kaspersky

Описание сенсора

Kaspersky DDoS Prevention+ (KDP+)

ООО «Модель защиты», 100% дочерняя компания
АО «Лаборатория Касперского»

10.02.2022

kaspersky

Содержание

Сенсор 2
Системные требования 2
Подготовка и настройка сенсора 2
Таблица 1. Перечень необходимых портов и протоколов для интерфейса управления сенсора 3
Защита шифрованного трафика 3
Приложение 1. Рекомендуемые аппаратные спецификации для сенсора 5
Таблица 2. Рекомендуемая конфигурация сенсора на базе оборудования Hewlett Packard 5
Таблица 3. Рекомендуемая конфигурация сенсора на базе оборудования Supermicro 6
Таблица 4. Рекомендуемая конфигурация сенсора на базе оборудования IBM 7
Таблица 5. Рекомендуемая конфигурация сенсора на базе оборудования DELL 8
Приложение 2. Поэтапный разбор процесса установки ОС сенсора на сервер 9

kaspersky

Сенсор

Компонент системы (ПО), который передается Клиенту. Устанавливается на сервере, который Клиент (Партнер) предоставляет и подключает к сетевому оборудованию, через которое проходит трафик Защищаемого ресурса. Осуществляет сбор статистики по трафику Защищаемого ресурса, необходимой для обнаружения аномалией и атак. Необходим для защиты шифрованного трафика без передачи сертификата за пределы инфраструктуры Клиента.

Системные требования

- Физическая или виртуальная машина, поддерживающая FreeBSD.
- Не менее 4-х процессорных ядер.
- 8-16 гигабайт оперативной памяти.
- Отказоустойчивое хранилище объемом не менее 200 - 500 Гб.
- 2 сетевых интерфейса.

Выше перечисленные требования предназначены для трафика с суммарным (входящий и исходящий) объемом SPAN трафика до 1 Gbit/s.

Подготовка и настройка сенсора

С аппаратной точки зрения сенсор должен обладать двумя сетевыми интерфейсами и иметь аппаратную спецификацию, соответствующую одному из вариантов, перечисленных в Приложении 1 «Рекомендуемые аппаратные спецификации для сенсора». Аппаратный компонент сенсора также может быть представлен виртуальной машиной, при условии сохранения уровня производительности не эквивалентных аппаратных решений, перечисленных в Приложении 1 «Рекомендуемые аппаратные спецификации для сенсора».

С точки зрения топологии сети сенсор должен быть установлен как можно ближе к границе сети и, по возможности, ниже точки терминации GRE-туннелей, но выше любых аппаратных\программных средств, которые могут вносить изменения в трафик (firewall, IPS и т.д.). После того как сенсор будет смонтирован, Клиент должен установить на него операционную систему, образ, который следует получить по ссылке (pass: 5QXRa6K06vEOkCe7).

Процесс установки ОС подробно описан в Приложении 2 данного документа. В процессе установки ОС необходимо назначить IP-адрес интерфейсу управления сенсора, указать маску сети для этого адреса и шлюз по умолчанию. IP-адрес для интерфейса управления должен быть выделен из пула PA-адресов провайдера.

Не допускается назначения IP-адреса из защищаемой подсети интерфейсу управления. В случае назначения сенсору IP-адреса из пула защищаемой подсети переключение трафика на маршрут защиты сделает систему мониторинга недоступной для управления. Для интерфейса управления должны быть выделены доступы согласно таблице 1.

IP-адрес и порты доступа, назначаемые непосредственно сетевому интерфейсу, предназначенному для управления сенсором, могут быть транслированы (использование внутреннего IP-адреса непосредственно на сетевом интерфейсе управления, использование нестандартного порта для доступа по протоколу SSH). Основное требование – обеспечение бесперебойной доступности от интернета до интерфейса управления по доступам, указанным в таблице 1.

