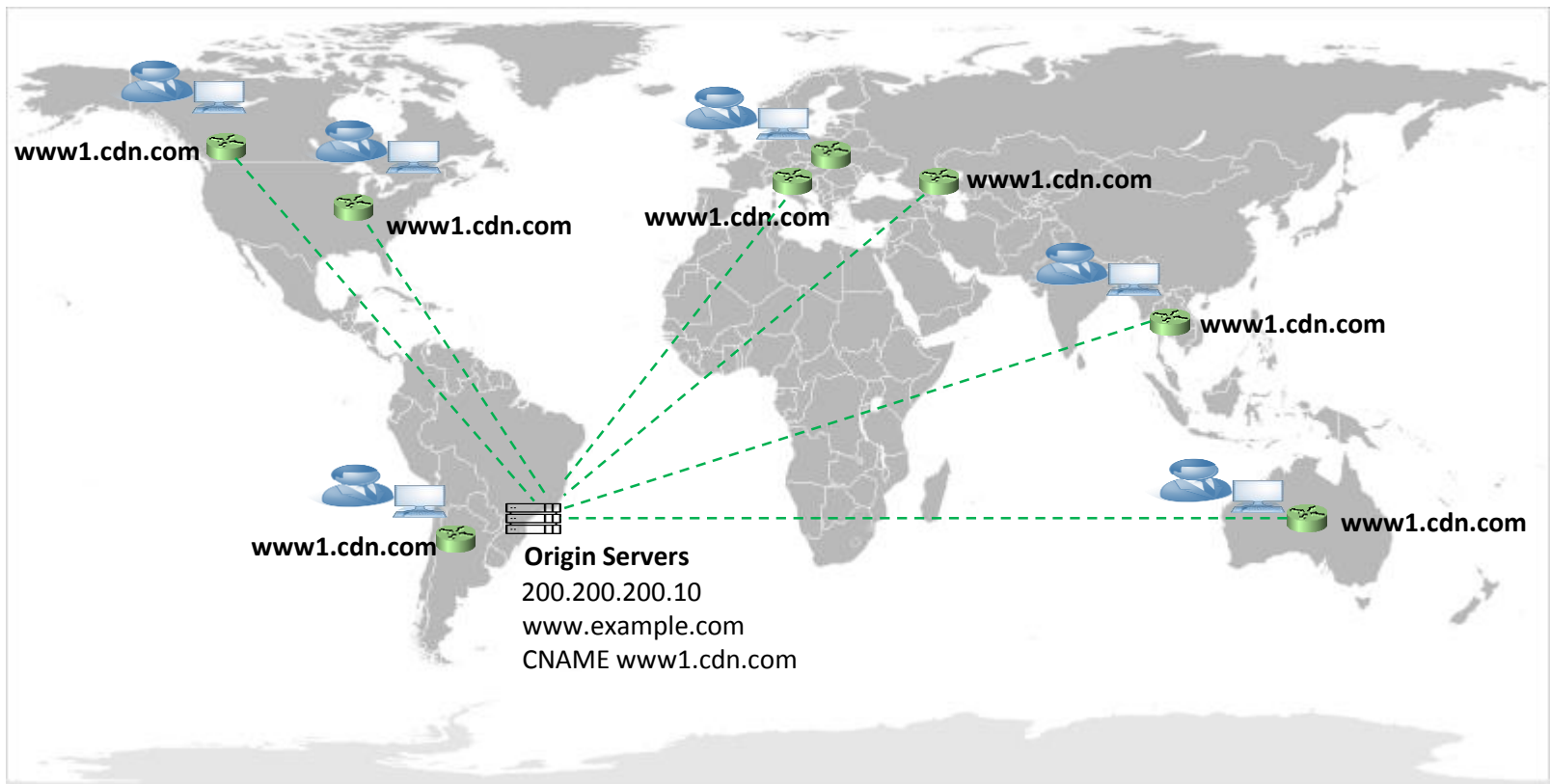


Best Practices for Using CDNs Against DDoS Attacks

Wilson Rogério Lopes
LACNIC 28 / LACNOG 2017
09/2017

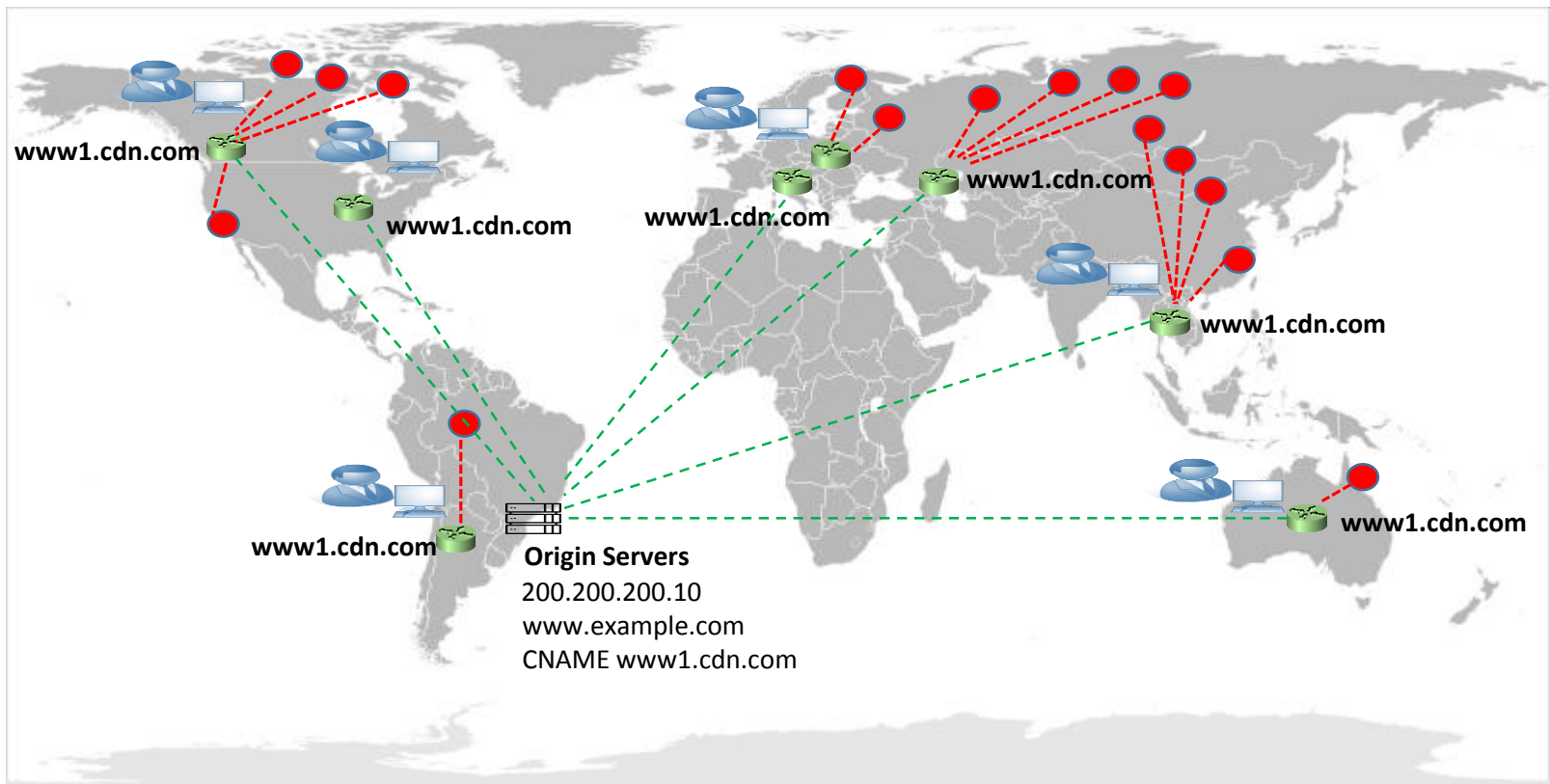
CDNs for DDoS Protection

- As your principle, CDNs distribute traffic around the world to the closest pop for client, using anycast
- Excellent approach to cache content, reduce time-to-access and load of “origin” servers



