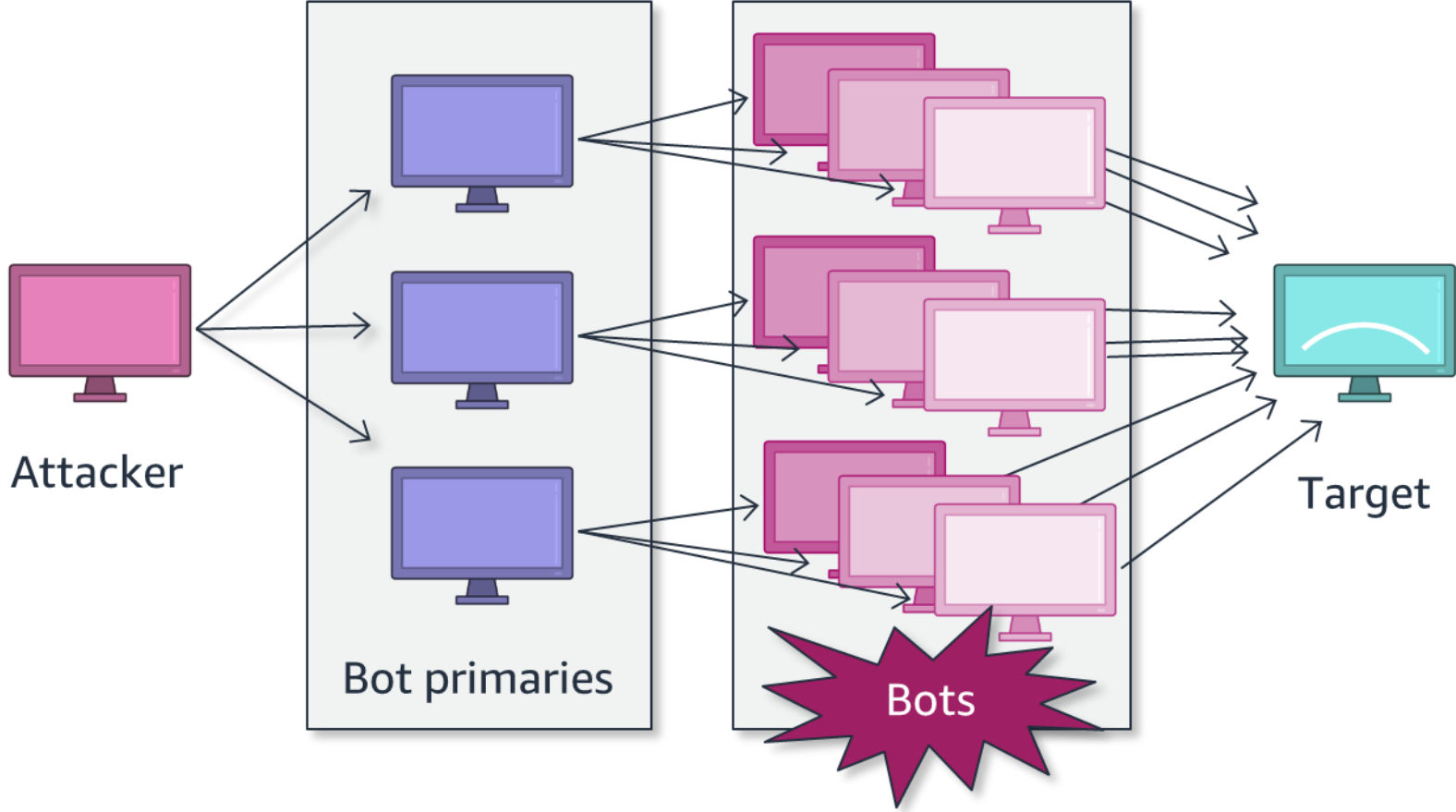![aws]