Наилучшим решением для обеспечения бесперебойного доступа является подключение сенсора к интернету отдельным каналом (>=10 Mbit/s), т.к. в случае атаки на канал, система мониторинга до переключения на маршрут защиты не будет недоступна.

kaspersky

Таблица 1. Перечень необходимых портов и протоколов для интерфейса управления сенсора

Protocol	Source IP:port	Destination IP:port
TCP	82.202.188.0/24:any	Sensor:22
UDP	Sensor:any	82.202.188.0/24:42042
UDP	Sensor:any	82.202.188.0/24:123

После установки ОС второй сетевой интерфейс сенсора будет находиться в состоянии down. Он будет активирован при удаленной настройке сенсора сотрудником ООО «Модель защиты». Тем не менее, сразу после установки ОС на второй сетевой интерфейс сенсора должен быть подана симметричная копия трафика всех защищаемых ресурсов.

Важное замечание! Порт для приема копии трафика на сенсоре работает в режиме «только на прием». Таким образом, может возникнуть ситуация, в которой суммарная полоса входящего и исходящего трафика ресурса превысит скорость физического канала передачи данных в сторону сенсора. Например, входящий трафик – 250 Мбит/сек, исходящий трафик – 900 Мбит/сек. Суммарно 1150 Мбит/сек, что превышает скорость гигабитного подключения. Для корректной работы сенсора потребуется агрегированный 2 Гбит/сек канал для приема копии трафика.

Допускается установка дополнительной сетевой карты или отдельного сенсора для принятия всего объема зеркалированного трафика. На данный момент не поддерживается возможность сбора статистики одного ресурса несколькими сенсорами. Данный факт необходимо учитывать при использовании нескольких сенсоров и настройке зеркалирования трафика на сетевом оборудовании.

Защита шифрованного трафика

Использование сенсора KDP+ позволяет очищать шифрованный трафик Клиента на уровне нешифрованного, то есть – с максимально возможным качеством, без передачи SSL-сертификата за пределы инфраструктуры Клиента. Для того, чтобы получать всю необходимую информацию о шифрованном трафике Клиентские серверы в режиме реального времени передают на сенсор лог-файлы в формате UDP Syslog, содержащие, среди прочего, следующие поля:

Строка записи журнала обязательно должна содержать следующие поля:

- server_addr - адрес сервера, принимающего запрос (адрес защищаемого ресурса)
- server_port - порт сервера, принимающий запрос
- remote_addr - адрес клиента, устанавливающего соединение с защищаемым ресурсом
- remote_port - порт клиента
- time_local - время запроса
- scheme - протокол прикладного уровня (http или https)
- request - запрос
- status- код ответа сервера
- http_host - значение заголовка Host в HTTP запросе
- http_referer - значение заголовка Referer в HTTP запросе
- http_user_agent - значение заголовка User-Agent в HTTP запросе

Крайне желательно чтобы строка записи журнала содержала следующие поля:

- ssl_session_id - идентификатор SSL сессии

- ssl_session_reused - 1, если SSL сессия используется повторно
- http_accept - значение заголовка Accept в HTTP запросе»

Применение данного механизма не требует передачи сертификата или расшифрованной копии шифрованного трафика на сенсор KDP. Таким образом, обеспечивается полное соответствие требованиям различных регуляторов.

kaspersky

Приложение 1. Рекомендуемые аппаратные спецификации для сенсора

Таблица 2. Рекомендуемая конфигурация сенсора на базе оборудования Hewlett Packard

№	Изготовитель	Модель	Описание	Артикул	Кол-во
1	Hewlett Packard	ProLiant DL165 G7	Однопроцессорный сервер для установки в стойку	663808-421	1
2	Hewlett Packard	500GB 3G SATA 7.2K	Жесткий диск 3.5" с поддержкой горячей замены	458928-B21	2
3	Hewlett Packard	LO100i Adv License	Лицензия на использование управляющего модуля LO100i Advanced	530521-B21	1

Примечание:

Типовая конфигурация построена на основе модели DL165-G7, включает в себя один процессор Opteron 6272 16 2.1ГГц, 8ГБ RAM, SmartArray P410, NC362i Dual-port Gigabit Ethernet (Intel igb).

