

Όνοματεπώνυμο: Ζευγολατάκος Παναγιώτης	Όνομα PC: panos-PC
Ομάδα: 1	Ημερομηνία: 11/05/2021

Εργαστηριακή Άσκηση 10

Τείχη προστασίας (Firewalls) και NAT

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 kldload ipfw

1.2 kldstat

1.3 Όχι, παίρνω μήνυμα λάθους Permission denied.

1.4 ipfw list

Υπάρχει μόνο ο προεπιλεγμένος κανόνας.

1.5 ipfw show

Εμφανίζει στοιχεία για τη χρήση του κανόνα.

1.6 ipfw zero

1.7 ipfw add 100 allow all from any to any via lo0

1.8 Ναι.

1.9 Όχι, παίρνω μήνυμα λάθους Permission denied.

1.10 ipfw add allow icmp from any to any

1.11 200

1.12 Μπορώ να κάνω και τα 2.

1.13 Δεν μπορώ επειδή χρησιμοποιούνται πακέτα UDP. Θα λάβω απάντηση αν βάλω επιλογή -I (ICMP).

1.14 ipfw add allow udp from any to any 33434-33534

1.15 Όχι (Permission denied).

1.16 ipfw add allow tcp from any to any established

ipfw add allow tcp from me to any setup

1.17 ipfw zero

1.18 ipfw show

Χρησιμοποιήθηκε 57 φορές ο κανόνας 00400 και 1 φορά ο κανόνας 00500 (πρώτο πακέτο τριμερούς χειραψίας):

```
00400 57 10198 allow tcp from any to any established
00500 1 60 allow tcp from me to any setup
```

1.19 Όχι, εφόσον έχω ορίσει κανόνες μόνο για απερχόμενες συνδέσεις.

1.20 `service ftpd onestart`

1.21 Ναι, μπορώ:

```
ftp 192.168.1.3
cd /usr/bin
ls
get flex++
bye
```

2

2.1 `kldload ipfw`

2.2 Όχι (Permission denied).

2.3 `ipfw add 100 allow all from any to any via lo0`

2.4 `ipfw add allow icmp from me to any icmptypes 8`

2.5 Όχι.

2.6 `ipfw show`

Από τους μετρητές πακέτων παρατηρώ πως περνούν τα requests, αλλά όχι τα replies.

2.7 `ipfw delete 200`

`ipfw add allow icmp from me to any icmptypes 8 keep-state`

Ναι, μπορώ.

2.8 Ναι, μπορώ.

2.9 Όχι, επειδή ο κανόνας που θέσαμε στο ερώτημα 2.7 είναι δυναμικός κανόνας (keep-state) που επιτρέπει την επικοινωνία μεταξύ των δύο PC (με αυτόν και τα δύο έχουν πλέον κανόνα 'allow icmp from me to any'), επομένως χωρίς να τρέχει το ping από το PC2 δε θα πετύχει.

2.10 `ipfw add allow icmp from any to me icmptypes 8 keep-state`

2.11 Βλέπω το δυναμικό κανόνα που έχει δημιουργηθεί:

```
## Dynamic rules (1):
00300  9  756 (5s) STATE icmp 192.168.1.2 0 <-> 192.168.1.3 0
```

2.12 Πλέον εμφανίζονται μόνο οι στατικοί κανόνες.

2.13 `ipfw add allow udp from any to me 33434-33534`

`ipfw add allow icmp from me to any icmptypes 3`

2.14 `ipfw add allow udp from me to any 33434-33534`

`ipfw add allow icmp from any to me icmptypes 3`

2.15 `ipfw add allow icmp from any to any` (υπάρχει από την προηγούμενη άσκηση)

2.16 `ipfw add allow tcp from 192.168.1.0/24 to me 22 setup keep-state`

2.17 `ssh lab@192.168.1.3`

2.18 `ipfw add allow tcp from me to any 22 setup keep-state`

2.19 `ipfw add allow tcp from 192.168.1.0/24 to me 22 setup`

2.20 Ναι.

2.21 ipfw add allow tcp from any to me 21 setup keep-state

2.22 Η εντολή `cd` χρησιμοποιεί TCP control connection, ενώ η εντολή `ls` χρησιμοποιεί TCP data connection, την οποία δεν επιτρέπει το firewall.

