Workshop Smart OmniEdge

Москва, 11 апреля 2019 г.

Extreme Smart OmniEdge

Pervasive Intelligence

AI/ML
Extensive APIs
Actionable Analytics

Адаптация под Задачи бизнеса

Consistent experience
Hybrid-cloud flexibility
Защита инвестиций

Intrinsically Secure

User security
Device security
Application security

Transforming the **Edge Experience**

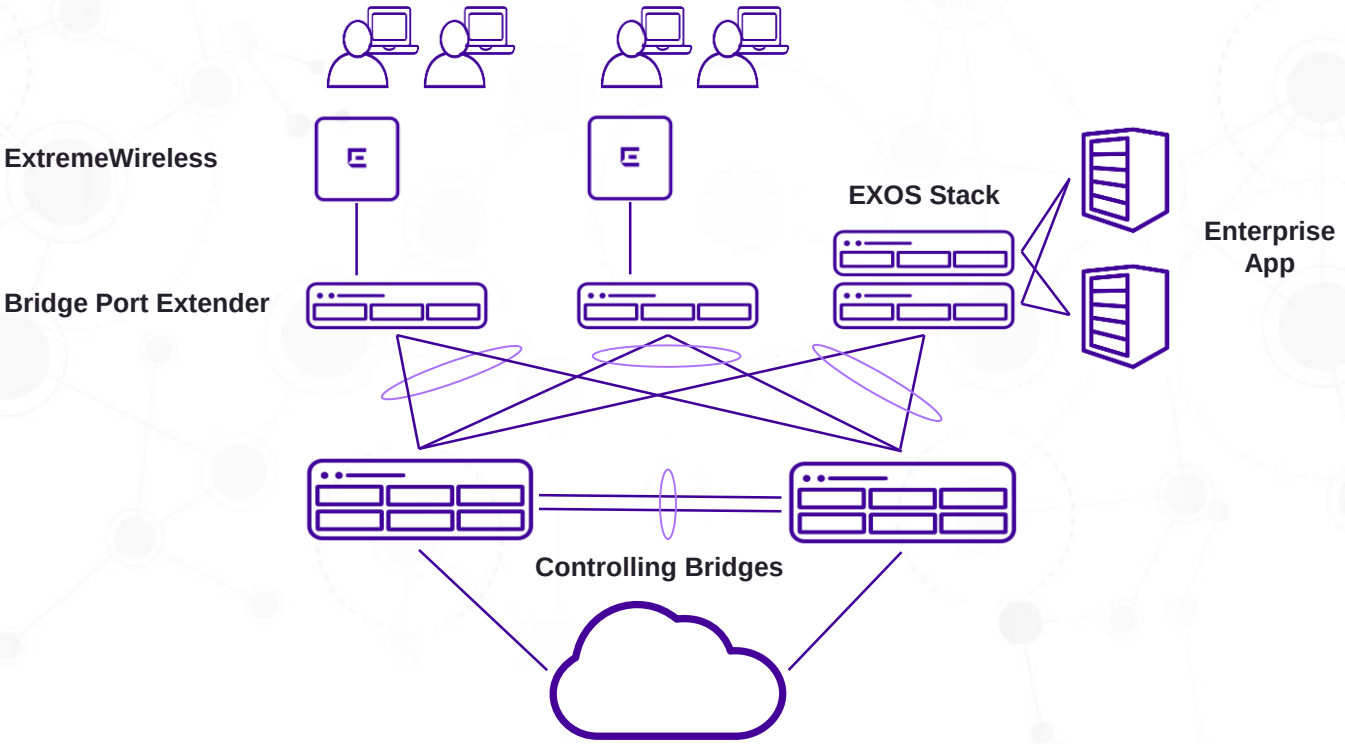
Содержание

Рекомендации Extreme Networks по построению сети

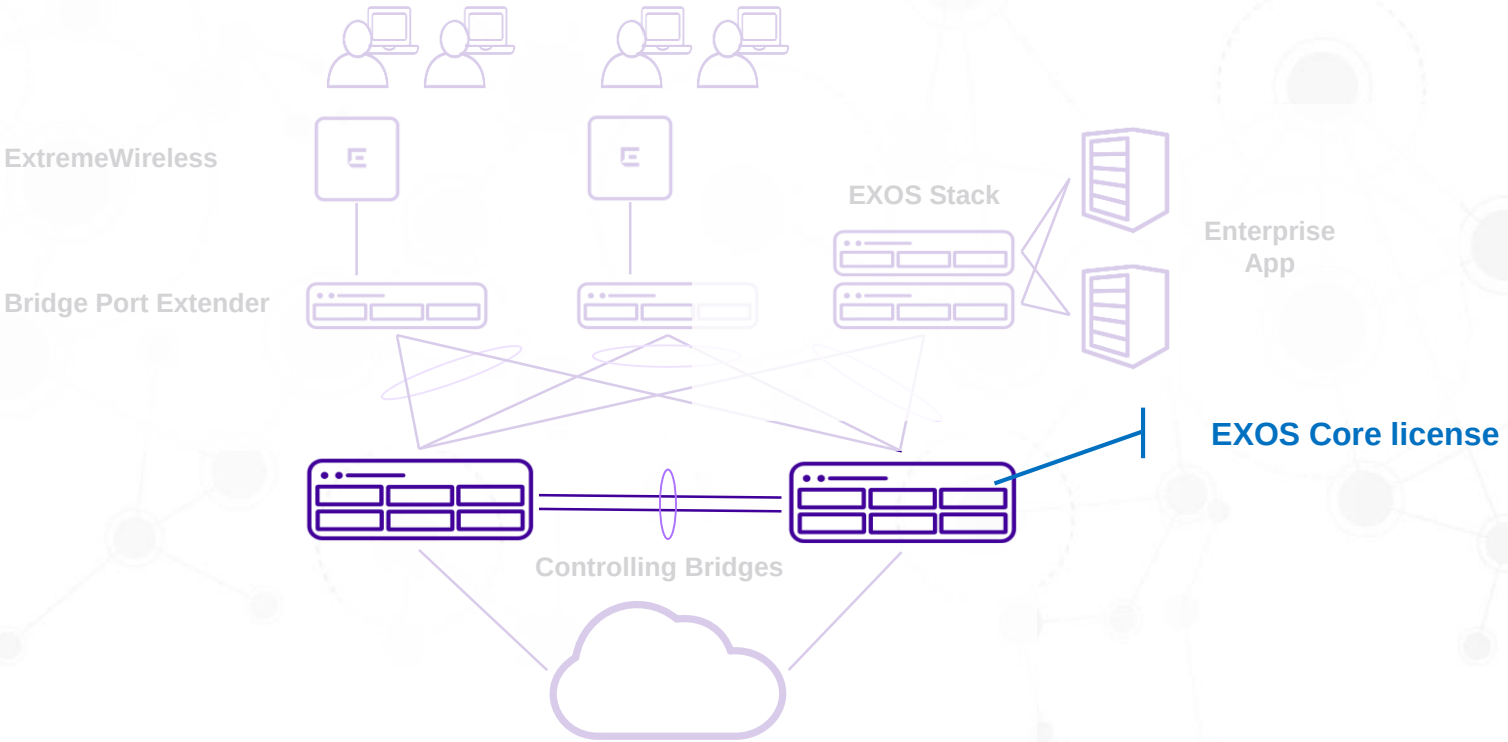
https://www.extremenetworks.com/extreme-validated-solutions/

Настройка проводного сегмента сети

Корпоративная сеть связи



Рекомендации по уровню лицензирования EXOS

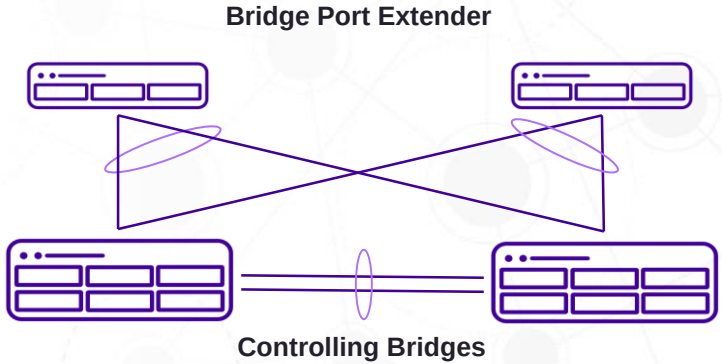


ZTPStack для автоматической настройки VPEX

ZTPStack предназначен для:

- Включения VPEX режима, если обнаружен подключенный BPE
- Автоматическая настойка MLAG со вторым CB
- Включение VPEX-autoconfiguration