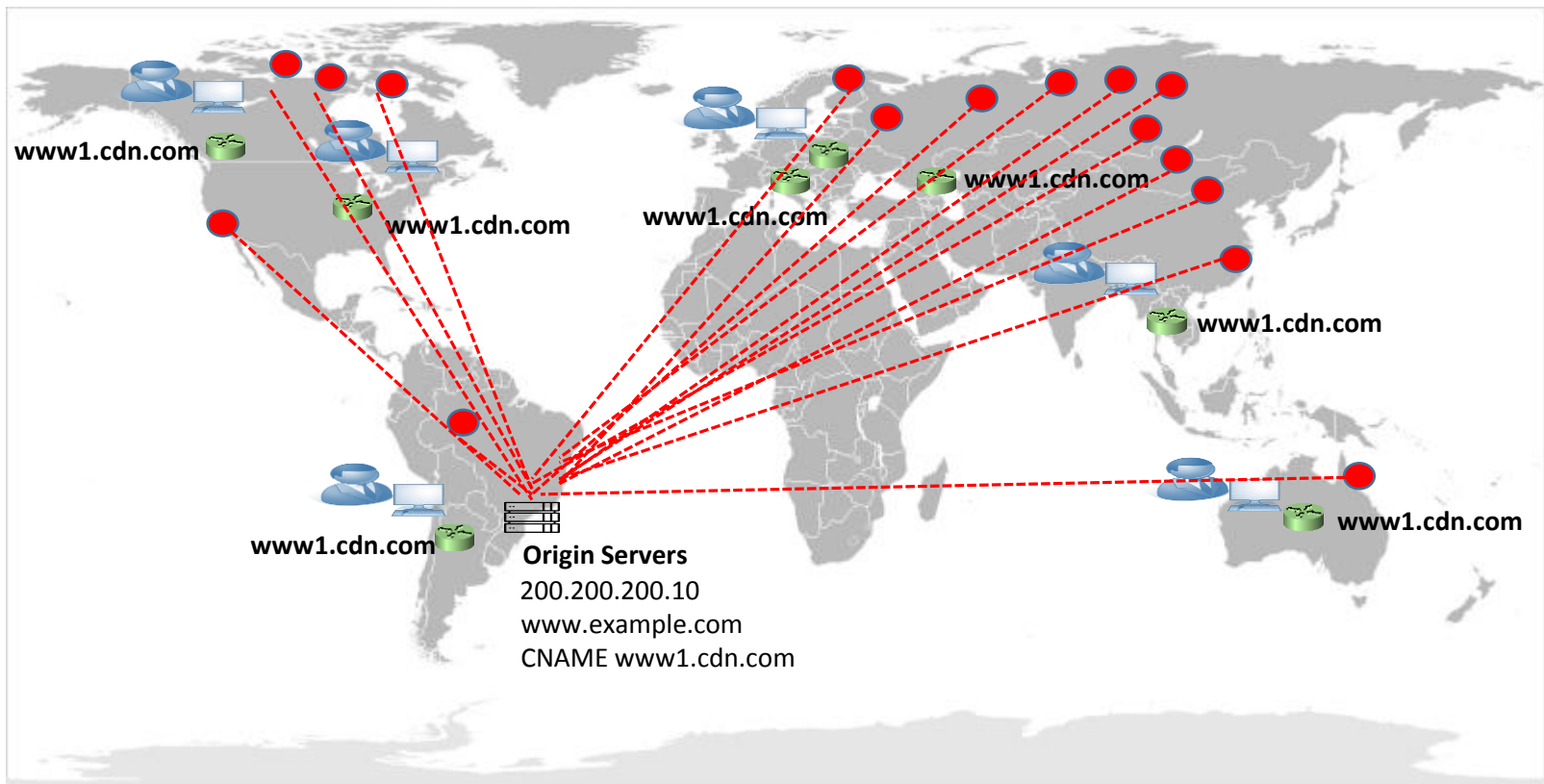
CDNs for DDoS Protection

- By distributing the traffic, it's reduce the power of a DDoS attack
- Even in an attack of hundreds of Gbps, a small amount will reach each pop



