



Mitigating DNS attacks and protocol abuse

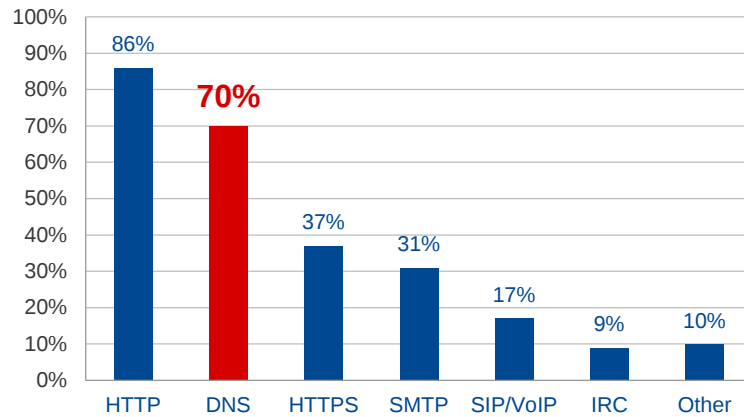
Nigel Ashworth

Solution Architect EMEA



Denial of Service Attacks Against DNS

APPLICATION LAYER ATTACKS



DNS is now the second most targeted protocol after HTTP.

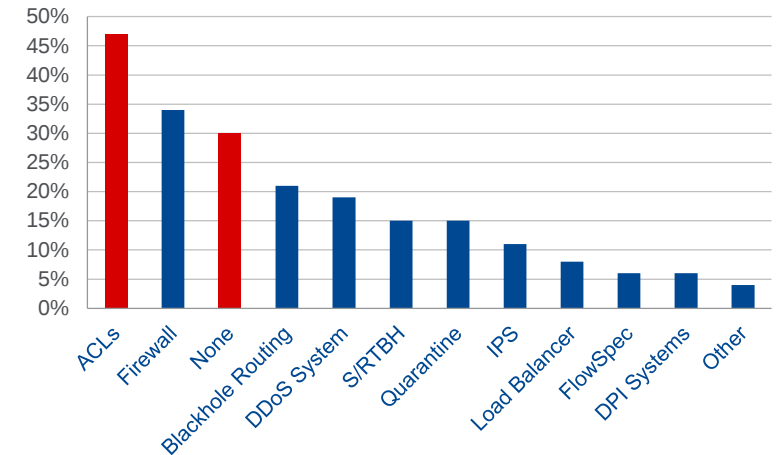
DNS DoS techniques range from:

- Flooding requests to a given host
- Reflection attacks against DNS infrastructure
- Reflect / Amplification attacks
- DNS Cache Poisoning attempts

“Cybercrime is a persistent threat in today’s world and, despite best efforts, no business is immune.”

Network Solutions

TRADITIONAL DDOS MITIGATION



Of the **customers that mitigate DDoS attacks**, many choose a **technique that inhibits the ability of DNS** to do its job

- DNS is based on UDP
- DNS DDoS often uses spoofed sources
- Using an ACL block legitimate clients
- DNS attacks use massive volumes of source addresses, breaking many firewalls.

DNS Attacks and Outages

AT&T hit by DDoS attack, suffers DNS outage

There are few details on the outage that appears to be hitting companies across the U.S.

By Martyn Williams | 15 August 12

A distributed denial-of-service attack aimed at AT&T's DNS (Domain Name System) servers has disrupted data traffic for some of the company's customers.

RELATED ARTICLES

[AT&T suffers DNS outage](#)

[Verizon Wireless outage outraging customers](#)

[VMware causes second outage while recovering from first](#)

[AT&T reports attempted customer data hack](#)

The multi-hour attack began Wednesday morning West Coast time and at the time of this writing, eight hours later, does not appear to have been mitigated.

"Due to a distributed denial of service attack attempting to flood our Domain Name System servers in two locations, some AT&T business customers are experiencing intermittent disruptions in service," an AT&T spokesman told IDG News Service by email. "Restoration efforts are underway and we apologize for any inconvenience to our customers."

The attack appears to have affected enterprise customers using AT&T's managed services DNS product.

Service Knocked Out In Southern Ontario, Atlantic Canada (TWITTER)

The Huffington Post Canada | Posted: 01/09/2013 9:48 pm EST | Updated: 01/10/2013 5:30 am EST



Lessons Learned in Historic DDoS Attack on Spamhaus

By Barry Levine
April 2, 2013 1:53PM



The DNS amplification vulnerability, which was exploited to the fullest in the attacks on Spamhaus, return incoming requests to a DNS server with as much as 100 times as much data. When the attackers have faked the source address for those incoming requests, the responses can overwhelm the victims' servers -- and possibly spill over and clog the Net.

GoDaddy Goes Down After Apparent DNS Server Outage

BY ROBERT MCMILLAN 09.10.12 4:21 PM

[Follow @bobmcmillan](#)



MAJOR DNS CACHE POISONING ISPS

by Dennis Fisher [Follow @dennissf](#)

There is a large-scale DNS cache-poisoning attack going on in Brazil at the moment, with potentially millions of users affected by a tactic that is forcing them to install a malicious Java applet before they can reach many popular sites, including Google, Gmail and Hotmail.

