

1 Goals

- Reinforce your computer interface configuration skills
- Understand Industry-grade firewall practices
- Learn how to set up useful firewall rules

2 Firewall Policy

The heart of a secure network system is a very specific security policy. The network that you will build will adhere to the following policies:

1. In and Out of the Company (Internet to/from DMZ)
 - (a) TELNET (TCP/23) is **never** allowed in or out of the company
 - (b) FTP control connections (TCP/21) are only allowed to/from the Mac OS machines.
 - (c) All other IP packets are allowed
2. From the internal network to the DMZ (Secure to/from DMZ)
 - (a) Secure Shell (TCP/22) connections are always allowed either in or out
 - (b) All outgoing (established) TCP connections are allowed
 - (c) All TCP connections to/from the DMZ are allowed
 - (d) All other IP packets are to be discarded

3 Per-Table Configuration

The exact details of the lab will depend on which table you're working at. This table shows the details that you will need to know for your particular table:

Item	Table 1	Table 2	Table 3	Table 4
FW1/DMZ	Buell 0/0	Buell 0/1	Buell 0/2	Buell 0/3
FW2/DMZ	Harley 0/0	Harley 0/2	Davidson 0/0	Davidson 0/2
FW2/Secure	Harley 0/1	Harley 0/3	Davidson 0/1	Davidson 0/3
DMZ Net	132.235.201.192/29	132.235.201.208/29	132.235.201.224/29	132.235.201.240/29
Secure Net	132.235.201.200/29	132.235.201.216/29	132.235.201.232/29	132.235.201.248/29
Access List IDs	110-119	120-129	130-139	140-149
Policy Route Name	pralpha	prbeta	prgamma	prdelta

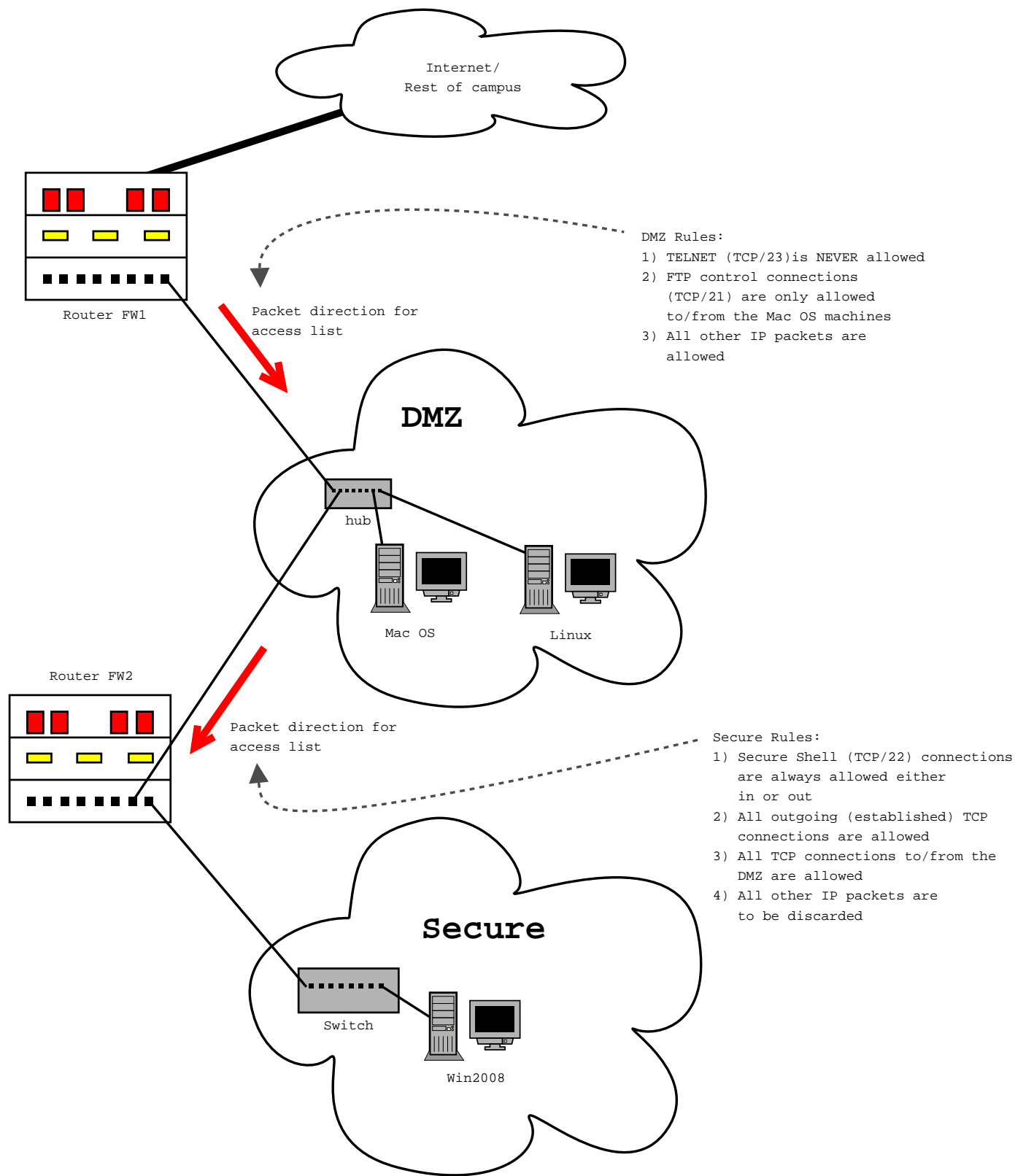
4 Useful Resources

Cisco website on firewall commands

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/>

Section on policy routing

[as above ...].../ios111/mods/4mod/4rbook/4riproun.htm#41157



5 Step-by-Step Instructions

1. Lab setup
 - Buell has a default route to the outside world
 - The FDDI ring is down the entire lab
2. Set up all 3 router interfaces (FW1/DMZ,FW2/DMZ,FW2/Secure). Use appropriate addresses from the ranges on the first page.
3. Patch in the hubs and switches for the 2 networks that you'll set up.
4. Install a route on Buell so that it can reach your Secure network via the link across the hub to FW2. Disable the admin interface.
5. Configure all three computers with appropriate IP addresses, masks, and routes. You should just need a default route for each of the computers.
 - DMZ machines should route through FW1
 - SECURE machines should route through FW2