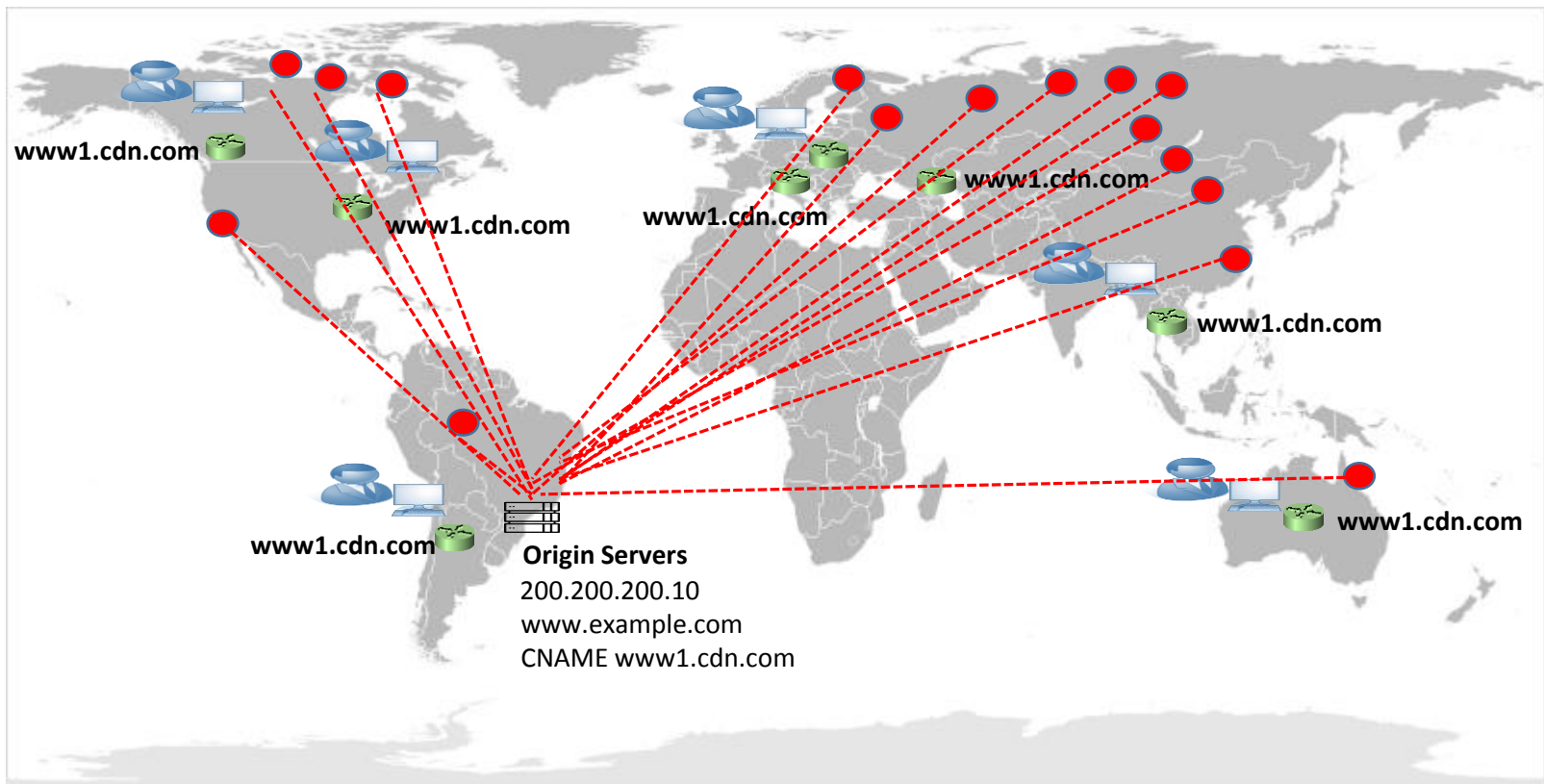
CDNs for DDoS Protection

- But, if the origin ip is the target?



CDNs for DDoS Protection

- But, if the origin ip is the target?
- It's impossible, nobody knows the origin ip, since the dns record pointing to cdn servers ☺



Discovering the “origin ip”

- If the target is an Autonomous System
 - Whois will show the ip prefixes associated with ASN of victim
 - aut-num: AS65000
 - owner: Example S.A.
 - inetnum: 200.200.200.0/24
 - Attacker can send requests to all ips of prefix to check for the same response of cdn servers

```
$curl http://www1.cdn.com  
<html>  
  
    Some content.....  
  
</html>
```

```
$for i in `seq 1 254`; do curl 200.200.200.$i; done  
<html>  
  
    Same content of cdn response.....  
  
</html>
```

- Or simply send volumetric attack to any ip in the prefix to saturate the bandwidth of origin network !

