

RE: [fw-wiz] Link level security with static arp tables

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-10/0102.html>

From: Sloane, David (*DSloane_at_vfa.com*)

Date: 10/14/03

To: <firewall-wizards@honor.icsalabs.com>

Date: Mon, 13 Oct 2003 18:12:57 -0400

Would it be easier to solve this at a switch? If you have a switch capable of filtering by mac-address (or mac-based VLANs), you'll probably get better performance all around. The last time I talked to a Cisco tech about VLAN options, I was told that VLAN's on Cisco switches perform best using MAC-address lists.

So a VLAN could isolate the traffic. Or an access-list. It depends on your switch and what kind of filtering it supports.

-David

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

From: firewall-wizards-admin@honor.icsalabs.com

[mailto:firewall-wizards-admin@honor.icsalabs.com] On Behalf Of Debian User

Sent: October 12, 2003 8:32 AM

To: firewall-wizards@honor.icsalabs.com

Subject: [fw-wiz] Link level security with static arp tables

Hello,

Problem:

```
[ INET ] ----- <eth1> [ NAT GATEWAY ] <eth0> ---- [ LOCAL NET, 50 clients ]
```

I need to limit access to the gateway according to allowed MACs, ie Ethernet frames from allowed MAC addresses are forwarded to and fro in the gateway, but others will be dropped (and logged if possible).

I could disable arp on eht0 and use static arp tables in the gw, but that would mean that the gateway won't answer any arp queries, hence the

Firewall-Wizards: RE: [fw-wiz] Link level security with static arp tables

clients
will not be able to find it's MAC. Setting up static arp tables in
clients is
not an option.

I could use netfilter MAC matching support in the kernel, but that would
mean
I have to add 50 rules to the ruleset adding considerable overhead.
Moreover,
it is a link level problem that could be solved in the same level, so
netfilter is not an attractive option. Please comment if I'm wrong.

Any solutions?

firewall-wizards mailing list firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>