# Tests

| **Test #** | **Test procedure / description** | **Expected Outcome** | **Actual Outcome & Remarks** | **Pass / Fail** |
| --- | --- | --- | --- | --- |
| 1 | Smoke test the firewall:   1. apply the firewall:    * sudo ./firewall.sh 2. run the test script:    * sudo ./test.sh [peer ip address] 3. run the test script from the peer computer:    * sudo ./test.sh [firewall ip address] 4. list firewall rules:    * sudo iptables -L -v -n | * During step 1, nothing is printed. * During step 2, all tests except for those under the "### testing firewall rules of $address ###" heading should pass. * During step 3, all tests under the "### testing firewall rules of $address ###" heading should pass * During step 4, all firewall rules are listed. most rules have a non-zero packet count. all user chains have a non-zero packet count. | As expected | Pass |
| 2 | Test DNS, HTTP and HTTPS:   1. apply the firewall:    * sudo ./ firewall.sh 2. open a web browser and go to a website that uses the HTTP protocol, then go to another site that uses a HTTPS protocol. 3. list firewall rules: | When listing firewall rules:   * all DNS rules associated with UDP protocols should have non-zero packet counts. * WWW\_CLIENT rules associated with the WAN interface should have non-zero packet counts. * the WWW\_CLNT and DNS chains should have non-zero packet counts. | As expected | Pass |
| 3 | Test SSH to peer from firewall:   1. apply the firewall:    * sudo ./ firewall.sh 2. set up an SSH server on a peer. 3. SSH to the peer from the firewall. 4. list firewall rules. | When SSH-ing to the peer from the firewall:   * A connection should be established; the program should not hang.   When listing firewall rules:   * SSH\_CLNT rules associated with the WAN interface should have non-zero packet counts. * SSH\_CLNT chain should have a non-zero packet count. | As expected | Pass |
| 4 | Test HTTP into the firewall from peer:   1. apply the firewall:    * sudo ./ firewall.sh 2. set up a web server on the firewall. 3. connect to the web server from peer. 4. list firewall rules. | When connecting to the firewall from a peer with a web browser:   * A connection should be established; the web browser should not hang. it should display a web page.   When listing firewall rules:   * WWW\_SVR rules associated with the WAN interface should have non-zero packet counts. * WWW\_ SVR chain should have a non-zero packet count. | As expected | Pass |
| 5 | Test SSH into the firewall from peer:   1. apply the firewall:    * sudo ./ firewall.sh 2. set up an SSH server on the firewall. 3. connect to the SSH server from peer. 4. list firewall rules. | When SSH-ing to the firewall from the peer:   * A connection should be established; the program should not hang.   When listing firewall rules:   * SSH\_SVR rules associated with the WAN interface should have non-zero packet counts. * SSH\_ SVR chain should have a non-zero packet count. | As expected | Pass |
| 6 | Test HTTP into firewall from firewall:   1. apply the firewall:    * sudo ./ firewall.sh 2. set up a web server on the firewall. 3. connect to the web server from the firewall. 4. list firewall rules. | When connecting to the firewall from a peer with a web browser:   * A connection should be established; the web browser should not hang. it should display a web page.   When listing firewall rules:   * WWW\_CLNT and WWW\_SVR rules associated with the loopback interface should have non-zero packet counts. * WWW\_CLNT and WWW\_ SVR chains should have a non-zero packet count. | As expected | Pass |
| 7 | Test SSH into firewall from firewall:   1. apply the firewall:    * sudo ./ firewall.sh 2. set up an SSH server on the firewall. 3. connect to the SSH server from the firewall. 4. list firewall rules. | When connecting to the firewall from a peer with a web browser:   * A connection should be established; the web browser should not hang. it should display a web page.   When listing firewall rules:   * SSH\_CLNT and SSH\_SVR rules associated with the loopback interface should have non-zero packet counts. * SSH\_CLNT and SSH\_SVR chains should have a non-zero packet count. | As expected | Pass |

