VPN между двумя Cisco ASA 5510 (ASDM и CLI)

Всем, привет - хочу, вкратце, рассказать о настройке site-to-site VPN между двумя Cisco ASA 5510

Есть три варината настроки, первый - это CLI(консоль), второй и третий - это ASDM, с помощью wizard и без него, сначала я пробегусь по скринам без визарда, потом с визардом, а в финале будет несколько проверок, итак, приступим:
1. Идём в раздел Configuration, Site-to-Site VPN, Connection Profiles и создаём новый, задаём адреса пира (vpn_cisco_asa_5510_cisco_asa_5510_1.jpg)
2. Добавим сети - локальную, и удалённую, прямо здесь же её можно создать (vpn_cisco_asa_5510_cisco_asa_5510_2.jpg)
3. Для нашего случая - в групповой политике можно оставить всё по умолчанию (vpn_cisco_asa_5510_cisco_asa_5510_3.jpg)
4. В политике обмена ключами нужно добавить или убедиться в том, что там есть подходящяя нам связка (vpn_cisco_asa_5510_cisco_asa_5510_4.jpg)
5. В свойствах IPSec нужно выбрать требуемый нам транформсет (vpn_cisco_asa_5510_cisco_asa_5510_5.jpg)
6. Параметры криптомапы може оставить по умолчанию (vpn_cisco_asa_5510_cisco_asa_5510_6.jpg)
Всё тоже самое можно проделать и с wizard:
1. Задаём ip пира и ключ (либо выбираем сертификат) (vpn_cisco_asa_5510_cisco_asa_5510_7.jpg)
2. Настраиваем IKE (vpn_cisco_asa_5510_cisco_asa_5510_8.jpg)
3. Настраиваем IPSec (vpn_cisco_asa_5510_cisco_asa_5510_9.jpg)
4. Определяем сети оставляем чекбокс, который отменяет трасляцию ip внутри туннеля(vpn_cisco_asa_5510_cisco_asa_5510_91.jpg)
5. На следующем окне мы увидим список всех применяемых настроек (оставляем чекбокс сделать исключения для acl на интерфейсах) иначе придётся добавлять правила ручками
В разделе Configuration-FIrewall-Access Rules нам нужно добавить исключения для шифрованного трафика, если мы не сделали этого в wizard, тут же можно найти packet tracer - самую удобную штуку для разбора "пакетных" полётов) (vpn_cisco_asa_5510_cisco_asa_5510_92.jpg)
В разделе Monitoring - VPN можно посмотреть состояния и статистику по нашим туннелям (vpn_cisco_asa_5510_cisco_asa_5510_93.jpg)
Полезен также Device Dashboard - он не настолько удобен, как SmartView Tracker от Check Point, но всё же помогает, при проблемах с настройкой, если консольный дебаг вас несколько пугает) (vpn_cisco_asa_5510_cisco_asa_5510_94.jpg)
Так выглядит Firewall Dashboard (vpn_cisco_asa_5510_cisco_asa_5510_95.jpg)
Убедимся в том, что устройства нас не обманывают (vpn_cisco_asa_5510_cisco_asa_5510_96.jpg)
Обновим борду (vpn_cisco_asa_5510_cisco_asa_5510_97.jpg)

Для второй асы делаете все тоже самое в "зеркале" - удачной недели, Амигос!

http://nexthop.ru/wp-content/uploads/2012/08/vpn_cisco_asa_5510_cisco_asa_5510.zip

http://nexthop.ru/wp-content/uploads/2012/08/vpn_cisco_asa_5510_cisco_asa_5510.pdf

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

http://nexthop.ru/wp-content/uploads/2012/08/asa196.pdf

http://nexthop.ru/wp-content/uploads/2012/08/asa205.pdf