COMP 8006 Set 5D

Assignment 2: Building A Personal Linux Firewall

29 Jan 2015

Thilina Ratnayake

A00802338

Table Of Contents:

<u>Page</u>	<u>Item</u>
3	Objective
4	Program Structure
4	Program Components
5	Firewall Design
5	Psuedo Code
6	Execution Instructions
7	Tests
8	Data & Results

Objective: To implement and test a simple personal Linux Firewall.

Program Structure:

```
[root@localhost 8006-Assignment-1]# tree
    Captures

    Newer\ Old\ Caps

           Test\ 1\ DHCP.pcapng
           Test\ 2\ DNS.pcapng

    Test\ 3A\ Inbound\ SSH.pcapng

    Test\ 3B\ Inbound\ SSH.pcapng

    Test\ 4A\ Outbound\ HTTP.pcapng

          - Test\ 4B\ Inbound\ HTTP.pcapng
        Old\ Caps
           - Test\ 01\ DHCP.pcapng
           - Test\ 02\ DNS.pcapng
          - Test\ 03\ SSH.pcapng
       Test1.pcapng
       Test2.pcapng
       Test3A.pcapng
       Test3B:\ Allow\ inbound\ SSH\ to\ a\ host.pcapng
       Test4A:\ Allow\ inbound\ HTTP.pcapng
       Test4A.pcapna
       Test4B.pcapng
       Test4C.pcapng
       Test4D.pcapng
   Firewall.sh
   FirewallTestNew

    FirewallTestNew.sh

  - FirewallTest.sh

    ResetFirewall.sh

    TEST.pcapng
```

3 directories, 24 files

Program Components:

- 1. **Firewall.sh** BASH Script that adds rules to IPtables
- 2. **ResetFirewall.sh** BASH Script that deletes all rules from IPtables and restores computer to lab default settings (e.g. All chains ALLOW)
- **3. FirewallTest.sh** BASH Script that automates the tests by performing HPINGS and opening wireshark windows at appropriate intervals.

Firewall Design:

- 1. Default policy of dropping everything unless stated other was invoked.
- 2. 12 chains were made, all representing an IN or OUT rule. The decision to use specific IN/OUT chains (e.g. SSH IN and SSH OUT versus SSHTRAFFIC) was made because it is much easier to view statistics at a glance and spot issues. (e.g. looking at SSHTRAFFIC during a DOS attack and not knowing where the problem lay)
- 3. More specific rules (like dropping all traffic going to or coming from a reserved port like 0) were put earlier in the firewall than later. This is because as a defense mechanism, we want to neutralize serious threats first and let our "catch-all" rules deal with all that get through.

Psuedo Code (Firewall.sh):

- 1. Make all the chains
- 2. Route the chains to appropriate functions (ACCEPT or DROP)
- 3. Create the rules and route to chain
 - a. Add the really specific rules first (e.g. Drop ALL /FROM port 0)
 - b. Broader rules near bottom.
- 4. RESET THE FIREWALL/IPTABLES WHEN SCRIPT IS FINISHED.

<u>Psuedo Code (FirewallTest.sh):</u>

- 1. Prompt user for all necessary info (e.g. Remote workstation ip, ssh user, password)
- 2. Test DHCP connectivity
 - a. DHCP release
 - b. DHCP renew
 - c. Check Wireshark
 - d. Check that mchine has IP
- 3. Test DNS connectivity
 - a. NSlookup www.google.com
 - b. Check wireshark
- 4. Test SSH connectivity
 - a. Check outbound by SSH'ing into remote terminal
 - b. Check wireshark
 - c. Check inbound by first SSH'ing into remote and sending HPing's on SSH port to local.
- 5. Test dropping packet 0
 - a. HPing remote with src port 0 (check for failure)
 - b. HPing remote with dest port 0 (check for failure)
 - c. Try the same from remote to local
 - d. Try from NON port 0's (check for success)
 - e. Check wireshark captures
- 6. Test Denied HTTP
 - a. SSH into remote
 - b. Try to access local with port in range 1-1024 (check for failure)
 - c. Check wireshark
 - d. Check with port OUTSIDE of range (check for success)

e. Test HTTP

- i. Outgoing: Check any normal website (hping google.com)
- ii. Outgoing: SSH into remote, start Apache, hping
- iii. Incoming: Check that HPing's get returned
- iv. Incoming: Start apache, try hpingining from remote
- v. Check wrieshark

Execution Instructions:

Run sh.FirewallTest.sh

Tests:

			Source	Destination		Wireshark	Capture		
#	Rule	Direction	Port	Port	Test	Screenshot	Name	Expected	Result
<u> </u>	Permit	Direction	1 011		1.631	301001131100	Ttaine	Expedica	As
1	DHCP	Out		68	dhclient -r	Fig 1	Test1.pcapng	Passed	expected
	Permit				dhclient	6 =			As
2	DHCP	In	68		2000000	Fig 1	Test1.pcapng	Passed	expected
							, , ,		As
3	Permit DNS	Out		53		Fig 2	Test2.pcapng	Passed	expected
					nslookup www.google.com		у составания		As
4	Permit DNS	In	53			Fig 2	Test2.pcapng	Passed	expected
	Permit SSH								
	connections						Test		As
5	Out	Out		22	SSH into remote machine	Fig 3.1	3A.pcapng	Passed	expected
	Permit SSH						Test		As
6	replies In	In		22		Fig 3.1	3A.pcapng	Passed	expected
	Permit SSH								
	connections				Let remote machine SSH into		Test		As
7	In	In	22		local	Fig 3.2	3B.pcapng	Passed	expected
	Permit SSH				local		Test		As
8	replies Out	Out	22			Fig 3.2	3B.pcapng	Passed	expected
	Drop all								
	incoming								
	traffic from				Remote machine:		Test		As
9	port 0	IN	0		hping3 LOCAL -S -s 0 -p 80	Fig 4.1	4A.pcapng	Dropped	expected
	Drop all								
	outgoing								
	traffic to			_	Local machine:				As
11	port 0	Out		0	hping3 REMOTE -S -s 90 -p 0	Fig 4.2	-	Dropped	expected
	Drop								
	inbound				Remote machine:		Test	As	
	traffic to	IN	1-1024	80	hping3 LOCAL -S -s 1019 -p 80	Fig 5.1	5A.pcapng	expected	

port 80 from select ports								
Allow outbound HTTP	Out		80	Local machine: hping3 www.tratnayake.me -s 600 -p 80	Fig 6.1	Test 6A.pcapng	As expected	
Allow inbound HTTP replies	ZI	80		Remote machine: hping3 LOCAL -S -s 80 -p 650	Fig 6.1	Test 6A.pcapng	As expected	
Allow inbound HTTP connections (to Apache)	IN		80	Remote machine: hping3 LOCAL -S -s 2000 -p 80	Fig 6.2	Test 6A.pcapng	As expected	
Allow outbound HTTP replies (from Apache)	Out	80	80	Local machine: hping3 Remote -S -s 80 -p 2000	Fig 6.2	Test 6A.pcapng	As expected	

<u>Screenshots</u>

No.	Time	Source	Destination	Protoco	Lengtl Info		Source Por	Destination Por New Column	
	5 1.162605000		255.255.255.255	DHCP	342 DHCP Discover	r - Transaction ID 0x852da013	bootpc	bootps DHCP	
	9 2.164009000	192.168.57.254	192.168.57.138	DHCP	342 DHCP Offer	- Transaction ID 0x852da013	bootps	bootpc DHCP	
1	10 2.166047000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request	- Transaction ID 0x852da013	bootpc	bootps DHCP	
1	11 2.166763000	192.168.57.254	192.168.57.138	DHCP	342 DHCP ACK	- Transaction ID 0x852da013	bootps	bootpc DHCP	

Fig1 – Evidence of DHCP

No.	Time	Source	Destination	Protoco	Lengtl Info	Source Por	Destination Por
	1 0.000000000	192.168.57.138	192.168.57.2	DNS	76 Standard query 0x4c46 A www.miniclip.com	58476	domain
	2 0.039148000	192.168.57.2	192.168.57.138	DNS	204 Standard query response 0x4c46 A 54.149.25.131 A	54. domain	58476

Fig 2: Evidence of DNS

No.	Time	Source	Destination	Protoco	Lengtl Info	Source Por	Destination
),	1 0.000000000	fe80::20c:29ff:fe3f:48l	4ff02::2	ICMPv6	62 Router Solicitation	VIII	
	2 0.640797000	192.168.57.138	192.168.57.139	TCP	74 59875 > ssh [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK	59875	
	3 0.641184000	192.168.57.139	192.168.57.138	TCP	74 ssh > 59875 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MS	: ssh	
	4 0.641230000	192.168.57.138	192.168.57.139	TCP	66 59875 > ssh [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4	59875	
	5 0.641670000	192.168.57.138	192.168.57.139	SSHv2	87 Encrypted request packet len=21	59875	
	6 0.641936000	192.168.57.139	192.168.57.138	TCP	66 ssh > 59875 [ACK] Seq=1 Ack=22 Win=29056 Len=0 TSval=	ssh	
	7 0.659384000	192.168.57.139	192.168.57.138	SSHv2	87 Encrypted response packet len=21	ssh	
	8 0.659471000	192.168.57.138	192.168.57.139	TCP	66 59875 > ssh [ACK] Seq=22 Ack=22 Win=29312 Len=0 TSval	59875	
	9 0.659677000	192.168.57.138	192.168.57.139	TCP	1514 [TCP segment of a reassembled PDU]	59875	
	10 0.659712000	192.168.57.138	192.168.57.139	SSHv2	450 Client: Key Exchange Init	59875	
	11 0.659860000	192.168.57.139	192.168.57.138	TCP	66 ssh > 59875 [ACK] Seq=22 Ack=1854 Win=32640 Len=0 TSv	ssh	
	12 0.661292000	192.168.57.139	192.168.57.138	TCP	1514 [TCP segment of a reassembled PDU]	ssh	
	13 0.661409000	192.168.57.139	192.168.57.138	SSHv2	138 Server: Key Exchange Init	ssh	
	14 0.661420000	192.168.57.138	192.168.57.139	TCP	66 59875 > ssh [ACK] Seq=1854 Ack=1542 Win=32128 Len=0 T	: 59875	
	15 0.662584000	192.168.57.138	192.168.57.139	SSHv2	146 Client: Diffie-Hellman Key Exchange Init	59875	
	16 0.664917000	192.168.57.139	192.168.57.138	SSHv2	722 Server: New Keys	ssh	
	17 0.665705000	192.168.57.138	192.168.57.139	SSHv2	82 Client: New Keys	59875	
	18 0.705898000	192.168.57.139	192.168.57.138	TCP	66 ssh > 59875 [ACK] Seq=2198 Ack=1950 Win=32640 Len=0 T	: ssh	
	19 0.705935000	192.168.57.138	192.168.57.139	SSHv2	118 Encrypted request packet len=52	59875	
	20 0.706068000	192.168.57.139	192.168.57.138	TCP	66 ssh > 59875 [ACK] Seq=2198 Ack=2002 Win=32640 Len=0 T	: ssh	
	21 0.706185000	192.168.57.139	192.168.57.138	SSHv2	118 Encrypted response packet len=52	ssh	

Fig 3.1: Outgoing SSH connection to a remote host.