## Screenshots

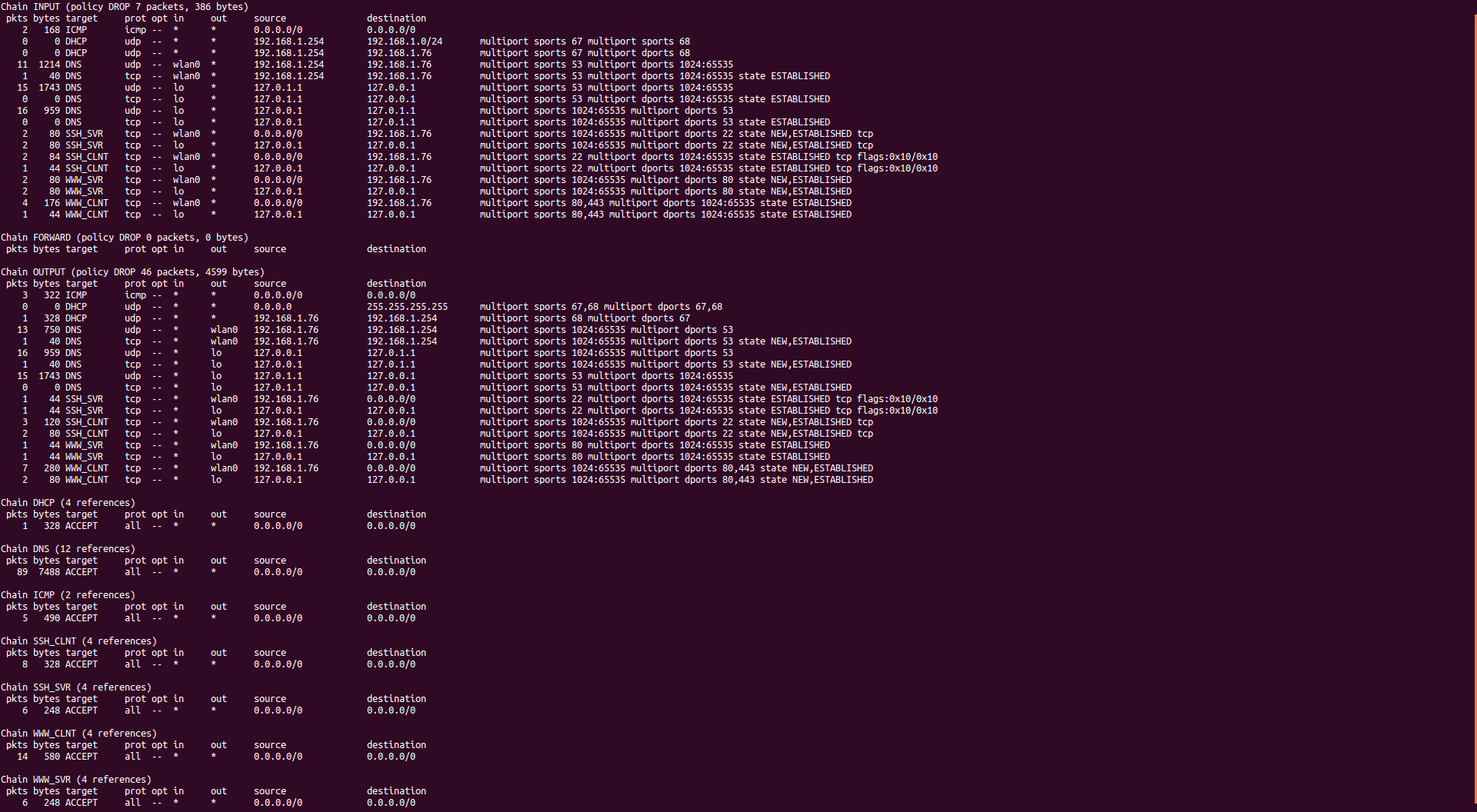


Figure test 1, all user chains have non-zero values, and most firewall rules also have non-zero values

