**Домен -** виртуальная машина

**Домен приложений -** пользовательские виртуалки для приложений. Виртуалка создается не для кажого приложения а для группы приложений схожих по функционалу (дабы экономить железо), группы этих приложений определяются и разграничиваются самим пользователем. Все домены данного типа имеют общую корневую файловую систему (Домен хранилища). Все пользовательские данные из доменов приложения хрантся в зашифрованном виде на домене хранилища и могут быть расшифрованны только с помощью ключа находящегося в домене приложения и административном домене. Для доступа к сети пробрасывается сетевой мост который позволяет получить доступ не только к сетевому оборудованию но и и к другим ВМ - по этому в момент создания доменов приложений сетевой домен не просто прокладывает виртуальныый интерфейс к физическому но и настраивает брандмауэр так что бы домены приложений не получали доступ друг к другу

**Административный домен(Dom0) -** корневая виртуальная машина,на уровне административного домена нельзя запускать (и скорее всего устанавливать приложения, собственно почему и возникли проблемы с установкой i2p

**Включает:**

XenStore используемый для хранения информации о доменах, и GUI-подсистема, основанная на оконной системе X Window и окружении рабочего стола KDE

Qubes имеет собственный X сервер работающим внутри каждого домена приложений. Когда происходит создание нового окна (или изменение содержимого существующего), демон получает его содержимое с помощью стандартной функции XGetImage системы X Window и, используя Xen Ring buffer protocol, отправляет его административному домену. Получив изображение, приложение AppViewer, работающее внутри административного домена, производит его отрисовку с помощью функции XRenderComposite.

**Сетевой домен(Network Domain) -** все сетевые процессы происходят на отдельном сетевом домене. Через дыру в драйвере злоумышленник может получить доступ к ядру. Однако в случаи изоляции сетевых процессов проникнув в сетевой домен злоумышленник может совершить 3 вещи:

1. прослушивать трафик
2. подменять трафик

В нашем случае 1 и 2 пунк решается по средствам i2p так как она использует свои не стандартные алгоритмы шифрования на каждом прокси сервере

1. обрушить домен - решение - обычное дело когда в виртуальных машинах присутствует такая функция как снимки и возможность откатиться до определенного снимка (состояния виртуально машины), собственно в Qubes os такая функция тоже есть. Предполагаю что проверка целостности сетевого домена и при необходимости откат его до определенного состояния происходит автоматически в момент запуска операционки.

В отличие от доменов приложений, он не разделяет общую корневую файловую систему с другими доменами, а вместо этого использует простое Linux-окружение, состоящее из брандмауэра, нескольких сетевых утилит и библиотек, нужных для их работы.

**Домен хранилища(Storage Domain)**

В рамках домена хранилища работает весь код драйверов устройств хранения и все необходимые для их работы подсистемы ядра и демоны уровня пользователя. Также он отвечает за хранение образов корневой файловой системы Linux, образов для хранения приватных данных доменов приложений и файлов, необходимых для загрузки ОС (загрузочный раздел) -  если загрузочные файлы будут модифицированы, операционная система просто не сможет загрузиться. 