No,	Time	Source	Destination	Protoco	Lengtl Info	Source Por	Destination Por New Column
	1 0.0000000000	192.168.57.138	192.168.57.139	TCP	74 59876 > ssh [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK	59876	ssh TCP
	2 0.000681000	192.168.57.139	192.168.57.138	TCP	74 ssh > 59876 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MS	ssh	59876 TCP
	3 0.000767000	192.168.57.138	192.168.57.139	TCP	66 59876 > ssh [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4	59876	ssh TCP
	4 0.001633000	192.168.57.138	192.168.57.139	SSHv2	87 Encrypted request packet len=21	59876	ssh SSHv2
	5 0.001936000	192.168.57.139	192.168.57.138	TCP	66 ssh > 59876 [ACK] Seq=1 Ack=22 Win=29056 Len=0 TSval=	ssh	59876 TCP
	6 0.014933000	192.168.57.139	192.168.57.138	SSHv2	87 Encrypted response packet len=21	ssh	59876 SSHv2
	7 0.015026000	192.168.57.138	192.168.57.139	TCP	66 59876 > ssh [ACK] Seq=22 Ack=22 Win=29312 Len=0 TSval:	59876	ssh TCP
	8 0.015343000	192.168.57.138	192.168.57.139	TCP	1514 [TCP segment of a reassembled PDU]	59876	ssh TCP
	9 0.015461000	192.168.57.138	192.168.57.139	SSHv2	450 Client: Key Exchange Init	59876	ssh SSHv2
	10 0.015685000	192.168.57.139	192.168.57.138	TCP	66 ssh > 59876 [ACK] Seq=22 Ack=1854 Win=34816 Len=0 TSv	ssh	59876 TCP
	11 0.017960000	192.168.57.139	192.168.57.138	TCP	1514 [TCP segment of a reassembled PDU]	ssh	59876 TCP
	12 0.018159000	192.168.57.139	192.168.57.138	SSHv2	138 Server: Key Exchange Init	ssh	59876 SSHv2
	13 0.018182000	192.168.57.138	192.168.57.139	TCP	66 59876 > ssh [ACK] Seq=1854 Ack=1542 Win=32128 Len=0 T	59876	ssh TCP
	14 0.020741000	192.168.57.138	192.168.57.139	SSHv2	146 Client: Diffie-Hellman Key Exchange Init	59876	ssh SSHv2
	15 0.025632000	192.168.57.139	192.168.57.138	SSHv2	722 Server: New Keys	ssh	59876 SSHv2
	16 0.027312000	192.168.57.138	192.168.57.139	SSHv2	82 Client: New Keys	59876	ssh SSHv2
	17 0.067772000	192.168.57.139	192.168.57.138	TCP	66 ssh > 59876 [ACK] Seq=2198 Ack=1950 Win=34816 Len=0 T	ssh	59876 TCP
	18 0.067836000	192.168.57.138	192.168.57.139	SSHv2	118 Encrypted request packet len=52	59876	ssh SSHv2
	19 0.068379000	192.168.57.139	192.168.57.138	TCP	66 ssh > 59876 [ACK] Seq=2198 Ack=2002 Win=34816 Len=0 T	ssh	59876 TCP
	20 0.068616000	192.168.57.139	192.168.57.138	SSHv2	118 Encrypted response packet len=52	ssh	59876 SSHv2
	21 0.070873000	192.168.57.138	192.168.57.139	SSHv2	134 Encrypted request packet len=68	59876	ssh SSHv2

Figure 3.2 – Incoming SSH connection and replies

		Test4/	.pcapng [Win	reshark 1,10).11 (Git Rev U	Jnknown from	unknown)]	
File Edi	t View Go C	Capture Analyze	Statistics T	elephony T	ools Internals	Help		
• •			x G	Q %	·» % \$	2		~
Filter:					Expression	Clear Apply	Save	
No.	Time	Source		Destination		Protoco Lo		
- 7	5 0.544052000	192.100.37.13		192.100.07		JJI 18 Z	Soz Encrypted request packet of	
	6 0.344174000	192.168.57.13	(T)	192.168.57		TCP	66 ssh > 60003 [ACK] Seq=2422	
	7 0.346241000	192.168.57.13	71	192.168.57	0.000	SSHv2	138 Encrypted response packet	
	8 0.364177000	192.168.57.13		192.168.57		TCP	60 0 > http [SYN] Seq=0 Win=5	
	9 0.386480000	192.168.57.13	177.	192.168.57		TCP	66 60003 > ssh [ACK] Seq=2574	ALCOHOL ST.
	0 1.364957000	192.168.57.13	177	192.168.57		TCP	60 [TCP Port numbers reused]	and the second second
	1 2.366581000	192.168.57.13		192.168.57		TCP	60 [TCP Port numbers reused]	-
	2 3.366892000	192.168.57.13 fe80::20c:29f		192.168.57	. 138	TCP ICMPv6	60 [TCP Port numbers reused] (62 Router Solicitation	⊎ > nt
	3 3.949840000				120			0 × b+
	4 4.367922000 5 5.369084000	192.168.57.13 192.168.57.13	100	192.168.57 192.168.57		TCP SSHv2	60 [TCP Port numbers reused]	
- 10	5 5.369084000 6 5.369159000	192.168.57.13		192.168.57		TCP	150 Encrypted response packet	
	5.369159000 7 5.369193000	192.168.57.13		192.168.57		SSHv2	66 60003 > ssh [ACK] Seq=2574	
- 67			7		0.7.7.5		166 Encrypted response packet 66 60003 > ssh [ACK] Seq=2574	
	8 5.369206000 9 5.369292000	192.168.57.13		192.168.57	247777	TCP SSHv2	150 Encrypted response packet	
4	4 S REGULATION	197 168 57 1-	(G	197 168 57	148	ZZHVZ	150 Encrypted response backet	I en=84
± Frame	56: 66 bytes	on wire (528 b	its), 66 by	tes capture	ed (528 bits)	on interfac	ce O	
		bigl	ooss@localhos	t:/home/bigb	ooss/Downloads	/8006-Assig	nment-1	×
File E	dit View Sea	rch Terminal H	lelp					
Chain	CUSTOMALLOWO	OUT (O refere	nces)					
pk		es target	prot opt i	n out	source		destination	
Pi			11 *	*	0.0.0.0/		0.0.0.0/0	
Chain	CUSTOMDENYIN	l (2 reference	es)					
pk		es target	prot opt i	ln out	source		destination	
8			li *	*	0.0.0.0/		0.0.0.0/0	
	9905 MAGRICAN	Manufacture (1) Inc.	150.00				(N = 88 A 58	

Fig 4.1: Custom drop from 0 rule dropping 5 packets.

```
[root@localhost 8006-Assignment-1]# sh ResetFirewall.sh
Firewalls are now reset :)
[root@localhost 8006-Assignment-1]# hping 192.168.57.139 -S -s 0 -p 2135
HPING 192.168.57.139 (eno16777736 192.168.57.139): S set, 40 headers + 0 data by
tes
len=46 ip=192.168.57.139 ttl=64 DF id=23332 sport=2135 flags=RA seq=0 win=0 rtt=
1.9 ms
len=46 ip=192.168.57.139 ttl=64 DF id=23333 sport=2135 flags=RA seq=1 win=0 rtt=
1.0 ms
len=46 ip=192.168.57.139 ttl=64 DF id=23334 sport=2135 flags=RA seq=2 win=0 rtt=
0.8 ms
len=46 ip=192.168.57.139 ttl=64 DF id=23335 sport=2135 flags=RA seq=3 win=0 rtt=
1.2 ms
^C
--- 192.168.57.139 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.8/1.2/1.9 ms
[root@localhost 8006-Assignment-1]# sh Firewall.sh
New IPTABLES SET
Redirecting to /bin/systemctl restart iptables.service
Failed to issue method call: Unit iptables.service failed to load: No such file
or directory.
[root@localhost 8006-Assignment-1]# hping 192.168.57.139 -S -s 0 -p 2135
HPING 192.168.57.139 (eno16777736 192.168.57.139): S set, 40 headers + 0 data by
tes
[send ip] sendto: Operation not permitted
[root@localhost 8006-Assignment-1]#
```

Fig 4.2 Custom rule denying ability to send packets TO port 0

```
f
                                                                                              prica
Failed to issue method call: Unit iptables.service failed to load: No such file or directory.
Press any key to START TEST 5A: Drop all incoming traffic TO port 80 from ports 1-1024 (START YOUR WIRES
HARK CAP)
                                                                                          Chain HTTPDENY
                                                                                              pkts
--- 192.168.57.138 hping statistic ---
                                                                                                0
```

Chain HTTPDENY

Chain HTTPIN (3 pkts

pkts

round-trip min/avg/max = 0.0/0.0/0.0 ms Press any key to END TEST 5A: Drop all incoming traffic TO port 80 from ports 1-1024 (STOP AND SAVE YOUR WIRESHARK CAP)

HPING 192.168.57.138 (eno16777736 192.168.57.138): S set, 40 headers + 0 data bytes

Fig 5.1: Deny packets to port 80 from source port 1-1023

5 packets transmitted, 0 packets received, 100% packet loss

1

Activiti	es ^{>} - Terminal					Thu 03	·1 E	
ACTIVITI	es Terminal					Thu O3	.15	
		Test5B.pcapng [V	Vireshark 1.10,11 (Git Rev Unl	known from	unknown)]	N N		
File E	dit View Go C	apture Analyze Statistic	s Telephony Tools Internals	Help		F	ile Edit Viev	w Search Termin
	1		2 Q 🐠 💖 🖏	¥ [·	0 dports 80,4 5	0 HTTPOUT 43 220 HTTPOUT
Filter:			Y Expression	Clear App	ly Save	3	sports 80,4	43
No.	Time	Source	Destination	Protoco	Lengti Info	CI	nain CUSTOM	ALLOWIN (0 refe
	34 0.221151000	192.168.57.139	192.168.57.138	SSHV2	138 Encrypted response packet	Lei	pkts	bytes target
	35 0.237135000	192.168.57.139	192.168.57.138	TCP	60 1027 > http [SYN] Seq=0 W:	in=:	0	0 ACCEPT
	36 0.237232000	192.168.57.138	192.168.57.139	TCP	58 http > 1027 [SYN, ACK] Sec			
9	37 0.237797000	192.168.57.139	192.168.57.138	TCP	60 1027 > http [RST] Seq=1 W			ALLOWOUT (0 re
	38 0.260568000	192.168.57.138	192.168.57.139	TCP	66 60009 > ssh [ACK] Seq=2574	C 2000	pkts	bytes target
	39 1.238386000	192.168.57.139	192.168.57.138	TCP	60 1028 > http [SYN] Seq=0 W		0	0 ACCEPT
	The second secon	192.168.57.138	192.168.57.139	TCP	58 http > 1028 [SYN, ACK] Sec			SERVITE / 4
	THE RESIDENCE OF THE PARTY OF T	192.168.57.139	192.168.57.138	TCP	60 1028 > http [RST] Seq=1 W			DENYIN (1 refe
		192.168.57.139	192.168.57.138	TCP	60 solid-mux > http [SYN] Sec		pkts	bytes target
		192.168.57.138	192.168.57.139	TCP	58 http > solid-mux [SYN, AC		0	0 DROP
		192.168.57.139	192.168.57.138	TCP	60 solid-mux > http [RST] Sec		onin CUSTOM	DENYOUT (1 ref
		fe80::20c:29ff:fe3d:		ICMPv6	62 Router Solicitation		pkts	No. 100 200 200 200 200
		192.168.57.139	192.168.57.138	TCP	60 iadl > http [SYN] Seq=0 W	ACCORDING TO A STATE OF THE PARTY OF THE PAR	pkts 0	bytes target 0 DROP
		192.168.57.138	192.168.57.139	TCP	58 http > iadl [SYN, ACK] Sec	q=0	O	O DROP
		192.168.57.139	192.168.57.138	TCP	60 iadl > http [RST] Seq=1 W		oain UTTDDE	NYIN (1 refere
		192.168.57.139	192.168.57.138	TCP	60 iad2 > http [SYN] Seq=0 W		pkts	bytes target
		192.168.57.138 192.168.57.139	192.168.57.139	TCP	58 http > iad2 [SYN, ACK] Sec 60 iad2 > http [RST] Seg=1 Wi		5	200 DROP
	51 4.242593000	192.168.57.139	192.168.57.138 192.168.57.138	SSHv2	150 Encrypted response packet	The second secon	0	0 DROP
	52 4.243367000	192.168.57.139	192.168.57.138	SSHVZ	150 Encrypted response packet	cei	· ·	O DITOI
- 10 Mg			11111			C	nain HTTPDF	VYOUT (0 refer
🔵 🌌 Fi	ile: "./Captures/Te	st5B.pcapng" 1 Packet	s: 69 · Displayed: 69 (100.0%) ·	Profile: [Default		pkts	bytes target
ress a	nv kev to END	TEST 5A: Drop all	incoming traffic TO port	80 from	ports 1-1024 (STOP AND SAVE	YOUR	0	0 DROP
	IARK CAP)	1201 211 2132 211			period 2 2027. (eros mile emile		1900	
						CI	nain HTTPIN	(3 references
ress a	nv kev to STA	RT TEST 5B : DON'T	drop all incoming traff:	Lc TO port	80 from ports !1-1024 (STAR	RT YOU	pkts	bytes target
	SHÁRK CAP)				s cascile paparess throse tree and processes its constant	NIS CONSTRU	10	400 ACCEPT
							10000000	
						CI	nain HTTPOU	T (2 reference
192	2.168.57.138 h	ping statistic					pkts	bytes target
packe	ets transmitte	d, 5 packets receiv	ed, 0% packet loss				5	220 ACCEPT
PING 1	92.168.57.138	(eno16777736 192.1	68.57.138): S set, 40 he	eaders + (data bytes			
en=46	ip=192.168.57	.138 ttl=64 DF id=0	sport=80 flags=SA seq=0	win=2920	00 rtt=0.9 ms	CI	hain OTHERI	V (4 reference
en=46	ip=192.168.57	.138 ttl=64 DF id=0	sport=80 flags=SA seq=1	l win=2920	00 rtt=0.9 ms		pkts	bytes target
en=46	ip=192.168.57	.138 ttl=64 DF id=0	sport=80 flags=SA seq=2	2 win=2920	00 rtt=1.3 ms		0	0 ACCEPT
			sport=80 flags=SA seq=3					
	*** X0 00 00 00		sport=80 flags=SA seq=4	4 win=2920	00 rtt=1.2 ms	CI	nain OTHERO	JT (4 referenc
		ax = 0.9/1.1/1.3 ms					pkts	bytes target
	7.000 to		p all incoming traffic	Γ0 port 80) from ports !1-1024 (STOP A	ND SA	0	0 ACCEPT
E VALIR	WIRESHARK CA	P)						
LIOUN						5178		
LIOUN						CI	nain SSHIN pkts	(3 references) bytes target

