Υποδομές Cloud

Διάλεξη 5η

Θωμάς Καμαλάκης

Χαροκόπειο Πανεπιστήμιο Αθηνών

Χειμερινό Εξάμηνο, 2024

Περιεχόμενα

1 SDN

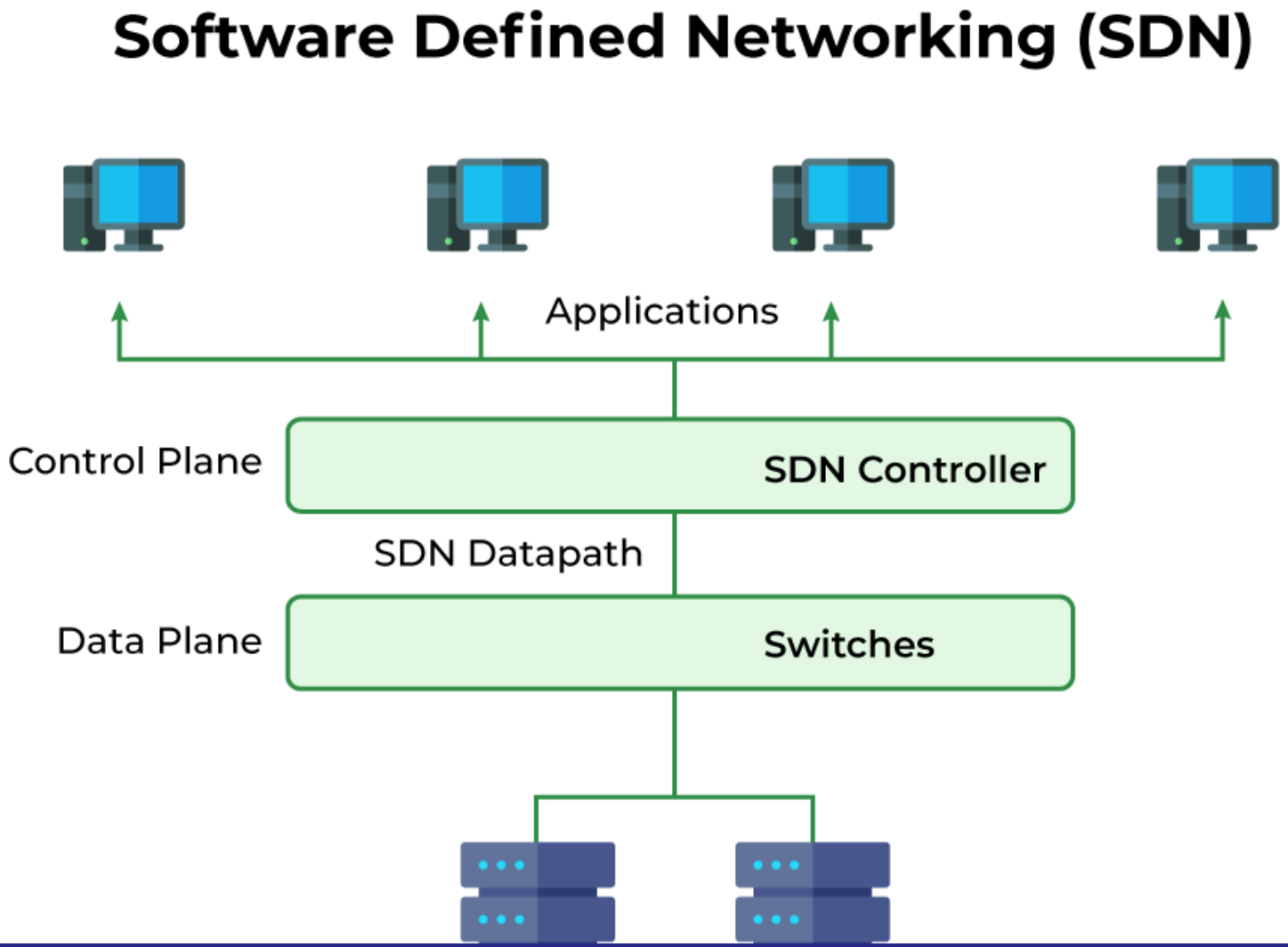
2 SDN + IPfire

3 Virtualmin

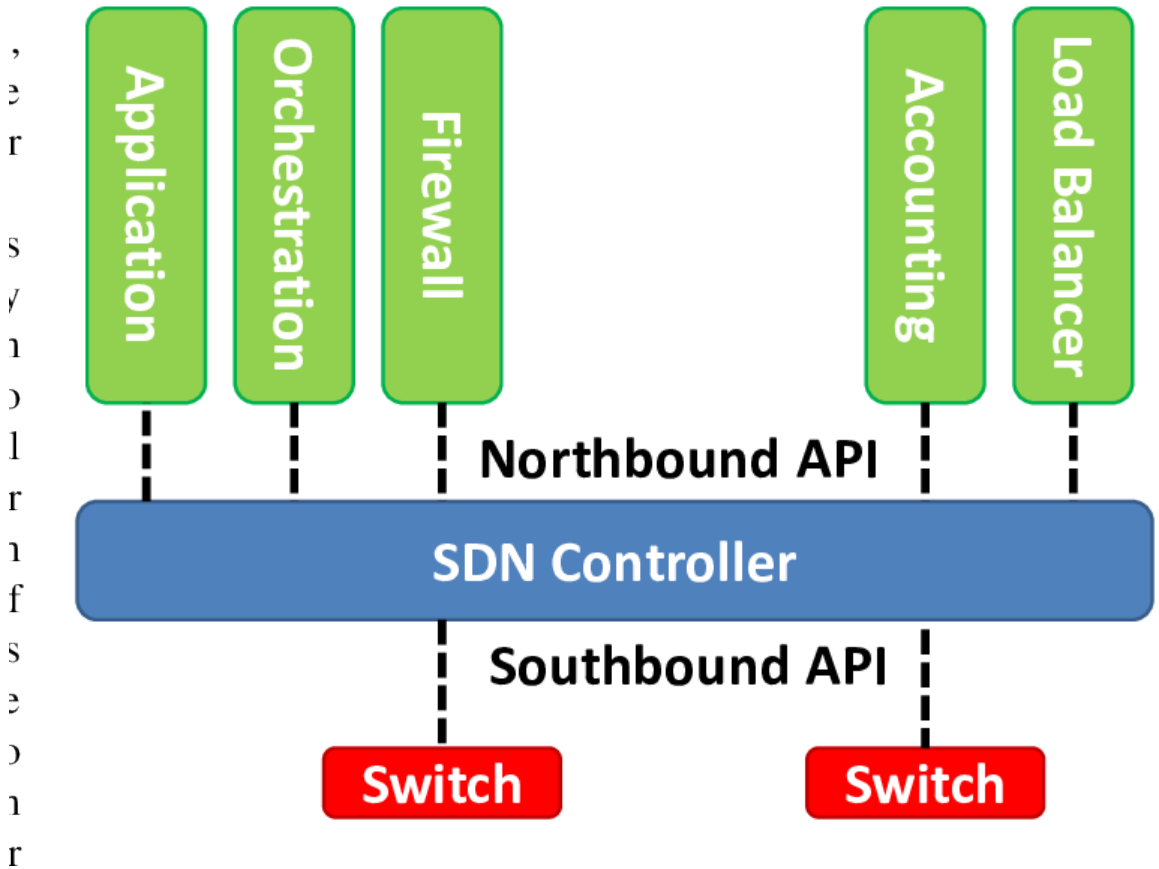
Εισαγωγικά

- Software Defined Networking (SDN): Μία τεχνική που στοχεύει στον κεντρικό έλεγχο και τη δυναμική διαχείριση των δικτυακών υποδομών μέσω λογισμικού.
- Διαχωρίζει το επίπεδο ελέγχου του δικτύου (control plane) από το επίπεδο δεδομένων (data plane).
- Το δίκτυο ελέγχεται από έναν κεντρικό ελεγκτή (controller) μέσω λογισμικού, κάτι που επιτρέπει ευκολότερη διαμόρφωση και διαχείριση.
- Μπορούμε να προγραμματίσουμε τη συμπεριφορά του δικτύου για να καθορίσουμε τις ροές των δεδομένων.

SDN


Software Defined Networking (SDN)
Applications
Control Plane
SDN Controller
SDN Datapath
Data Plane
Switches

SDN APIs


Application
Orchestration
Firewall
Accounting
Load Balancer
Northbound API
SDN Controller
Southbound API
Switch
Switch

SDN APIs

- Southbound APIs: διεπαφές μεταξύ του κεντρικού ελεγκτή SDN και τον εξοπλισμό δικτύου (switches κτλ).
- Στέλνουν εντολές από το control plane στο επίπεδο data plane για την διαχείριση της κυκλοφορία δεδομένων στο φυσικό δίκτυο.
- Παράδειγμα: OpenFlow.

SDN APIs

- Northbound APIs: επιτρέπουν την επικοινωνία μεταξύ του SDN ελεγκτή και των εφαρμογών ή των ανώτερων επιπέδων διαχείρισης.
- Με τον τρόπο αυτό οι εφαρμογές εκμεταλλεύονται τη λειτουργικότητα του SDN ελεγκτή, ώστε να μπορούν να προγραμματίζουν και να διαχειρίζονται το δίκτυο με βάση τις ανάγκες τους.

SDN χαι Proxmox

- Μια ζώνη (zone) ορίζει ένα εικονικά απομονωμένο δίκτυο.
- Οι ζώνες μπορεί να περιορίζονται σε συγκεκριμένους κόμβους και καθορισμένα δικαιώματα
- Διαφορετικές τεχνολογίες μπορούν να χρησιμοποιηθούν για την υλοποίηση:

‘

SDN χαι Proxmox

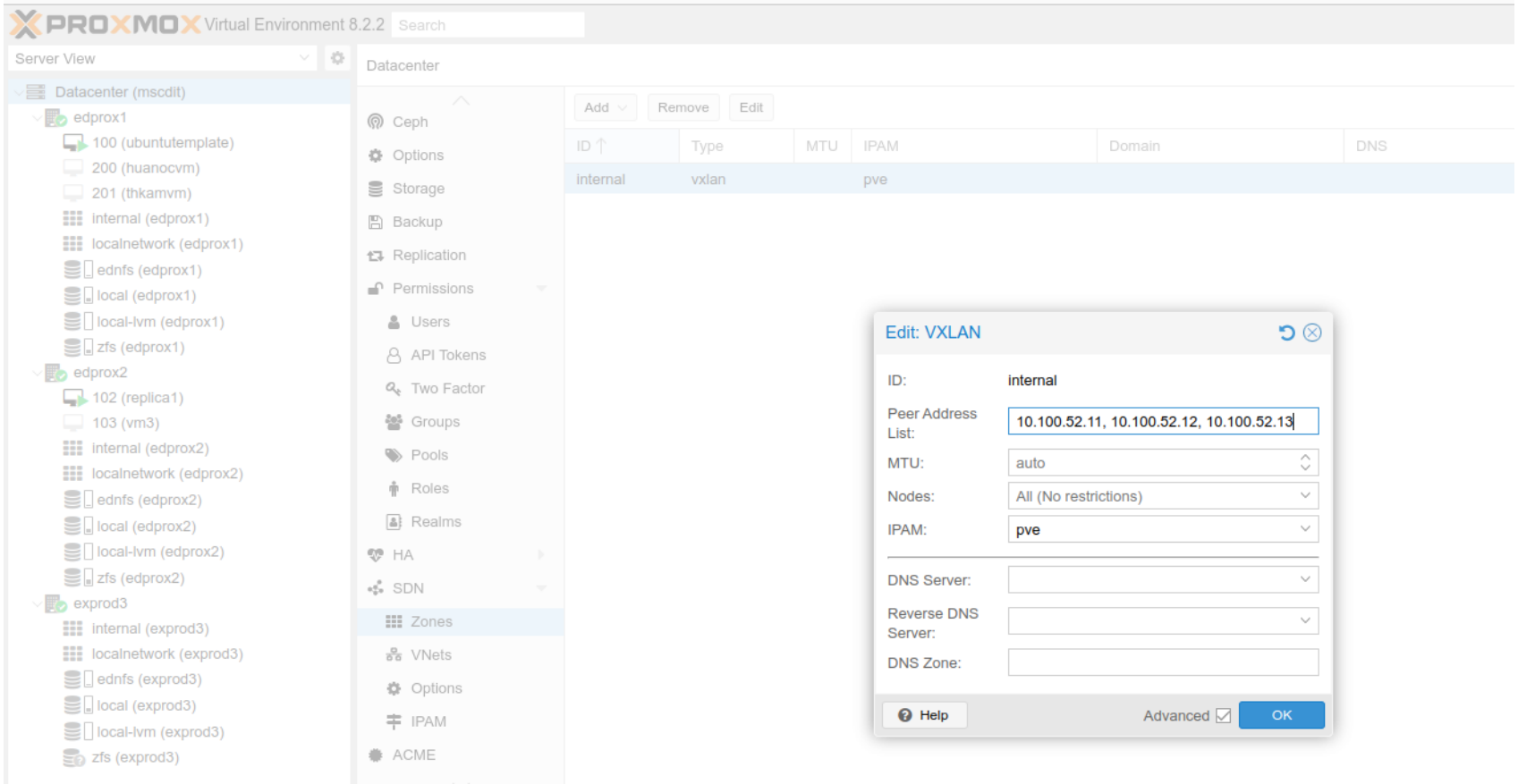
- Απλό: Απομονωμένη γέφυρα. Μια απλή γέφυρα δρομολόγησης Layer 3 (NAT).
- VLAN: Τα εικονικά LANs είναι η χλασική μέθοδος υποδιαίρεσης ενός LAN.
- QinQ: Στοίβαξη VLANs (επίσημα γνωστό ως IEEE 802.1ad).
- VXLAN: Δίχτυο Layer 2 VXLAN μέσω σήραγγας UDP.
- EVPN (BGP EVPN): VXLAN με BGP για να χαθιερωθεί δρομολόγηση Layer 3.

‘

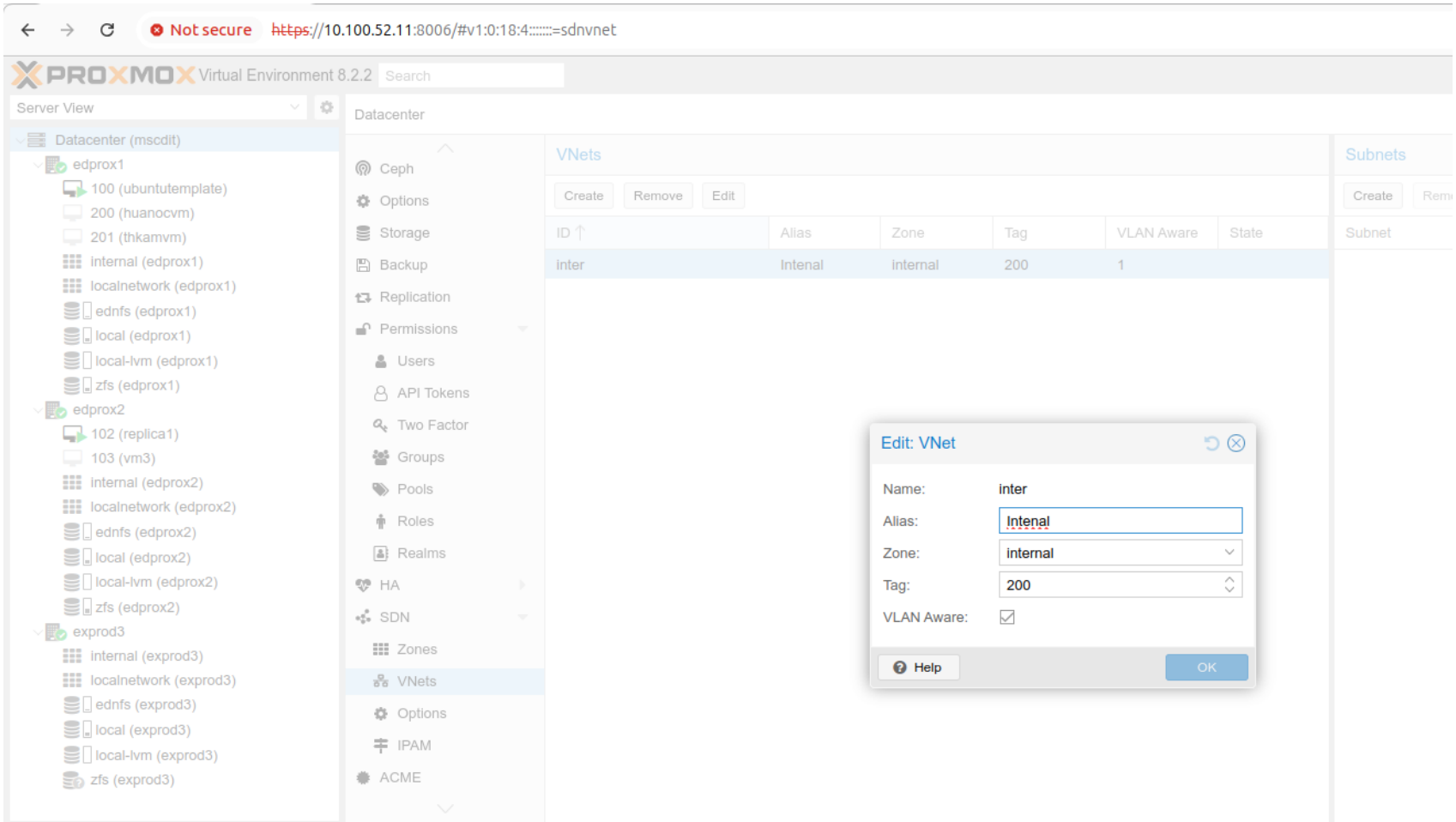
Παράδειγμα: VXLAN

- Το VXLAN δημιουργεί μια σήραγγα UDP μέσω ενός IP δικτύου, χάνοντας encapsulation πακέτων Ethernet σε πακέτα UDP.
- Σε χάθε δίκτυο VXLAN αντιστοιχεί σε ένα VNI (VXLAN Network Identifier), το οποίο λειτουργεί όπως οι ετικέτες VLAN, αλλά σε πολύ μεγαλύτερη κλίμακα.
- Υποστηρίζει εκατομμύρια εικονικά δίκτυα, κάτι που ξεπερνά τον περιορισμό των VLAN.
- Λόγω του encapsulation, το Maximum Transmission Unit (MTU) πρέπει να είναι 50 bytes μικρότερο από αυτό του φυσικού interface (συνήθως δηλαδή 1450).