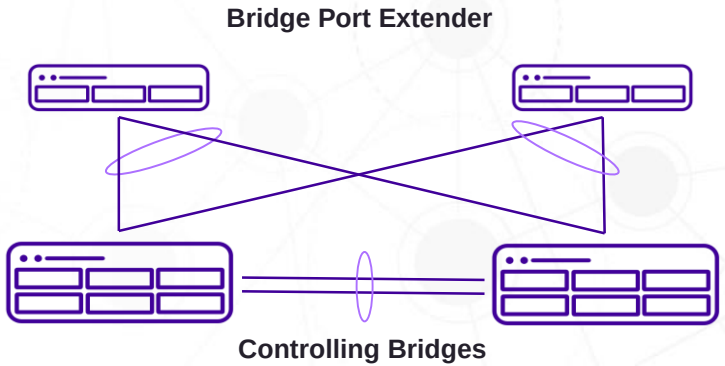
```
* Slot-1 VPEX X670G2-48x-4q.17 # sh slot
Slots      Type                 Configured           State       Ports  Flags
-------------------------------------------------------------------------------
Slot-1     X670G2-48x-4q        X670G2-48x-4q        Operational   64   M
Slot-100   V400-48t-10GE4       V400-48t-10GE4       Operational   52   M
Slot-101   V400-24t-10GE2       V400-24t-10GE2       Operational   26   M

Flags : M - Backplane link to Master is Active
        B - Backplane link to Backup is also Active
        D - Slot Disabled
        I - Insufficient Power (refer to "show power budget")
* Slot-1 VPEX X670G2-48x-4q.18 #
* Slot-1 VPEX X670G2-48x-4q.18 # sh vpex

Virtual Port Extender: Enabled
Auto-Configuration:    Enabled

Cascade
Port     Slot
=============
1:23     100
100:50   101
* Slot-1 VPEX X670G2-48x-4q.19 #
```



Синхронизация настроек Controlling Bridges

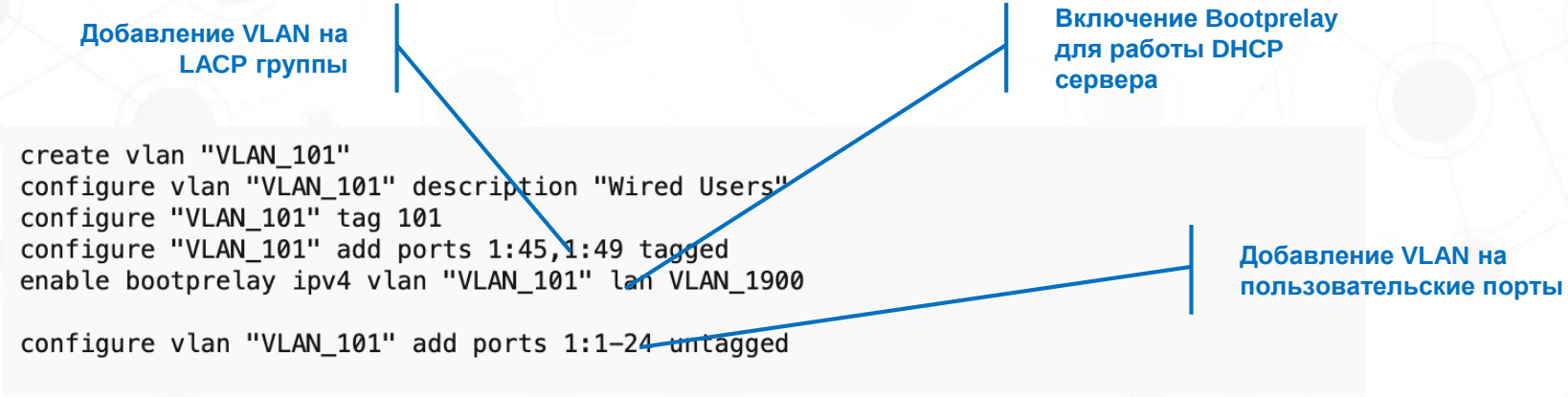
- Все настройки выполняются на одном устройстве
- Команды автоматически копируются на второй коммутатор
- Требуется предварительная настройка MLAG пары
- Может использоваться для настройки других технологий

```
# start orchestration mlag vpex_peer
(orchestration vpex_peer) # enable sharing 1:23 grouping 1:23 lacp
(orchestration vpex_peer) # enable mlag port 1:23 peer vpex_peer id 100
(orchestration vpex_peer) # config vpex port 1:23 slot 100
(orchestration vpex_peer) # enable sharing 100:49 grouping 100:49-50 lacp
(orchestration vpex_peer) # config vpex port 100:49 slot 101
WARNING: This command will remove VLAN membership from the
         port 100:49.
         Do you want to continue? (y/N) Yes
(orchestration vpex_peer) #
(orchestration vpex_peer) # sh slot
Slots      Type                Configured          State       Ports  Flags
-------------------------------------------------------------------------------
Slot-1     X670G2-48x-4q       X670G2-48x-4q       Operational   64   M
Slot-100   V400-48t-10GE4      V400-48t-10GE4      Operational   52   M
Slot-101   V400-24t-10GE2                          Booting       26

Flags : M - Backplane link to Master is Active
        B - Backplane link to Backup is also Active
        D - Slot Disabled
        I - Insufficient Power (refer to "show power budget")
(orchestration vpex_peer) #
```



Создание пользовательских VLAN

- Симметричные настройки должны быть сделаны на обоих CB-коммутаторах
- Допустимо использовать ***mlag orchestration*** режим для синхронизации настроек
- IP адреса и другие индивидуальные параметры должны настраиваться на каждом устройстве




```
create vlan "VLAN_101"
configure vlan "VLAN_101" description "Wired Users"
configure "VLAN_101" tag 101
configure "VLAN_101" add ports 1:45,1:49 tagged
enable bootprelay ipv4 vlan "VLAN_101" lan VLAN_1900

configure vlan "VLAN_101" add ports 1:1-24 untagged
```

Настройка VRRP для пользовательских VLAN

- Симметричные настройки должны быть сделаны на обоих CB-коммутаторах
- Допустимо использовать ***mlag orchestration*** режим для синхронизации настроек
- IP адреса и другие индивидуальные параметры должны настраиваться на каждом устройстве

Настройка IP адреса на VLAN

Настройка VRRP группы на VLAN

Controlling Bridge 1

```
configure "VLAN_101" ipaddress 172.16.101.2/24
enable ipforwarding "VLAN_101"

create vrrp vlan VLAN_101 vrid 101
configure vrrp "VLAN_101" vrid 101 fabric-routing on
configure vrrp "VLAN_101" vrid 101 add 172.16.101.1
configure vrrp "VLAN_101" vrid 101 priority 255
enable vrrp "VLAN_101" vrid 101
```

Fabric-routing включает ответ от ближайшего маршрутизатора в группе

Приоритет для балансировки нагрузки

Настройка Loopback интерфейсов

- Для удаленного управления через XMC
- Для Router-ID в протоколах маршрутизации
- Настраивается на каждом устройстве индивидуально

Controlling Bridge 1

```
create vlan "lo0"
configure vlan "lo0" tag 1001
enable loopback-mode vlan "lo0"
configure vlan "lo0" ipaddress 192.168.200.1 255.255.255.255
enable ipforwarding vlan "Lo0"
```

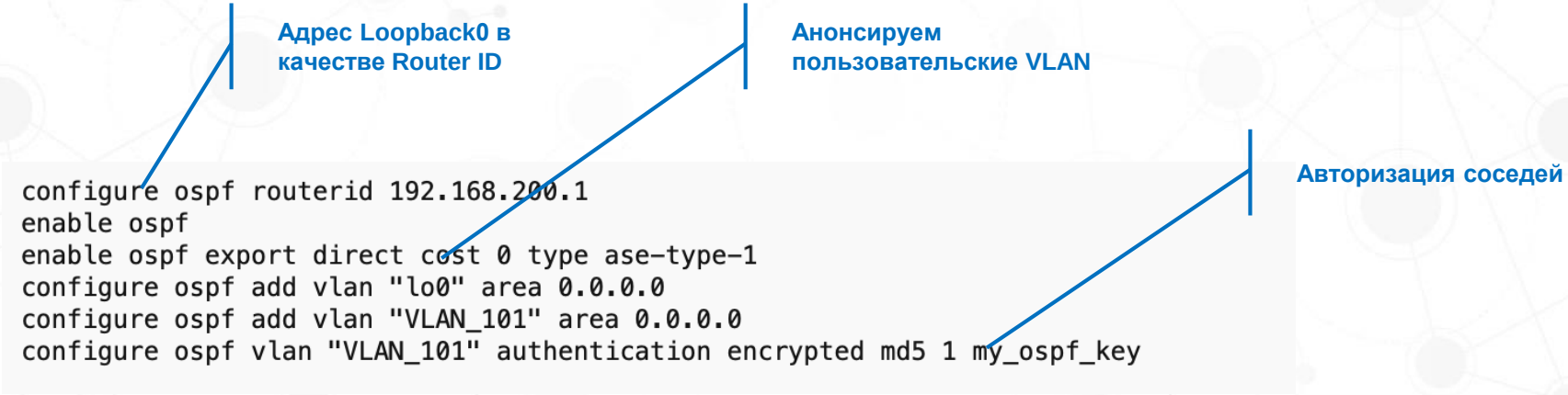
Controlling Bridge 2

```
create vlan "lo0"
configure vlan "lo0" tag 1001
enable loopback-mode vlan "lo0"
configure vlan "lo0" ipaddress 192.168.200.2 255.255.255.255
enable ipforwarding vlan "Lo0"
```

