

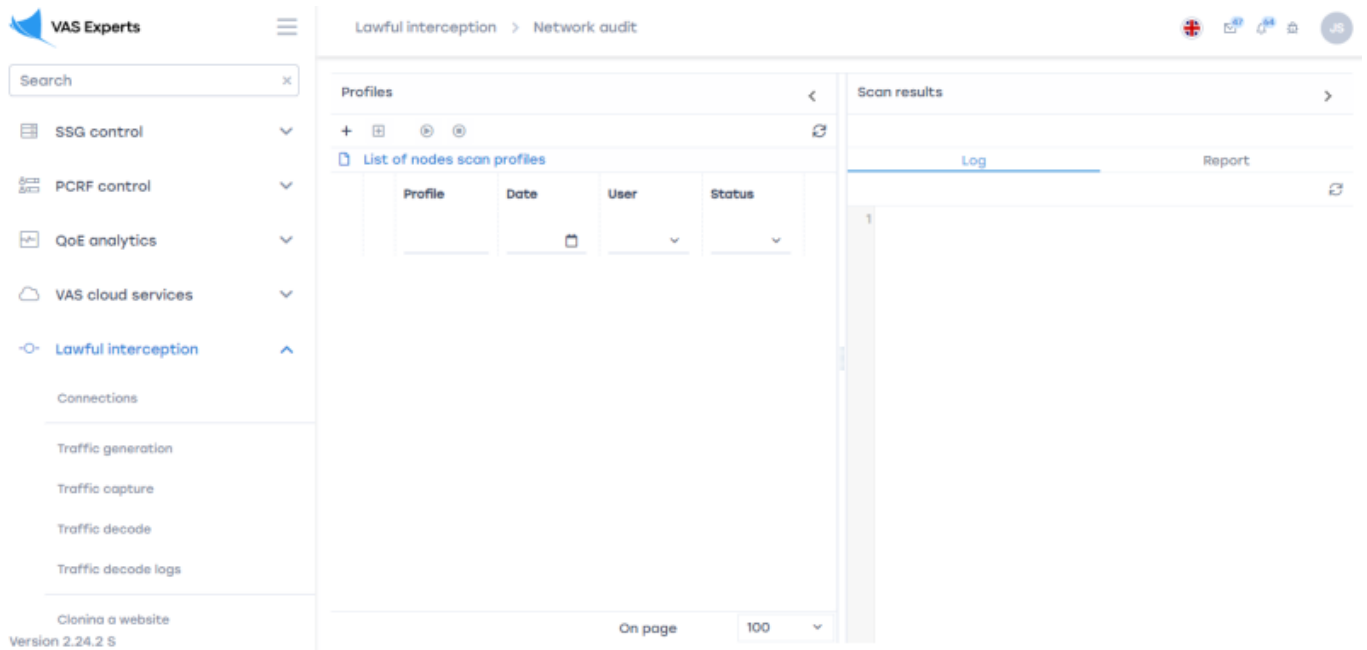
# Содержание

- 6 Network audit ..... 3
  - Profiles* ..... 3
  - Additional parameters:* ..... 4
    - Hosts ..... 4
    - Ports ..... 5
    - Order ..... 6
    - Service ..... 6
    - OS ..... 6
    - Firewall ..... 7
    - Misc ..... 7
    - Time ..... 8
  - Add underProfile* ..... 8
  - Start or stop scanning* ..... 8
  - Update the list* ..... 9
  - Delete a list item* ..... 9
  - Scan result* ..... 9



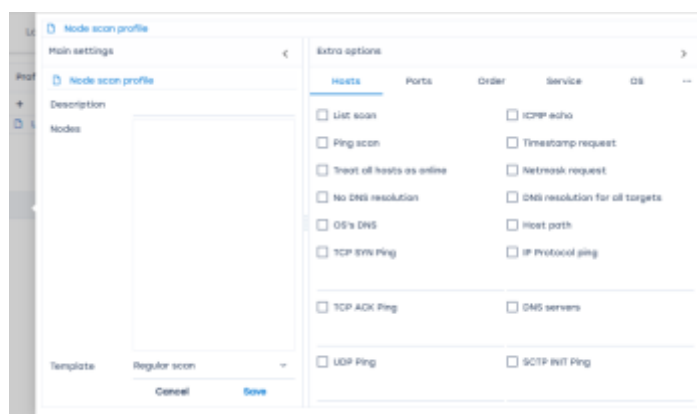
# 6 Network audit

To go to the section, click the **LAWFUL INTERCEPTION** menu item, then click the **NETWORK AUDIT** menu item.



## Profiles

To add a scan profile, click on the **"Add Profile"** button located in the toolbar. In the window that opens, enter the parameters.



Basic parameters:

1. Description. This field contains the name or description of the profile
2. Nodes. This field contains host names, IP addresses, networks, etc. Each with a new line.
3. The template. This field is filled in by selecting a template from the drop-down list.

