False Positive Report: TCP Source Port Pass Firewall (CVSS Base Score 5.0)

Category: Firewall
CVE: Not Applicable
Host: 172.67.214.135
Threat: TCP Source Port Pass Firewall
Impact: Medium (CVSS Base Score: 5.0)
Port: Destination port 24567, Source port 53
Result: The host responded to 4 TCP SYN probes sent to destination port 24567 using source port 53. However, it did not respond to 4 TCP SYN probes sent to the same destination port using a random source port.
Severity: Medium (CVSS Temporal Score: 3.6)
Host OS: Not provided
PCI Compliance Status: Non-compliant

Details and Analysis:

We have carefully reviewed the findings from the recent PCI scan related to IP `172.67.214.135`, and we confirm that this issue is a **false positive**. The following details provide clarification and justification for this conclusion:

1. **Cloudflare Infrastructure:** The IP address `172.67.214.135` does not belong to our server or internal network. This IP is part of the Cloudflare infrastructure, which we use as a CDN and DDoS protection service. Cloudflare routes all incoming traffic to our server through

their network, using a variety of dynamic IP addresses, including the one flagged in this report. As a result, the activity observed from this IP is a result of Cloudflare’s legitimate traffic routing, not any misconfiguration on our part.

2. **Port 53 Security:** Our internal network and firewall are properly configured, and **port 53** (DNS) is securely locked down. We have strict firewall rules in place to prevent unauthorized access or exploitation of port 53. In this case, the reported probes that used source port 53 are not reaching our server directly; instead, they are a result of Cloudflare's proxy traffic, which can explain why responses were detected from this IP.

3. **TCP SYN Probes (Port 24567):** The scan results indicate that the host responded to TCP SYN probes using **source port 53** but not to probes from a random source port. This behavior is consistent with the way Cloudflare's network operates, as it uses various mechanisms to handle traffic differently based on the source. Our firewall rules are configured to handle incoming traffic appropriately, but Cloudflare's proxy could affect how certain probes are handled, creating the appearance of a potential vulnerability.

4. **Firewall Configuration Review:** After conducting an internal review, we have reconfirmed that all our filtering rules are correctly configured and in line with PCI DSS standards. Specifically, our firewall is set to block any unauthorized TCP SYN connections, regardless of the source port. This configuration ensures that our network remains secure and protected from any potential threats.

5. **No Internal Exposure:** Importantly, no internal resources or systems are exposed due to this scan result. The flagged IP is part of Cloudflare's secure network, which is designed to protect and enhance the performance of our website. Additionally, our own network monitoring and security tools have not detected any anomalies or breaches related to this issue.

Conclusion:

Given that the flagged IP address is part of the Cloudflare network and not directly related to our internal infrastructure, and considering the secure configuration of our firewall (including port 53), we kindly request that this finding be marked as a **false positive**. Our network remains fully compliant with all PCI DSS requirements, and there are no vulnerabilities related to this report.

We appreciate your understanding and request that this false positive be cleared from the PCI scan results.

DevOps Team