Специальный режим для Loopback интерфейсов

/32 маска для Loopback

Настройка OSPF маршрутизации



Взаимодействие с RADIUS сервером

- Для авторизации сетевых подключений используется RADIUS сервер
- Настраивается взаимодействие с двумя серверами для отказоустойчивости
- В качестве RADIUS сервера используется ExtremeControl

Controlling Bridge 1

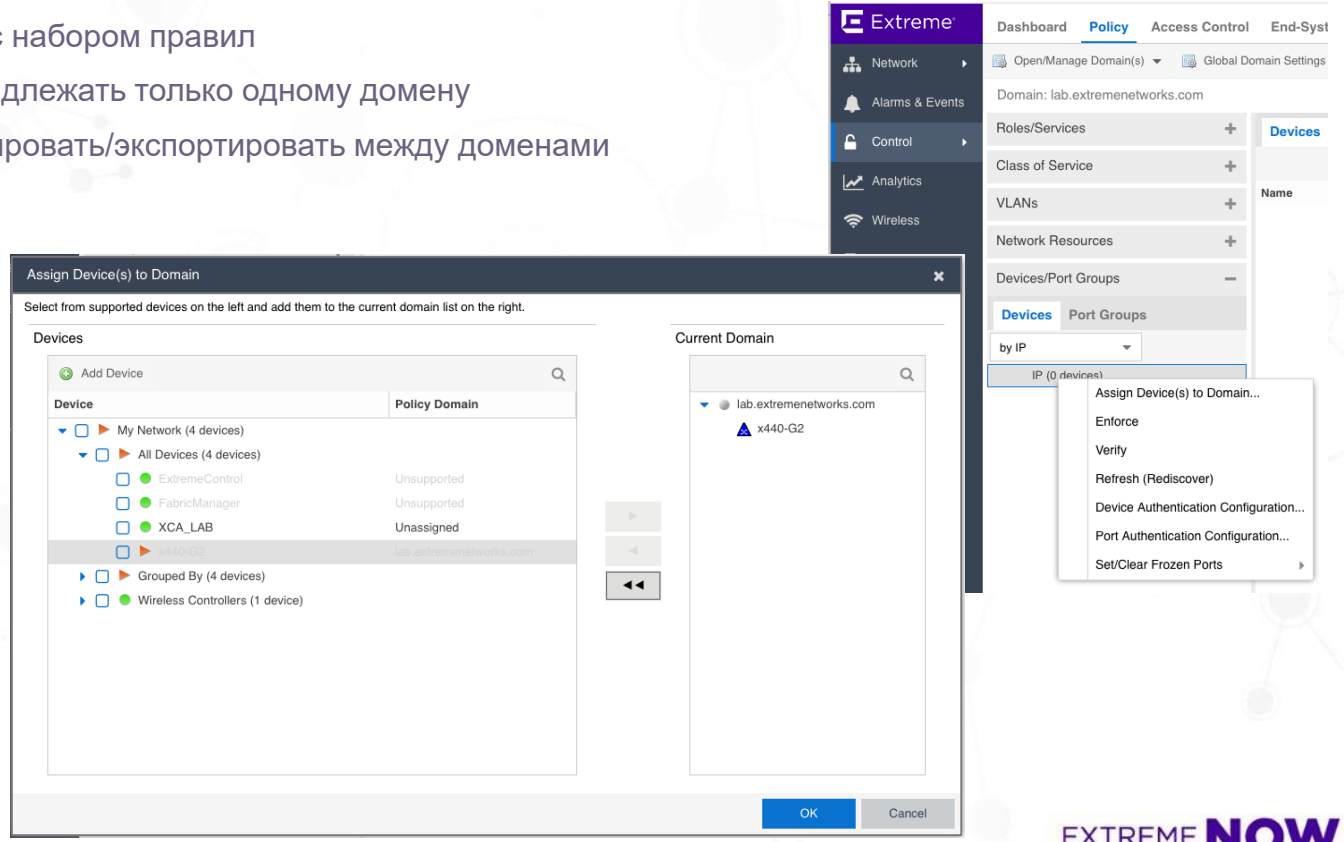
```
configure radius 1 server 192.168.250.253 1812 client-ip 192.168.200.1 VR VR-Default
configure radius 1 shared-secret encrypted "My_Radius_Key"
configure radius-accounting 1 server 192.168.250.253 1813 client-ip 192.168.200.1 VR VR-Default
configure radius-accounting 1 shared-secret encrypted "My_Accounting_Key"

enable radius
enable radius mgmt-access
enable radius netlogin

enable radius-accounting
enable radius-accounting mgmt-access
enable radius-accounting netlogin
```

Разграничение правд доступа пользователей

Алгоритм создания политики доступа

Создание домена политик

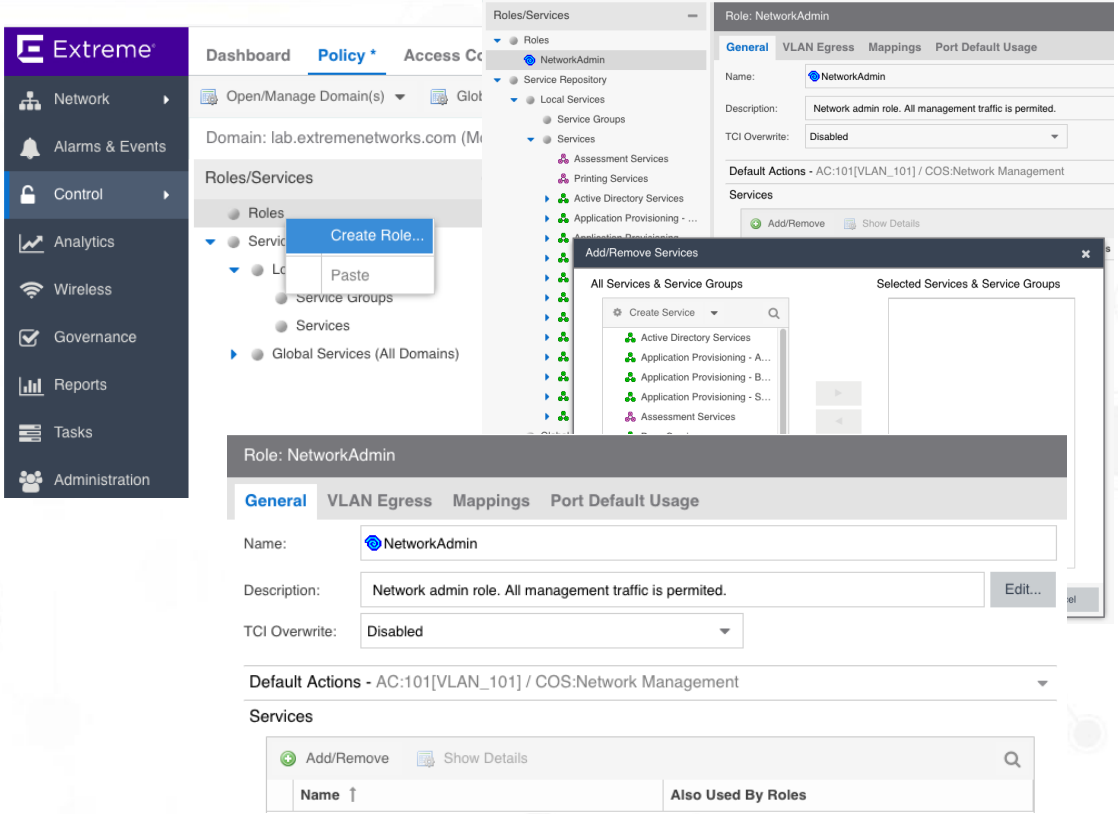
- Домен это – контейнер с набором правил
- Устройство может принадлежать только одному домену
- Правила можно импортировать/экспортировать между доменами