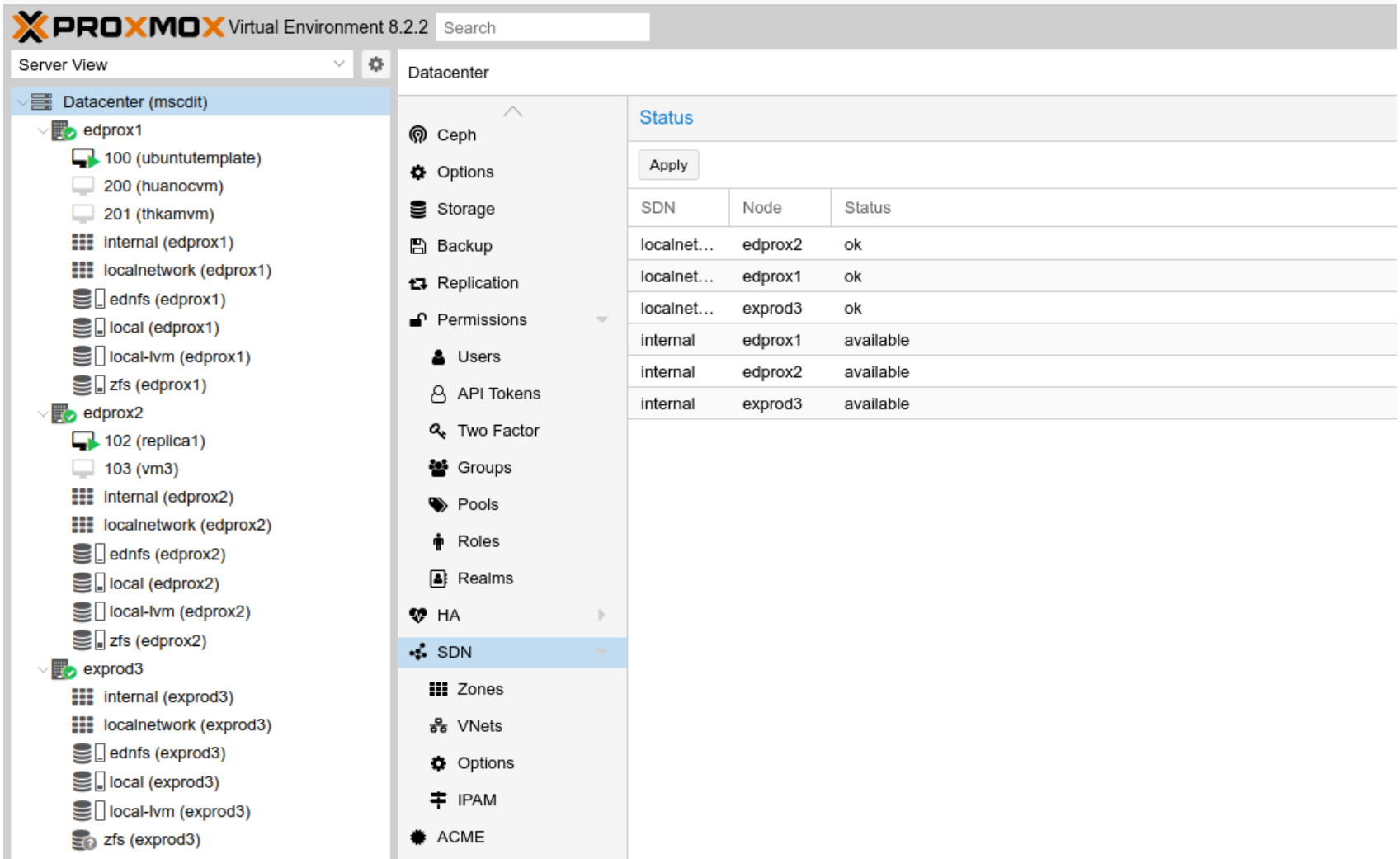
VXLAN zone


PROXMOX Virtual Environment 8.2.2
Search
Server View
Datacenter (mscdit)
edprox1
100 (ubuntutemplate)
200 (huanocvm)
201 (thkamvm)
internal (edprox1)
localnetwork (edprox1)
ednfs (edprox1)
local (edprox1)
local-lvm (edprox1)
zfs (edprox1)
edprox2
102 (replica1)
103 (vm3)
internal (edprox2)
localnetwork (edprox2)
ednfs (edprox2)
local (edprox2)
local-lvm (edprox2)
zfs (edprox2)
exprod3
internal (exprod3)
localnetwork (exprod3)
ednfs (exprod3)
local (exprod3)
local-lvm (exprod3)
zfs (exprod3)
Datacenter
Ceph
Options
Storage
Backup
Replication
Permissions
Users
API Tokens
Two Factor
Groups
Pools
Roles
Realms
HA
SDN
Zones
VNets
Options
IPAM
ACME
Add
Remove
Edit
ID
Type
MTU
IPAM
Domain
DNS
internal
vxlan
pve
Edit: VXLAN
ID:
internal
Peer Address List:
10.100.52.11, 10.100.52.12, 10.100.52.13
MTU:
auto
Nodes:
All (No restrictions)
IPAM:
pve
DNS Server:
Reverse DNS Server:
DNS Zone:
Help
Advanced
OK

VXLAN: Vnet


Not secure https://10.100.52.11:8006/#v1:0:18:4:::::=sdnvnet
PROXMOX Virtual Environment 8.2.2
Search
Server View
Datacenter
Datacenter (mscdit)
edprox1
100 (ubuntutemplate)
200 (huanocvm)
201 (thkamvm)
internal (edprox1)
localnetwork (edprox1)
ednfs (edprox1)
local (edprox1)
local-lvm (edprox1)
zfs (edprox1)
edprox2
102 (replica1)
103 (vm3)
internal (edprox2)
localnetwork (edprox2)
ednfs (edprox2)
local (edprox2)
local-lvm (edprox2)
zfs (edprox2)
exprod3
internal (exprod3)
localnetwork (exprod3)
ednfs (exprod3)
local (exprod3)
local-lvm (exprod3)
zfs (exprod3)
Datacenter
Ceph
Options
Storage
Backup
Replication
Permissions
Users
API Tokens
Two Factor
Groups
Pools
Roles
Realms
HA
SDN
Zones
VNets
Options
IPAM
ACME
VNets
Create
Remove
Edit
ID
Alias
Zone
Tag
VLAN Aware
State
inter
Intenal
internal
200
1
Subnets
Create
Subnet
Edit: VNet
Name: inter
Alias: Intenal
Zone: internal
Tag: 200
VLAN Aware:
Help
OK

Εφαρμογή παραμετροποίησης



Εφαρμογή παραμετροποίησης

```
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        ens18:
            mtu: 1450
            dhcp4: false
            addresses:
            - 192.168.100.3/24
            routes:
            - to: default
              via: 192.168.100.1

    version: 2
```

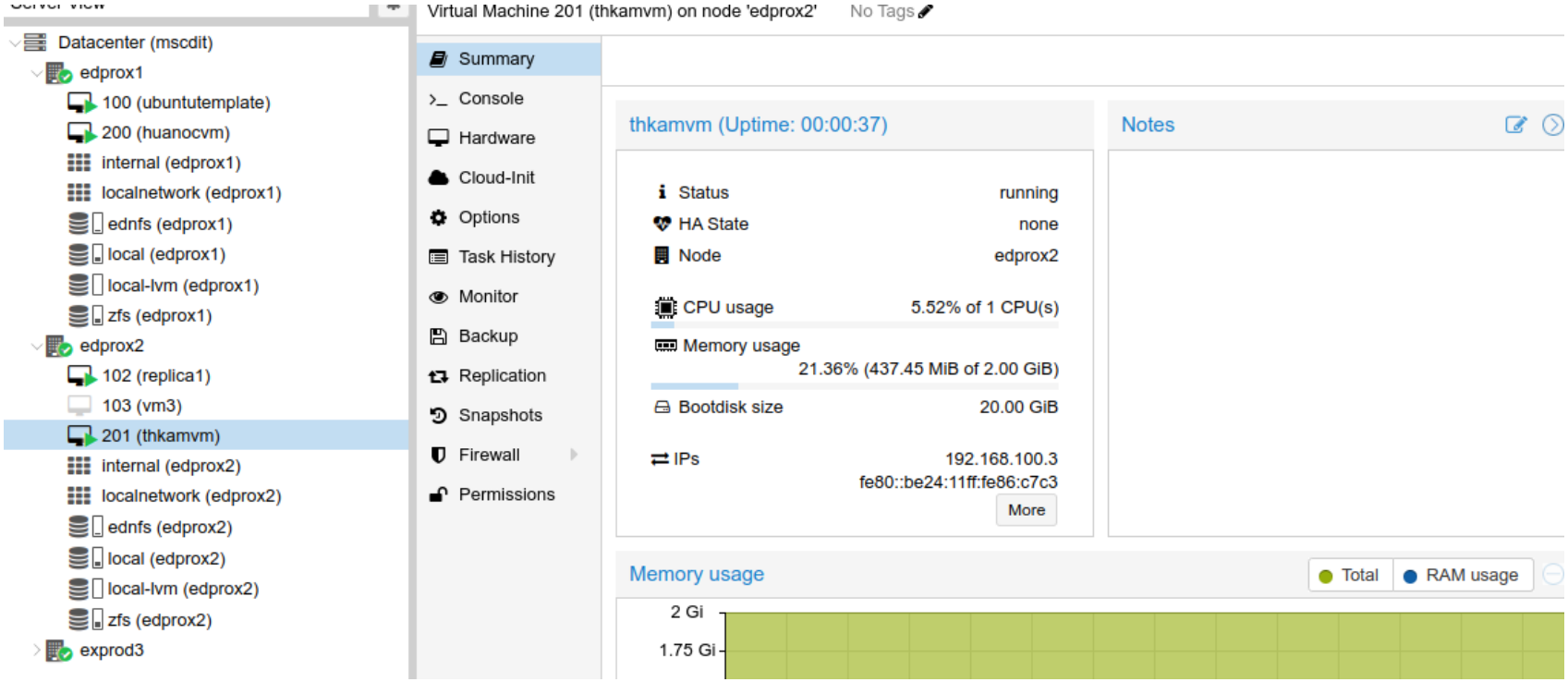
Εφαρμογή παραμετροποίησης

```
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        ens18:
          mtu: 1450
          dhcp4: false
          dhcp6: false
          addresses:
          - 192.168.100.2/24
          routes:
          - to: default
            via: 192.168.100.1
          nameservers:
            addresses: [8.8.8.8, 8.8.4.4]
    version: 2
```

Εφαρμογή παραμετροποίησης

```
root@ubuntutemplate:/home/thomas# ping 192.168.100.3
PING 192.168.100.3 (192.168.100.3) 56(84) bytes of data.
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=0.805 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.949 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=1.03 ms
64 bytes from 192.168.100.3: icmp_seq=4 ttl=64 time=0.886 ms
64 bytes from 192.168.100.3: icmp_seq=5 ttl=64 time=1.02 ms
64 bytes from 192.168.100.3: icmp_seq=6 ttl=64 time=1.54 ms
64 bytes from 192.168.100.3: icmp_seq=7 ttl=64 time=1.30 ms
64 bytes from 192.168.100.3: icmp_seq=8 ttl=64 time=1.25 ms
64 bytes from 192.168.100.3: icmp_seq=9 ttl=64 time=1.27 ms
64 bytes from 192.168.100.3: icmp_seq=10 ttl=64 time=1.18 ms
64 bytes from 192.168.100.3: icmp_seq=11 ttl=64 time=1.06 ms
64 bytes from 192.168.100.3: icmp_seq=12 ttl=64 time=1.01 ms
64 bytes from 192.168.100.3: icmp_seq=13 ttl=64 time=1.13 ms
64 bytes from 192.168.100.3: icmp_seq=14 ttl=64 time=1.27 ms
^C
--- 192.168.100.3 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13024ms
rtt min/avg/max/mdev = 0.805/1.121/1.540/0.187 ms
```

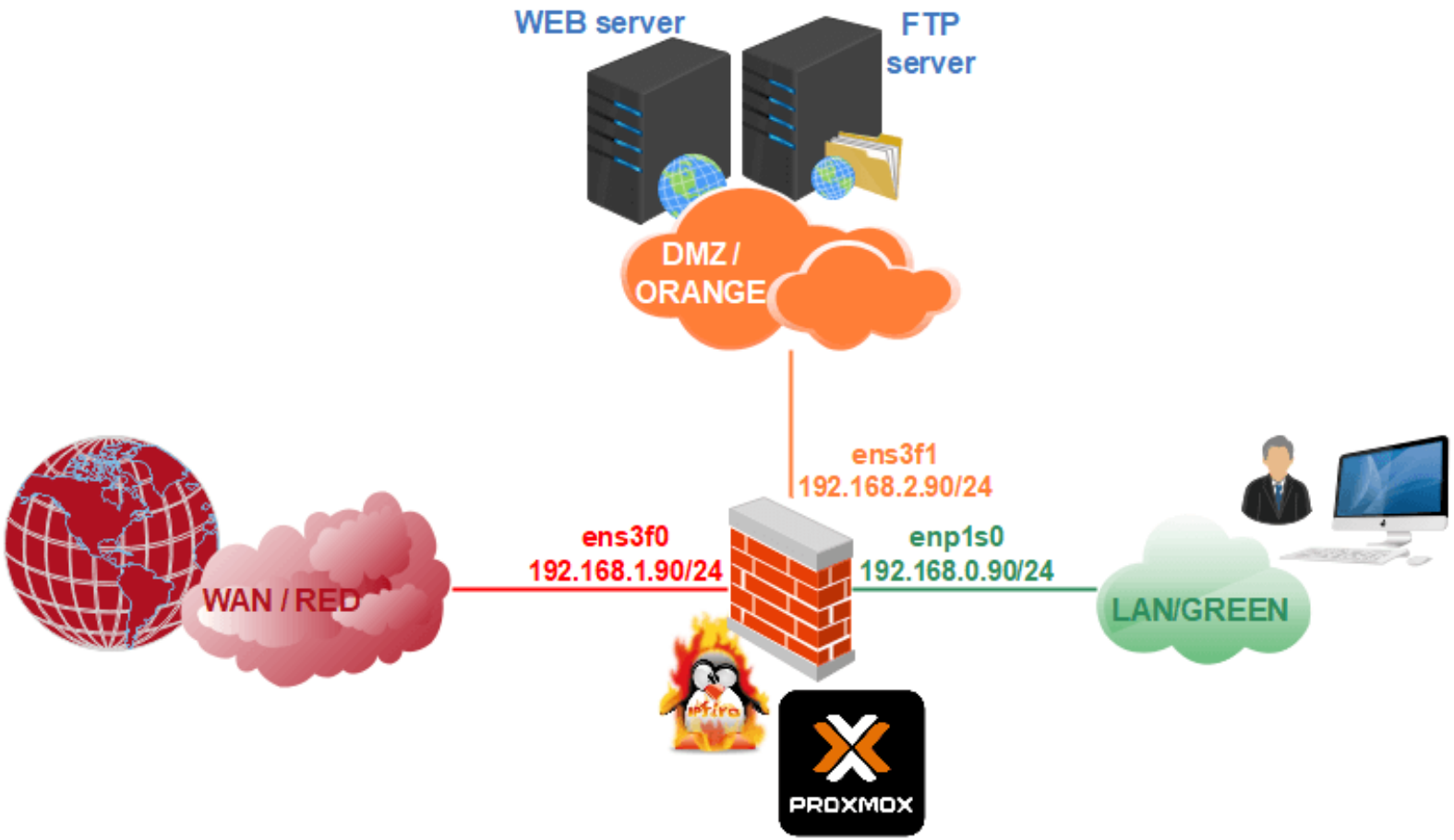
Εφαρμογή παραμετροποίησης



Χρώματα Διχτύου

- Πράσινο (LAN): Είναι η αξιόπιστη ζώνη όπου βρίσχονται οι συσχευές που θεωρούνται ασφαλείς, όπως υπολογιστές, διαχομιστές χαι άλλοι πόροι του οργανισμού.
- Κόχχινο (WAN): Το εξωτεριχό δίχτυο - είναι η πιο επιχίνδυνη ζώνη χαι τα interfaces που συνδέονται με αυτή τη ζώνη συνήθως έχουν πολύ αυστηρές ρυθμίσεις ασφαλείας.
- Πορτοχαλί (DMZ): Είναι μια ζώνη απομόνωσης που φιλοξενεί πόρους χαι υπηρεσίες που είναι προσβάσιμες από το εξωτεριχό δίχτυο (όπως δημόσιοι web servers ή servers email), αλλά απομονώνονται από το εσωτεριχό δίχτυο (LAN).
- Μπλε (Guest): Δίχτυο των επισχεπτών ή για το δίχτυο του Internet of Things (IoT) με περιορισμένη πρόσβαση στο δίχτυο χαι διαχωρίζονται από το βασιχό LAN για λόγους ασφαλείας.

