

From IDS to IPS mode:

Deploying Network Critical Bypass TAPS with  
Sourcefire Solutions

3/23/2010



**Network Critical**  
The Window to your Network™

---

## From IDS to IPS: Deploying Network Critical Bypass TAPs with Sourcefire Solutions

---

No IDP solution will provide a benefit to your environment if you are not effectively capturing traffic from the network. While not a difficult process, network traffic capture is critical to a successful deployment. While some may think "... place a sensor behind the firewall and we're covered" this turns out to be very limited solution. Because the predominant threat is found to be originating not from the Internet, but from the very systems that already have privileged access to your network this solution is rarely a fix to the problem.

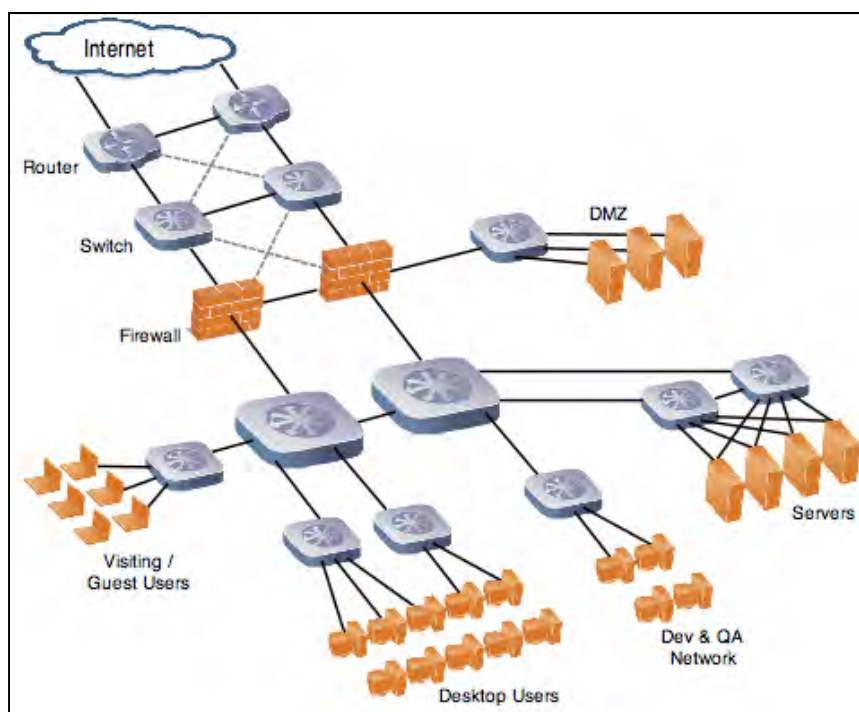
An in-depth monitoring solution can easily monitor the majority of network traffic and provide much more granularity in identifying attacks to the networks, pre-cursors to vulnerabilities in the network that may be exploited, and out-right policy violations that may require enforcement.

The challenge to a successful deployment requires balancing the needs for monitoring (based on policy or comfort with risk) with the cost of widespread deployment (in equipment, operations and management). Additionally, different parts of your network will need to be monitored in different ways for:

- a) the type of protection you are intending to provide
- b) the type of policy you are trying to enforce
- c) the type of traffic you are hoping to monitor

Different segments of the network provide different types of data and will allow you to either protect or monitor for certain types of activities. For example, monitoring in front of a firewall and behind a firewall provide extremely different IDS event results. In fact, many would argue that there is little value in placing an IDS external to your security perimeter, since you'll be filtering the traffic anyways. However, an IPS, external to the firewall, can provide a reduction of traffic that may be beneficial to gateway security products (ie. reducing high volume denial-of-service events).

Taking a sample network below, there are a number of items to take note of in the network configuration for providing passive and active monitoring.



---

## From IDS to IPS: Deploying Network Critical Bypass TAPs with Sourcefire Solutions

---

In placing an IDP just behind the firewalls, do we place one or two? Well, is the routing asymmetric or not? Then the next obvious segment is providing security to the DMZ, should IDS or IPS be used? Let's assume an IPS for the moment between the firewall and the DMZ switch. There are only a few assets, and that network segment is very tightly controlled. But how should the server farm be addressed? An IPS implementation (on each line into the redundant switches) might add a layer of protection, but what if an asset is already compromised? Or an authorized user accidentally brings something into the server segment while doing operational work? An automated network threat could be moving between servers (or between users in other segments) without ever being identified until it has cause to leave the broadcast domain of the server farm and be routed across an IPS.

