

**POSITIVE TECHNOLOGIES**

ЗАО «ПОЗИТИВ ТЕКНОЛОДЖИЗ»  
107061, МОСКВА, ПРЕОБРАЖЕНСКАЯ ПЛ., Д. 8  
ТЕЛ. +7 495 744-01-44, ФАКС +7 495 744-01-87, PT@PTSECURITY.COM  
PTSECURITY.RU, MAXPATROL.RU, SECURITYLAB.RU

# СИСТЕМА ЗАЩИТЫ ПРИЛОЖЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА POSITIVE TECHNOLOGIES APPLICATION FIREWALL

РУКОВОДСТВО ПО УСТАНОВКЕ

Copyright © 2006–2016, Positive Technologies. Все права защищены. Настоящее руководство защищено законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности. Руководство является собственностью ЗАО «Позитив Текнолоджиз» и предоставляется пользователю в соответствии с условиями лицензионного соглашения на программное обеспечение PT Application Firewall. Пользователю запрещается копирование руководства либо его фрагментов, а также их передача третьим лицам без письменного разрешения Positive Technologies.

## ОГЛАВЛЕНИЕ

1	ВВЕДЕНИЕ.....	4
2	УСТАНОВКА ОС.....	4
2.1	Дополнительные настройки системы.....	13
3	УСТАНОВКА PT AF.....	16

# 1. Введение

Установка PT AF из дистрибутива сводится к двум шагам: установка ОС и самого PT AF.

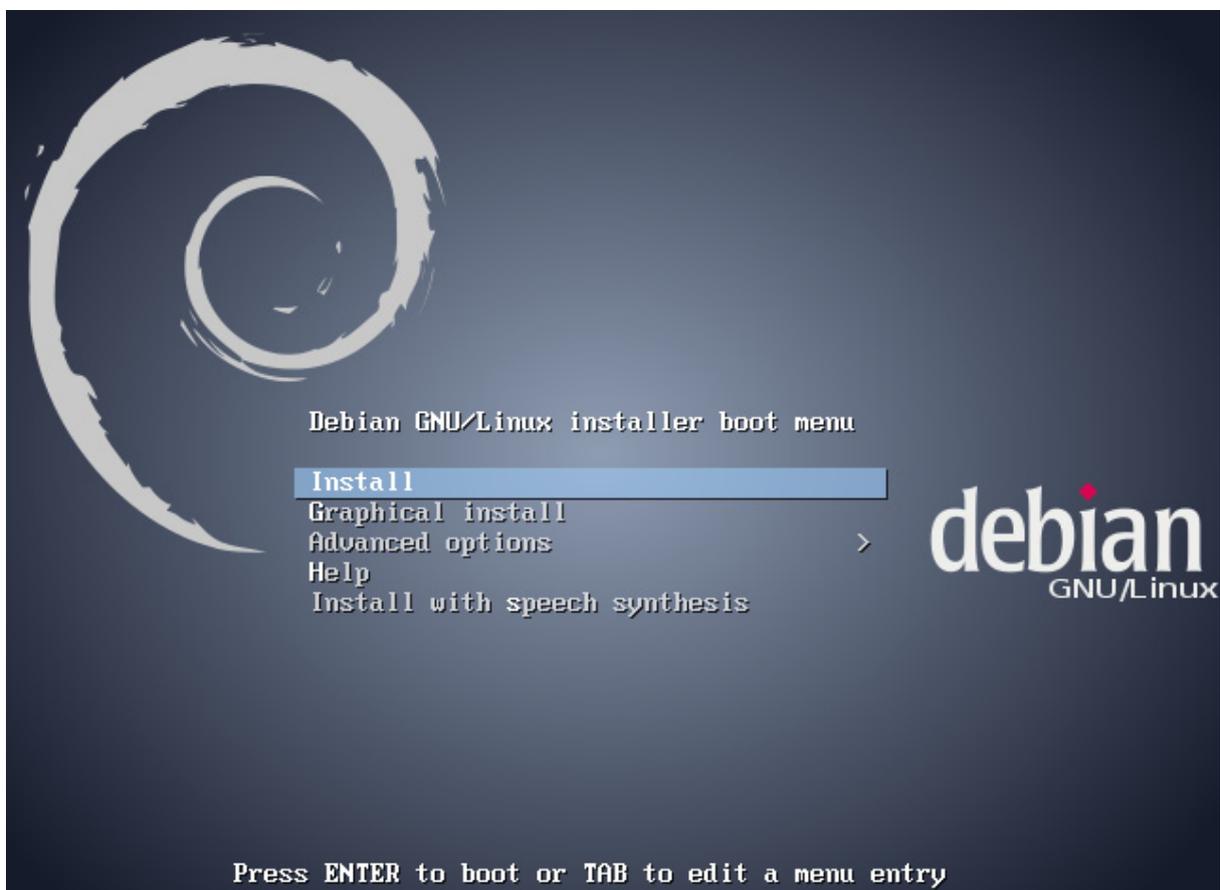
## 2. Установка ОС

Если используется физический сервер, могут потребоваться дополнительные драйвера для RAID контроллера, которых нет в стандартной сборке Debian 7.x (например, для Dell R430, R630). Для такого оборудования приходится добавлять недостающие драйвера в ISO-образ, чтобы они подхватывались на этапе установки и устанавливались вместе с ОС (сотрудники компании Positive Technologies могут предоставить сборки для моделей Dell и HP). Если все же возникла проблема, когда на этапе разметки диска не отображается ни один раздел, то:

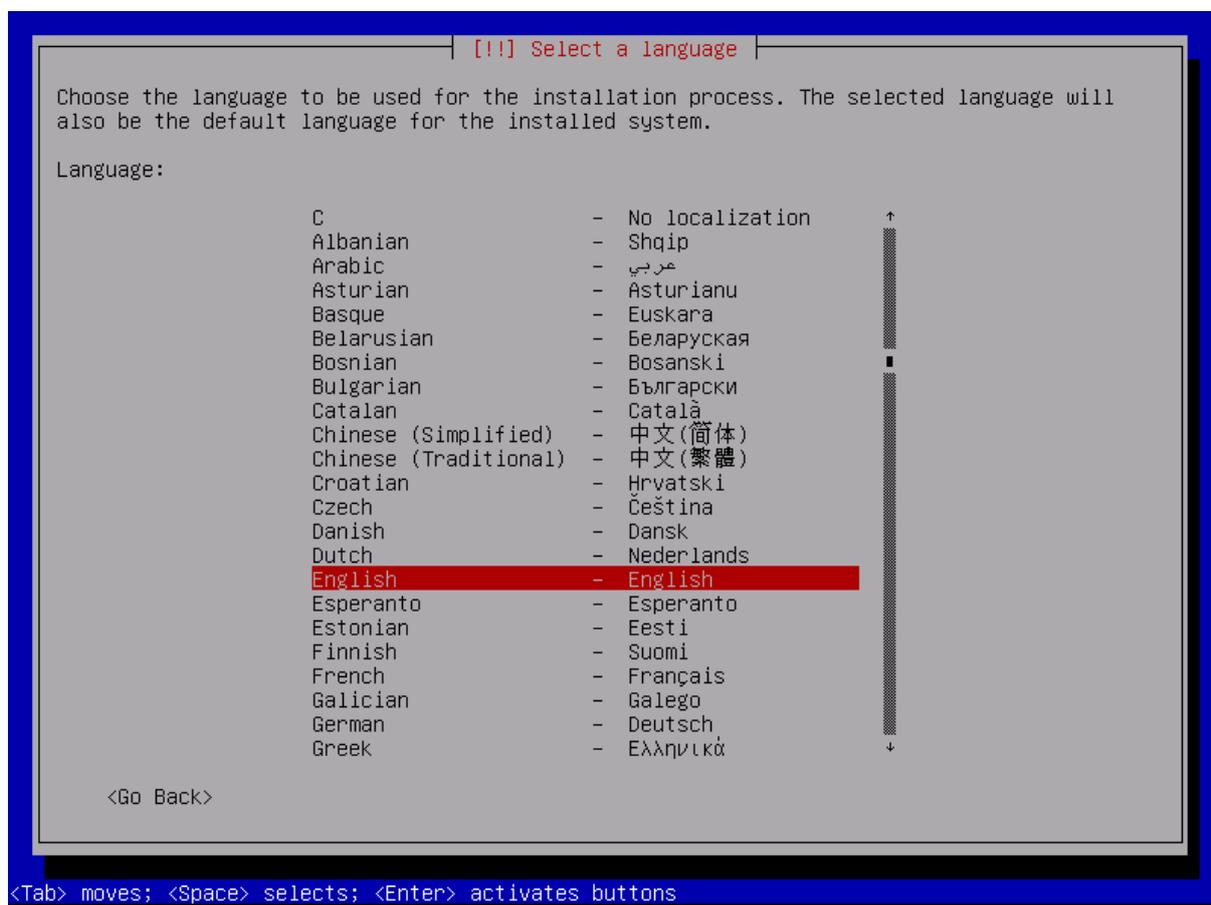
- Проверьте, собран ли RAID;
- Сообщите сотрудникам компании Positive Technologies о необходимости добавления дополнительных драйверов в сборку.

Для установки ОС требуется выполнить следующие шаги:

