VPN между UTM-1 Edge и CP 4200 (site-to-site)

1. VPN можно устанавливать как по сертификату так и по ключу, ВНИМАНИЕ если ваш ёжик (UTM-1 Edge) подключается к интернету через серый (не прямой) ip то VPN вы сможете устанавливать только по сертификату!
2. Приступим (внешние ip edge 194.226.34.51 и 4200 194.226.34.1, внутренние подсети на ёжике 192.168.199.0 и на 4200 192.168.11.0):

настройки 4200
- в Smart Dashboard 4200 добавляем ежа (ez_4200_1.jpg)
- задаём имя (edge199) и registration key (любые цифры - с VPN он никак не связан, да и в целом не понятно его назначение в сочетании с ёжиком), затем сохраняем (ez_4200_2.jpg)
- создаём комьюнити, куда будут входить оба устройства (более удобная форма создания VPN от CP, сохранилась и поддержка традиционного режима) (ez_4200_3.jpg)
- задаём имя, если отмечена галка Accept All Encrypted Traffic то весь трафик внутри туннеле, для шлюзов с внутренним управление будет разрешён (ez_4200_4.jpg)
- добавляем центральный шлюз, наш 4200 (ez_4200_5.jpg)
- добавляем сателлиты - наши ёжики (ez_4200_6.jpg)
-задаём IKE и IPSec параметры (ez_4200_7.jpg)
- выбираем типы туннелей (ez_4200_8.jpg)
- решаем как будет бегать трафик, в данном случае, куда угодно (ez_4200_9.jpg)
- отключаем NAT для участников комьюнити (ez_4200_91.jpg)

(вкладки, которые пропустил - **MEP**, для настроек VPN при наличии более одного центрального шлюза или при работе в кластере, **Excluded Services** - протоколы, которые вы не считаете нужным шифровать, **Shared Secret**- при установлении VPN по ключу, свой для каждого сателлита, **Wire Mode** - режим, разрешающий отключать проверку трафика внутри установленных туннелей)

- создаём объект подсеть (ez_4200_92.jpg) в данном случае 192.168.199.x
- идём в объект edge199, топология, выбираем созданную нами подсеть (ez_4200_93.jpg)
- IPSec VPN (добавляем комьюнити edge) и экспортируем сертификат Export p 12 (ez_4200_94.jpg)
- сохраняем изменения, инсталлируем политику и переходим к настройкам ёжика

настройки ёжика
- инсталлируем выгруженный с 4200 сертификат (ez_4200_95.jpg)
- создаём VPN соединение site-to-site (ez_4200_96.jpg)
- задаём адрес 4200, напомню, для ёжика мы используем серый адрес, поэтому тот адрес, который мы указываем как внешний особого значения не имеет, главное чтобы ёж смог достучаться до 4200 (ez_4200_97.jpg)
- выбираем тип конфигурирования, в нашем случае, в ручную (ez_4200_98.jpg)
- задаём подсети, в нашем случае 192.168.11.0 (ez_4200_99.jpg)
- пропускаем следующий пункт, для конфигурирования резервного адреса подключения
- тип аутентификации сертификат (ez_4200_991.jpg)
- задаём методы IKE и IPSec (ez_4200_992.jpg)
- пробуем подключаться, вне зависимости от результатов, сохраняем соединение

диагностика
- проверяем активные туннели (ez_4200_993.jpg)
- проверяем доступность адрес 192.168.11.22 компьютер из внутренней подсети 4200 (ez_4200_994.jpg)
- и в обратную сторону (ez_4200_995.jpg)
- запускаем SmartView Monitor смотрим на активные туннели (ez_4200_996.jpg)
- запускаем SmartView Tracker проверяем, что трафик шифруется (ez_4200_997.jpg)
- проверяем, что нас не обманывают (ez_4200_998.jpg)
- скрин до кучи (ez_4200_999.jpg)

Удачного дня, Амигос

http://nexthop.ru/wp-content/uploads/2012/08/vpn_edge_4200.zip

http://nexthop.ru/wp-content/uploads/2012/08/vpn_edge_4200.pdf