IPfire + Proxmox



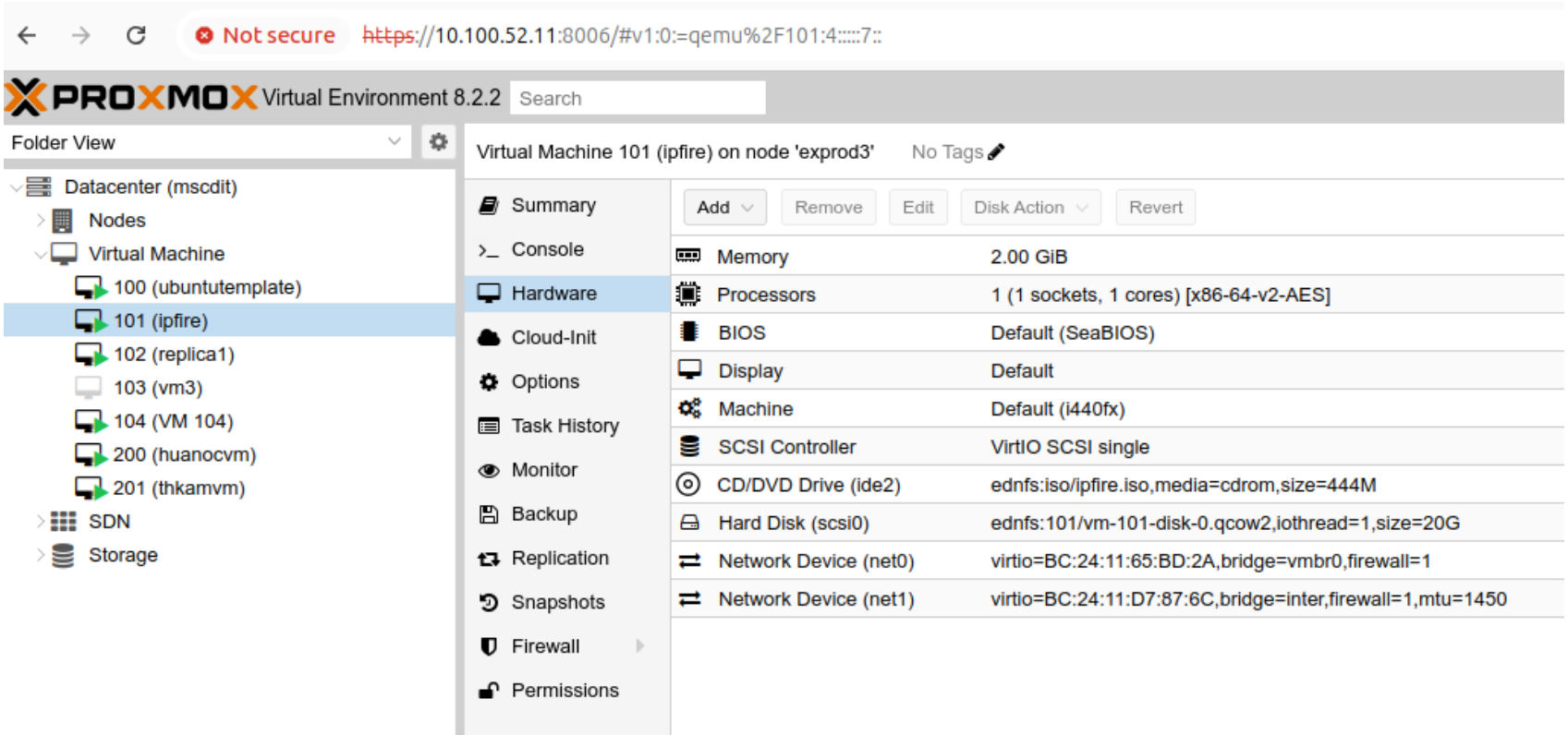
IPfire

- Το IPFire είναι ένα ανοιχτού κώδικα λειτουργικό σύστημα για firewall που βασίζεται στο Linux
- παρέχει ισχυρές δυνατότητες προστασίας δικτύου, δρομολόγησης και διαχείρισης ασφάλειας.
- Χρησιμοποιείται για την προστασία εταιρικών και οικιακών δικτύων από επιθέσεις, για την παρακολούθηση της δικτυακής κίνησης και για τη δημιουργία ασφαλών συνδέσεων, όπως VPN (Virtual Private Networks).
- Χρησιμοποιεί το iptables, το οποίο αποτελεί μέρος του Linux kernel, για την εφαρμογή πολιτικών δικτύου και προστασίας.

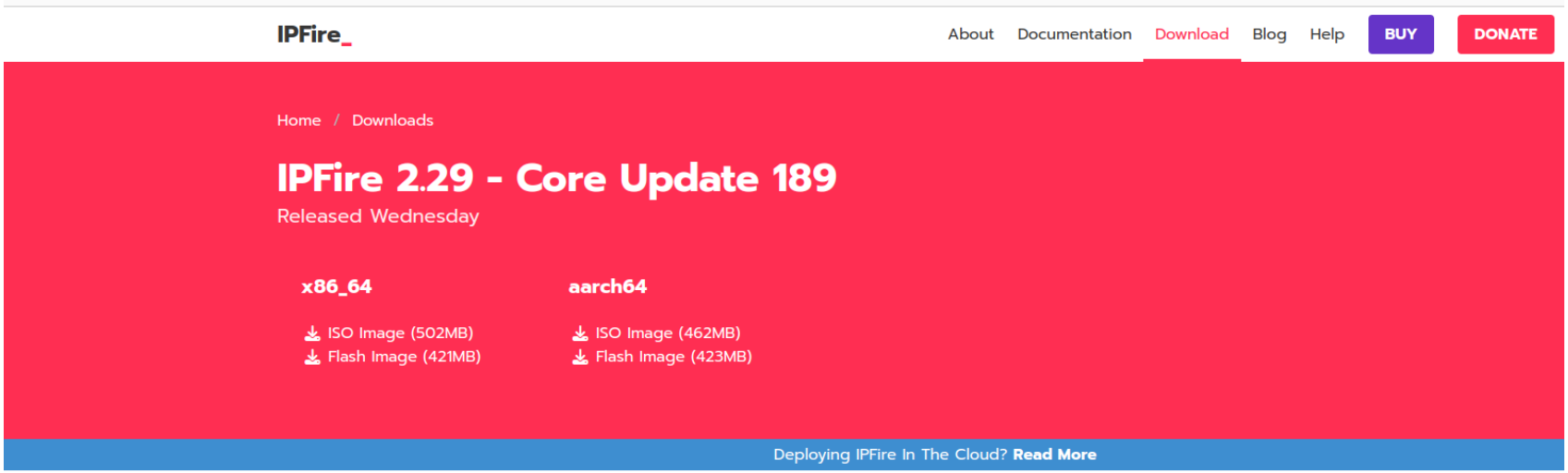
IPfire

- Υποστηρίζει την εγκατάσταση OpenVPN, προσφέροντας ασφαλή απομακρυσμένη πρόσβαση στο δίκτυο ή συνδέσεις μεταξύ διαφορετικών τοποθεσιών (site-to-site VPN).
- Περιλαμβάνει σύστημα ανίχνευσης εισβολών (IDS), το οποίο επιτρέπει την παρακολούθηση της δικτυακής κίνησης για ύποπτη ή κακόβουλη δραστηριότητα και την ανάληψη δράσης για να αποτραπούν επιθέσεις.
- Συλλογή δεδομένων σχετικά με την κίνηση του δικτύου, τα οποία αποθηκεύονται σε logs.

IPfire + Proxmox



IPfire ISO



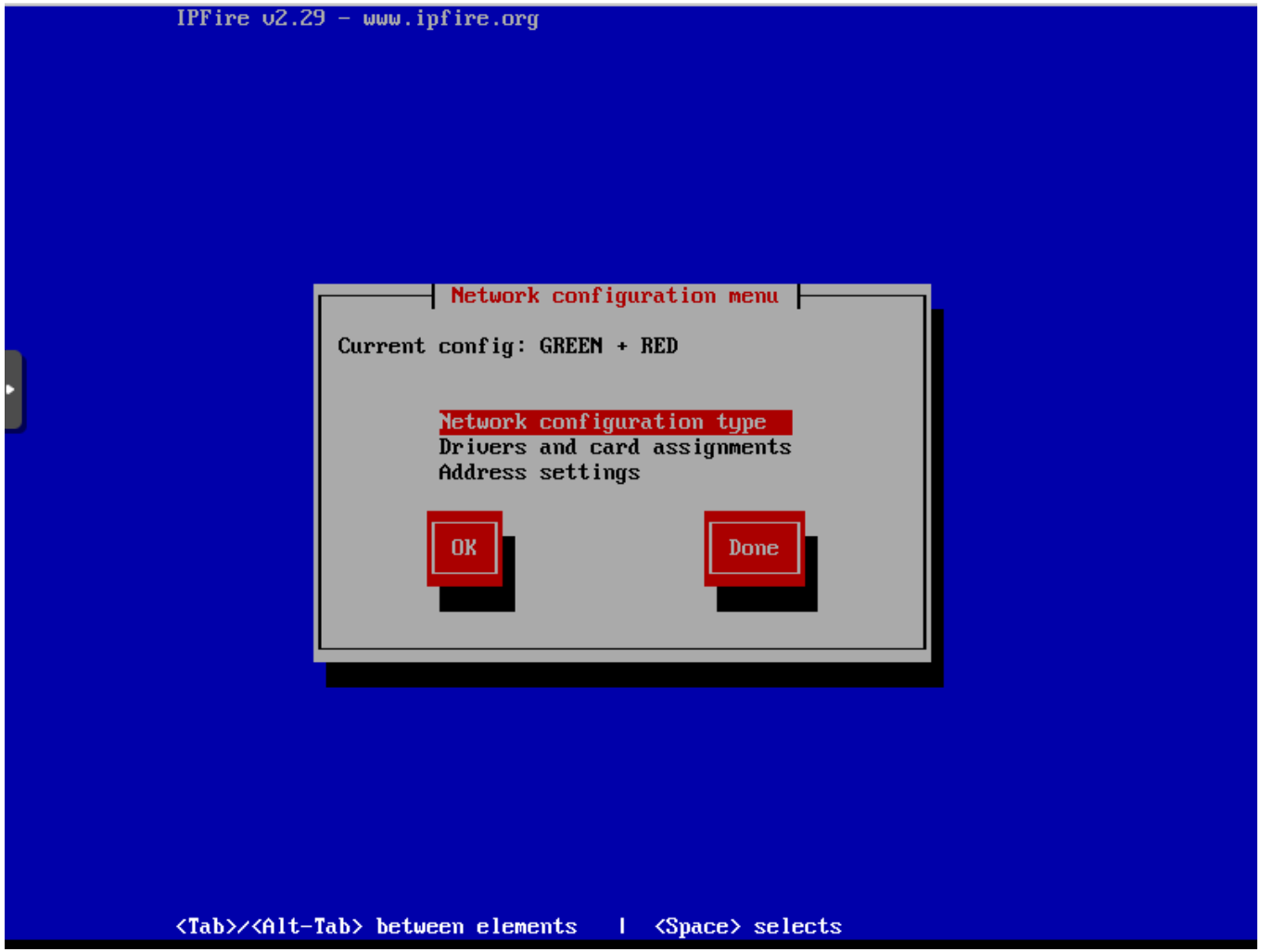
Release Notes

Get ready for a new release of IPFire: Version 2.29 - Core Update 189. It comes with a security fix and a new graph for the IPS as well as a large number of package updates. It is one of the largest update that we have ever shipped because it brings a large number of new and updated firmware files for a lot of hardware.

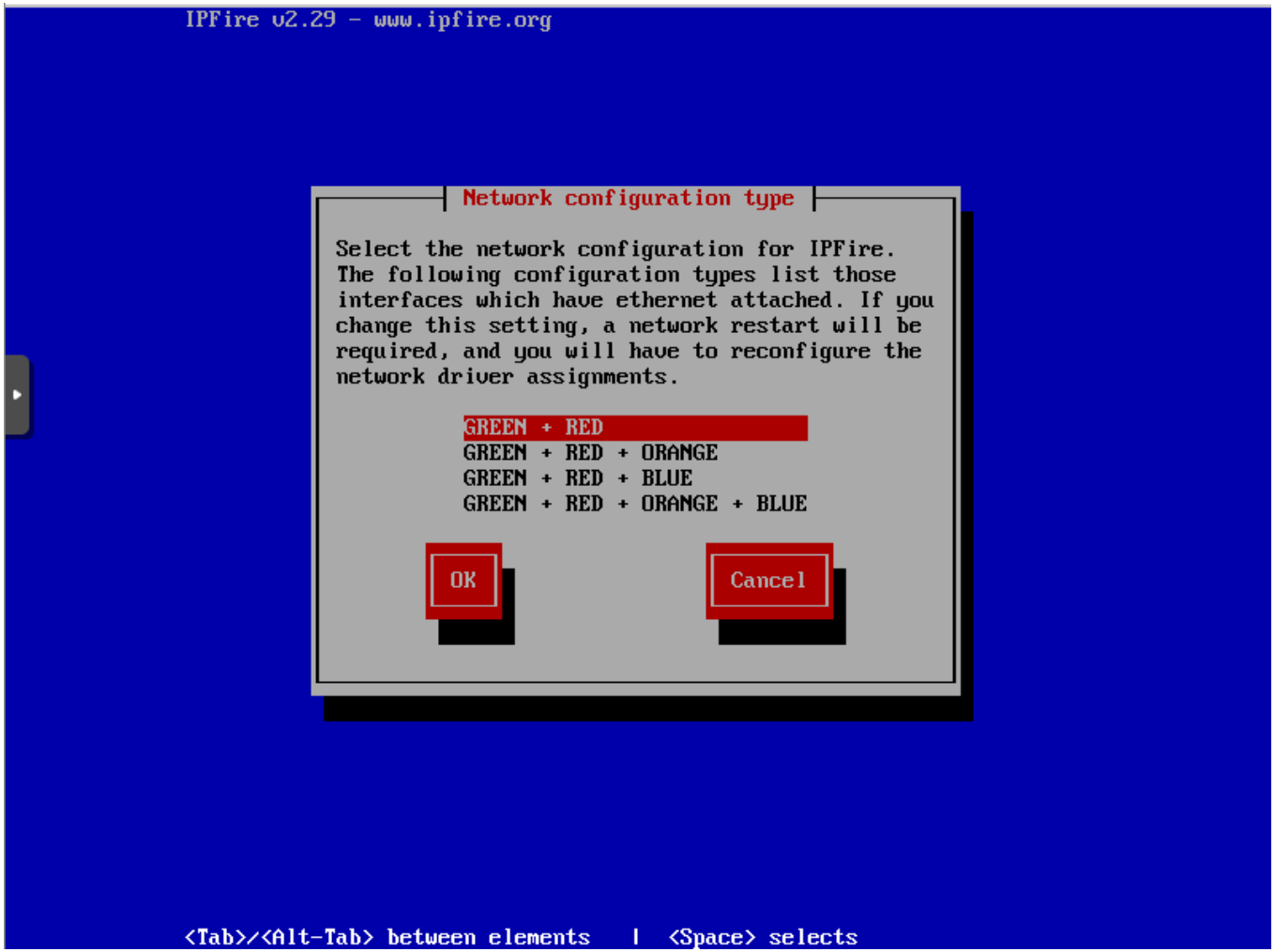
Before we talk about the changes in detail, we would like to ask for your support by sending us a donation. Without them, it is not possible for us to bring you these updates and keep IPFire the modern, versatile and secure distribution it is today. We are currently looking to fund development of a WireGuard implementation for IPFi

Intrusion Prevention System (IPS)

