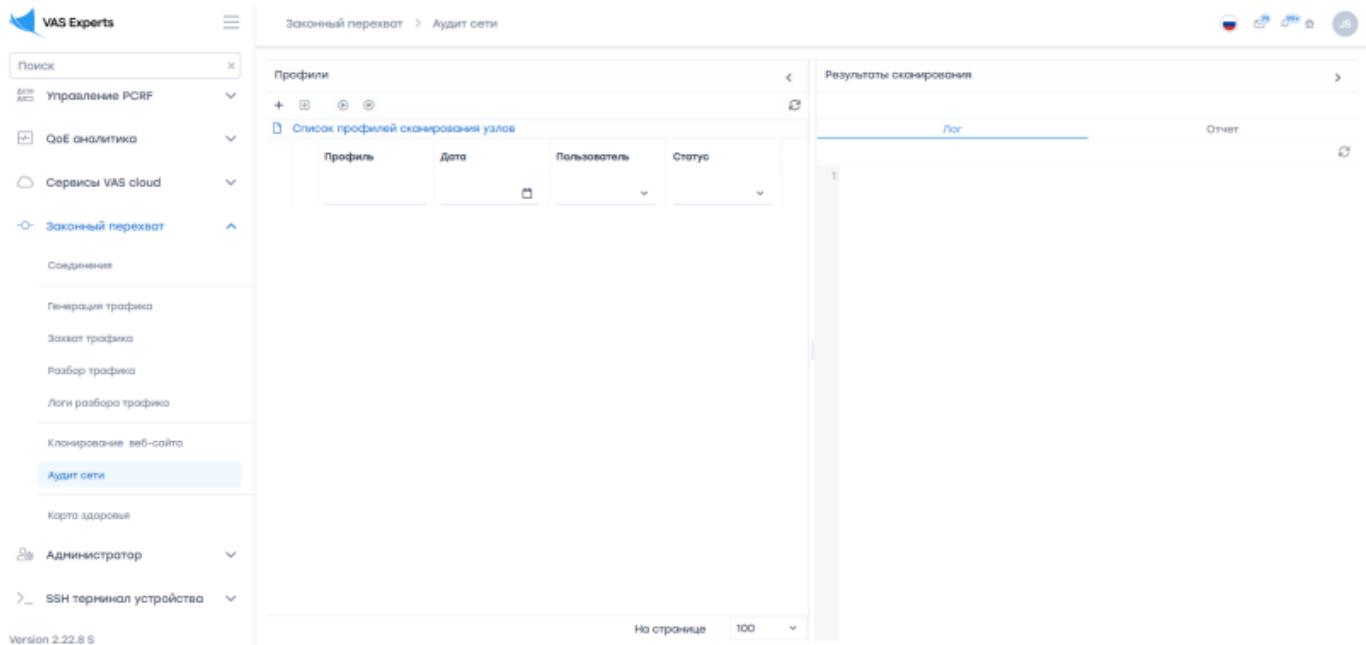


Содержание

7 Аудит сети	3
 Профили	3
Добавить подпрофиль	10
Запустить сканирование	11
Остановить сканирование	11
Остановить сканирование	12
Обновить список	12
Изменить элемент списка	12
Удалить элемент списка	13
 Результат сканирования	13