kaspersky

Таблица 3. Рекомендуемая конфигурация сенсора на базе оборудования Supermicro

№	Изготовитель	Модель	Описание	Артикул	Кол-во
1	Supermicro	SuperServer 5017R-MTF	Single socket rackmount server platform with four 3.5" hot swap	SYS-5017R-MTF	1
2	Intel	Xeon E5-1620	E5-1620 CPU 4C 10M Cache, 3.60 GHz	CM8062101038606	2
3	Seagate	500GB SATA HDD	500GB 7.2K RPM SATA 3.5in Hard Drive	ST500NM0011	3
4	Adaptec	6405E	SAS/SATA RAID-controller	2271700-R	4
5	Kingston	1333 MHz DIMM	2GB DIMM, DDR1333 Reg ECC	KVR13LR9S8/2HC	5

kaspersky

Таблица 4. Рекомендуемая конфигурация сенсора на базе оборудования IBM

№	Изготовитель	Модель	Описание	Артикул	Кол-во
1	IBM	x3250M4	Однопроцессорный сервер для установки в стойку на 2 жёстких диска	2583-C2G	1
2	IBM	4 GB RAM	2Rx8, 1.5V PC3-12800 CL11 ECC DDR3 1600MHz LP UDIMM	00D4955	1
3	IBM	500 GB HDD	500GB 7.2K 6Gbps NL SATA 2.5" SFF HS HDD жесткий диск 2.5" с поддержкой горячей замены	42D0637	2
4	IBM	Remote Management License	IBM Integrated Management Module Standard Upgrade	90Y3900	1
5	IBM	Remote Management License	IBM Integrated Management Module Advanced Upgrade (requires Std Upgrade)	90Y3901	1
6	IBM	2 port Network ad.	Intel Ethernet Dual Port Server Adapter I340-T2 for IBM System x	49Y4230	1

Примечание:

Типовая конфигурация построена на основе модели C2G, включает в себя один процессор Intel Xeon E3-1230v2 3.3GHz 4C, 4ГБ RAM, ServeRAID H1110. При необходимости может быть использована заказная конфигурация (CTO).

kaspersky

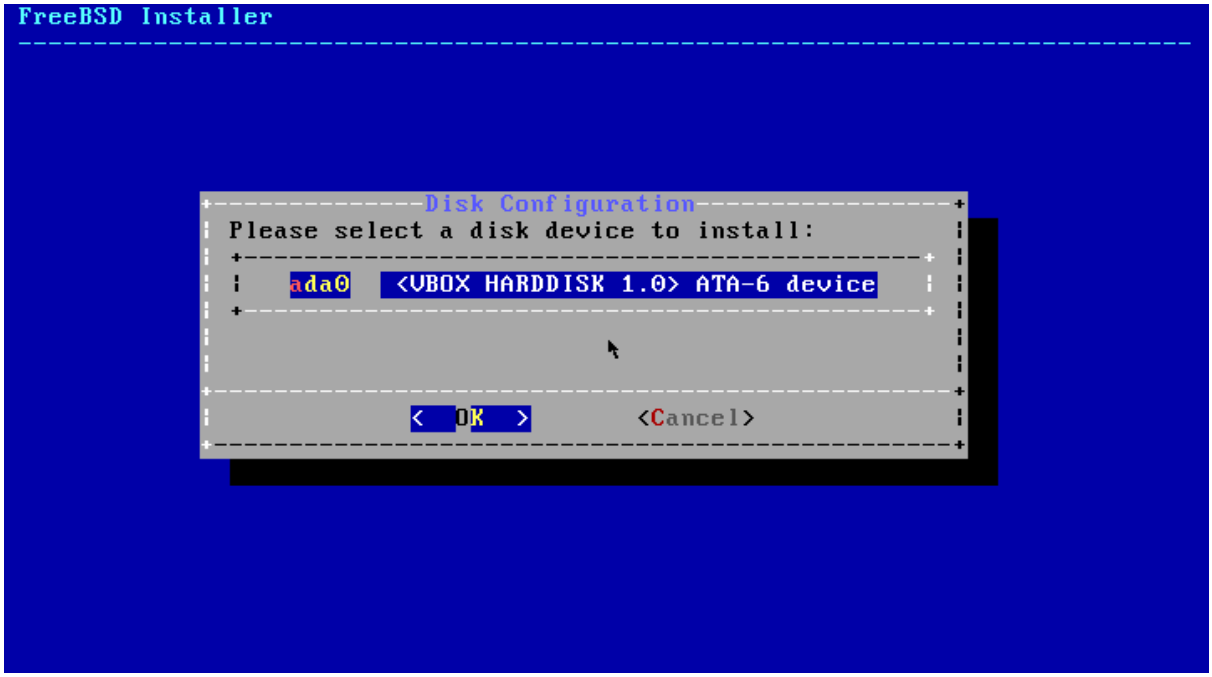
Таблица 5. Рекомендуемая конфигурация сенсора на базе оборудования DELL