Создание роли пользователя

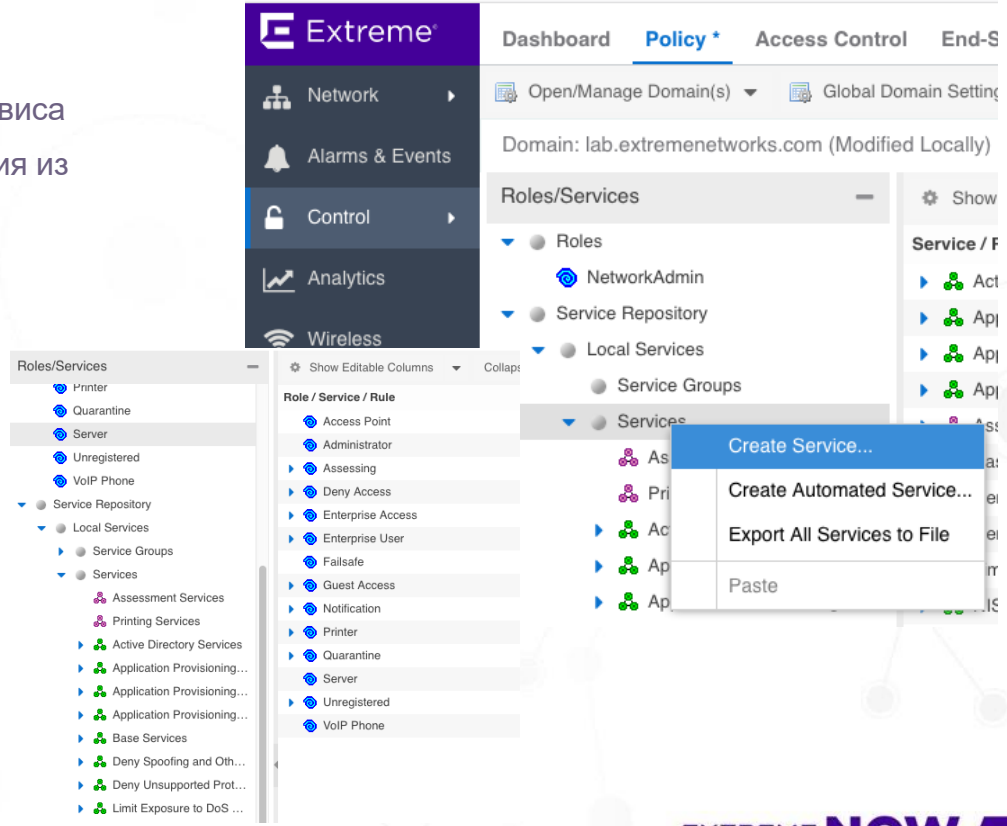
Роль это – контейнер с набором правил, определяющих характеристики трафика пользователей:

- Список разрешенных или запрещенных сетевых сервисов
- QoS маркировка пакетов
- Номер пользовательского VLAN

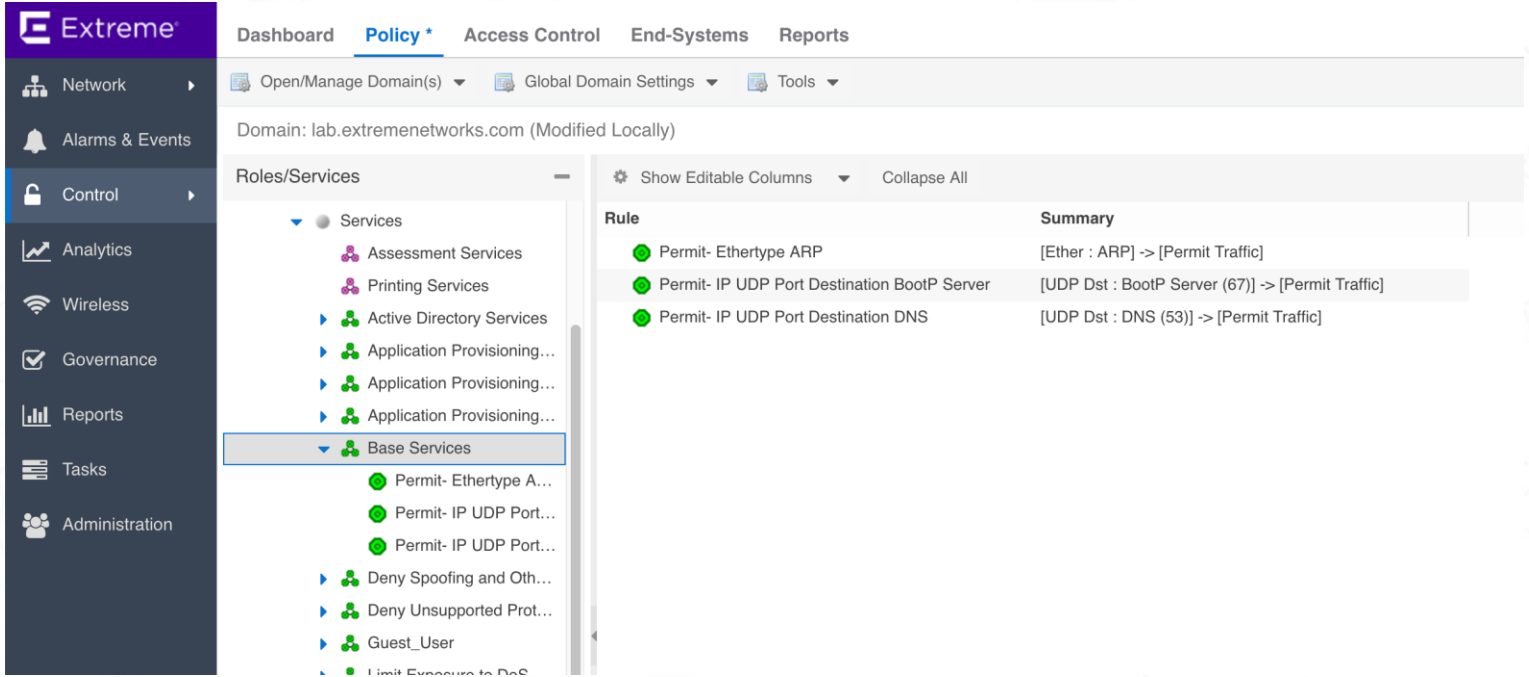


Создание сервиса

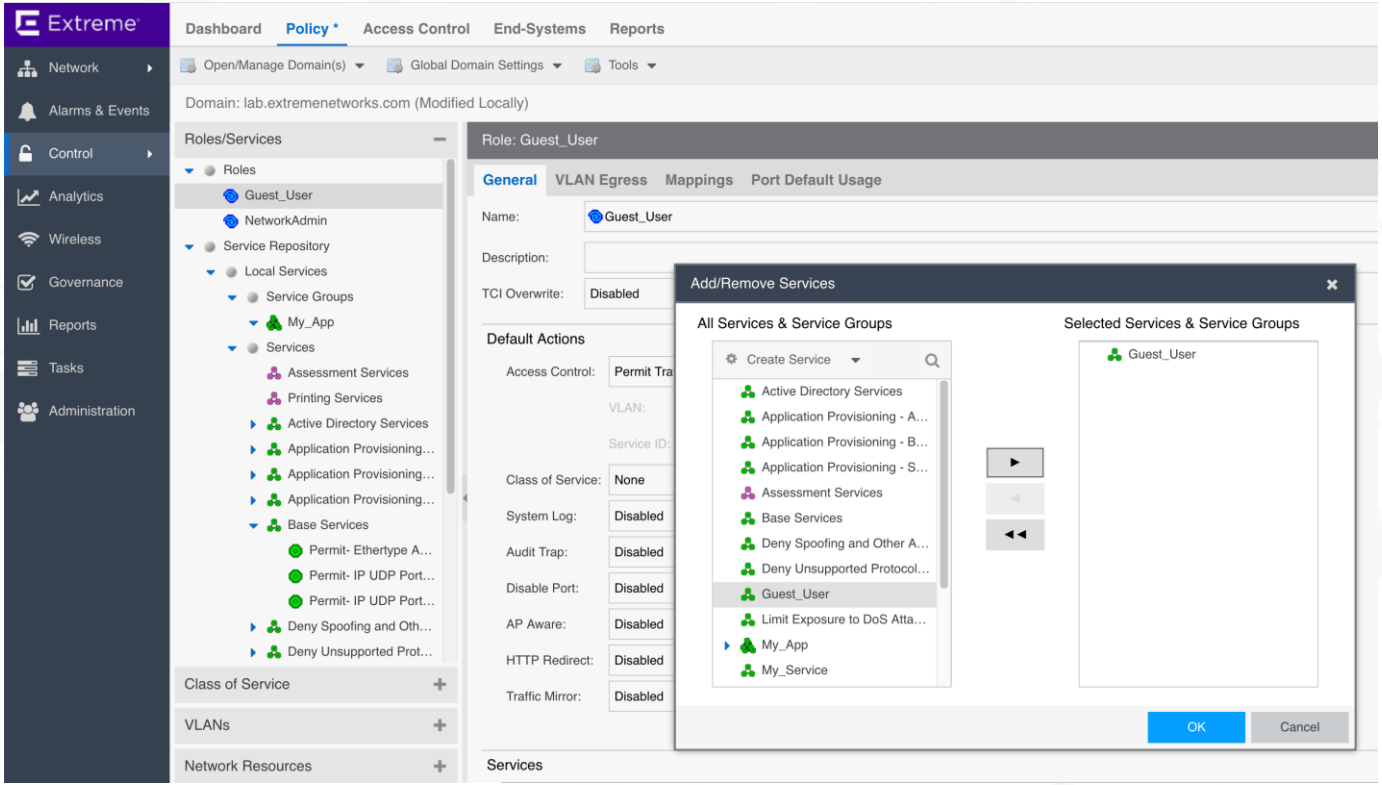
- Сервис это – группа правил разрешающих или запрещающих работу определенного сетевого сервиса
- Для составление правил используются информация из L2 или L3 заголовка пакета.
- Стандартные поля
- Точные значения полей или диапазоны значений



