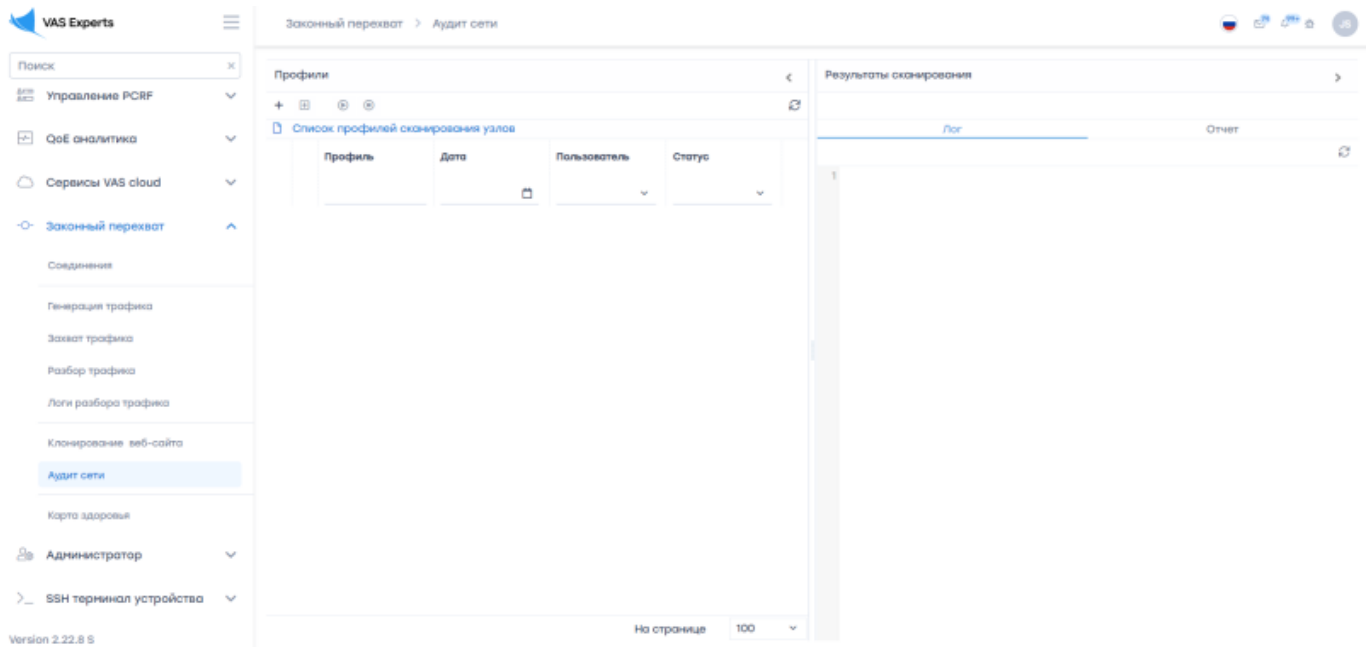
Содержание

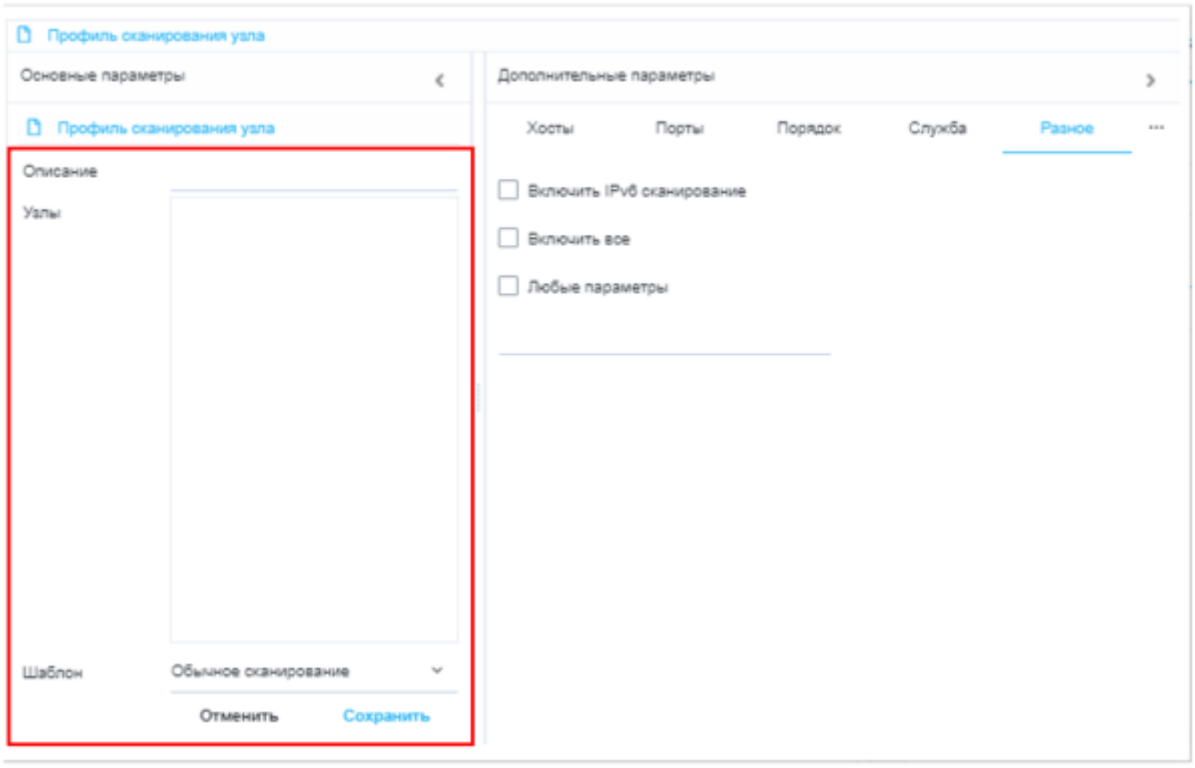
7 Аудит сети

Для перехода в раздел нажмите пункт меню Законный перехват, затем нажмите пункт меню Аудит сети.

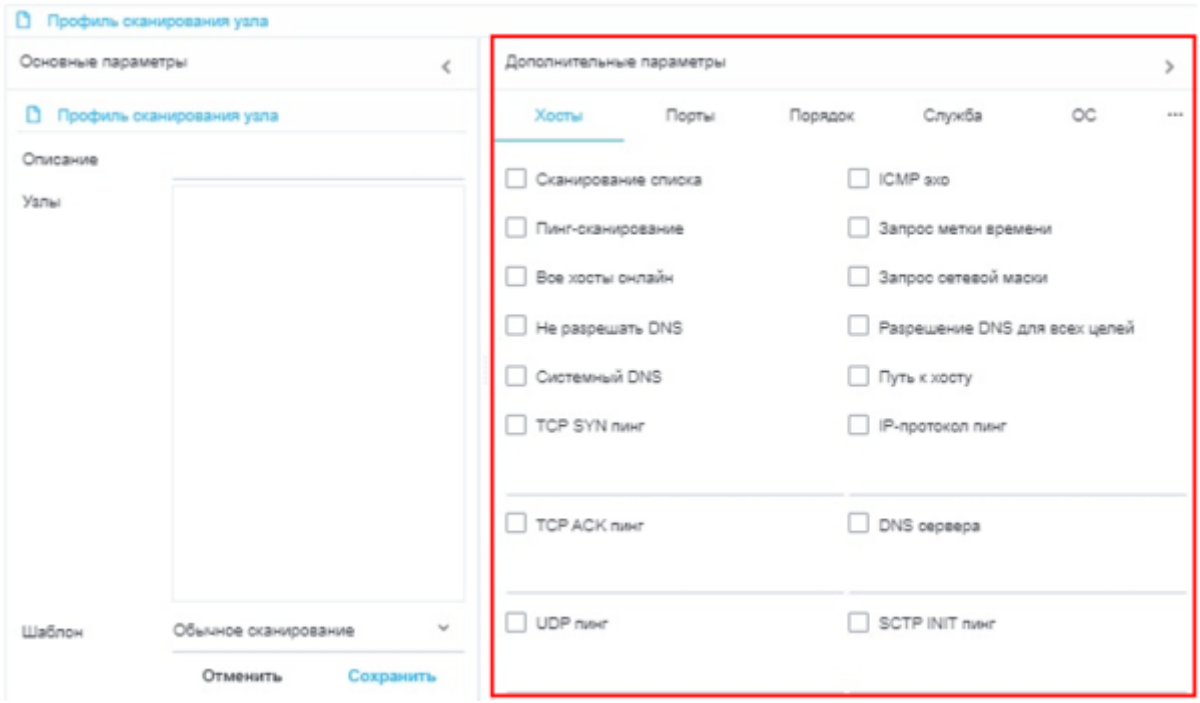


Данный раздел состоит из двух подразделов: "Профили" и "Результаты сканирования".

Профили



Чтобы добавить профиль сканирования, нажмите на кнопку "**Добавление профиля**", расположенную в туллбаре.
В раскрывшемся окне введите параметры.



Основные параметры:

1. **Описание**. Данное поле содержит название или описание профиля
2. **Узлы**. Данное поле содержит имена хостов, IP адреса, сети и т.д. Каждый с новой строки.
3. **Шаблон**. Данное поле заполняется путем выбора шаблона из выпадающего списка.

Дополнительные параметры:

Хосты

1. Сканирование списка. Данная опция позволяет получить пользователю список хостов, заданной сети.

2. Пинг-сканирование. Данная опция позволяет произвести определение хостов, а затем вывести список доступных хостов, т.е. тех, которые ответили на запросы.

3. Все хосты онлайн. Данная опция позволяет полностью пропустить этап обнаружения хостов.

4. Не разрешать DNS. Данная опция позволяет не делать обратного DNS-разрешения на найденных активных IP-адресах.

5. Системный DNS преобразователь. Данная опция позволяет использовать системный DNS преобразователь.

6. TCP SYN пинг. Данная опция осуществляется для обнаружения хостов путем установки связи с хостом и отправки TCP пакета на введный пользователем порт.

7. TCP ACK пинг.

8. UPD пинг. Данная опция осуществляется для обнаружения хостов, которая посылает пустой пакет на данные порты. Если порты не заданы, то по умолчанию используется 31338.

9. ICMP эхо.

10. Запрос временной метки. Опция предназначена для выведения текущего времени на хосте.

