Дәріс №12: Checkpoint NGX брандмауэрінің негізгі мүмкіндіктерін зерттеу

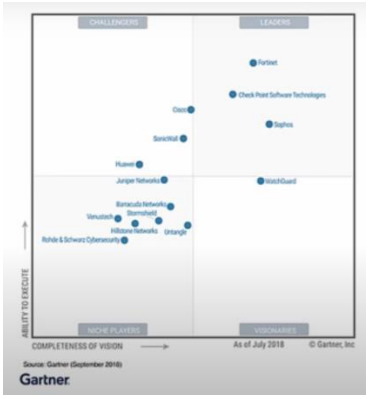
Unified threat management (UTM, UTM-жүйе, UTM-шешім, UTM-құрылғы, қауіпсіздік шлюзі) — әмбебап құрылғы, желілік қауіптерден қуатты кешенді қорғауды қамтамасыз ететін компьютерлік қауіпсіздік саласындағы шешім. UTM мәні - бір шешімде бірнеше қорғаныс құралдарын шоғырландыру. Ең көп таралған нұсқа: брандмауэр, IPS, Proxy (URL сүзу), ағындық Антивирус, Анти-спам, VPN және т.б.

Next Generation Firewall (NGFW) - келесі буын брандмауэрі. Бұл тұжырымдама UTM-ге қарағанда әлдеқайда кешірек пайда болды. Ngfw негізгі идеясы - кірістірілген IPS көмегімен пакеттерді терең талдау (DPI) және қолданбалы деңгейдегі қол жетімділікті бөлу (Application Control). Бұл жағдайда IPS пакеттердің ағынында оны шешуге немесе тыйым салуға мүмкіндік беретін осы немесе басқа қосымшаны анықтау үшін қажет. Мысал: біз Skype жұмысына рұқсат бере аламыз, бірақ файлдарды жіберуге тыйым саламыз. Torrent немесе RDP пайдалануға тыйым сала аламыз. Сондай-ақ, веб-қосымшаларға қолдау көрсетіледі: кіруге рұқсат етіледі VK.com.бірақ ойындарға, хабарламаларға немесе бейнелерді көруге тыйым салыңыз. Негізінен, NGFW сапасы ол анықтай алатын қосымшалардың санына байланысты. Көптеген адамдар Ngfw тұжырымдамасының пайда болуы Palo Alto өзінің қарқынды өсуін бастаған әдеттегі маркетингтік қадам болды деп санайды.

Check Point Software Technologies Ltd. 1993ж. құрылған, 4500-ден аса қызметкері бар Израиль компаниясы. Жылдық табысы 31 наурыз 2020 есеп бойынша 1,349 млн. АҚШ долларын құрайды.

Негізгі артықшылықтары:

1) Тек қана Ақпараттық қауіпсіздік саласымен айналысады;
2) Gartner және NSS Labs зерттеулері бойынша лидер;
3) Check Point өнімі 100 000 компанияларда қолданылады.



2018

2020

2020

2020 жылдың бірінші тоқсанында шешімдер портфелін жаңартудағы басты назар **Infinity** архитектурасын қауіптердің алдын-алу, сұраныстың

масштабталуын қамтамасыз ету және бірыңғай қауіпсіздік жүйесін қамтамасыз ету үшін кеңейтуге арналған шешімдерге аударылды.

Сәуір айында Қауіпсіздік шлюздерін **Quantum Security Gateways** жаңа буынына жаңарту ұсынылды. Қауіпсіздік шлюздерінің 15 үлгісінен тұратын жаңа желі **Infinity** архитектурасын филиалдардан деректер орталығына дейін кеңейтеді. Барлық кванттық модельдер **Sandblast Zero-day Protection** негізінде қауіп-қатердің алдын алу және қауіпсіздікті қамтамасыз ету бойынша 60-тан астам қызмет түрлерін ұсынады. **Quantum Security Gateways** жоғары масштабталуы және 1,5 терабит/с-қа дейін қауіп-қатердің алдын-алу жылдамдығына ие.

R80.40 жаңартылған нұсқасы Check Point бірыңғай басқару мүмкіндіктерін кеңейтуге мүмкіндік берді. R80-қауіп-қатерді болдырмауға және деректер орталығының, бұлтты сақтаудың, мобильді құрылғылардың, соңғы нүктелердің және ***IoT*** қауіпсіздігін басқаруға арналған жетілдірілген бағдарламалық жасақтама. ***R80.40***-тың соңғы нұсқасында 100-ден астам жаңа мүмкіндіктер бар, оның ішінде жылдам (бес минут) жаңа қауіпсіздік құрылғыларын орнатуға және іске қосуға мүмкіндік беретін нөлдік сенсорлық орналастыру мүмкіндігі бар. Сондай-ақ, ***R80.40*** нұсқасы бұлтты қауіпсіздікті басқаруды қамтамасыз етеді, бұл оны тиімдірек етеді және басқа шешімдермен салыстырғанда жұмыс уақытын 60% - ға дейін қысқартады. Бұл Check Point бірыңғай қауіпсіздік жүйесін веб-шолғыштан барлық қауіпсіздік инфрақұрылымына орналастыруды жеңілдетеді және IT-мамандардың қатысуымен үнемі техникалық қызмет көрсетуді немесе жаңартуды қажет етпейді.

Операционная система Check Point

Говоря об операционной системе Check Point можно вспомнить сразу четыре: SPLAT, IPSO, Gaiaи Gaia Embedded.

1. SPLAT — собственная разработка Check Point, основана на ядре RedHat. Больше не развивается.
2. IPSO — операционная система компании Ipsilon Networks, которая принадлежала компании Nokia. В 2009 года Check Point купила этот бизнес. Больше не развивается.
3. Gaia — актуальная операционная система от Check Point, которая появилась в результате слияния IPSO и SPLAT. Появилась в 2012 году и продолжает активно развиваться.
4. Gaia Embedded — для ARM устройств.