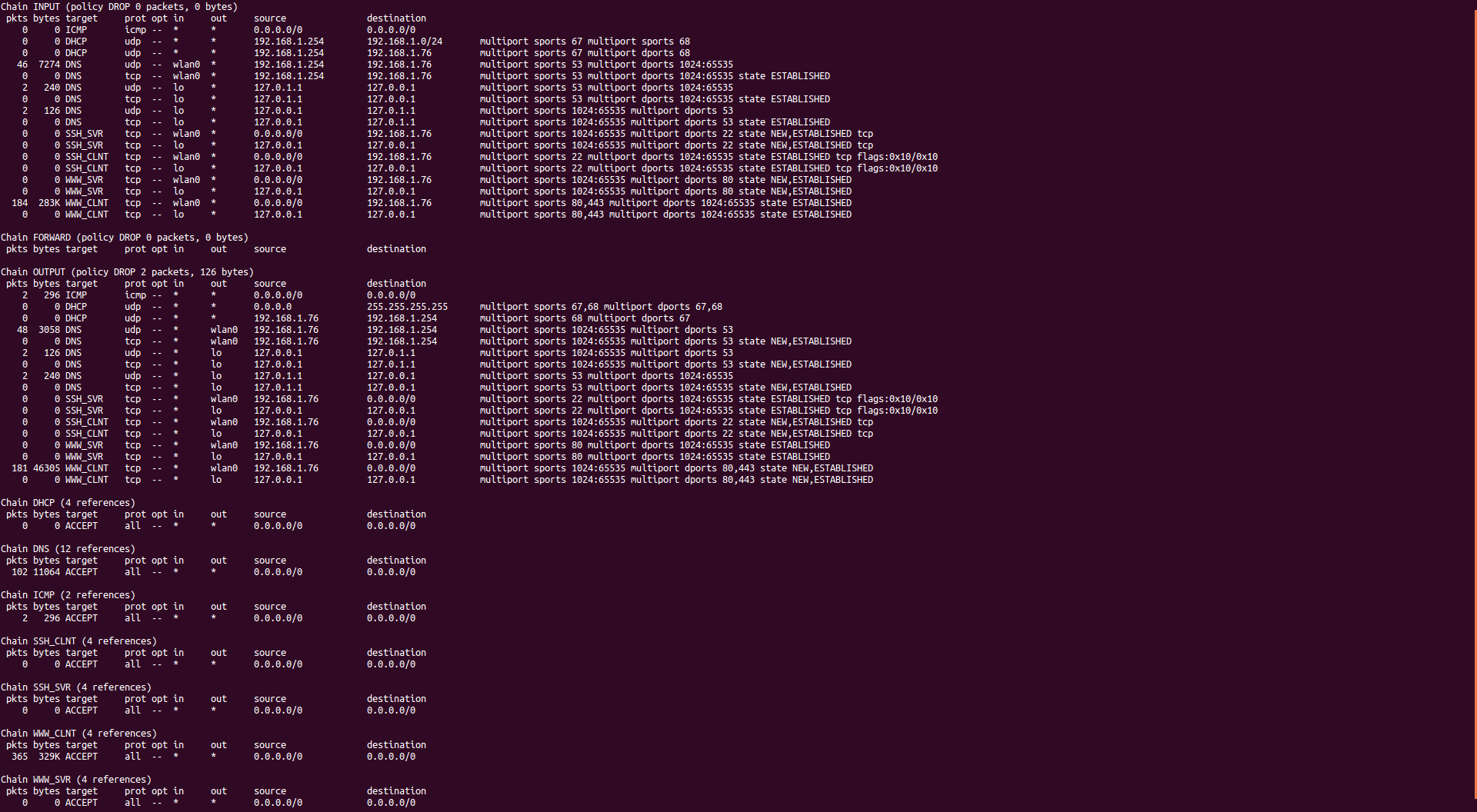


Figure test 2, all DNS rules have non-zero packet count, and www\_clnt rules associated with wlan0 interface has a non-zero packet count

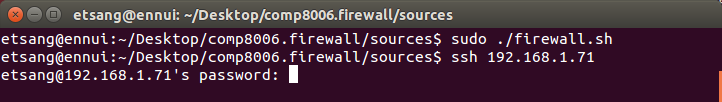


Figure test 3, ssh connection established successfully

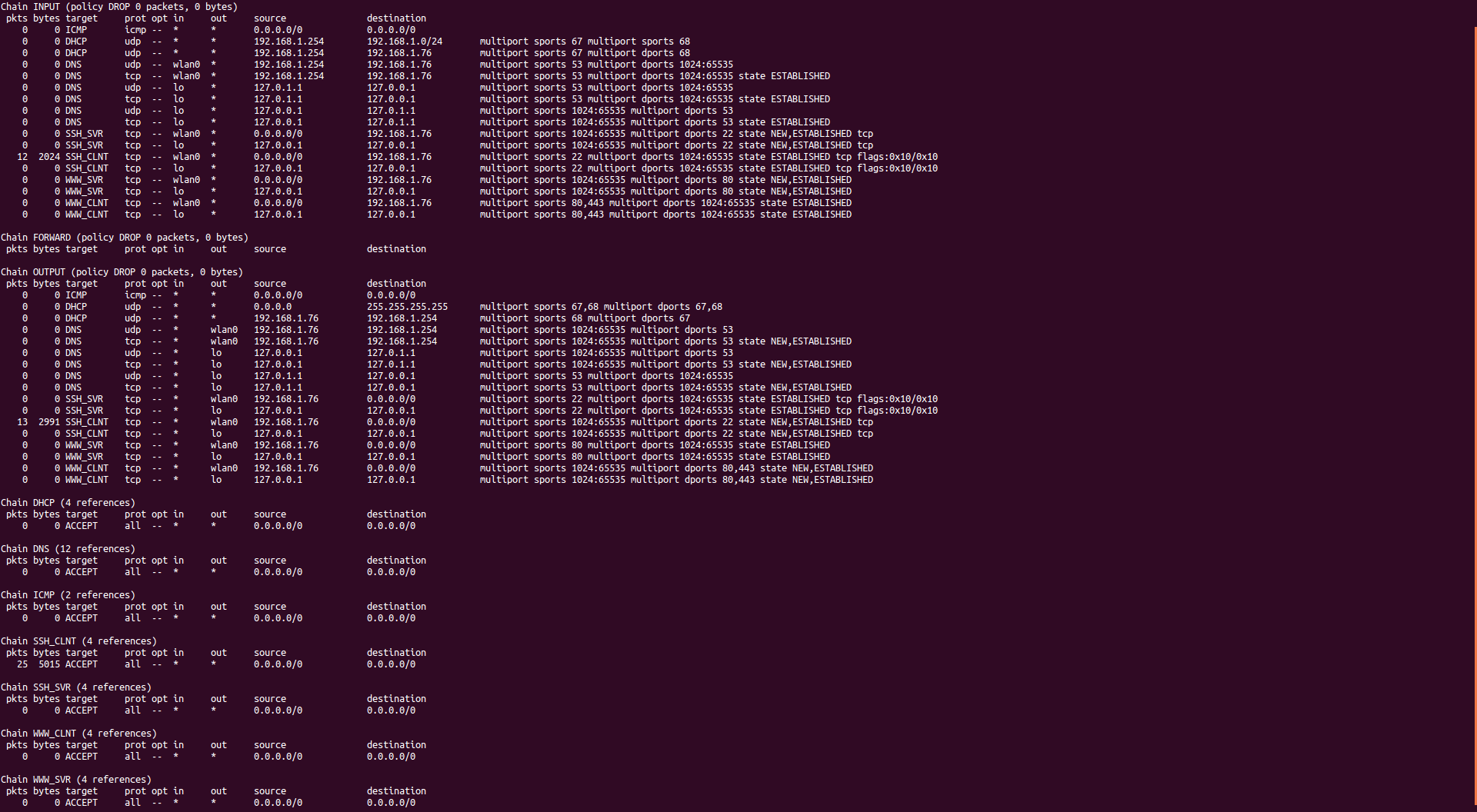


Figure test 3, all SSH\_CLNT rules associated with wlan0 interface as well as the SSH\_CLNT chain have non-zero packet counts