2.23 ipfw add allow tcp from any 1024-65535 to me 1024-65535 setup keep-state

2.24 Ναι.

2.25 PC1: ipfw add allow tcp from any 20 to me 1024-65535 setup

PC2: ipfw add allow tcp from me 20 to any 1024-65535 setup keep-state

2.26 Σε FTP Active ο πελάτης πρέπει να δέχεται συνδέσεις σε δυναμικά ports, ενώ σε FTP Passive υπάρχει λιγότερη ασφάλεια, εφόσον χρειάζονται παραπάνω κανόνες που να επιτρέπουν συνδέσεις.

2.27 kldunload ipfw

3

3.1 route add default 192.168.1.1

3.2 cli

configure terminal

hostname R1

interface em0

ip address 192.0.2.2/30

exit

interface em1

ip address 192.0.2.6/30

exit

3.3 sysrc hostname=SRV1

ifconfig em0 192.0.2.5/30

route add default 192.0.2.6

3.4 service ftpd onestart

3.5

```
root@FW1:~ # kldstat
Id Refs Address      Size      Name
 1    7 0xc0400000 1276c0c   kernel
 2    2 0xc614b000 12000     ipfw.ko
 3    1 0xc616a000 4000      ipfw_nat.ko
 4    1 0xc616e000 e000      libalias.ko
```

3.6 To IPFW.

3.7 UNKNOWN.

3.8 11, ο τελευταίος είναι ο προεπιλεγμένος 'deny ip from any to any'.

3.9 ipfw nat show config

3.10 Όχι.

3.11 Όχι.

3.12 ipfw nat 123 config ip 192.0.2.1 unreg_only reset

3.13 `ipfw add nat 123 all from any to any`

3.14 Ναι.

3.15 `ipfw show`

Ο κανόνας του ερωτήματος 3.13

3.16 `tcpdump -n -i em0`

3.17 `ipfw show && ipfw zero`

3.18 Η διεύθυνση του FW1 στο WAN1.

3.19 Η διεύθυνση του R1 στο WAN1.

3.20 Έχει εφαρμοσθεί ο κανόνας που του ερωτήματος 3.13, 204(=4*51) φορές, όπου 51 είναι τα πακέτα Echo Request που στάλθηκαν και εφαρμόστηκε μια φορά πριν τη μετάφραση και μια μετά τη μετάφραση, δύο φορές για το ζεύγος request και reply, άρα 4*51.

3.21 Ναι.

3.22 Ο κανόνας του ερωτήματος 3.13, αλλά δεν ωθείται προς μετάφραση διευθύνσεων, εφόσον η διεύθυνση των πακέτων δεν είναι private.

3.23 Ναι.

3.24 Ο R1 δεν μπορεί να προωθήσει τα πακέτα στο LAN1, επομένως είναι θέμα δρομολόγησης.

3.25 `ipfw nat 123 config 192.0.2.1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1`

3.26 Ναι, και έχω συνδεθεί στο PC2 (ifconfig για να δω τη διεύθυνση των καρτών δικτύου).

3.27 `ipfw nat 123 config ip 192.0.2.1 unreg_only reset redirect_port tcp 192.168.1.3:22 192.0.2.1:22`

3.28 Στο PC2 και το εξακριβώνω πάλι κοιτώντας τη διεύθυνση των καρτών δικτύου.

3.29 Στο PC2 και το εξακριβώνω πάλι κοιτώντας τη διεύθυνση των καρτών δικτύου.

3.30 Ναι.

3.31 Το FW1.

3.32 Το PC2.

4

4.1 Όχι.

4.2 Γίνονται δεκτά, αλλά συνεχίζουν στη λίστα κανόνων και χρησιμοποιείται ο προεπιλεγμένος κανόνας.

4.3 `ipfw add 1100 allow all from any to any via em0`

4.4 Ναι.

4.5 Το FW1.