Актуальные версии:

R77.30, R80.10 R80.20
R80.30 - EA

Сертификат ФСТЭК:

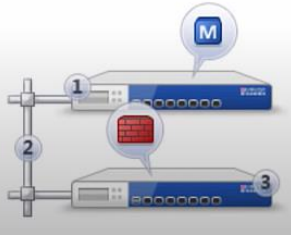
1) 77.10

2) 77.30 в середине 2019

Варианты установки:

1. Standalone (SG+SMS)

2. Distributed



Режимы работы:

1. Routed

2. Bridge

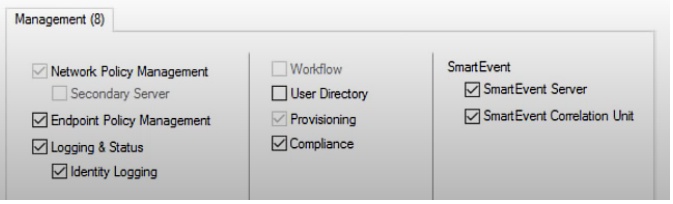
Отказоустойчивость:

1. Active-Active (load sharing)
2. Active-Standby (high availability)

Блейд - белгілі бір Check Point функциясы

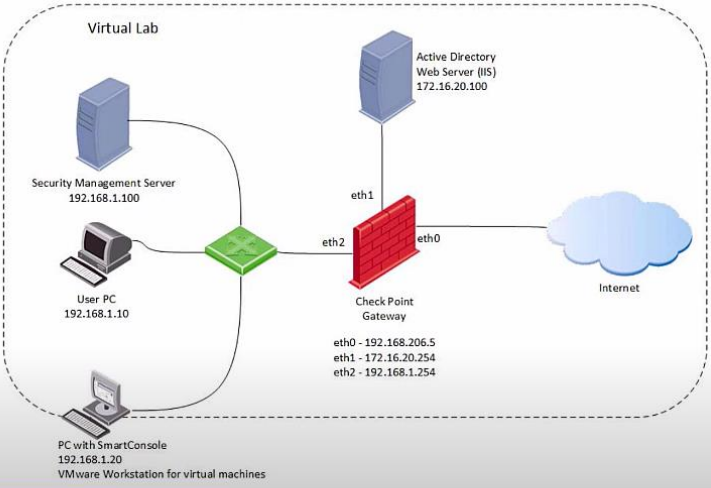
1)Блейды Network Security

2)Блейды Management



Макет состоит из:

1. Security Management Server (SMS);
2. Security Gateway (SG);
3. User PC;
4. PC with SMART Console;
5. Windows Server.



Софт для виртуализации:

1. ESXi;
2. VMware Workstation;
3. VirtualBox.

Образ Gaia:

1. SMS - Check_Point_R80.20_T101_Security_Management.iso
2. SG - Check_Point_R80.20_T101_Security_Gateway.iso

Системные требования для R80.20:

Component	Security Gateway	VSX Gateway	Security Management Server/Standalone	Multi-Domain Server
Processor	Intel Pentium IV, 2 GHz or equivalent	Intel Pentium IV, 2 GHz or equivalent	Intel Pentium IV, 2.6 GHz or equivalent	Dual Socket 2x Xeon E5-2609v2 4 cores, 2.5 GHz or equivalent
Total CPU Cores	2	2	2	8
Memory	4 GB RAM	4 GB RAM	6 GB RAM	32 GB RAM
Free Disk Space	15 GB	12 GB + 1 GB per VS	500 GB (Installation includes OS)	1 TB (Installation includes OS)

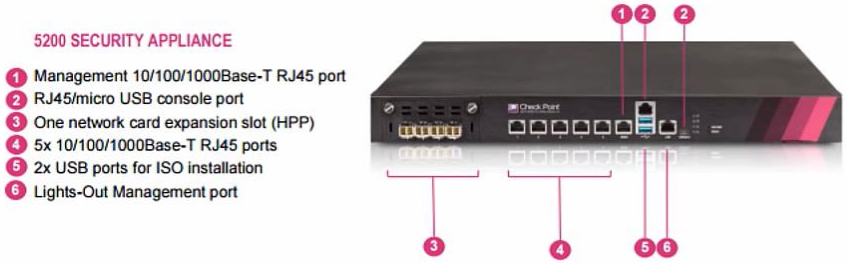
Note - The above numbers do not apply to SmartEvent & SmartLog.

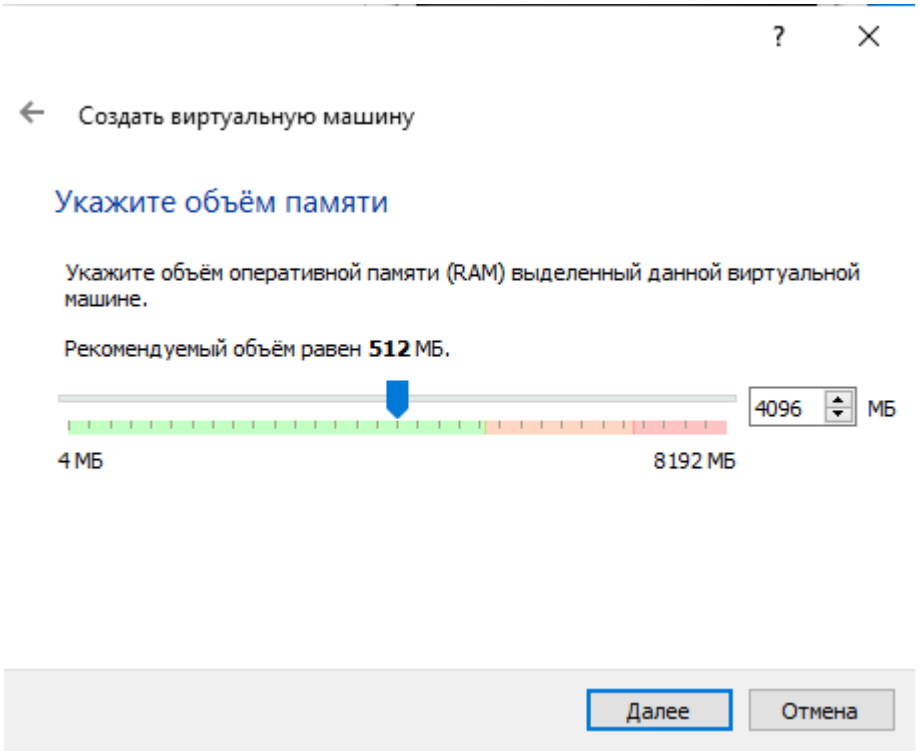
Выделяемые ресурсы:

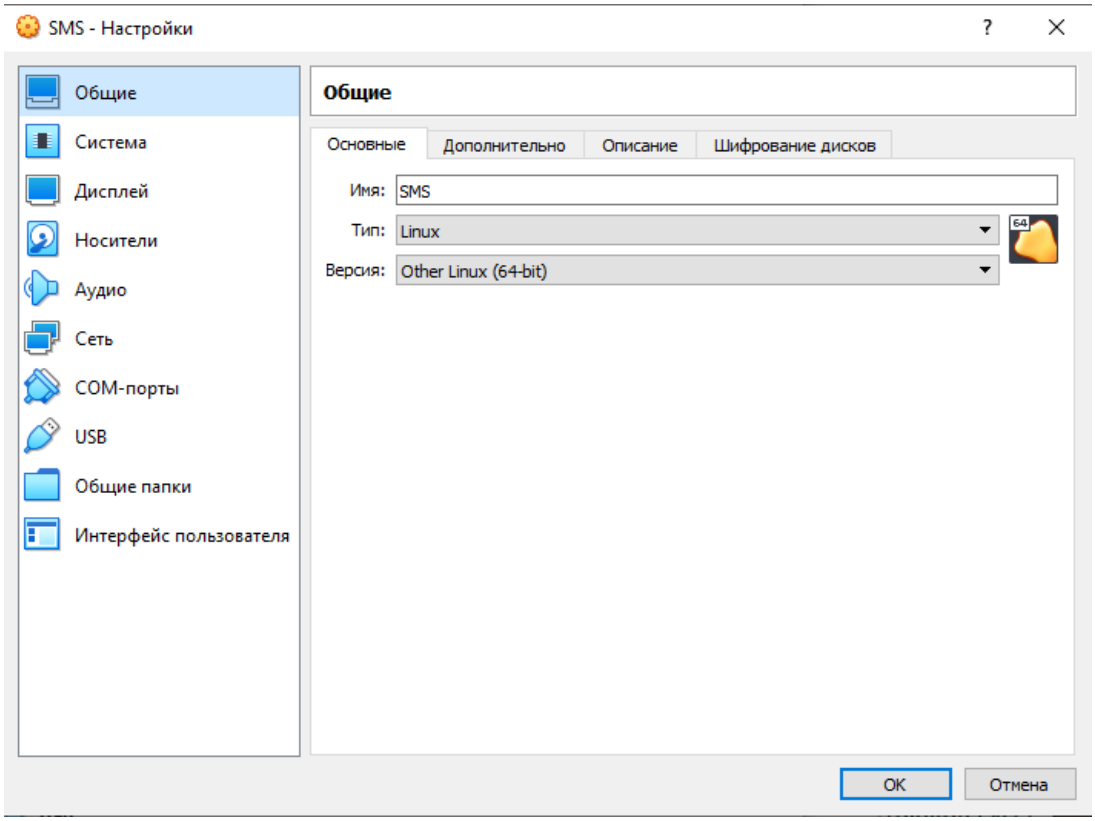
- SMS: 6GB RAM, 2 vCPU Cores, 50GB HDD;
- SG: 4GB RAM, 2 vCPU Cores, 50GB HDD;
- 3 виртуальных адаптера.

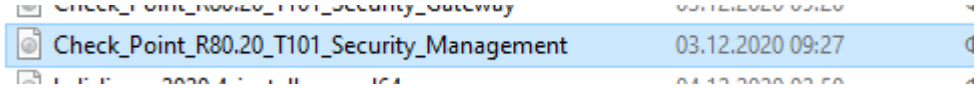
Мой ПК (тоже виртуальная машина!): CPU - 4 vCPU Cores, RAM - 16GB, HDD - 200GB

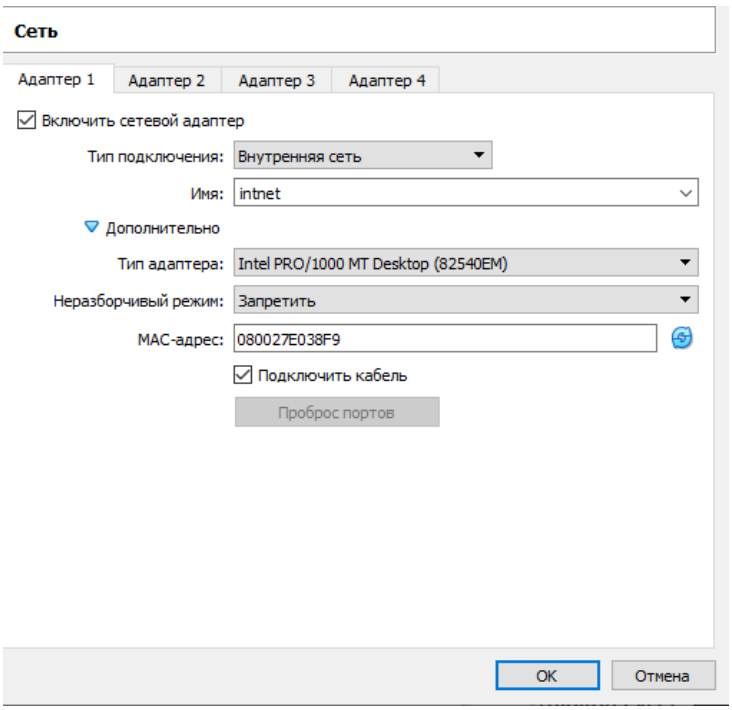
Типовой сценарий установки:

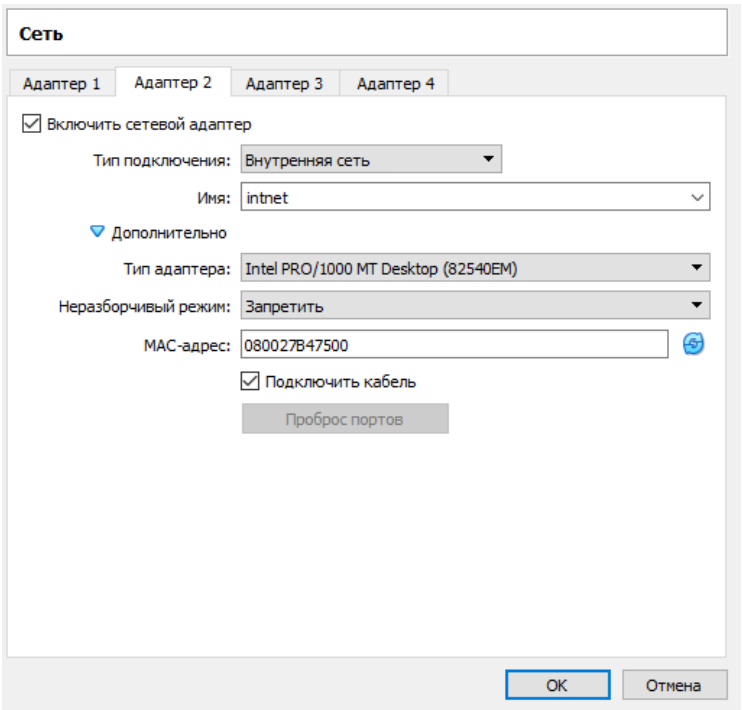


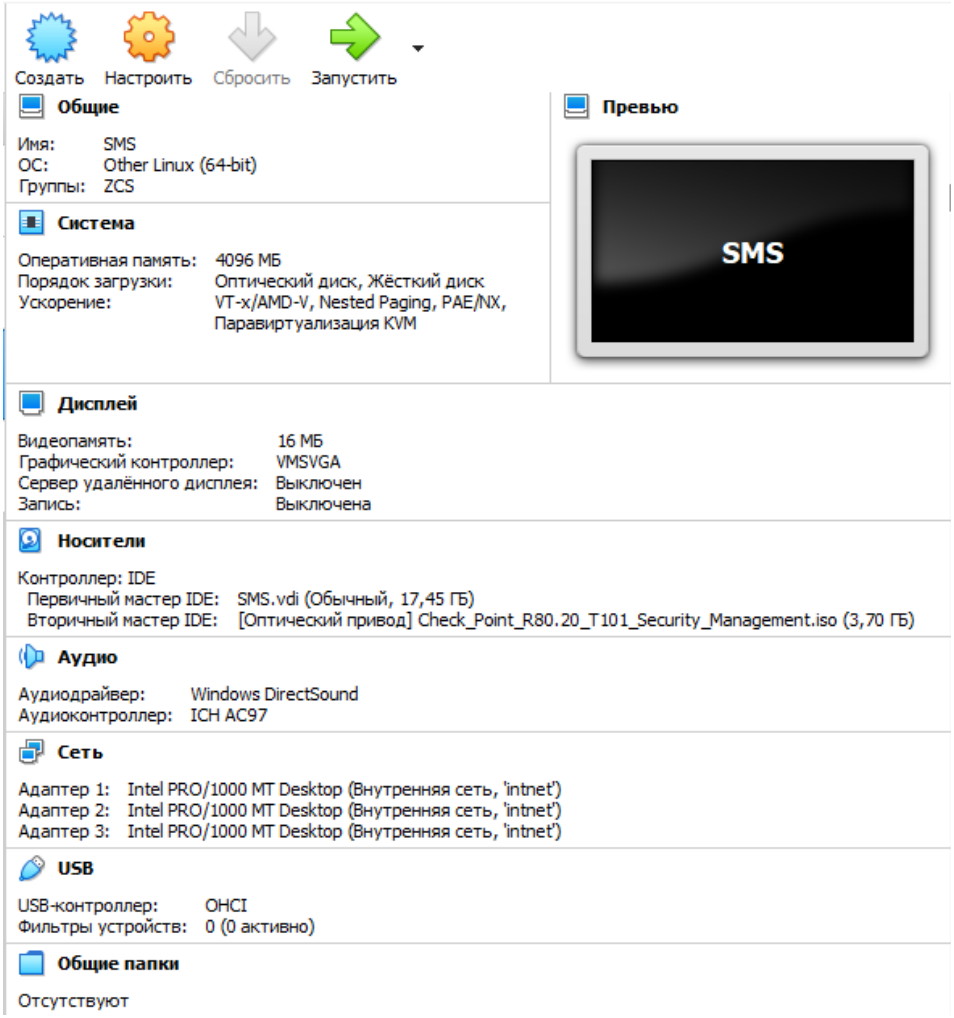

Создать виртуальную машину
Укажите объём памяти
Укажите объём оперативной памяти (RAM) выделенный данной виртуальной машине.
Рекомендуемый объём равен 512 МБ.
4096
МБ
4 МБ
8192 МБ
Далее
Отмена

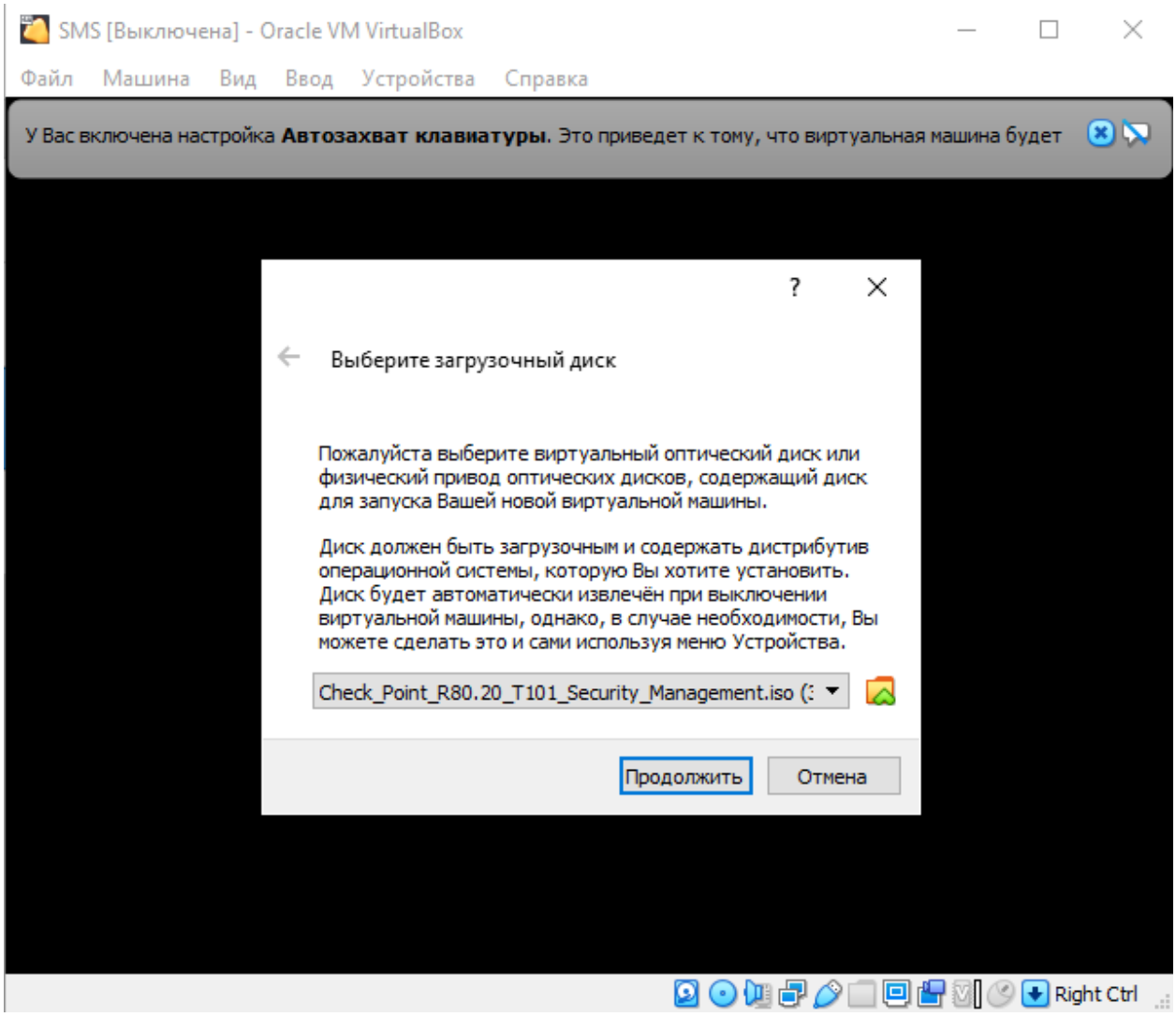

SMS - Настройки
Общие
Система
Дисплей
Носители
Аудио
Сеть
COM-порты
USB
Общие папки
Интерфейс пользователя
Общие
Основные
Дополнительно
Описание
Шифрование дисков
Имя: SMS
Тип: Linux
Версия: Other Linux (64-bit)
OK
Отмена