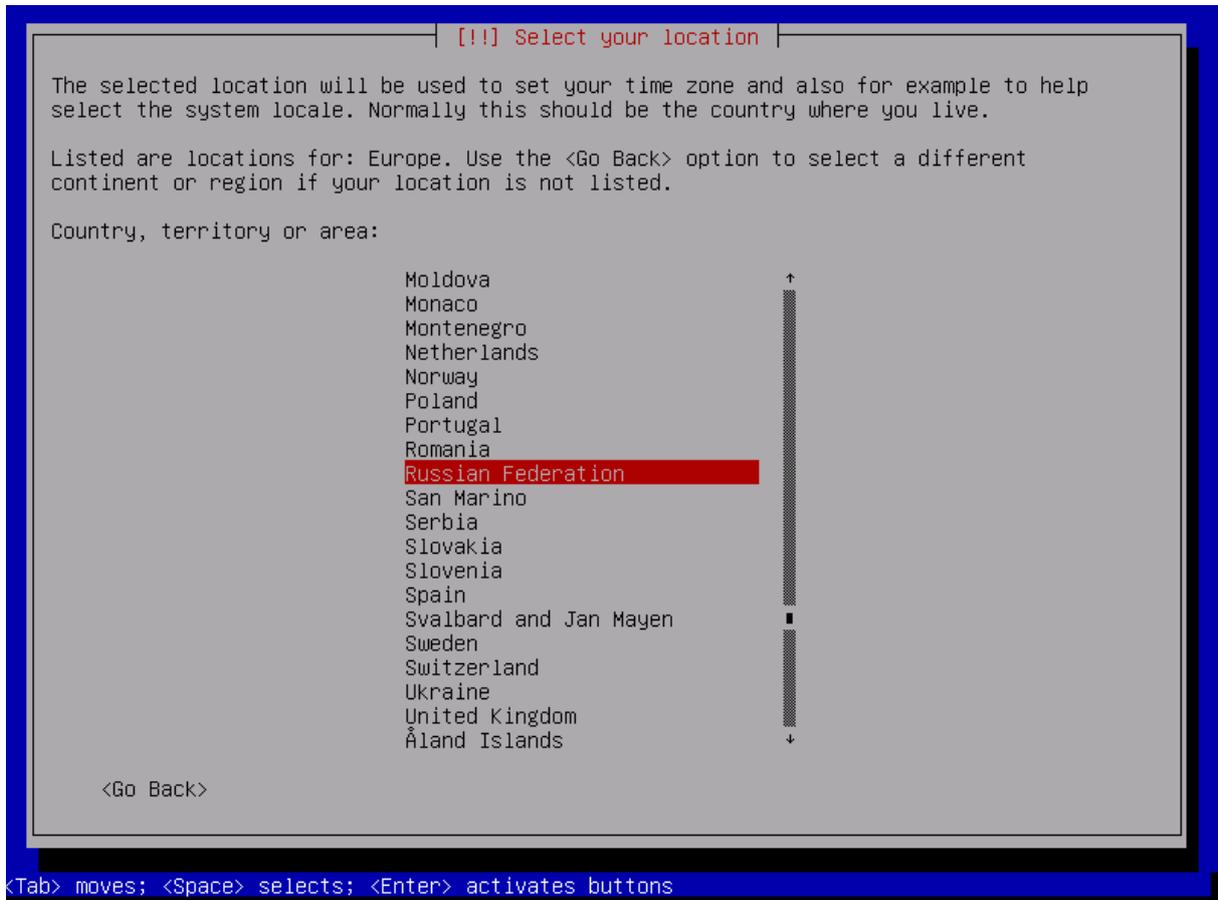
- Запустить установщик ОС;
- Выбрать опцию Install:



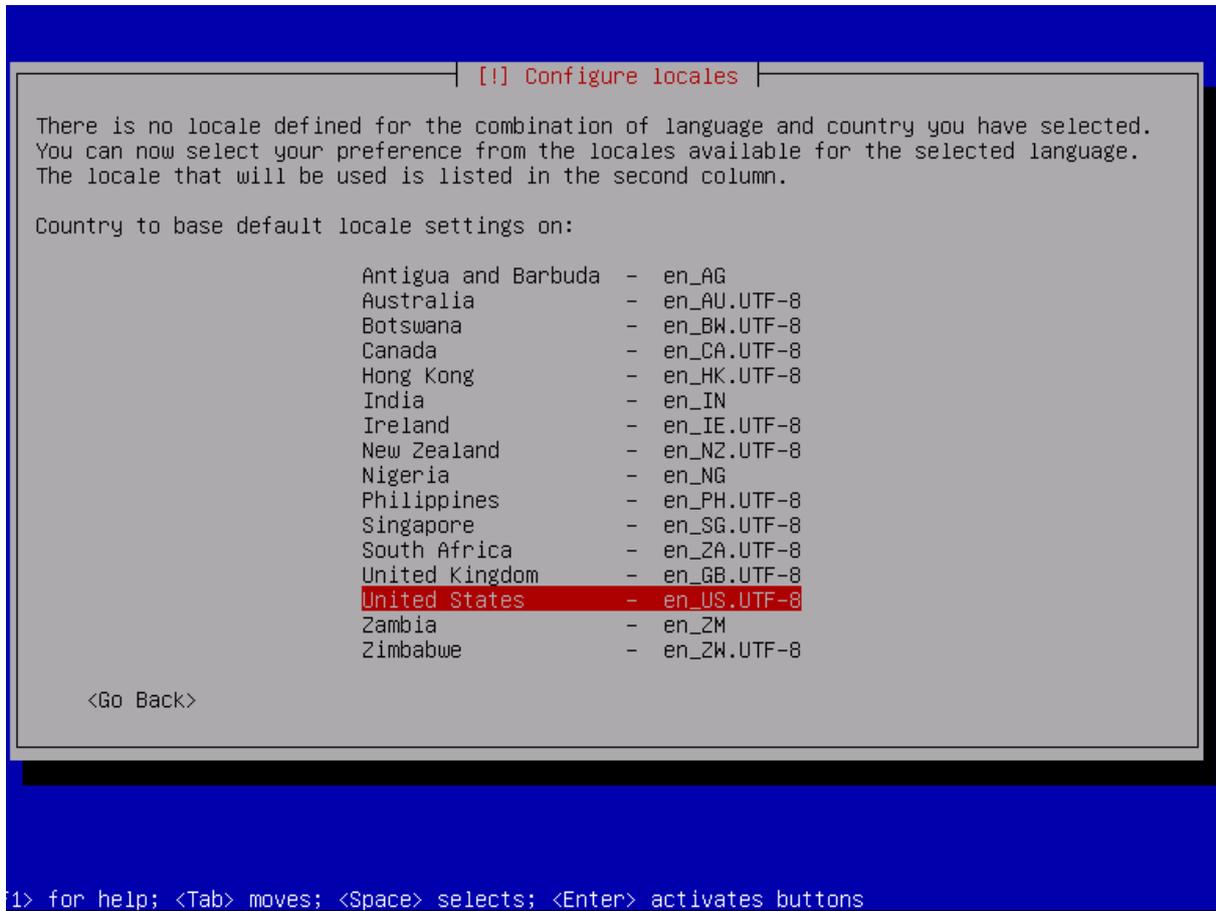
- Выбрать язык: English;



