VPN между Check Point 4200 и Cisco ASA

Команды для настройки ASA через CLI можно посмотреть в топике

Начнём с настройки асы через **ASDM**

1. Идём Configuration - Site-to-Site VPN - Connection Proflies и создаём профиль, добавляем ключ или сертификат (vpn_cp4200_cisco_asa_5510_1.jpg)
2. Добавляем подсети для туннеля (vpn_cp4200_cisco_asa_5510_2.jpg)
3. Групповую политику можем оставить по умолчанию (vpn_cp4200_cisco_asa_5510_3.jpg)
4. Настроим правила обмена ключами (vpn_cp4200_cisco_asa_5510_4.jpg)
5. Правила для шифрования и проверки целостности (vpn_cp4200_cisco_asa_5510_5.jpg)
6. Криптомапу можно тоже оставить без изменений (vpn_cp4200_cisco_asa_5510_6.jpg)

Все теже шаги можно сделать через wizard

1. Wizards - Site-to-Site VPN оставляем галку для добавления исключений, иначе придётся делать ручками (vpn_cp4200_cisco_asa_5510_7.jpg)
2. Добавляем ключ или сертификат и адрес пира (vpn_cp4200_cisco_asa_5510_8.jpg)
3. Задаём параметры IKE (vpn_cp4200_cisco_asa_5510_9.jpg)
4. Задаём параметры IPSec (vpn_cp4200_cisco_asa_5510_91.jpg)
5. Определим подсети для туннеля, галку оставим - нат внутри нам не нужен, сохраним все изменения(vpn_cp4200_cisco_asa_5510_92.jpg)
6. В данном разделе вам придётся играться с ацл, если сняли галку в пункте 1 или у вас сложная инфраструктура (vpn_cp4200_cisco_asa_5510_93.jpg)

- Идём в раздел Monitoring - VPN смотрим поднятые туннели (vpn_cp4200_cisco_asa_5510_94.jpg)
- Там же можно глянуть и статистику (vpn_cp4200_cisco_asa_5510_95.jpg)
- Ещё пару окошек с данными (vpn_cp4200_cisco_asa_5510_96.jpg) (vpn_cp4200_cisco_asa_5510_97.jpg)(vpn_cp4200_cisco_asa_5510_98.jpg)(vpn_cp4200_cisco_asa_5510_99.jpg)

Можно перейти к настройкам Check Point

1. SmartDashboard - IPSec VPN создаём комьюнити (vpn_cp4200_cisco_asa_5510_991.jpg)
2. Добавляем центральный шлюз (vpn_cp4200_cisco_asa_5510_992.jpg)
3. Добавляем пиров, если ещё не созданы перейдите к пункту 7(vpn_cp4200_cisco_asa_5510_993.jpg)
4. В разделе Encryption задаём параметры IKE и IPSec, а в идущем за ним Tunnel Management выбираем тип For each pair of hosts(vpn_cp4200_cisco_asa_5510_994.jpg)
5. Задаем ключи (сертификаты на Check Point хранятся у каждого отдельно взятого объекта) (vpn_cp4200_cisco_asa_5510_995.jpg)
6. Расширенные параметры IKE и IPSec - включим PFS (vpn_cp4200_cisco_asa_5510_996.jpg)
7. Создаём подсеть для туннеля (vpn_cp4200_cisco_asa_5510_997.jpg)
8. Добавляем ASA как Interoperable Device, задаём адрес (vpn_cp4200_cisco_asa_5510_998.jpg)
9. Добавляем созданную подсеть (vpn_cp4200_cisco_asa_5510_999.jpg)
10. Если вы пропустили пукт 3 добавляем шлюз в наше комьюнити (vpn_cp4200_cisco_asa_5510_9991.jpg)

Запускаем SmartView Monitor - проверяем статус туннеля) (vpn_cp4200_cisco_asa_5510_9992.jpg)

В SmartView Tracker можем убедится в том, что пакеты бегаю правильно (vpn_cp4200_cisco_asa_5510_9993.jpg)

В конечном итого, дабы "спасть спокойно" удостоверимся в том, что железяки нам не врут (vpn_cp4200_cisco_asa_5510_9994.jpg)

http://nexthop.ru/wp-content/uploads/2012/08/vpn_cp4200_cisco_asa_5510.zip

http://nexthop.ru/wp-content/uploads/2012/08/vpn_cp4200_cisco_asa_5510.pdf