4.6 Ο κανόνας του ερωτήματος 4.3

4.7 `ipfw add 3000 nat 123 all from any to any xmit em1`

4.8 `ipfw add 3001 allow all from any to any`

4.9 ipfw add 2000 nat 123 all from any to any recv em1

4.10 ipfw add 2001 check-state

4.11 To FW1.

4.12 To FW1.

4.13 To FW1.

4.14 To PC2.

4.15 To FW1.

4.16 Ναι.

4.17 Ναι.

4.18 Ναι.

4.19 ipfw add 2999 deny all from any to any via em1

4.20 Κανένα.

4.21 ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state

4.22 Ναι.

4.23 ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 keep-state

4.24 Ναι.

4.25 ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state

4.26 To FW1.

4.27 ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state

4.28 Στο PC2 (και στο FW1 από το PC1).

4.29 Όχι.

5

5.1 192.168.1.1/24

5.2 10.0.0.1/30

5.3 97% (έβαλα 1024MB όταν το έφτιαχνα)

Memory usage

3%

5.4 Παρατηρώ 4 σε σωστή δικτύωση.

5.5 172.22.1.1/24

5.6 fw

5.7

System: General setup

Hostname

fw1

name of the firewall host, without domain part
e.g. *firewall*

5.8 Όχι.

5.9 Interfaces/WAN

Static IP configuration	
IP address	192.0.2.1 / 30
Gateway	192.0.2.2

☒ **Block private networks**

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Save

5.10 Ναι:

	Proto	Source	Port	Destination	Port	Description
✗	*	RFC 1918 networks	*	*	*	Block private networks

5.11 Όχι.

5.12

☒ **Enable DNS forwarder**

5.13

Enable IPv4 DHCP server on LAN interface		<input checked="" type="checkbox"/> Enable
Deny unknown clients	<input type="checkbox"/> Only respond to reserved clients listed below.	
Subnet	192.168.1.0	
Subnet mask	255.255.255.0	
Available range	192.168.1.1 - 192.168.1.254	
Range	192.168.1.2 to 192.168.1.3	

5.14 dhclient em0

```
DHCP OFFER from 192.168.1.1
DHCP REQUEST on em0 to 255.255.255.255 port 67
DHCP ACK from 192.168.1.1
bound to 192.168.1.2 -- renewal in 3600 seconds.
```

```
netstat -rn
```

```
Internet:
Destination      Gateway          Flags    Refs      Use    Netif  Expire
default          192.168.1.1     UGS      0         0      em0
```

5.15 Για να μη χρειαστεί να οριστεί DNS Server manually.

5.16 DHCP Leases.

5.17

Diagnostics: ARP table

	IP address	MAC address	Hostname	Interface
<input type="checkbox"/>	172.22.1.1	08:00:27:c0:77:6a		DMZ
<input type="checkbox"/>	192.168.56.1	0a:00:27:00:00:0c		MNG
<input type="checkbox"/>	192.168.56.2	08:00:27:04:2b:2f		MNG
<input type="checkbox"/>	192.0.2.1	08:00:27:2f:b8:9c		WAN
<input type="checkbox"/>	192.168.1.1	08:00:27:71:4c:82		LAN
<input type="checkbox"/>	192.168.1.2	08:00:27:07:e6:30	PC1	LAN

5.18 Όχι.

5.19 Βλέπω log για το ring που έκανα και την απόρριψή του.

5.20 3

5.21 Κανέναν.

5.22 (τα υπόλοιπα τα άφησα ως έχουν)

Firewall: Rules: Edit

Action	<div>Pass</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>LAN</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>any</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>

5.23 Ναι.

5.24 Όχι.

5.25 arp -a

```
? (192.0.2.2) at 08:00:27:3c:bd:9a on em0 permanent [ethernet]
? (192.0.2.1) at 08:00:27:2f:b8:9c on em0 expires in 1081 seconds [ethernet]
```

5.26

Firewall: Rules: Edit

Action	<div>Pass</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>WAN</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>ICMP</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
ICMP type	<div>any</div> <p>If you selected ICMP for the protocol above, you may specify an ICMP type here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any</div> Address: <div></div> / <div></div>
Source port range	<div>from: (other)</div> <div></div> <div>to: (other)</div> <div></div> Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>WAN address</div> Address: <div></div> / <div></div>

5.27 Ναι.

