Engaging Networks - ASV Scanning and Static IP Addresses

1. Purpose of This Document

This document is provided to our Approved Scanning Vendor (ASV) in response to requests for static IP addresses or a fixed IP-to-hostname mapping to configure the quarterly PCI DSS external vulnerability scan.

The organization uses Cloudflare as a reverse proxy and content delivery network (CDN) in front of all externally accessible web infrastructure. Because of this architecture, the public IP addresses that resolve for our domain names are owned and operated by Cloudflare, Inc., and are not static, not under our control, and not representative of the origin servers that actually process, store, or transmit cardholder data.

This document explains the technical basis for that constraint, identifies the correct scan targets per PCI DSS ASV Program Guide requirements, and proposes the compliant scanning approach we request the ASV use for this engagement.

2. Network Architecture Overview

The following describes our externally facing infrastructure topology as it relates to ASV scanning scope:

```
Internet Client  -->  DNS Resolution  -->  Cloudflare Anycast IP (Edge PoP)
                                                        |
                                          Cloudflare Proxy Layer (WAF, DDoS, CDN)
                                                        |
                                          Origin Server  (CDE — actual scan target)
```

Key architectural facts relevant to ASV scanning:

- DNS A records for all public-facing hostnames resolve to Cloudflare Anycast IP addresses — not to origin server IPs.
- Cloudflare Anycast IPs are shared global infrastructure. A single IP may serve traffic for thousands of unrelated customers worldwide.

- Cloudflare routes traffic from its edge to our origin server over an encrypted tunnel (Cloudflare Tunnel / Argo) or over a private network path. The origin server IP is not exposed in DNS.
- The origin server IP address changes are outside our control for the DNS-published addresses, as Cloudflare rotates and manages its Anycast pool dynamically.
- The origin server (where cardholder data is processed) has a stable private or cloud-provider IP, which we are able to provide separately under appropriate confidentiality controls.

> **IMPORTANT: Scanning** the Cloudflare proxy IP does NOT satisfy PCI DSS Requirement 11.3.2. The Cloudflare edge is a third-party intermediary, not a component of our Cardholder Data Environment. Vulnerabilities on Cloudflare infrastructure are Cloudflare's responsibility, not the merchant/service provider's. Only the origin server and any directly reachable in-scope components constitute the CDE for scan purposes.

3. PCI DSS Requirement & ASV Program Guide Basis

The following PCI DSS v4.0 requirements and ASV Program Guide provisions govern this situation and support the scanning approach described in Section 5:

Reference	Provision & Relevance
PCI DSS v4.0 Req. 11.3.2	Requires quarterly external vulnerability scanning by an ASV of all externally accessible in-scope system components. 'System components' means components that store, process, or transmit CHD, or that could impact the security of the CDE — i.e., the origin servers, not a CDN proxy.
ASV Program Guide v3.1 Section 4.4	Specifically, the scan customer must identify all in-scope IP addresses and provide an accurate scope. The customer must document and attest that the scan covers all applicable components.
ASV Program Guide v3.1 Section 4.4 (Load Balancer Provision)	States that when load balancers or similar technologies prevent scanning of all in-scope IPs, the scan customer must provide written assurance that all back-end systems are equivalent. This provision applies equally to reverse proxies such as Cloudflare.
ASV Program Guide v3.1 Section 6.3	Defines Special Consideration: Hosted Services. When a third-party provides hosting, the ASV must scan the IP addresses that serve the in-scope system. Cloudflare's shared IPs serve thousands of customers and are not in scope.
PCI DSS v4.0 Req. 12.8 / 12.9	Third-party service providers (TPSPs) such as Cloudflare manage their own PCI compliance for the services they provide. Cloudflare maintains a current PCI DSS Attestation of Compliance (AoC). The merchant's scan obligation covers their own infrastructure only.
Cloudflare PCI AoC	Cloudflare, Inc. is a certified PCI DSS Level 1 Service Provider. Their AoC is available at https://www.cloudflare.com/trust-hub/compliance-resources/ and covers the Cloudflare proxy infrastructure that sits in front of our origin.