WAF protection

"How can we protect public-facing applications?"
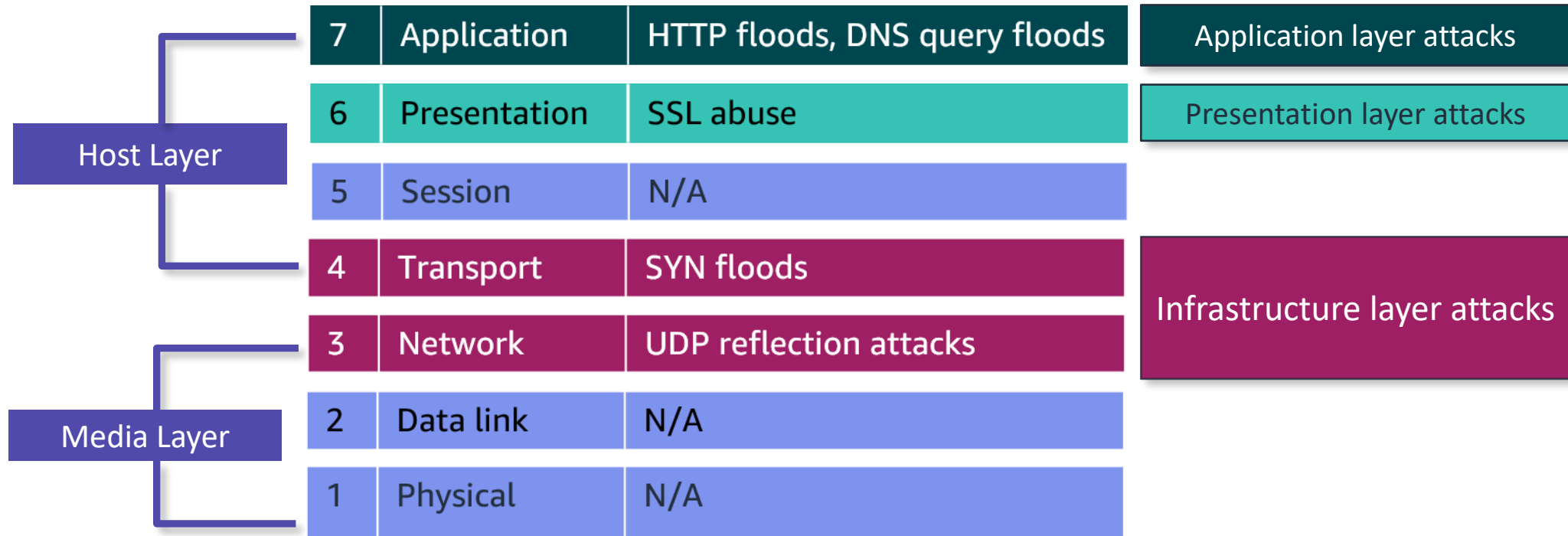
DDoS attacks

Each of the compromised hosts participates in the attack, generating a flood of requests to overwhelm the intended target.

Attacker

Bot primaries

Bots

Target

OSI layer attacks

DDoS attacks can be categorized by the
Open Systems Interconnection (OSI) layer they attack.

7	Application	HTTP floods, DNS query floods	Application layer attacks
6	Presentation	SSL abuse	Presentation layer attacks
5	Session	N/A	
4	Transport	SYN floods	
3	Network	UDP reflection attacks	Infrastructure layer attacks
2	Data link	N/A	
1	Physical	N/A	

Host Layer — layers 7, 6, 5, 4

Media Layer — layers 3, 2, 1

AWS Shield

Managed DDoS protection service that protects your applications on AWS

Two types of protection:

- AWS Shield Standard
- AWS Shield Advanced

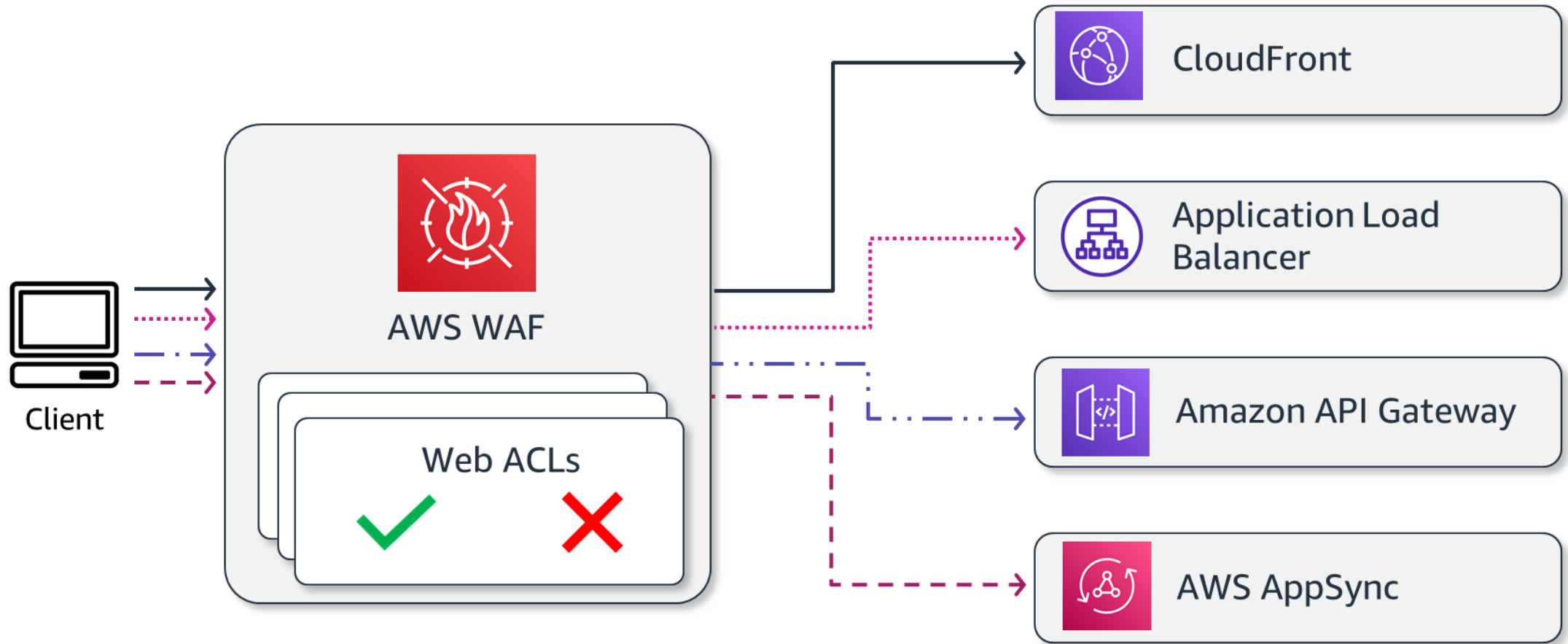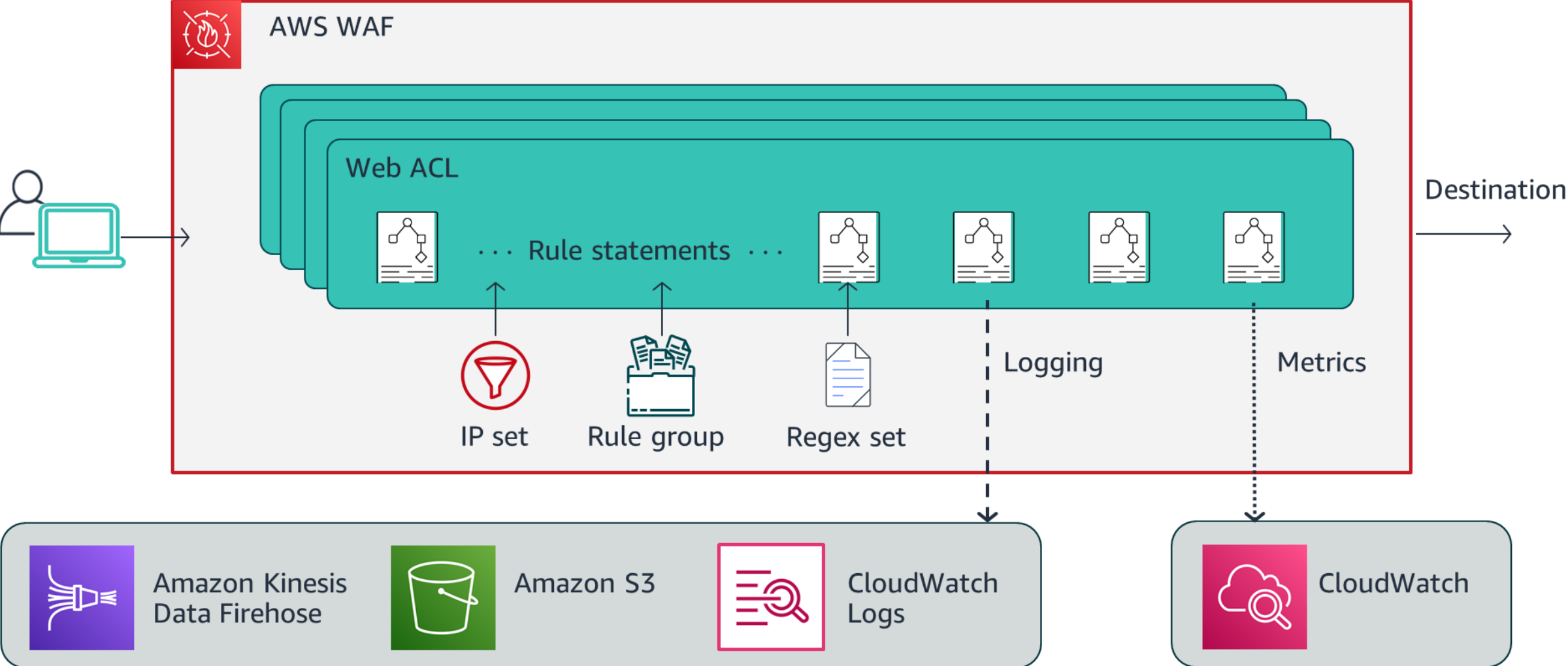| 7	Application	HTTP floods, DNS query floods
6	Presentation	SSL abuse
5	Session	N/A
4	Transport	SYN floods
3	Network	UDP reflection attacks
2	Data link	N/A
1	Physical	N/A

Shield Advanced

Shield Standard

AWS WAF

Components of access control

Control traffic with ACL rule statements

Attack prevention

- SQL injection and cross-site scripting detection
- AWS Managed Rules for AWS WAF
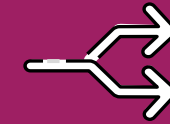- AWS Marketplace managed rule groups

Traffic filtering

- Rate limiting
- IP filtering with full Classless Inter-Domain Routing (CIDR) range support
- Geo-fencing by country

Pattern matching

- Regex match
- String match
- Size constraint match

Logical operation

- AND statement
- OR statement
- NOT statement

DDoS-resilient reference architecture