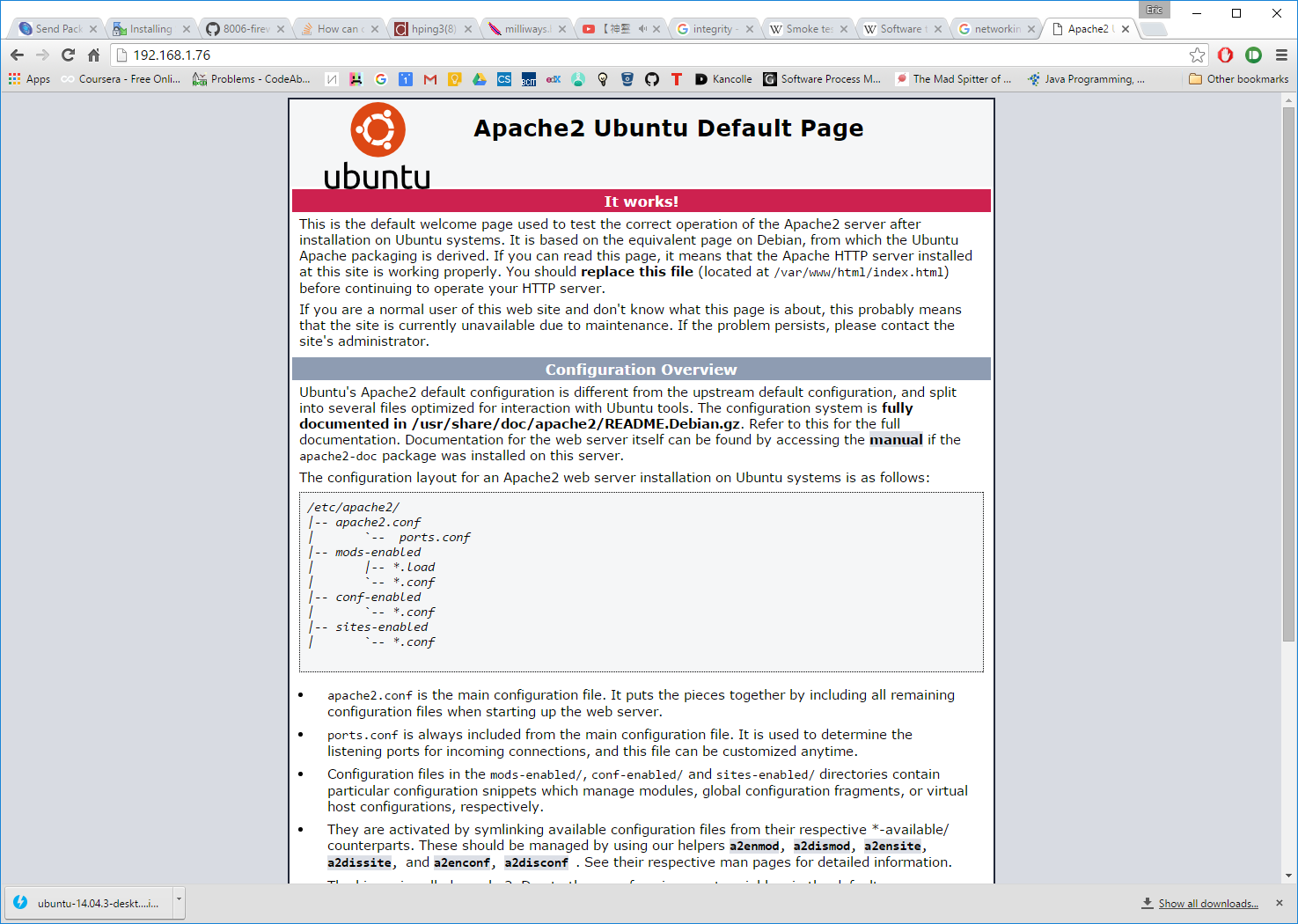


Figure test 4, browser can connect to the firewall, and it is displaying a web page delivered by the web server on the firewall