Fig 5.2: Allowing traffic from ports !1-1024 into port 80

File Edit V	View Go Ca	pture Analyze Statistic	cs Telephony Tools Interna	als Help			File Edit Viev	w Search Ter
				- 100			10	400 HTTPOU
			2 Q 🐠 % 🕉 7] ~	dports 80,4	
							5	220 HTTPOU
Filter:			Y Expression.	. Clear App	ly Save		sports 80,4	43
lo. T	Γime	Source	Destination	Protoco	Lengti Info		Chain CUSTOM	ALLOWIN (0 r
		192.168.57.2	192.168.57.138	DNS	154 Standard query res	ponse Oxb6	pkts	bytes targ
6 1.	.320078000	192.168.57.138	173.194.33.179	TCP	54 psprserver > http	[SYN] Seq=	0	0 ACCEP
7 1.	.336790000	173.194.33.179	192.168.57.138	TCP	60 http > psprserver		Chada CUCTOM	ALLOWOLLT CO
		192.168.57.138	173.194.33.179	TCP	54 psprserver > http		Chain CUSTOM pkts	
		192.168.57.138	173.194.33.179	TCP	54 psdbserver > http		pkts 0	bytes targ
		173.194.33.179	192.168.57.138	TCP	60 http > psdbserver		0	U ACCEF
		192.168.57.138	173.194.33.179	TCP	54 psdbserver > http		Chain CUSTOM	DENYTH (1 re
		192.168.57.138 173.194.33.179	173.194.33.179	TCP TCP	54 gxtelmd > http [SYI 60 http > gxtelmd [SYI		pkts	bytes tar
		192.168.57.138	192.168.57.138 173.194.33.179	TCP	54 gxtelmd > http [RS		0	0 DROP
		192.168.57.138	173.194.33.179	TCP	54 gxtetma > nttp [RS 54 unihub-server > ht		17.0	
		173.194.33.179	192.168.57.138	TCP	60 http > unihub-serve		Chain CUSTOM	DENYOUT (1
		192.168.57.138	173.194.33.179	TCP	54 unihub-server > ht		pkts	bytes tar
		fe80::20c:29ff:fe3d:d		ICMPv6	62 Router Solicitation		0	0 DROP
19 5.	.323614000	192.168.57.138	173.194.33.179	TCP	54 futrix > http [SYN]	Seq=0 Wii		
20 5.	.340221000	173.194.33.179	192.168.57.138	TCP	60 http > futrix [SYN	, ACK] Seq:	Chain HTTPDE	
The second second			170 104 00 170					bytes tar
21 5.	.340272000	192.168.57.138	173.194.33.179	TCP	54 futrix > http [RST]		pkts	
22 6.	.333226000	Vmware_3f:48:14	Vmware_ef:91:3e	ARP	42 Who has 192.168.57	.2? Tell	5	200 DROP
22 6.	.333226000			1000		.2? Tell		
22 6. 23 6.	.333226000 .333523000	Vmware_3f:48:14 Vmware_ef:91:3e	Vmware_ef:91:3e Vmware_3f:48:14	ARP ARP	42 Who has 192.168.57 60 192.168.57.2 is at	.2? Tell	5 0	200 DROP 0 DROP
22 6. 23 6.	.333226000 .333523000	Vmware_3f:48:14 Vmware_ef:91:3e	Vmware_ef:91:3e	ARP ARP	42 Who has 192.168.57 60 192.168.57.2 is at	.2? Tell	5	200 DROP 0 DROP VYOUT (0 re
22 6. 23 6. File: "./ 192.168.5	.333226000 .333523000 /Captures/Tes 57.138 hpi	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic	Vmware_ef:91:3e Vmware_3f:48:14	ARP ARP	42 Who has 192.168.57 60 192.168.57.2 is at	.2? Tell	5 0 Chain HTTPDE	200 DROP 0 DROP NYOUT (0 re
22 6. 23 6. File: "./ 192.168.5 ckets tra	.333226000 .333523000 /Captures/Tes 57.138 hpi	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received	Vmware_ef:91:3e Vmware_3f:48:14 :::::::::::::::::::::::::::::::::	ARP ARP Profile: Default	42 Who has 192.168.57 60 192.168.57.2 is at	.2? Tell	5 0 Chain HTTPDEI pkts 0	200 DROP 0 DROP VYOUT (0 re bytes tar 0 DROP
22 6. 23 6. File: "./ 192.168.5 ckets tra G 192.168	.333226000 .333523000 /Captures/Tes 57.138 hpi ransmitted, 88.57.138 (Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received eno16777736 192.168	Vmware_ef:91:3e Vmware_3f:48:14 ::: 23 · Displayed: 23 (100 d, 0% packet loss 3.57.138): S set, 40 h	ARP ARP Profile: Default	42 Who has 192.168.57 60 192.168.57.2 is at	.2? Tell	5 0 Chain HTTPDEI pkts 0 Chain HTTPIN	200 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen
22 6. 23 6. 23 6. File: "./ 192.168.5 ckets tra G 192.168 46 ip=192	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 68.57.138 (02.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ns statistic 5 packets received eno16777736 192.166 38 ttl=64 DF id=0 s	Vmware_ef:91:3e Vmware_3f:48:14 :s: 23 · Displayed: 23 (100 d, 0% packet loss 8.57.138): S set, 40 h. sport=80 flags=SA seq=	ARP ARP Profile: Default eaders + 0 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms	.2? Tell	5 0 Chain HTTPDEI pkts 0 Chain HTTPIN pkts	200 DROP 0 DROP VYOUT (0 re bytes tar 0 DROP (3 referen bytes tar
22 6. 23 6. 192.168.5 ckets tra G 192.168 46 ip=192 46 ip=192	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 88.57.138 (92.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets received eno16777736 192.168 38 ttl=64 DF id=0 \$ 38 ttl=64 DF id=0 \$	Vmware_ef:91:3e Vmware_3f:48:14 	ARP ARP Profile: Default eaders + 0 win=29200 win=29200 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms	.2? Tell	5 0 Chain HTTPDEI pkts 0 Chain HTTPIN	200 DROP 0 DROP VYOUT (0 re bytes tan 0 DROP (3 referen- bytes tan
22 6. 23 6. 192.168. 192.168. 192.168 192.168 46 ip=192 46 ip=192 46 ip=192	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 68.57.138 (02.168.57.1 12.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received eno16777736 192.168 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s	Vmware_ef:91:3e Vmware_3f:48:14 S: 23 · Displayed: 23 (100	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=1.3 ms	.2? Tell	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15	200 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP
22 6. 23 6. Pile: "./ 192.168.5 ckets tra G 192.166 46 ip=192 46 ip=192 46 ip=192	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 88.57.138 (92.168.57.1 12.168.57.1 12.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received eno16777736 192.168 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 3.57.138): S set, 40 hesport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq=	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200 3 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms	.2? Tell	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU	200 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP
22 6. 23 6. 192.168.5 ckets tra 6 192.168 46 ip=192 46 ip=192 46 ip=192 46 ip=192	.333226000 .333523000 //Captures/Tes 57.138 hpi sensmitted, 88.57.138 (92.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received eno16777736 192.166 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s	Vmware_ef:91:3e Vmware_3f:48:14 S: 23 · Displayed: 23 (100	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200 3 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms	.2? Tell	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts	200 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar
22 6. 23 6. File: "./ 192.168.5 ckets tra 6 192.166 46 ip=192 46 ip=192 46 ip=192 46 ip=193 d-trip m	.333226000 .333523000 /Captures/Tes 57.138 hpi ansmitted, 88.57.138 (92.168.57.1 92.168.57.1 92.168.57.1 12.168.57.1 12.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received enol6777736 192.166 38 ttl=64 DF id=0 38 ttl=64 DF id=0 = 0.9/1.1/1.3 ms	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h. sport=80 flags=SA seq=	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200 3 win=29200 4 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at c data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU	200 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP
22 6. 23 6. 192.168.5 ckets tra 6 192.168 46 ip=192 46 ip=192 46 ip=194 de ip=194	.333226000 .333523000 /Captures/Tes 57.138 hpi ansmitted, 88.57.138 (92.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received enol6777736 192.166 38 ttl=64 DF id=0 38 ttl=64 DF id=0 = 0.9/1.1/1.3 ms	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h. sport=80 flags=SA seq=	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200 3 win=29200 4 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15	200 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar 620 ACCEP
22 6. 23 6. 192.168.5 192.168.5 106.192.168 106.192.168 106.192.168 106.192.168 106.192.168 106.192.168 106.192.168 106.192.168 106.192.168 107.192.1	.333226000 .333523000 /Captures/Tes 57.138 hpi ansmitted, 88.57.138 (92.168.57.1 92.168.57.1 92.168.57.1 12.168.57.1 12.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received enol6777736 192.166 38 ttl=64 DF id=0 38 ttl=64 DF id=0 = 0.9/1.1/1.3 ms	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h. sport=80 flags=SA seq=	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200 3 win=29200 4 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at c data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII	200 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar 620 ACCEP V (4 refere
22 6. 23 6. 23 6. File: "/ Fi	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 8.57.138 (2.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 sin/avg/max by to END T	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets received eno16777736 192.168 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200 3 win=29200 4 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts	200 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar 620 ACCEP N (4 refere bytes tar
22 6. 23 6. 23 6. File: "/ Fi	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 8.57.138 (2.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 sin/avg/max by to END T	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets received eno16777736 192.168 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h. sport=80 flags=SA seq=	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200 3 win=29200 4 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII	200 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar 620 ACCEP N (4 refere bytes tar
22 6. 23 6. 23 6. 26 File: "/ 192.168.! 192.168.! 104.169.168. 105.168. 106.192.168. 106.192.168. 106.192. 106.192. 106.192. 106.192. 107.	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 68.57.138 (22.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets receivec eno16777736 192.166 38 tt1=64 DF id=0 s 38 tt1=64 DF id=0 s 38 tt1=64 DF id=0 s 38 tt1=64 DF id=0 s 38 tt1=64 DF id=0 s 58 tt1=64 DF id=0 s 59 TS B: DON'T drop	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 3.57.138): S set, 40 h sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic	ARP ARP Profile: Default eaders + 0 9 win=29200 1 win=29200 2 win=29200 3 win=29200 4 win=29200	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts	200 DROP 0 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar 620 ACCEP N (4 refere bytes tar 140 ACCEP