11. Запрос сетевой маски. Опция предназначен для выведения сетевой маски хоста.

12. Разрешение DNS для всех целей. Опция всегда выполняет обратное разрешение DNS имен для каждого целевого IP адреса.

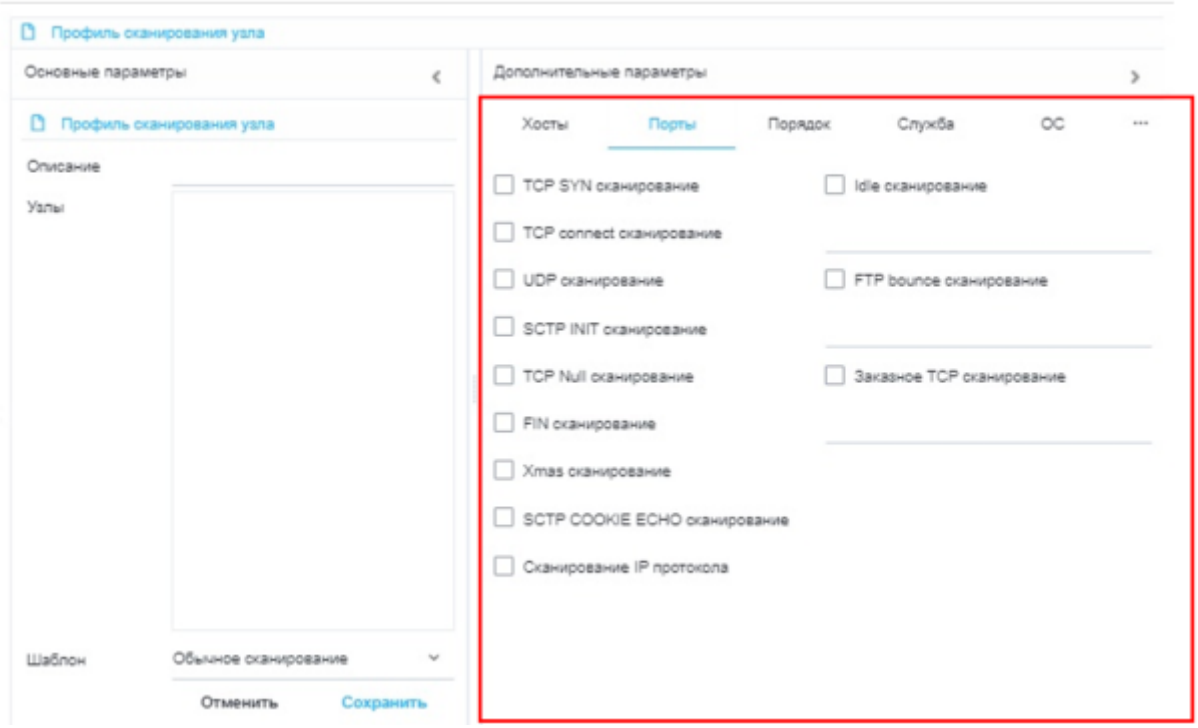
13. Путь к хосту. Опция осуществляется после сканирования, используя результаты для определения порта и протокола, с помощью которых можно будет достичь цели.

14. IP-протокол пинг. Опция осуществляется для обнаружения хостов является пингование с использованием IP протокола, которая посылает IP пакеты с номером протокола, указанным в заголовке пакета.

15. DNS сервер. Данная опция позволяет задать собственный сервер.

16. SCTP INIT пинг. Эта опция отправляет пакет SCTP, содержащий минимальный кусок INIT на введёный пользователь порт.

Порты



1.TCP SYN сканирование. По умолчанию и наиболее популярный тип сканирования.

2. TCP connect сканирование. По умолчанию тип TCP сканирования, когда недоступно SYN сканирование, но на получение той же самой информации потребуется больше времени и пакетов.

3. UPD сканирование. Сканирование по протоколу UPD.

4. SCTP INIT сканирование. Данная опция является новой альтернативой протоколам TCP и UPD, объединяя большинство характеристик TCP и UPD, а также добавляя новые функции, такие как многопоточность и многопоточность.

5. TCP Null сканирование. Не устанавливаются никакие биты (Флагов в TCP заголовке 0).

6. FIN сканирование. Устанавливается только TCP FIN бит.

7. Xmas сканирование. Устанавливаются FIN, PSH и URG флаги.

8. SCTP COOKIE ECHO сканирование.

9. Сканирование IP протокола. Опция позволяет определить, какие IP протоколы (TCP, ICMP, IGMP и т.д.) поддерживаются целевыми машинами.

10. idle сканирование. Опция позволяет осуществить действительно незаметное TCP сканирование портов цели. Необходимо ввести номер порта.

11. FTP bounce сканирование. Опция позволяет сканировать порты с помощью FTP протокола. Необходимо ввести адрес FTP сервера.

12. Заказное TCP сканирование.

Порядок

1. Быстрое сканирование.