The attack has been going on for some time already, researchers say, and the effort could be quite widespread, given the scope of the problem. Several large ISPs in t

Comcast suffers DNS outage

Service provider says problem unrelated to recent spate of 'pharming' scams

By Paul Roberts

April 8, 2005 12:00 PM ET [Add a comment](#)

[Share](#) [Twitter](#) [StumbleUpon](#) [Reddit](#) [Email](#) [More](#)

IDG News Service - Problems with the Domain Name System (DNS) servers at Internet service provider Comcast Corp. prevented customers around the U.S. from surfing the Web yesterday, but the company said the interruptions

Comcast Suffers Major East Coast Outage DNS server related, no explanation given

by Karl Bode Monday 29-Nov-2010 tags: [business](#) · [cable](#) · [trouble](#) · [networking](#) · [consumers](#) · [Comcast](#)

As this [four page thread](#) in our Comcast forum documents, Comcast suffered a major network outage around Boston and a huge chunk of the east coast on Sunday. Judging from user posts, it appears to have been a DNS problem -- resolved by switching to an alternative DNS server (something to try if you're still having problems). Some users in our forums indicate the problem seems to be resolved for them, but Comcast's [official Twitter accounts](#) haven't been updated since last night -- when the company had no ETA or explanation for what caused the outage. It's unfortunate for Comcast, given they've been [beefing up DNS services](#) to try and keep users from switching to OpenDNS, and every outage of this kind is simply free advertising for the alternative DNS operator.



[Follow](#)

Charter DNS outage was resolved as of 10a CST. If you are still having Net issues, please try resetting your modem: charter.com/modemreset

[Reply](#) [Retweet](#) [Favorite](#) [More](#)

1 FAVORITE

10:42 AM - 21 Jul 12

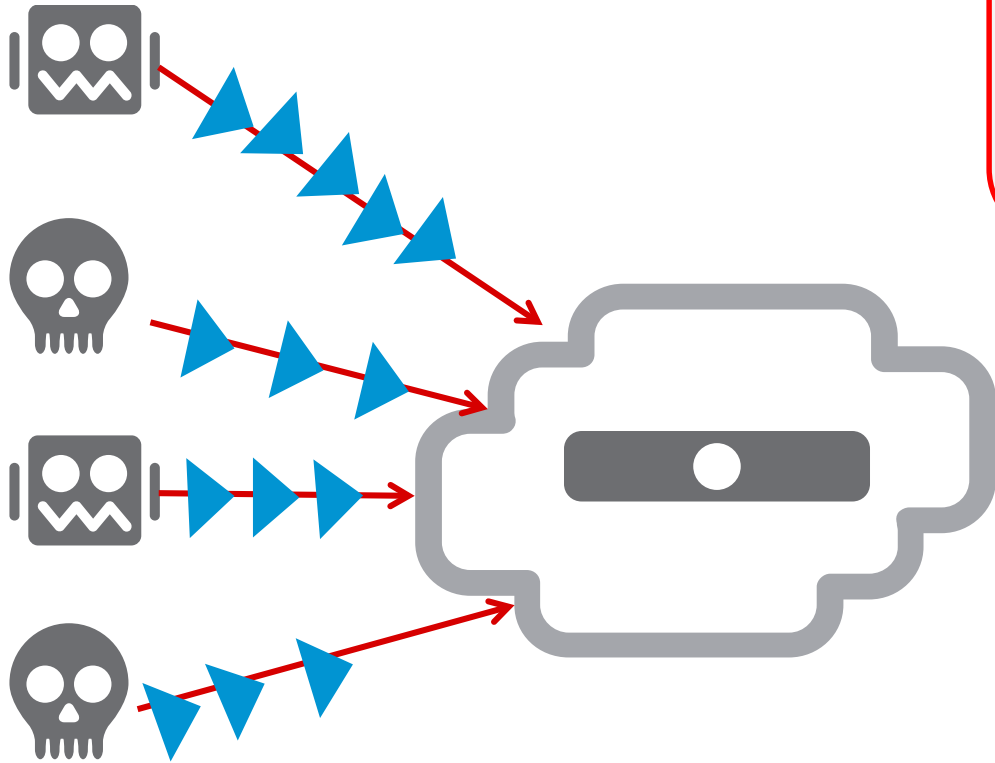
Attacks on DNS do not commonly target stealing £\$€¥ but impacts the availability of the businesses applications which makes the business less effective and hence loose £\$€¥ .

Today the applications are the life blood of the business do not put them at risk

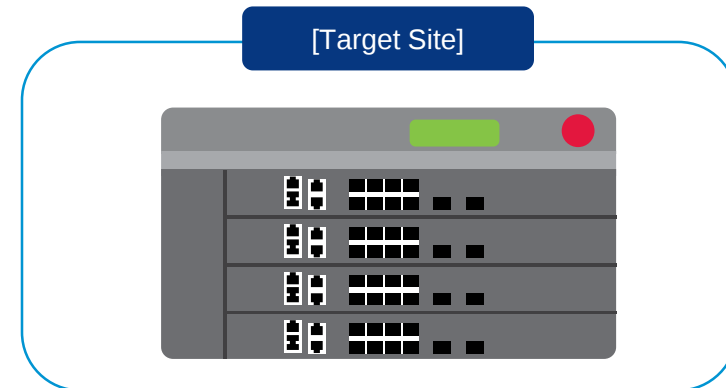
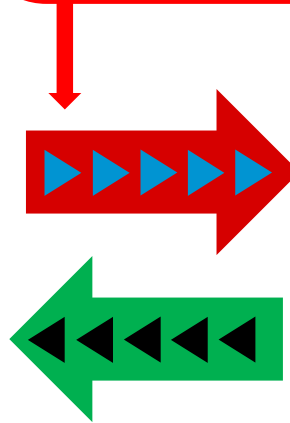
DNS Flood Attacks and Mitigation