7 Аудит сети

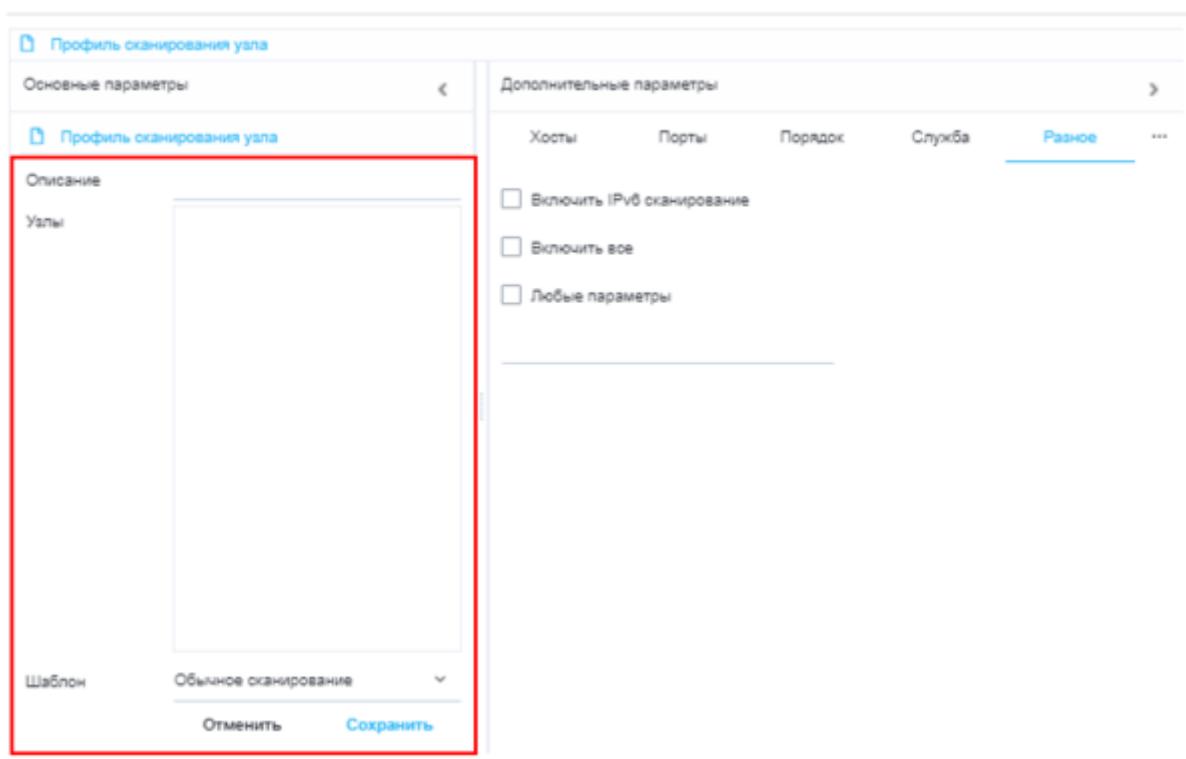
Для перехода в раздел нажмите пункт меню Законный перехват, затем нажмите пункт меню Аудит сети.



The screenshot shows the VAS Experts software interface. On the left, there is a sidebar with various menu items: Управление PCRF, QoE аналитика, Сервисы VAS cloud, Законный перехват (which is expanded), Соединения, Генерация трафика, Захват трафика, Разбор трафика, Логи разбора трафика, Клонирование веб-сайта, and Аудит сети (which is selected and highlighted in blue). Below this is a user section for 'Администратор' and a 'Version 2.22.8 S' note. The main content area has two tabs: 'Профили' (Profiles) and 'Результаты сканирования' (Scan results). The 'Профили' tab displays a table with columns: Профиль, Дата, Пользователь, and Статус. The 'Результаты сканирования' tab shows a log entry with the number '1'.

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

Профили



This screenshot shows the 'Profile configuration' dialog. It has two main sections: 'Основные параметры' (Main parameters) and 'Дополнительные параметры' (Additional parameters). The 'Основные параметры' section contains a title 'Профиль сканирования узла' and a large text area labeled 'Описание' (Description) which is currently empty. The 'Дополнительные параметры' section has tabs for 'Хосты' (Hosts), 'Порты' (Ports), 'Порядок' (Order), 'Служба' (Service), and 'Разное' (Miscellaneous). The 'Разное' tab is selected. Under this tab, there are three checkboxes: 'Включить IPv6 сканирование' (Enable IPv6 scanning), 'Включить все' (Enable all), and 'Любые параметры' (Any parameters). At the bottom of the dialog, there are buttons for 'Отменить' (Cancel) and 'Сохранить' (Save).