22 6. 23 6. File: "J 192.168.! ckets tra 6 192.164 6 ip=19; 46 ip=19; 46 ip=19; 46 ip=19; 46 ip=19; 0 trip m: s any key 0 UR WIRES s any key	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 8.57.138 (2.168.57.1 22.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets received eno16777736 192.166 38 tt1=64 DF id=0 s 38 tt1=64 DF id=0 s 38 tt1=64 DF id=0 s 38 tt1=64 DF id=0 s 38 tt1=64 DF id=0 s 58 tt1=64 DF id=0 s Test 58: DON'T drop	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 h	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200 3 win=29200 10 port 80 UR WIRESHAR eaders + 0	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms from ports !1-1024 (S	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts 1 Chain OTHERII	200 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar 620 ACCEP N (4 refere bytes tar 140 ACCEP
22 6. 23 6. 23 6. 23 6. 23 6. 23 6. 24 6. 25 2. 168.: 26 192.166. 26 192.166. 26 192.266. 26 192.266. 26 192.266. 26 192.266. 26 192.266. 26 192.266. 27 26 27 26. 28	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 88.57.138 (22.168.57.1 122.168.57.1 122.168.57.1 122.168.57.1 121.168.57.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets received eno16777736 192.166 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s 59 ttl=64 DF id=0 s 60 septimental constants of the constant of the constants of the	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 3.57.138): S set, 40 h sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic	ARP ARP Profile: Default eaders + 0 0 win=29200 1 win=29200 2 win=29200 3 win=29200 (0 port 80 UR WIRESHAR eaders + 0 1=0 win=642	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S K CAP) data bytes 40 rtt=16.9 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts 1	200 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar 140 ACCEP JT (4 referen bytes tar
22 6. 23 6. 23 6. 23 6. 23 6. 23 6. 24 6 jp=19: 24 6 jp=17: 24 6 j	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 88.57.138 (92.168.57.1 92.168	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received eno16777736 192.168 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s 59 ttl=64 DF id=0 s 60 poly1.1/1.3 ms EST 5B: DON'T drop TEST 6A : Allow outliness and the second of the second	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h. sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 h. sport=80 flags=SA seq=	ARP ARP ARP Profile: Default eaders + 0 9 win=29200 2 win=29200 3 win=29200 4 win=29200 10 port 80 UR WIRESHAR eaders + 0 q=0 win=642 q=1 win=642	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S K CAP) data bytes 40 rtt=16.9 ms 40 rtt=15.9 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts 1	200 DROP 0 DROP 0 DROP NYOUT (0 re bytes tarn 0 DROP (3 reference bytes tarn 620 ACCEP T (2 reference bytes tarn 140 ACCEP JT (4 reference bytes tarn 140 ACCEP
22 6. 23 6. 23 6. 23 6. 23 6. 24 6. 25 7. 26 19-19: 26 19-19: 26 19-19: 27 27 28 28 28 28 28 28 28 28 28 28 28 28 28	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 8.57.138 (2.168.57.1 12.168.57	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2, Packet ng statistic 5 packets received eno16777736 192.166 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s Allow out eno16777736 173.194 79 ttl=128 id=45797 79 ttl=128 id=45797 79 ttl=128 id=45797	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 he sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 he sport=80 flags=SA seq= all sport=80 flags=SA seq= all sport=80 flags=SA seq= all sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= 7 sport=80 flags=SA seq= 7 sport=80 flags=SA seq= 80 sport=80 flags=SA seq= 81 sport=80 flags=SA seq= 82 seq=83 seq=84 seq=84 seq=85 seq=	ARP	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S K CAP) data bytes 40 rtt=16.9 ms 40 rtt=15.9 ms 40 rtt=21.9 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts 1	200 DROP 0 DROP 0 DROP 1 O PE
22 6. 23 6. 23 6. 23 6. 23 6. 23 6. 24 6. 25 2. 16 2. 26 2. 16 2. 26 2. 16 2. 26 2. 26 2. 26 2. 26 2. 26 2. 26 2. 26 2. 26 2. 26 2. 26 2. 26 2. 26 2. 27 2. 26 2. 28 2. 26 2. 28 2. 26 2. 28 28 28 28 28 28 28 28 28 28 28 28 28 2	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 8.57.138 (2.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 13.194.33.1 3.194.33.1 3.194.33.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets received eno16777736 192.168 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s Test of the second of the	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 3.57.138): S set, 40 h sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 h 6 sport=80 flags=SA seq= 7 sport=80 flags=SA seq= all sport=80 flags=SA seq= all sport=80 flags=SA seq= all sport=80 flags=SA seq= all sport=80 flags=SA seq= brighter flags=Brighter flags=Brighter flags=Brighter flags=Brighter flags=Brighter flags=Brighter flags=Brighter flags=Brighter flags=	ARP ARP ARP ARP Profile: Default peaders + 0 0 win=29200 1 win=29200 2 win=29200 4 win=29200 [70 port 80] JR WIRESHAR peaders + 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S K CAP) data bytes 40 rtt=16.9 ms 40 rtt=15.9 ms 40 rtt=21.9 ms 40 rtt=17.7 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts 1 Chain OTHERO pkts 1 Chain SSHIN pkts	200 DROP 0 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar 620 ACCEP V (4 refere bytes tar 140 ACCEP JT (4 refere bytes tar 60 ACCEP (3 reference) bytes tar 60 ACCEP
22 6. 23 6. 23 6. 23 6. 23 6. 23 6. 23 6. 23 6. 24 6. 25 2. 26 2.	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 8.57.138 (2.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets received eno16777736 192.168 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s Test of the second of the	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h. sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 h. sport=80 flags=SA seq= all sport=80 flags=SA seq= all sport=80 flags=SA seq= all sport=80 flags=SA seq= browner sport=80 flags=SA seq=	ARP ARP ARP ARP Profile: Default peaders + 0 0 win=29200 1 win=29200 2 win=29200 4 win=29200 [70 port 80] JR WIRESHAR peaders + 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S K CAP) data bytes 40 rtt=16.9 ms 40 rtt=15.9 ms 40 rtt=21.9 ms 40 rtt=17.7 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts 1 Chain OTHERII pkts 1 Chain OTHERII pkts 1 Chain OTHEROI	200 DROP 0 DROP 0 DROP 0 DROP NYOUT (0 re bytes tar 0 DROP (3 referen bytes tar 620 ACCEP T (2 refere bytes tar 620 ACCEP V (4 refere bytes tar 140 ACCEP JT (4 refere bytes tar 60 ACCEP (3 reference bytes tar 60 ACCEP
22 6. 23 6. 23 6. 23 6. 23 6. 23 6. 25 6. 26 7. 27 2. 168.5 28 2. 168.5 28 2. 168.5 28 2. 168.5 28 2. 168.5 28 2. 168.5 28 2.	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 8.57.138 (2.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets received eno16777736 192.166 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s 78 ttl=64 DF id=0 s 18 ttl=12B id=457979 18 ttl=12B id=45797 18 ttl=12B id=45797 19 ttl=12B id=45807 19 ttl=12B id=45807 19 ttl=12B id=45807	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 h sport=80 flags=SA seq= sport=80 flags=SA seq= all seq=180 flags=SA seq=180 flags=SA seq=180 flags=SA seq=180 flags=SA seq=180 flags=SA seq=180 flags=SA seq=180 sport=80 sport=	ARP ARP ARP ARP Profile: Default peaders + 0 0 win=29200 1 win=29200 2 win=29200 4 win=29200 [70 port 80] JR WIRESHAR peaders + 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S K CAP) data bytes 40 rtt=16.9 ms 40 rtt=15.9 ms 40 rtt=21.9 ms 40 rtt=17.7 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts 1 Chain OTHERO pkts 1 Chain SSHIN pkts	200 DROP 0 DROP 0 DROP 10 DROP 10 DROP 11 O re 12 DROP 13 reference 14 DROP 14 reference 15 DROP 16 ACCEP 17 (4 reference 16 DROP 18 DROP 19 DROP 19 DROP 19 DROP 10 D
22 6. 23 6. 23 6. 23 6. 23 6. 23 6. 23 6. 23 6. 24 6: 25 2. 168.5. 26 2. 168.5. 26 2. 168.5. 26 2. 168.5. 26 2. 168.5. 26 2. 168.5. 26 2. 168.5. 27 2. 168.5. 28 2	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 8.57.138 (2.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 110/avg/max 12.168.57.1 110/avg/max 12.168.57.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets received eno16777736 192.166 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s 40 ST	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h. sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 h. sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 h. sport=80 flags=SA seq= 9 sport=80 flags=SA seq=	ARP ARP ARP ARP Profile: Default peaders + 0 0 win=29200 1 win=29200 2 win=29200 4 win=29200 [70 port 80] JR WIRESHAR peaders + 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S K CAP) data bytes 40 rtt=16.9 ms 40 rtt=15.9 ms 40 rtt=21.9 ms 40 rtt=17.7 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts 1 Chain OTHERII pkts 1 Chain SSHIN pkts 48	200 DROP 0 DROP 0 DROP 10 DROP 10 DROP 11 O re 12 DROP 13 reference 14 DROP 14 reference 15 DROP 16 ACCEP 17 (4 reference 16 DROP 18 DROP 19 DROP 19 DROP 19 DROP 10 D
22 6. 23 6. 23 6. 23 6. 23 6. 23 6. 23 6. 23 6. 24 6. 25 2. 26 2.	.333226000 .333523000 //Captures/Tes 57.138 hpi ransmitted, 88.57.138 (2.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 12.168.57.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1 13.194.33.1	Vmware_3f:48:14 Vmware_ef:91:3e t6A.pcapng" 2 Packet ng statistic 5 packets receivec eno16777736 192.168 38 ttl=64 DF id=0 s 38 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s 58 ttl=64 DF id=0 s 59 ttl=64 DF id=0 s 50 ttl=64 DF id=0 s 50 ttl=128 id=45796 79 ttl=128 id=45796 79 ttl=128 id=45796 79 ttl=128 id=45796 79 ttl=128 id=45806 79 ttl=128 id=45806	Vmware_ef:91:3e Vmware_3f:48:14 d, 0% packet loss 8.57.138): S set, 40 h. sport=80 flags=SA seq= sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 h. sport=80 flags=SA seq= sport=80 flags=SA seq= all incoming traffic utbound HTTP (START YOU 4.33.179): S set, 40 h. sport=80 flags=SA seq= 9 sport=80 flags=SA seq=	ARP ARP ARP Profile: Default eaders + 0 9 win=29200 1 win=29200 2 win=29200 3 win=29200 4 win=29200 IO port 80 UR WIRESHAR eaders + 0 and win=642 and win=642 and win=642 and win=642 and win=642 and win=642	42 Who has 192.168.57 60 192.168.57.2 is at data bytes rtt=0.9 ms rtt=0.9 ms rtt=1.3 ms rtt=1.2 ms rtt=1.2 ms from ports !1-1024 (S K CAP) data bytes 40 rtt=16.9 ms 40 rtt=15.9 ms 40 rtt=21.9 ms 40 rtt=17.7 ms 40 rtt=16.9 ms	.2? Tell 00:50:56:	Chain HTTPDEI pkts 0 Chain HTTPIN pkts 15 Chain HTTPOU pkts 15 Chain OTHERII pkts 1 Chain OTHERII pkts 1 Chain SSHIN pkts 48 Chain SSHOUT	200 DROP 0 DROP 0 DROP 10 DROP 10 DROP 11 O re 12 bytes tan 12 a ACCEP 11 (2 reference 14 a ACCEP 14 ACCEP 15 (4 reference 14 a ACCEP 16 ACCEP 17 (4 reference 16 ACCEP 17 (5 reference 17 (6 reference 18 reference 18 reference 19 a reference 18 reference 19 referenc