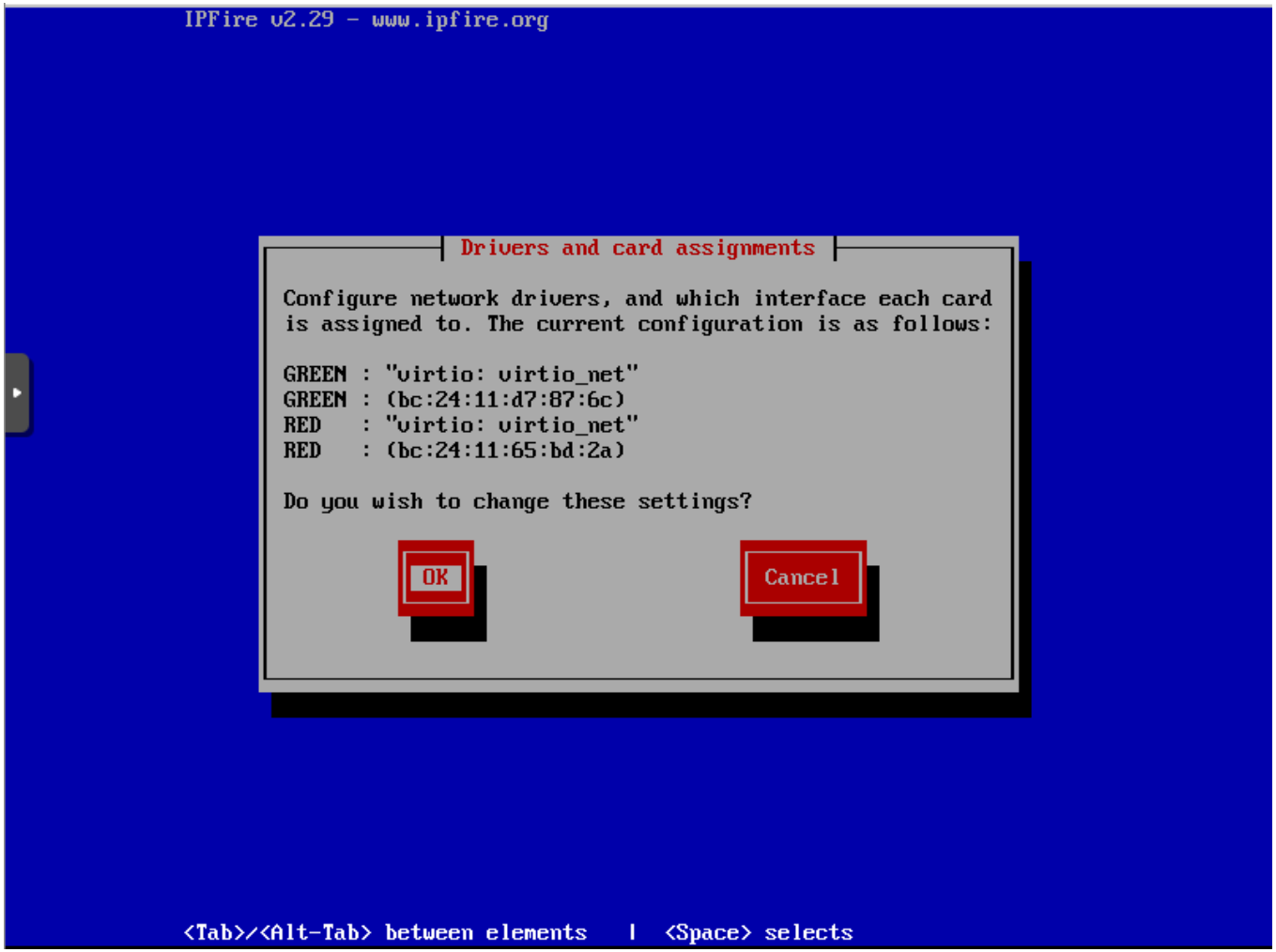
IPfire Setup



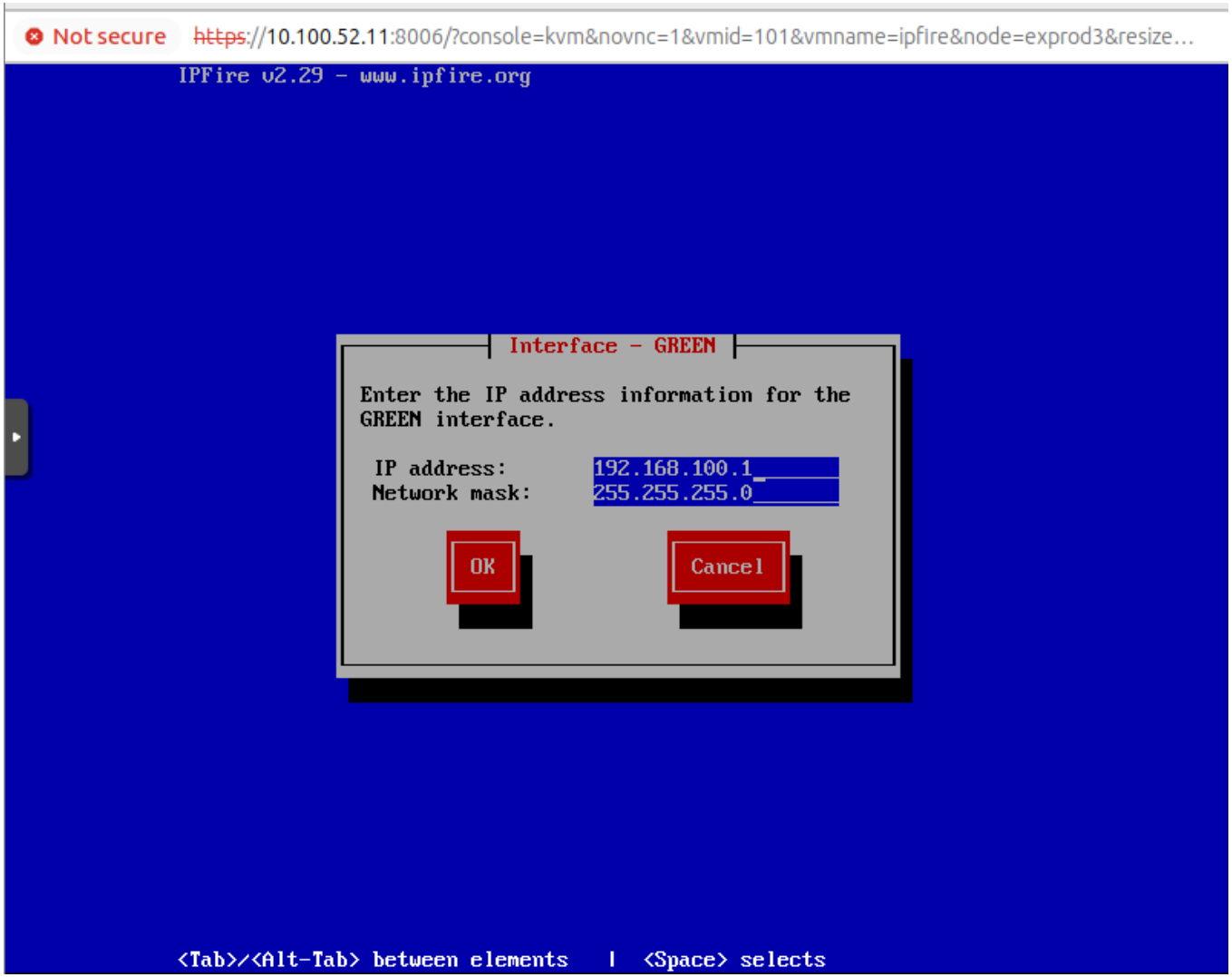
IPfire Setup



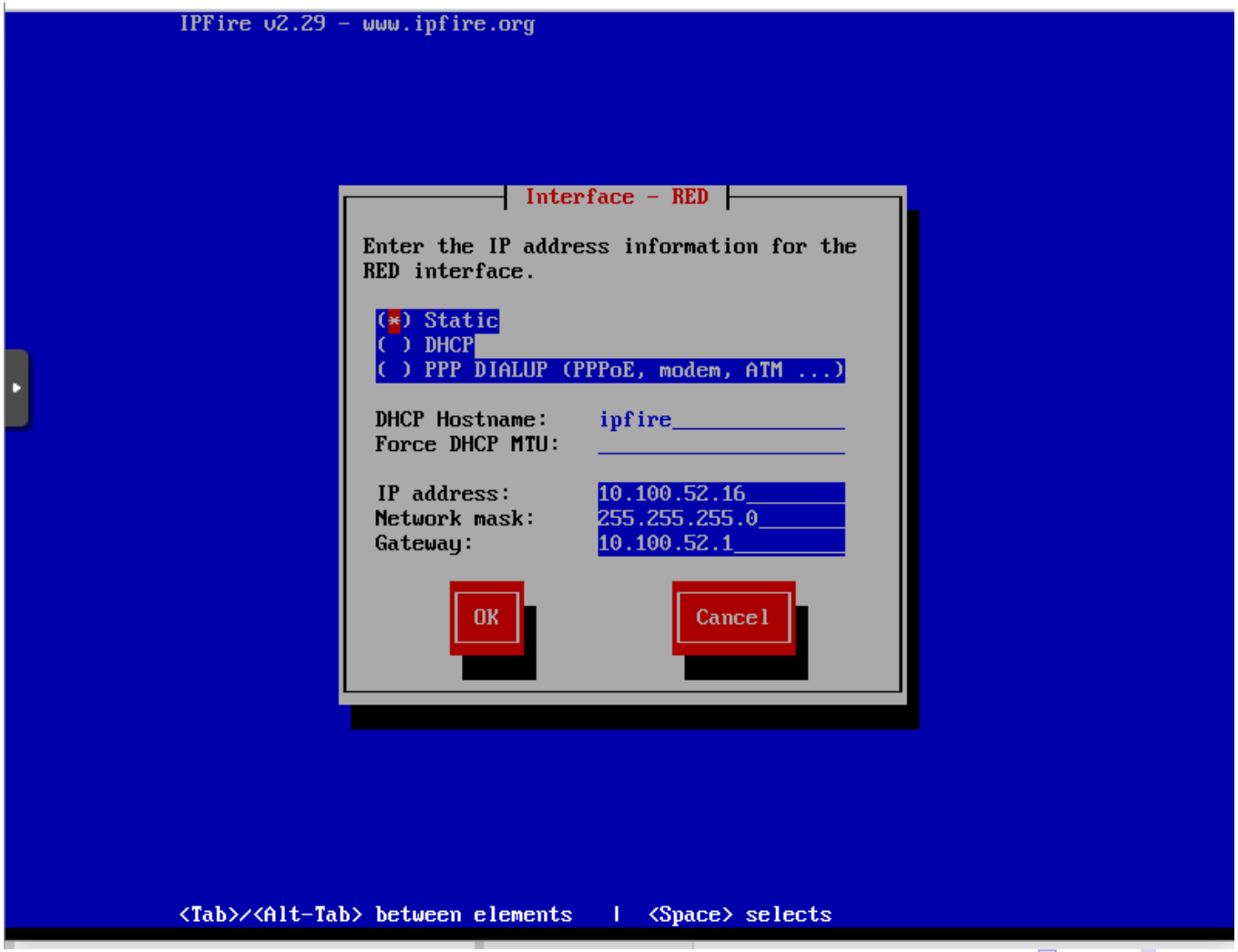
IPfire Setup



IPfire Setup



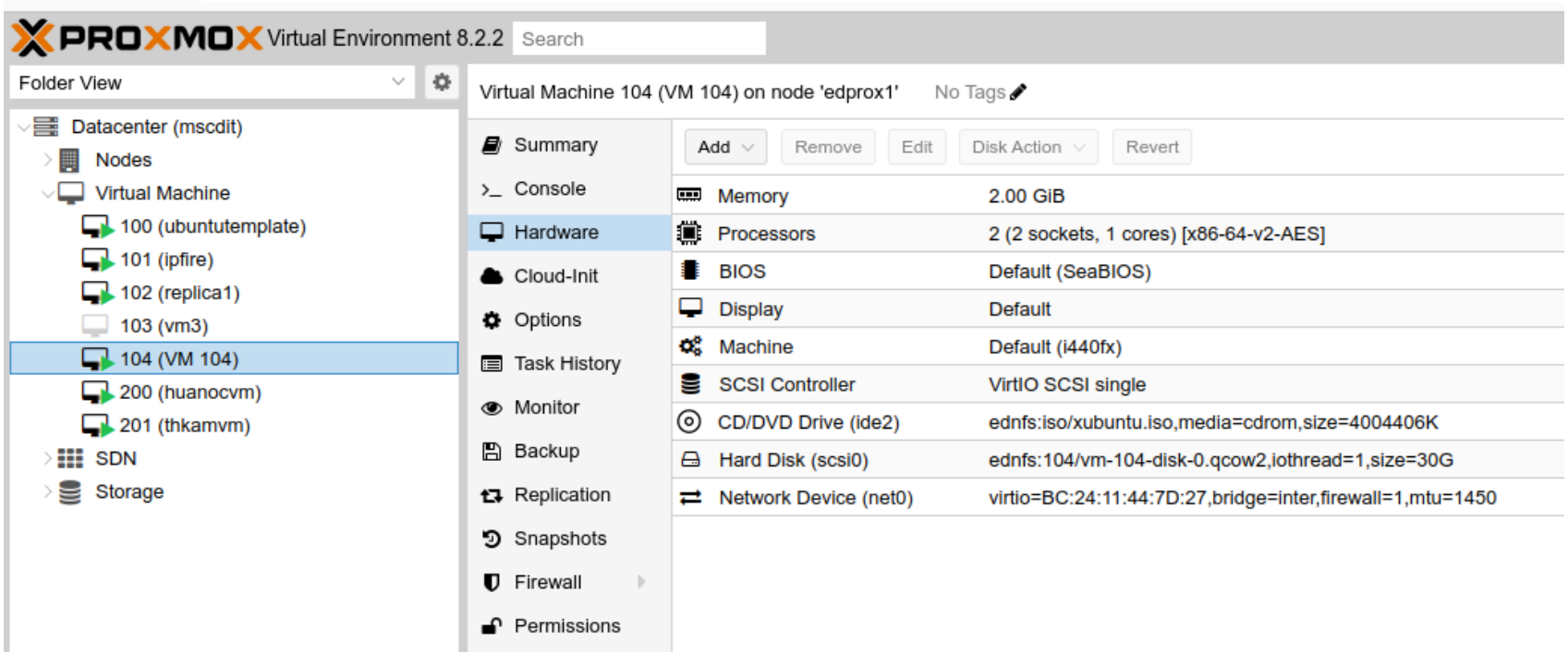
IPfire Setup



IPfire Administration

- Θα χρειαστούμε ένα μικρό VM για την διαχείριση του IPfire.
- Πρέπει να είναι στο Green interface (το Web GUI είναι κλειστό από το Red interface).
- Βάζουμε ένα light desktop λειτουργικό όπως το Xubuntu.

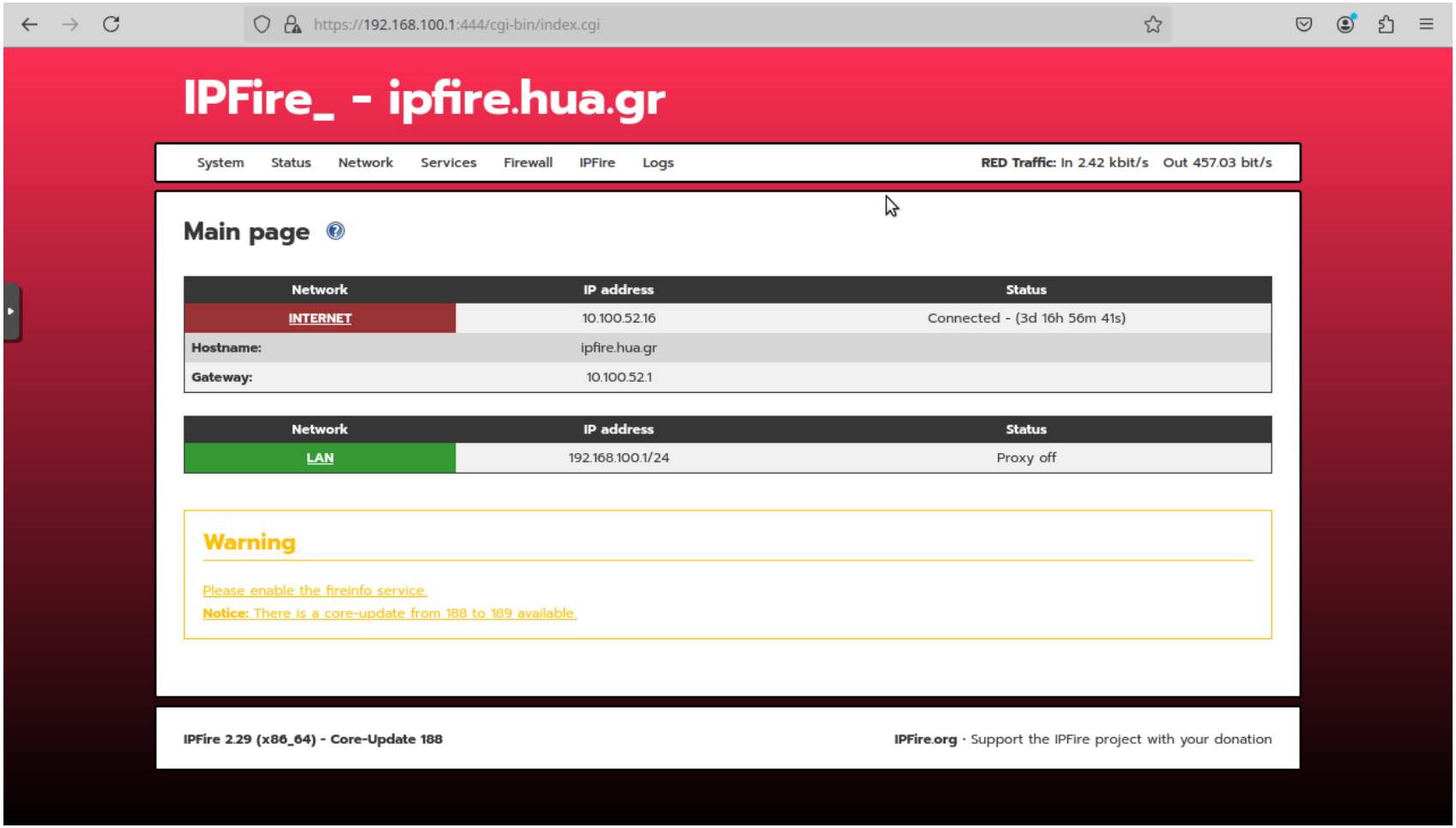
IPfire Administration



IPfire Administration

```
root@xubuntu:/home/thomas# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pfifo_fast state UP group default qlen 1000
    link/ether bc:24:11:44:7d:27 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.100.5/24 brd 192.168.100.255 scope global noprefixroute ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe44:7d27/64 scope link
       valid_lft forever preferred_lft forever
root@xubuntu:/home/thomas# ping www.hua.gr
PING www.hua.gr (195.251.31.114) 56(84) bytes of data.
64 bytes from 195.251.31.114: icmp_seq=1 ttl=60 time=2.58 ms
64 bytes from 195.251.31.114: icmp_seq=2 ttl=60 time=2.64 ms
^C
--- www.hua.gr ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 2.581/2.608/2.635/0.027 ms
```