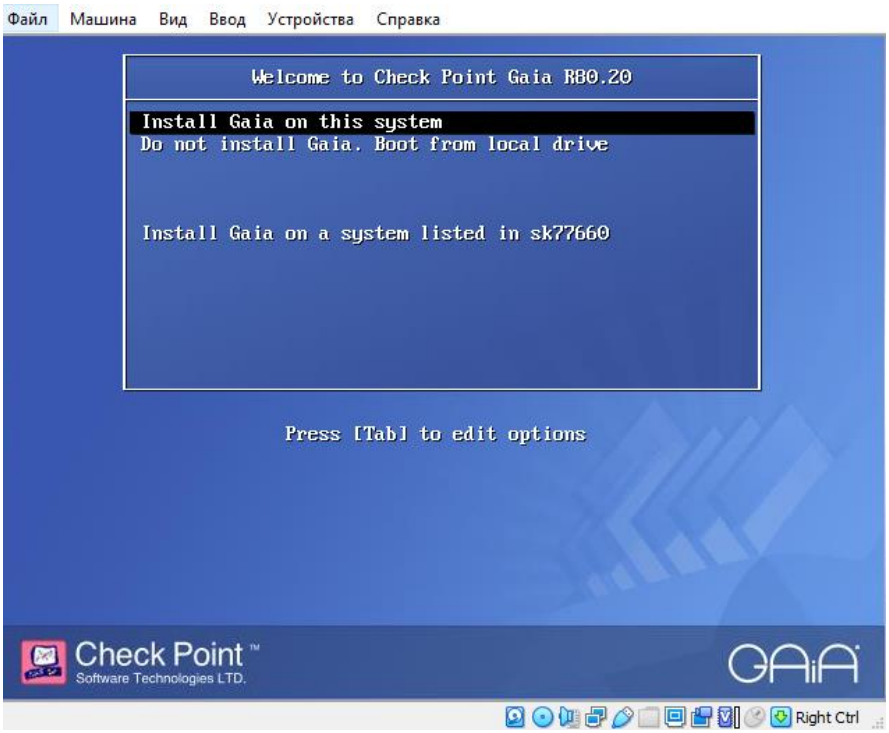

Check_Point_R80.20_T101_Security_Management
03.12.2020 09:27

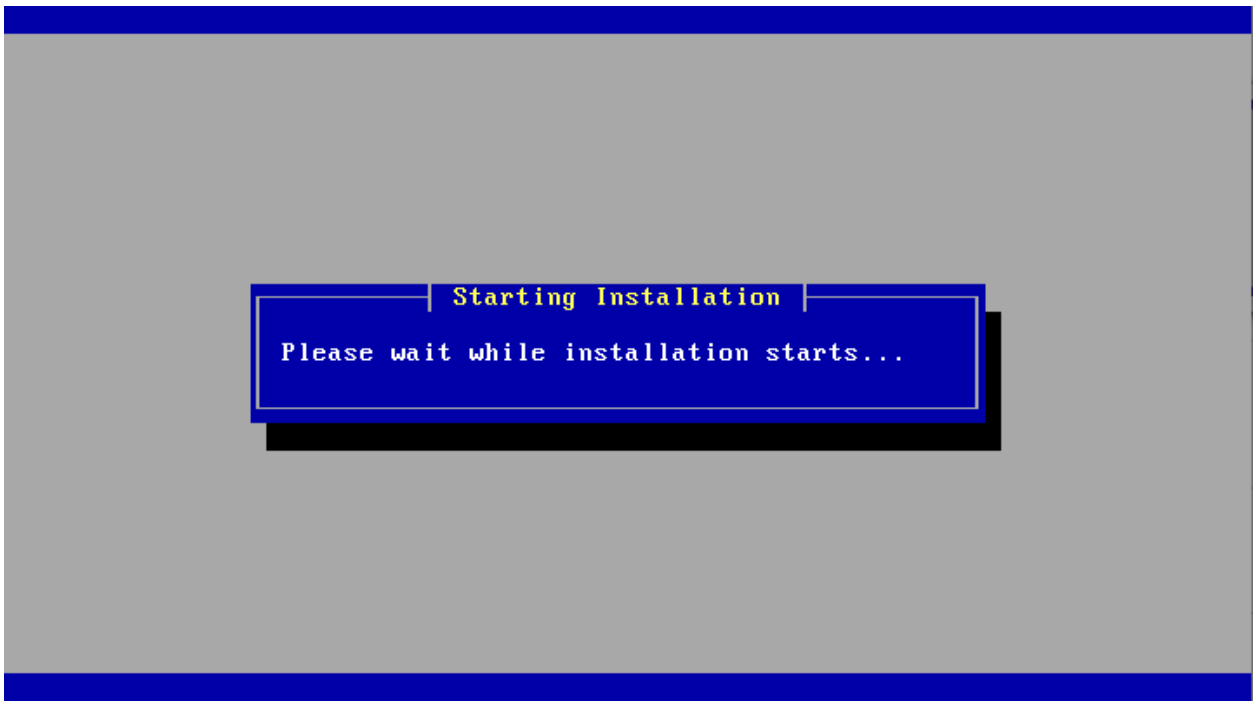

Сеть
Адаптер 1
Адаптер 2
Адаптер 3
Адаптер 4
Включить сетевой адаптер
Тип подключения:
Внутренняя сеть
Имя:
intnet
Дополнительно
Тип адаптера:
Intel PRO/1000 MT Desktop (82540EM)
Неразборчивый режим:
Запретить
MAC-адрес:
080027E038F9
Подключить кабель
Проброс портов
OK
Отмена