Fig 6.1: Allow outbound HTTP

```
--- 192.168.57.138 hping statistic ---
HPING 192.168.57.138 (eno16777736 192.168.57.138): S set, 40 headers + 0 data bytes
len=46 ip=192.168.57.138 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=1.4 ms
DUP! len=46 ip=192.168.57.138 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=1001.7 ms
DUP! len=46 ip=192.168.57.138 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=2002.9 ms
DUP! len=46 ip=192.168.57.138 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=3003.9 ms
DUP! len=46 ip=192.168.57.138 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=4005.1 ms
Dup! len=46 ip=192.168.57.138 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=4005.1 ms
Fress any key to END TEST 6B: Allow inbound HTTP (STOP AND SAVE YOUR WIRESHARK CAP)
```

Fig 6.2: Allowing inbound HTTP (screenshot taken from an SSH session pinging LOCAL machine)

Fig 7. Log file containing test by test comparison of iptables and packets allowed or dropped by chains.

Format is: START TEST X --tables— END TEXT X --tables—

Notable occurences are highlighted.

START Test 1: Allow Inbound/Outbound DHCP

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes target prot opt in	า	out source	destinat	ion
0	0 OTHERIN udp *	*	0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp *	*	0.0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:68
0	0 SSHIN tcp * *		0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHIN tcp * *		0.0.0.0/0	0.0.0.0/0	tcp spt:22

0 SSHIN	udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:22
0 CUSTOM	DENYIN tcp		* * 0.0.0.0	/0 0.0.0.0	/0 tcp spt:0
0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
0 HTTPDEN	IYIN tcp	*	* 0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
(O CUSTOM O HTTPIN O HTTPDEN O HTTPIN	O CUSTOMDENYIN tcp O HTTPIN tcp * O HTTPDENYIN tcp O HTTPIN tcp *	O CUSTOMDENYIN tcp O HTTPIN tcp * O HTTPDENYIN tcp * O HTTPIN tcp *	O CUSTOMDENYIN tcp * * 0.0.0.0, O HTTPIN tcp * * 0.0.0.0/0 O HTTPDENYIN tcp * * 0.0.0.0/0 O HTTPIN tcp * * 0.0.0.0/0	O CUSTOMDENYIN tcp * * 0.0.0.0/0 0.0.0.0, O HTTPIN tcp * * 0.0.0.0/0 0.0.0.0/0 O HTTPDENYIN tcp * * 0.0.0.0/0 0.0.0.0/0 O HTTPIN tcp * * 0.0.0.0/0 0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)

	11 /		, , ,		
pkts	bytes target prot op	t in	out source	destinatio	on
0	0 OTHEROUT udp	* *	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp	* *	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:68
0	0 SSHOUT tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHOUT tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:22
0	0 CUSTOMDENYOUT t	ср	* * 0.0.0	.0/0 0.0.0	.0/0 tcp dpt:0
0	0 HTTPOUT tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Page: 17

A00802338

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination

O 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

```
Chain SSHOUT (3 references)
```

pkts bytes target prot opt in out source destination

END Test 1: Allow Inbound/Outbound DHCP

Chain INPUT (policy DROP 0 packets, 0 bytes)

		,	
pkts	bytes target prot opt in out	source destin	ation
1	122 OTHERIN udp * * 0	0.0.0.0/0	0 udp spt:53
0	0 OTHERIN tcp * * 0.0	0.0.0/0 0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp * * 0.0	0.0.0/0 0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp * * 0.0	0.0.0/0 0.0.0.0/0	tcp spt:68
0	0 SSHIN tcp * * 0.0.0	0.0.0.0/0	tcp dpt:22
0	0 SSHIN tcp * * 0.0.0	0.0.0.0/0	tcp spt:22
0	0 SSHIN udp * * 0.0.0	0.0.0/0	udp dpt:22
0	0 CUSTOMDENYIN tcp * *	0.0.0.0/0 0.0.	0.0/0 tcp spt:0
0	0 HTTPIN tcp * * 0.0.0	0.0.0/0 0.0.0.0/0	tcp spts:!1:1023 dpt:80
0	0 HTTPDENYIN tcp * *	0.0.0.0/0 0.0.0.0/	0 tcp spts:1:1023 dpt:80
0	0 HTTPIN tcp * * 0.0.0	0.0.0/0 0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN tcp * * 0.0.0	0.0.0/0 0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 15 packets, 3106 bytes)

	11 / / /	,	
pkts	bytes target prot opt in out source	e destination	า
1	73 OTHEROUT udp * * 0.0.0.0/	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp * * 0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp * * 0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp * * 0.0.0.0/0	0.0.0.0/0	tcp dpt:68
0	0 SSHOUT tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHOUT tcp * * 0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp * * 0.0.0.0/0	0.0.0.0/0	udp dpt:22
0	0 CUSTOMDENYOUT tcp * * 0.0	0.0.0/0	0/0 tcp dpt:0
0	0 HTTPOUT tcp * * 0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT tcp * * 0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Page: 19

A00802338

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

```
A00802338
Chain OTHERIN (4 references)
  pkts bytes target prot opt in out source
                                                   destination
  1 122 ACCEPT all -- * *
                                 0.0.0.0/0
                                               0.0.0.0/0
Chain OTHEROUT (4 references)
                                                   destination
  pkts bytes target protopt in out source
  1 73 ACCEPT all -- * *
                                0.0.0.0/0
                                              0.0.0.0/0
Chain SSHIN (3 references)
        bytes target prot opt in out source
                                                   destination
  pkts
        O ACCEPT all -- * *
   0
                                0.0.0.0/0
                                              0.0.0.0/0
Chain SSHOUT (3 references)
        bytes target prot opt in out source
                                                   destination
        0 ACCEPT all -- * *
                                0.0.0.0/0
                                              0.0.0.0/0
START Test 2: Allow Inbound/Outbound DNS
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target protopt in out source
                                                   destination
       122 OTHERIN udp -- * * 0.0.0.0/0
                                                               udp spt:53
   1
                                                 0.0.0.0/0
       O OTHERIN tcp -- * *
                                 0.0.0.0/0
   0
                                               0.0.0.0/0
                                                             tcp spt:53
                                                0.0.0.0/0
                                                             udp spt:68
   0
        0 OTHERIN udp -- * *
                                  0.0.0.0/0
   0
        0 OTHERIN tcp -- * *
                                 0.0.0.0/0
                                               0.0.0.0/0
                                                             tcp spt:68
                 tcp -- * *
                               0.0.0.0/0
                                                           tcp dpt:22
   0
        0 SSHIN
                                             0.0.0.0/0
                 tcp -- * *
   0
        0 SSHIN
                                0.0.0.0/0
                                             0.0.0.0/0
                                                           tcp spt:22
                                                            udp dpt:22
   0
        0 SSHIN
                 udp -- * *
                                0.0.0.0/0
                                              0.0.0.0/0
                                                     0.0.0.0/0
   0
        0 CUSTOMDENYIN tcp -- * * 0.0.0.0/0
                                                                  tcp spt:0
        0 HTTPIN tcp -- * *
                                              0.0.0.0/0
                                                            tcp spts:!1:1023 dpt:80
   0
                                0.0.0.0/0
```

Chain FORWARD (policy DROP 0 packets, 0 bytes)

0 HTTPIN tcp -- * *

O HTTPIN tcp -- * *

0

0

0

0 HTTPDENYIN tcp -- * * 0.0.0.0/0

bytes target prot opt in out source destination

0.0.0.0/0

0.0.0.0/0

0.0.0.0/0

0.0.0.0/0

0.0.0.0/0

tcp spts:1:1023 dpt:80

multiport sports 80,443

multiport dports 80,443

	Chain OUTPUT (policy DROP 16 packets, 3146 bytes)						
-	bytes target prot opt in out source						
1	,	0.0.0.0/0	udp dpt:53				
0	0 OTHEROUT tcp * * 0.0.0.0/0						
0	0 OTHEROUT udp * * 0.0.0.0/0	0.0.0.0/0	udp dpt:68				
0	0 OTHEROUT tcp * * 0.0.0.0/0	0.0.0.0/0	tcp dpt:68				
0	0 SSHOUT tcp * * 0.0.0.0/0 0 SSHOUT tcp * * 0.0.0.0/0	0.0.0.0/0 t	cp spt:22				
0	0 SSHOUT tcp * * 0.0.0.0/0	0.0.0.0/0 t	cp dpt:22				
0	0 SSHOUT udp * * 0.0.0.0/0						
0	0 CUSTOMDENYOUT tcp * * 0.0.						
0	0 HTTPOUT tcp * * 0.0.0.0/0	0.0.0.0/0	multiport dports 80,443				
0	0 HTTPOUT tcp * * 0.0.0.0/0	0.0.0.0/0	multiport sports 80,443				
	USTOMALLOWIN (0 references) bytes target prot opt in out source 0 ACCEPT all * * 0.0.0.0/0						
Chain C	USTOMALLOWOUT (0 references)						
	bytes target prot opt in out source	destination					
. 0	,						
Chain C	USTOMDENYIN (1 references)						
	bytes target prot opt in out source	destination					
0	,						
ol : 0							
	USTOMDENYOUT (1 references)	4					
-	bytes target prot opt in out source						
0	0 DROP all * * 0.0.0.0/0	0.0.0.0/0					
Chain H	TTPDENYIN (1 references)						
pkts	bytes target prot opt in out source	destination					
0	0 DROP all * * 0.0.0.0/0	0.0.0.0/0					
0	0 DROP all * * 0.0.0.0/0	0.0.0.0/0					

			A00802338		
Chain H ⁻ pkts 0	TTPDENYOUT (0 references bytes target prot opt in 0 DROP all * *	•	destination 0.0.0.0/0		
Chain H	TTPIN (3 references)				
pkts	bytes target prot opt in	out source	destination		
0	0 ACCEPT all * *	0.0.0.0/0	0.0.0.0/0		
Chain HTTPOLIT (2 references)					

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination

1 122 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination

1 73 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

END Test 2: Allow Inbound/Outbound DNS

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes target	prot opt i	n	out source	destinatio	on
2	312 OTHERIN	udp *	:	* 0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN	udp *	*	0.0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:68

0	0 SSHIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHIN	udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:22
0	0 CUSTON	IDENYIN tcp)	* * 0.0.0.0	0.0.0.0)/0 tcp spt:0
0	0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
0	0 HTTPDE	NYIN tcp	*	* 0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0	0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 16 packets, 3146 bytes)

	on or (poncy bitor to packet	.s, 5± 10 by (cs)		
pkts	bytes target prot opt in	out source	destination	n
2	135 OTHEROUT udp *	* 0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:68
0	0 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:22
0	0 CUSTOMDENYOUT tcp	* * 0.0.0	.0/0 0.0.0.0	0/0 tcp dpt:0
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

destination

pkts bytes target prot opt in out source destination 0 DROP all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain CUSTOMDENYOUT (1 references) pkts bytes target prot opt in out source destination 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPDENYIN (1 references) pkts bytes target prot opt in out source destination 0 DROP all -- * * 0.0.0.0/0 0 0.0.0.0/0 0 DROP all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain HTTPDENYOUT (0 references) pkts bytes target prot opt in out source destination 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPIN (3 references) pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPOUT (2 references) pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain OTHERIN (4 references) pkts bytes target prot opt in out source destination 2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0Chain OTHEROUT (4 references) pkts bytes target prot opt in out source destination 2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain SSHIN (3 references)

pkts bytes target protopt in out source

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination

START Test 3A: Allow outbound SSH to a host

Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out so

pkts	bytes target prot of	pt in	out source	destinati	ion
2	312 OTHERIN udp -	- *	* 0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN tcp	* *	0.0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp	* *	* 0.0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp	* *	0.0.0.0/0	0.0.0.0/0	tcp spt:68
0	0 SSHIN tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHIN tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHIN udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:22
0	0 CUSTOMDENYIN t	ср	* * 0.0.0.0	0.0.0.0	0/0 tcp spt:0
0	0 HTTPIN tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
0	0 HTTPDENYIN tcp	*	* 0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0	0 HTTPIN tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 16 packets, 3146 bytes)

bytes target prot opt in out source	destination	
135 OTHEROUT udp * * 0.0.0.0/0	0 0.0.0.0/0 udp dpt:53	
0 OTHEROUT tcp * * 0.0.0.0/0	0.0.0.0/0 tcp dpt:53	
0 OTHEROUT udp * * 0.0.0.0/0	0.0.0.0/0 udp dpt:68	
0 OTHEROUT tcp * * 0.0.0.0/0	0.0.0.0/0 tcp dpt:68	
0 SSHOUT tcp * * 0.0.0.0/0	0.0.0.0/0 tcp spt:22	
0 SSHOUT tcp * * 0.0.0.0/0	0.0.0.0/0 tcp dpt:22	
0 SSHOUT udp * * 0.0.0.0/0	0.0.0.0/0 udp dpt:22	
0 CUSTOMDENYOUT tcp * * 0.0.	.0.0/0 0.0.0.0/0 tcp dpt:0	
	135 OTHEROUT udp * * 0.0.0.0/0 0 OTHEROUT tcp * * 0.0.0.0/0 0 OTHEROUT udp * * 0.0.0.0/0 0 OTHEROUT tcp * * 0.0.0.0/0 0 SSHOUT tcp * * 0.0.0.0/0 0 SSHOUT tcp * * 0.0.0.0/0 0 SSHOUT udp * * 0.0.0.0/0	135 OTHEROUT udp * * 0.0.0.0/0 0.0.0.0/0 udp dpt:53 0 OTHEROUT tcp * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:53 0 OTHEROUT udp * * 0.0.0.0/0 0.0.0.0/0 udp dpt:68 0 OTHEROUT tcp * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:68 0 SSHOUT tcp * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22 0 SSHOUT tcp * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 0 SSHOUT udp * * 0.0.0.0/0 0.0.0.0/0 udp dpt:22

0 0 HTTPOUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 multiport dports 80,443 0 0 HTTPOUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

0.0.0.0/0 0 ACCEPT all -- * * 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination 2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination

2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination

0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination

0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

END Test 3A: Allow outbound SSH to a host

Chain INPUT (policy DROP 0 packets, 0 bytes)

