

## Re: Vlan and Firewall

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-09/0793.html>

---

**From:** Walter Roberson (*roberson\_at\_ibd.nrc-cnrc.gc.ca*)

**Date:** 09/19/05

Date: Mon, 19 Sep 2005 12:54:38 +0000 (UTC)

In article <1127114124.536497.113260@g43g2000cwa.googlegroups.com>, <Sid.lochan@gmail.com> wrote:

:I know a little about firewalls. In my new company right now we have  
:150 systems including servers behind 198.168.165.0 IP range. We have a  
:PIX 501/IOS 6.2-firewall which protects us.

PIX questions are usually better put to comp.dcom.sys.cisco.

:Now i have been told to  
:create vlans for 5-6 departments as well as one vlan for servers with  
:access limited to some vlans.We have 7 2950 series swtichs.  
:I want to know that  
:1. Do i have to change setting in PIX too for Vlans.?

Not directly: the PIX 501 has no understanding of VLANs. You might, though, need to adjust it to handle multiple IP address ranges.

:Will firewall be  
:able to see all diffrent VLANS under 1 ip range that is 192.168.165.0

No. And multiple VLANs with a single IP address range is -usually- asking for trouble.

:2. IF i created vlans on switches then how i'll direct them to use  
:Firewall to gain access to VPN and Internet.?

You cannot, not with a PIX 501.

A PIX 501 is not an appropriate PIX model for 150 internal devices, not unless only a fraction of those devices need to communicate with the outside world.

The architecture you will need to adopt will depend upon whether those VLANs need to be firewalled from each other, or whether the VLANs exist for broadcast reduction purposes instead of for access control purposes.

If the VLANs exist for access control purposes, you will need a firewall that handles VLANs directly, or one with multiple physical interfaces (with you breaking out one VLAN per physical interface.)

If the VLANs exist for traffic control purposes, then if you want to stick with the PIX 501, you need an internal router or layer 3 switch such as a Cisco 3550 or Cisco 3750.

Cisco firewalls that will handle 6 VLANs include:

- Cisco PIX 515/515E with an Unrestricted license, running PIX 6.2 or 6.3
- Cisco PIX 520 running PIX 6.2 or PIX 6.3
- Cisco PIX 525 with Restricted or Unrestricted license, running PIX 6.2 or 6.3
- Cisco PIX 535 with Restricted or Unrestricted license, running PIX 6.2 or 6.3
- [if I recall correctly] Cisco PIX 515/515E, 525, or 535, running PIX 7.0
- the new Cisco ASA Security Appliance series, running 7.0 software

Notes:

- The 520 will not be supported beyond 6.3
- the 515E is about 1/3 faster than the 515
- most 515 would require a memory upgrade to run PIX 7.0. Newer 515E do not require a memory upgrade; older 515E do.

--

Look out, there are llamas!