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

The screenshot shows a software interface for creating a network scanning profile. On the left, there's a sidebar with 'Основные параметры' (Main parameters) and a large text input field for 'Описание' (Description). Below it are sections for 'Узлы' (Nodes), 'Шаблон' (Template), and a dropdown menu set to 'Обычное сканирование' (Normal scanning). At the bottom are 'Отменить' (Cancel) and 'Сохранить' (Save) buttons. To the right is the 'Дополнительные параметры' (Additional parameters) tab, which is highlighted with a red border. This tab contains a table with two columns: 'Хосты' (Hosts) and 'Порты' (Ports). The 'Хосты' column lists several scanning methods with checkboxes: 'Сканирование списка' (Scan list), 'Пинг-сканирование' (Ping scan), 'Все хосты онлайн' (All hosts online), 'Не разрешать DNS' (Do not resolve DNS), 'Системный DNS' (System DNS), 'TCP SYN пинг' (TCP SYN ping), 'TCP ACK пинг' (TCP ACK ping), 'UDP пинг' (UDP ping), and 'SCTP INIT пинг' (SCTP INIT ping). The 'Порты' column lists corresponding options: 'ICMP эхо' (ICMP echo), 'Запрос метки времени' (Time stamp request), 'Запрос сетевой маски' (Request subnet mask), 'Разрешение DNS для всех целей' (Resolve DNS for all targets), 'Путь к хосту' (Path to host), 'IP-протокол пинг' (IP protocol ping), 'DNS сервера' (DNS servers), and 'SCTP INIT пинг' (SCTP INIT ping). The 'Порты' column has a red 'X' icon at its top right corner.

Хосты	Порты
<input type="checkbox"/> Сканирование списка	<input type="checkbox"/> ICMP эхо
<input type="checkbox"/> Пинг-сканирование	<input type="checkbox"/> Запрос метки времени
<input type="checkbox"/> Все хосты онлайн	<input type="checkbox"/> Запрос сетевой маски
<input type="checkbox"/> Не разрешать DNS	<input type="checkbox"/> Разрешение DNS для всех целей
<input type="checkbox"/> Системный DNS	<input type="checkbox"/> Путь к хосту
<input type="checkbox"/> TCP SYN пинг	<input type="checkbox"/> IP-протокол пинг
<input type="checkbox"/> TCP ACK пинг	<input type="checkbox"/> DNS сервера
<input type="checkbox"/> UDP пинг	<input type="checkbox"/> SCTP INIT пинг

Основные параметры:

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

Дополнительные параметры:

Хосты



- Сканирование списка.** Данная опция позволяет получить пользователю список хостов, заданной сети.
- Пинг-сканирование.** Данная опция позволяет произвести определение хостов, а затем вывести список доступных хостов, т.е. тех, которые ответили на запросы.
- Все хосты онлайн.** Данная опция позволяет полностью пропустить этап обнаружения хостов.
- Не разрешать DNS.** Данная опция позволяет не делать обратного DNS-разрешения на найденных активных IP-адресах.
- 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 введенный пользователем порт.

7. TCP ACK пинг.

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

9. ICMP эхо.

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

11. Запрос сетевой маски. Опция предназначен для выводения 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 посыпает 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 введённый пользователь порт.

Порты

Хосты	Порты	Порядок	Служба	ОС	...
<input type="checkbox"/> TCP SYN сканирование	<input type="checkbox"/> Idle сканирование				
<input type="checkbox"/> TCP connect сканирование	<input type="checkbox"/> FTP bounce сканирование				
<input type="checkbox"/> UDP сканирование	<input type="checkbox"/> Заданное TCP сканирование				
<input type="checkbox"/> SCTP INIT сканирование					
<input type="checkbox"/> TCP Null сканирование					
<input type="checkbox"/> FIN сканирование					
<input type="checkbox"/> Xmas сканирование					
<input type="checkbox"/> SCTP COOKIE ECHO сканирование					
<input type="checkbox"/> Сканирование IP протокола					

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. UDP 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

The screenshot shows the 'Service' tab selected in a 'Scan profile settings' dialog. The tab contains five options: 'Service definition', 'Easy requests', 'Each request', 'Detailed information', and 'Intensiveness'. A red box highlights this tab and its content.