5.28 Όχι, εφόσον ο R1 δεν ξέρει πως να δρομολογήσει πακέτα στο LAN1.

5.29 Ναι. Επιτρέπει την απερχόμενη κίνηση από τη WAN1 προς την κάρτα δικτύου.

5.30 Όχι, επειδή δεν ξέρει πως να απαντήσει ο SRV1.

5.31 route add default 172.22.1.1

5.32 Ναι.

5.33 Όχι, εξαιτίας του firewall.

5.34 Όχι, εξαιτίας του firewall.

5.35

Firewall: Rules: Edit

Action	<div>Pass</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>DMZ</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>any</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
ICMP type	<div>any</div> <p>If you selected ICMP for the protocol above, you may specify an ICMP type here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>DMZ subnet</div> Address: <div></div> / <div></div>
Source port range	from: <div>(other)</div> <div></div> to: <div>(other)</div> <div></div> Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port
Destination	<input checked="" type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>LAN subnet</div> Address: <div></div> / <div></div>

5.36 Ναι.

5.37 Ναι.

5.38 Όχι, επειδή δεν ξέρει πως να το δρομολογήσει.

5.39 Ναι, αφού επιτρέπεται όλη η απερχόμενη κίνηση (πλην του LAN1).

5.40 dhclient em0

```
DHCPOFFER from 192.168.1.1
DHCPREQUEST on em0 to 255.255.255.255 port 67
DHCPACK from 192.168.1.1
bound to 192.168.1.3 -- renewal in 3600 seconds.
```

netstat -rn

```
Internet:
Destination      Gateway          Flags    Refs      Use  Netif  Expire
default          192.168.1.1     UGS             0        0    em0
```

5.41

Firewall: Rules: Edit

Action	<div>Block ▾</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>any ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
ICMP type	<div>any ▾</div> <p>If you selected ICMP for the protocol above, you may specify an ICMP type here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias ▾</div></p> <p>Address: <div>192.168.1.3</div> / <div>▾</div></p>
Source port range	<p>from: <div>(other) ▾</div> <div></div></p> <p>to: <div>(other) ▾</div> <div></div></p> <p>Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port</p>
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias ▾</div></p> <p>Address: <div>172.22.1.2</div> / <div>▾</div></p>



5.42 Πριν, για να εκτελείται πρώτος και να γίνει σωστά το φιλτράρισμα:

LAN

WAN

MNG

DMZ

Proto	Source	Port	Destination	Port	Description
<input type="checkbox"/> 	*	*	*	*	
<input checked="" type="checkbox"/> 	*	192.168.1.3	172.22.1.2	*	

←

→

←


→


+


←


×


+


 pass


 block


 reject

 log

 pass (disabled)

 block (disabled)

 reject (disabled)

 log (disabled)

5.43 'O χ i.

5.44 Ναι, εφόσον ο κανόνας απαγορεύει μόνο την διεύθυνση IP του SRV1 (172.22.1.1).

6

```
6.1 cli
configure terminal
ip route 203.0.118.0/24 192.0.2.1
```

6.2☒ **Enable advanced outbound NAT****Save****6.3****Firewall: NAT: Edit outbound mapping**

Interface	<div>WAN ▾</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
Source	<div>192.168.1.2 / 32 ▾</div> <div>Enter the source network for the outbound NAT mapping.</div>
Destination	<div><input type="checkbox"/> not Use this option to invert the sense of the match.</div> <div>Type: any ▾</div> <div>Address: <div></div> / 24 ▾</div> <div>Enter the destination network for the outbound NAT mapping.</div>
Target	<div>203.0.118.14</div> <div>Packets matching this rule will be mapped to the IP address given here. Leave blank to use the selected interface's IP address.</div>
Portmap	<div><input type="checkbox"/> Avoid port mapping This option avoids remapping of the source port number for outbound packets whenever possible (i.e. when there is no other mapping for the same port). This may help with software that insists on the source ports being left unchanged when applying NAT (such as some IPsec VPN gateways, games and VoIP applications).</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>