4. Technical Reasons Static IP Addresses Cannot Be Provided

The following technical constraints prevent us from providing static, stable IP addresses that map to our publicly accessible domain names:

4.1 Cloudflare Anycast Routing

Cloudflare uses Anycast routing to distribute traffic across its global network of over 300 Points of Presence (PoPs). When a DNS query is made for our domain, the returned IP address reflects the nearest Cloudflare PoP to the requester's location, not a fixed IP address. The same hostname may resolve to different IPs depending on the source geography of the query, and these IPs change over time as Cloudflare rebalances its network.

4.2 Shared Infrastructure

Cloudflare's Anycast IPs are shared across all Cloudflare customers. Providing our 'Cloudflare IP address' to the ASV would result in scanning shared infrastructure that is not part of our CDE and that also serves traffic for thousands of other organizations. This creates both a scope inaccuracy and a potential compliance issue.

4.3 Origin IP Is Not Published in DNS

Our origin server IP address is intentionally not published in public DNS records. Exposing the origin IP would allow attackers to bypass Cloudflare's WAF, DDoS protection, and rate limiting to attack the origin server directly. Maintaining origin IP confidentiality is a deliberate and necessary security control. We can provide the origin IP directly to the ASV through a secure, out-of-band channel as documented in Section 5.

4.4 Cloudflare Orange-Cloud Proxy Status

All in-scope hostnames are configured with Cloudflare's proxy enabled (orange-cloud status). DNS lookups for these names return Cloudflare edge IPs. The following table shows what DNS returns versus what the actual in-scope target is:

Hostname	DNS-Resolved IP (What ASV Sees)
[yourdomain.com]	Cloudflare Anycast IP (e.g., 104.21.x.x)
[api.yourdomain.com]	Cloudflare Anycast IP (e.g., 172.67.x.x)
[checkout.yourdomain.com]	Cloudflare Anycast IP (e.g., 104.21.x.x)

> **NOTE: Actual** origin IP addresses will be provided to the ASV via encrypted email or the ASV's secure portal. They are withheld from this document as it may be stored or transmitted outside secure channels.

5. Handling Scan Findings Attributable to Cloudflare Infrastructure

If the ASV scans the publicly resolved DNS IPs (Cloudflare Anycast addresses) and returns findings, the following guidance applies to determining whether findings are disputable as false positives:

Finding Type	Basis for Dispute / Resolution
Open non-standard ports (e.g., 2052, 2082, 8080, 8443)	Cloudflare opens non-standard ports on its edge IPs as documented at developers.cloudflare.com/fundamentals/get-started/reference/network-ports. These ports do not pass traffic to our origin and are not part of our CDE. Dispute as false positive with reference to Cloudflare's published port documentation.
TCP source port pass firewall	This finding is generated by Cloudflare's edge infrastructure, not by our origin server. Cloudflare's edge IP is a shared platform, not a component of our CDE. Dispute citing Cloudflare AoC.
SSL/TLS weak cipher or protocol (TLS 1.0/1.1)	If found on Cloudflare edge IPs, confirm whether Cloudflare's minimum TLS version setting is set to 1.2+ in SSL/TLS settings. If Cloudflare is configured correctly, dispute as Cloudflare infrastructure finding. Remediate in Cloudflare SSL/TLS settings if needed.
SSL certificate mismatch or wildcard cert	Cloudflare issues its own edge certificates. These are valid, CA-signed certificates managed by Cloudflare. They are not misconfigurations of our infrastructure.
Scan blocked / no response / challenge page	Cloudflare WAF or DDoS protection challenged scanner traffic. This is not a vulnerability. Whitelist scanner IPs and rescan, or target origin directly.
Cloudflare-specific HTTP response headers	Headers such as cf-ray, cf-cache-status, server: cloudflare are Cloudflare infrastructure headers. They are not vulnerabilities and indicate the scan reached Cloudflare's edge, not the origin.

Appendix A: Reference Documents

Document	Location / Reference
PCI DSS v4.0	https://www.pcisecuritystandards.org/document_library/
ASV Program Guide v3.1	https://www.pcisecuritystandards.org/document_library/
Cloudflare PCI DSS AoC	https://www.cloudflare.com/trust-hub/compliance-resources/
Cloudflare IP Ranges (Anycast)	https://www.cloudflare.com/ips/
Cloudflare Network Ports	https://developers.cloudflare.com/fundamentals/get-started/reference/network-ports/
Cloudflare AS13335 WHOIS	https://bgp.he.net/AS13335 — confirms Cloudflare IP ownership for any disputed finding