# Additional parameters:

## Hosts

Hosts	Ports	Order	Service	OS	...
<input type="checkbox"/> List scan			<input type="checkbox"/> ICMP echo		
<input type="checkbox"/> Ping scan			<input type="checkbox"/> Timestamp request		
<input type="checkbox"/> Treat all hosts as online			<input type="checkbox"/> Netmask request		
<input type="checkbox"/> No DNS resolution			<input type="checkbox"/> DNS resolution for all targets		
<input type="checkbox"/> OS's DNS			<input type="checkbox"/> Host path		
<input type="checkbox"/> TCP SYN Ping			<input type="checkbox"/> IP Protocol ping		
<input type="checkbox"/> TCP ACK Ping			<input type="checkbox"/> DNS servers		
<input type="checkbox"/> UDP Ping			<input type="checkbox"/> SCTP INIT Ping		

- 1. Scan the list.** This option allows the user to get a list of hosts of a given network.
- 2. Ping scan.** This option allows you to identify hosts, and then display a list of available hosts, i.e. those that have responded to requests.
- 3. All hosts are online.** This option allows you to completely skip the host discovery stage.
- 4. Do not resolve DNS.** This option allows you not to do reverse DNS resolution on the found active IP addresses.
- 5. System DNS converter.** This option allows you to use the system DNS converter.
- 6. TCP SYN ping.** This option is used to detect hosts by establishing a connection with the host and sending a TCP packet to the port entered by the user.
- 7. TCP ACK ping.**
- 8. UPD ping.** This option is used to detect hosts that send an empty packet to these ports. If no ports are specified, 31338 is used by default.
- 9. ICMP echo.**
- 10. Request a timestamp.** The option is designed to display the current time on the host.
- 11. Network mask request.** The option is intended for displaying the network mask of the host.
- 12. DNS resolution for all purposes.** The option always performs reverse DNS name resolution for each target IP address.

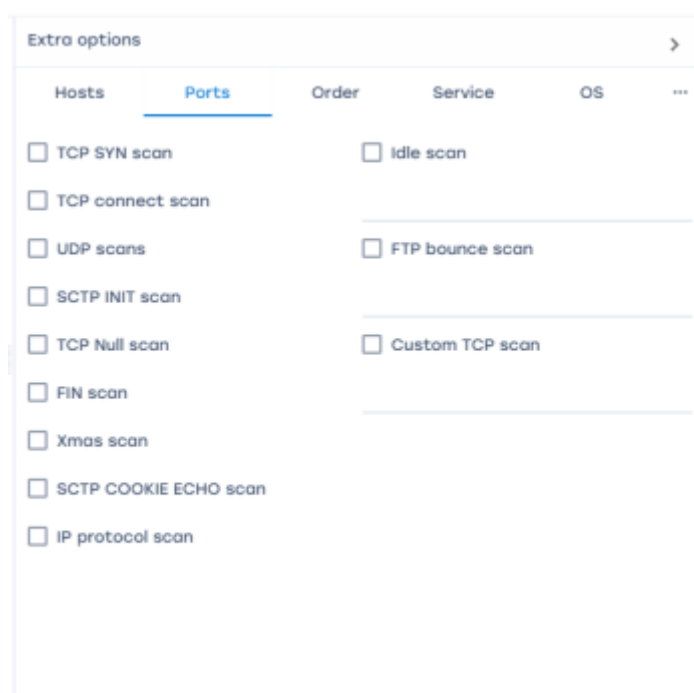
**13. The path to the host.** The option is carried out after scanning, using the results to determine the port and protocol with which it will be possible to achieve the goal.

**14. IP ping protocol.** The option implemented to detect hosts is pinging using the IP protocol, which sends IP packets with the protocol number specified in the packet header.

**15. DNS server.** This option allows you to set your own server.

**16. SCTP INIT ping.** This option sends a SCTP packet containing a minimal chunk of INIT to the user-entered port.

## Ports



The screenshot shows a window titled "Extra options" with a right-pointing arrow. Inside, there are tabs: "Hosts", "Ports" (which is selected and underlined), "Order", "Service", "OS", and "...". Below the tabs is a list of checkboxes for different scanning methods:

- ☐ TCP SYN scan
- ☐ TCP connect scan
- ☐ UDP scans
- ☐ SCTP INIT scan
- ☐ TCP Null scan
- ☐ FIN scan
- ☐ Xmas scan
- ☐ SCTP COOKIE ECHO scan
- ☐ IP protocol scan
- ☐ Idle scan
- ☐ FTP bounce scan
- ☐ Custom TCP scan

**1. TCP SYN scan.** By default and the most popular type of scanning.

**2. TCP connect scan.** By default, the TCP scan type is when SYN scanning is not available, but it will take more time and packets to get the same information.

**3. UPD scanning. Scanning using the UPD protocol.**

**4. SCTP INIT scan.** This option is a new alternative to the TCP and UPD protocols, combining most of the characteristics of TCP and UPD, as well as adding new features such as multithreading and multithreading.

**5. TCP Null scan.** No bits are set (Flags in TCP header 0).

**6. FIN scan.** Only the TCP FIN bit is set.

**7. Xmas scan.** The FIN, PSH and URG flags are set.

**8. SCTP COOKIE ECHO scan.**

**9. Scan the IP protocol.** This option allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by the target machines.

**10. idle scan.** This option allows you to perform a really inconspicuous TCP port scan of the target. You must enter the port number.