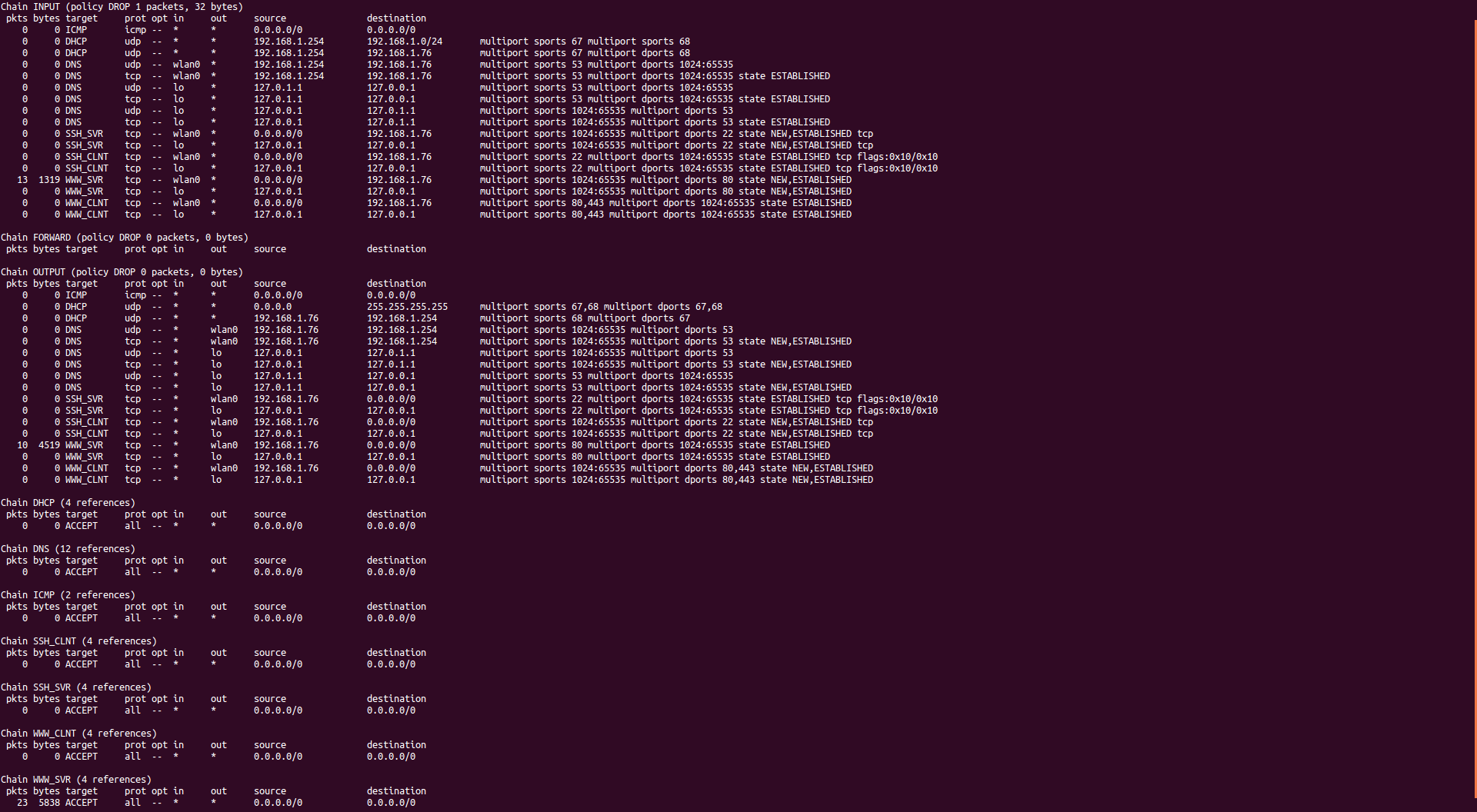


Figure test 4, WWW\_SVR rules associated with wlan0 as well as the WWW\_SVR chain display non-zero packet counts

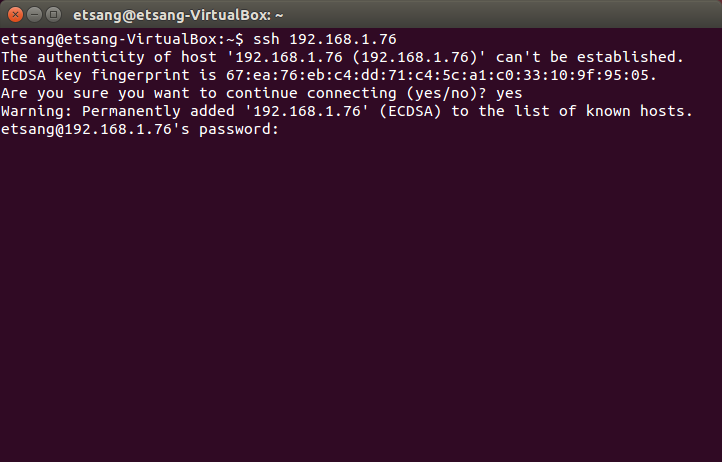


Figure test 5, SSH into the firewall from a peer on the same network. The SSH client has established a connection with the firewall.

