

Bridging vlans w/firewall and selective HTTP redirect?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2004-09/0330.html>

From: Kevin Schmidt (*kps_at_ucsb.edu*)

Date: 09/28/04

To: freebsd-net@freebsd.org

Date: Tue, 28 Sep 2004 10:10:02 -0700

Hi all,

I'm interested in placing an FBSD box (prefer 4.x since it's production, though I've also used 5.2) inline on a link with 802.1Q-tagged vlans with firewalling and selective HTTP redirects. Bridging a couple of ethernet isn't a problem, and it appears I can enable ipf or ipfw (but not pf; too bad, ALTQ and pfsync would be nice). What does not appear viable is the interception and transparent redirect of HTTP traffic in this bridged environment. Anyone know of a good way to do this?

The purpose of the above is to support a wireless network where users may be associated with various vlans, some of which will require selective traffic filtering and transparent http redirects. For example, there might be an SSID for a "readme" vlan network where people could log in to a web page and download an 802.1X supplicant. The supplicant would be preconfigured to join another SSID, e.g. "campus wireless", which would allow authenticated users full Internet access. If a particular user is known to have a compromised/infected system, they'd be mapped to a quarantine vlan, which ideally would block most traffic and redirect them to a web page with additional information and remediation tools. Similar techniques would be used to support an https login process that would selectively open the firewall for authenticated users. I'm sure someone reading this is wondering, "why not do the web redirects on a routed interface instead of with an inline bridge, since redirects at an L3 interface work?" The answer is scalability and roaming: I'd like routing to be done at a couple of upstream Cisco boxes, with two or more FBSD boxes inline on the downstream vlans supporting wireless and (ultimately) some wired ports. I'll do it routed if I must, but it would be great if I could redirect locally at the bridge.

I'm looking at Linux/OpenBSD/NetBSD, too, though I've always preferred FBSD (still have my 1.x CDs) and have happily used it for DNS, web, ftp, etc. servers for years.

Any suggestions/comments/questions welcome.

freebsd-net: Bridging vlans w/firewall and selective HTTP redirect?

Cheers,

--

Kevin Schmidt
Campus Network Programmer
Office of Information Technology
University of California, Santa Barbara
North Hall 2124
Santa Barbara, CA 93106-3201
805-893-7779
805-893-5051 FAX
kps@ucsb.edu

freebsd-net@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-net>

To unsubscribe, send any mail to "freebsd-net-unsubscribe@freebsd.org"