Детальное описание сервиса



Назначение сервиса на роль



Сохранение изменений в домене и активация

- Изменения в параметрах ролей и политик нужно сохранить
- Применить новые параметры для всех устройств в домене

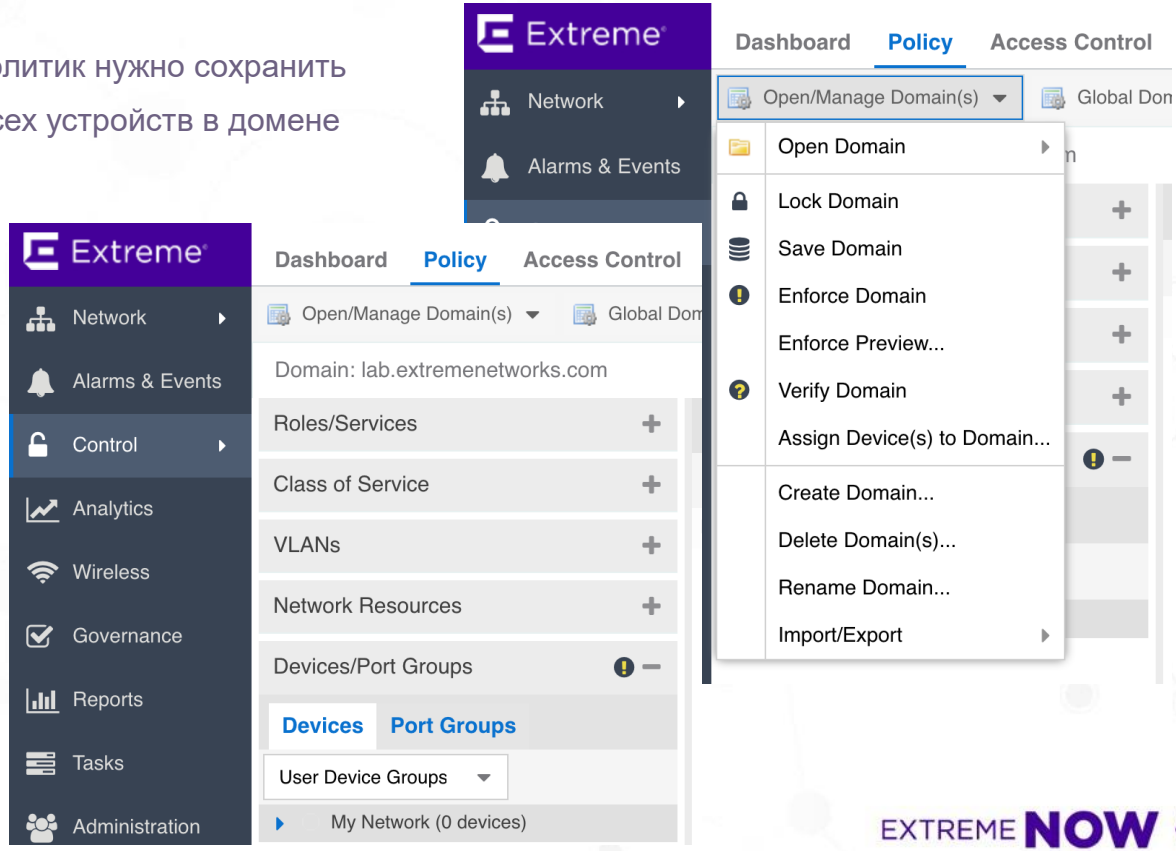
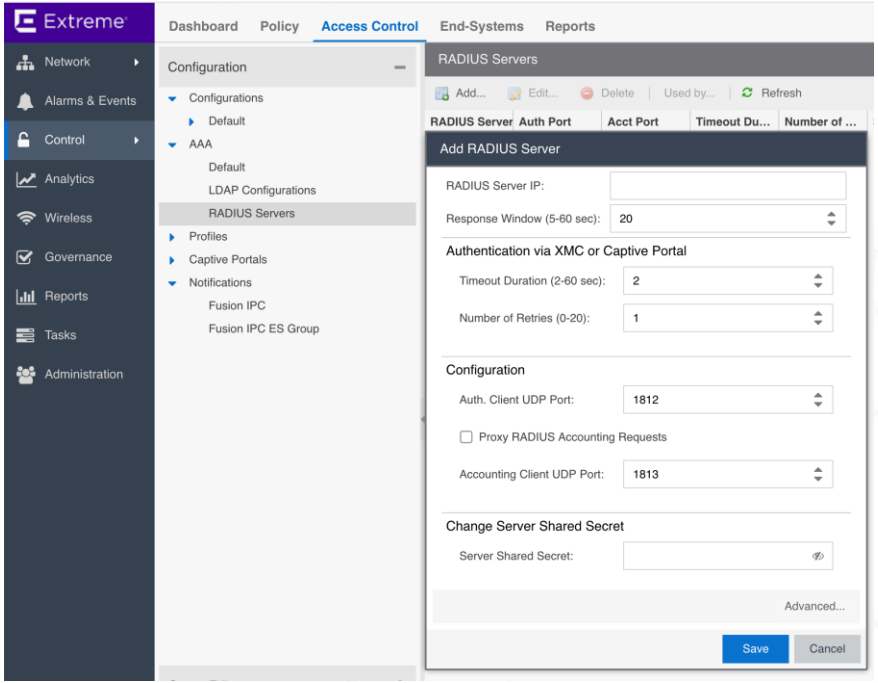


Схема авторизации пользователя

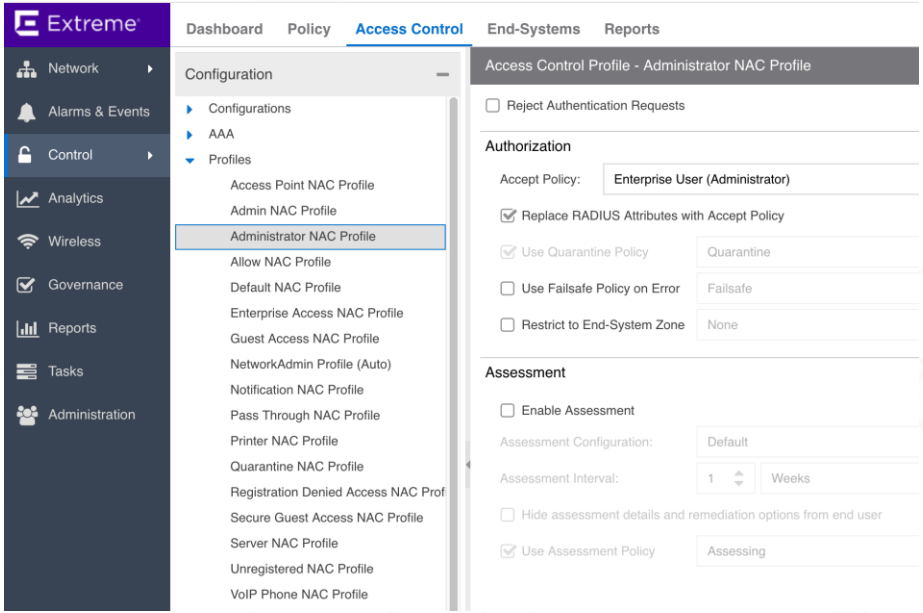
Доступны три способа авторизации пользователей:

- На внешнем RADIUS сервере
- На внешнем LDAP сервере
- С использованием встроенной базы пользователей