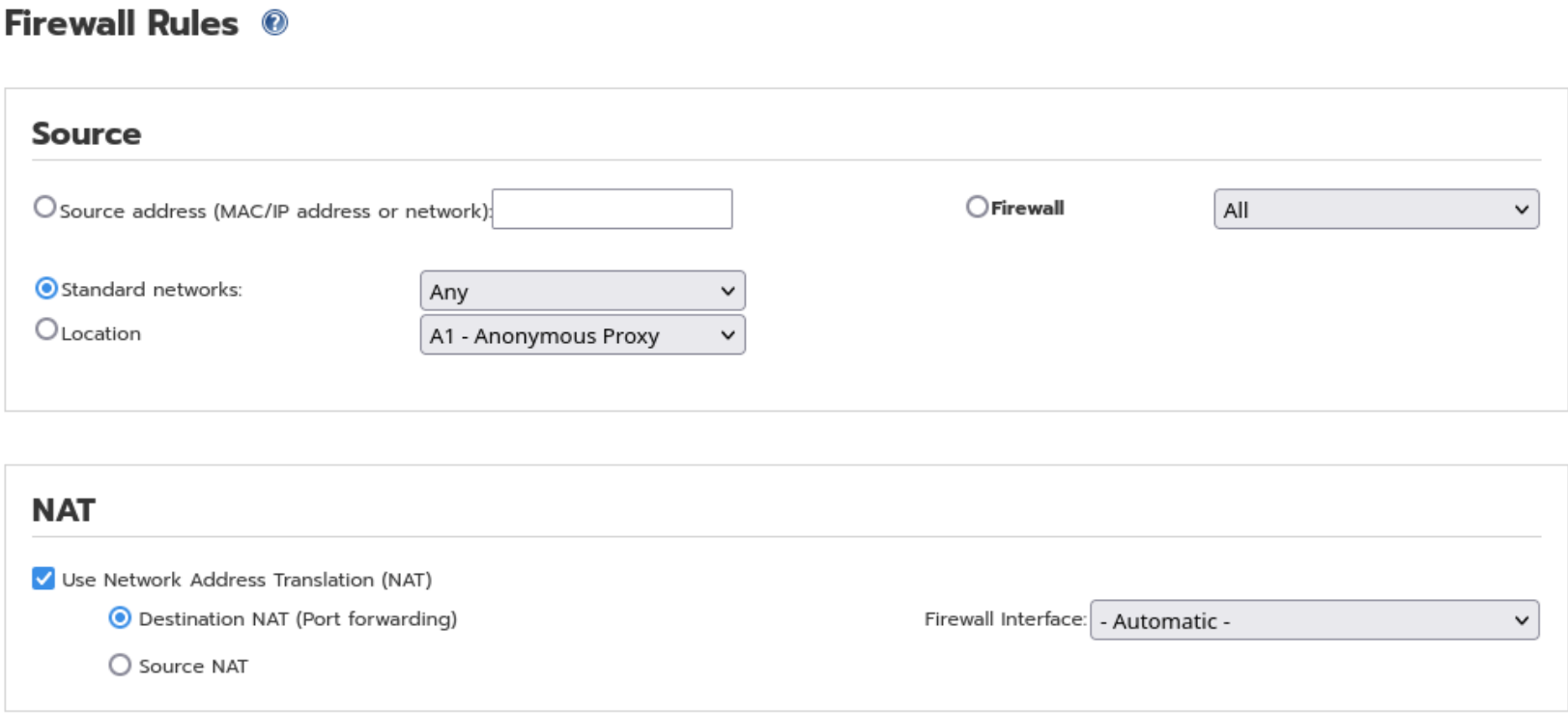
IPfire Administration



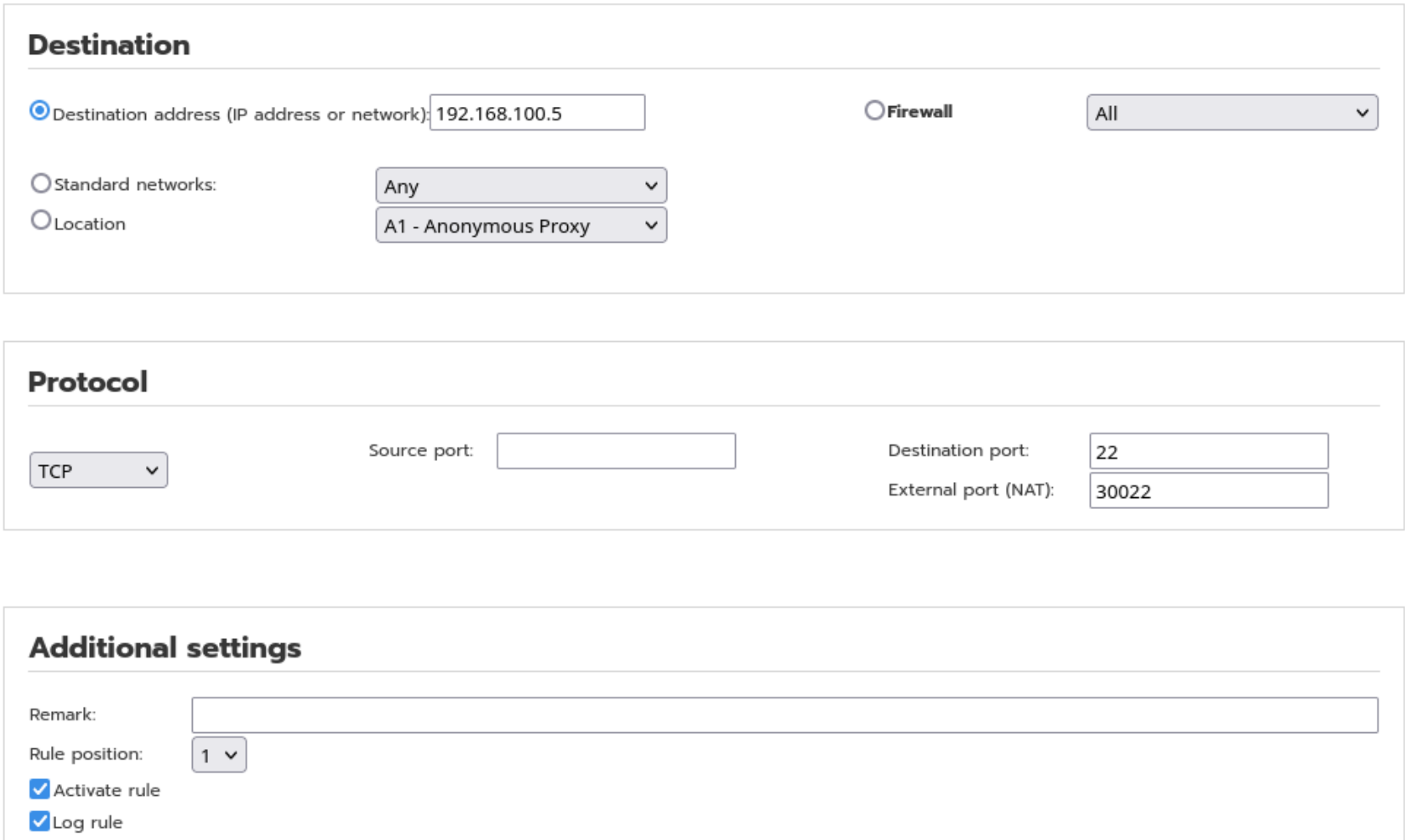
Παράδειγμα παραμετροποίησης

- Ένα πρώτο παράδειγμα είναι να ανοίξουμε το SSH για το διαχειριστικό VM από το RED.
- Θα χρησιμοποιήσουμε το port 30022 στο RED interface για να συνδεθούμε στην πόρτα 22 του VM.
- Μετά μπορούμε να βάλουμε το `x2go-server` για να έχουμε πρόσβαση και στο γραφικό περιβάλλον του VM.

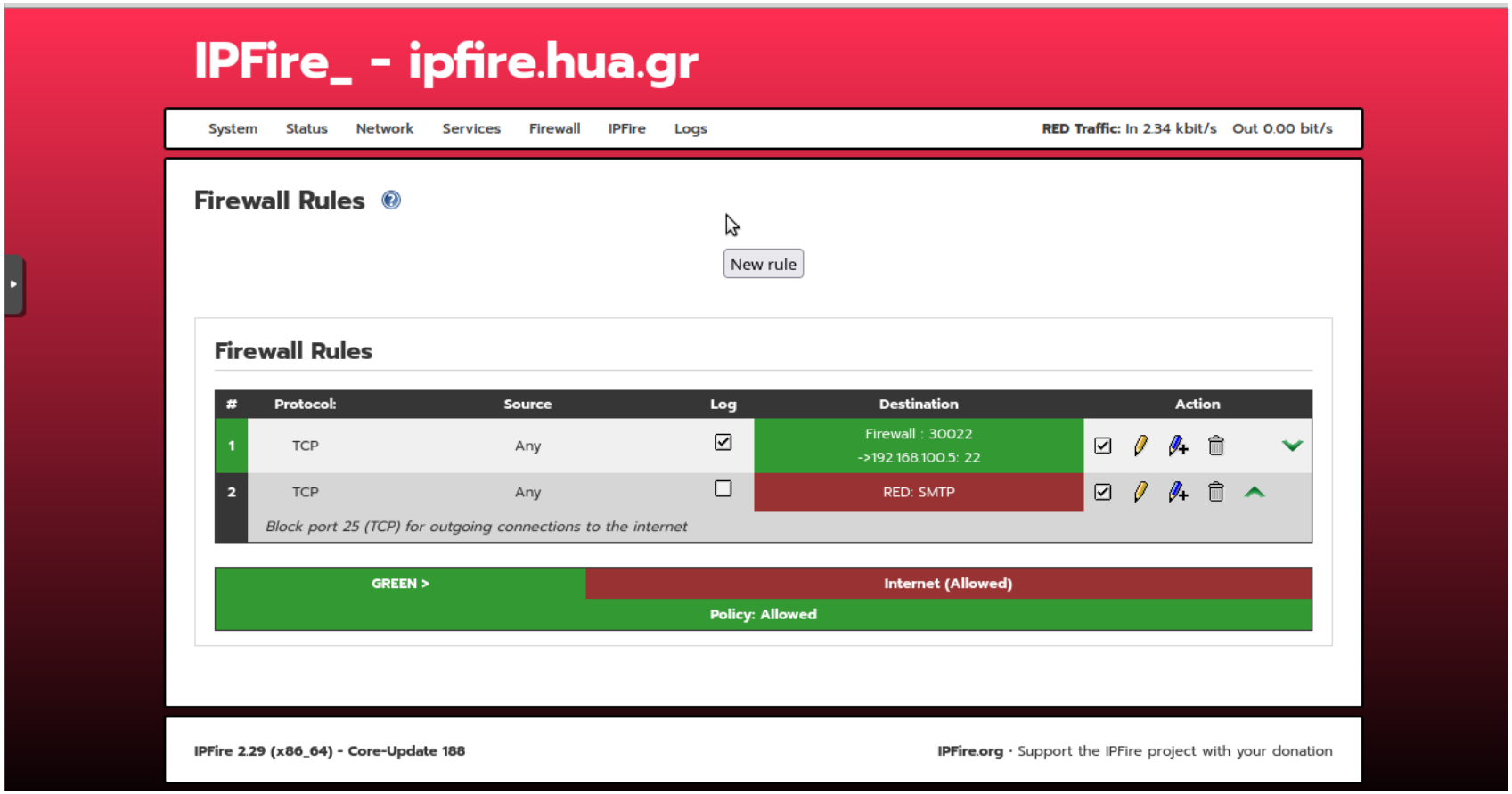
Firewall Rule



Firewall Rule



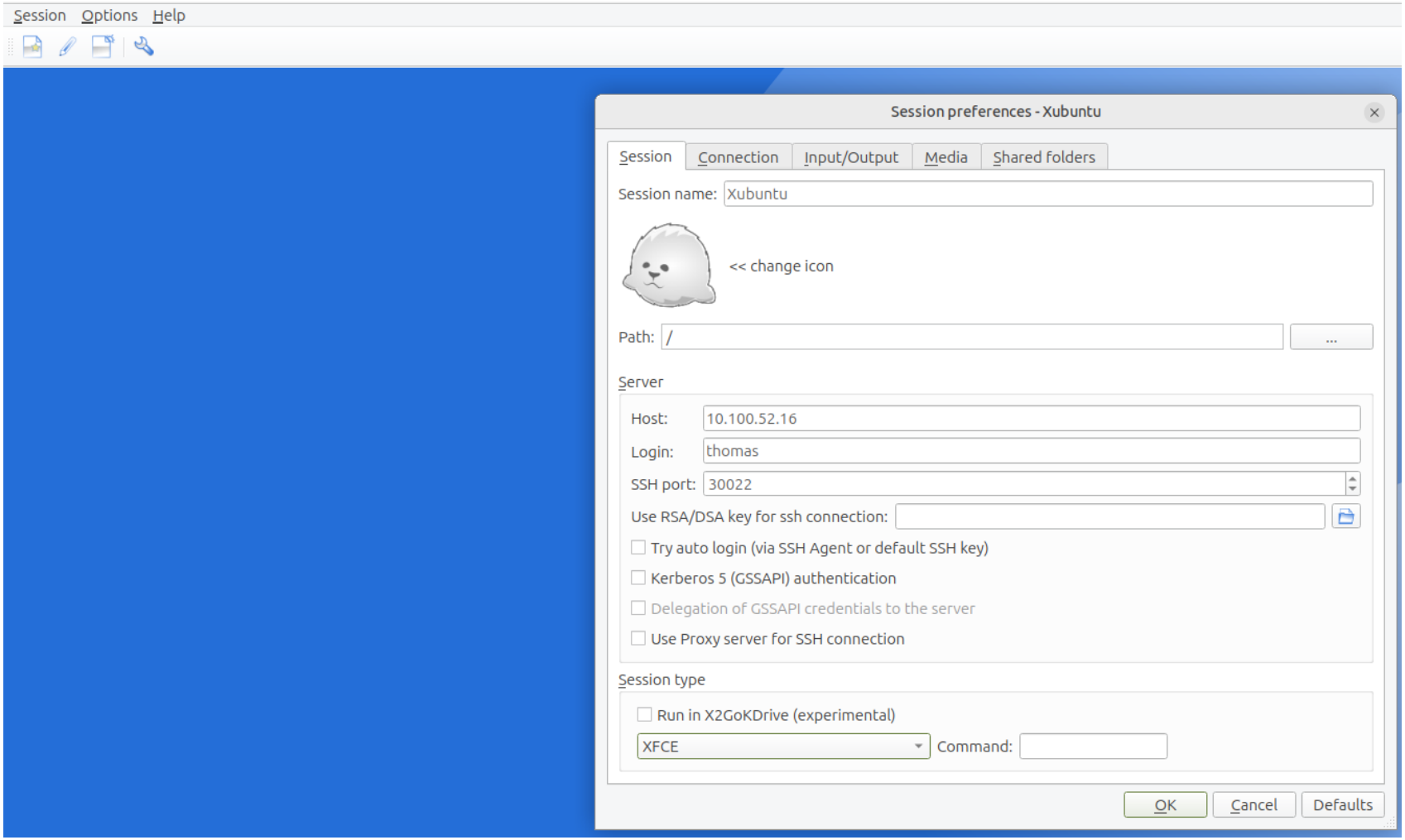
Firewall Rule



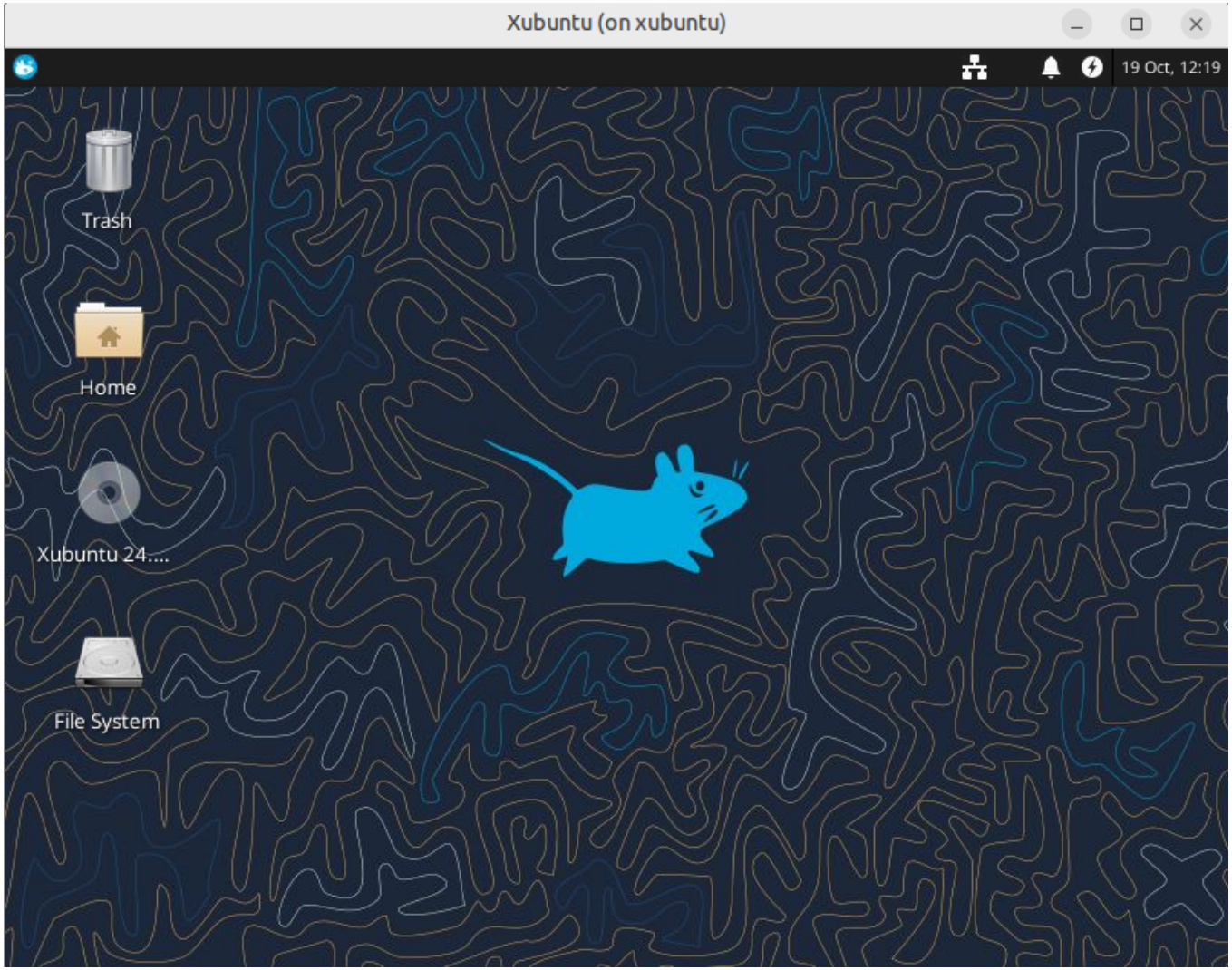
Firewall Rule

```
thomas@kirklaptop:~$ ssh thomas@10.100.52.16 -p 30022
thomas@10.100.52.16's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

32 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat Oct 19 08:50:55 2024 from 195.130.90.147
```

Firewall Rule



Firewall Rule



Webmin

- Το Webmin είναι ένα εργαλείο διαχείρισης συστημάτων που βασίζεται σε web περιβάλλον.
- Επιτρέπει στους διαχειριστές να διαχειρίζονται εύκολα διακομιστές Linux.
- Διαχείριση χρηστών και ομάδων.
- Διαμόρφωση υπηρεσιών δικτύου όπως DNS, FTP, και Apache.
- Ρύθμιση και παρακολούθηση firewall.
- Διαχείριση και δημιουργία βάσεων δεδομένων (MySQL, PostgreSQL).
- Διαχείριση απομακρυσμένης πρόσβασης SSH.

Virtualmin

- Το Virtualmin επιτρέπει τη διαχείριση πολλαπλών virtual server που σηκώνουν ιστοσελίδες.
- Διαχείριση πολλαπλών domains.
- Δημιουργία και διαχείριση email λογαριασμών.
- Διαχείριση βάσεων δεδομένων (MySQL, PostgreSQL).
- Αυτόματη εγκατάσταση SSL/TLS πιστοποιητικών για ασφάλεια.
- Διαχείριση DNS και FTP υπηρεσιών.
- Αυτόματη εγκατάσταση δημοφιλών CMS όπως WordPress και Joomla.

