

## Re: [fw-wiz] Pix 535 Logging

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-11/msg00012.html>

---

- *From:* "David Swafford" <[dswafford@xxxxxxxxxxxxxxxxxxxxxx](mailto:dswafford@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 08 Nov 2006 10:58:18 -0500
- 

Have you thought about just blocking all outbound port 25 connections except for your authorized MX and mail servers? We did that at my company about a year back and eliminated the problem of infected machines flooding spam out from our network.

Just a thought,

David.

---

David A. Swafford, Network Engineer  
Information Technology Team  
Archbishop Alter High School

EC-Council Certified Ethical Hacker

A Cisco Systems, Inc., Certified Network Associate (CCNA)  
and a CompTIA Network+ and Security+ Certified Professional

james.burns@xxxxxxxxxxxxxxxxxxx 11/8/2006 5:50 am >>>

Hi,

I have a quick question regarding logging on a Pix 535.

We're currently getting a lot of CERT notifications for spammers operating within our network – mainly just students with 0wned machines, but we're looking into ways to automate the procedure slightly.

Anyway, what I'm looking to do, and what I need help with.... I want to know if it's possible to log all outbound port 25 connection attempts, EXCEPT those that come from our authorised MX's and mail servers. AND I would like to be able to do this in addition to the normal logging that takes place.

So, is it possible?

Re: [fw-wiz] Pix 535 Logging

Any thoughts and guidance you can provide are very much appreciated.

Cheers,  
James

—  
James Burns

Network Advisor \* Student & Learning Support  
University of Sunderland

—  
University of Sunderland – life-changing: see our new TV advert at  
<http://www.lifechangingsunderland.com> or <http://www.sunderland.ac.uk>

---

firewall-wizards mailing list  
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

---

Founded in Faith – Preserved with Pride – Sustained by Spirit

---

Upcoming Events:  
ALTER OPEN HOUSE  
November 16  
7 – 9 p.m.

---

firewall-wizards mailing list  
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>