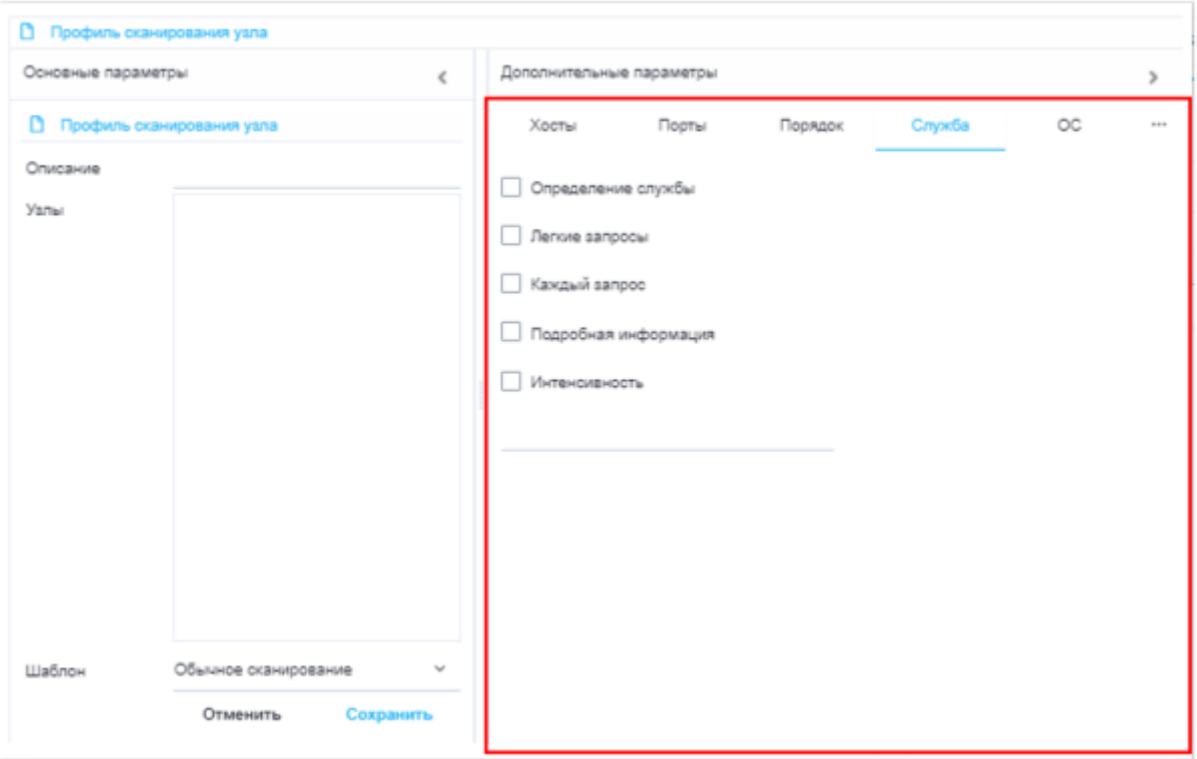
2. Неслучайный порядок портов. По умолчанию используется произвольный порядок сканирования портов.

3. Только определенные порты. Позволяет определить, какие порты необходимо просканировать и переопределить установки по умолчанию. Указание отдельных номеров портов допустимо, как и задание диапазона портов, разделенных дефисом.

4. Наиболее распространенные порты.

5. Сканирование портов с рейтингом. Сканирует все порты, чей рейтинг больше числа, указанного как аргумент (десятичное число между 0 и 1).

Служба



1. Определение службы. Исследовать открытые порты для определения информации о службе/ версии.

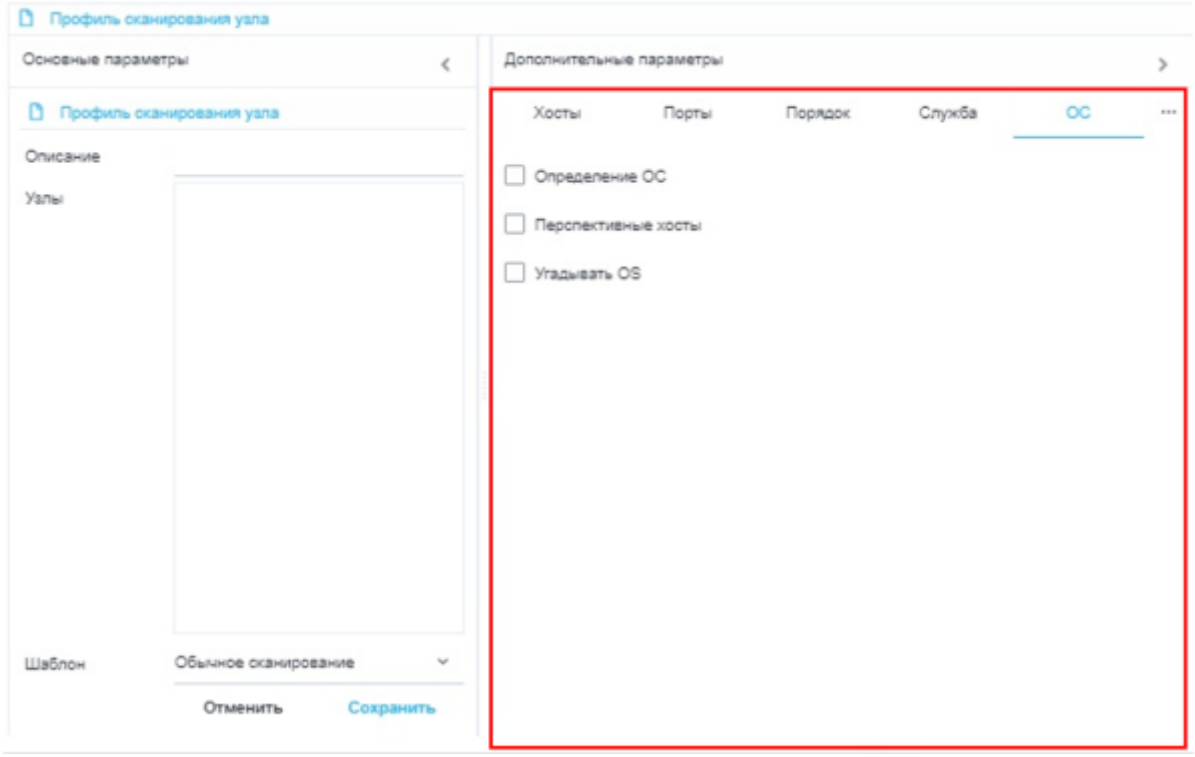
2. Легкие запросы. Этот режим существенно уменьшает время сканирования, но вероятность определения служб сокращается.