Virtualmin installation

```
root@virtualmin:~# sudo sh -c "$(curl -fsSL https://software.virtualmin.com/gpl/scripts/virtualmin-install.sh)" -- --bundle LAMP
[INFO] Log will be written to: /root/virtualmin-install.log

  Welcome to the Virtualmin GPL installer, version 7.4.0

  This script must be run on a freshly installed supported OS. It does not
  perform updates or upgrades (use your system package manager) or license
  changes (use the "virtualmin change-license" command).

  The systems currently supported by the install script are:

    Red Hat Enterprise Linux and derivatives
      - RHEL 8 and 9 on x86_64
      - Alma and Rocky 8 and 9 on x86_64
      - CentOS 7 on x86_64

    Debian Linux and derivatives
      - Debian 10, 11 and 12 on i386 and amd64
      - Ubuntu 20.04 LTS, 22.04 LTS and 24.04 LTS on i386 and amd64

  If your OS/version/arch is not listed, installation will fail. More
  details about the systems supported by the script can be found here:

    https://www.virtualmin.com/os-support

  The selected package bundle is LAMP and the size of install is
  full. It will require up to 2 GB of disk space.

  Exit and re-run this script with --help flag to see available options.

 Continue? (y/n)
```

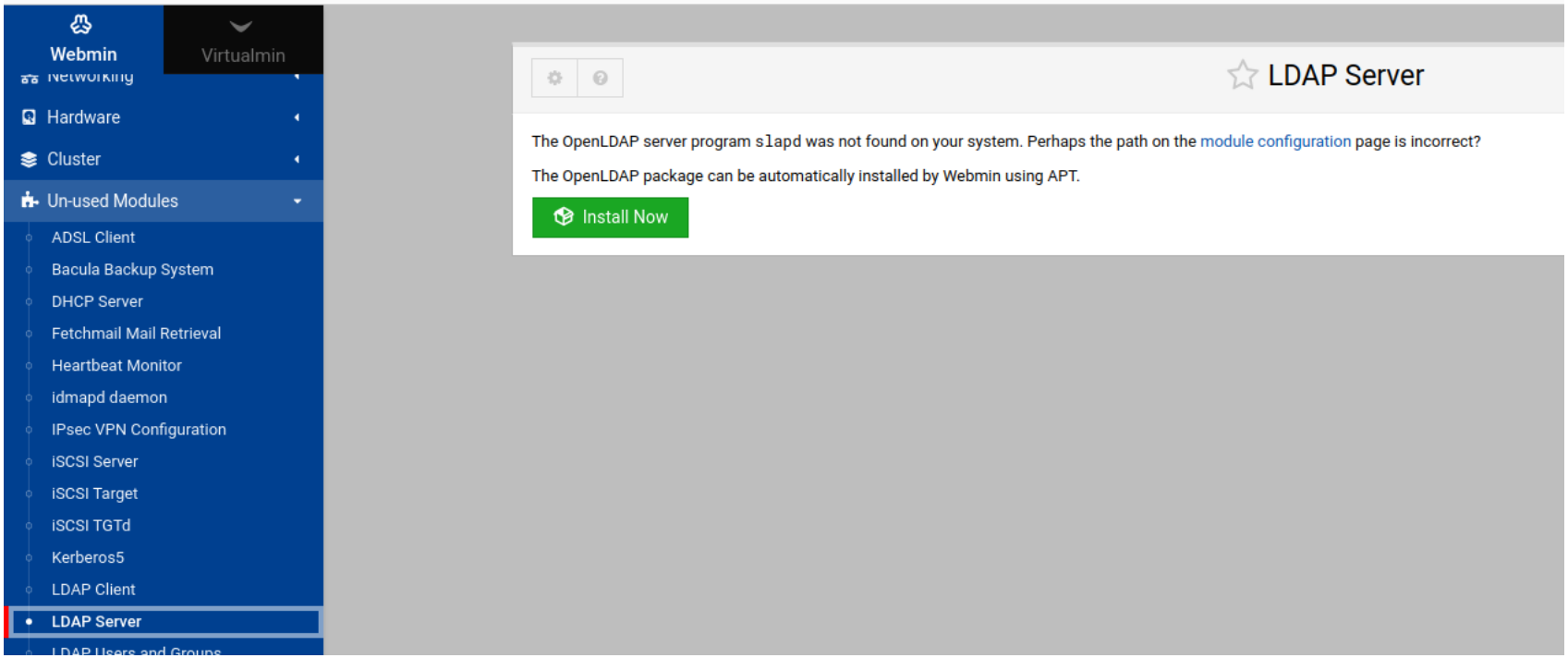
Virtualmin installation

```
root@virtualmin:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

root@virtualmin:~# ufw allow 53
Rule added
Rule added (v6)
root@virtualmin:~# ufw allow 80
Rule added
Rule added (v6)
root@virtualmin:~# ufw allow 443
```

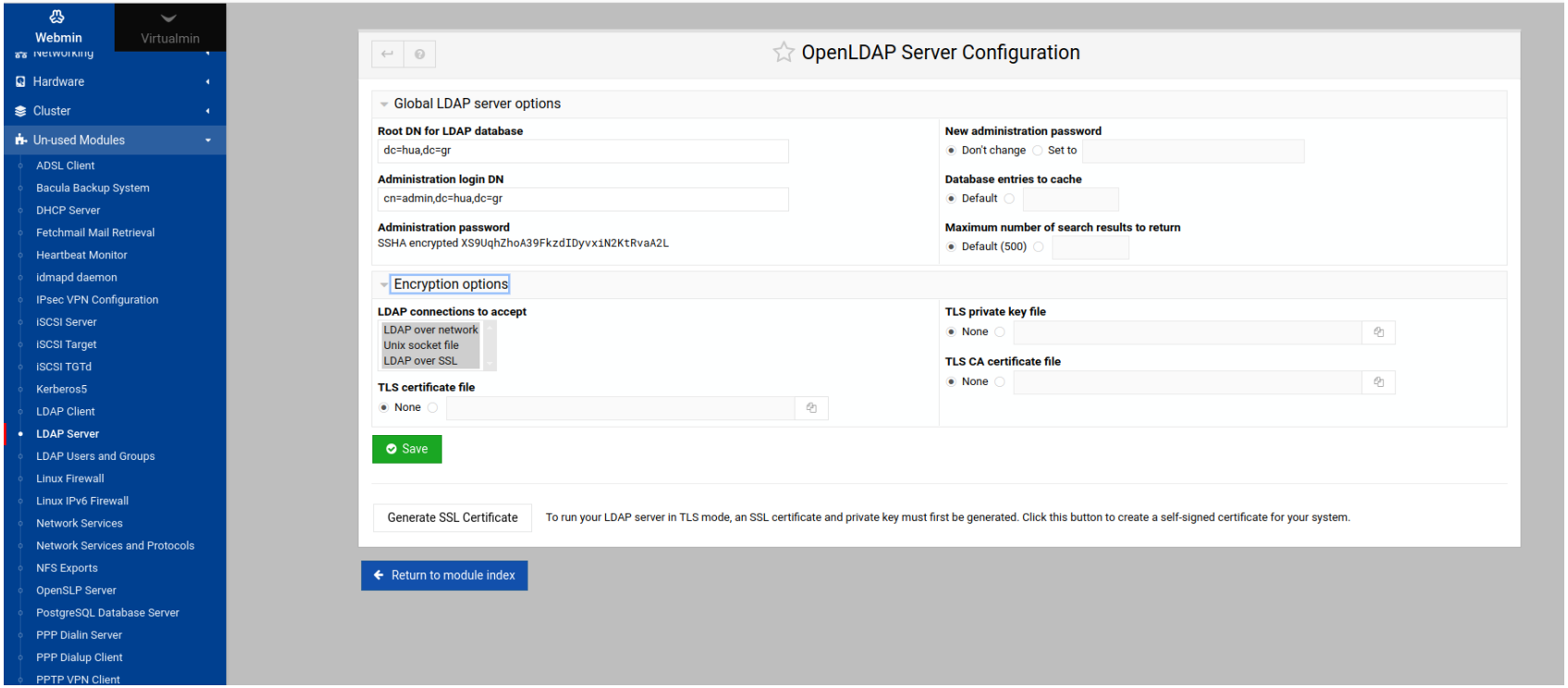
Virtualmin installation

```
■■□□ Phase 2 of 4: Setup
[ERROR] Your system hostname virtualmin is not fully qualified.
Please enter a fully qualified hostname (e.g.: host.example.com): vmin.hua.gr
Downloading Virtualmin 7 key                                        ✓
Installing Virtualmin 7 key                                         ✓
Downloading repository metadata                                     ✓
Enabling universe repositories, if not already available            ✓
Disabling cdrom: repositories                                       ✓
Cleaning up software repo metadata                                  ✓

■■■□ Phase 3 of 4: Installation
Checking and installing system package updates                      ✓
Installing Virtualmin 7 and all related packages                    ✓
Installing Virtualmin 7 related package updates                     ✓

■■■■ Phase 4 of 4: Configuration
[1/21] Configuring AWStats                                          ✓
[2/21] Configuring Apache                                           ✓
[3/21] Configuring Bind                                             ✓
[4/21] Configuring ClamAV                                           ✓
[5/21] Configuring Dovecot                                          ✓
[6/21] Configuring Etckeeper                                        ✓
[7/21] Configuring Firewalld                                        ✓
[8/21] Configuring MariaDB                                          ✓
[9/21] Configuring Postfix                                          ✓
[10/21] Configuring ProFTPd                                         ✓
[11/21] Configuring Procmail                                        ✓
[12/21] Configuring Quotas                                          ✓
[13/21] Configuring SASL                                            ✓
[14/21] Configuring Shells                                          ✓
[15/21] Configuring SpamAssassin                                    ✓
[16/21] Configuring Status                                          ✓
[17/21] Configuring Upgrade                                         ✓
[18/21] Configuring Usermin                                         ✓
[19/21] Configuring Webmin                                          ✓
[20/21] Configuring Fail2banFirewalld                               ✓
[21/21] Configuring Virtualmin                                      ✓
■■■ Cleaning up

[SUCCESS] Installation Complete!
[SUCCESS] If there were no errors above, Virtualmin should be ready
[SUCCESS] to configure at https://vmin.hua.gr:10000 (or https://10.100.52.17:10000).
[SUCCESS] You may receive a security warning in your browser on your first visit.
root@virtualmin:~#
```

