Allowing Barracuda Vulnerability Manager IP Addresses

https://campus.barracuda.com/doc/46893256/

If you have any protection elements on your network, like a firewall, they might mistakenly block Barracuda Vulnerability Manager, thinking it is creating malicious traffic.

Before running any scans, Barracuda Networks recommends that you add the IP addresses used by Barracuda Vulnerability Manager to your allow list, or whitelist.

How to Allow Barracuda Vulnerability Manager IP Addresses

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

Allow the following IP addresses:

- 18.235.72.149
- 54.158.232.245
- 18.205.55.118
- 54.156.74.187
- 3.210.84.75

Why Allow Barracuda Vulnerability Manager 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 Manager 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 Barracuda Vulnerability Manager. When blocked, Barracuda Vulnerability Manager cannot access your application, typically causing the scan abort with an error.

Some protection elements may 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 Barracuda Vulnerability Manager; all web application vulnerability scanners require the same procedure. In fact, to be compliant with the PCI Security Standard, you *must* allow IP addresses. 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. This can be a nuisance and add extra work to the administration team. Allowing the IP addresses of Barracuda Vulnerability Manager will ensure that your protection elements will not generate logs due to scans.