3. Каждый запрос. Этот режим гарантирует, что каждый единичный запрос будет направлен на каждый порт.

4. Подробная информация. Этот режим выводит подробную отладочную информацию о процессе сканирования.

5. Интенсивность. Уровень интенсивности должна быть задана числом от 0 до 9. По умолчанию уровень интенсивности равен 7.

ОС



1. Определение ОС. Опция включает функцию определения операционной системы.

2. Перспективные хосты.

3. Угадывать OS. Данная опция будет сообщать, когда будет найдено не идеальное совпадение, а также отображать степень соответствия (в процентах) для каждого набора характеристик.

Фаервол

1.Фрагментиторать пакеты. При задании данной опции все типы сканирования (включая различные типы пингования) будут использовать маленькие фрагментированные IP пакеты.

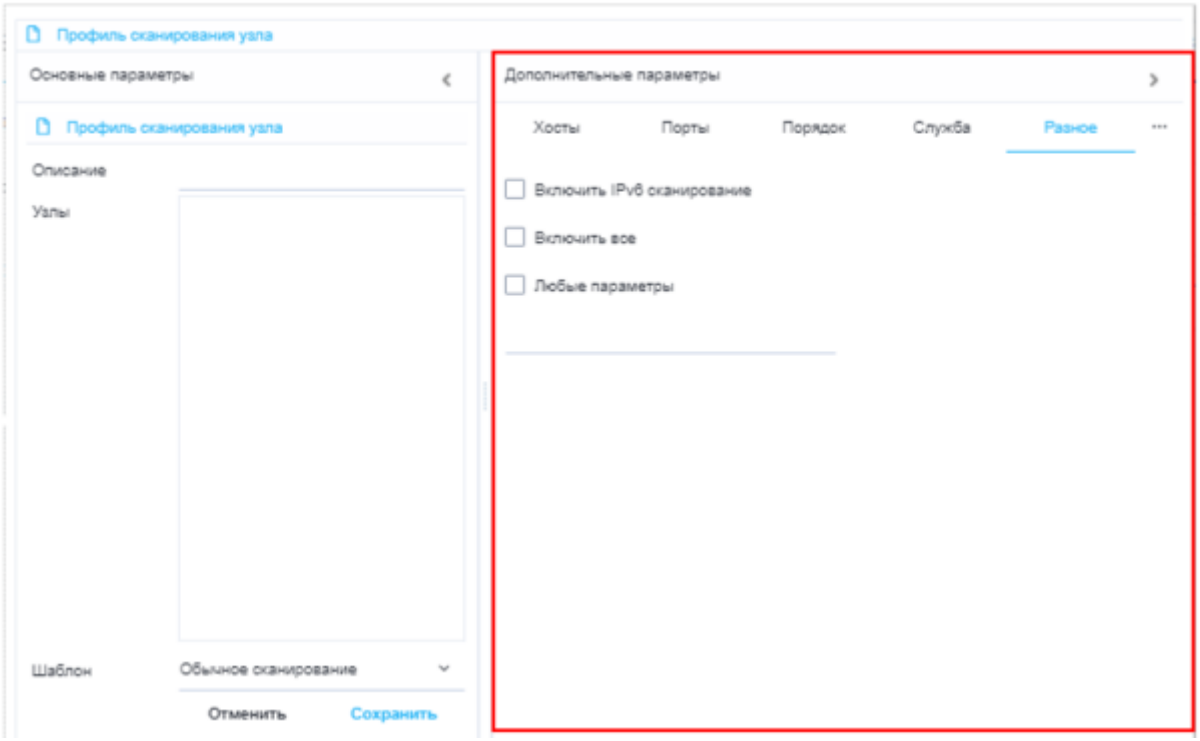
2. MTU фрагментации. Данная опция позволяет задать свой собственный размер фрагмента. Размер должен быть кратным 8.

3. Маскировка сканирования. Данная опция позволяет скрыть IP адрес с помощь фиктивных хостов. При задании фиктивных хостов необходимо разделить их запятыми.

4. Изменить адрес.

5. Изменить исходный адрес. Для использования данной опции необходимо в качестве параметра IP адрес, чтобы указать интерфейс, который вы хотите использовать для отправки пакетов.

