

JUSTIFYING THE NEED FOR TAPS

The Problem

Over the past decade or so, the use of switches to replace hubs has increased substantially. This is largely due to the increased size of networks, and the requirement for increasingly faster and more efficient networks. On most networks, the data must now be dependable and timely. This transition from hubs to switches, however, has generated a conflict with already deployed and designed network intrusion detection systems.

Why Use TAPs ?

To understand why TAPs should be used in these situations, it may be helpful to look at some of the options that have been traditionally used for implementing a nIDS into a switched environment. The most commonly used alternative is port spanning, also known as port mirroring. This option, although used often, has inherent flaws that create problems in implementing nIDS systems with it. Most switches in use today offer support for port mirroring but one needs to understand the issues with port mirroring first:

Almost all switches today support SPAN (Mirror) port. The span port essentially gets a copy of all the traffic on the switch thereby enabling one monitor network traffic and use with intrusion detection systems. The major issues surrounding SPAN port are:

a) Port Spanning on a switch often increases the CPU cycles and memory requirements as the switch has to buffer the network traffic that has to be copied to the mirror port.

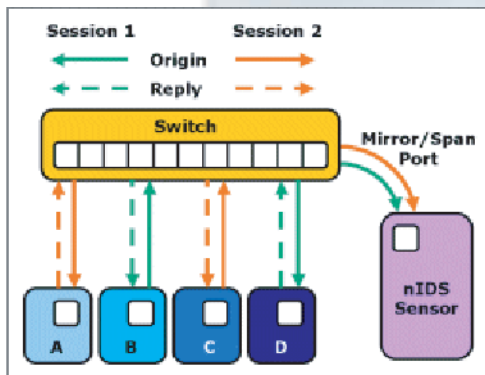


FIG 1: Note that half of the session is not being sent to the Mirror/SPAN Port ; thus the nIDS is not able to detect events within these messages.

b) The switches are designed remove the low level (Layer 1 & 2) errors from the data stream. That means the monitoring device connected to the SPAN port does not receive error packets or VLAN information and this makes low level troubleshooting impossible.

c) With a span port running at full bandwidth rate to get both direction of network traffic, could result in large amounts of data to be lost. Most switches consider mirrored traffic as low priority and when the switch is overloaded it disables port mirroring and potentially leaving you vulnerable. Another important factor to note is that a SPAN port behaves like a port on a hub. This means that there will be a higher rate of packet collisions, as other ports on the switch continually send packets to the mirror/span port.

d) SPAN Port or mirroring only presents one side of a full-duplex connection. Thus, the nIDS sitting on a mirror port is severely limited as it is completely blind to half of the traffic on the link. (See FIG 1)

e) SPAN ports are usually bi-directional ports versus being unidirectional (receive only) ports. Such a configuration could leave a nIDS sensor vulnerable to being detected and attacked by a sophisticated attacker.

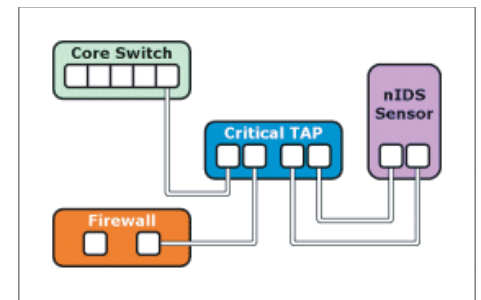
What is a TAP (Test Access Port) ?

To combat design conflicts between network intrusion detection systems (nIDS) and switches, network TAPs were created. Network TAPs essentially allow all traffic on a network device to be monitored. Network TAPs are also very useful for passive network troubleshooting and analysis. Further, the TAP makes the related nIDS system more secure, preventing attackers from being able to directly attack the nIDS system. They negate the expense and the problems associated with all of the above mentioned drawbacks using the traditional method.

TAPs Enhance Security

Taps can actually increase the security of an intrusion detection system installation. The reason for this is quite simple: nIDS's behind a TAP does not require an address because the TAP is a passive device that takes any and all data off the line and throws it directly to the nIDS sensor with a unidirectional interface that has no address; therefore, no traffic can be directed specifically towards the nIDS. This prevents directed attacks against the nIDS system, and can actually make attackers believe that no nIDS is present to identify and track their attacks. By preventing the detection of the nIDS by attackers, the survivability of the system is significantly increased. After all, what

good is an nIDS, if it can be detected, attacked and disabled?



A typical installation of a TAP between a firewall and a core switch. This placement will send all incoming and outgoing traffic to the nIDS sensor allowing it to see any attacks that manage to bypass the firewall security.

Cost Benefits of Using TAPs

Most organizations have already made significant investments in the network and network security infrastructure. If a nIDS was in use before the TAP was implemented, no change in the nIDS technology would be required to implement it with a TAP. As no new nIDS systems are being deployed, implementation costs are virtually non-existent.

Critical TAP

Critical TAP technology supports network monitoring, analysis and intrusion detection for almost any network configuration. Critical TAP's are extremely reliable and incorporate fail safe technology i.e. in the event of a power loss the data flow is never interrupted. They feature passive-link integrity enabling the network to operate at continuous flow. All Critical TAP's are rack mountable that are extremely easy to install with broad network compatibility. They are compatible with all major vendors' analyzer and IDS products.

Securicore Inc.

Tel: 416-444-7530

Fax: 416-383-1639

E-mail: sales@securicore.ca

Web: www.securicore.ca