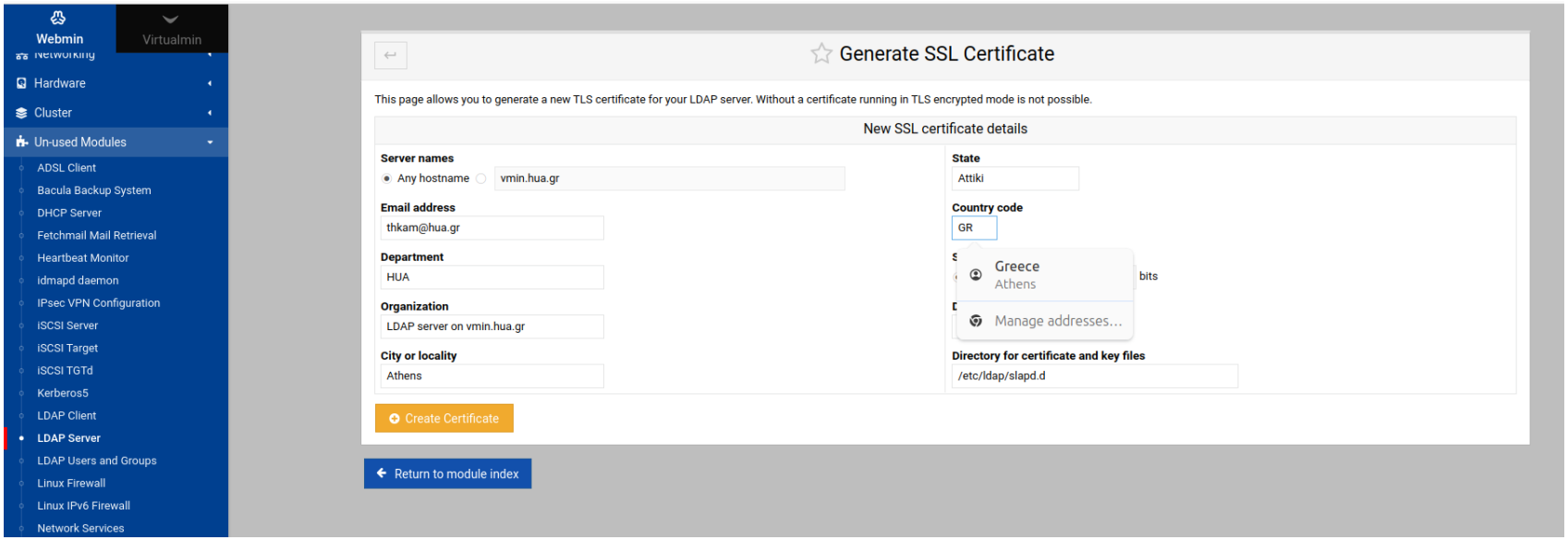
Webmin: LDAP server installation



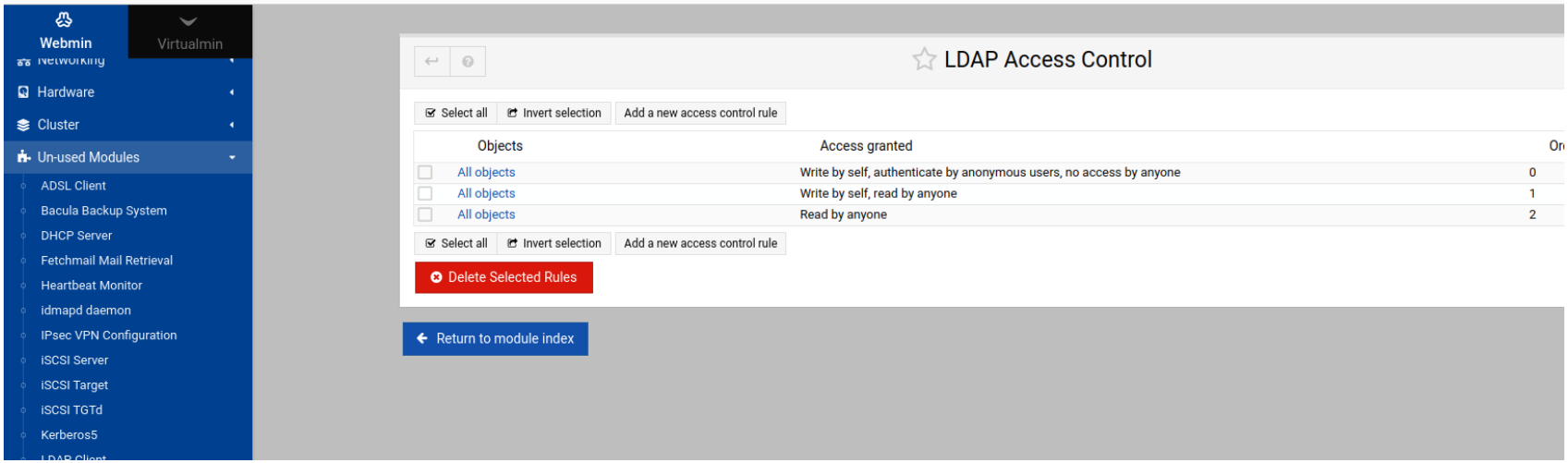
Webmin: LDAP server configuration



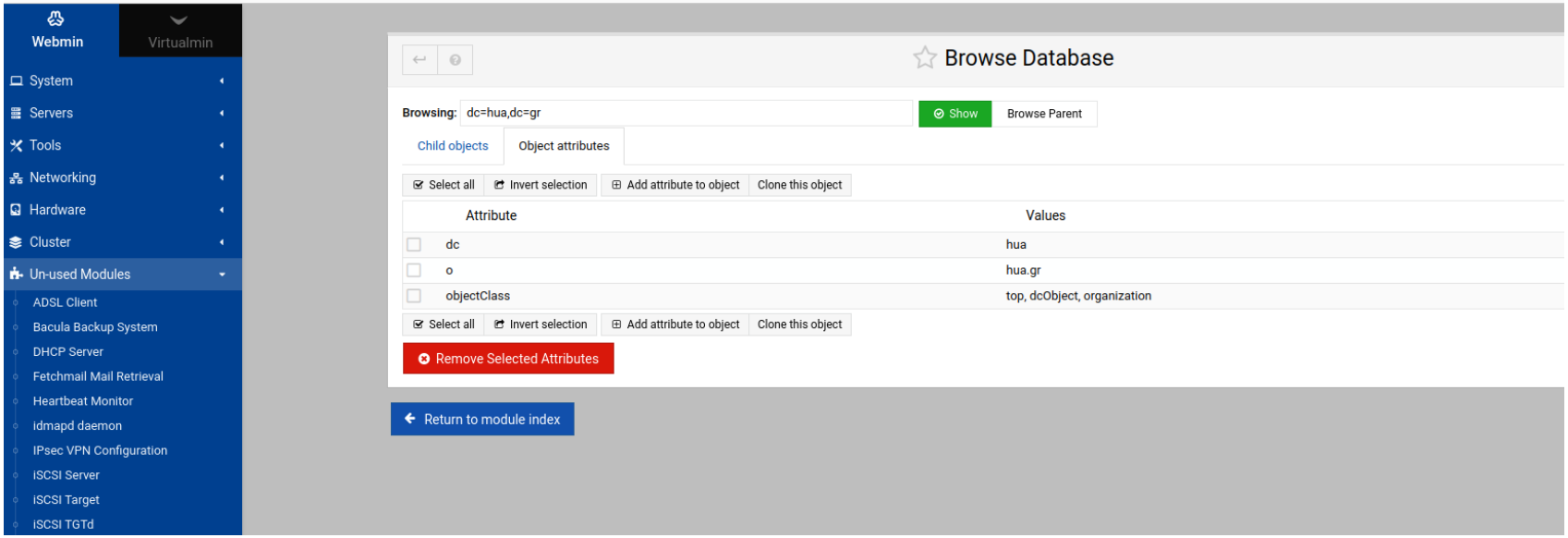
Webmin: LDAP server SSL



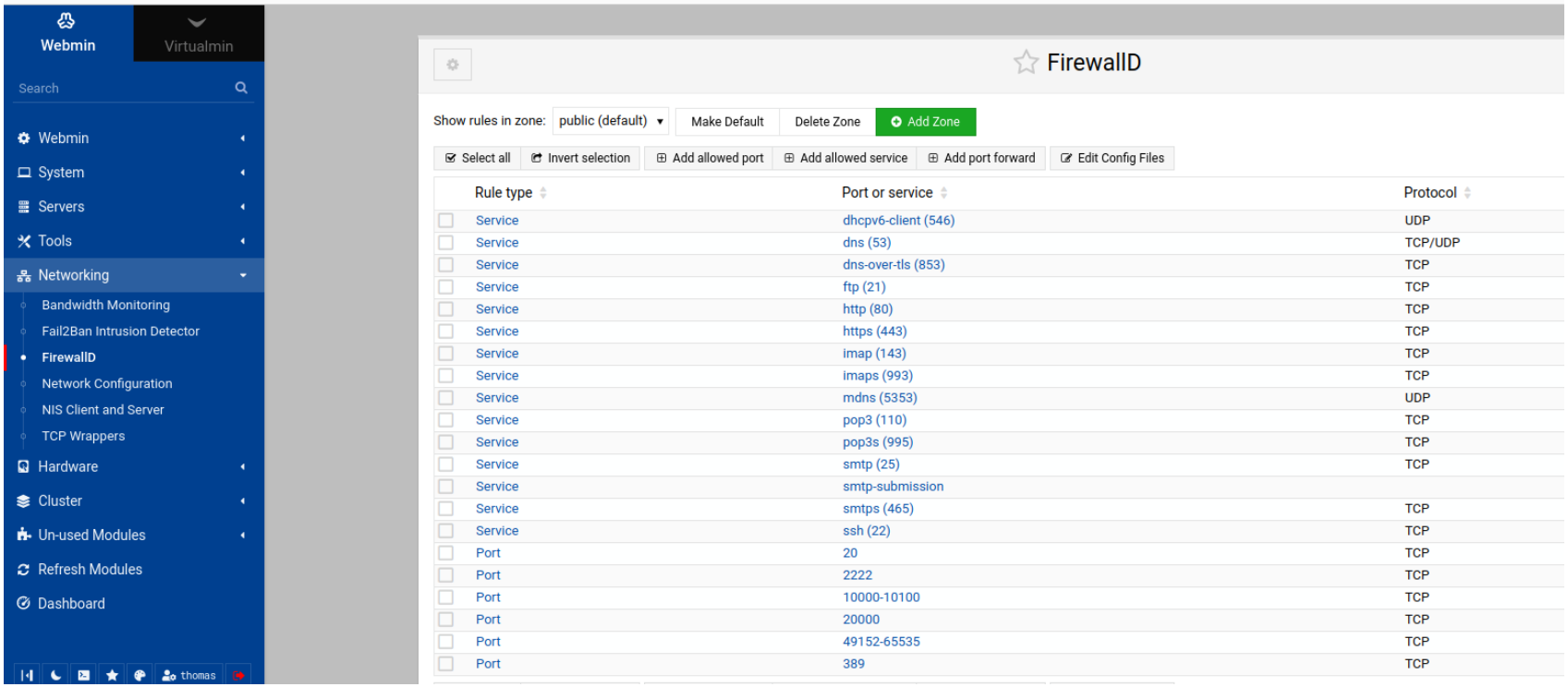
Webmin: LDAP server access control



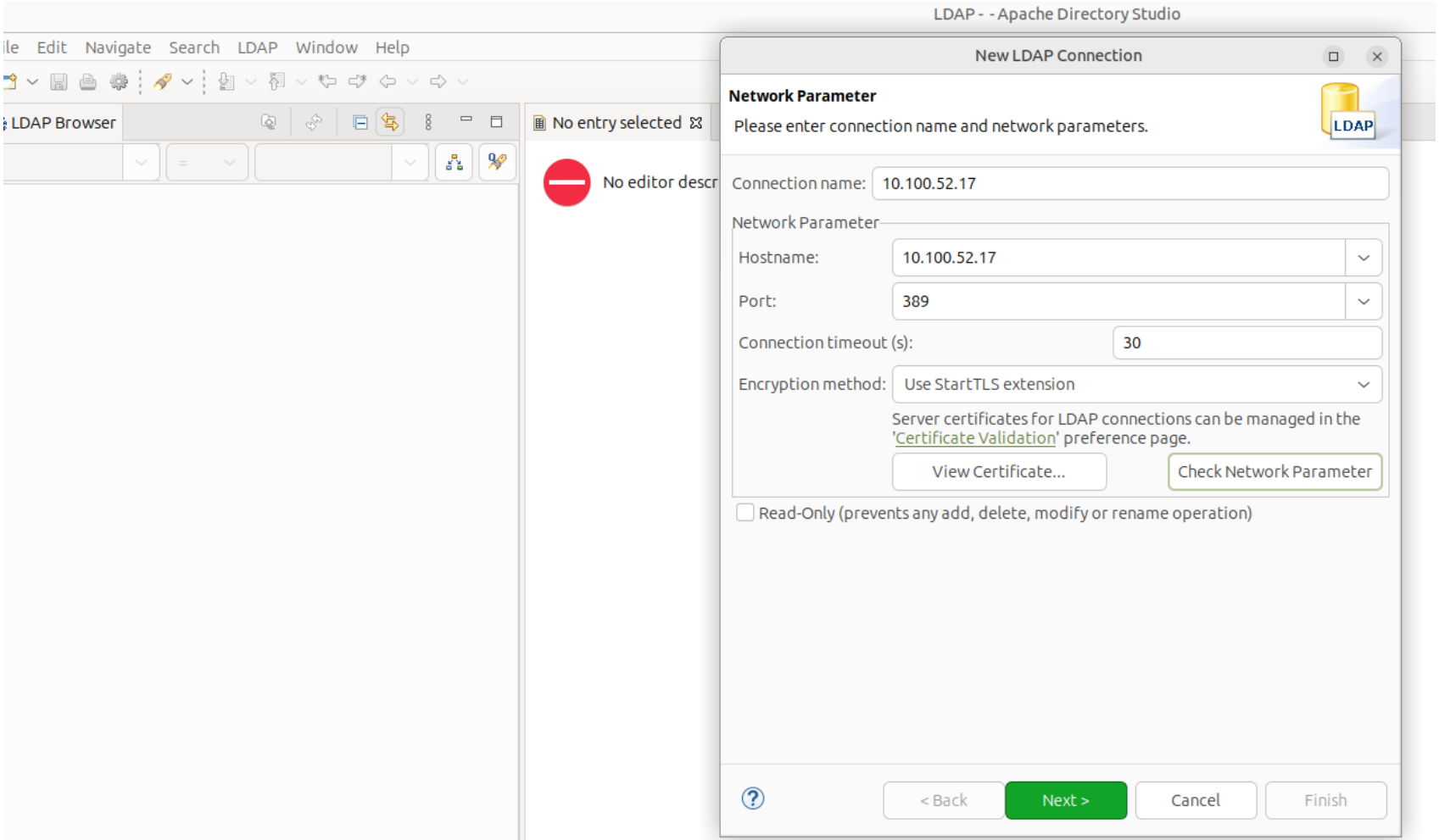
Webmin: LDAP server browser



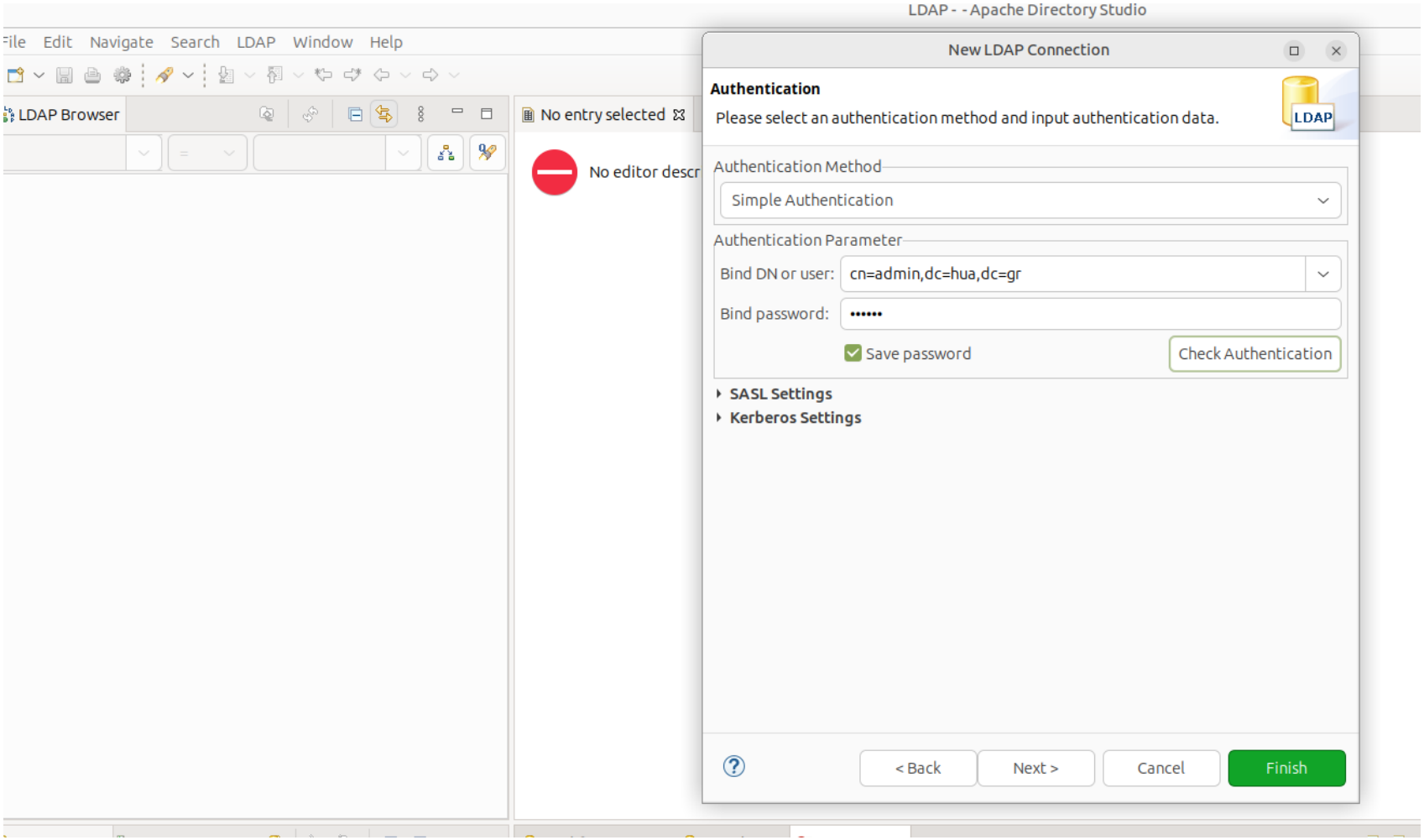
Webmin: LDAP server firewalld



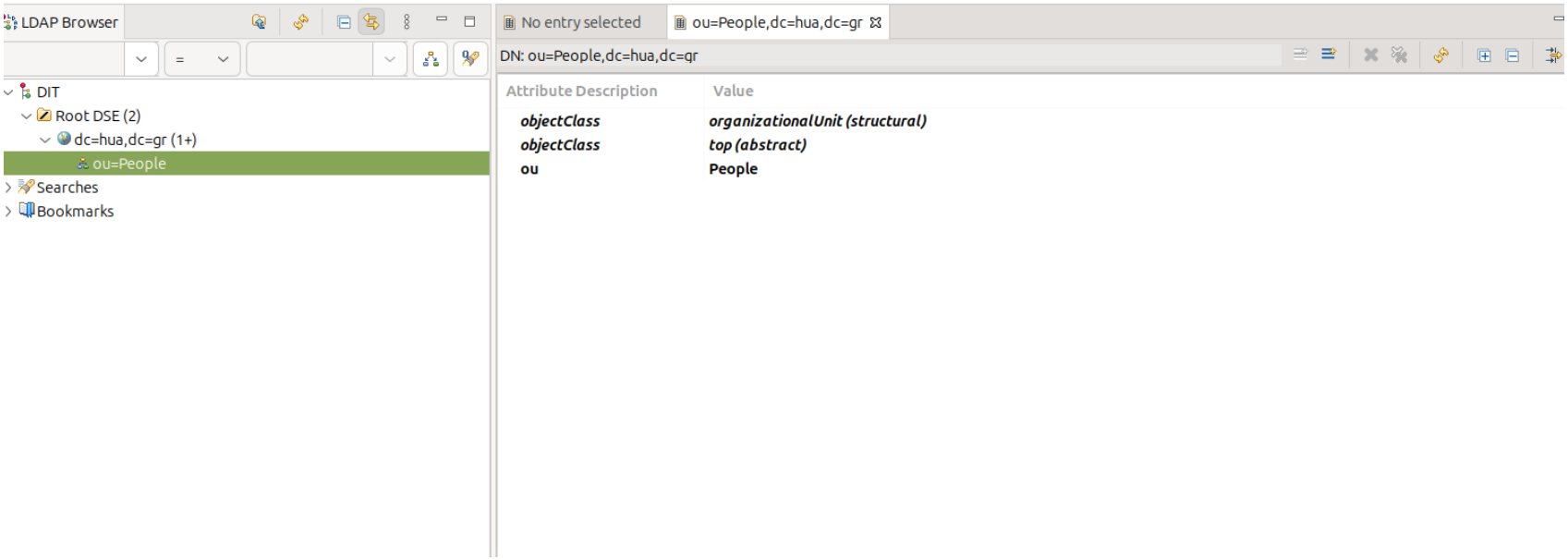
Apache Directory Studio



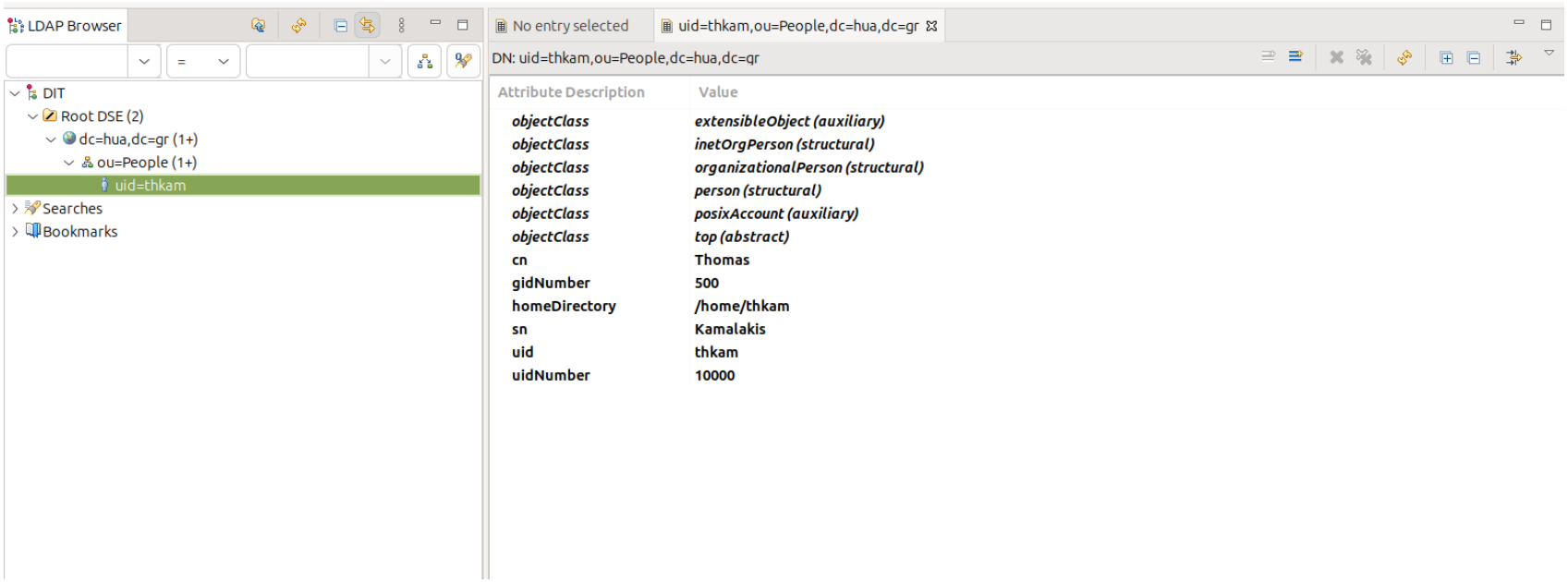
Apache Directory Studio



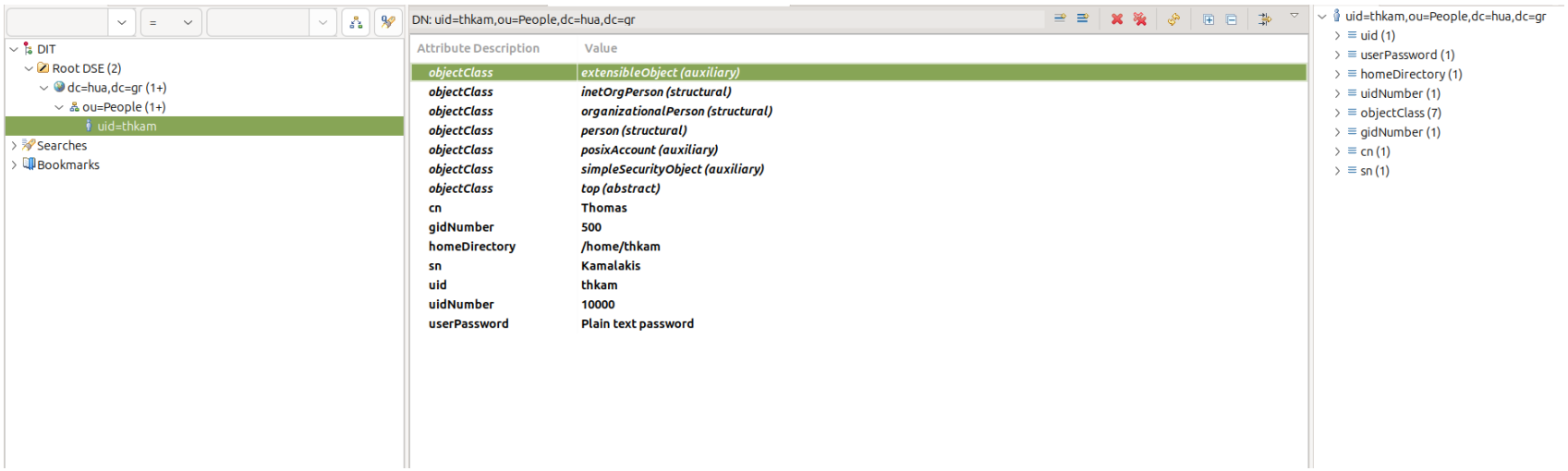
Apache Directory Studio



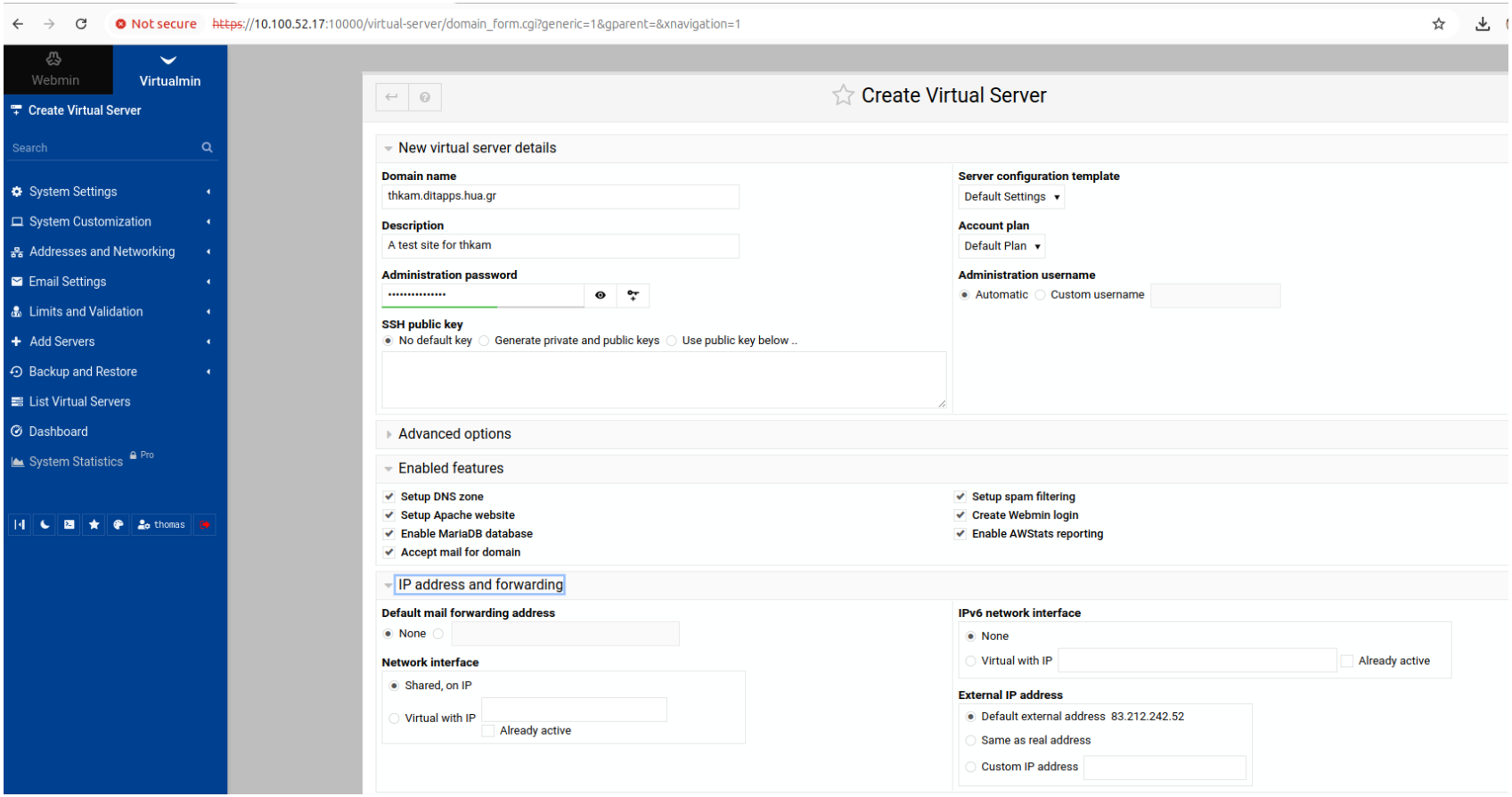
Apache Directory Studio



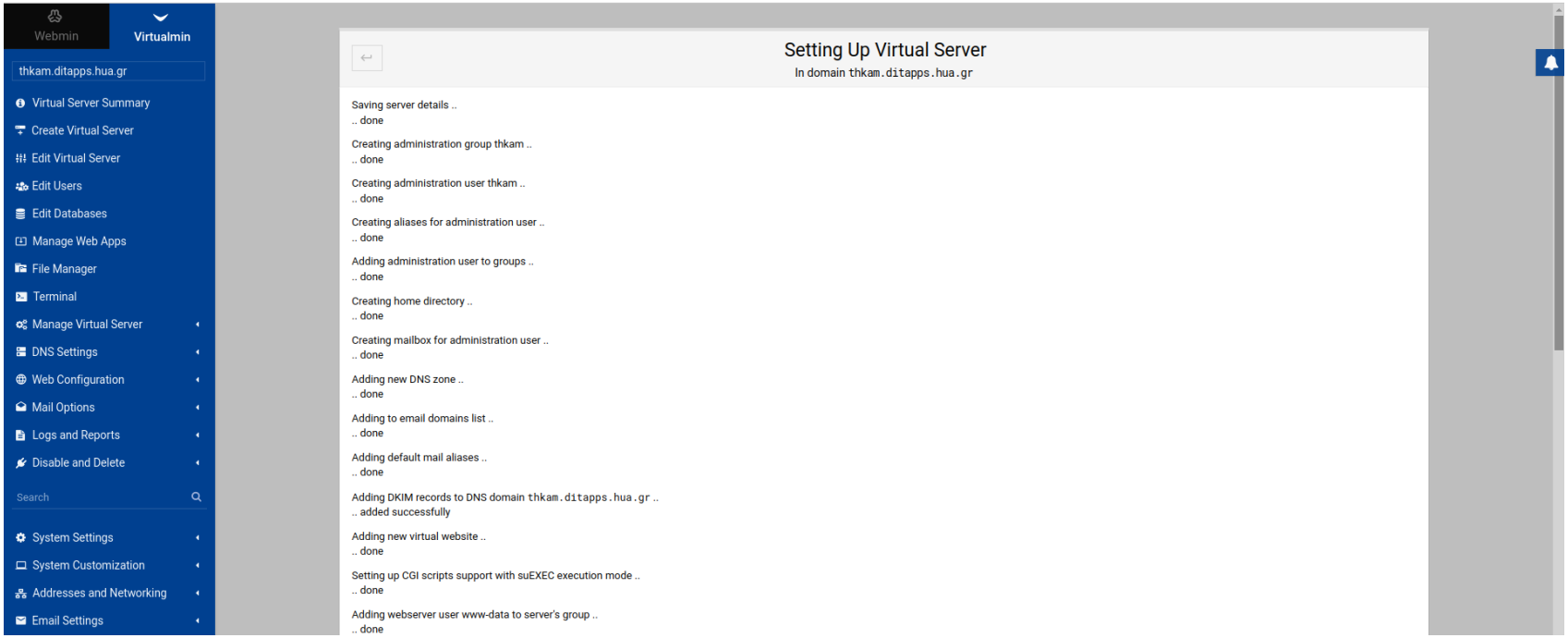
Apache Directory Studio



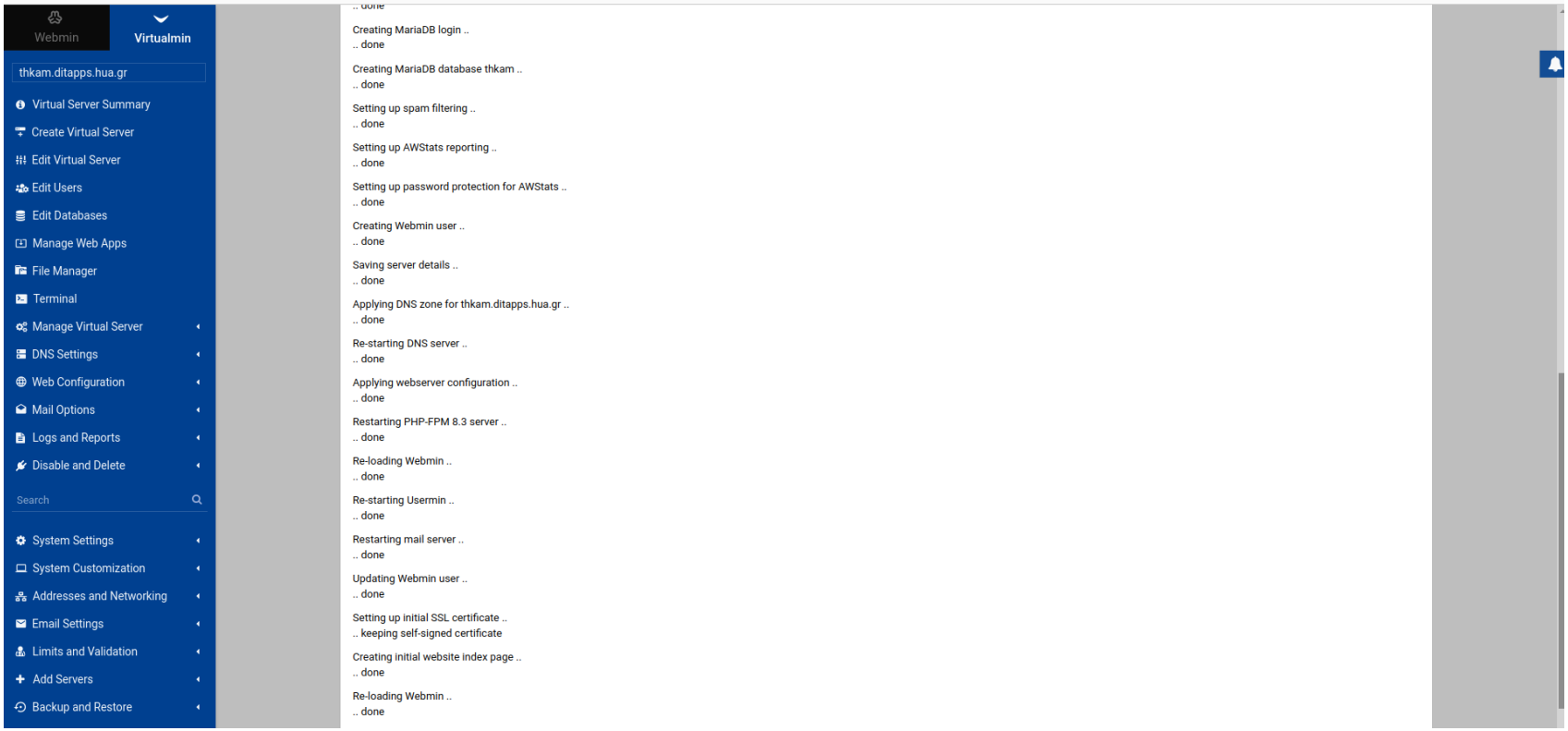
Virtualmin: New VS



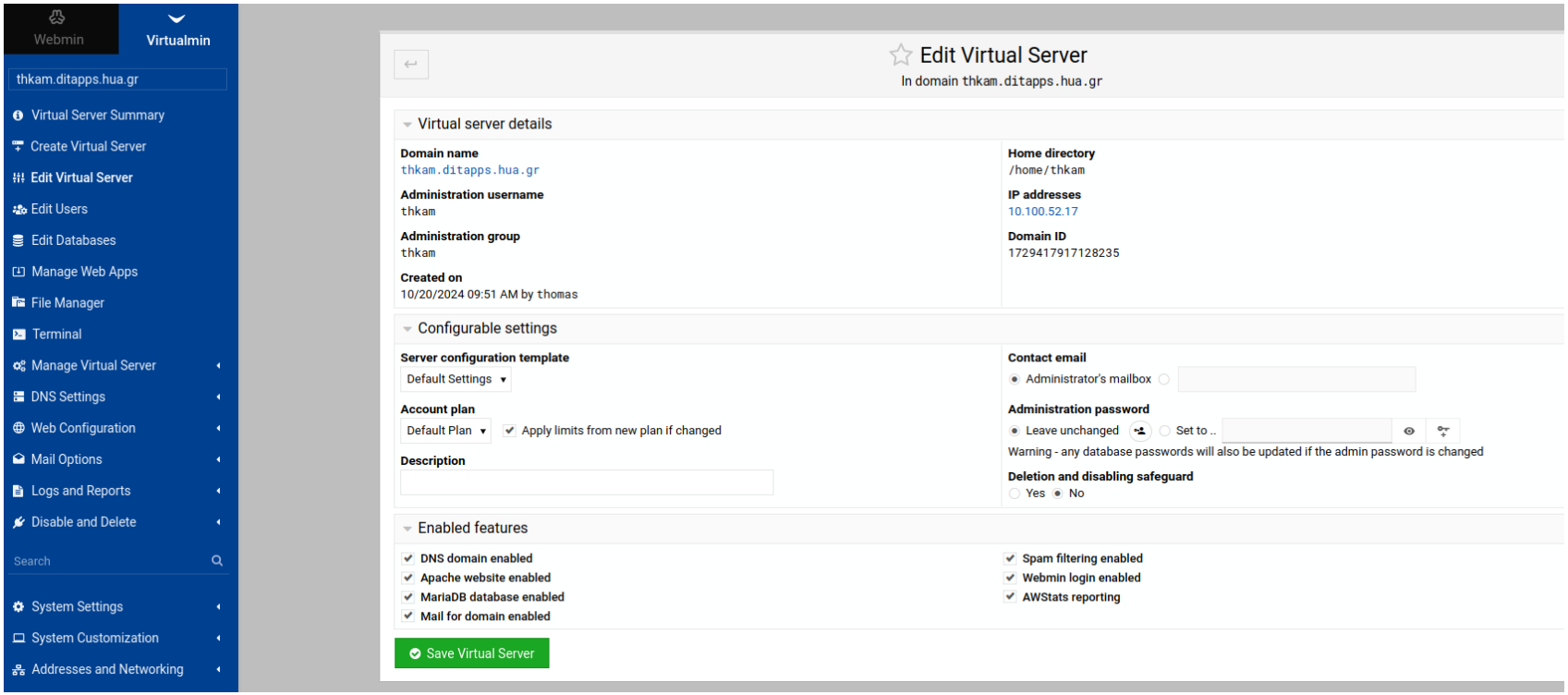