- Выбрать страну: Russian Federation;



- Выбрать страну для установки локальных опций по умолчанию: United States;

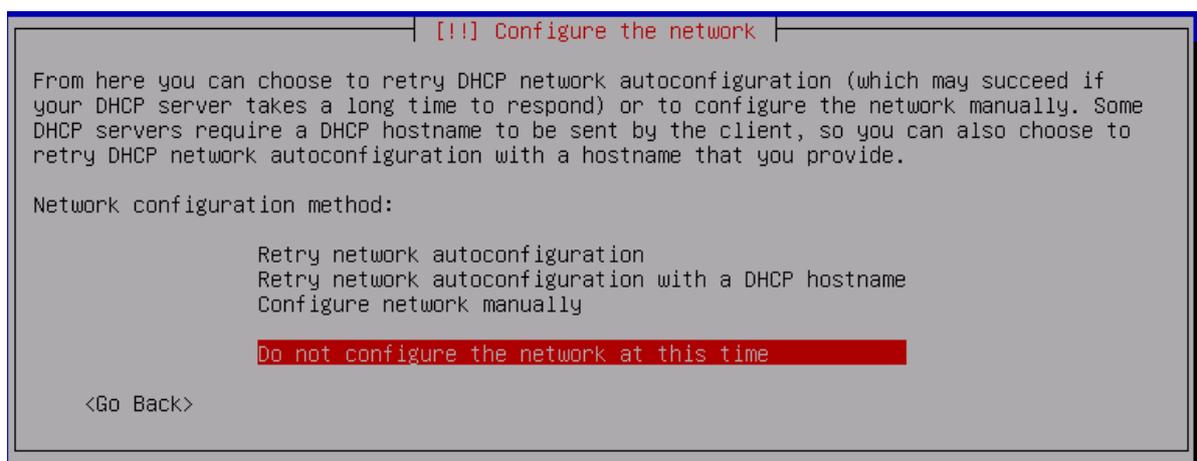


- Выбрать раскладку: American English;



- Если есть соединение с сетью, можно автоматически получить IP-адрес по DHCP, и позже получится установить пакеты типа OpenSSH во время процедуры установки. Однако, в данном руководстве рассмотрен случай, когда DHCP не настроено, или вовсе нет соединения с сетью.

Выбрать метод конфигурации сети: Do not configure network this time;



- Задать имя узла, например «ptaf»:

[!!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

ptaf

<Go Back> <Continue>

- Ввести пароль для root:

[!!] Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

jjjjjjjj

<Go Back> <Continue>

- Создать нового пользователя pt:

[!!] Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:

pt

<Go Back> <Continue>

- Задать пароль для pt:

```
[!] Set up users and passwords

Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:
*****

<Go Back>                                <Continue>
```