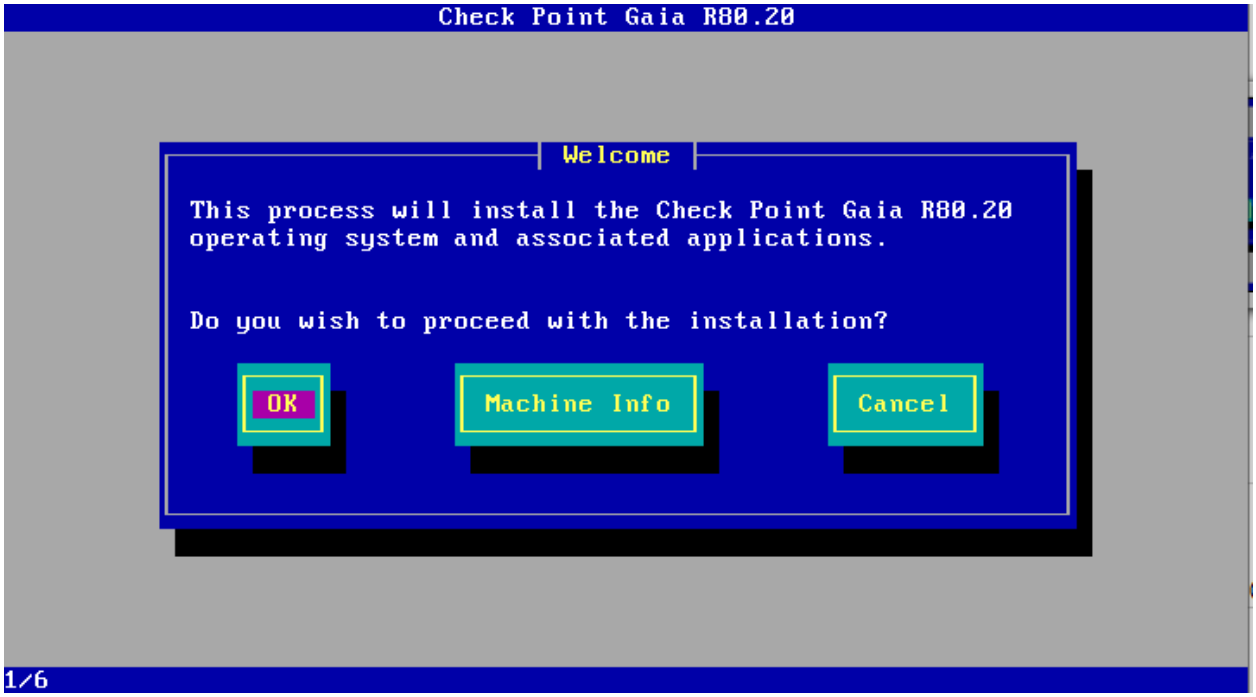

Сеть
Адаптер 1
Адаптер 2
Адаптер 3
Адаптер 4
Включить сетевой адаптер
Тип подключения:
Внутренняя сеть
Имя:
intnet
Дополнительно
Тип адаптера:
Intel PRO/1000 MT Desktop (82540EM)
Неразборчивый режим:
Запретить
MAC-адрес:
080027B47500
Подключить кабель
Проброс портов
OK
Отмена

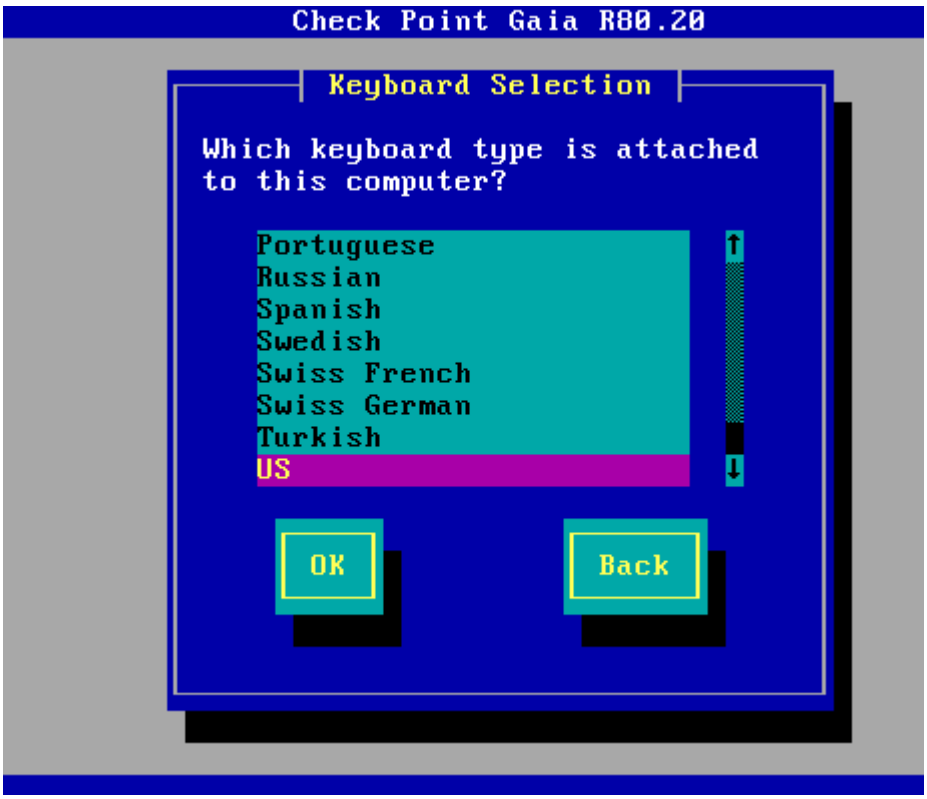

Создать
Настроить
Сбросить
Запустить
Общие
Имя: SMS
ОС: Other Linux (64-bit)
Группы: ZCS
Система
Оперативная память: 4096 МБ
Порядок загрузки: Оптический диск, Жёсткий диск
Ускорение: VT-x/AMD-V, Nested Paging, PAE/NX, Паравиртуализация KVM
Превью
SMS
Дисплей
Видеопамять: 16 МБ
Графический контроллер: VMSVGA
Сервер удалённого дисплея: Выключен
Запись: Выключена
Носители
Контроллер: IDE
Первичный мастер IDE: SMS.vdi (Обычный, 17,45 ГБ)
Вторичный мастер IDE: [Оптический привод] Check_Point_R80.20_T101_Security_Management.iso (3,70 ГБ)
Аудио
Аудиодрайвер: Windows DirectSound
Аудиоконтроллер: ICH AC97
Сеть
Адаптер 1: Intel PRO/1000 MT Desktop (Внутренняя сеть, 'intnet')
Адаптер 2: Intel PRO/1000 MT Desktop (Внутренняя сеть, 'intnet')
Адаптер 3: Intel PRO/1000 MT Desktop (Внутренняя сеть, 'intnet')
USB
USB-контроллер: OHCI
Фильтры устройств: 0 (0 активно)
Общие папки
Отсутствуют