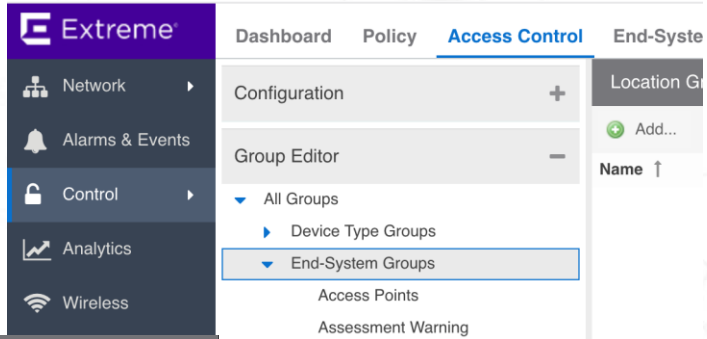
Профайл авторизации

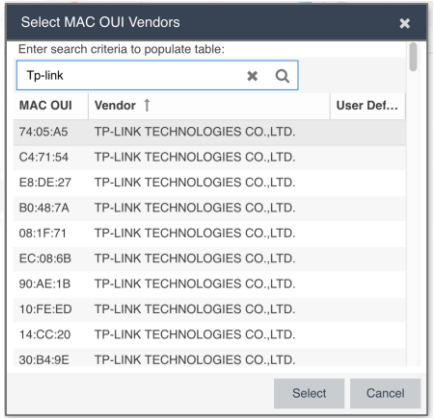
- Набор правил по авторизации абонента
- Определяет назначаемую роль
- Выбор альтернативной роли для аварийного режима
- Ограничения для использования только на отдельной группе устройств
- Включение дополнительных регулярных проверок на соответствие устройства профилю

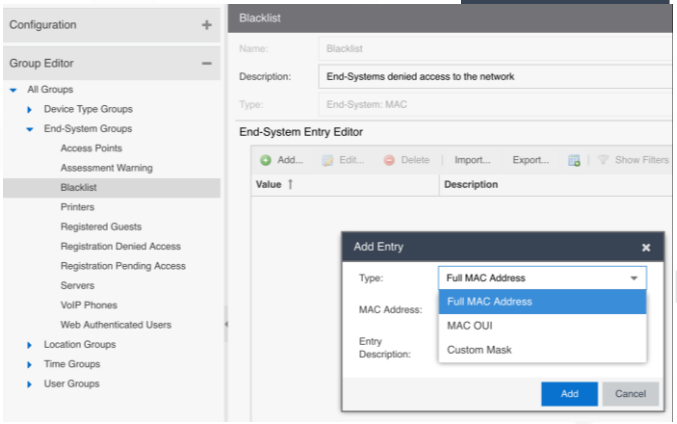


Черные и белые списки устройств

- Списки оконечных устройств на основе MAC-адресов
- Возможность назначения специальных политик для группы устрйств
- На основе полного MAC-адреса
- OUI производителя с возможностью поиска по списку
- Фрагмента MAC-адреса

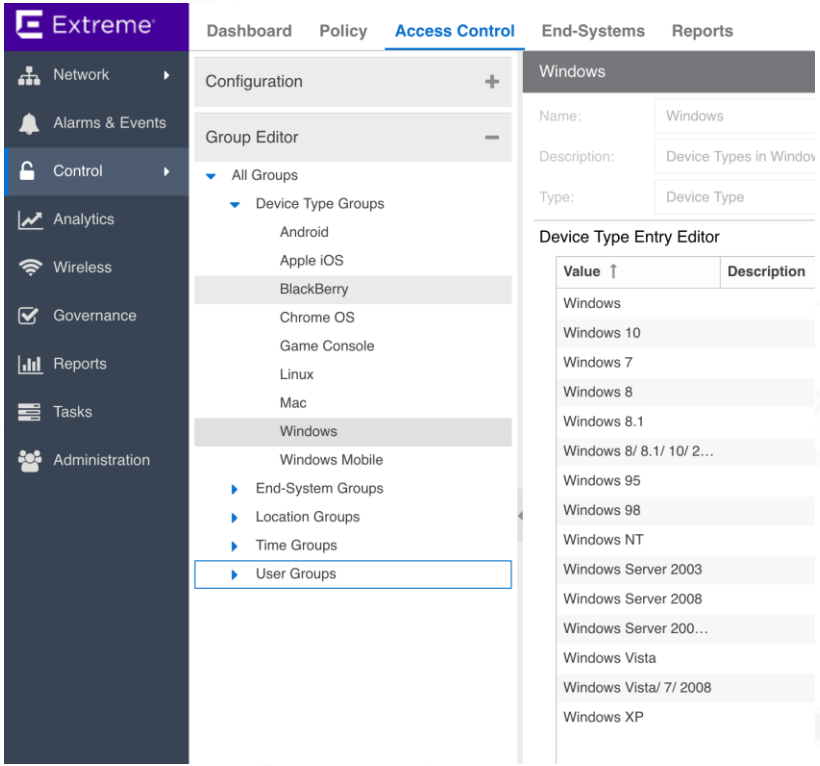






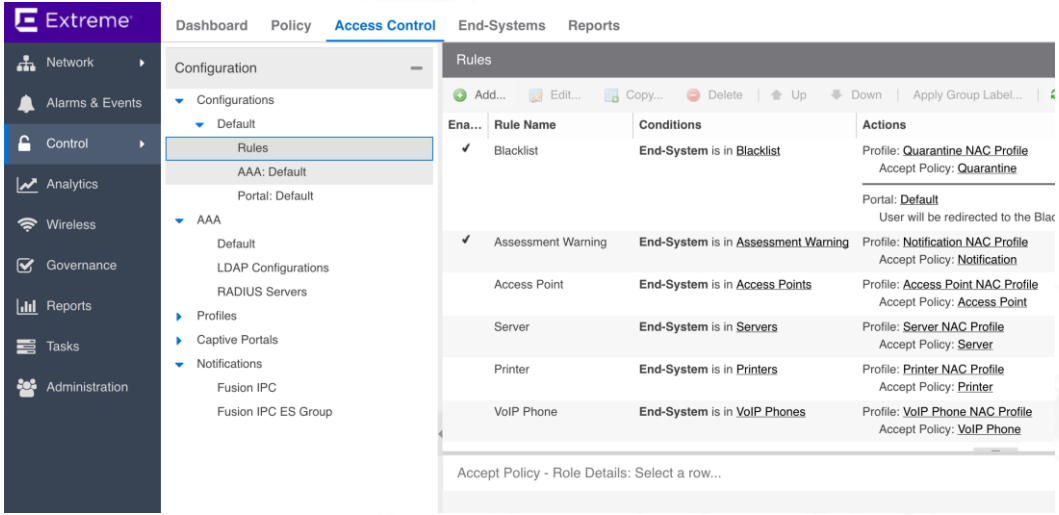
Типы оконечных устройств

- Категоризация оконечных устройств в зависимости от типа операционной системы
- Возможность назначения разных ролей в зависимости от типа операционной системы
- Встроенные профайлы для большого количества различных типов устройств
- Возможность создавать собственные списки на основе имеющихся профайлов