Разное

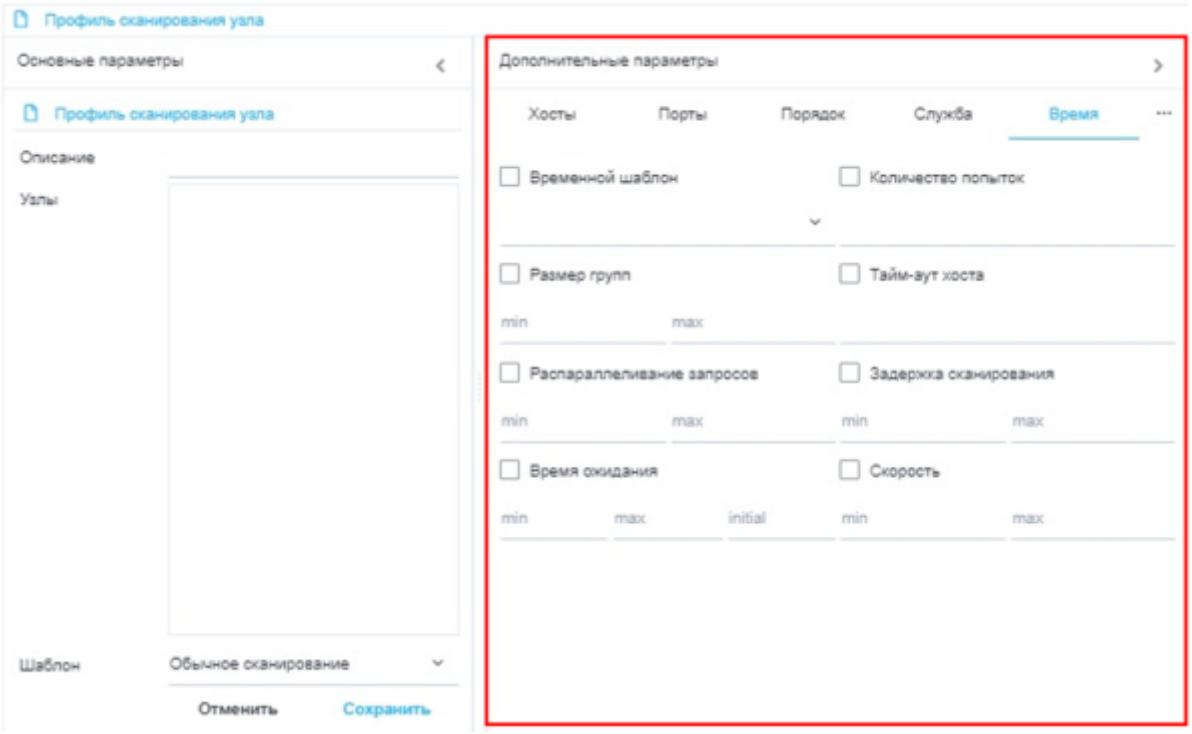


1. Включить IPv6 сканирование.

2. Включить все. Активировать функции определения операционной системы и версии, сканирование с использованием скриптов и трассировку.

3. Любые параметры.

Время



1. Временный шаблон. Режимы paranoid(паранойдный) и sneaky(хитрый) предназначены для обхода IDS. Вежливый (polite) режим снижает интенсивность сканирования с целью меньшего потребления пропускной способности и машинных ресурсов. Обычнй (normal) режим устанавливается по умолчанию, поэтому опция -T3 ничего не делает. Агрессивный (aggressive) режим повышает интенсивность сканирования, предполагая, что пользователь использует довольно быструю и надежную сеть. Наконец, безумный (insane) режим предполагает, что пользователь использует чрезвычайно быструю сеть и готов пожертвовать точностью ради скорости.

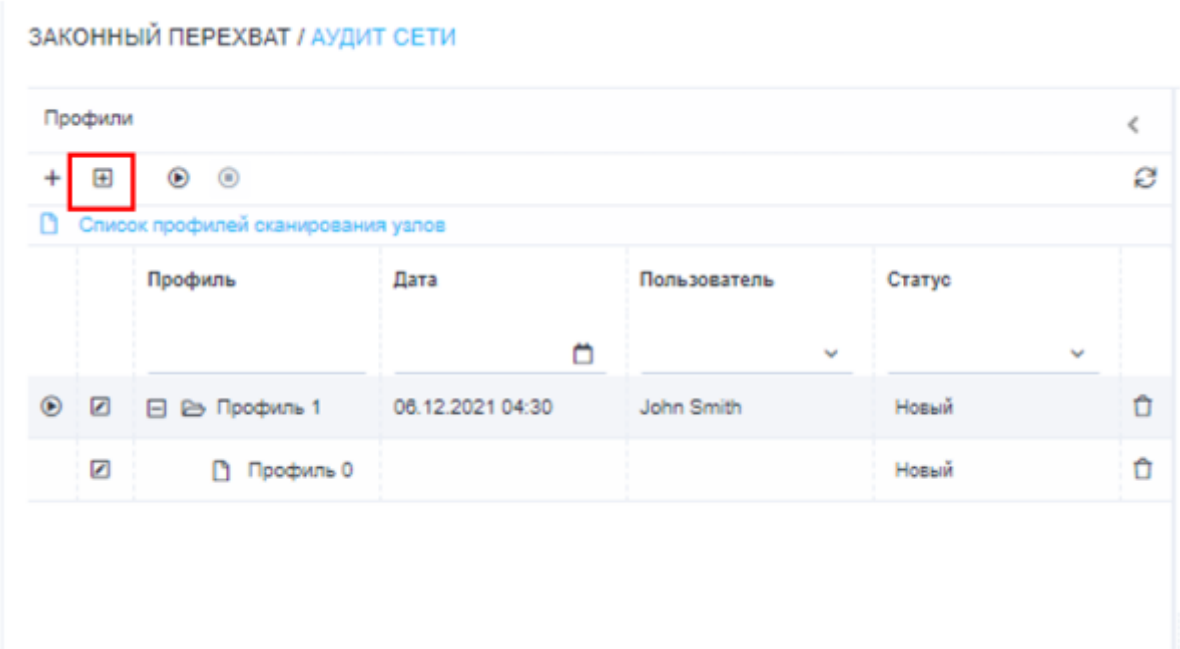
2.Размер групп. Необходимо установить размер групп хостов для параллельного сканирования.