It is important to remember, that IDS approaches (passive, alert-only detection) still play a significant role in the security model. Passive monitoring still tends to be less processor intensive; since deployments are passive (and dealing with only copies of traffic) there is no chance for introducing traffic latency, or disruption to traffic content.

### **Sourcefire IDS to IPS implementation**

For customers wanting the flexibility of using Sourcefire solutions in a passive, alert-only detection mode and then migrate to an active, in-line implementation, the recommended solution is to use a bypass tap solution with the Sourcefire sensor that allows the customer to make those changes remotely.

Network Critical's V-Line (virtually in-line) bypass tap solutions provide options for customers who want a seamless migration from IDS (passive, alert-only mode) to IPS (active, inline mode). The three modes are as follows:

- a) Breakout TAP
- b) Aggregating TAP
- c) V-Line (bypass)

**Breakout TAP** mode separates the bi-directional full-duplex network traffic into Rx and Tx streams, and uses one Monitor Port for each stream. This mode is used when 100% guaranteed traffic collection is required, and the network tool has dual ports running at the same speed as the Live Network.





Note: the Sourcefire 3D 9900 sensor has a TAP mode configuration. However, the Network Critical V-Line TAP offers the benefit of inserting and removing the sensor without network downtime

**Aggregating TAP** mode combines the bi-directional full-duplex network traffic into a single stream, and can present two copies of the traffic, one on each Monitor Port. This mode is used when the network tool has only a single interface. If the aggregated traffic rate exceeds the inbound network bandwidth of the network tool then excess packets will be dropped at the Monitor Port. If 100% guaranteed traffic collection required then the network tool interface must run faster than the Live Network, or Breakout mode must be used.

**V-Line (bypass)** mode is a way of safely deploying and maintaining inline network tools without risk of downtime to the Live Network. The TAP provides extra layers of failsafe for any inline tool, by continually checking throughput and availability it can seamlessly switch the tool into or out of the network path; with the tool now *virtually inline* it can be freely reconfigured and rebooted without affecting the Live Network link.

## From IDS to IPS: Deploying Network Critical Bypass TAPs with Sourcefire Solutions

### Network Critical products for use with Sourcefire IDS/IPS Solutions

	Smart Network Access System with V-Line Modules	1U Chassis modular chassis with aggregating and regenerating backplane, choice of Multi-mode or single mode fiber or copper RJ-45 modules with V-Line, Aggregating and Breakout modes
	VL-1005	1U Integrated Chassis Gigabit Copper RJ-45 V-Line (Bypass) TAP
	VL-1010	1U Integrated Chassis Multi-mode Fiber V-Line (Bypass) TAP
	VL-1015	1U Integrated Chassis Single mode Fiber V-Line (Bypass) TAP

### Conclusion

Network Critical Bypass solutions offer a unique approach to customers who prefer deploying Sourcefire solutions in passive-monitor mode (IDS mode) but need a seamless migration when configuring Sourcefire sensors to in-line/ active mode (IPS mode) in the future. The combination of Network Critical and Sourcefire solutions allow the customer to determine the right deployment path to pursue when considering an overall IDP strategy.

### Who is Network Critical?

Network Critical, the creator of the leading enterprise access technology solutions, provides lab-certified, innovative, carrier-grade technology which allows complete access to network traffic for analysis, monitoring, security and auditing purposes. Our unique products provide flexibility and functionality for any network, whether large or small. Network Critical's portable and enterprise solutions provide 100% network visibility with zero packet loss 24 hours a day, 365 days a year.

Network Critical solutions have been tested, certified and utilized in Fortune 500 organizations and government agencies around the world. Network Critical is a global access technology solution provider with operations based in Buffalo, NY USA; Reading, Berkshire UK; and Amsterdam, the Netherlands. For more information, visit [www.networkcritical.com](http://www.networkcritical.com).