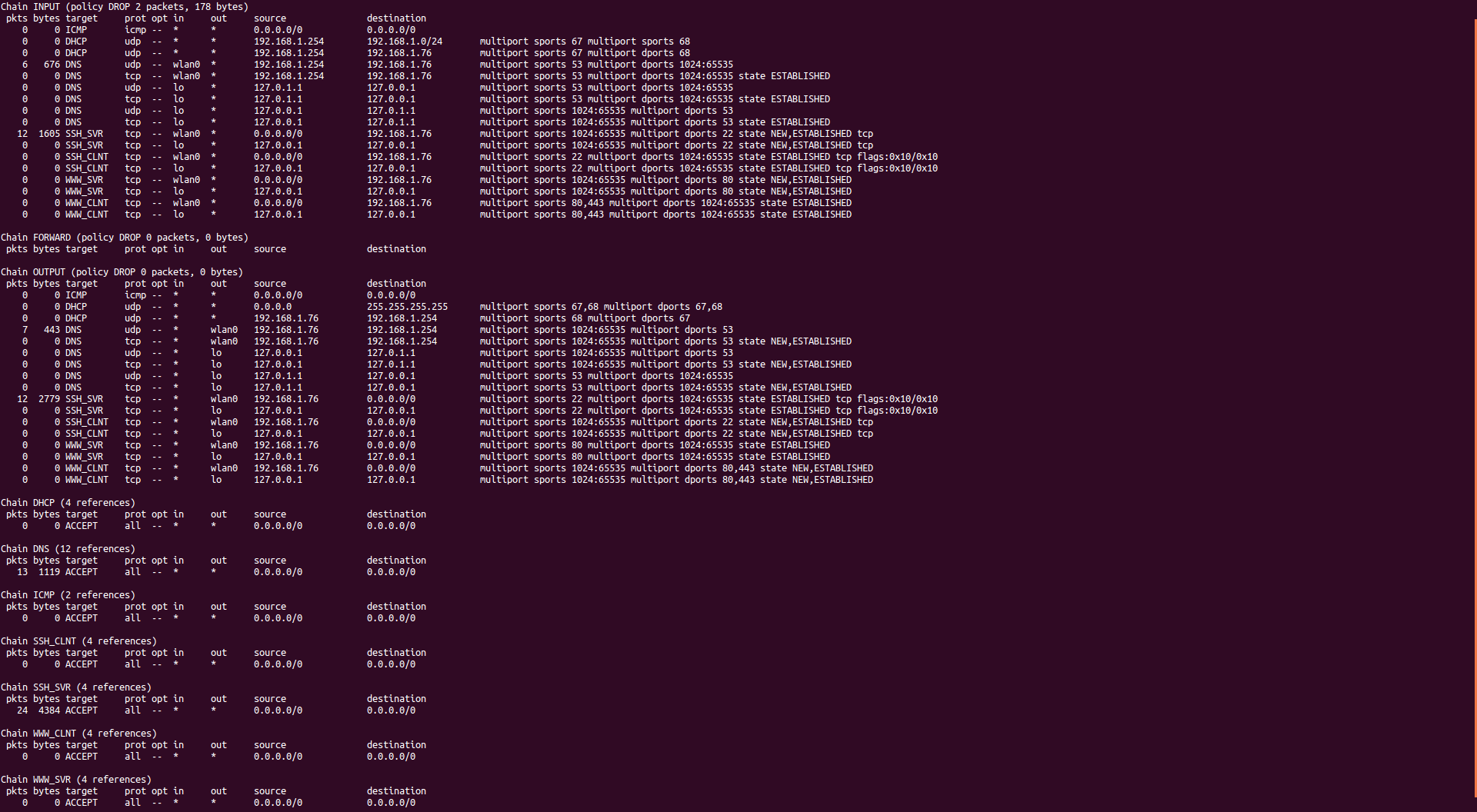


Figure test 5, SSH\_SVR rules associated with wlan0 and SSH\_SVR chain have non-zero packet counts

