

RE: IPS and Trunking

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2007-02/msg00019.html>

- *From:* Luis Lopez Sanchez <luis.lopez@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 13 Feb 2007 11:27:56 +0100
-

Hi all,

The top leader in the "Magic Quadrant for Network Intrusion Prevention Systems Appliances, 2H06[1] –in addition to mentioned Cisco and McAfee products– are able to decoding the dot1q from ethernet frames to analyze data information encapsulated in differents VLANs. I've perform an recent study about this feature in main IDS/IPS products:

* 3Com/TippingPoint Intrusion Prevention Systems

=====
http://www.tippingpoint.com/pdf/resources/datasheets/400918-005_ipstechspecs.pdf

Supported VLAN

Feature:

"Protocols/Applications (partial list)

* VLAN "

* Sourcefire/Snort

=====
It has a 802.1q decoder which supports inspection of VLANs using low communications layers from OS (Linux kernel and others *nix)

* IBM/ISS

=====
Proventia Intrusion Prevention System

http://documents.iss.net/literature/proventia/ProventiaNetworkIPS_Brochure.pdf

Feature:

"Policy per VLAN tag"

* Juniper Networks IDP 50/200/600/1100

=====
<http://www.juniper.net/products/intrusion/dsheet/110037.pdf>

RE: IPS and Trunking

Feature
"Enterprise Networking 802.1Q VLAN Support"

References:

[1]
<http://mediaproducts.gartner.com/reprints/juniper/vol2/article2/article2.html>

Regards,

--

Luis Lopez
InfoSec / IT-IS
Atos Origin
Albarracin 25 Madrid 28037
Spain
Phone: +34912148329
PCell: +34649836261
Fax: +34912148871
luis.lopez@xxxxxxxxxxxxxxxxx
<http://www.atosorigin.com>

pub 1024D/8A688104 1999/07/28 Luis Lopez luis.lopez@xxxxxxxxxxxxxxxxx
Key fingerprint = 550F 3545 C847 F61E 821C 3D8C 1A12 2C19 8A68 8104

"These are the thoughts and opinions of Luis Lopez, and does not represent Atos Origin company policy."

"Estos son los pensamientos y las opiniones de Luis Lopez, y no representan la política de compañía de Atos Origin."

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxx>] On Behalf Of Chris Brown
Sent: lunes, 12 de febrero de 2007 17:54
To: 'Gary Halleen'; 'Eric Hines'; 'Andrew Plato'
Cc: focus-ids@xxxxxxxxxxxxxxxxx
Subject: RE: IPS and Trunking

Also supported by McAfee IntruShield, you can also specify a separate policy for each VLAN you see on the Trunk. This can be further broken down and a policy can be defined for each individual host either inbound or outbound if you so wish.

Regards

Chris

---Original Message---

From: listbounce@xxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxx>] On Behalf Of Gary Halleen

RE: IPS and Trunking

RE: IPS and Trunking

Sent: 09 February 2007 01:46
To: Eric Hines; Andrew Plato
Cc: trav_2@xxxxxxxxxxxxxx; focus-ids@xxxxxxxxxxxxxxxxxxxxxx
Subject: Re: IPS and Trunking

I've seen several replies saying essentially the same thing: "This is a feature of the switch – not the IDS."

However, this is only partially true.

It is certainly a function of the switch to be able to copy traffic to a destination port using something like SPAN, VACL Capture, or other similar features. Many switches support sending this captured traffic to an 802.1q or ISL trunk port. All currently shipping Cisco switches, to the best of my knowledge, support this.

Most IDS products should be able to at least analyze traffic that arrives via trunk ports. All Cisco IDS/IPS products have supported this for as long as I can remember. Additionally, Cisco IDS/IPS sensors are able to track the VLAN traffic arrives on through the trunk port, rather than simply grouping the traffic all together. The event action can be dependent on which VLAN the malicious traffic was seen on. In the alert that is triggered, the VLAN from the trunk port is displayed.