№	Изготовитель	Модель	Описание	Артикул	Кол-во
1	DELL	PowerEdge R320 LFF	Single socket rackmount server with four 3.5" hot swap HDD bays,	225-2955	1
2	Intel	Xeon E5-1410	2.80GHz, 10M Cache, Turbo, 4C, 80W, Max Mem 1333MHz	317-9826, 319-0146	1
3	DELL	1333 MHz UDIMMs	4GB UDIMM, 1333 MT/s, Low Volt, Dual Rank, x8 Data Width	317-6881	2
4	DELL	PERC H310	Integrated SAS/SATA RAID-controller	342-3528	1
5	DELL	500GB SATA HDD	500GB 7.2K RPM SATA 3.5in Hot-plug Hard Drive	341-8728	2
6	DELL	iDRAC Enterprise	Intel Ethernet Dual Port Server Adapter I340-T2 for IBM System x	421-5340, 421-6085	1
7	Intel	I350-T2	Intel Ethernet I350 DualPort 1Gb Server Adapter	430-4443	1
8	DELL	Rack Rails	ReadyRails™ Sliding Rails Without Cable Management Arm	331-4766	1

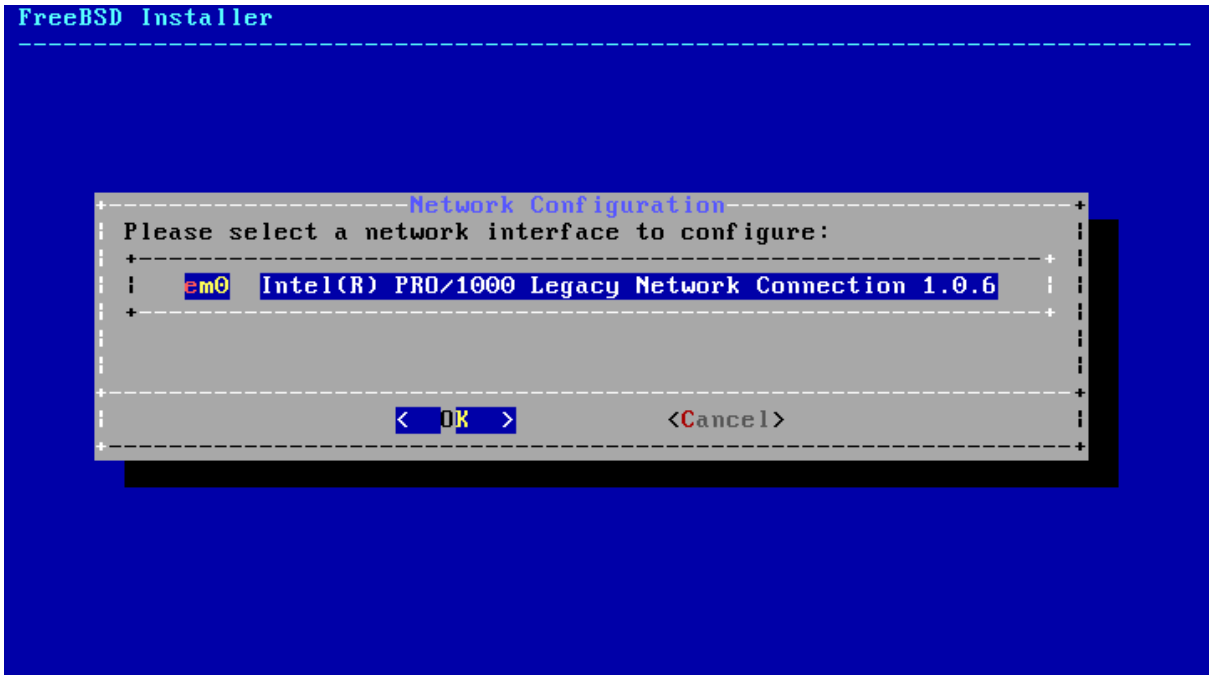
Приложение 2. Поэтапный разбор процесса установки ОС сенсора на сервер

