VPN между двумя UTM-1 Edge (site-to-site)

1. VPN можно создавать как с ключём, так и с сертификатом
2. Браузер для настроек с импортом сертификатов и загрузкой файлов, **только Internet Explorer**
3. При тестировании устройств в лабе, не забудьте снять галку Probe Next Hope в настройках WAN (скрин edge1.jpg)
4. Устройство может также выступать в качестве VPN сервера (remote access), поддерживается встроенный клиент MS Windows (скрин edge2.jpg)
5. Приступаем к настройке, обозначение (**Network-Ports**) - основная вкладка Network, подраздел Ports:

- задайте ip адреса на внешнем интерфейсе (**Network-Internet**), в нашем случае 195.226.34.2 и .3 (скрин edge3.jpg), адреса OfficeMode (**Network- My Network**) (скрин edge5.jpg) для проверки работоспособности туннелей, убедитесь, что устройства видят друг друга (**Setup-Tools**)(скрин edge4.jpg)
- перейдите на вкладку VPN, если вы настраиваете соединение с помощью сертификатов, перейдите в раздел certificate, добавьте сертификат в формате PKCS# 12 (*.p12)(скрин edge6.jpg)
- далее идём (**VPN-VPN Sites**), выбираем New Site(скрин edge7.jpg)
- Site-to-Site VPN, указываем ip адрес соседнего устройства, отмечаем галки - не использовать NAT и игнорировать правила брандмауэра, чтобы он пропускал соответствующие пакеты, в том случае, если вам не подходит данный вариант, вы можете настроить правила вручную, после создания подключения(скрин edge8.jpg)
- выбираем Specify Configuration (мы сами укажем, какие сети у нас будут гулять в туннеле), указываем их на следующей вкладке - в нашем случае 192.168.99.x и 199.x(скрин edge9.jpg)
- тип аутентификации сертификат или ключ(скрин edge91.jpg)
- выбираем параметры шифрования и проверки целостности (в нашем случае AES-256/SHA1)(скрин edge92.jpg)
- пробуем соединиться с соседом, если это первое устройство - просто снимите галку и сохраните соединение, указав понятное вам имя(скрин edge93.jpg)
- (**Network-Routes**) добавляем постоянный маршрут на подсеть соседа(скрин edge94.jpg)
- если вы не отметили галку игнорировать правила брандмауэра (**Security-Rules**) добавьте правило, разрешающее ICMP для тестов этого будет достаточно(скрин edge95.jpg)

На втором устройстве необходимо повторить все те же самые шаги, используя адреса соседа (в нашем случае на 34.2 у нас адрес 99.1, на 34.3 адрес 199.1), проверки:

- (**Reports-Status**) смотрим пункт VPN(скрин edge96.jpg), (**Reports-Tunnels**) поднятые туннели(скрин edge97.jpg), в разделе Logs можно почерпнуть нужную информацию для устранения проблем, проверяем работоспособность туннеля (**Setup-Tools**)(скрин edge98.jpg)

- и последнее, убеждаемся в том, что трафик действительно шифруется!(скрин edge99.jpg) 

http://nexthop.ru/wp-content/uploads/2012/07/edge-vpn.zip

http://nexthop.ru/wp-content/uploads/2012/07/edge2edge_vpn.pdf