirement in several ways. If the IPS fails, for example due to a power failure or a software crash, the Bypass switch will immediately connect network ports 1 (N1) and 2 (N2) to each other, allowing the traffic to continue. Interface Masters offers 1G, 10G and 40G Niagara Series Bypass Switches.

The Niagara Bypass Switches can be configured to fail open or fail close. Fail open will guarantee that the network stays open and traffic will flow without interruption while fail close will close the network so traffic does not flow. Fail close is useful for networks that have redundant paths. Appropriate devices on the network will detect that the traffic is not flowing on the route where the Niagara bypass unit is present, and will then reroute the traffic using the backup path. Niagara intelligent active Bypass switches also can be configured to transmit management messages to alert the network administrator on critical events like link down, power failure, bypass state and others.

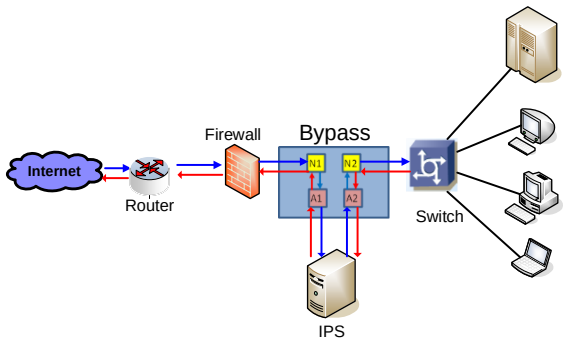

Figure 3: Network Bypass Connected to IPS

Many IPS appliances have built in Bypass, which is helpful because in the event that the IPS fails, the traffic flow will not get interrupted. Also, if the IPS needs a firmware of software update, the IPS can be put into bypass mode so that the network is not affected. However, internal Bypass lacks an important function – if the IPS itself needs to be replaced, the network will come down. Using an external Bypass provides the ability to preserve the link while replacing the appliance and by that avoiding the need for a service call. On top of that the external intelligent bypass switch can be accessed remotely via a secure shell and it provides remote management capabilities with traffic statistics to debug and resolve network issues. You can read more about the deeper feature sets of our Bypass Switch in The Interface Masters Bypass switch application notes.

TAP Systems and Bypass Switches offer network administrators very important capabilities – they offer high availability and fail safe methods for connecting, servicing and replacing security and monitoring tools on the network. Interface Masters Bypass Switches can be configured in TAP mode or Bypass mode. This allows a simple migration from IDS to IPS without network down time.

Installing multiple tools

The example above illustrated how to connect 1 passive tool (with a TAP) or 1 in-line tool (with a Bypass Switch) to a network in a fault tolerant manner. Let's consider how to connect multiple tools to a network. A Network Packet Broker such as Niagara 4248 PacketMaster™ is very useful in these cases.

PacketMaster™ performs key functions such as port mirroring, filtering and load balancing. In this way, packets can be copied, sorted and properly distributed to the right tool(s). Advanced features such as load balancing will allow one input port to be split up into multiple sessions and sent to several tools over several outputs. This is especially important when the network link to be monitored is higher bandwidth than a particular tool can handle. You can read more about our PacketMaster line in our application notes.

If we already have a Bypass Switch connected, we can upgrade the security and monitoring capabilities by adding a PacketMaster™ to the Bypass switch and then connecting passive and in-line tools to the PacketMaster™. Since the Bypass switch will ensure network uptime, the PacketMaster™ can be added without any network downtime. If there is not a Bypass/TAP already connected, we may consider a more advanced Bypass product such as Niagara 2818PT. Niagara 2818PT is capable of connecting to 4 x 10G network links and providing them to a PacketMaster™ with both Bypass connections and TAP connections. Keeping the Bypass connections and TAP connections separate simplifies network deployment, debug and upgrades.

Figure 4 illustrates how a PacketMaster™ such as Niagara 4248 (48 ports of 1G or 10G) and a Bypass switch such as Niagara 2818PT can be used together to connect multiple passive and active tools to a network. As the needs of the enterprise grow, tools can be added to increase network visibility and protection. In figure 4, an Intrusion Prevention System and a Distributed Denial of Service Device (DDoS) are connected in line and each can modify the network traffic. An Application Performance Management and Network Behavior Analysis device are connected passively without modifying the network traffic. Using an Network Packet Broker such as Niagara 4248, the in-line appliances can be connected in series or portions of the traffic can be filtered to one appliance or the other.

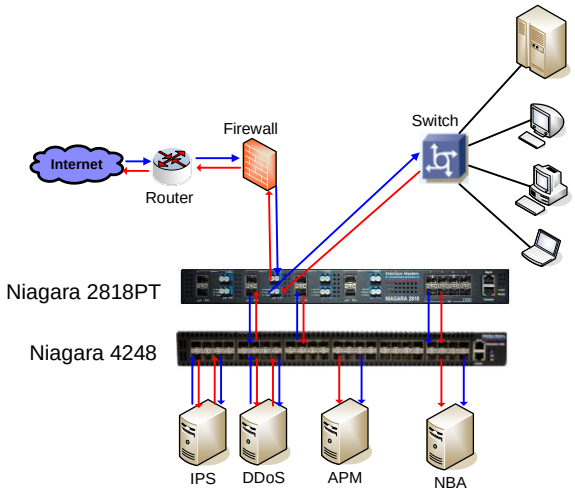

Figure 4: Bypass and NPB

Migrating from 1G to 10G or 10G to 40G / 100G

In the descriptions above, network speed was not discussed. Assume that you have invested in some 1G in-line and passive monitoring tools. Now assume you upgrade your network to 10G. When first upgrading a network from 1G to 10G, traffic does not automatically increase to 10G

overnight. Initially, network traffic is still under 1G, but over time increases to 2G, 3G and higher. Figure 5 shows how PacketMaster™ can enable re-use of existing tools in a higher speed network.

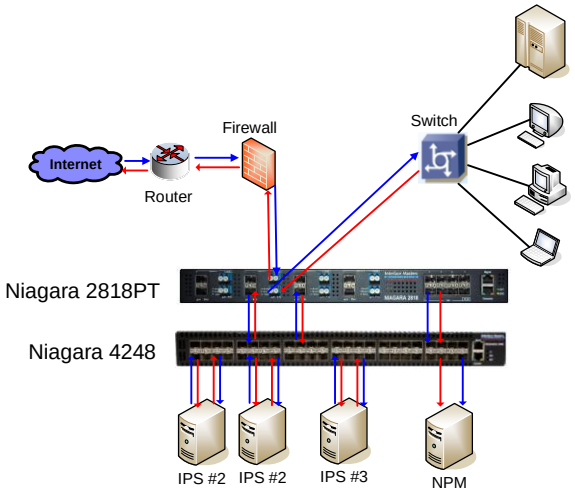

Figure 5: Network Upgrade

Niagara 4248 supports both 1G and 10G connections, while Niagara 4232-4XL supports also 40G connections. These systems also have the ability to filter, sort and load balance traffic in a session aware manner among multiple outputs. Therefore, it can connect to a 40GE or 10G input from the Bypass Switch and co-ordinate traffic flows to multiple in-line appliances such as IPS, Traffic Shaping/QoS, WAN acceleration or Data Loss Prevention tools. On the return path, the PacketMaster re-assembles the traffic flows back to the Bypass Switch.

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.

150 East Brokaw ● San Jose, CA 95112
Sales: 408.441.9341 ext. 100
Support: 408.441.9341 ext. 2
www.interfacemasters.com