

Re: IPS and Trunking

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2007-02/msg00008.html>

- *From:* Paul daSilva <pdasilva@xxxxxxxx>
 - *Date:* Thu, 08 Feb 2007 16:21:02 -0500
-

The function that you speak of on the Cisco is a feature of the switch itself (called DSPAN), not a feature on the IDS/IPS devices. This feature is common across enterprise-grade switches, and allows for the monitoring of all traffic flowing through the ports on that switch.

IDS (Intrusion Detection) devices typically connect to DSPAN ports to "see" all traffic. This holds true for most (if not all) vendors mentioned.

IPS (Intrusion Prevention) devices ideally connect in-line, between your router and your firewall, blocking all intrusions at the network gateway.

HTH,
Paul

trav_2@xxxxxxxxxxxxx wrote:

Cisco has a great feature where I can configure all traffic on a switch to go to a trunk port, plug in the IPS/IDS to the trunk port and see all traffic. Can other vendors, such as Sourcefire, TippingPoint, ISS do this?

Thanks,

Test Your IDS

Is your IDS deployed correctly?

Find out quickly and easily by testing it with real-world attacks from CORE IMPACT.

Go to

http://www.coresecurity.com/index.php5?module=Form&action=impact&campaign=intro_sfw
to learn more.

Test Your IDS

Re: IPS and Trunking

Is your IDS deployed correctly?

Find out quickly and easily by testing it with real-world attacks from CORE IMPACT.

Go to http://www.coresecurity.com/index.php5?module=Form&action=impact&campaign=intro_sfw to learn more.
