Force10 - управление только с разрешенных IP

Опубликовано muff в Пнд, 2017-09-25 23:52

По просьбе знакомого, решил разобраться, почему коммутатор **Force10 S4810** только через нескольких попыток "разрешает" подключиться по **telnet** или **ssh** для управления. После подключения никаких "залипаний" и задержек в работе комутатора не замечалось...

Просматривая логи, обнаруживаем много вхождений ошибочной авторизации с разных IP-адресов. Тоесть, проблема в следующем... **Force10 S4810** - это **L3 (Layer3)** коммутатор, который поддерживает маршрутизацию и IP-интерфейсы соответственно. В даном случае на коммутаторе присутствуют маршрутизируемые IP-адреса, доступные из сети **Internet** . Соответственно, имеем банальный brute force из бот-нетов, которые "долбят" комутатор своими подключениями, занимая все свободные **VTY** (**VirtualTeletYpe** - виртуальный интерфейс, который обеспечивает удаленный доступ к устройству). В этой модели коммутатора их десять.

Решением вопроса будет ограничение доступа к **VTY** коммутатора только с разрешенных IP-адресов. Сделать это не так и сложно.

Подключаемся к коммутатору через **telnet** или **ssh**.

Переходим в режим конфигурирования:

```
S4810# configure terminal
```

Создаем **access-list** с разрешенными IP-адресами/сетями. Не забываем, что в **ACL** политика по умолчанию - запретить все, тоесть в конце любого **ACL** есть невидимое правило "**deny ip any any**". Соответственно, достаточно добавить в **access-list** IP-адреса, с которых мы будем подключаться, а все остальные будут блокироваться:

```
S4810(conf)# ip access-list standard VTY_ACCESS
S4810(config-std-nacl)# remark 0 Deny access to switch
S4810(config-std-nacl)# seq 10 permit 10.227.206.0/24
S4810(config-std-nacl)# seq 15 permit 10.209.139.0/24
S4810(config-std-nacl)# seq 20 permit 10.229.67.0/23
S4810(config-std-nacl)# seq 25 permit 10.168.207.0/23
S4810(config-std-nacl)# seq 30 permit 10.105.41.0/24
S4810(config-std-nacl)# exit
```

После создания **access-list** необходимо "наложить" его на **VTY**:

```
S4810(conf)# line vty 0 9
S4810(config-line-vty)# access-class VTY_ACCESS
S4810(config-line-vty)# exit
```

Выходим из режима конфигурации и сохраняем изменения:

```
S4810(conf)# exit
S4810# write memory
```

Источник (получено *2025-04-25 05:47*):

http://muff.kiev.ua/content/force10-upravlenie-tolko-s-razreshennykh-ip