Хосты	Порты	Порядок	Служба	ОС	...
<input type="checkbox"/> Определение службы					
<input type="checkbox"/> Легкие запросы					
<input type="checkbox"/> Каждый запрос					
<input type="checkbox"/> Подробная информация					
<input type="checkbox"/> Интенсивность					

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

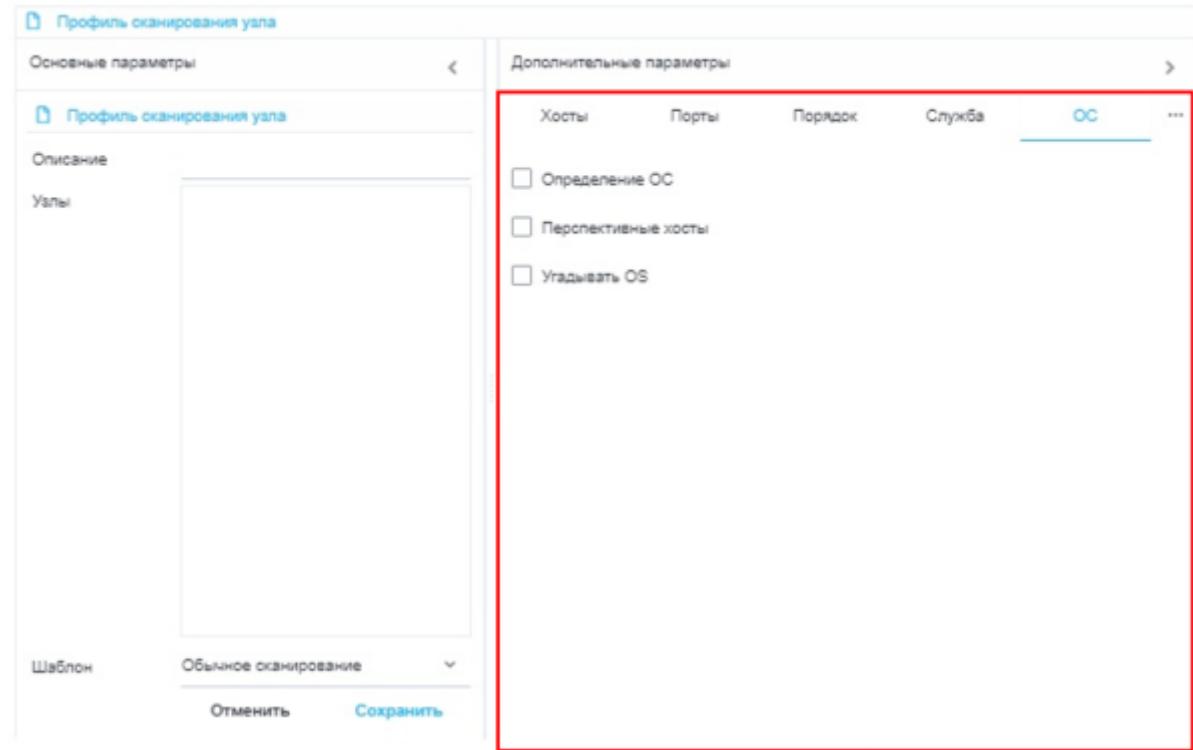
2. Легкие запросы. Этот режим существенно уменьшает время сканирования, но вероятность определения служб сокращается.