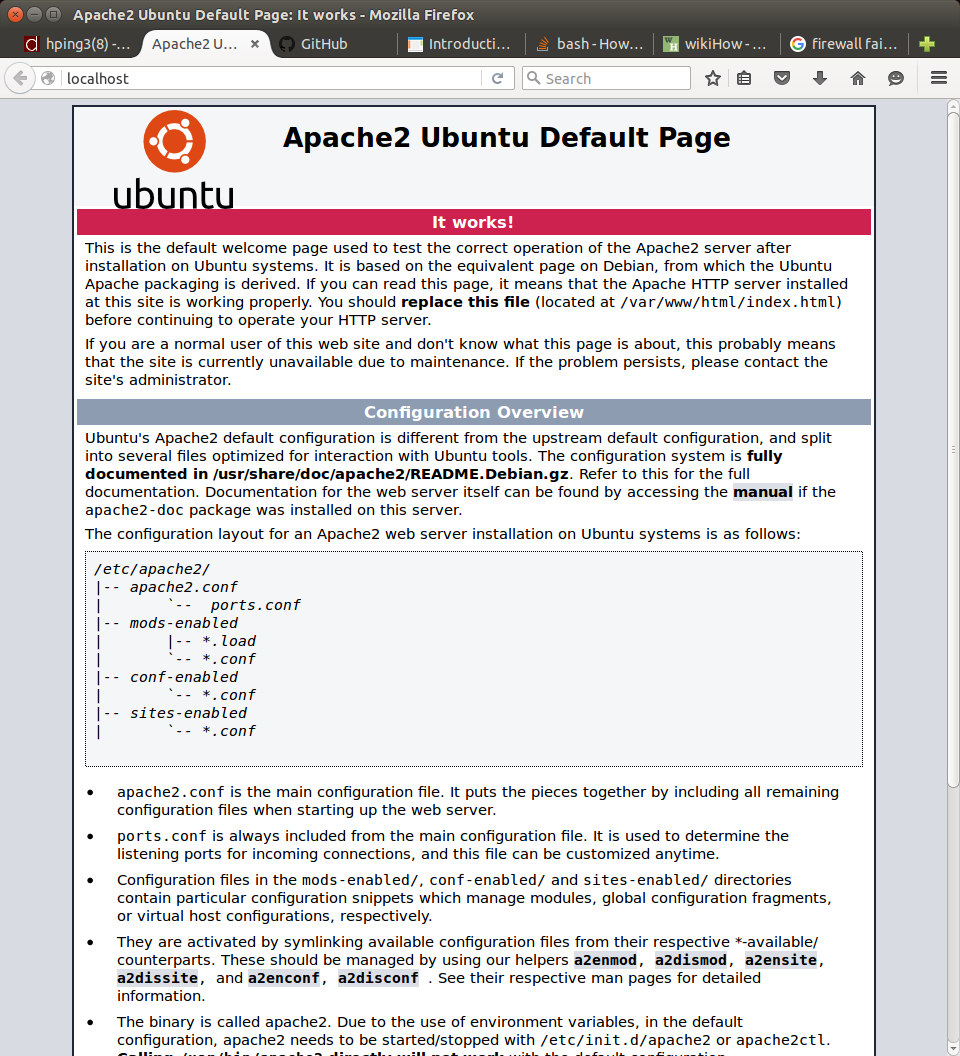


Figure test 6, web browser on the firewall is able to connect to localhost on the firewall

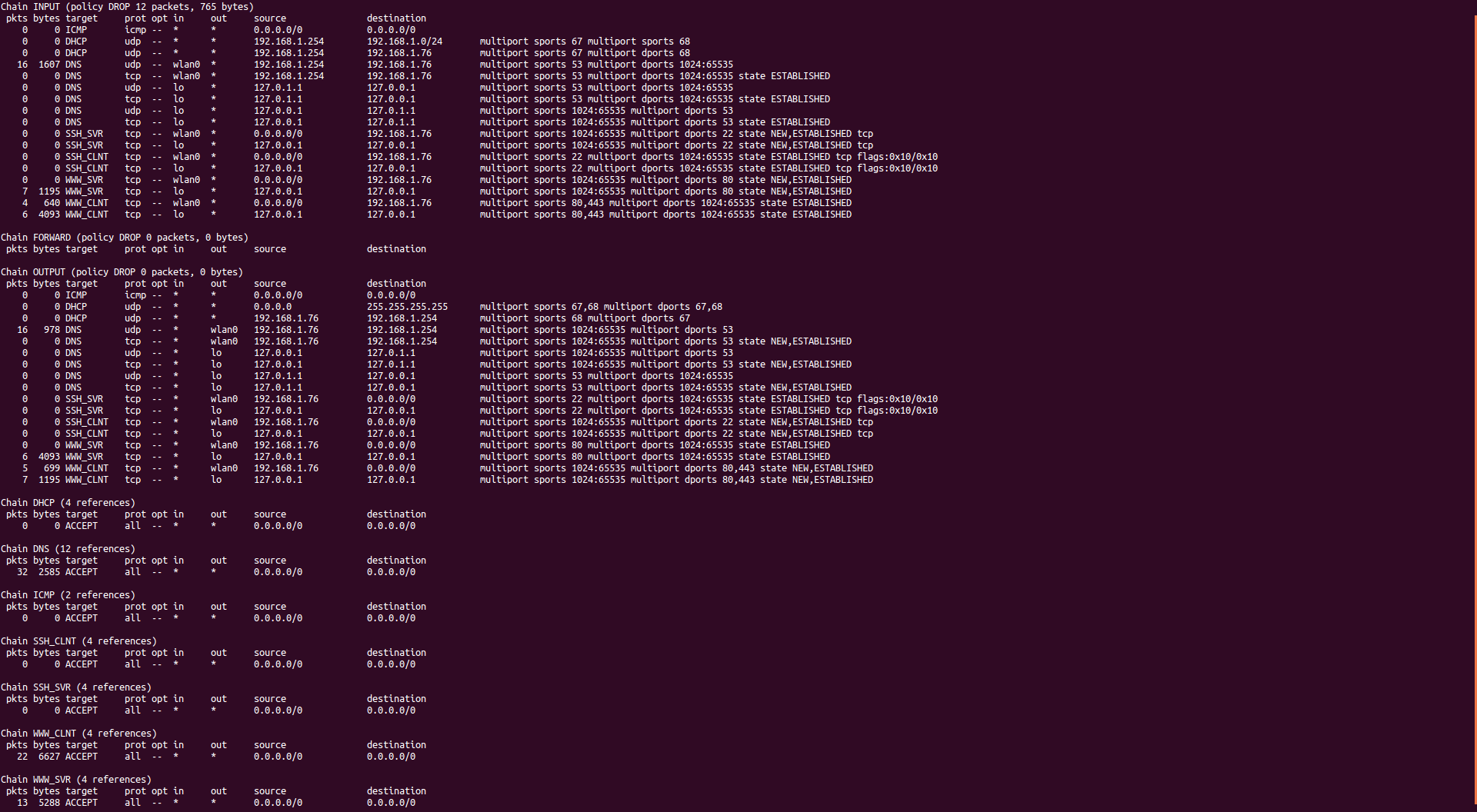


Figure test 6, the WWW\_CLNT and WWW\_SVR rules associated with the lo interface, and chains have non-zero packet counts

