

---

## Allowing Barracuda Vulnerability Remediation Service IP Addresses

<https://campus.barracuda.com/doc/53676695/>

If you have any protection elements on your network, like a firewall, they might block the Barracuda Vulnerability Remediation Service by mistake because they think it is creating malicious traffic.

Before running any scans, Barracuda Networks recommends that you add the IP addresses that the Barracuda Vulnerability Remediation Service uses to your allow list.

Note: If you are using a Barracuda Web Application Firewall, this step is performed automatically by default. See the WAF Bypass section of [Actions on Existing Scans and Web Applications](#) for more information.

### How to Allow Barracuda Vulnerability Remediation Service IP Addresses

---

Consult the technical documentation associated with your protection element for instructions on allowing an IP address.

Allow the following IP addresses:

- 18.205.55.118
- 18.235.72.149
- 54.156.74.187
- 54.158.232.245
- 64.235.151.153
- 64.235.153.133
- 64.235.153.134
- 64.235.153.135
- 64.235.153.136
- 64.235.153.34
- 3.210.84.75

### Why Allow Barracuda Vulnerability Remediation Service IP Addresses

---

A network protection element, like a firewall, web application firewall (WAF), or intrusion detection/prevention system (IDS/IPS), typically cannot distinguish between an actual malicious user and a non-malicious scan, since the two look alike. Based on this potential confusion, a protection element on your network might block Barracuda Vulnerability Remediation Service by mistake,

prohibiting it from accessing your web application.

Most protection elements have rules that block IP addresses based on rate limit violations (e.g., protecting against denial of service and brute force attacks). During a scan, these protection rules are likely to trigger, causing the protection element to entirely block the Barracuda Vulnerability Remediation Service. When blocked, the Barracuda Vulnerability Remediation Service cannot access your application, typically causing the scan abort with an error.

Some protection elements might also block IP addresses after a set number of failures (known as “fail2ban”). This also causes the scan to abort with an error.

Allowing IP addresses is not specific to the Barracuda Vulnerability Remediation Service; all web application vulnerability scanners require the same procedure. In fact, to be compliant with the PCI Security Standard, you *must* allow these IP addresses when running your scan. The following is a quote from the [PCI Security Scanning Procedures document](#) , where ASV is the Approved Security Vendor, in this case Barracuda Networks:

*13. Arrangements must be made to configure the intrusion detection system/intrusion prevention system (IDS/IPS) to accept the originating IP address of the ASV. If this is not possible, the scan should be originated in a location that prevents IDS/IPS interference*

Not allowing IP addresses might cause your protection element to generate false logs and/or alerts, which can be a nuisance and add extra work to the administration team. Allowing the IP addresses of the Barracuda Vulnerability Remediation Service will ensure that your protection elements will not generate logs due to scans.

© Barracuda Networks Inc., 2021 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.