Virtualmin: New VS



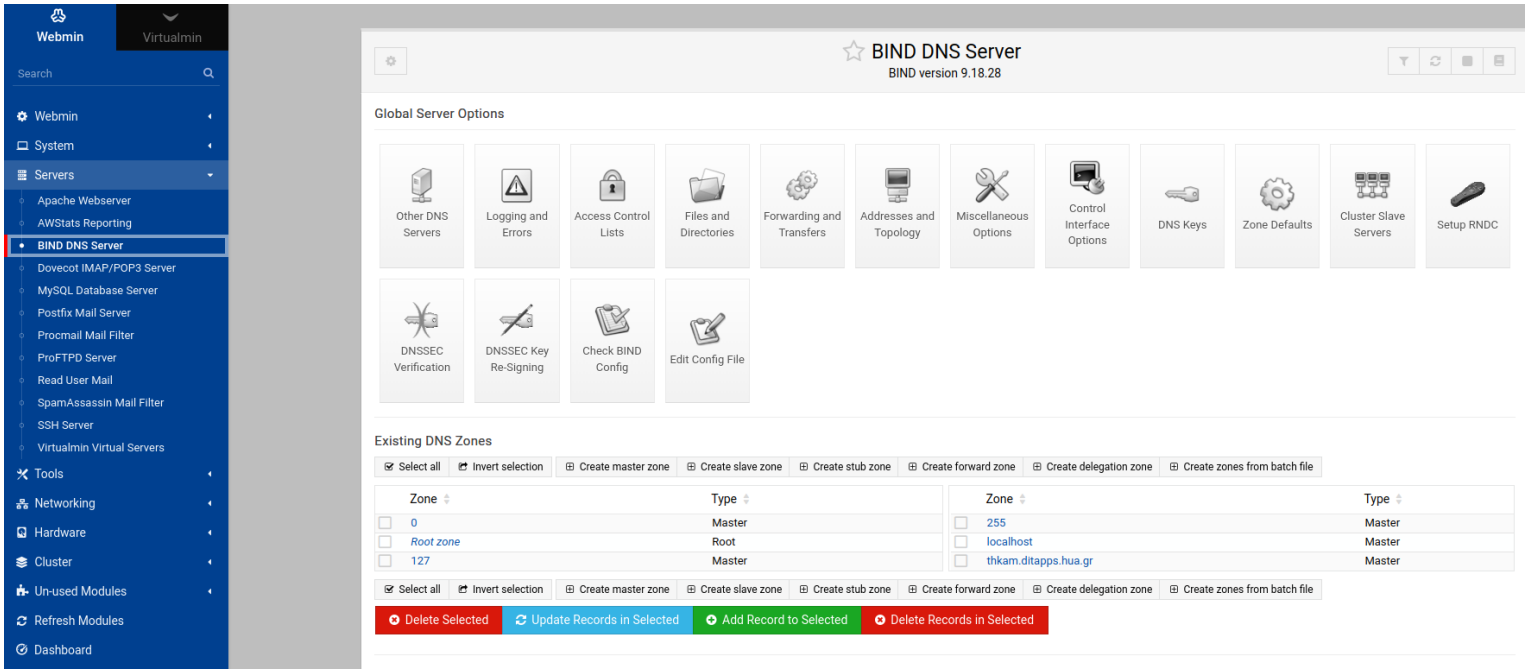
Virtualmin: New VS



Virtualmin: New VS



Virtualmin: New VS



Virtualmin: New VS

```
root@kirklaptop:/home/thomas# nc -zv 10.100.52.17 53
Connection to 10.100.52.17 53 port [tcp/domain] succeeded!
root@kirklaptop:/home/thomas# nslookup thkam.ditapps.hua.gr 10.100.52.17
Server:         10.100.52.17
Address:        10.100.52.17#53

Name:   thkam.ditapps.hua.gr
Address: 10.100.52.17
```

```
  GNU nano 7.2                          /etc/hosts
127.0.0.1 localhost
127.0.1.1 kirklaptop
10.100.59.150 overleaf.hua.gr
#83.212.224.137 dns1.hua.gr
#195.130.90.36 dns4.hua.gr
10.100.50.180 vcenter.hua.gr
10.100.125.20 nocvcenter.hua.gr
10.100.52.17 thkam.ditapps.hua.gr
#10.100.59.214 lime.ditapps.hua.gr
#10.100.51.80 earth.hua.gr
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Virtualmin: New VS