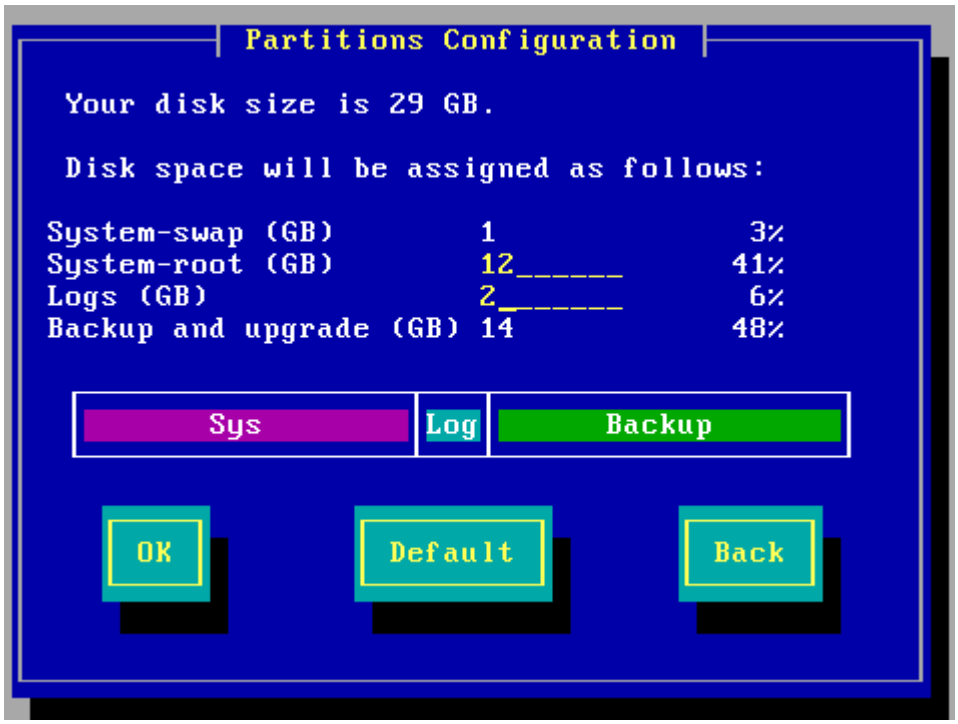

SMS [Выключена] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
У Вас включена настройка **Автозахват клавиатуры**. Это приведет к тому, что виртуальная машина будет
Выберите загрузочный диск
Пожалуйста выберите виртуальный оптический диск или физический привод оптических дисков, содержащий диск для запуска Вашей новой виртуальной машины.
Диск должен быть загрузочным и содержать дистрибутив операционной системы, которую Вы хотите установить. Диск будет автоматически извлечён при выключении виртуальной машины, однако, в случае необходимости, Вы можете сделать это и сами используя меню Устройства.
Check_Point_R80.20_T101_Security_Management.iso
Продолжить
Отмена
Right Ctrl

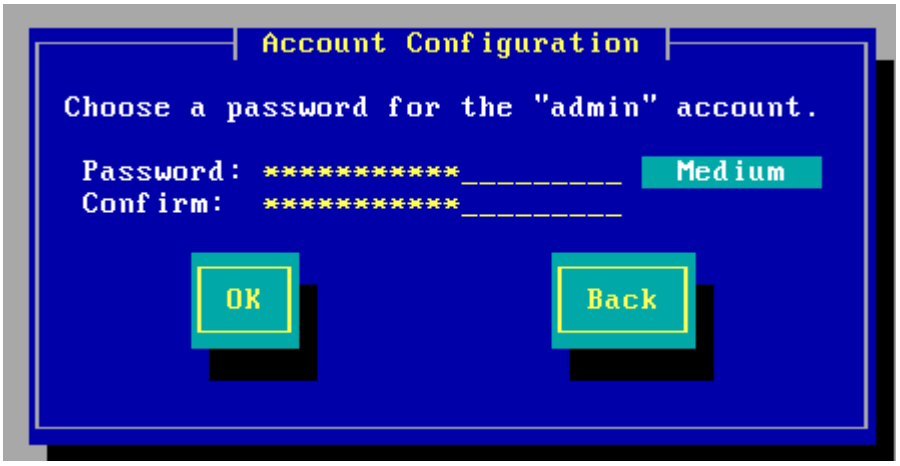

Файл Машина Вид Ввод Устройства Справка
Welcome to Check Point Gaia R80.20
Install Gaia on this system
Do not install Gaia. Boot from local drive
Install Gaia on a system listed in sk77660
Press [Tab] to edit options
Check Point
Software Technologies LTD.
GAiA
Right Ctrl

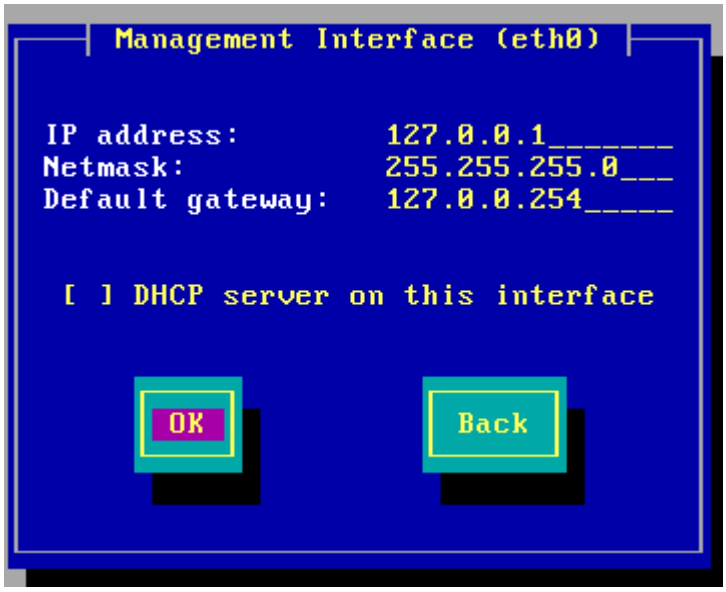

Starting Installation
Please wait while installation starts...


Check Point Gaia R80.20
Welcome
This process will install the Check Point Gaia R80.20
operating system and associated applications.
Do you wish to proceed with the installation?
OK
Machine Info
Cancel
1/6