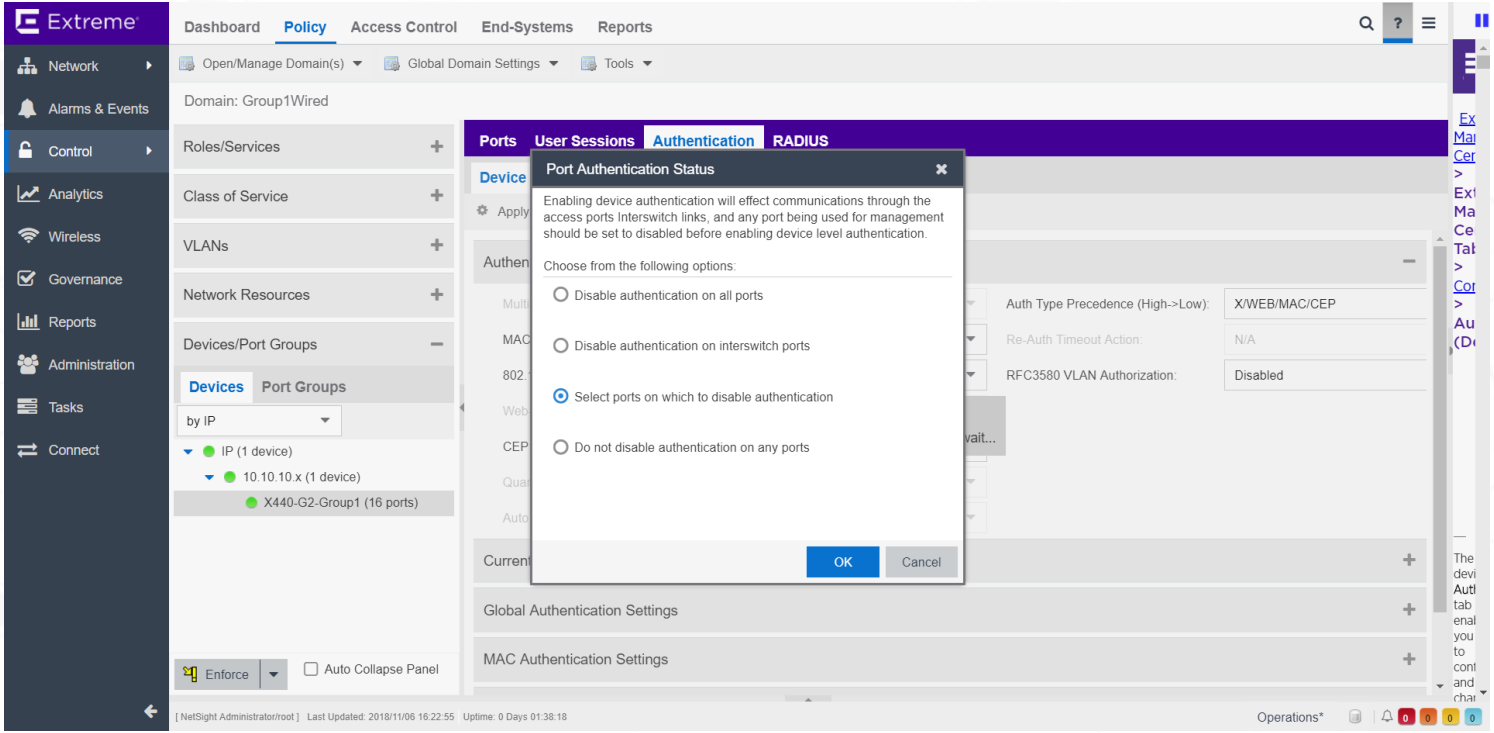


Авторизация пользователя

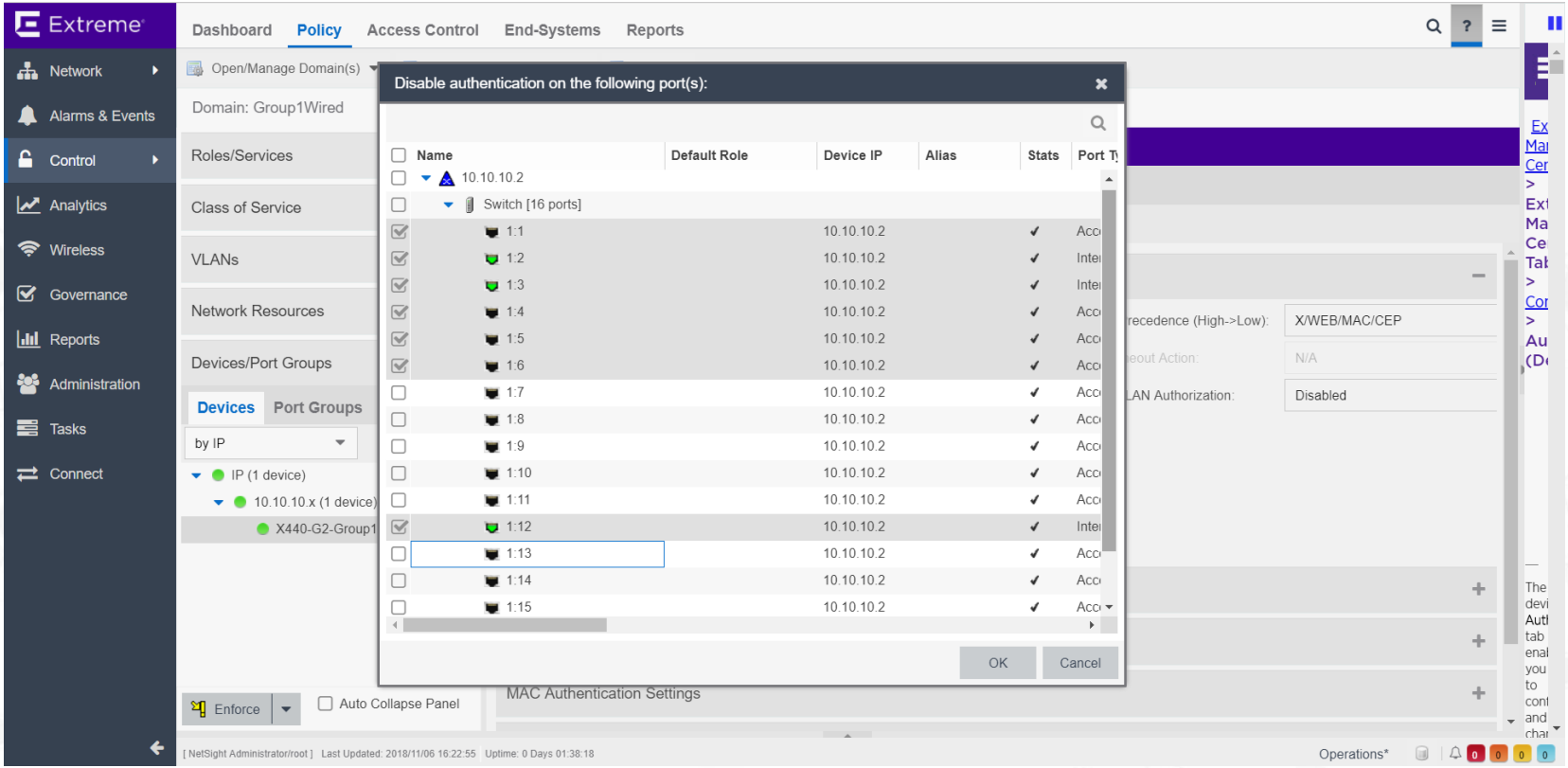
- Упорядоченный список правил
- Просмотр списка сверху вниз до первого совпадения критериев
- Черные и белые списки устройств
- Группы оконечных устройств по типу
- Общее правило для всех в конце списка