- Загрузитесь с загрузочного USB или CD/DVD носителя, который ранее был создан с помощью файла образа операционной системы. Образ операционной системы доступен для загрузки доступен по ссылке (pass: 5QXRa6K06vEOkCe7).
  Пожалуйста, убедитесь, что на сервере корректно сконфигурирован RAID-массив и есть доступное дисковое пространство.
- На экране выбора варианта загрузки операционной системы выберите вариант 1 (нажмите «Enter» или дождитесь автоматического выбора по истечении времени таймера).

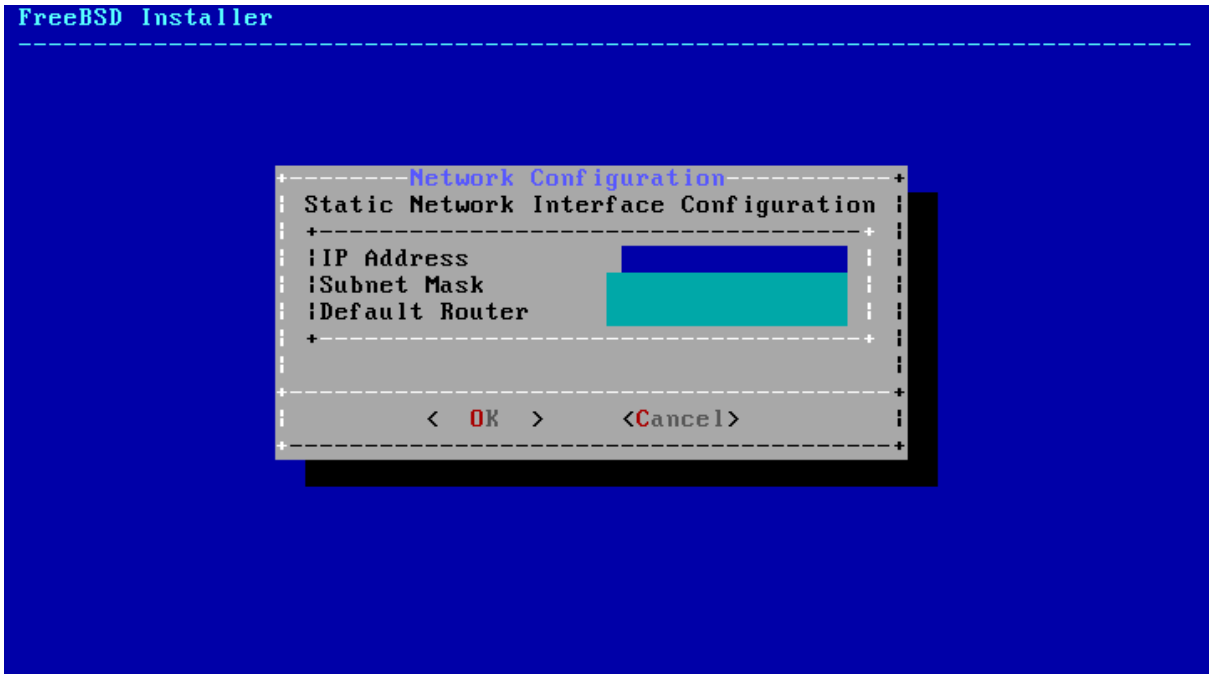
- На следующем шаге выберите дисковое устройство, на которое будет установлена операционная система. **ВНИМАНИЕ!** Системный диск форматируется без предупреждения!