3. Распараллеливание запросов. Данная опция регулируют общее количество запросов для группы хостов. Необходимо установить размер групп хостов.

4. Время ожидания. Данная опция регулирует время ожидания ответа на запрос.

Добавить подпрофиль

Чтобы добавить подпрофиля сканирования, нажмите на кнопку **«Добавление подпрофиля»**, которая находится в туллбаре и проделайте вышеописанные задачи.

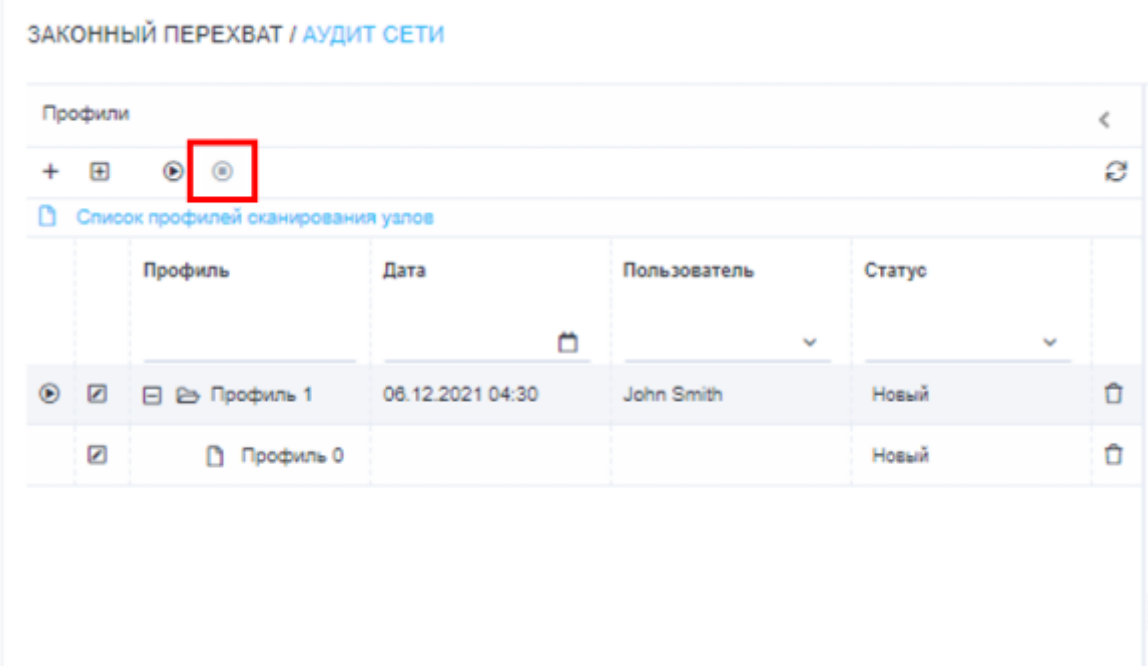


Запустить сканирование

Чтобы запустить сканирование профиля, выберете профиль из списка и нажмите на кнопку **«Запустить сканирование»**.
Запустить выбранный профиль можно также с помощью кнопки, которая расположена слева от каждого профиля списка.

Остановить сканирование

Чтобы остановить запущенное сканирование профиля, нажмите на кнопку **«Остановить сканирование»**.