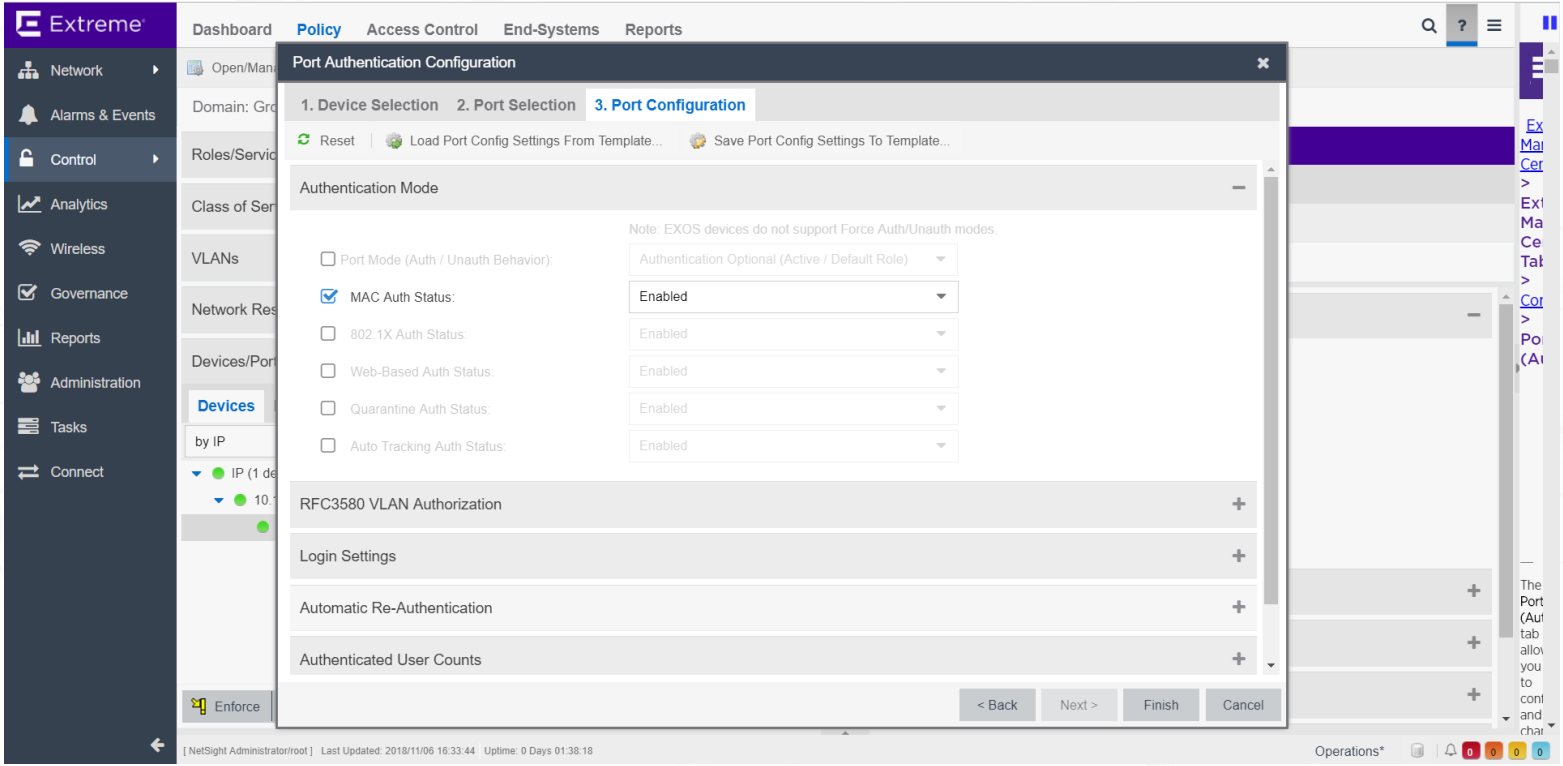
Настройка авторизации на коммутаторе



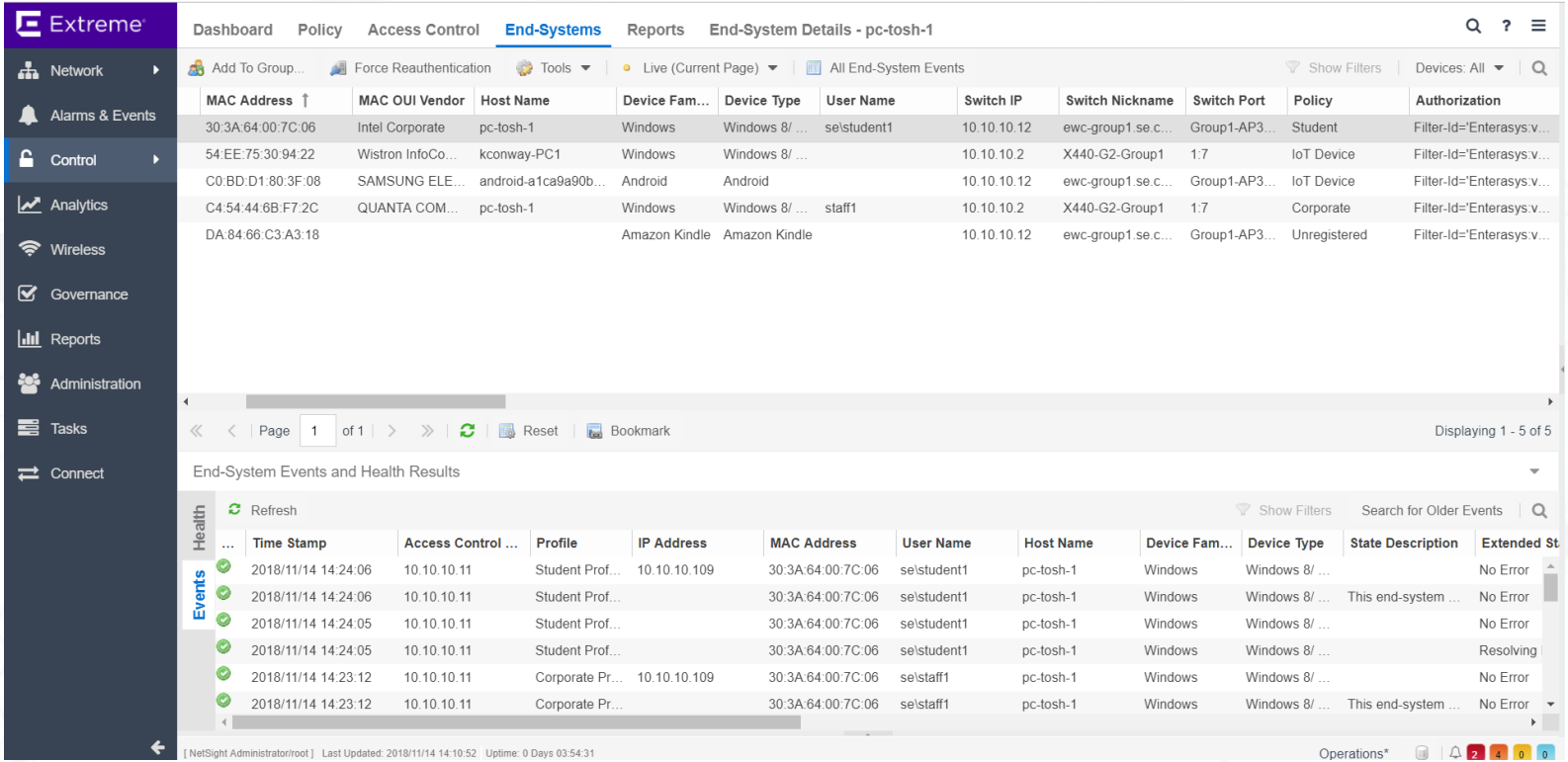
Настройка авторизации на коммутаторе



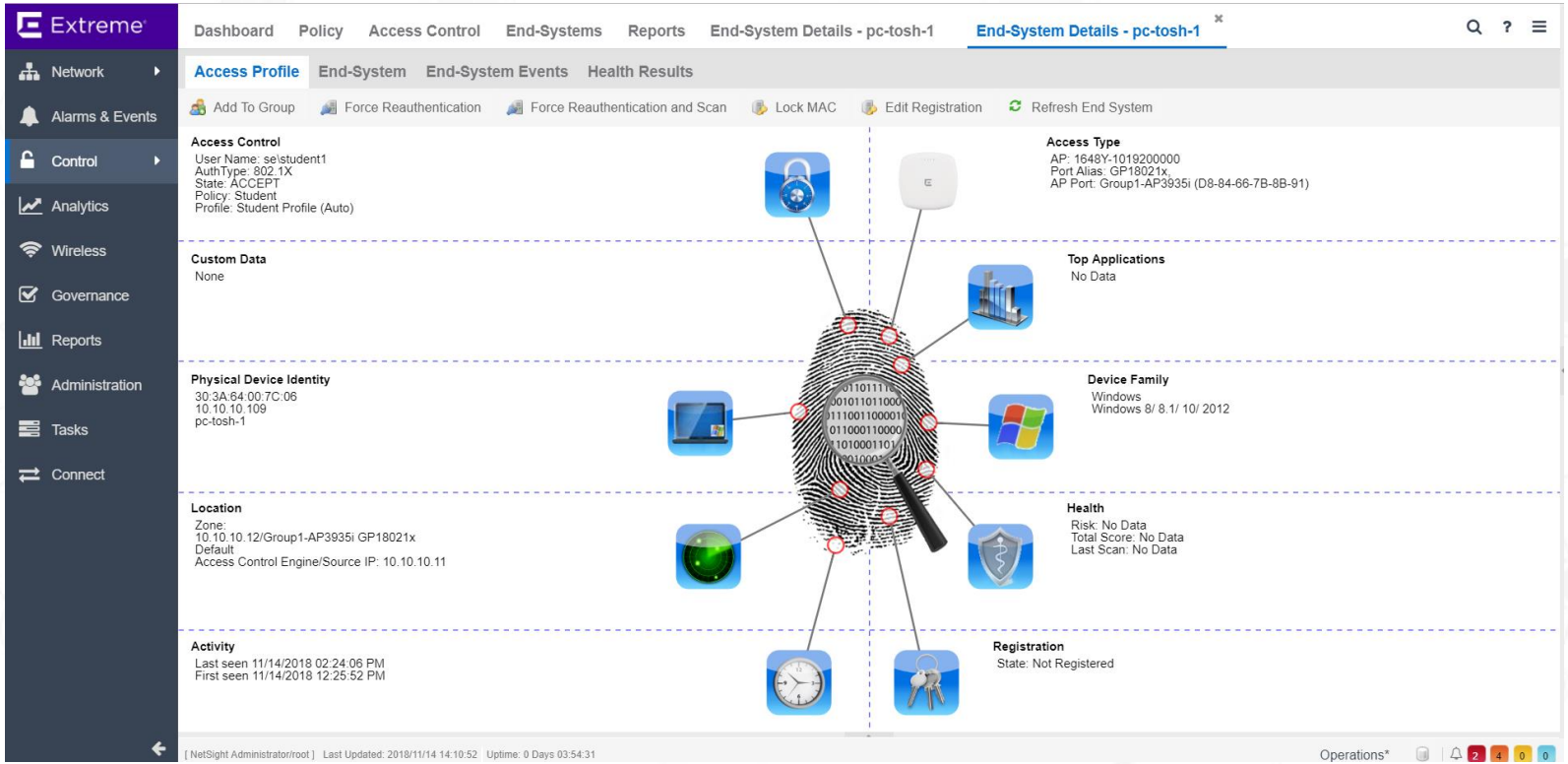
Настройка авторизации на коммутаторе



Отчет по подключенным пользователям



Детальная информация по пользователю




EXTREME
NOW
WORLD TOUR