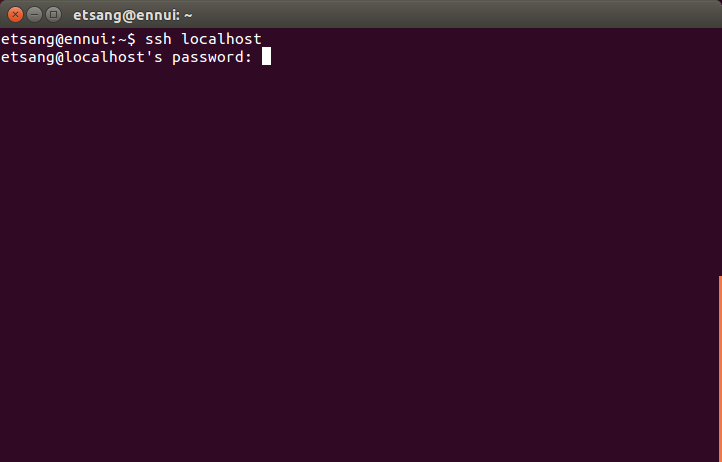


Figure test 7, SSH on the firewall into the firewall is successful as the SSH client is able to connect to the SSH server

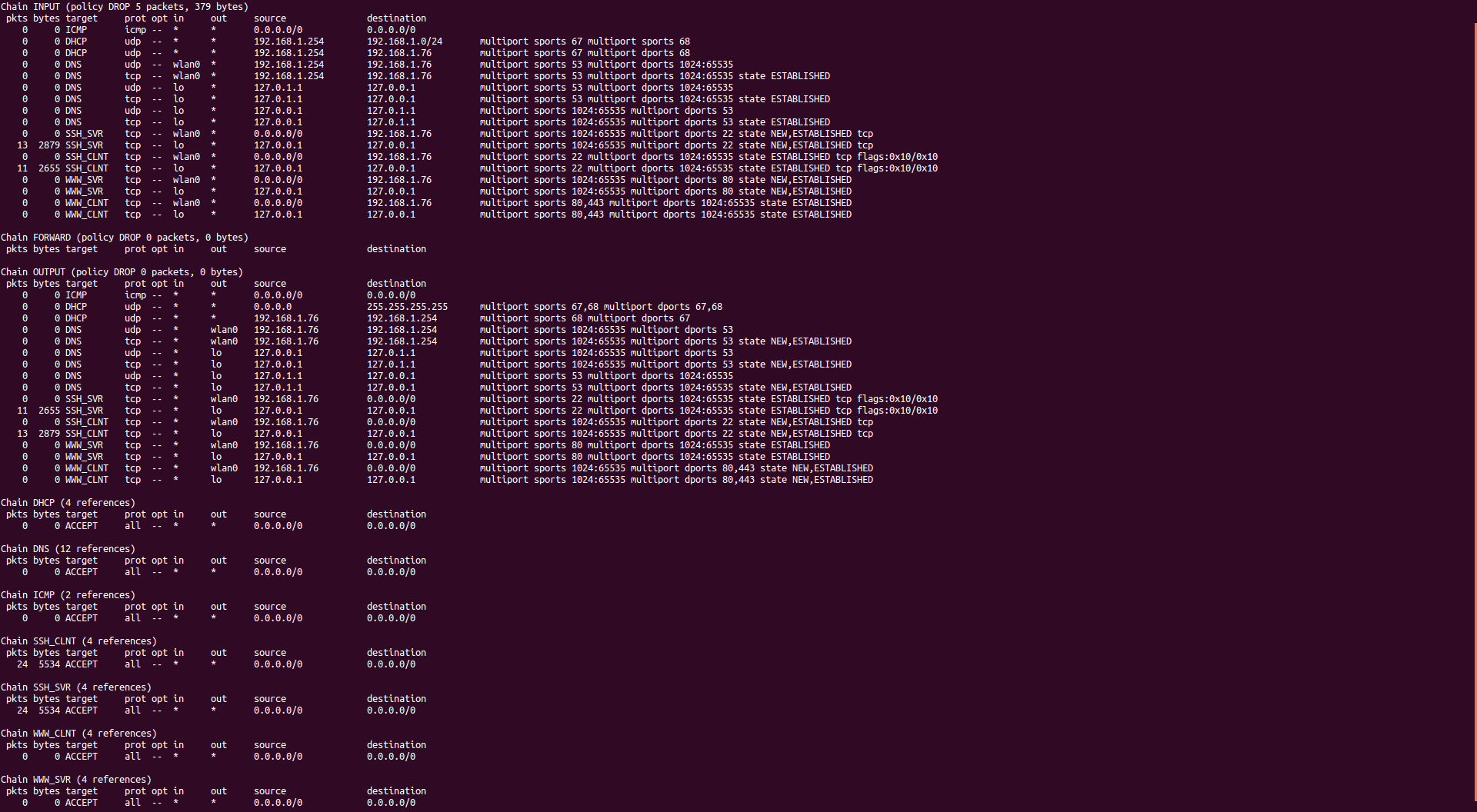


Figure test 7, SSH\_SVR and SSH\_CLNT firewall rules associated with the lo interface and chains have non-zero packet counts