DNS Flood



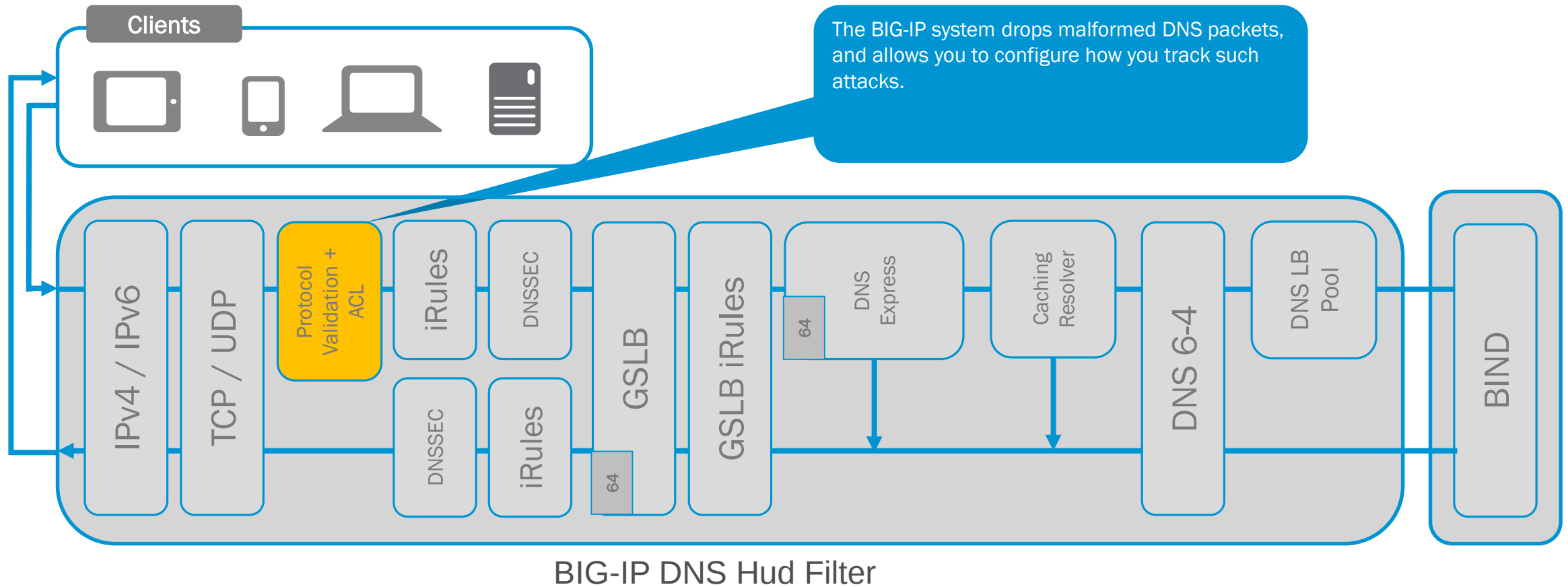
Many attackers or botnets flood an **authoritative** name server, attempting to exceed its capacity. Dropped responses = reduced or no site availability.



Capacity, over 2M RPS blade and to over 30M RPS per chassis. Identify unusually high traffic patterns to specific clients via DNS DoS Profiles.

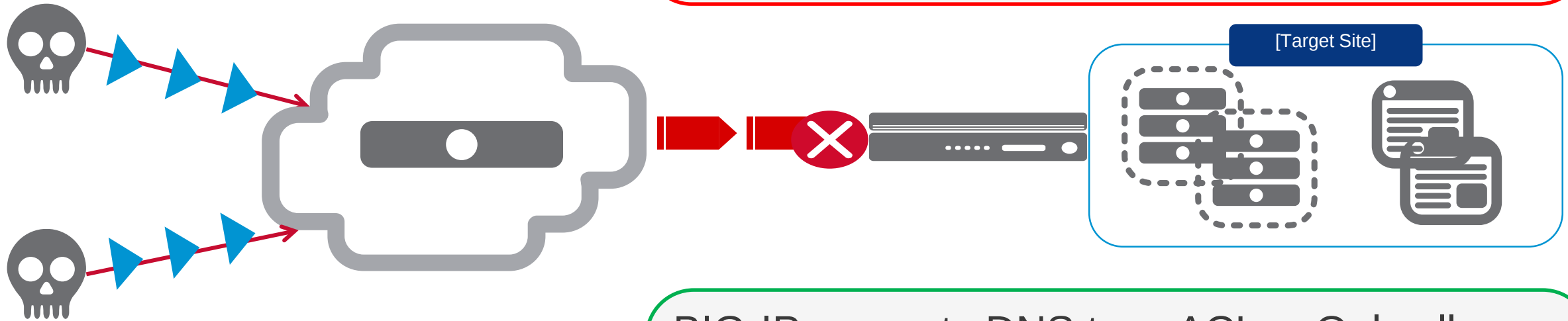
Malformed Packets

Malformed DNS packets can be used to consume processing power on the BIG-IP system, ultimately causing slowdowns like a DNS flood.



DNS Amplification Attack

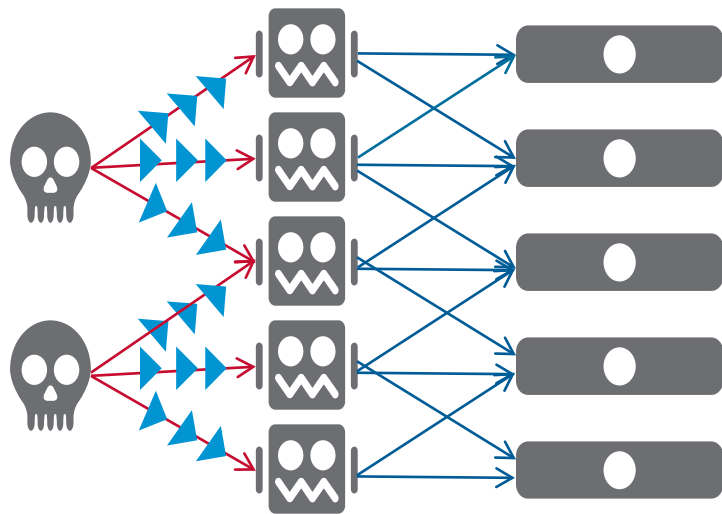
By spoofing a UDP source address, attackers can target a common source. By requesting for large record types (ANY, DNSSEC, etc), a 36 byte request can result in a response over 100 times larger.