- Выбрать временную зону: Moscow+00;

```
[!] Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language"
and select a country that uses the desired time zone (the country where you live or are
located).

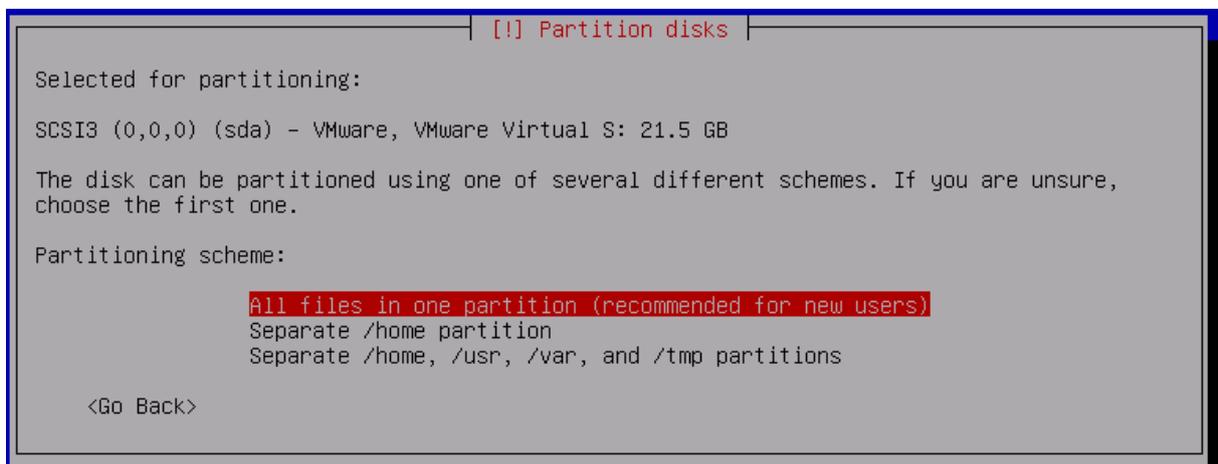
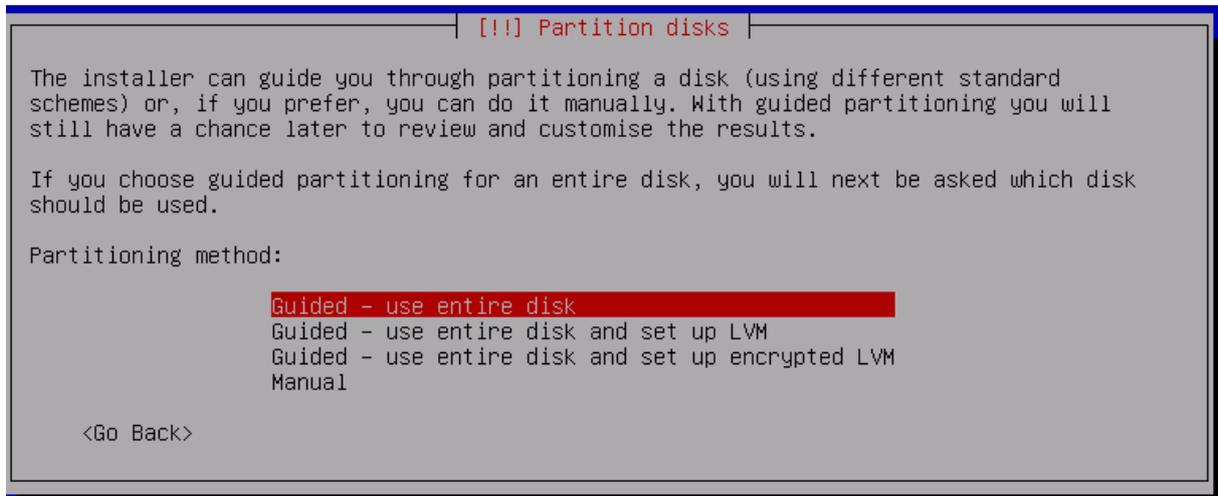
Select your time zone:

Moscow-01 - Kaliningrad
Moscow+00 - Moscow
Moscow+02 - Yekaterinburg
Moscow+03 - Omsk
Moscow+04 - Krasnoyarsk
Moscow+05 - Irkutsk
Moscow+06 - Yakutsk
Moscow+07 - Vladivostok
Moscow+08 - Magadan

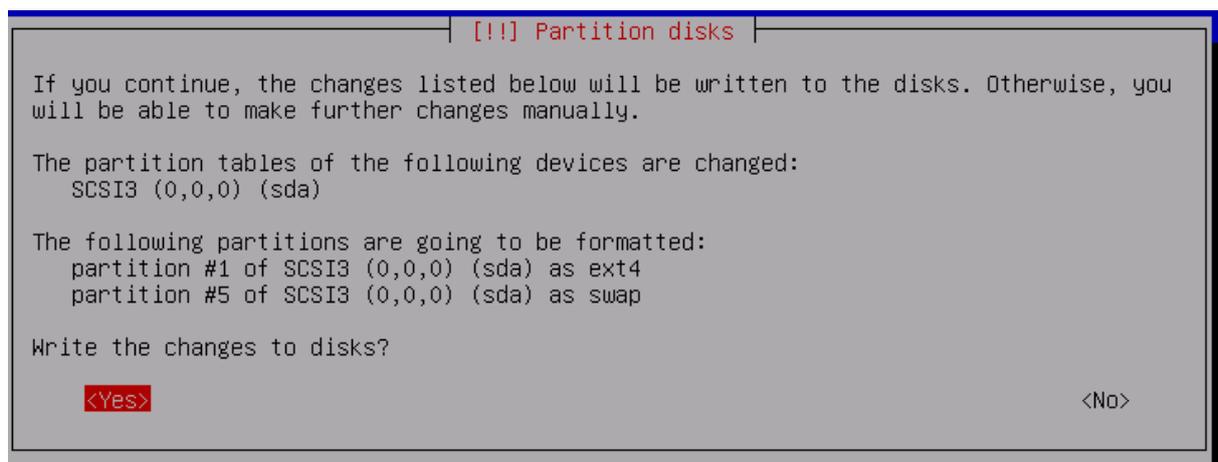
<Go Back>
```

- В зависимости от объема диска выбрать «Guided – use entire disk» («All files in one partition») или разбить диск вручную. Для ручной настройки разделов рекомендуется:

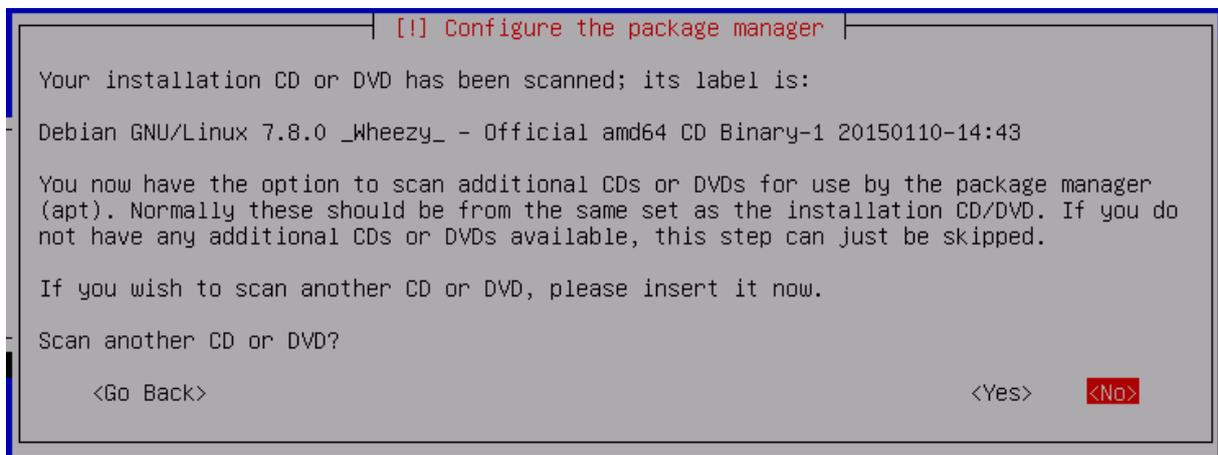
50 ГБ — /  
50 ГБ — /tmp  
20 ГБ — /home  
20 ГБ — /opt  
RAM-2xRAM — swap  
Остальное — /var



