Scaling and securing the DNS Cache/Resolver infrastructure

Nigel Ashworth

Solution Architect EMEA

Agenda

Cache / Resolver
Filtering and Caching
Protocol Abuse
Parental Control
Use cases
Summary

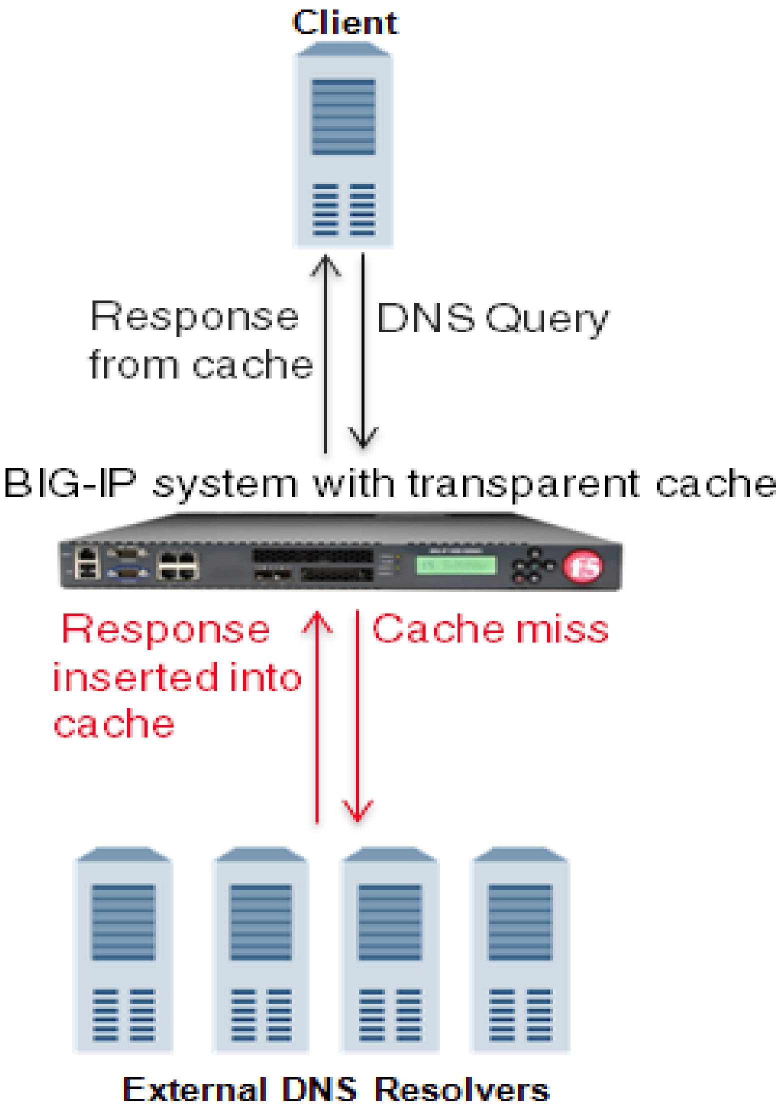
Cache / Resolver

Cache / Resolver

Options:

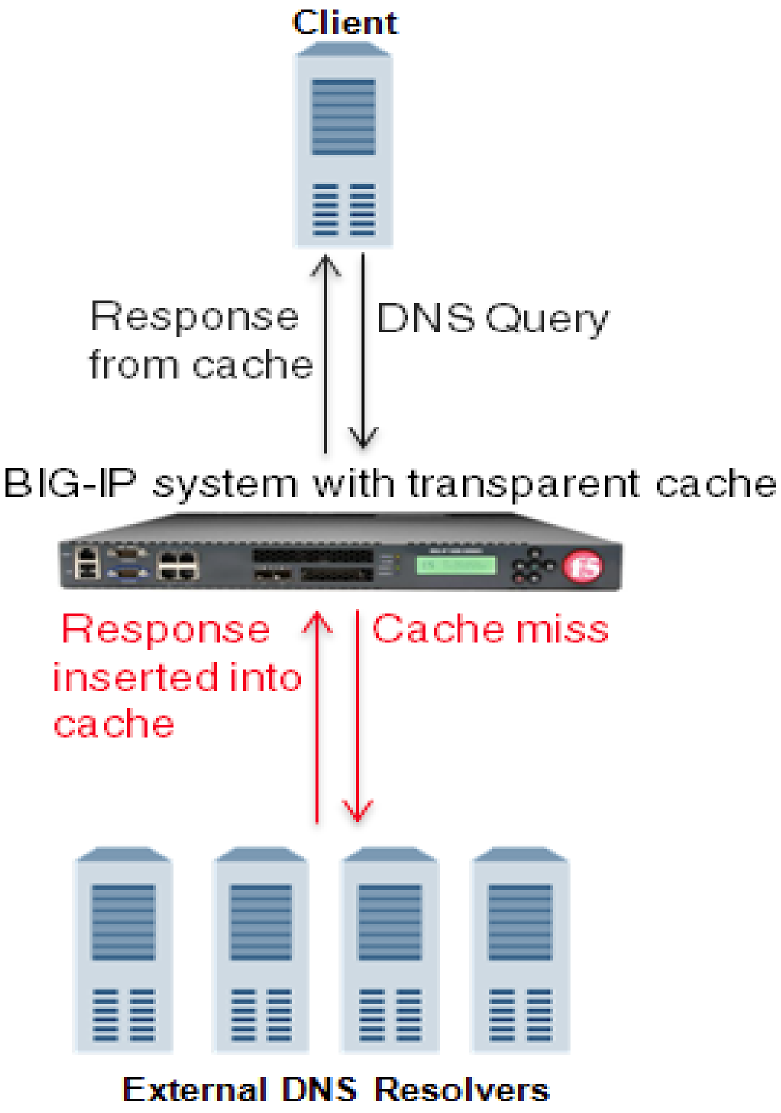
- Transparent Cache
- Transparent Cache and separate resolver
- Cache + Resolver
- Resolver
- IPv4 and IPv6
  - + DNSec

Transparent DNS Cache



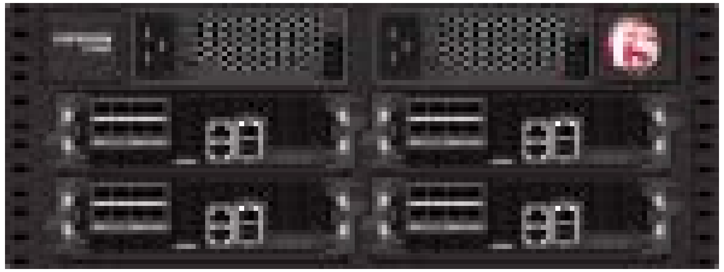
1. Client send DNS query to BigIP .If requested RR exists in cache then answer is given back immediately from the cache.
2. If requested RR does not exist in cache, them BigIP forwards query to pool member for resolution.
3. Pool member handles all iterative look-ups until authorative response is received.
4. BigIP “steals” a copy of the authortative response as the answer is returned to the pool member. This response is then added to cache.
5. Subsequent queries for the given RR will be handed back from the BigIP DNS cache until the TTL expires.

Cache Hit Ratio



- Four caches in BIG-IP DNS
- Hardware 10K vs Software only limited by TTL and Ram allocated
- Hit ratio 80-90%
- Miss ratio, is the cache empty vs steady state
- Performance Marketing vs Real world
- Extends the current deployment
- User response time - Acceleration

Cache and Random Queries



VIPRION 2400 Chassis

2250 Viprion Blade

V12.0

Software enabled

Differences from Default

SPDAG on

36*36 = 1296 cache entries, Random request selection

100% cache hit (CPU TMM = 99%, Latency 1ms)

Result = 2.18M Queries

90% cache hit (CPU TMM = 99%, Latency 1ms)

Result = 1.55M Queries

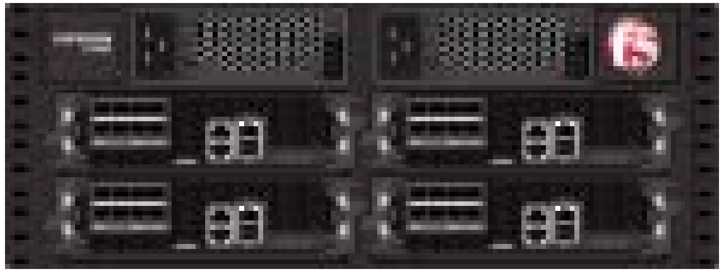
80% cache hit (CPU TMM = 99%, Latency 1ms)