Save**6.4**

Firewall: NAT: Edit outbound mapping

Interface	<div>WAN</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
Source	<div>192.168.1.3 / 32</div> <div>Enter the source network for the outbound NAT mapping.</div>
Destination	<div><input type="checkbox"/> not Use this option to invert the sense of the match.</div> <div>Type: any</div> <div>Address: / 24</div> <div>Enter the destination network for the outbound NAT mapping.</div>
Target	<div>203.0.118.15</div> <div>Packets matching this rule will be mapped to the IP address given here. Leave blank to use the selected interface's IP address.</div>
Portmap	<div><input type="checkbox"/> Avoid port mapping This option avoids remapping of the source port number for outbound packets whenever possible (i.e. when there is no other mapping for the same port). This may help with software that insists on the source ports being left unchanged when applying NAT (such as some IPsec VPN gateways, games and VoIP applications).</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>

Save

6.5 tcpdump -i em0

6.6 Ναι και φτάνουν με τη διεύθυνση 203.0.118.14

6.7 Ναι και φτάνουν με τη διεύθυνση 203.0.118.15

6.8 Αποτυγχάνει επειδή είναι outbound NAT.

6.9

Firewall: NAT: Edit Server NAT

External IP address	<div>203.0.118.18</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>

Save

6.10





Firewall: NAT: Edit

Interface	<div>WAN ▾</div> <p>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</p>
External address	<div>203.0.118.18 () ▾</div> <p>If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define IP addresses on the Server NAT page first).</p>
Protocol	<div>TCP ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
External port range	<p>from: <div>SSH ▾</div> <div></div></p> <p>to: <div>SSH ▾</div> <div></div></p> <p>Specify the port or port range on the firewall's external address for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port</p>
NAT IP	<div>172.22.1.2</div> <p>Enter the internal IP address of the server on which you want to map the ports. e.g. <i>192.168.1.12</i></p>
Local port	<div>SSH ▾</div> <div></div> <p>Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above</p>
Description	<div></div> <p>You may enter a description here for your reference (not parsed).</p>

☒ **Auto-add a firewall rule to permit traffic through this NAT rule**

Save

6.11 Ο κανόνας που επιτρέπει την κίνηση από any port 22 προς το SRV1:

<input type="checkbox"/>		TCP	*	*	172.22.1.2	22 (SSH)	NAT	  
--------------------------	---	-----	---	---	------------	----------	-----	---

6.12 Ναι, συνδέομαι στο SRV1.

6.13 Όχι, εφόσον ο κανόνας που όρισα αφορά μόνο το SSH port.

6.14 Ναι και τα πακέτα χρησιμοποιούν τη διαδρομή PC2 → FW1 → R1 → FW1 → SRV1, το οποίο το εξακρίβωσα με την καταγραφή στο R1, όπου επικοινωνεί με τέτοιον τρόπο με τη διεύθυνση 203.1.118.15 (PC2).

6.15 Όχι, εφόσον στα πακέτα του PC1 δε γίνεται μετάφραση NAT και δεν απαντάει το R1.

6.16 Ναι, εφόσον δημιουργούνται αυτόματα κανόνες NAT για outbound κίνηση και τα πακέτα παίρνουν τη διεύθυνση 192.0.2.1

6.17 Ναι. Όχι.

6.18 Αποτυγχάνει επειδή χωρίς το advanced outbound NAT, το FW1 στέλνει στο SRV1 πακέτα με τη δική του διεύθυνση ως source αντί για την 203.0.118.15 (PC2), επομένως όταν το SRV1 στέλνει Syn-Ack, αυτό στέλνει Reset.

6.19 Σύμφωνα με τη σημείωση που βρίσκεται στην καρτέλα Inbound NAT, δεν είναι εφικτό να γίνει πρόσβαση σε υπηρεσίες που χρησιμοποιούν NAT χρησιμοποιώντας τη WAN διεύθυνση IP από κάποιο LAN, για αυτό και αποτυγχάνει το ssh:

Note:

It is not possible to access NATed services using the WAN IP address from within LAN (or an optional network).