		•		
pkts	bytes target prot opt in o	out source	destinati	on
2	312 OTHERIN udp * *	0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp * *	0.0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:68
0	0 SSHIN tcp * * 0.	0.0.0/0	0.0.0.0/0	tcp dpt:22
22	4753 SSHIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHIN udp * * 0	0.0.0.0	0.0.0.0/0	udp dpt:22
0	0 CUSTOMDENYIN tcp *	* 0.0.0.0	0.0.0.0	/0 tcp spt:0
0	O HTTPIN tcp * * 0	0.0.0.0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
0	0 HTTPDENYIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0	O HTTPIN tcp * * 0	0.0.0.0	0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN tcp * * 0	0.0.0.0	0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target protopt in out source destination Chain OUTPUT (policy DROP 16 packets, 3146 bytes) pkts bytes target prot opt in out source destination 135 OTHEROUT udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:53 0 OTHEROUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 0 tcp dpt:53 0 OTHEROUT udp -- * * 0.0.0.0/0 0 0.0.0.0/0 udp dpt:68 0 OTHEROUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 0 tcp dpt:68 0 SSHOUT tcp -- * * 0.0.0.0/0 0 0.0.0.0/0 tcp spt:22 3885 SSHOUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 24 0 SSHOUT udp -- * * 0.0.0.0/0 0 0.0.0.0/0 udp dpt:22 0 CUSTOMDENYOUT tcp -- * * 0.0.0.0/0 0 0.0.0.0/0 tcp dpt:0 0 HTTPOUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 multiport dports 80,443 0 0 HTTPOUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 0 multiport sports 80,443 Chain CUSTOMALLOWIN (0 references) pkts bytes target protopt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain CUSTOMALLOWOUT (0 references) pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain CUSTOMDENYIN (1 references) pkts bytes target protopt in out source destination 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain CUSTOMDENYOUT (1 references) pkts bytes target protopt in out source destination 0 DROP all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain HTTPDENYIN (1 references) pkts bytes target prot opt in out source destination 0 DROP all -- * * 0.0.0.0/0 0 0.0.0.0/0

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination

2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination

2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination

22 4753 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination

24 3885 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

START Test 3B: Allow inbound SSH to a host

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

2 312 OTHERIN udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:53

0 0 OTHERIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:53

0	0 OTHERIN udp * * 0.0	0.0.0/0 0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp * * 0.0	.0.0/0 0.0.0.0/0	tcp spt:68
0	0 SSHIN tcp * * 0.0.0	.0/0 0.0.0.0/0	tcp dpt:22
22	4753 SSHIN tcp * * 0.0	0.0.0/0 0.0.0.0/0	tcp spt:22
0	0 SSHIN udp * * 0.0.0	0.0.0/0	udp dpt:22
0	0 CUSTOMDENYIN tcp * *	0.0.0.0/0 0.0.0.	0/0 tcp spt:0
0	0 HTTPIN tcp * * 0.0.0	0.0.0/0	tcp spts:!1:1023 dpt:80
0	0 HTTPDENYIN tcp * * (0.0.0.0/0 0.0.0.0/0	tcp spts:1:1023 dpt:80
0	0 HTTPIN tcp * * 0.0.0	0.0.0/0	multiport sports 80,443
0	0 HTTPIN tcp * * 0.0.0	0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 16 packets, 3146 bytes)

pkts	bytes target	prot opt in	out	source	destinatio	n
2	135 OTHEROU	T udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT	tcp *	* 0	.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT	udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT	tcp *	* 0	.0.0.0/0	0.0.0.0/0	tcp dpt:68
0	0 SSHOUT t	cp * *	0.0	.0.0/0	0.0.0.0/0	tcp spt:22
24	3885 SSHOUT	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT ι	ıdp * *	0.0	0.0.0/0	0.0.0.0/0	udp dpt:22
0	0 CUSTOMDE	NYOUT tcp	*	* 0.0.0	0.0.0.	0/0 tcp dpt:0
0	0 HTTPOUT	tcp * *	0.0	0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT	tcp * *	0.0	0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination

Page: 31

A00802338

Chain CUSTOMDENYIN (1 references)							
pkts	bytes target	prot opt in	out source	destination			
0	0 DROP all	* *	0.0.0.0/0	0.0.0.0/0			
Chain CUSTOMDENYOUT (1 references)							

pkts bytes target prot opt in out source destination

0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination

0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination

0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination

2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination 2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

```
A00802338
Chain SSHIN (3 references)
 pkts bytes target prot opt in out source
                                                   destination
  22 4753 ACCEPT all -- * * 0.0.0.0/0
                                                0.0.0.0/0
Chain SSHOUT (3 references)
 pkts bytes target prot opt in out source
                                                   destination
  24 3885 ACCEPT all -- * *
                                  0.0.0.0/0
                                                0.0.0.0/0
END Test 3B: Allow inbound SSH to a host
Chain INPUT (policy DROP 0 packets, 0 bytes)
      bytes target prot opt in out source
                                                   destination
  pkts
       312 OTHERIN udp -- * *
                                   0.0.0.0/0
                                                               udp spt:53
                                                 0.0.0.0/0
        0 OTHERIN tcp -- * *
                                 0.0.0.0/0
                                               0.0.0.0/0
                                                             tcp spt:53
   0
                                  0.0.0.0/0
                                                0.0.0.0/0
                                                              udp spt:68
        O OTHERIN udp -- * *
   0
       0 OTHERIN tcp -- * *
                                 0.0.0.0/0
   0
                                               0.0.0.0/0
                                                             tcp spt:68
                                 0.0.0.0/0
                                               0.0.0.0/0
                                                            tcp dpt:22
   5
       200 SSHIN
                   tcp -- * *
       9474 SSHIN tcp -- * * 0.0.0.0/0
                                                0.0.0.0/0
                                                            tcp spt:22
   0
       0 SSHIN udp -- * *
                                0.0.0.0/0
                                              0.0.0.0/0
                                                            udp dpt:22
        0 CUSTOMDENYIN tcp -- * * 0.0.0.0/0
                                                     0.0.0.0/0
   0
                                                                   tcp spt:0
        0 HTTPIN tcp -- * *
                                                            tcp spts:!1:1023 dpt:80
   0
                                 0.0.0.0/0
                                               0.0.0.0/0
        0 HTTPDENYIN tcp -- *
                                                                tcp spts:1:1023 dpt:80
                               * 0.0.0.0/0
                                                  0.0.0.0/0
   0
        O HTTPIN tcp -- * *
                                              0.0.0.0/0
                                                            multiport sports 80,443
   0
                                 0.0.0.0/0
        0 HTTPIN tcp -- * *
                                0.0.0.0/0
                                              0.0.0.0/0
                                                            multiport dports 80,443
```

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 16 packets, 3146 bytes)

pkts	bytes target prot opt in	1 0	ut source	destination	
2	135 OTHEROUT udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:68
5	200 SSHOUT tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
<mark>49</mark>	7870 SSHOUT tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

```
Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination
```

Chain OTHEROUT (4 references)

2 312 ACCEPT all -- * *

pkts bytes target prot opt in out source destination 2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

0.0.0.0/0

0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination

50 9674 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination

54 8070 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

START Test 4A: Drop all incoming traffic from port 0

Chain INPUT (policy DROP 0 packets, 0 bytes)

		-		
pkts	bytes target prot opt in out	source	destinatio	n
2	312 OTHERIN udp * *	0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN tcp * * 0.0	0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp * * 0	0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp * * 0.0	0.0.0/0	0.0.0.0/0	tcp spt:68
5	200 SSHIN tcp * * 0.0	.0.0/0	0.0.0.0/0	tcp dpt:22
45	9474 SSHIN tcp * * 0	.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHIN udp * * 0.0	0.0/0	0.0.0.0/0	udp dpt:22
0	0 CUSTOMDENYIN tcp * *	0.0.0.0/	0.0.0.0/	0 tcp spt:0
0	0 HTTPIN tcp * * 0.0	0.0/0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
0	0 HTTPDENYIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0	0 HTTPIN tcp * * 0.0	0.0/0	0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN tcp * * 0.0	0.0/0	0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes) pkts bytes target protopt in out source destination Chain OUTPUT (policy DROP 16 packets, 3146 bytes) pkts bytes target prot opt in out source destination 2 135 OTHEROUT udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:53 0 OTHEROUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:53 0 OTHEROUT udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:68 0 O OTHEROUT tcp -- * * 0 0.0.0.0/0 0.0.0.0/0 tcp dpt:68 200 SSHOUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22 7870 SSHOUT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 49 0 SSHOUT udp -- * * 0.0.0.0/0 udp dpt:22 0.0.0.0/0 0 0 CUSTOMDENYOUT tcp -- * * 0.0.0.0/0 0 0.0.0.0/0 tcp dpt:0 0 HTTPOUT tcp -- * * multiport dports 80,443 0.0.0.0/0 0.0.0.0/0 0 HTTPOUT tcp -- * * 0 0.0.0.0/0 0.0.0.0/0 multiport sports 80,443 Chain CUSTOMALLOWIN (0 references) pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain CUSTOMALLOWOUT (0 references) pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain CUSTOMDENYIN (1 references) pkts bytes target protopt in out source destination 0 DROP all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain CUSTOMDENYOUT (1 references) bytes target prot opt in out source destination pkts

0.0.0.0/0

Chain HTTPDENYIN (1 references)

0 DROP all -- * * 0.0.0.0/0

pkts bytes target prot opt in out source destination all -- * * 0 0 DROP 0.0.0.0/0 0.0.0.0/0 all -- * * n 0 DROP 0.0.0.0/0 0.0.0.0/0 Chain HTTPDENYOUT (0 references) pkts bytes target protopt in out source destination 0 DROP all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain HTTPIN (3 references) pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0 0.0.0.0/0 0.0.0.0/0 Chain HTTPOUT (2 references) pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain OTHERIN (4 references) pkts bytes target prot opt in out source destination 2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain OTHEROUT (4 references) pkts bytes target prot opt in out source destination 2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain SSHIN (3 references) pkts bytes target prot opt in out source destination 50 9674 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0Chain SSHOUT (3 references) pkts bytes target prot opt in out source destination 54 8070 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 END Test 4A: Drop all incoming traffic from port 0 Chain INPUT (policy DROP 0 packets, 0 bytes) pkts bytes target protopt in out source destination

2	312 OTHERIN udp -	* *	0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN tcp	* *	0.0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp	* *	0.0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp	* *	0.0.0.0/0	0.0.0.0/0	tcp spt:68
5	200 SSHIN tcp *	* *	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
69	13799 SSHIN tcp	- * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHIN udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:22
5	200 CUSTOMDENYIN	tcp	* * 0.0.0	0.0.0	<mark>.0/0 tcp spt:0</mark>
0	0 HTTPIN tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
0	0 HTTPDENYIN tcp	*	* 0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0	0 HTTPIN tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain C	OUTPUT (policy DROP 16 packets, 3146 by	ces)	
pkts	bytes target prot opt in out sour	ce destination	า
2	135 OTHEROUT udp * * 0.0.0.	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp * * 0.0.0.0/	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp * * 0.0.0.0,	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp * * 0.0.0.0/	0.0.0.0/0	tcp dpt:68
5	200 SSHOUT tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spt:22
74	11855 SSHOUT tcp * * 0.0.0.0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp * * 0.0.0.0/0	0.0.0.0/0	udp dpt:22
0	0 CUSTOMDENYOUT tcp * * 0	0.0.0.0	0/0 tcp dpt:0
0	0 HTTPOUT tcp * * 0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT tcp * * 0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

destination

pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain CUSTOMDENYIN (1 references) pkts bytes target prot opt in out source destination 5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain CUSTOMDENYOUT (1 references) pkts bytes target prot opt in out source destination 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPDENYIN (1 references) pkts bytes target prot opt in out source destination 0 DROP all -- * * 0.0.0.0/0 0 0.0.0.0/0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPDENYOUT (0 references) pkts bytes target prot opt in out source destination 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPIN (3 references) pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPOUT (2 references) pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0Chain OTHERIN (4 references) pkts bytes target protopt in out source destination 2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain OTHEROUT (4 references)

pkts bytes target protopt in out source

2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination 74 13999 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination 79 12055 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

START Test 4C: Drop all outgoing packets to 0

Chain INPUT (policy DROP 0 packets, 0 bytes)

