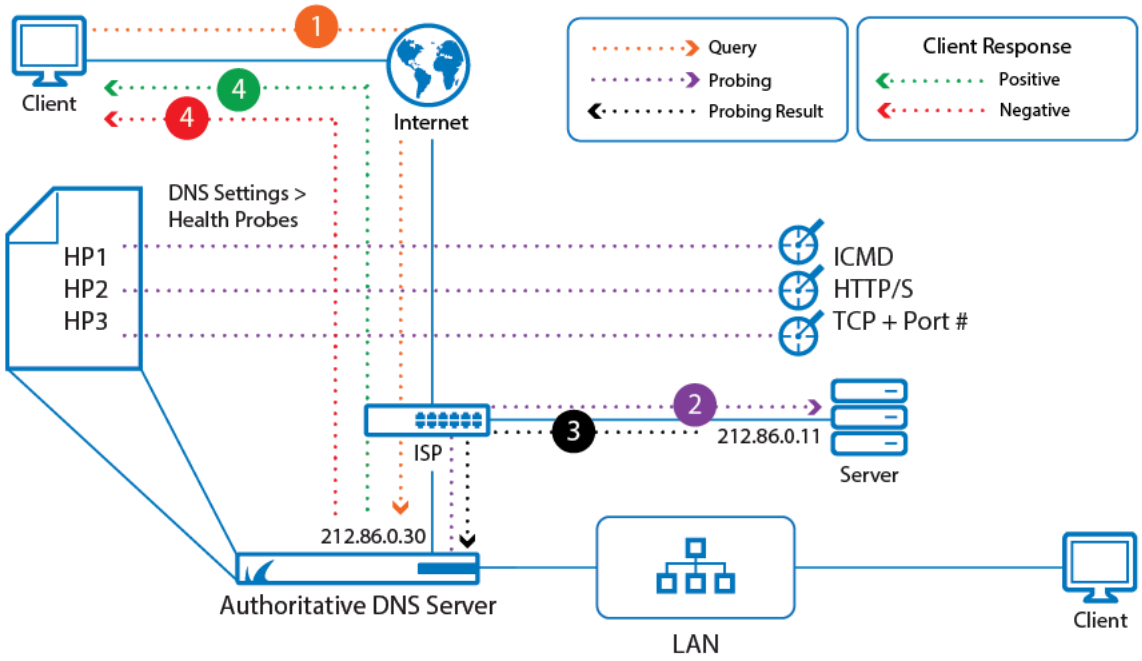
How to Configure a DNS Health Probe

https://campus.barracuda.com/doc/85493817/

Use a health probe to verify the availability of a certain target. When the target is available, the health probe returns a positive result. Depending on the result, a configured IP address can be returned for a DNS query if the probed target is available.

Health probes can be used only for A, AAAA, and MX records.

Although client queries are processed asynchronously from probing, the following image lays out the basic communication flow that lies between requesting and responding. For more information, see the paragraph "Probe Timing and Pattern" in the article DNS.



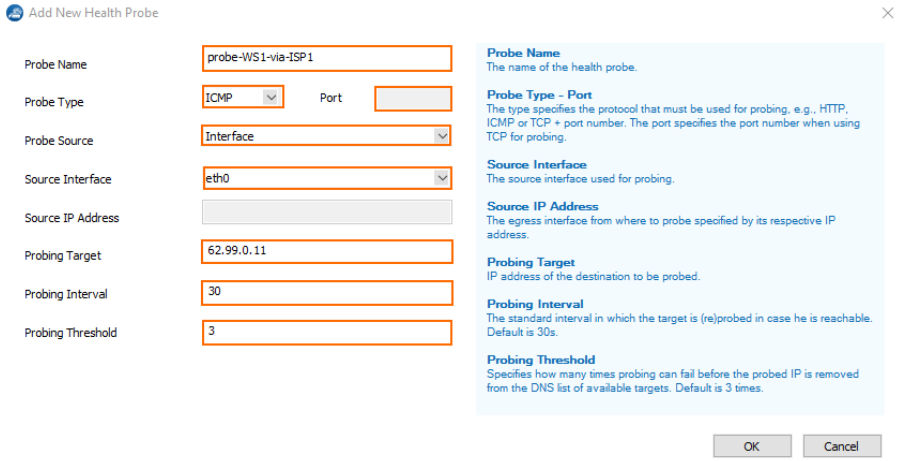
Before You Begin

- Verify that all service IP addresses are already configured that are necessary for answering DNS queries on the respective incoming interfaces. For more information, see How to Assign Services.

Configure a DNS Health Probe

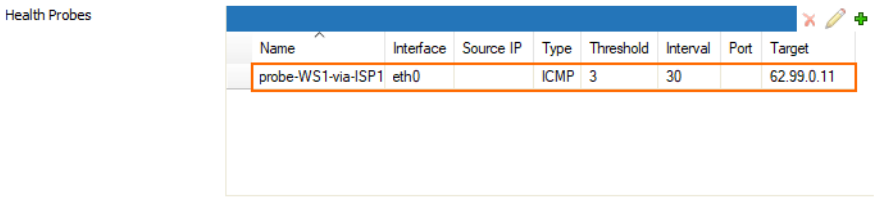
Create and attach a health probe to a certain interface / IP address on the firewall from where probing packets are sent to a certain target IP address.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > DNS > DNS-Service**.
2. In the left menu, click **DNS Settings**.
3. In the main window, select **Yes** for **ADNS Health Probing** if you want to activate it.
4. In the main window, click **+** to the right of the table of the section **Health Probes**.
5. The **Add New Health Probes** window is displayed.
6. For **Probe Name**, enter a name that clearly lets you identify the health probe, e.g., probe-WS1-via-ISP1.
7. For **Probe Type**, select the method how you want the target to be probed.
    1. **ICMP** – Select this option if your target must be probed using the ICMP protocol (`ping`).
    2. **(Alternatively) TCP** – Alternatively select TCP:
        1. **Probing Target** – Add the IP address for the probing target.
        2. **Port** – Add the port number.
    3. **HTTP/S** – Select this option if you want to probe a target that provides information on port 80/443, e.g. web server.
        1. **Probing Target** – Add a HTTP/S URL.
    4. **TCP + Port** – Select this option if none of the above options cover your requirements, and enter your individual values as needed.
8. **Probe Source** – Select the egress interface either via the **IP Address** or the **Interface** option.
    1. **Source Interface** – Select the egress interface on your firewall.
    2. **IP Address** – Select the egress interface by its related IP address.
9. **Probing Target** – Enter the IP address of the target host that must be probed for its availability.
10. **Probing Interval** – The standard interval in which the target is (re-)probed in case it is not reachable. The default value is 30 sec. Enter another value if required.
11. **Probing Threshold** – Specifies how many times probing can fail before the probed IP is removed from the DNS list of available targets. The default value is 3 times. Enter another value if required.



12. Click **OK**.
13. Click **Send Changes**.
14. Click **Activate**.

After sending the configuration, the health probe is displayed in the main window in the list.



The health probe can now be used in conjunction with IP addresses that will be part of a DNS response in case the probed target is available.

Figures

1. health_probes.png
2. add_new_health_probe_window.png
3. health_probe_added.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.