**11. FTP bounce scan.** This option allows you to scan ports using the FTP protocol. You must enter the FTP server address.

**12. Custom TCP scan.**

## Order



**1. Quick scan.**

**2. Non-random order of ports.** By default, an arbitrary order of port scanning is used.

**3. Only certain ports.** Allows you to determine which ports need to be scanned and override the default settings. Specifying individual port numbers is acceptable, as is specifying a range of ports separated by a hyphen.

**4. The most common ports.**

**5. Scan ports with rating.** Scans all ports whose rating is greater than the number specified as an argument (a decimal number between 0 and 1).

## Service



**1. Service definition.** Examine open ports to determine service/version information.

**2. Easy queries.** This mode significantly reduces the scanning time, but the probability of detecting services is reduced.

**3. Each request.** This mode ensures that every single request will be sent to every port.

**4. Detailed information.** This mode displays detailed debugging information about the scanning process.

**5. Intensity.** The intensity level should be set as a number from 0 to 9. By default, the intensity level is 7.

## OS



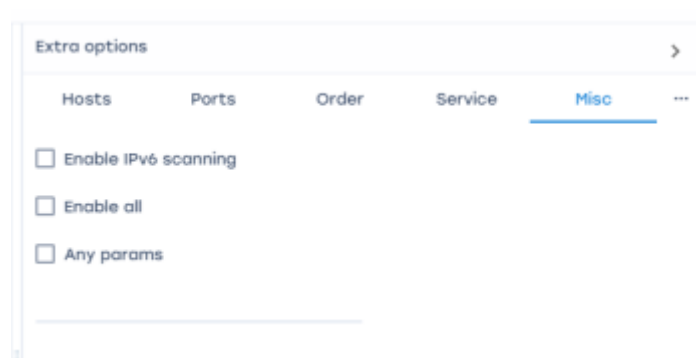
- 1. OS definition.** The option enables the function of determining the operating system.
- 2. Promising hosts.**
- 3. Guess OS.** This option will report when a non-perfect match is found, as well as display the degree of compliance (in percent) for each set of characteristics.

## Firewall



- 1.Fragment packages.** When this option is set, all types of scanning (including various types of pinging) will use small fragmented IP packets.
- 2. Fragmentation MTU.** This option allows you to set your own fragment size. The size must be a multiple of 8.
- 3. Scan masking.** This option allows you to hide the IP address using dummy hosts. When specifying dummy hosts, you need to separate them with commas.
- 4. Change the address.**
- 5. Change the source address.** To use this option, you need an IP address as a parameter to specify the interface that you want to use to send packets.

## Misc



- 1. Enable IPv6 scanning.**
- 2. Enable all.** Activate the functions of determining the operating system and version, scanning using scripts and tracing.
- 3. Any parameters.**

## Time

Extra options

Hosts Ports Order Service **Time** ...

☐ Timing template ☐ Retries number

☐ Group sizes ☐ Host time-out

min max

☐ Probe parallelization ☐ Scan delay

min max min max

☐ Waiting time ☐ Rate

min max initial min max

**1. Temporary template.** The paranoid and sneaky modes are designed to bypass IDS. Polite (polite) mode reduces the intensity of scanning in order to reduce the consumption of bandwidth and machine resources. Normal the mode is set by default, so the -T3 option does nothing. Aggressive mode increases the intensity of scanning, assuming that the user uses a fairly fast and reliable network. Finally, insane mode assumes that the user uses an extremely fast network and is willing to sacrifice accuracy for speed.

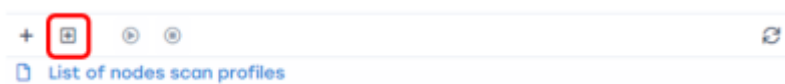
**2.Group size.** It is necessary to set the size of host groups for parallel scanning.

**3. Parallelization of queries.** This option regulates the total number of requests for a group of hosts. You need to set the size of the host groups.

**4. Waiting time.** This option regulates the waiting time for a response to a request.

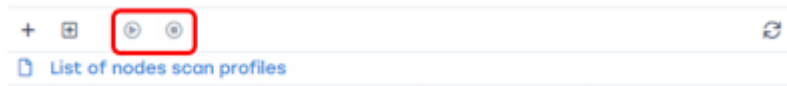
## Add underProfile

To add a scan subprofile, click on the button **"Add a subprofile"**, which is located in the toolbar and perform the tasks described above.



## Start or stop scanning

To start scanning a profile, select a profile from the list and click on the **"Start scanning"** button. You can also launch the selected profile using the button located to the left of each profile in the list. To stop the running profile scan, click on the **"Stop scanning"** button.




## Update the list

To update the list of profiles, click on the **"Update"** button.



## Delete a list item

To delete an item from the list, click on the **"Delete"**, which is located to the right of each list item.

List of nodes scan profiles					
	Profile	Date	User	Status	
<input checked="" type="checkbox"/>	Profile 0			New	

## Scan result

This block consists of two segments that are responsible for the status of the checked nodes.