Use ping and traceroute on each computer to verify your path to:

- The Internet (except from Win2008)
 - The DMZ computers
 - The Secure computers
 - FW1 interface on Buell
 - Buell's 132.235.201.40 address
6. Install a *policy route* on the FW2/Secure interface so that the *next-hop* for all packets **from** your Secure network is through the DMZ. This step is required because 2 tables are using that router and there's no other way to differentiate the routing tables.
 - (a) Create an access list that matches all packets from your Secure network **except those that are going to the DMZ**
 - (b) Go into interface-config mode for your FW2/Secure interface
 - (c) Type `ip policy route-map PRNAME` (see page 1 for name)
 - (d) Exit from interface-config mode
 - (e) Type

```
route-map PRNAME
match ip address YYY
set ip next-hop ZZZ.ZZZ.ZZZ.ZZZ
```

where PRNAME is the route-map name above, YYY is the access list number, and ZZZ.ZZZ.ZZZ.ZZZ is the IP address of Router FW1/DMZ

7. Quick check to verify connectivity and correct paths:
 - Buell to Win2008
 - Win2008 to 132.235.64.1
 - **Graduate students only/extra credit for undergrads** Do a packet capture on your Win2008 box of a ftp file transfer from 132.235.201.114 to your Win2008 system using "get file" with a filename "testfile". This capture is to be used in answering the question in step 15 on the lab report.

8. On the back page is a list of things that should and shouldn't work. Before we install the firewall rules, verify that all of those tests succeed (even if the sheet says that they should fail later).
9. Set up an access list (see first page for the appropriate number) on your FW1 router. It should implement the "Internet to/from DMZ" policy on the first page. Because of the way the policy is specified, we'll just need to control the "out" direction: packets going from FW1 to DMZ.
10. Attach the FW1 access lists to the FW1 to DMZ interface (in mode **out**).
11. Verify all of the tests on the back page for the DMZ network.
12. Set up an access list (see first page for the appropriate number) on your FW2 router. It should implement the "Secure to/from DMZ" on the first page. In this case, we'll just control the "in" direction of packets traveling from the DMZ to FW2.
13. Attach the FW2 access list to the DMZ to FW2 interface (in mode **in**).
14. Verify all of the tests on the back page for both the DMZ and the SECURE networks.
15. **Graduate Only/Undergrad extra credit** Attempt to do a ftp file transfer from your Win2008 box on the secure network to 132.235.201.114 like you successfully did in a previous step. Research the ftp file transfer protocol and explain why ftp does not work from your secure network with your firewall. Propose how to update your access list to permit these transfers. Research ftp passive mode connections and explain why they would have work without changes. Compare the security of these two types of ftp transfers.

Lab Report

General Guidelines

Follow all of the same guidelines for submission as in the previous labs...

Include in your report

- Patch panel chart
- Ping/traceroute matrix from below with instructor's signature indicating that you got everything working (or telling what didn't work)
- Network layout picture with details added *in red*:
 - Show the address/mask for all 3 computers
 - Show the address/mask/interface for all router interfaces that you used

Include a copy of the routing table for FW1, FW2, and your 3 computers

Include a copy of all access lists and route-map entries

Research and answer the question from step 15 of the lab.

Correctness check

If you have followed the instructions, your DMZ network should behave as follows:

	Task	Instructor Check
1	your Mac OS machine can FTP to 132.235.201.114	
2	your Linux machine cannot FTP to 132.235.201.114	
3	from 132.235.201.114, you can FTP to Mac OS	
4	from 132.235.201.114, you cannot FTP to Linux	
5	TELNET fails from Mac OS/Linux to 132.235.201.114	
6	ping works from Mac OS/Linux to 132.235.67.21	
7	ping works from Mac OS/Linux to 128.10.2.1	

If you have followed the instructions, your SECURE network should behave as follows:

	Task	Instructor Check
1	Win2008 can ssh to 132.235.8.44 (oak)	
2	Win2008 can TELNET to your linux machine	
3	Ping fails from Win2008 (to everywhere; try 132.235.64.1)	
4	WWW to 132.235.67.20 from Win2008 works	
5	WWW to Win2008 from Mac OS works	
6	WWW to Win2008 from 132.235.201.114 fails	

Be sure that your lab instructor has initialed that all of the above tests work before leaving the lab. Note: to get full credit, all tests must work all at the same time (without changing any configuration during the test).

Prelab: Print 4 copies of page 2 containing the network diagram and fill out the diagram with interface names and source and destination networks/host IPs and masks for both “arrows” for each of the 4 lab tables. Bring all four diagrams and a print out of a draft of your access rules for Buell (which you may want to bring to class on your USB flash to save typing).

Outside Work

Find documentation on the TCP protocol, in particular the 3-way handshake and the meaning of the SYN/FIN/ACK bits. Explain exactly how the *established* keyword in the access-list specification works. Good references are Comer Volume I, Stevens Volume I, RFC 793.

ICMP

Some sites choose to disable ICMP either partially or fully. Explain how disabling ICMP would make it more difficult to use the ping and traceroute utilities that we rely on in lab (in detail).