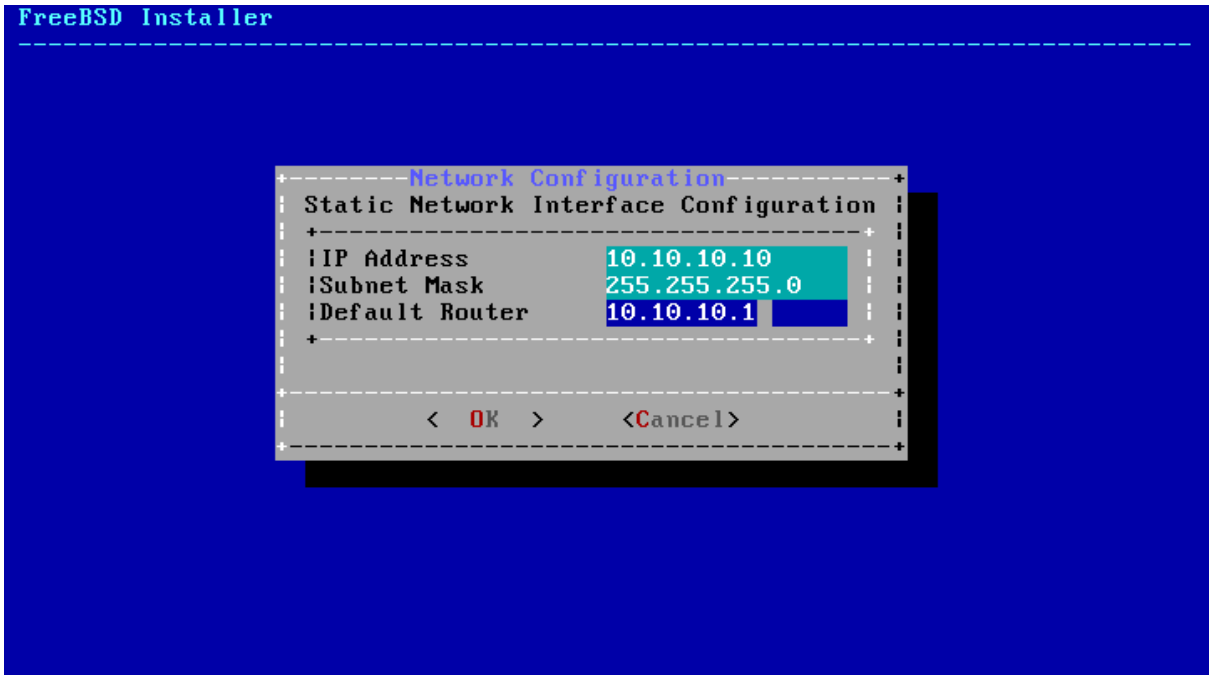


- Выберите сетевой интерфейс, который будет использован в качестве интерфейса управления.