Result = 1.35M Queries

Cache and Random Queries

2250 Viprion Blade
V12.0
Software enabled
Differences from Default
SPDAG on
36*36 = 1296 cache entries, Random request selection

100% cache hit (CPU TMM = 99%, Latency 1ms)
Result = 2.18M Queries
90% cache hit (CPU TMM = 99%, Latency 1ms)
Result = 1.55M Queries
80% cache hit (CPU TMM = 99%, Latency 1ms)
Result = 1.35M Queries

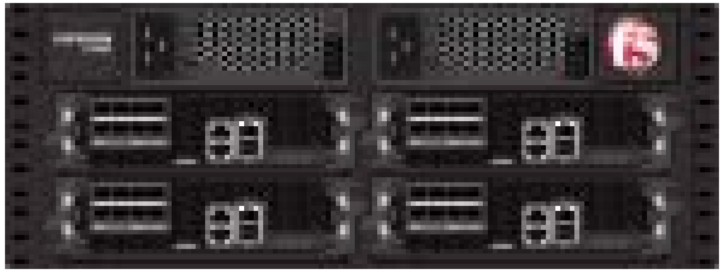


VIPRION 2400 Chassis

4300 blade = 97%

VIPRION 44xx Chassis

Cache and Random Queries



VIPRION 2400 Chassis

2250 Viprion Blade

V12.0

Hardware enabled (10K entries)

Differences from Default

SPDAG on

36*36 = 1296 cache entries, Random request selection

100% cache hit (CPU TMM = 3%, Latency 1ms)

Result = 8.5M Qps

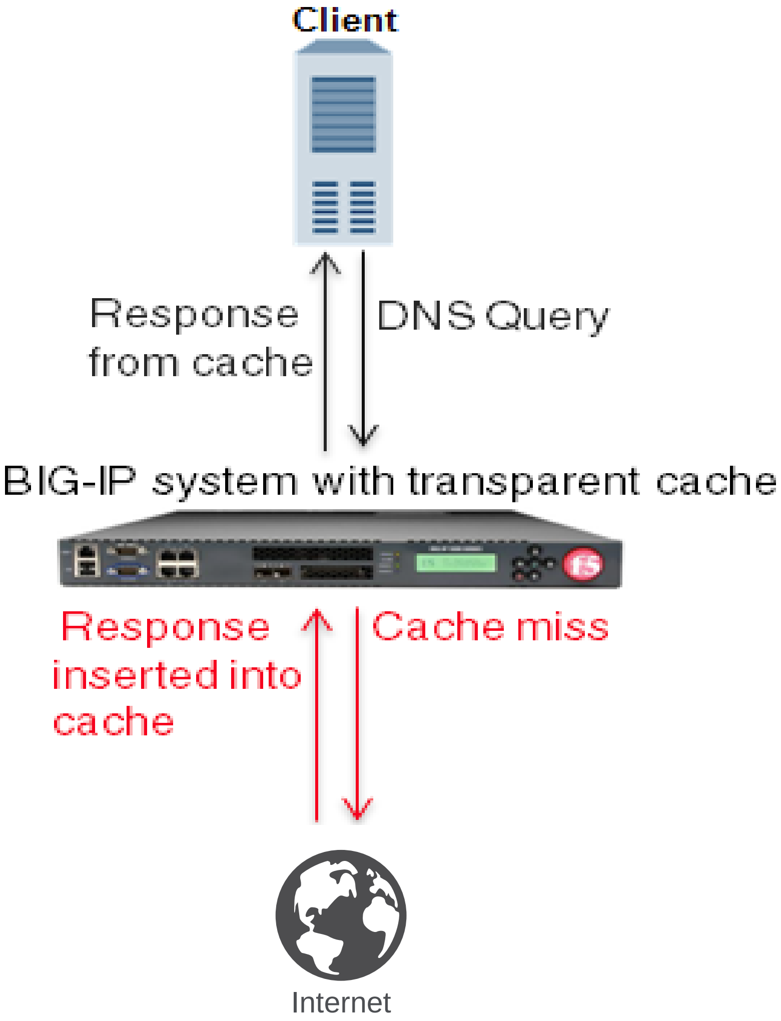
90% cache hit (CPU TMM = 98%, Latency 1ms)