	" ' ' ' '		
pkts	bytes target prot opt in out source	destinati	on
2	312 OTHERIN udp * * 0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp * * 0.0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spt:68
5	200 SSHIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp dpt:22
69	13799 SSHIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHIN udp * * 0.0.0.0/0	0.0.0.0/0	udp dpt:22
5	200 CUSTOMDENYIN tcp * * 0.0.0	0.0.0	.0/0 tcp spt:0
0	0 HTTPIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
0	0 HTTPDENYIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0	0 HTTPIN tcp * * 0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN tcp * * 0.0.0.0/0	0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 16 packets, 3146 bytes)

pkts	bytes target	prot opt in	01	ut source	destination	
2	135 OTHEROUT	dp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT	udp *	*	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:68

5	200 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
74	11855 SSHOUT tcp *	* 0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:22
0	0 CUSTOMDENYOUT tcp	* * 0.0.0	0.0.0	0/0 tcp dpt:0
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination
5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination

2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination

2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination

74 13999 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination 79 12055 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

END Test 4C: Drop all outgoing packets to 0

pkts bytes target prot opt in out source

Chain INPUT (policy DROP 0 packets, 0 bytes)

2	312 OTHERIN udp *	* 0.0.0.0/0	0.0.0.0/0	udp spt:53	
0	0 OTHERIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:53	
0	0 OTHERIN udp * *	0.0.0.0/0	0.0.0.0/0	udp spt:68	
0	0 OTHERIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:68	
5	200 SSHIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:22	
69	13799 SSHIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22	
0	0 SSHIN udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:22	
				_	

destination

200 CUSTOMDENYIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:0

0 HTTPIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 0 tcp spts:!1:1023 dpt:80

0 HTTPDENYIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spts:1:1023 dpt:80 0

0	0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 16 packets, 3146 bytes) pkts bytes target prot opt in out source

pkts	bytes target prof	t opt in o	ut source	destination	
2	135 OTHEROUT ud	p * *	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp	* *	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp	* *	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp	* *	0.0.0.0/0	0.0.0.0/0	tcp dpt:68
5	200 SSHOUT tcp	* *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
74	11855 SSHOUT tcp) * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp -	_ * *	0.0.0.0/0	0.0.0.0/0	udp dpt:22
1	40 CUSTOMDENYO	UT tcp [:]	* * 0.0.0.0	0.0.0.0	<mark>)/0 tcp dpt:0</mark>
0	0 HTTPOUT tcp -	- * *	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT tcp -	_ * *	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination 5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination

1 40 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

0.0.0.0/0

Chain HTTPDENYIN (1 references) bytes target prot opt in out source destination all -- * * 0 DROP 0.0.0.0/0 0 0.0.0.0/0 all -- * * 0 DROP 0.0.0.0/0 0.0.0.0/0 Chain HTTPDENYOUT (0 references) pkts bytes target prot opt in out source destination 0 DROP all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain HTTPIN (3 references) pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 0 Chain HTTPOUT (2 references) pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0Chain OTHERIN (4 references) pkts bytes target prot opt in out source destination 2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain OTHEROUT (4 references) pkts bytes target prot opt in out source destination 2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain SSHIN (3 references) pkts bytes target prot opt in out source destination 74 13999 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 Chain SSHOUT (3 references) pkts bytes target prot opt in out source destination

79 12055 ACCEPT all -- * * 0.0.0.0/0

START Test 5A: Drop all incoming traffic TO port 80 from ports 1-1024

Chain I	NPUT (policy DROP 0 packets, 0 bytes)		
pkts	bytes target prot opt in out source	destinati	on
2	312 OTHERIN udp * * 0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp * * 0.0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spt:68
5	200 SSHIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp dpt:22
69	13799 SSHIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHIN udp * * 0.0.0.0/0	0.0.0.0/0	udp dpt:22
5	200 CUSTOMDENYIN tcp * * 0.0.0	.0/0 0.0.0	.0/0 tcp spt:0
0	0 HTTPIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
0	0 HTTPDENYIN tcp * * 0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0	0 HTTPIN tcp * * 0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
0	0.11TTDIN	0 0 0 0 10	
0	0 HTTPIN tcp * * 0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
	FORWARD (policy DROP 0 packets, 0 bytes)	0.0.0.0/0 destinati	, , ,

Chain OUTPUT (policy DROP 16 packets, 3146 bytes)

pkts	bytes target prot opt in c	out source	destination	
2	135 OTHEROUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:68
5	200 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
74	11855 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:22
1	40 CUSTOMDENYOUT tcp	* * 0.0.0.	0.0.0.0)/0 tcp dpt:0
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination

5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination

1 40 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination

2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

```
Chain OTHEROUT (4 references)
  pkts bytes target prot opt in out source
                                                   destination
   2 135 ACCEPT all -- * *
                                 0.0.0.0/0
                                               0.0.0.0/0
Chain SSHIN (3 references)
  pkts bytes target protopt in out source
                                                   destination
  74 13999 ACCEPT all -- * * 0.0.0.0/0
                                                 0.0.0.0/0
Chain SSHOUT (3 references)
  pkts bytes target prot opt in out source
                                                   destination
  79 12055 ACCEPT all -- * * 0.0.0.0/0
                                                 0.0.0.0/0
END Test 5A: Drop all incoming traffic TO port 80 from ports 1-1024
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target prot opt in out source
                                                   destination
      312 OTHERIN udp -- * * 0.0.0.0/0
                                                 0.0.0.0/0
                                                              udp spt:53
       0 OTHERIN tcp -- * *
   0
                                 0.0.0.0/0
                                               0.0.0.0/0
                                                             tcp spt:53
       O OTHERIN udp -- * *
                                  0.0.0.0/0
                                                0.0.0.0/0
                                                             udp spt:68
   0
                                               0.0.0.0/0
   0
       0 OTHERIN tcp -- * *
                                 0.0.0.0/0
                                                            tcp spt:68
                                 0.0.0.0/0
       200 SSHIN
                  tcp -- * *
                                              0.0.0.0/0
                                                            tcp dpt:22
      18124 SSHIN tcp -- * * 0.0.0.0/0
                                                0.0.0.0/0
                                                              tcp spt:22
                                                           udp dpt:22
   0
       0 SSHIN udp -- * *
                                0.0.0.0/0
                                              0.0.0.0/0
       200 CUSTOMDENYIN tcp -- * * 0.0.0.0/0
                                                      0.0.0.0/0
                                                                   tcp spt:0
       O HTTPIN tcp -- * *
                                                            tcp spts:!1:1023 dpt:80
   0
                                0.0.0.0/0
                                              0.0.0.0/0
   5
       200 HTTPDENYIN tcp -- * * 0.0.0.0/0
                                                  0.0.0.0/0
                                                                tcp spts:1:1023 dpt:80
        O HTTPIN tcp -- * *
                                0.0.0.0/0
                                              0.0.0.0/0
   0
                                                            multiport sports 80,443
                                              0.0.0.0/0
                                                           multiport dports 80,443
   0
        0 HTTPIN tcp -- * *
                                0.0.0.0/0
Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target protopt in out source
                                                   destination
Chain OUTPUT (policy DROP 16 packets, 3146 bytes)
 pkts bytes target prot opt in out source
                                                   destination
   2 135 OTHEROUT udp -- * *
                                    0.0.0.0/0
                                                  0.0.0.0/0
                                                                udp dpt:53
       0 OTHEROUT tcp -- * * 0.0.0.0/0
                                                 0.0.0.0/0
   n
                                                              tcp dpt:53
```

0	0 OTHEROUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:68
5	200 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
99	15840 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:22
1	40 CUSTOMDENYOUT tcp	* * 0.0.0	0.0.0	.0/0 tcp dpt:0
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination
5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination
1 40 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination

5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references) pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination 2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination 2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination 98 18324 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

5

pkts bytes target prot opt in out source destination 104 16040 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

START Test 5B: DON'T drop all incoming traffic TO port 80 from ports !1-1024 Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination 312 OTHERIN udp -- * * 0.0.0.0/0 2 0.0.0.0/0 udp spt:53 0 OTHERIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:53 0 0 OTHERIN udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:68 0 0.0.0.0/0 0 0 OTHERIN tcp -- * * 0.0.0.0/0 tcp spt:68 tcp -- * * 0.0.0.0/0 0.0.0.0/0 200 SSHIN tcp dpt:22 93 18124 SSHIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22 0 SSHIN udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:22 0 200 CUSTOMDENYIN tcp -- * * 0.0.0.0/0

0.0.0.0/0

tcp spt:0

0	0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
5	200 HTTPDE	NYIN tcp	*	* 0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0	0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN	tcp *	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 16 packets, 3146 bytes)

pkts	bytes target prot opt in	out source	destination	
2	135 OTHEROUT udp *	* 0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:68
5	200 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
99	15840 SSHOUT tcp *	* 0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:22
1	40 CUSTOMDENYOUT tcp	* * 0.0.0.	0.0.0.0)/0 tcp dpt:0
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination
5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination
1 40 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination
5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination 2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination
2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination 98 18324 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

104 16040 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

END Test 5B: DON'T drop all incoming traffic TO port 80 from ports !1-1024

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes target prot opt in	out source	destinatio	on
2	312 OTHERIN udp * *	0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp * *	0.0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:68
5	200 SSHIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
117	22865 SSHIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0 SSHIN udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:22
5	200 CUSTOMDENYIN tcp	* * 0.0.0.	0.0.0	0/0 tcp spt:0
10	400 HTTPIN tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spts:!1:1023 dpt:80
5	200 HTTPDENYIN tcp *	* 0.0.0.0/0	0.0.0.0/0	tcp spts:1:1023 dpt:80
0	0 HTTPIN tcp * *	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
0	0 HTTPIN tcp * *	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 16 packets, 3146 bytes)

pkts	bytes target prot of	pt in out	source	destination	
2	135 OTHEROUT udp	* *	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp	* * 0.0	0.0.0/0 0.	0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp	- * * 0.	0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp	* * 0.0	0.0.0/0 0.	0.0.0/0	tcp dpt:68
5	200 SSHOUT tcp	* * 0.0	.0.0/0 0.0	0.0.0/0	tcp spt:22
124	19825 SSHOUT tcp	* *	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp			0.0.0/0 u	dp dpt:22
1	40 CUSTOMDENYOUT	Г tcp *	* 0.0.0.0/0	0.0.0.0/	0 tcp dpt:0
0	0 HTTPOUT tcp	* * 0.0	0.0/0 0.0).0.0/0 n	nultiport dports 80,443
5	220 HTTPOUT tcp	* * 0.	0.0.0/0	.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination 0 ACCEPT all -- * * 0.0.0.0/0 0 0.0.0.0/0 Chain CUSTOMALLOWOUT (0 references) pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0Chain CUSTOMDENYIN (1 references) pkts bytes target prot opt in out source destination 5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain CUSTOMDENYOUT (1 references) pkts bytes target protopt in out source destination 1 40 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPDENYIN (1 references) pkts bytes target prot opt in out source destination 5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPDENYOUT (0 references) pkts bytes target prot opt in out source destination 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 Chain HTTPIN (3 references) pkts bytes target prot opt in out source destination 10 400 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0Chain HTTPOUT (2 references) pkts bytes target protopt in out source destination 5 220 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination

2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination

122 23065 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination

129 20025 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

START Test 6A: Allow outbound HTTP

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

2 312 OTHERIN udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:53

0 0 OTHERIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:53

0 0 OTHERIN udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:68

0 0 OTHERIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:68

5 200 SSHIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22

117 22865 SSHIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22

0 0 SSHIN udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:22

5 200 CUSTOMDENYIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:0

10 400 HTTPIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spts:!1:1023 dpt:80

5 200 HTTPDENYIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spts:1:1023 dpt:80

0 0 HTTPIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 multiport sports 80,443

0 0 HTTPIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 multiport dports 80,443

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 16 packets, 3146 bytes)

2	135 OTHEROUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:53
0	0 OTHEROUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:53
0	0 OTHEROUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:68
0	0 OTHEROUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:68
5	200 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp spt:22
124	19825 SSHOUT tcp * *	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
0	0 SSHOUT udp * *	0.0.0.0/0	0.0.0.0/0	udp dpt:22
1	40 CUSTOMDENYOUT tcp '	* * 0.0.0	.0/0 0.0.0.	0/0 tcp dpt:0
0	0 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
5	220 HTTPOUT tcp * *	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination
5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination
1 40 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination
5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination 10 400 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination 5 220 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination 2 312 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination 2 135 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination 122 23065 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination 129 20025 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