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

Фаервол



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

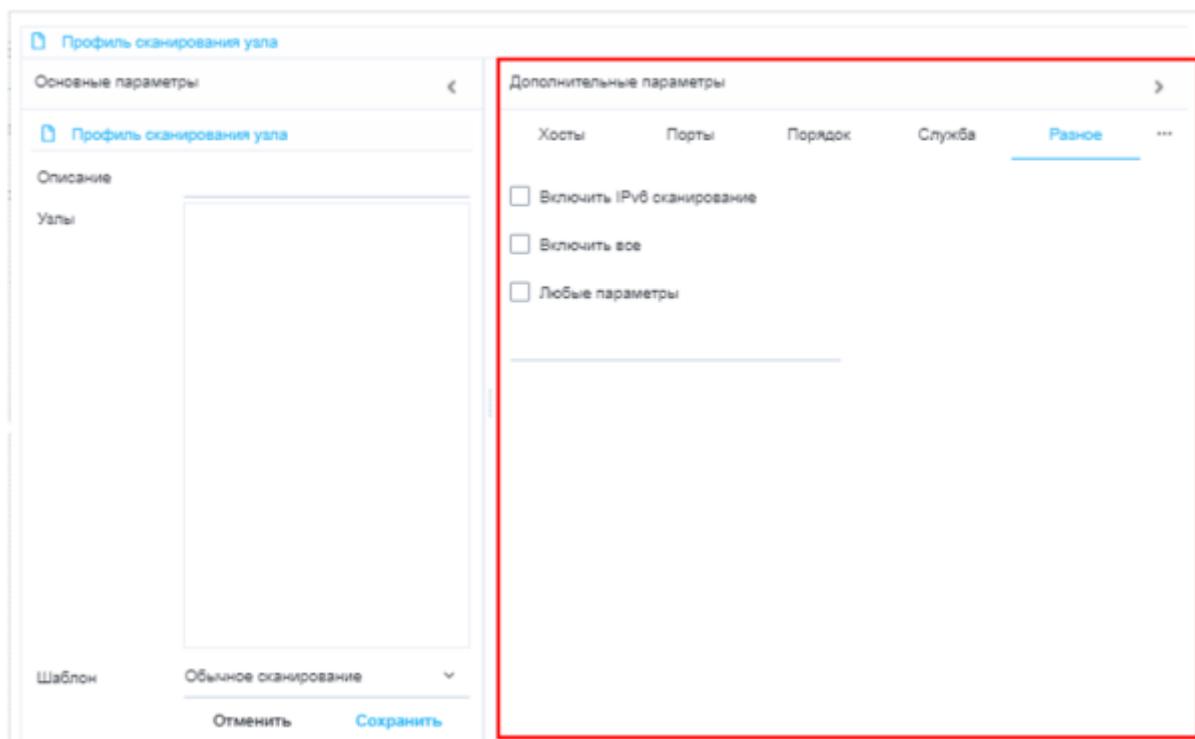
2. MTU фрагментации. Данная опция позволяет задать свой собственный размер фрагмента. Размер должен быть кратным 8.

3. Маскировка сканирования. Данная опция позволяет скрыть IP адрес с помощью 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

Профиль сканирования узла

Основные параметры

Профиль сканирования узла

Описание

Узлы

Шаблон

Обычное сканирование

Хосты Порты Порядок Служба Время

Временной шаблон Количество попыток

Размер групп Тайм-аут хоста

min max

Распараллеливание запросов Задержка сканирования

min max min max

Время ожидания Скорость

min max initial min max

Отменить Сохранить

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. Обычный (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 тулбаре и проделайте вышеописанные задачи.

Профили				
+				
	Профиль	Дата	Пользователь	Статус
 <input checked="" type="checkbox"/> 	Профиль 1	06.12.2021 04:30	John Smith	Новый
 <input type="checkbox"/> 	Профиль 0			Новый

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».

Профили

+

Список профилей сканирования уловов

Профиль	Дата	Пользователь	Статус
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Профиль 1	06.12.2021 04:30	John Smith	Новый
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Профиль 0			Новый

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 параметры профиля или подпрофиля, нажмите на кнопку "Изменить", которая расположена слева от каждого элемента списка.

ЗАКОННЫЙ ПЕРЕХВАТ / АУДИТ СЕТИ

Профили

+ ⌂ ⌄ ⌅ ⌆

Список профилей сканирования узлов

	Профиль	Дата	Пользователь	Статус	
⌚	<input checked="" type="checkbox"/> Профиль 1	06.12.2021 04:30	John Smith	Новый	
⌚	<input checked="" type="checkbox"/> Профиль 0			Новый	

Удалить элемент списка

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

ЗАКОННЫЙ ПЕРЕХВАТ / АУДИТ СЕТИ

Профили

+ ⌂ ⌄ ⌅ ⌆

Список профилей сканирования узлов

	Профиль	Дата	Пользователь	Статус	
⌚	<input checked="" type="checkbox"/> Профиль 1	06.12.2021 04:30	John Smith	Новый	
⌚	<input checked="" type="checkbox"/> Профиль 0			Новый	

Результат сканирования

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