Result = 8.3M Qps

80% cache hit (CPU TMM = 98%, Latency 1ms)

Result = 7.0M Qps

Cache Hit Ratio


Client
Response from cache
DNS Query
BIG-IP system with transparent cache
Response inserted into cache
Cache miss
Internet

- 10-20% miss
- Resolver Consolidation
- Number of requests in flight
- ITC London test environment

Filtering and Caching

Protecting the Client

The internet isn’t an altogether safe place

MALICIOUS THREATS

BotNets

Inadvertently downloaded and used to mount distributed attacks.

Viruses

Once installed, causes malicious activity on end-user device, sometimes for ransom.

OS Vulnerabilities

Unprotected, unpatched devices are extremely vulnerable.

UNDESIRABLE CONTENT

Offensive

Content may violate HR or local rules.

Violation of decency standards.

Be age inappropriate.

Irrelevant

Distractive content incompatible with job function or policy.

Illegal content

File sharing or sites identified as hosting banned material.

DUPING THE USER

Phishing scams and Man in the Middle

Websites which impersonate real websites, often linked from email or a website.

Scammers aim to capture credentials.

Site redirection

DNS traffic is captured and sent to a malicious DNS server serving bad DNS results.

DNS IP and Name Reputation Choices

RESPONSE POLICY ZONES INHIBITS THREATS BY FQDN	Screens a DNS request against domains with a bad reputation.
IP INTELLIGENCE INHIBITS THREATS BY IP	Intercept a DNS response in iRules. Categorize & make a decision.
URL FILTERING INHIBITS THREATS BY FQDN POLICY CONTROL BY FQDN	Intercept a DNS request in iRules. Categorize & make a decision.

Technical Use Cases

	Nature of Threat	RPZ	IP INTELLIGENCE	URL FILTERING
http://www.badsite.com	Virus, malware etc. DNS lookup required.	✓	Limited to IP address reputation.	✓
http://194.71.107.15	Virus, malware etc No DNS lookup issued	No DNS lookup to filter.	✓	No URL or FQDN to examine.
http://www.facebook.com	Social networking Against corp policy.	Cover malicious content only.	Limited to IP address reputation.	✓

Domain Category Filtering

Additional Granularity with a URL Filtering License

- Identify the request to one of over 130 categories
  - Social networking
  - Inappropriate content
  - Games
- Further customize via client identification
  - Subnet
  - Query signature
- Live feed, updated every 5 minutes
- Do specific actions on a category match for a query
  - NXDOMAIN
  - Redirect

```
when RULE_INIT {
  set static::blocked_categories {
    /Common/Bot_Networks
    /Common/Spyware
    /Common/Malicious_Web_Sites
  }
}
when DNS_REQUEST {
    set lookup_category [getfield [CATEGORY::lookup "http://[DNS::question name]"] " " 1]
    if { [lsearch -exact $static::blocked_categories $lookup_category] >= 1 } {
      if { $static::request_debug } {
         log local0. "BLOCKED: Category $lookup_category matching [DNS::question name] is filtered."
      }
      DNS::answer clear
      if { [DNS::question type] equals "A" } {
         DNS::answer insert "[DNS::question name]. 111 [DNS::question class] [DNS::question type]
             $static::192.168.57.253"
         }
      }
      DNS::return
    } else {
      if { $static::request_debug } {
         log local0. "Category $lookup_category matching [DNS::question name] is not filtered"
      }
    }
  }
```

DNS IP Intelligence

- The IP Intelligence License allows DNS responses to be queried for reputation.