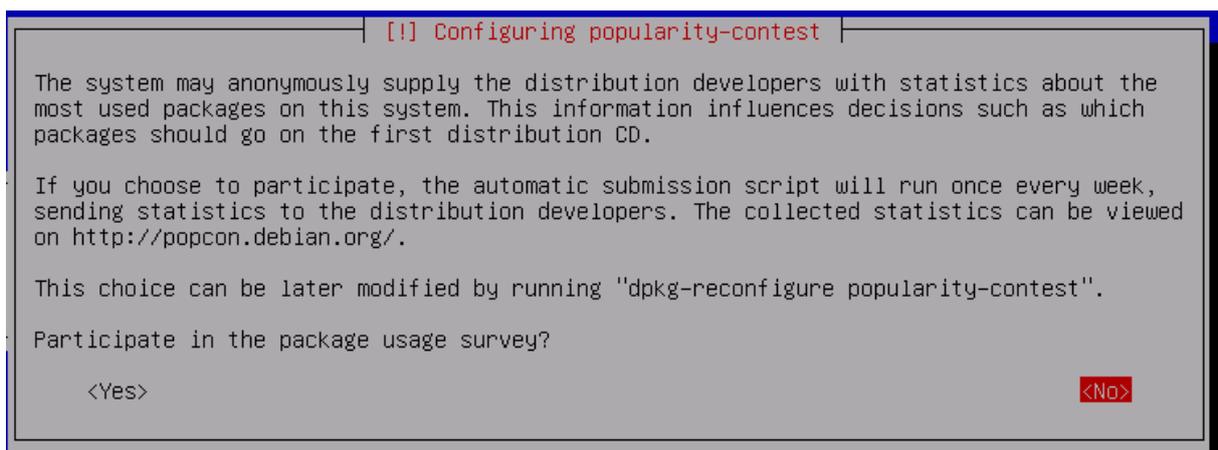
- Записать изменения на диск:



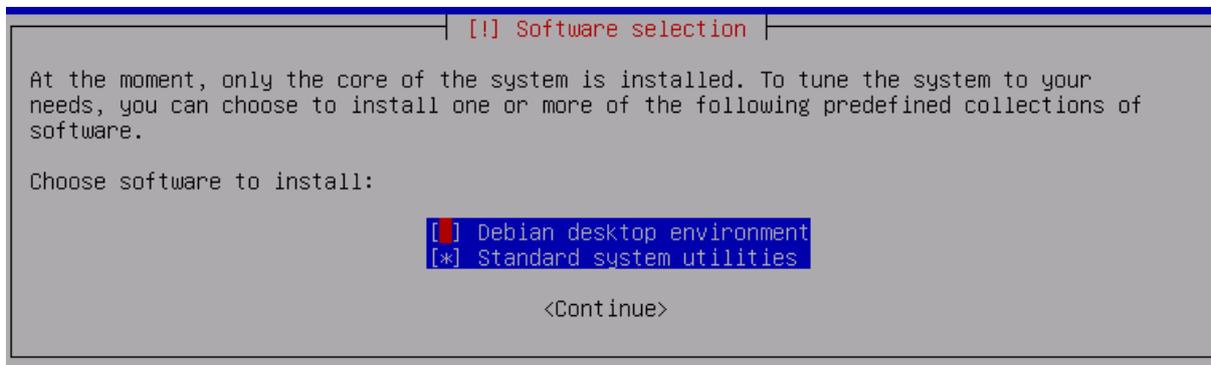
- Не сканировать другой CD-ROM: Scan another SD or DVD? - NO;



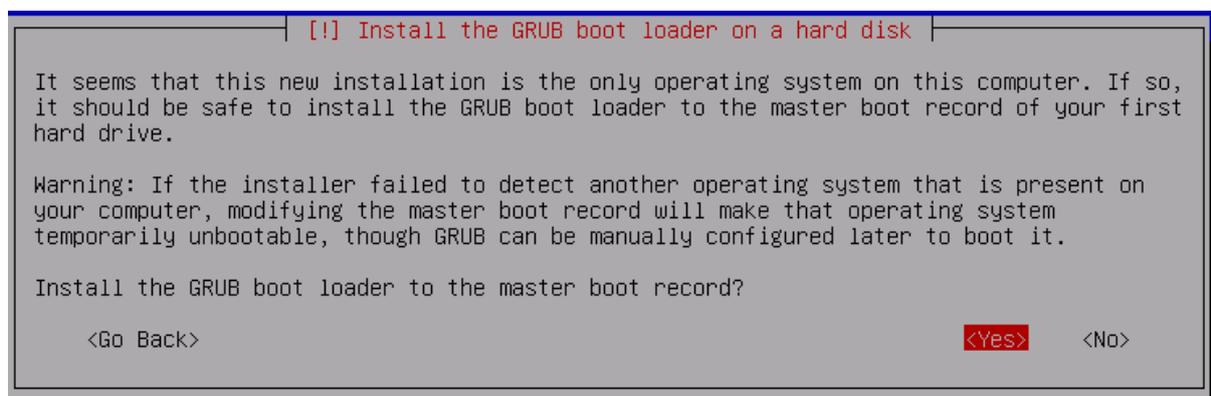
- Если нет соединения с сетью, задать зеркало для репозитория не получится;
- Выбрать «No» в ответе на вопрос о сборе информации:



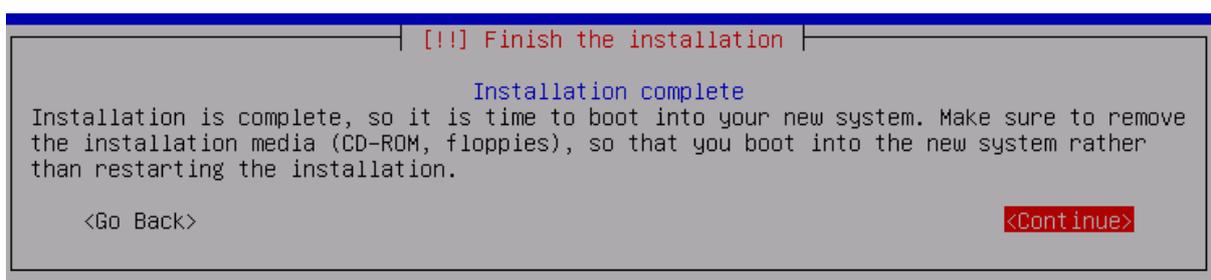
- Установить только опцию Standard system utilities без Desktop environment. Если в процессе установки удалось настроить соединение с интернетом, то выберите дополнительно опцию OpenSSH server (если она появится в списке);



- Установить GRUB:



- Завершить установку.



## 2.1. Дополнительные настройки системы

Дополнительно требуется провести следующие настройки:

- Авторизоваться под учетной записью pt и повысить привилегии до root (su – и ввести пароль root);
- Примонтировать cdrom:
  - Если используется USB-накопитель, то можно с помощью fdisk определить имя устройства (например, /dev/sdb1):

```
fdisk -l
...
Disk /dev/sdb: 4032 MB, 4032626688 bytes
255 heads, 63 sectors/track, 490 cylinders, total 7876224 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x10e563be
```

```
Device Boot      Start          End      Blocks   Id  System
/dev/sdb1  *        2048      7876223     3937088    c   W95 FAT32 (LBA)
```

**- Примонтировать устройство:**

```
mkdir debian
mount /dev/cdrom debian
В случае USB-флешки: mount /dev/sdb1 debian
```

**• Установить openssh и sudo:**

```
dpkg -i /debian/pool/main/o/openssh/openssh-server_6.0p1-4+deb7u2_amd64.deb
dpkg -i /debian/pool/main/o/openssh/openssh-client_6.0p1-4+deb7u2_amd64.deb
dpkg -i /debian/pool/main/s/sudo/sudo_1.8.5p2-1+nmul_amd64.deb
```

**• Добавить пользователя pt в группу sudoers:**

```
usermod -aG sudo pt
```

**• Настроить сеть и подключиться к серверу по SSH;**

**• Добавить безопасные настройки в SSH:**

- Чтобы отключить доступ root к системе, следует поменять в файле `/etc/ssh/sshd_config` строку на:

```
PermitRootLogin no
```

**- Перезапустить службу SSH:**

```
sudo service ssh restart
```

**• Добавить опции безопасности в ядро linux:**

- Добавить в конец файла `/etc/sysctl.conf` следующие строки:

```
kernel.core_uses_pid = 1
kernel.ctrl-alt-del = 0
kernel.kptr_restrict = 1
kernel.sysrq = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.bootp_relay = 0
net.ipv4.conf.all.forwarding = 0
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.proxy_arp = 0
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.send_redirects = 0
```

```
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.log_martians = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_timestamps = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_redirects = 0
net.ipv6.conf.default.accept_source_route = 0
```

- Применить их:

```
sysctl -p
```

• Настроить репозитории:

- Отредактировать файл `/etc/apt/sources.list` таким образом, чтобы он содержал только следующие строки:

```
deb http://mirror.yandex.ru/debian/ wheezy main non-free contrib
deb-src http://mirror.yandex.ru/debian/ wheezy main non-free
contrib
deb http://security.debian.org/ wheezy/updates main contrib non-
free
deb-src http://security.debian.org/ wheezy/updates main contrib
non-free
```

- Обновить информацию о пакетах:

```
sudo apt-get update
```

- Установить пакеты:

```
sudo apt-get install curl ngrep tcpdump pv vim htop
```

## 3. Установка PT AF

Дистрибутив PT AF представляет собой архивный файл tarball. Его необходимо скопировать на сервер и выполнить ряд действий:

- Разархивировать:

```
tar xvf waf_kickstart_xxx.tar
```

- Установить PT AF:

```
cd waf_kickstart
./install.sh
```

**Примечание.** Если во время установки появится приглашение для ввода «node>», туда нужно ввести слово «single».

- Отключить модуль `bypass` для сетевых карт (включен по умолчанию для карт Silicom):

- Разархивировать `bypass.tgz`:

```
tar xvf bypass.tgz
```

- Запустить скрипт установки:

```
./install_bypass.sh
```

**Примечание.** Если в процессе установки появлялись ошибки с зависимостями, выполнить: `sudo apt-get install -f`

- Отключить режим `bypass`:

```
bpctl_util all set_bypass off
```

- Чтобы отключать `bypass` при загрузке системы, добавить в файл `/etc/rc.local` строки:

```
/bin/bpctl_start
/bin/bpctl_util all set_bypass off
```

- Настроить сеть:

- Использовать системные утилиты для настройки сети:

```
ifconfig eth0 192.168.0.10 netmask 255.255.255.0
```

- Запустить `wsc` и применить сетевые настройки:

```
config commit
if mark eth0 eth1 eth2
config sync
```

**Примечания.**

Команда `config commit` перезапишет системные конфигурационные файлы и перезапустит сеть. Прежде чем выполнять ее при подключении через SSH, рекомендуется убедиться, что сеть настроена правильно и присутствуют все нужные маршруты.

При необходимости удалите файлы, где хранятся текущие настройки, чтобы восстановить `wsc` настройки по умолчанию: `rm /opt/waf/conf/local-waf-sync-config.json`

- Подключитесь к веб-интерфейсу PT AF (по умолчанию используется 80 порт);
- Активируйте ключ Guardant (ключ должен быть подключен заранее);
- Проверьте, что в системе созданы необходимые роли (WAN, LAN, MGMT, SPAN), или создайте роли на вкладке *Конфигурация* -> *Алиасы сетевых интерфейсов*;

**АЛИАСЫ СЕТЕВЫХ ИНТЕРФЕЙСОВ**

Список (4)    Создать    С выбранным    Поиск

Имя	Тип	Открытые TCP порты
Default	DB	4000, 10050, 5380, 27017, 27018, 6379, 9900, 9200, 8082, 9300, 2812
WAN	WAN	
LAN	LAN	
MGMT	MGMT	22

2012-2015 © POSITIVE TECHNOLOGIES

- Назначьте роли на используемые сетевые интерфейсы на вкладке *Конфигурация* - > *Шлюзы* -> *Сеть* (например, eth0: WAN+MGMT, eth1: SPAN);

**ШЛЮЗЫ**

Основные    Сеть    Прокси

Сетевой интерфейс

eth0    Сеть    x WAN-WAN    x MGMT-MGMT

Модули

DNS

Дата и время

DHCP   

IP    192.168.0.10

Netmask    255.255.255.0

Gateway    192.168.0.1

MAC Address    00:0c:29:06:e6:96

- Включите опцию *Активен* на вкладке *Конфигурация* -> *Шлюзы* - > *Основные* и сохраните настройки.

**Positive Technologies** — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Компания входит в число наиболее динамично развивающихся участников российской IT-отрасли, демонстрируя ежегодный рост более 50%. Офисы и представительства Positive Technologies расположены в Москве, Лондоне, Риме, Сеуле и Тунисе.

Разработанные экспертами компании программные продукты заслужили международное признание в сфере практической информационной безопасности.

### **Продукты**

Система контроля защищенности и соответствия стандартам MaxPatrol помогает обеспечивать безопасность корпоративных информационных систем и формировать комплексное представление о реальном уровне защищенности IT-инфраструктуры организации. Система позволяет контролировать выполнение требований государственных, отраслевых и международных стандартов, таких как Федеральный закон № 152-ФЗ «О персональных данных», СТО БР ИББС, ISO 27001/27002, SOX 404, PCI DSS. В MaxPatrol объединены активные механизмы оценки защищенности, включая функции системных проверок, тестирования на проникновение, контроля соответствия стандартам — в сочетании с поддержкой анализа различных операционных систем, СУБД и веб-приложений.

Система анализа защищенности XSpider более 10 лет является признанным лидером среди средств сетевого аудита ИБ. На сегодняшний день это один из лучших интеллектуальных сканеров безопасности в мире. Более 1000 международных компаний успешно используют XSpider для анализа и контроля защищенности корпоративных ресурсов.

### **Услуги**

Компания Positive Technologies специализируется на проведении комплексного аудита информационной безопасности, на оценке защищенности прикладных систем и веб-приложений, тестировании на проникновение и внедрении процессов мониторинга информационной безопасности. Статус PCI DSS Approved Scanning Vendor позволяет проводить работы по проверке соответствия данному стандарту.

### **Клиенты**

В числе заказчиков Positive Technologies — более 1000 государственных учреждений, финансовых организаций, телекоммуникационных и розничных компаний, промышленных предприятий России, стран СНГ и Балтии, а также Великобритании, Германии, Голландии, Израиля, Ирана, Китая, Мексики, США, Таиланда, Турции, Эквадора, ЮАР и Японии.

### **Вклад в индустрию**

Принимая активное участие в развитии IT-отрасли, Positive Technologies выступает организатором международного форума по информационной безопасности Positive Hack Days и развивает SecurityLab.ru — самый популярный ИБ-портал на русском языке.

Более подробную информацию можно получить на сайте [www.ptsecurity.ru](http://www.ptsecurity.ru)