Discovering the “origin ip”

- Using related hosts
 - `www.example.com CNAME www1.cdn.com` ✓
 - `static.example.com A 200.200.200.100`
 - `webmail.example.com A 200.200.200.10`
 - `ns1.example.com A 200.200.200.20`

Guess the victim are hosted at `200.200.200.x`

- As in the previous example, use `curl` to check the ips that answers are identical of cdn servers to have the origin ip

Discovering the “origin ip”

- **Outbound connections**

Im some situations, the origin server establish outbound connections, directly to destination

Example:

- Pages “Forgot my password” send email messages directly from application servers

The email header will show the origin ip

- **Server Leaking ip address**

- HTTP error messages (like 404), can reveal the server ip address

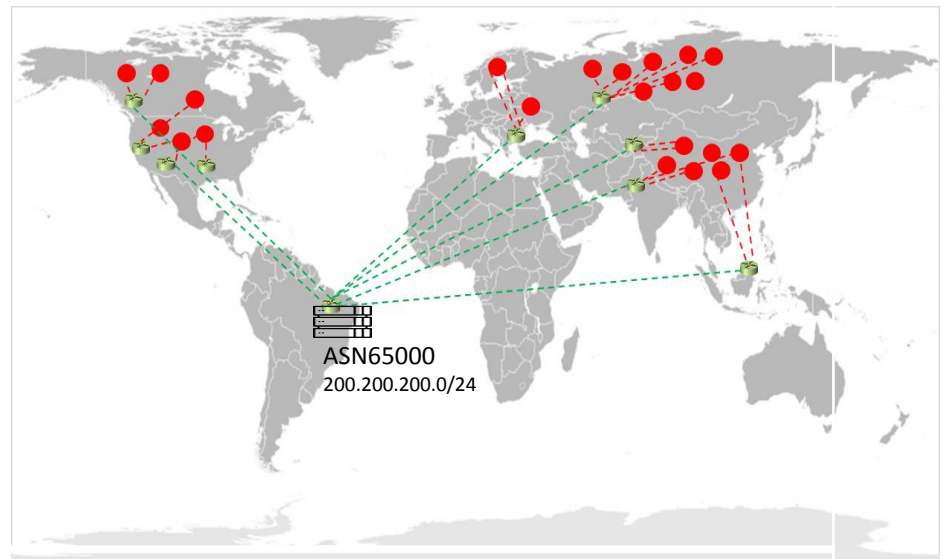
Best Practices


- If you are an Autonomous System:

Prefer to use BGP mitigation systems, to effective protection of entire network

- GRE tunnels between client and anti-DDoS provider
- BGP sessions under gre tunnels
- Provider announce the client prefixes and mitigate attacks
- Cleaned traffic delivered in gre tunnels

--- Attack Traffic
--- Cleaned Traffic via gre



 *Cleaning Centers*
Announce
200.200.200.0/24

--- GRE tunnel

Best Practices

- If you aren't an Autonomous System, and choose for CDN protection

It can be safer if you follow some checklist:

- Remove all DNS records pointing to the origin
- As possible, host the protected systems in a exclusive infrastructure
- Use DNS servers in the CDN also
- Check all applications for outbound connections
- Check error messages for ip leakages
- Ask you service provider to put ACLs in the edge to protect your ips – generally not acceptable, complex maintenance
- Change the origin ip always that it was leaked
- Hide and seek

References

- **DDoS Protection Bypass Techniques - Allison Nixon and Christopher Camejo**
<https://media.blackhat.com/us-13/US-13-Nixon-Denying-Service-to-DDOS-Protection-Services-WP.pdf>
<https://www.youtube.com/watch?v=bmzHIB18XT8>
- **DDoS Attacks - Overview, Mitigation and Evolution – Wilson Lopes**
<https://www.dropbox.com/s/odd4k3mdfi8ntxi/22%20-%20Wilson%20Rogerio%20Lopes%20%20Ataques%20DDoS%20-%20Panorama%2C%20Mitiga%C3%A7%C3%A3o%20e%20Evolu%C3%A7%C3%A3o%20-%20LACNOG.pdf?dl=0>