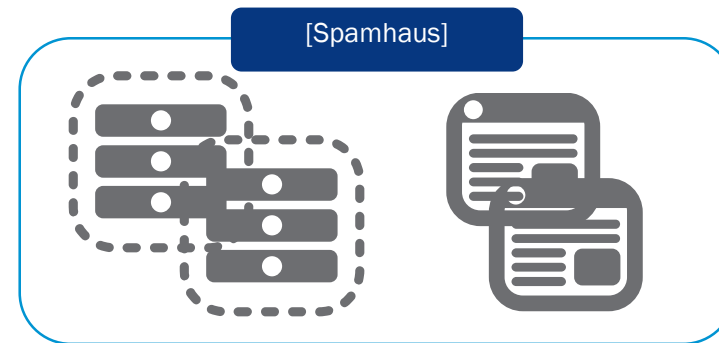
BIG-IP supports DNS type ACLs. Only allow DNS types you need to support. Drop all unsolicited responses (default behavior). Identify unusually high traffic patterns to specific clients via DNS DoS Profiles.

DNS Amplification Attack With Open Resolvers

1. The attackers send small DNS requests to about 1,000 computers under their control.
2. Each computer, pretending to be target site, sends requests for information to open resolvers.
3. The resolvers respond with a much larger message than the initial request, amplifying the size of the attack.

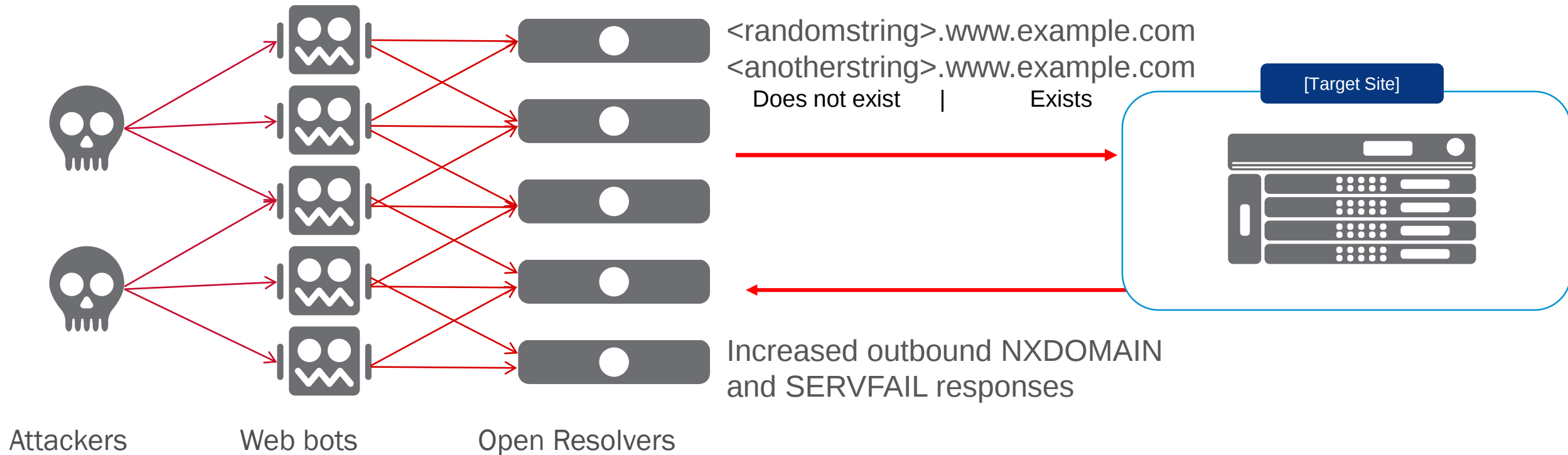


Attackers Web bots Open Resolvers



Target Site can not handle the amount of traffic and ceases to respond to legitimate traffic. The internet is interrupted for millions of people in Europe/

