

## router rules

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-01/0119.html>

---

**From:** Rahul ([Rahul@unsecure.co.uk](mailto:Rahul@unsecure.co.uk))

**Date:** 01/08/03

From: "Rahul" <[Rahul@unsecure.co.uk](mailto:Rahul@unsecure.co.uk)>  
To: <[security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)>  
Date: Wed, 8 Jan 2003 13:13:40 -0000

hi everyone,

i have a vigor router, (2600), which i just brought. it seems pretty slim on documentation on the firewall. i am very new to firewall concepts. i have a network (well, ok a workgroup), of 4 static computers, and about 3 dynamic ones (laptops), these get their ip off the router.

i created a block all in/out filter on the firewall unless it matches the following rules;

```
allow always if destination port=80 & protocol = tcp
allow always if destination port=443 & protocol = tcp
allow always if destination port=53 & protocol = udp
allow always if destination port=25 & protocol = tcp/udp
allow always if destination port=110 & protocol = tcp/udp
```

this allows the people in the network to browse and retrieve their emails from the email server and send emails (the email server is external). maybe i have to allow ports like 3128, 8080 etc. but this kinda works.

i couldnt really find any info on what i should allow and disallow, just looked up a port list of protocols and allowed them via destined ports.

my question is,

- #1: is this the correct way to specify filters? (i.e. via destination ports)
- #2: my theory is, if a trojan was running on the machines, the traffic would have to goto port 80,443,53,25,110, so the attacker will have to have these ports open / use a box that had these ports open. correct?
- #3: should i allow anything else?
- #4: can anyone recommend a good syslog program for windows where i can see the traffic by IP? (long term)