7

7.1

<input checked="" type="checkbox"/>	Connect Network Adapter 1
<input checked="" type="checkbox"/>	Connect Network Adapter 2
<input checked="" type="checkbox"/>	Connect Network Adapter 3
<input checked="" type="checkbox"/>	Connect Network Adapter 4

7.2

IP configuration	
Bridge with	<input type="text" value="none"/>
IP address	<input type="text" value="192.168.56.3"/> / <input type="text" value="24"/>
<input type="button" value="Save"/>	

7.3

<input checked="" type="checkbox"/>	Connect Network Adapter 1
<input checked="" type="checkbox"/>	Connect Network Adapter 2
<input checked="" type="checkbox"/>	Connect Network Adapter 3
<input checked="" type="checkbox"/>	Connect Network Adapter 4

7.4 Ναι.

7.5

Hostname	<input type="text" value="fw2"/>
name of the firewall host, without domain part e.g. <i>firewall</i>	

7.6

Static IP configuration	
IP address	<input type="text" value="192.0.2.5"/> / <input type="text" value="30"/>
Gateway	<input type="text" value="192.0.2.6"/>

☒ **Block private networks**

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

7.7

IP address	192.168.2.1 / 24
Save	

7.8

```
m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
Enter a number: 5
```

7.9

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN Choose on which interface packets must come in to match this rule.
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
ICMP type	any If you selected ICMP for the protocol above, you may specify an ICMP type here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: any Address: /
Source port range	from: (other) to: (other) Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: any Address: /

7.10

Action	<div>Pass ▾</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>WAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>ICMP ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
ICMP type	<div>any ▾</div> <p>If you selected ICMP for the protocol above, you may specify an ICMP type here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any ▾</div> Address: <div></div> / <div>▾</div>
Source port range	from: <div>(other) ▾</div> <div></div> to: <div>(other) ▾</div> <div></div> Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>WAN address ▾</div> Address: <div></div> / <div>▾</div>

7.11 `ifconfig em0 192.168.2.2/24``route add default 192.168.2.1`

7.12 Ναί.

7.13 Ναί.

7.14 Όχι, εφόσον ο R1 δεν ξέρει πως να τα δρομολογήσει.

7.15

☒ **Enable IPsec****Save**

VPN: IPsec: Edit tunnel

Mode	Tunnel
Disabled	<input type="checkbox"/> Disable this tunnel Set this option to disable this tunnel without removing it from the list.
Interface	LAN <input type="text"/> Select the interface for the local endpoint of this tunnel.
NAT-T	<input type="checkbox"/> Enable NAT Traversal (NAT-T) Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
DPD interval	<input type="text"/> seconds Enter a value here to enable Dead Peer Detection (e.g. 60 seconds).
Local subnet	Type: LAN subnet <input type="text"/> Address: <input type="text"/> / <input type="text"/>
Remote subnet	192.168.2.0 / 24 <input type="text"/>
Remote gateway	192.0.2.5 <input type="text"/> Enter the public IP address or host name of the remote gateway. For ipv6, use an ipv6 IP address.
Description	<input type="text"/> You may enter a description here for your reference (not parsed).
Pre-Shared Key	panos <input type="text"/>

7.16

	Proto	Source	Port	Destination	Port	Description
<input type="checkbox"/>	*	*	*	*	*	Default IPsec VPN

7.17 Όχι:

Diagnostics: IPsec

SAD	SPD
No IPsec security associations.	

7.18 Ναι:

SAD	SPD																		
<table border="1"> <thead> <tr> <th></th> <th>Source</th> <th>Destination</th> <th>Direction</th> <th>Protocol</th> <th>Tunnel endpoints</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>192.168.2.0/24</td> <td>192.168.1.0/24</td> <td>➔</td> <td>ESP</td> <td>192.0.2.5 - 192.168.1.1</td> </tr> <tr> <td><input type="checkbox"/></td> <td>192.168.1.0/24</td> <td>192.168.2.0/24</td> <td>➔</td> <td>ESP</td> <td>192.168.1.1 - 192.0.2.5</td> </tr> </tbody> </table>			Source	Destination	Direction	Protocol	Tunnel endpoints	<input type="checkbox"/>	192.168.2.0/24	192.168.1.0/24	➔	ESP	192.0.2.5 - 192.168.1.1	<input type="checkbox"/>	192.168.1.0/24	192.168.2.0/24	➔	ESP	192.168.1.1 - 192.0.2.5
	Source	Destination	Direction	Protocol	Tunnel endpoints														
<input type="checkbox"/>	192.168.2.0/24	192.168.1.0/24	➔	ESP	192.0.2.5 - 192.168.1.1														
<input type="checkbox"/>	192.168.1.0/24	192.168.2.0/24	➔	ESP	192.168.1.1 - 192.0.2.5														
➔ incoming (as seen by firewall) ➔ outgoing (as seen by firewall)																			