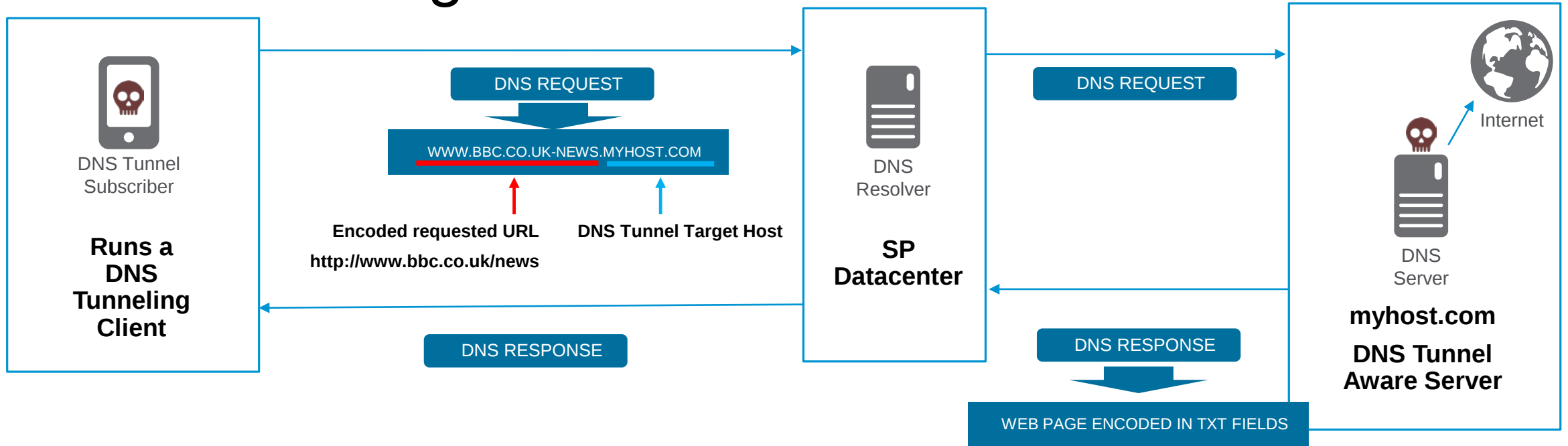
Random Sub-domain / NXDOMAIN



Protocol Abuse and Mitigation



DNS Tunneling

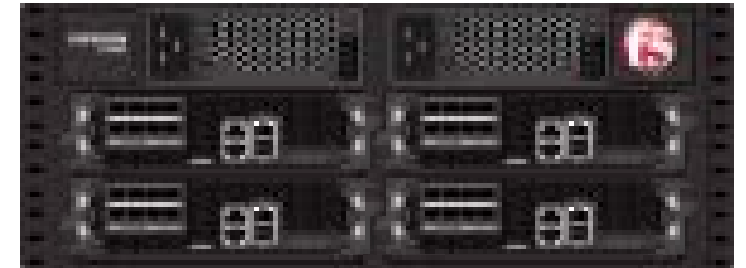


- Few organizations block DNS traffic
- Very effective for bypassing security measures
- Can transport any data by encoding it into DNS messages
- Wide support and availability of the global DNS infrastructure
- Can be used for nearly any two-way communication

Mitigation of protocol abuse and enforcement

iRule + iApp

- Client blacklisted?
- Above XXX RPS?
- Duplicate request?
- Name longer than XX?
- Response NXDOMAIN?
- Response larger than XXX?



VIPRION 2400 Chassis

<randomstring>.www.example.com
<anotherstring>.www.example.com
Does not exist | Exists

Mitigation of protocol abuse and enforcement

UK DNS Tunnel Mitigation Configuration template

Introduction	This template supports configuring limits and other parameters for UK DNS tunnel mitigation
About this Template	This template was created on 17-06-2015 by F5 Professional Services to facilitate the deployment of DNS Tunnel Mitigation iRule for UK
Prerequisites (Virtual Servers)	Before using this template to configure the BIG-IP system, please ensure that applicable Virtual Servers are already created
(About iRule)	The iApp will generate the iRule based on the input parameters and apply iRule to selected Virtual Servers
(Profiles)	Please ensure that appropriate profiles(UDP/TCP and DNS) have been applied to the relevant Virtual Servers
(SysLogPool)	Please ensure that SysLogPool has been created for remote High Speed Logging
(SP-Dag)	Please ensure that source based SP-Dag has been configured for external/client facing VLAN to reduce performance impact

Global Settings

Enable/Disable Request dropping for blacklisted clients:	Yes ▼
Configure the filtering/sampling time(in milliseconds):	1000
Configure the blacklisting/penalty period(in seconds):	10
Enable/Disable reverse DNAT translation for logging client IP:	Yes ▼
Configure Logging:	Remote Only ▼

Mitigation of protocol abuse and enforcement

DNS Request Enforcement Settings	
Configure global connection rate limit(cps) for the Virtual Server (pre-cache)	110000
Note::	The following limits are per filtering/sampling time configured above
Configure TCP Connections(pre-cache) Per Client Limit:	200
Configure Maximum allowed Query Length(in bytes):	80
Configure Longer Queries per Client Limit:	10
Configure Unusual Queries per Client Limit:	20
Configure Resolutions per Client Limit:	100

DNS Response Enforcement Settings	
Note::	The limits are per filtering/sampling time configured above
Configure Maximum allowed Response Length(in bytes):	200
Configure Longer Responses per Client Limit:	20
Configure NXDOMAIN and SERVFAIL responses per Client Limit:	20