- iRules only
  - Customize the action
  - Log, drop, redirect etc

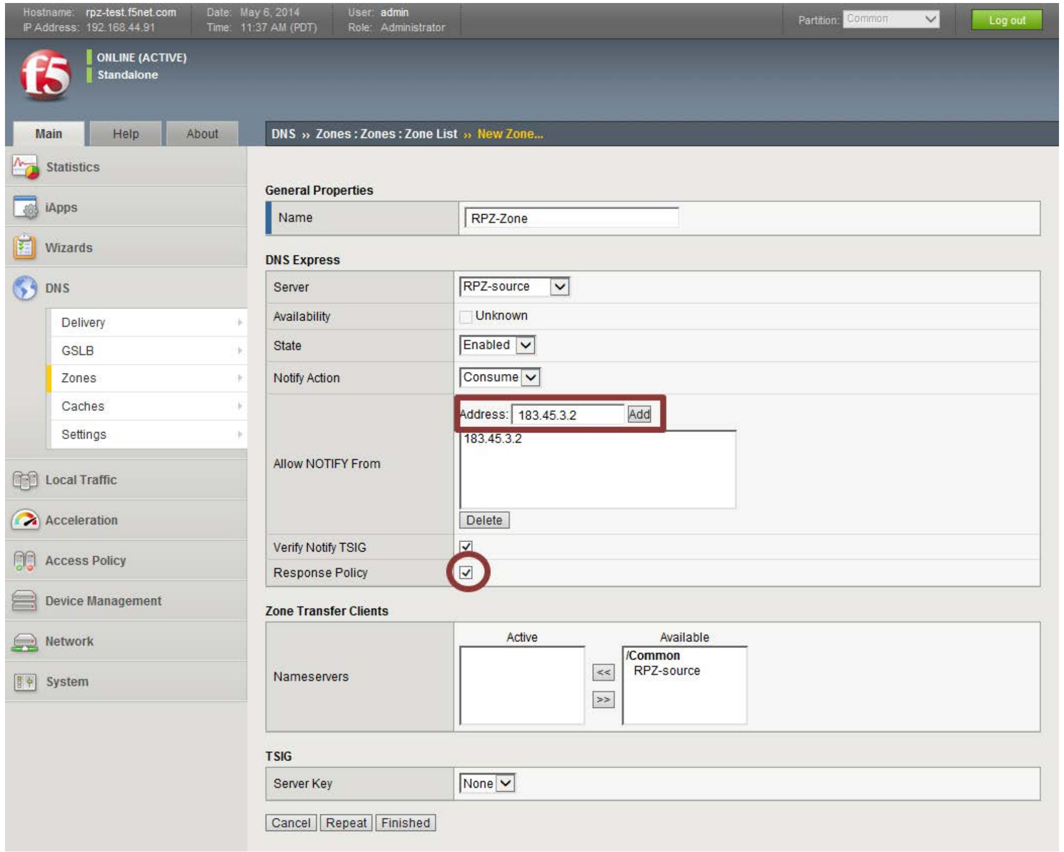
- Support for 8 categories
  - Windows Exploits
  - Web Attacks
  - Botnets
  - Scanners
  - Denial of Service
  - Infected Sources
  - Phishing
  - Proxy

- Based on the resolved IP address
  - For queries, look to RPZ or URL filtering

```
when DNS_RESPONSE
{
   # If Query type was A and response is an answer.
   if { ([DNS::question type] eq "A") and ([DNS::ptype] == "ANSWER") }
   {
       set rrs [DNS::answer]
       foreach rr $rrs
       {
          if { [DNS::type $rr] eq "A" }
          {
             if {[llength [IP::reputation [DNS::rdata $rr]]] != 0}
             {
                 # Bad IP Reputation for destination detected
                 log local0. "$rr: \"[IP::reputation $ip]\", count: [llength [IP::reputation $rr]]"
             }
          }
       }
   }
}
```

```
<RULE_INIT>: 8.5.1.16: "{Web Attacks} BotNets Scanners Proxy", count: 4
<RULE_INIT>: 1.1.17.0: "{Web Attacks} Scanners", count: 2
<RULE_INIT>: 1.161.40.194: "{Windows Exploits} Scanners", count: 2
<RULE_INIT>: 2.32.20.157: "Proxy", count: 1
<RULE_INIT>: 2.50.32.55: "{Spam Sources} Proxy", count: 2
<RULE_INIT>: 2.56.0.0: "{Spam Sources} {Web Attacks}", count: 2
<RULE_INIT>: 254.46.202.147: "Phishing", count: 1
```

Response Policy Zones



DNS » Zones : Zones : Zone List » New Zone...