I don't know what vendors support this capability, but it is certainly supported by Cisco sensors.

If we talk about IPS instead of IDS, the feature remains for us. You can plug an interface on a Cisco IPS sensor into a trunk port, and the sensor can treat each VLAN on the trunk separately.

Gary Halleen, CISSP, ISSAP
Cisco Systems, Inc.

On 2/8/07 3:00 PM, "Eric Hines" <eric.hines@xxxxxxxxxxxxxxxxxxxx> wrote:

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Trav_2:

You're talking about two separate things.

1) Cisco is a switch and you're talking about a mirror/span port.
Though, network taps > Span ports :)

2) Its not the IDS/IPS that is performing that capability, its the switch. So its inaccurate to ask if the IDS/IPS vendors you mentioned can do the same thing. A span port doesn't care whats hooked up to it, whether its Snort or a sniffer.

Hope this helps.

RE: IPS and Trunking

Best Regards,

Eric Hines, GCIA, CISSP
CEO, President
Applied Watch Technologies, LLC
1095 Pingree Road
Suite 221
Crystal Lake, IL 60014
Toll Free: (877) 262-7593
Fax: (847) 854-5106
Cell: (847) 456-6785
Web: www.appliedwatch.com

Andrew Plato wrote:

If you create a mirror port and plug in any IPS/IDS, it will see the traffic. TippingPoint, ISS, etc. All can do that.

Also, pretty much any decent managed switch can have mirror ports. This is not unique to Cisco.

Keep in mind, you cannot do real-time IPS (intrusion prevention) in any reliable manner this way. You have to be IN-LINE to do real-time blocking and filtering. Passive monitoring off a mirror port only allows you to send RSTs to stop stuff, and that is not a very reliable way to block bad stuff.

Andrew Plato, CISSP, CISM
President/Principal Consultant
Anitian Enterprise Security

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx
[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]
On Behalf Of trav_2@xxxxxxxxxxxxx
Sent: Monday, February 05, 2007 10:44 AM
To: focus-ids@xxxxxxxxxxxxxxxxxxxxx
Subject: IPS and Trunking

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,

RE: IPS and Trunking

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

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

ro_sfw
to learn more.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.5 (Darwin)

Comment: Using GnuPG with Mozilla - <http://enigmail.mozdev.org>

iD8DBQFFy6t31va6QYTV0EMRAuSkAJ4+1WTm+ugpOAK4Ghzv8ooYyFYi1gCfSC69
cXQfDMCJ7O14l+ZnE/lpTsY=
=ego2

-----END PGP SIGNATURE-----

Test Your IDS

Is your IDS deployed correctly?
Find out quickly and easily by testing it with real-world attacks from

RE: IPS and Trunking

CORE IMPACT.
Go to

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

to learn more.

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

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.

This e-mail and the documents attached are confidential and intended solely for the addressee; it may also be privileged. If you receive this e-mail in error, please notify the sender immediately and destroy it. As its integrity cannot be secured on the Internet, the Atos Origin group liability cannot be triggered for the message content. Although the sender endeavours to maintain a computer virus-free network, the sender does not warrant that this transmission is virus-free and will not be liable for any damages resulting from any virus transmitted.

Este mensaje y los ficheros adjuntos pueden contener informacion confidencial destinada solamente a la(s) persona(s) mencionadas anteriormente. Pueden estar protegidos por secreto profesional Si usted recibe este correo electronico por error, gracias de informar inmediatamente al remitente y destruir el mensaje.

RE: IPS and Trunking

RE: IPS and Trunking

Al no estar asegurada la integridad de este mensaje sobre la red, Atos Origin no se hace responsable por su contenido. Su contenido no constituye ningun compromiso para el grupo Atos Origin, salvo ratificacion escrita por ambas partes.

Aunque se esfuerza al maximo por mantener su red libre de virus, el emisor no puede garantizar nada al respecto y no sera responsable de cualesquiera danos que puedan resultar de una transmision de virus

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.