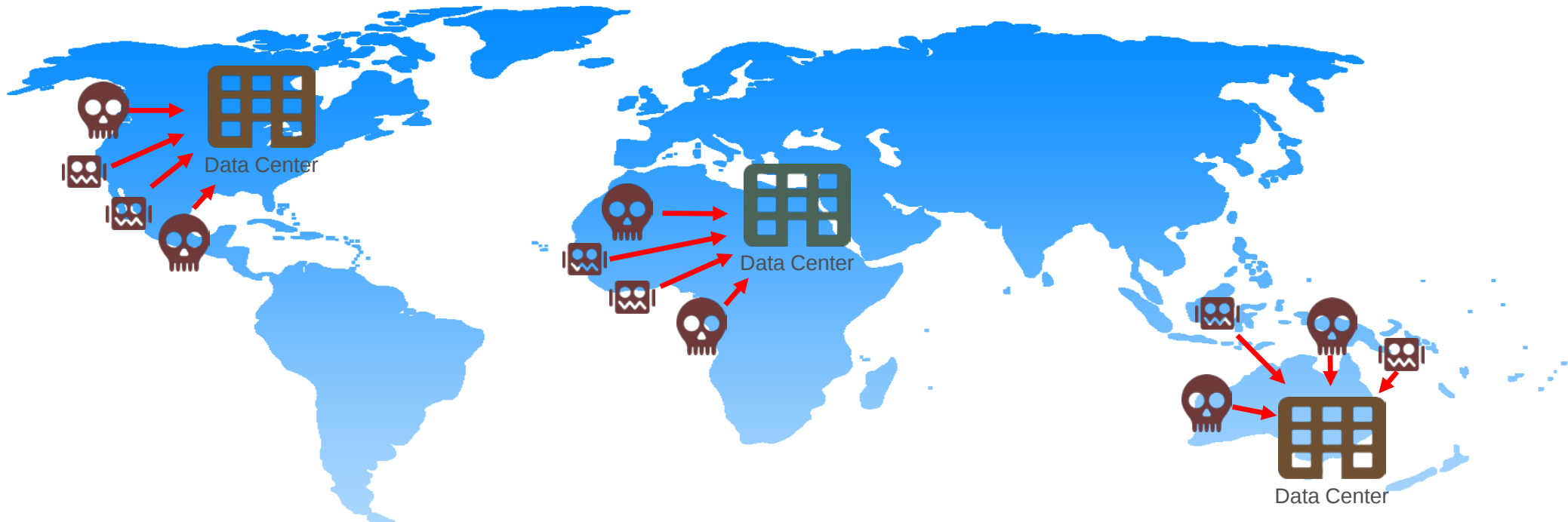
Geographical Mitigation



DNS Attack Mitigation

Spread the attack with IP Anycast

- Thwart an attack by spreading the load to multiple data centers.
- Attackers will target the attack using a single IP address representing the victim, your datacenter.
- IP Anycast advertises a common IP address into the internet routing tables which route to different DCs.



IP Anycast and DNS

Makes DNS more reliable

- Geographically dispersed servers
- Simple network-based failover during network/server outage

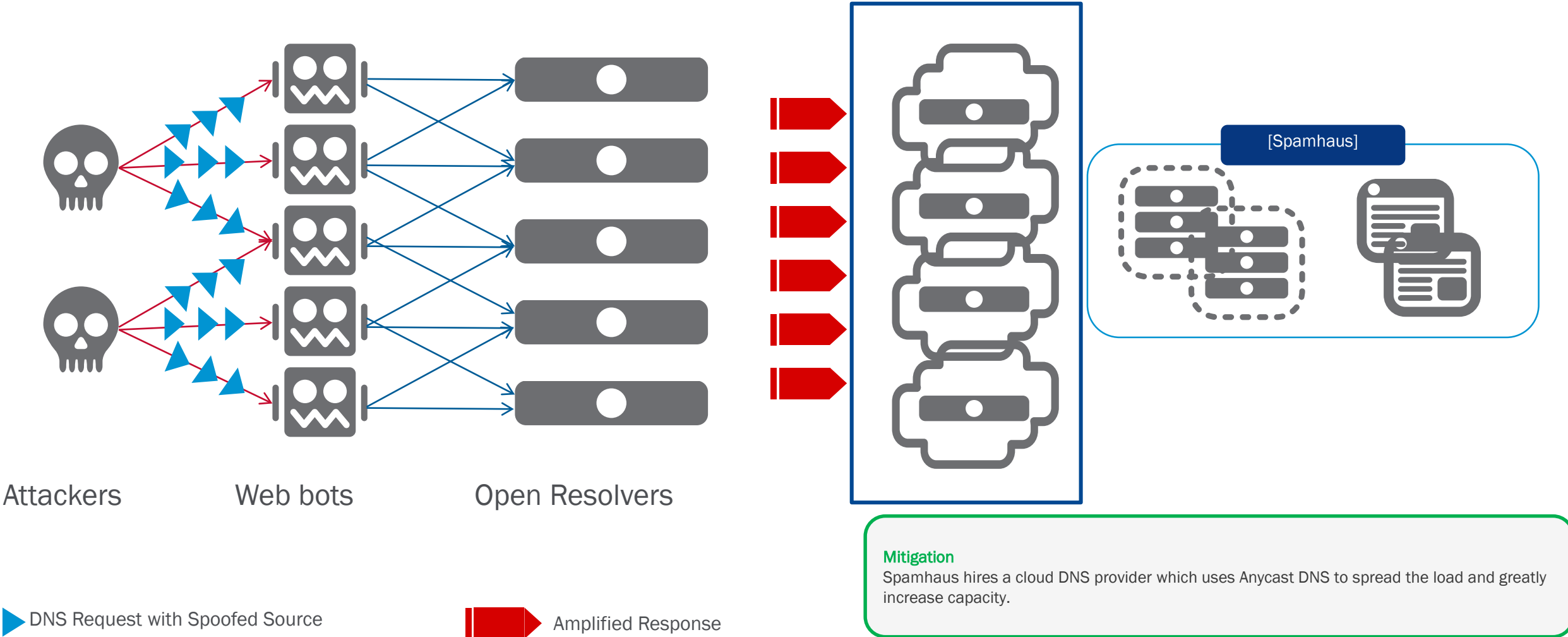
Improves DNS performance

- Provides simple preference for “close” servers
- Spreads global load across servers
- Resilience against DDoS attacks