Остановить сканирование

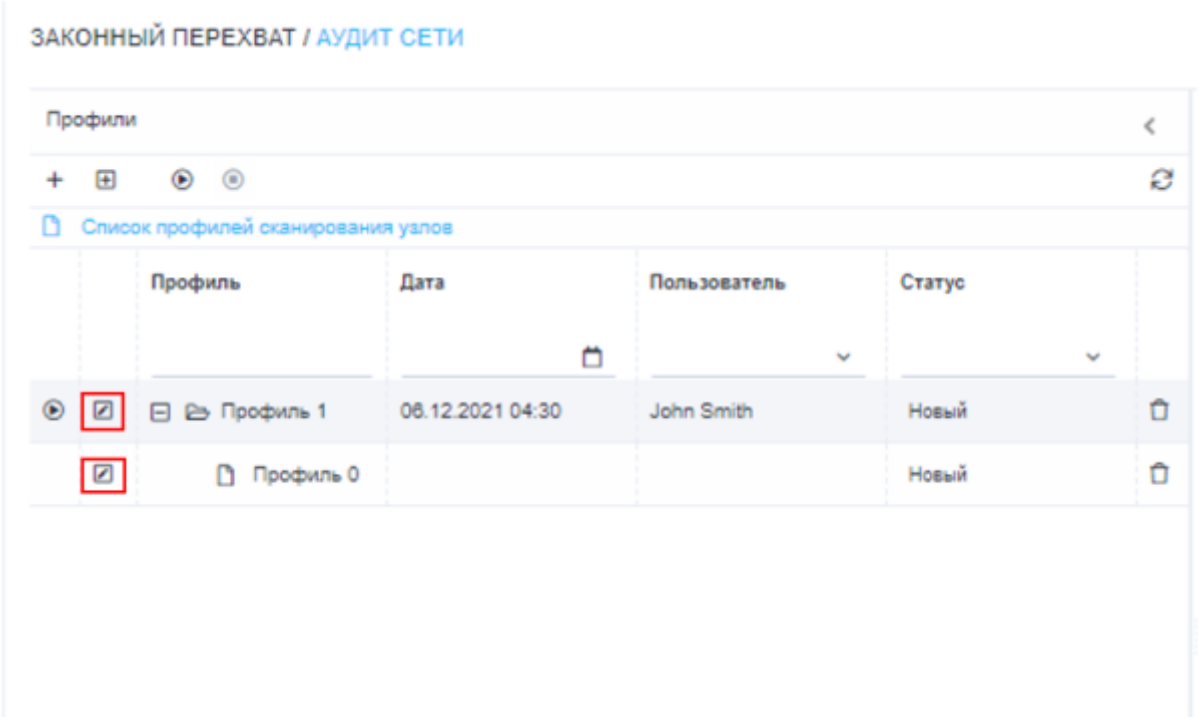
Чтобы обновить список профилей,нажмите на кнопку **«Обновить»**.

Обновить список

Чтобы обновить список профилей,нажмите на кнопку **«Обновить»**.

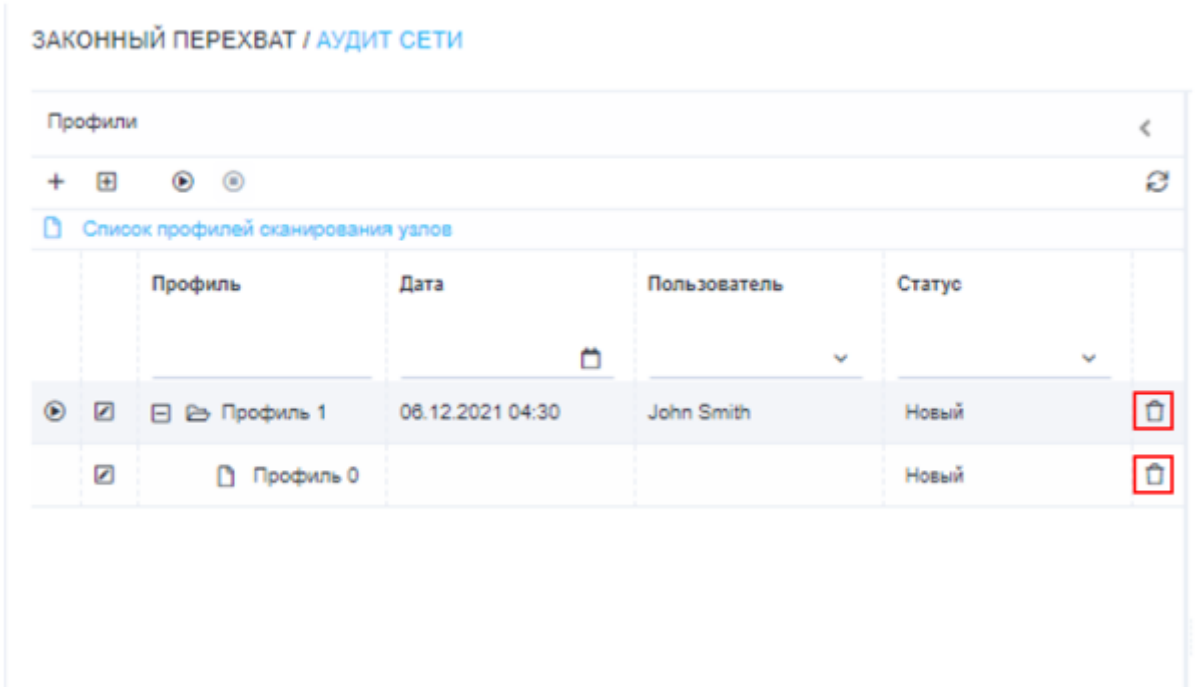
Изменить элемент списка

Чтобы изменить параметы профиля или подпрофиля, нажмите на кнопку **"Изменить"**, которая расположена слева от каждого элемента списка.



Удалить элемент списка

Чтобы удалить элемент списка, нажмите на кнопку "**Удалить**", которая расположена справа от каждого элемента списка.



Результат сканирования

Данный блок состоит из двух сегментов, которые отвечают за состояние проверенных узлов.