7.19

☒ **Enable IPsec**

Save

VPN: IPsec: Edit tunnel

Mode	Tunnel
Disabled	<input type="checkbox"/> Disable this tunnel Set this option to disable this tunnel without removing it from the list.
Interface	<div>LAN ▾</div> Select the interface for the local endpoint of this tunnel.
NAT-T	<input type="checkbox"/> Enable NAT Traversal (NAT-T) Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
DPD interval	<div></div> seconds Enter a value here to enable Dead Peer Detection (e.g. 60 seconds).
Local subnet	Type: <div>LAN subnet ▾</div> Address: <div></div> / <div>▾</div>
Remote subnet	<div>192.168.1.0</div> / <div>24 ▾</div>
Remote gateway	<div>192.0.2.1</div> Enter the public IP address or host name of the remote gateway. For ipv6, use an ipv6 IP address.
Description	<div></div> You may enter a description here for your reference (not parsed).

Pre-Shared Key	<div>panos</div>
-----------------------	------------------

7.20 Όχι:

Diagnostics: IPsec

SAD
SPD

No IPsec security associations.

7.21 Ναι:

SAD
SPD

	Source	Destination	Direction	Protocol	Tunnel endpoints
<input type="checkbox"/>	192.168.1.0/24	192.168.2.0/24	➔	ESP	192.0.2.1 - 192.168.2.1
<input type="checkbox"/>	192.168.2.0/24	192.168.1.0/24	➔	ESP	192.168.2.1 - 192.0.2.1

➔ incoming (as seen by firewall)
 ➔ outgoing (as seen by firewall)

7.22 Ναι.

7.23 Ναι.

7.24 Έχουν προστεθεί 2 σχέσεις:

SAD

SPD

	Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
<input type="checkbox"/>	192.0.2.1	192.0.2.5	ESP	079bb5a8	3des-cbc	hmac-sha1
<input type="checkbox"/>	192.0.2.5	192.0.2.1	ESP	03303493	3des-cbc	hmac-sha1

7.25 Έχουν προστεθεί 2 σχέσεις:

SADSPD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.0.2.5	192.0.2.1	ESP	03303493	3des-cbc	hmac-sha1
192.0.2.1	192.0.2.5	ESP	079bb5a8	3des-cbc	hmac-sha1

7.26 tcpdump -i em0 -vvv

7.27 Όχι.

7.28 Πακέτα ESP, με πηγή και προορισμό τις διεπαφές των FW1, FW2 στα WAN, ενώ δεν υπάρχει πουθενά πληροφορία για τα PC1, PC2:

```
192.0.2.1 > 192.0.2.5: ESP(spi=0x079bb5a8,seq=0xf), length 116
07:08:09.113181 IP (tos 0x0, ttl 63, id 3192, offset 0, flags [none], proto ESP
(50), length 136)
192.0.2.5 > 192.0.2.1: ESP(spi=0x03303493,seq=0xf), length 116
```

7.29 Ναι και αυτό που έχει αλλάξει είναι ότι πλέον δρομολογούνται στο FW2 με το σωστό source IP.

7.30 Παρατηρώ πακέτα είδους ssh με πηγή τη διεύθυνση 192.0.2.5 και με προορισμό τη διεύθυνση 203.0.118.18 και δεν είναι κρυπτογραφημένα με IPsec, εφόσον επικοινωνούν υποδίκτυα για τα οποία δεν έχουν οριστεί IPsec:

```
07:16:01.534432 IP (tos 0x0, ttl 62, id 1888, offset 0, flags [DF], proto TCP (6
), length 52)
192.0.2.5.33434 > 203.0.118.18.ssh: Flags [.], cksum 0x217b (correct), seq 4
8, ack 1496, win 1018, options [nop,nop,TS val 37825243 ecr 3564639299], length
0
```