Eases management

- Smaller number of IP's can be used and listed in the root server

Spamhaus Attack

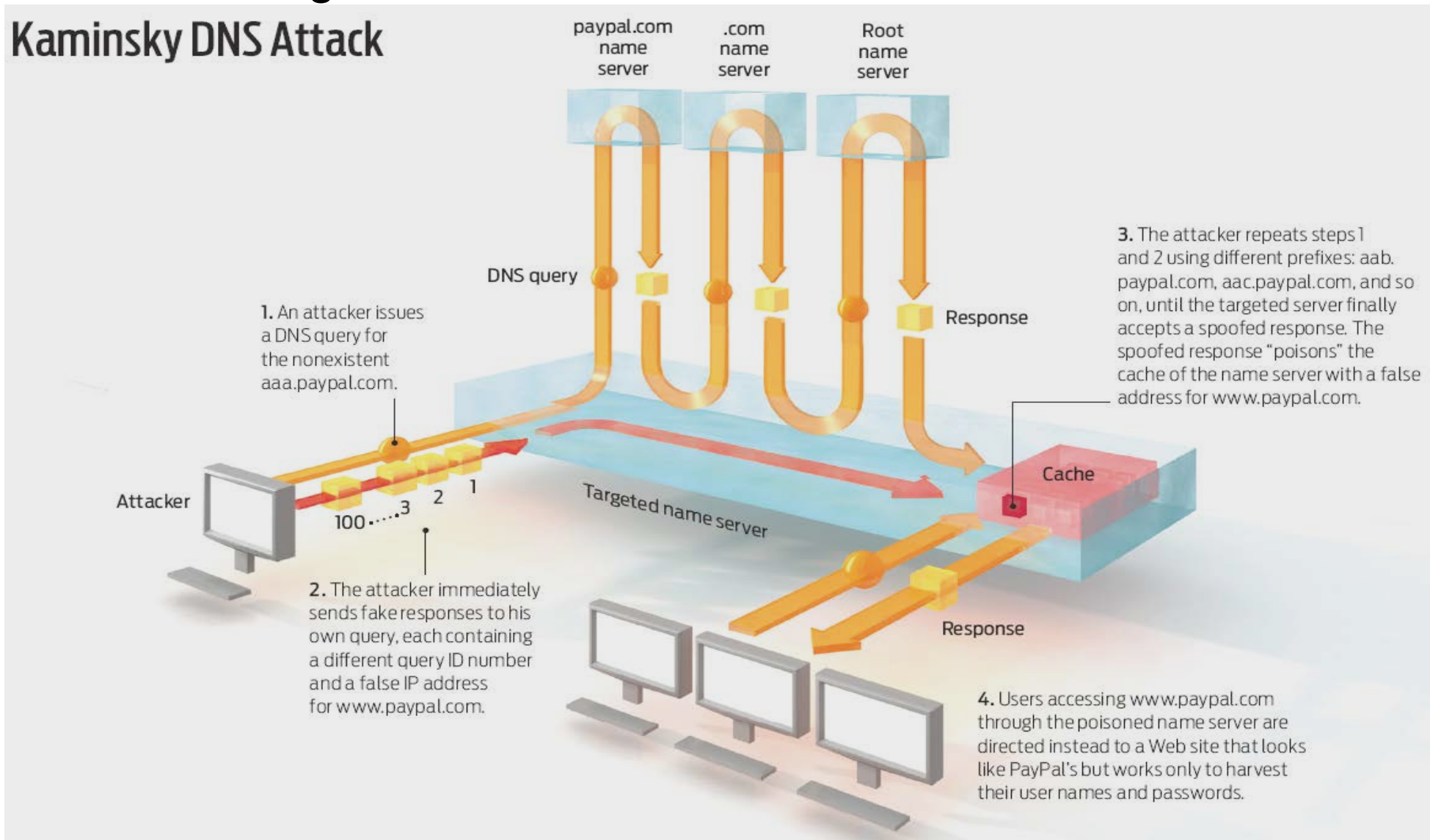


Cache Poisoning

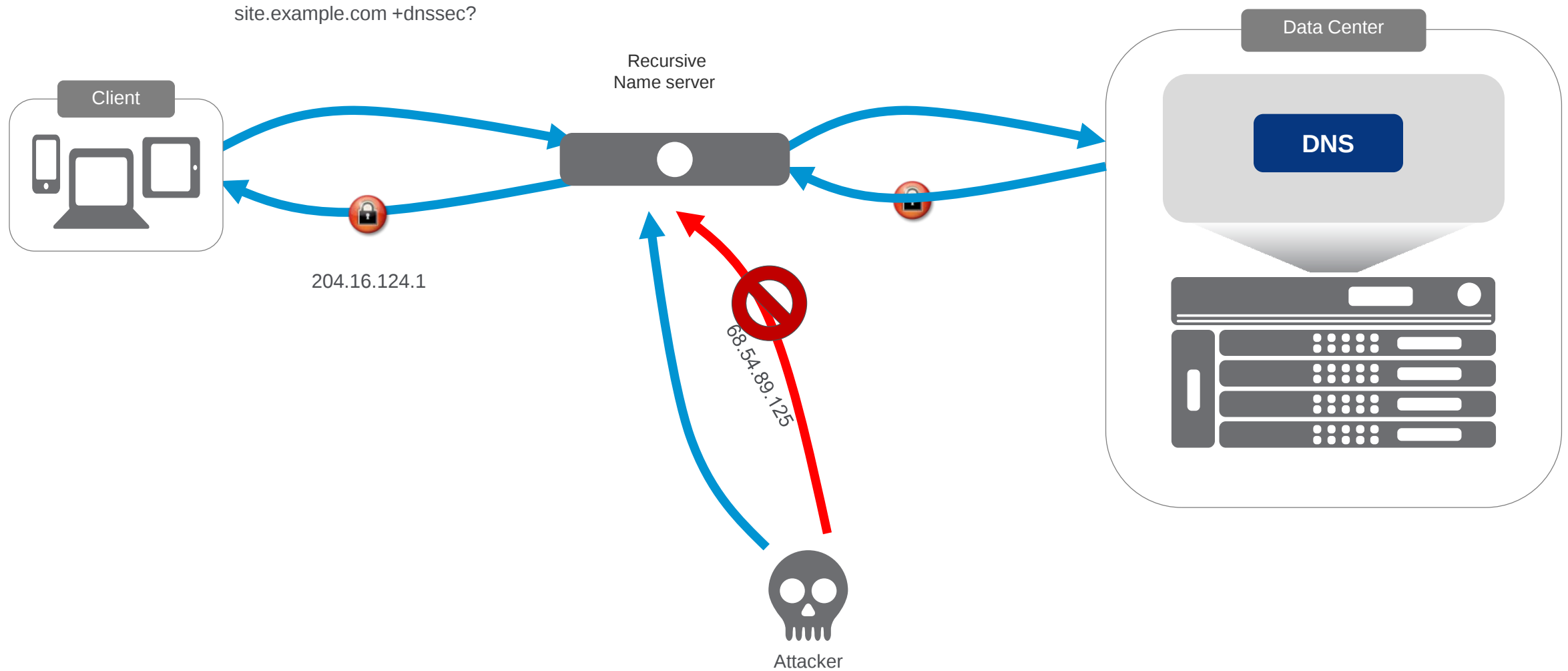


DNS Cache Poisoning

Kaminsky DNS Attack



DNS Cache Poisoning



DNS Firewalling rather than
a Firewall for a DNS server



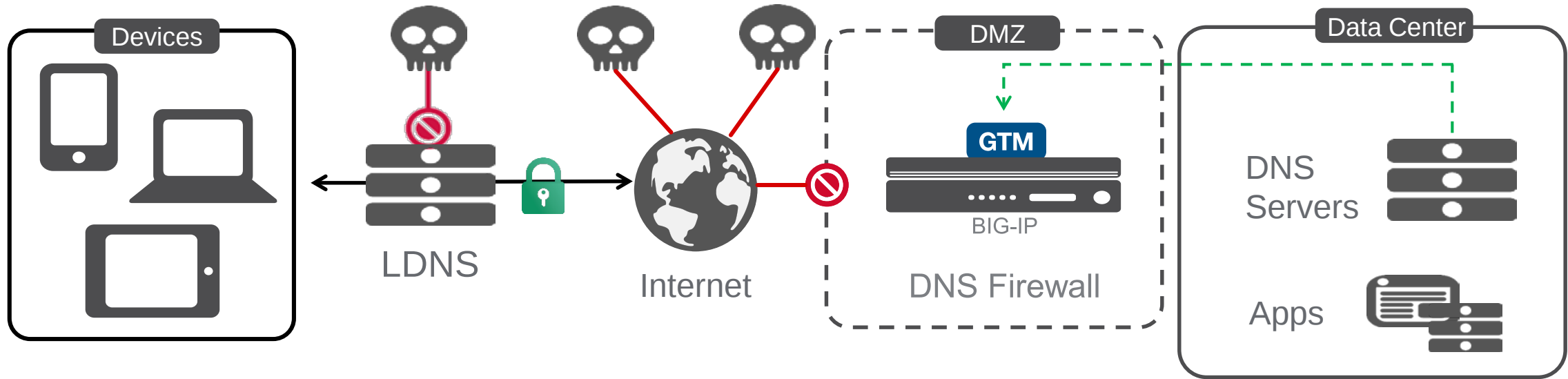
DNS Firewalling rather than a Firewall for a DNS server

When under attack Traditional Firewalls do not provide security for DNS servers
Consolidate services to allow for scaling and availability, remove single points of failure
Maintain security certification



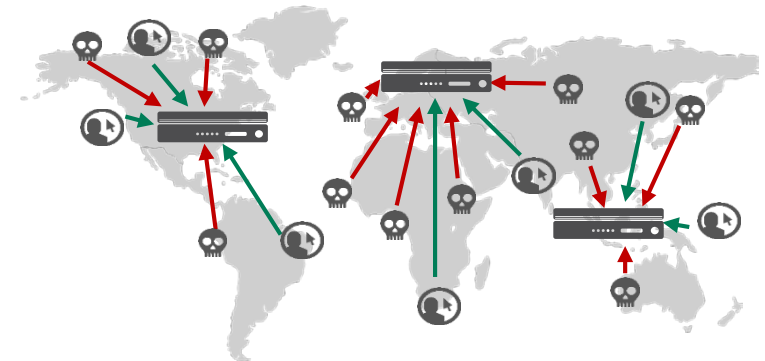
- Increases availability when under attack, and scalability
- Maintains all Security Certifications
- Reduces Vendor and hardware requirements for Capex and Opex

Complete DNS Protection & Performance



F5 DNS Firewall Services

- DNS DDoS mitigation with DNS Express
- Protocol inspection and validation
- DNS record type ACL*
- Block access to Malicious IPs (DNS Firewall)
- High performance DNS cache
- Stateful – Never accepts unsolicited responses
- ICSA Certified - deployment in the DMZ
- Scale across devices – IP Anycast
- Secure responses – DNSSEC
 - DNSSEC responses rate limited
- Complete DNS control – iRules
- DDoS threshold alerting*
- DNS logging and reporting
- Hardened F5 DNS code – NOT BIND



DNS attack Demonstration



ITC Demonstration

Summary



Attacks on DNS do not commonly target stealing £\$€¥ but impacts the availability of the businesses applications which makes the business less effective and hence loose £\$€¥ .

Today the applications are the life blood of the business do not put them at risk

DNS Flood Attacks and Mitigation

Protocol Abuse and Mitigation

Geographical Mitigation

Cache Poisoning



Next Steps: Ensure Life blood to Business Applications



Always on
Availability



Scale DNS
services



Secure DNS
services

- If I can be of further assistance please contact me:
- n.ashworth@f5.com | +44 77 88 436 325



SOLUTIONS FOR AN APPLICATION WORLD