END Test 6A: Allow outbound HTTP

Chain INPUT (policy DROP 0 packets, 0 bytes)

	(,	/ /		
pkts	bytes target prot o	pt in	out source	destinati	on
3	452 OTHERIN udp	* *	0.0.0.0/0	0.0.0.0/0	udp spt:53
0	0 OTHERIN tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:53
0	0 OTHERIN udp *	* *	0.0.0.0/0	0.0.0.0/0	udp spt:68
0	0 OTHERIN tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp spt:68
5	200 SSHIN tcp *	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
117	22865 SSHIN tcp	* *	0.0.0.0/0	0.0.0.0/0	tcp spt:22

```
0 SSHIN udp -- * * 0.0.0.0/0
   0
                                            0.0.0.0/0
                                                         udp dpt:22
      200 CUSTOMDENYIN tcp -- * * 0.0.0.0/0
                                                                tcp spt:0
                                                    0.0.0.0/0
      400 HTTPIN tcp -- * * 0.0.0.0/0
                                              0.0.0.0/0
                                                           tcp spts:!1:1023 dpt:80
      200 HTTPDENYIN tcp -- * * 0.0.0.0/0
                                                             tcp spts:1:1023 dpt:80
                                                 0.0.0.0/0
   5
      220 HTTPIN tcp -- * * 0.0.0.0/0
                                             0.0.0.0/0
                                                          multiport sports 80,443
       0 HTTPIN tcp -- * * 0.0.0.0/0
                                                         multiport dports 80,443
                                            0.0.0.0/0
   0
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target protopt in out source
                                                 destination
Chain OUTPUT (policy DROP 16 packets, 3146 bytes)
 pkts bytes target prot opt in out source
                                                 destination
      195 OTHEROUT udp -- * * 0.0.0.0/0
                                                             udp dpt:53
                                                0.0.0.0/0
       0 OTHEROUT tcp -- * * 0.0.0.0/0
                                               0.0.0.0/0
                                                            tcp dpt:53
       0 OTHEROUT udp -- * * 0.0.0.0/0
                                               0.0.0.0/0
                                                            udp dpt:68
   0
       0 OTHEROUT tcp -- * * 0.0.0.0/0
   0
                                              0.0.0.0/0
                                                           tcp dpt:68
      200 SSHOUT tcp -- * *
                                 0.0.0.0/0
                                              0.0.0.0/0
                                                           tcp spt:22
  124 19825 SSHOUT tcp -- * * 0.0.0.0/0
                                                0.0.0.0/0
                                                             tcp dpt:22
       0 SSHOUT udp -- * * 0.0.0.0/0
                                              0.0.0.0/0
                                                           udp dpt:22
       40 CUSTOMDENYOUT tcp -- * * 0.0.0.0/0 0.0.0.0/0
                                                                  tcp dpt:0
  10 400 HTTPOUT tcp -- * * 0.0.0.0/0 0.0.0.0/0
                                                            multiport dports 80,443
      220 HTTPOUT tcp -- * *
                                 0.0.0.0/0
                                               0.0.0.0/0
                                                            multiport sports 80,443
Chain CUSTOMALLOWIN (0 references)
       bytes target protopt in out source
                                                 destination
       0 ACCEPT all -- * * 0.0.0.0/0
                                            0.0.0.0/0
Chain CUSTOMALLOWOUT (0 references)
 pkts bytes target prot opt in out source
                                                 destination
       0 ACCEPT all -- * * 0.0.0.0/0
   0
                                            0.0.0.0/0
Chain CUSTOMDENYIN (1 references)
 pkts bytes target prot opt in out source
                                                 destination
   5 200 DROP all -- * *
                               0.0.0.0/0
                                            0.0.0.0/0
```

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination

1 40 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination

5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

O O DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination

15 620 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

15 620 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination

3 452 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination

3 195 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination 122 23065 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

```
Chain SSHOUT (3 references)
        bytes target prot opt in out source
                                                    destination
  129 20025 ACCEPT all -- *
                                    0.0.0.0/0
                                                  0.0.0.0/0
START Test 6B: Allow inbound HTTP
Chain INPUT (policy DROP 0 packets, 0 bytes)
        bytes target prot opt in
                                 out source
                                                    destination
       452 OTHERIN udp -- * *
                                    0.0.0.0/0
   3
                                                  0.0.0.0/0
                                                                udp spt:53
        O OTHERIN tcp -- * *
                                  0.0.0.0/0
                                                0.0.0.0/0
                                                              tcp spt:53
       0 OTHERIN udp -- * *
                                                              udp spt:68
   0
                                  0.0.0.0/0
                                                0.0.0.0/0
   0
        0 OTHERIN tcp -- * *
                                  0.0.0.0/0
                                                0.0.0.0/0
                                                              tcp spt:68
                                 0.0.0.0/0
                                                             tcp dpt:22
       200 SSHIN
                   tcp -- * *
                                               0.0.0.0/0
       22865 SSHIN tcp -- * * 0.0.0.0/0
                                                  0.0.0.0/0
  117
                                                                tcp spt:22
       0 SSHIN udp -- * *
                                                             udp dpt:22
                                 0.0.0.0/0
                                               0.0.0.0/0
   0
       200 CUSTOMDENYIN tcp -- * * 0.0.0.0/0
                                                       0.0.0.0/0
                                                                     tcp spt:0
       400 HTTPIN tcp -- * *
                                                               tcp spts:!1:1023 dpt:80
  10
                                   0.0.0.0/0
                                                 0.0.0.0/0
       200 HTTPDENYIN tcp -- * * 0.0.0.0/0
                                                    0.0.0.0/0
                                                                 tcp spts:1:1023 dpt:80
   5
   5
       220 HTTPIN tcp -- * *
                                  0.0.0.0/0
                                                0.0.0.0/0
                                                              multiport sports 80,443
                                                             multiport dports 80,443
   0
        O HTTPIN tcp -- * *
                                 0.0.0.0/0
                                               0.0.0.0/0
Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target prot opt in out source
                                                    destination
Chain OUTPUT (policy DROP 16 packets, 3146 bytes)
        bytes target prot opt in out source
                                                    destination
  pkts
       195 OTHEROUT udp -- * *
                                     0.0.0.0/0
                                                   0.0.0.0/0
                                                                 udp dpt:53
       0 OTHEROUT tcp -- * *
                                                 0.0.0.0/0
                                   0.0.0.0/0
                                                               tcp dpt:53
   0
        0 OTHEROUT udp -- * *
                                                                udp dpt:68
   0
                                    0.0.0.0/0
                                                  0.0.0.0/0
        0 OTHEROUT tcp -- * *
                                   0.0.0.0/0
                                                 0.0.0.0/0
   0
                                                               tcp dpt:68
   5
       200 SSHOUT tcp -- * *
                                   0.0.0.0/0
                                                 0.0.0.0/0
                                                               tcp spt:22
                                     0.0.0.0/0
  124 19825 SSHOUT tcp -- * *
                                                    0.0.0.0/0
                                                                 tcp dpt:22
        0 SSHOUT udp -- * *
   0
                                  0.0.0.0/0
                                                0.0.0.0/0
                                                              udp dpt:22
       40 CUSTOMDENYOUT tcp -- * * 0.0.0.0/0
                                                        0.0.0.0/0
   1
                                                                      tcp dpt:0
       400 HTTPOUT tcp -- *
                                    0.0.0.0/0
                                                  0.0.0.0/0
                                                                multiport dports 80,443
  10
       220 HTTPOUT tcp -- * *
   5
                                    0.0.0.0/0
                                                  0.0.0.0/0
                                                                multiport sports 80,443
```

Chain CUSTOMALLOWIN (0 references)

pkts bytes target prot opt in out source destination

Chain CUSTOMALLOWOUT (0 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYIN (1 references)

pkts bytes target prot opt in out source destination

5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CUSTOMDENYOUT (1 references)

pkts bytes target prot opt in out source destination

1 40 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYIN (1 references)

pkts bytes target prot opt in out source destination

5 200 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination

15 620 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

15 620 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

```
Chain OTHERIN (4 references)
 pkts bytes target prot opt in out source
                                                  destination
   3 452 ACCEPT all -- * *
                                 0.0.0.0/0
                                              0.0.0.0/0
Chain OTHEROUT (4 references)
 pkts bytes target prot opt in
                                out source
                                                  destination
   3 195 ACCEPT all -- * *
                                 0.0.0.0/0
                                               0.0.0.0/0
Chain SSHIN (3 references)
  pkts bytes target prot opt in out source
                                                  destination
  122 23065 ACCEPT all -- * *
                                   0.0.0.0/0
                                                 0.0.0.0/0
Chain SSHOUT (3 references)
  pkts bytes target prot opt in out source
                                                  destination
  129 20025 ACCEPT all -- * *
                                   0.0.0.0/0
                                                 0.0.0.0/0
END Test 6B: Allow inbound HTTP
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target prot opt in out source
                                                  destination
      452 OTHERIN udp -- * * 0.0.0.0/0
                                                 0.0.0.0/0
                                                              udp spt:53
       O OTHERIN tcp -- * *
                                 0.0.0.0/0
                                                            tcp spt:53
                                               0.0.0.0/0
                                               0.0.0.0/0
                                                             udp spt:68
   0
       0 OTHERIN udp -- * *
                                  0.0.0.0/0
       0 OTHERIN tcp -- * *
                                 0.0.0.0/0
                                               0.0.0.0/0
                                                            tcp spt:68
                                              0.0.0.0/0
                                                            tcp dpt:22
   5
       200 SSHIN
                  tcp -- * *
                                 0.0.0.0/0
  141 27638 SSHIN tcp -- * * 0.0.0.0/0
                                                 0.0.0.0/0
                                                              tcp spt:22
       0 SSHIN udp -- * *
                                                           udp dpt:22
                                0.0.0.0/0
                                              0.0.0.0/0
      200 CUSTOMDENYIN tcp -- * * 0.0.0.0/0
                                                      0.0.0.0/0
                                                                   tcp spt:0
                                               0.0.0.0/0
       800 HTTPIN tcp -- * * 0.0.0.0/0
                                                             tcp spts:!1:1023 dpt:80
                                                  0.0.0.0/0
       200 HTTPDENYIN tcp -- * * 0.0.0.0/0
                                                                tcp spts:1:1023 dpt:80
   5
       220 HTTPIN tcp -- * * 0.0.0.0/0
                                               0.0.0.0/0
                                                            multiport sports 80,443
                                              0.0.0.0/0
   0
        0 HTTPIN tcp -- * *
                                0.0.0.0/0
                                                           multiport dports 80,443
Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

pkts 3 0 0 0 5 149	195 OTHEROUT udp * * 0.0.0.0/0 0 OTHEROUT tcp * * 0.0.0.0/0 0 OTHEROUT udp * * 0.0.0.0/0 0 OTHEROUT tcp * * 0.0.0.0/0 200 SSHOUT tcp * * 0.0.0.0/0	destination 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0	tcp dpt:53 udp dpt:68 tcp dpt:68 tcp spt:22
1	40 CUSTOMDENYOUT tcp * * 0.0.0		
	400 HTTPOUT tcp * * 0.0.0.0/0		
	440 HTTPOUT tcp * * 0.0.0.0/0		
Chain C	CUSTOMALLOWIN (0 references) bytes target prot opt in out source	destination	
pkts	bytes target prot opt in out source 0 ACCEPT all * * 0.0.0.0/0		
pkts	bytes target prot opt in out source 200 DROP all * * 0.0.0.0/0		
pkts	CUSTOMDENYOUT (1 references) bytes target prot opt in out source 40 DROP all * * 0.0.0.0/0		
pkts 5	ITTPDENYIN (1 references) bytes target prot opt in out source 200 DROP all * * 0.0.0.0/0 0 DROP all * * 0.0.0.0/0	0.0.0.0/0	

Chain HTTPDENYOUT (0 references)

pkts bytes target prot opt in out source destination

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPIN (3 references)

pkts bytes target prot opt in out source destination

25 1020 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain HTTPOUT (2 references)

pkts bytes target prot opt in out source destination

20 840 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHERIN (4 references)

pkts bytes target prot opt in out source destination

3 452 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OTHEROUT (4 references)

pkts bytes target prot opt in out source destination

3 195 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHIN (3 references)

pkts bytes target prot opt in out source destination

146 27838 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0

Chain SSHOUT (3 references)

pkts bytes target prot opt in out source destination 154 24010 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0