

RE: Firewall and VLAN security design

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-11/0090.html>

From: Paul Benedek (paul.benedek_at_excis.co.uk)

Date: 11/03/04

To: "'Ivan Coric'" <ivan.coric@workcoverqld.com.au>, <bsampsel@libertyactivist.org>, <security-basics@securityfocus.com>
Date: Wed, 3 Nov 2004 19:34:49 -0000

Because of the way that switches deal with broadcasts, they can be insecure. VLANs as a form of separation is not a thorough method of separating a network. There is however a technology called a private VLAN that is more secure and allows you to control traffic at layer 2 by installing access lists on your switches and by designating ports with differing levels of control. Cisco and Nortel switches have this capability and Cisco does recommend it for use within the SAFE methodology.

The SAFE methodology calls for defence in depth and Private VLANs are one of their recommendations for Layer 2 defence. They further recommend other devices such as IDS, firewalls and filtering to give additional security at this and other layers.

Paul Benedek
Director
Excis Networks Limited

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

From: Ivan Coric [<mailto:ivan.coric@workcoverqld.com.au>]

Sent: 03 November 2004 04:44

To: bsampsel@libertyactivist.org; security-basics@securityfocus.com

Subject: RE: Firewall and VLAN security design

I beg to differ, using VLANs to segregate your external and internal network is a bad idea.

I don't think even Cisco recommends VLANs as a security mechanism

<http://www.sans.org/resources/idfaq/vlan.php>

<http://www.spirit.com/Network/net0103.html>

<http://www.terena.nl/conferences/tnc2003/programme/slides/s1c3.ppt>

<http://www.sans.org/rr/whitepapers/networkdevs/1090.php>

<http://www.google.com.au/search?q=vlan+hopping&hl=en&lr=&start=10&sa=N>

SecurityFocus BASICS: RE: Firewall and VLAN security design

cheers
Ivan

Ivan Coric, CISSP
IT Technical Security Officer
Information Technology
WorkCover Queensland
Ph: (07) 30066414 Fax: (07) 30066424
Email: ivan.coric@workcoverqld.com.au

>>> "Bryan S. Sampsel" <bsampsel@libertyactivist.org> 2/11/2004 2:56:11
pm >>>

>
>> *Is VLAN segmentation enough to segment between the internet, DMZ
and
>> the internal network, or should I also use different switches for
>> each, and be connected through the firewall.*
>
> *This is a FAQ, and the usual answer is that no, VLAN separation is
not
> a robust security barrier, an separate switches are recommended where
the
> different subnets need separation for security reasons.*
>

Actually, if you don't offer up your management interface to the
publicly
accessible side of things, the VLAN separation makes things function
exactly like a physically separate switch. Without the routing
between
those VLANs, the traffic does not magically go from one VLAN to
another
and the ability to exploit/crack the switch is no greater than having
a
separate switch in place. In fact, if you have a managed switch, and
do
not logically isolate your management interface/IP, you're opening up
that
standalone switch.

If you're not crazy enough to put the management IP on the publicly
accessible side, there is no risk unless you allow access through a
firewall or other routing solution. This is a fundamental concept of
managed switches and VLANs.

This is at least true of Foundry Networks and Cisco switches. Mileage
may
vary. ;)

Sincerely,

RE: Firewall and VLAN security design

SecurityFocus BASICS: RE: Firewall and VLAN security design

Bryan S. Sampsel
LibertyActivist.org
FNCNE

Messages included in this e-mail and any of its attachments are those of the author unless specifically stated to represent WorkCover Queensland. The contents of this message are to be used for the intended purpose only and are to be kept confidential at all times.

This message may contain privileged information directed only to the intended addressee/s. Accidental receipt of this information should be deleted promptly and the sender notified.

This e-mail has been scanned by Sophos for known viruses. However, no warranty nor liability is implied in this respect.