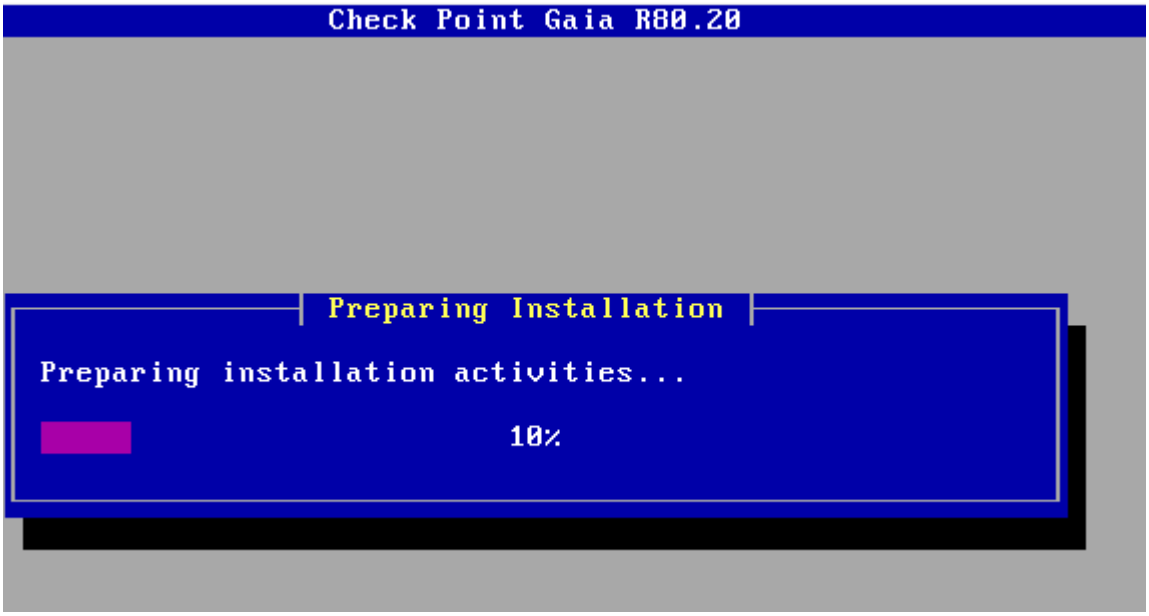

Check Point Gaia R80.20
Keyboard Selection
Which keyboard type is attached
to this computer?
Portuguese
Russian
Spanish
Swedish
Swiss French
Swiss German
Turkish
US
OK
Back

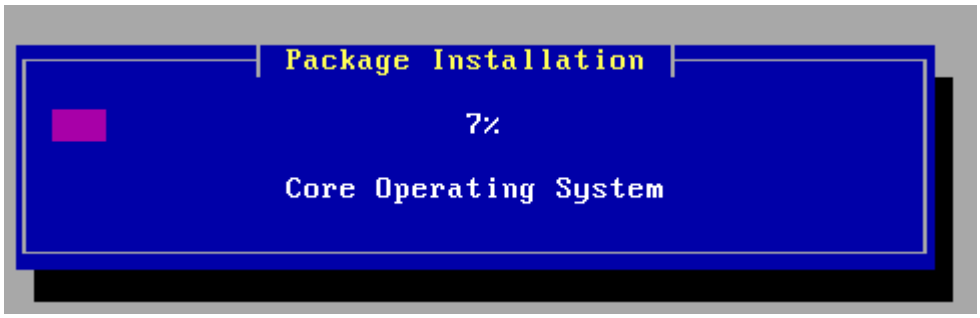

Partitions Configuration
Your disk size is 29 GB.
Disk space will be assigned as follows:
System-swap (GB) 1 3%
System-root (GB) 12_____ 41%
Logs (GB) 2_____ 6%
Backup and upgrade (GB) 14 48%
Sys
Log
Backup
OK
Default
Back

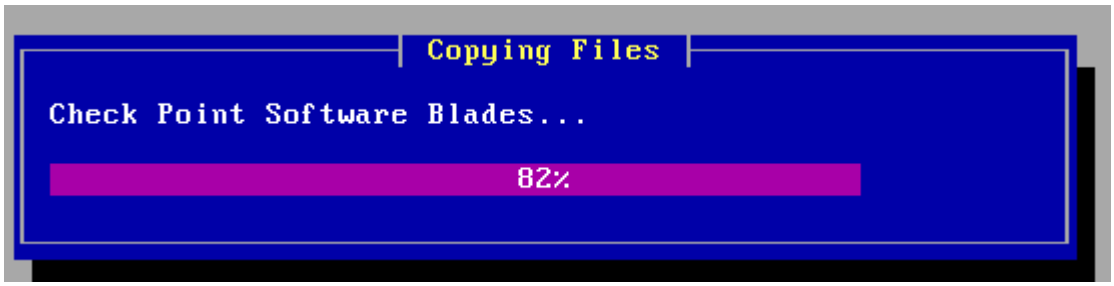

Account Configuration
Choose a password for the "admin" account.
Password: ************_________
Medium
Confirm: ************_________
OK
Back

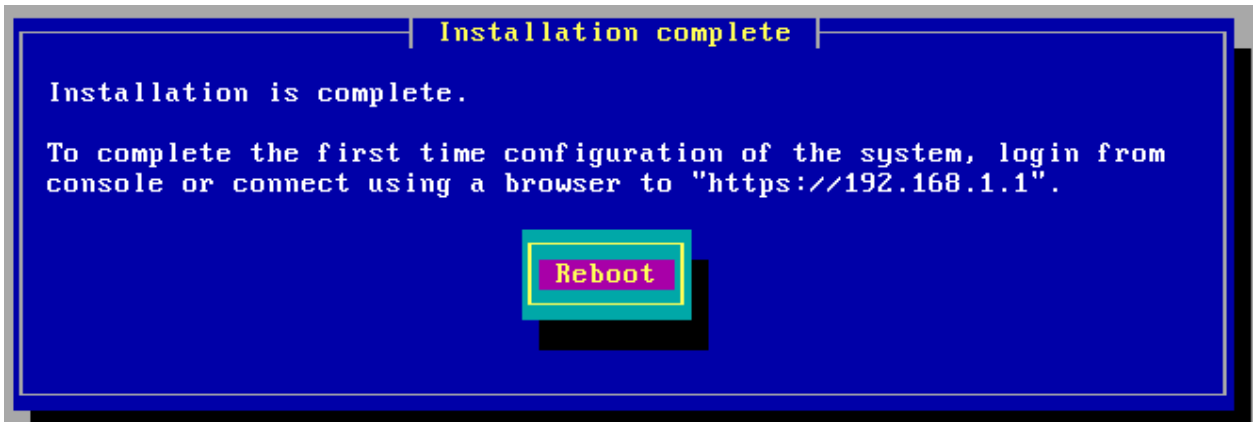

Management Interface (eth0)
IP address: 127.0.0.1_______
Netmask: 255.255.255.0___
Default gateway: 127.0.0.254_____
[ ] DHCP server on this interface
OK
Back

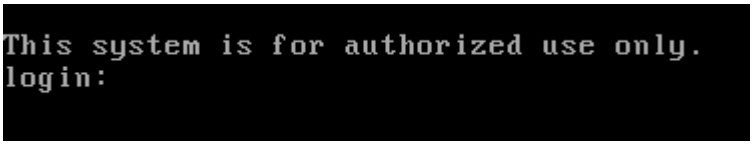

Confirmation
The next stage of the installation process
will format all your hard drives.
Are you sure you want to continue?
Back
OK


Check Point Gaia R80.20
Preparing Installation
Preparing installation activities...
10%


Package Installation
7%
Core Operating System


Copying Files
Check Point Software Blades...
82%


Installation complete
Installation is complete.
To complete the first time configuration of the system, login from console or connect using a browser to "https://192.168.1.1".
Reboot


This system is for authorized use only.
login:

https://127.0.0.1