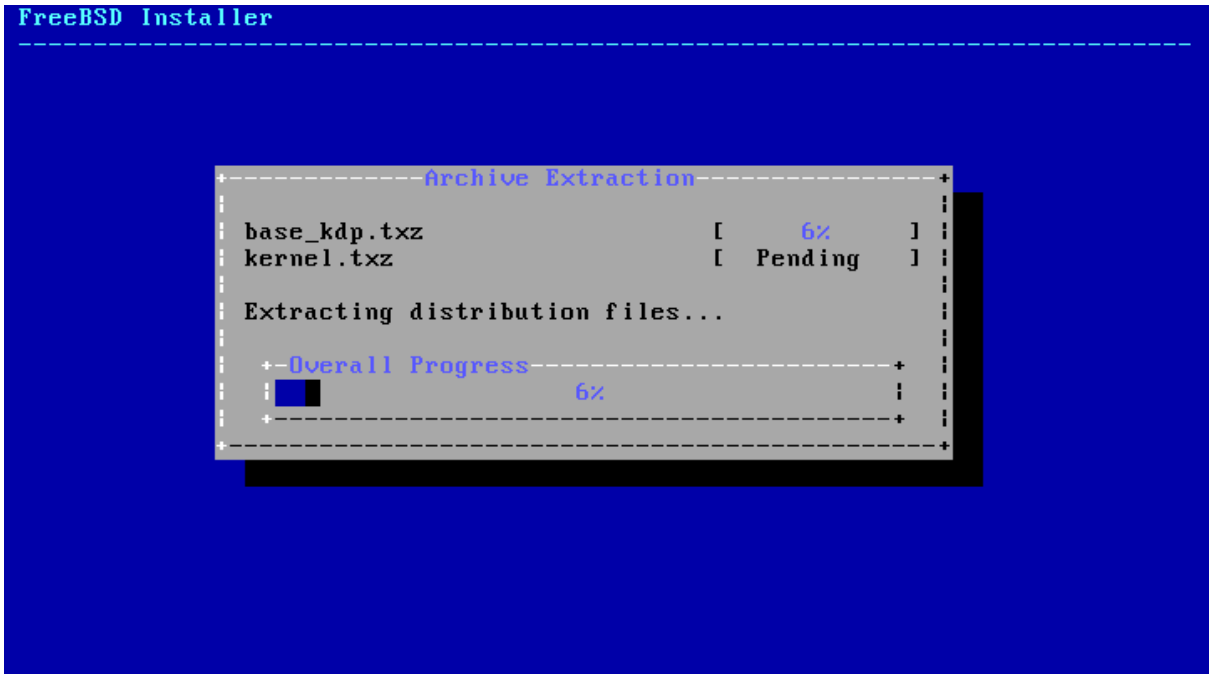


- Задайте необходимые параметры сетевого интерфейса: IP-адрес, маску подсети, шлюз по умолчанию.

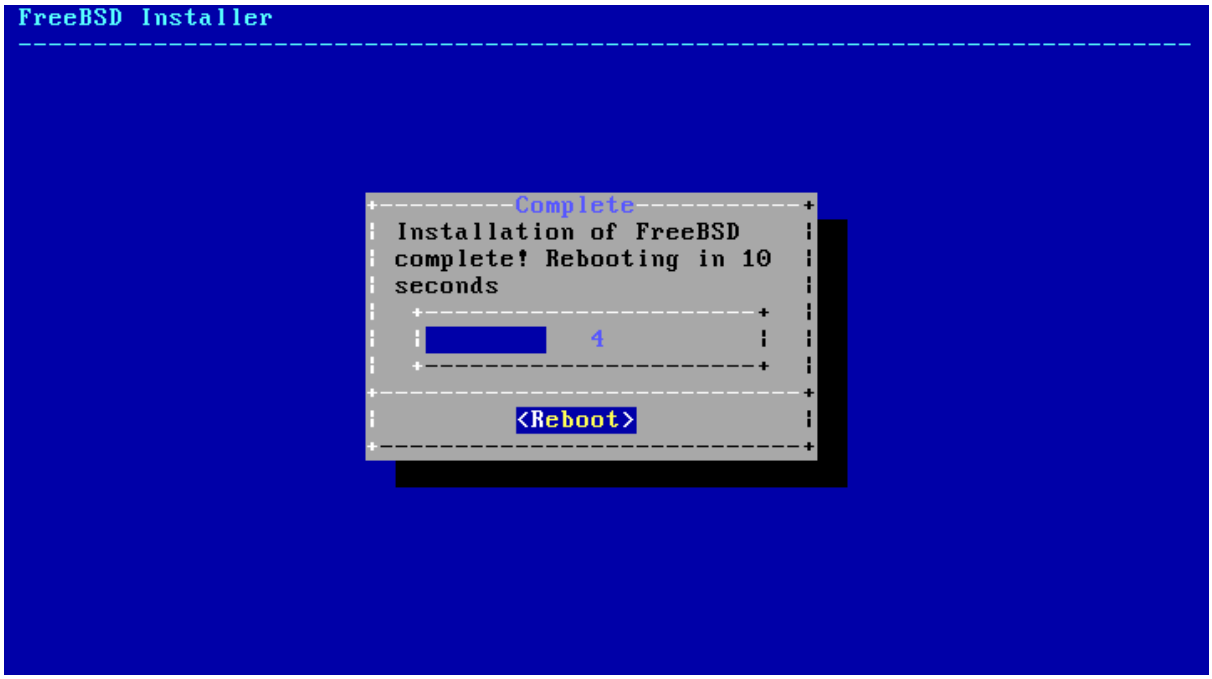




- Далее начнется процесс установки.



- По завершении процесса установки, будет предложена перезагрузка. Нажмите «Enter» или дождитесь истечения времени таймера.



- После установки и перезагрузки появится приглашение на авторизацию. Установка закончена