CS 482: Selected Topics in Information Security
Spring 2005 – Section 1

Module 4 Assignment: Shorewall

I. Firewall

One way to test a firewall for durability and vulnerabilities is to make sure it denies or allows access to certain resources on different computers from different external or internal sources.

In our configuration of the Shorewall firewall we setup the basic policy for the network and we defined rules (or exceptions to the policy).

Deliverable

For each of the following test you are to submit the policy and rules file, the results of the test, how your team implemented the requirement, and any problems that you encountered during the configuration. State whether or not your team had to implement the rule unidirectional or bidirectional, in order words were you able to test the rule going one way or did you have to insert the rules that went in the other direction as well.

Note: Pinging from the computer that you have denied or allowed access to or from is not a sufficient test, you must also show if other machines can access the same resource.

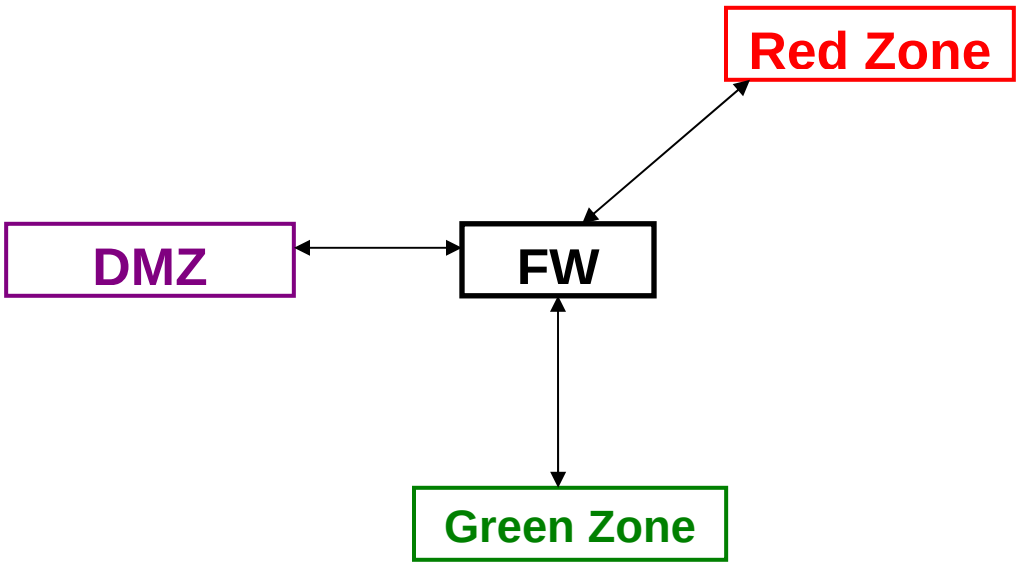

Figure 1: Simplified diagram of the business network

Perform the following test within your team's business network. The image indicates the direction of the rule.

Unidirectional rule: ➔

Bidirectional rule: ←➔

Deny/Allow Access To/From Anywhere

Test 1: Disable the firewall and demonstrate that all the computers can ping each other.

Test 2: Now, enable the firewall and show that access is denied of the traffic has to be routed through the Linux-FW machine.

Access Control with Zones Using Ping Request

Test 1: Deny access to the Green Zone and the DMZ from the Red Zone.

RZ  **GZ** **RZ**  **DMZ**

Test 2: Deny access from the Green Zone to the DMZ but allow access to the FW and the Red Zone.

GZ  **DMZ** **GZ**  **RZ**

Test 3: Deny access from the DMZ to the FW.

DMZ  **FW**

Test 4: Allow access from the Green Zone to the DMZ; disable access to the Red Zone.

GZ  **DMZ** **GZ**  **RZ**

Test 5: Allow access from the DMZ to Red Zone only.

DMZ  **RZ** **DMZ**  **GZ**

Test 6: Allow access from Red Zone to DMZ only.

RZ  **DMZ** **RZ**  **GZ**

Test 7: Allow access from DMZ to everywhere but deny access from everywhere to DMZ.

DMZ  **ALL** **ALL**  **DMZ**

Test 8: Allow access from the DMZ and Green Zone only to anywhere.

DMZ  **ALL** **GZ**  **ALL**

ALL  **DMZ** **ALL**  **GZ**

Access Control with IP Addresses Using ICMP Ping Request

Test 1: Deny access to the Green Zone, FW, and DMZ zones from WinXP-R1.

Test 2: Deny access to 192.168.[n].128/27 from DMZ.

Test 3: Deny access to 192.168.[n].32/27 from Win2003-NET.

Test 4: Allow access from Linux-C1 to 192.168.[n].128/27 and 192.168.[n].96/27 only.

II. Shorewall Accounting

Shorewall provides a mechanism for keeping track of the number of packets entering or leaving an interface, the source, destination, and protocol of the packets. Your task is to implement the accounting feature of Shorewall.

You are to include in your deliverable:

- The files used to implement this feature
- The result of issuing the **show accounting** command with the different chains implemented. You are required to have the following chains: **web, inside, outside, firewall**. You may decide to implement additional chains as you see fit.

  Chain Definitions

  Web: traffic entering or leaving the Linux-WEB on eth0 on port 80

  Inside: traffic entering or leaving eth1 on any port

  Outside: traffic entering or leaving eth2 on any port

  Firewall: traffic destined specifically for the firewall on any port.

III. Shorewall Logging

By default Shorewall's traffic is logged with **syslogd**. We would like to log all Shorewall traffic to another location. Download, install, and implement **ulogd** as the logging facility to be used for Shorewall's traffic.

Your deliverable must include the following:

- Instruction on how your installed ulogd
- The segment of the ulogd config file that you modified.
- The first page of the text file containing the log generated by ulogd.