General Properties

Name	RPZ-Zone

DNS Express

Server	RPZ-source
Availability	Unknown
State	Enabled
Notify Action	Consume
Allow NOTIFY From	Address: 183.45.3.2 Add 183.45.3.2 Delete
Verify Notify TSIG	☑
Response Policy	☑

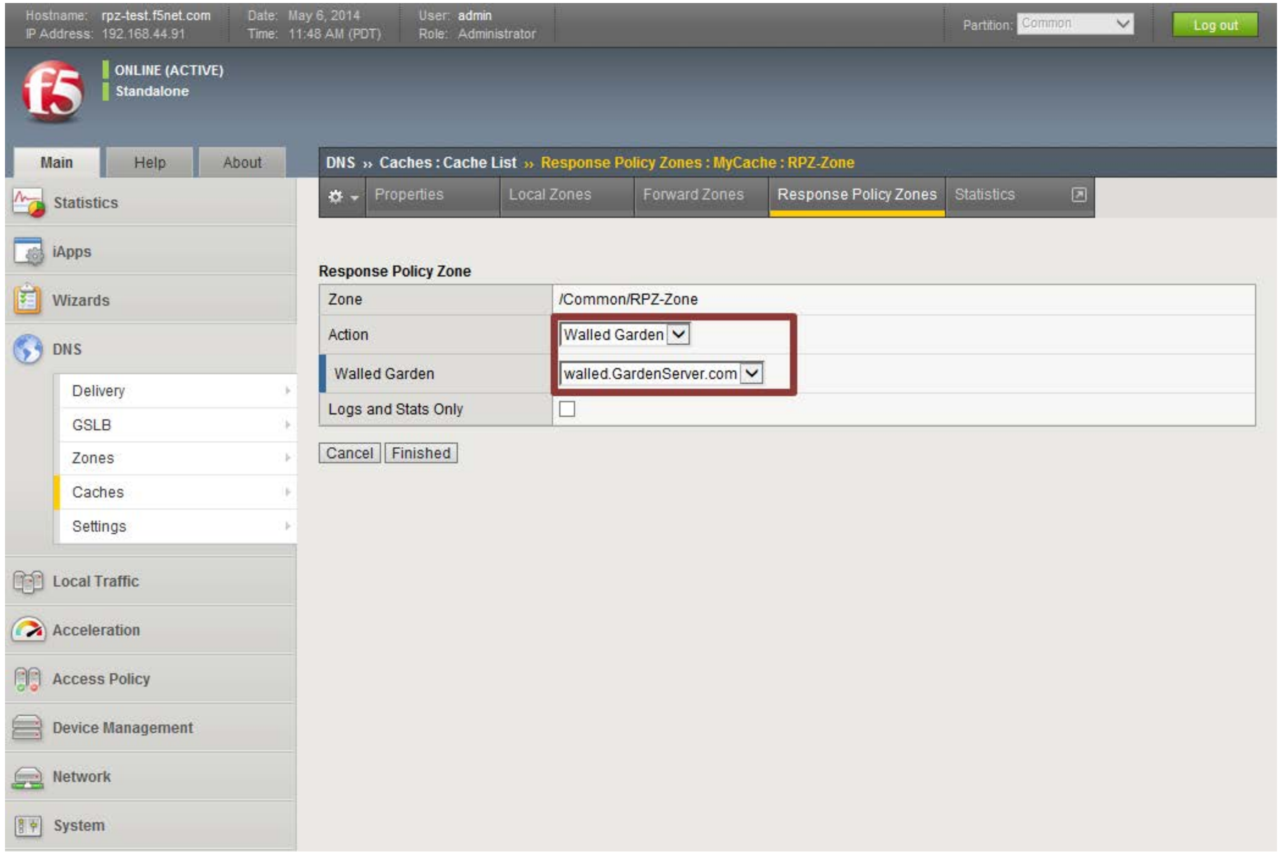
Zone Transfer Clients

	Active	Available
Nameservers		/Common RPZ-source

TSIG

Server Key	None

Cancel Repeat Finished



DNS » Caches : Cache List » Response Policy Zones : MyCache : RPZ-Zone

Response Policy Zone

Zone	/Common/RPZ-Zone
Action	Walled Garden
Walled Garden	walled.GardenServer.com
Logs and Stats Only	☐

Cancel Finished

Create a new zone to host the RPZ Zone.

Set it up to allow NOTIFY commands from the RPZ Source.

Specify that this is a Response Policy.

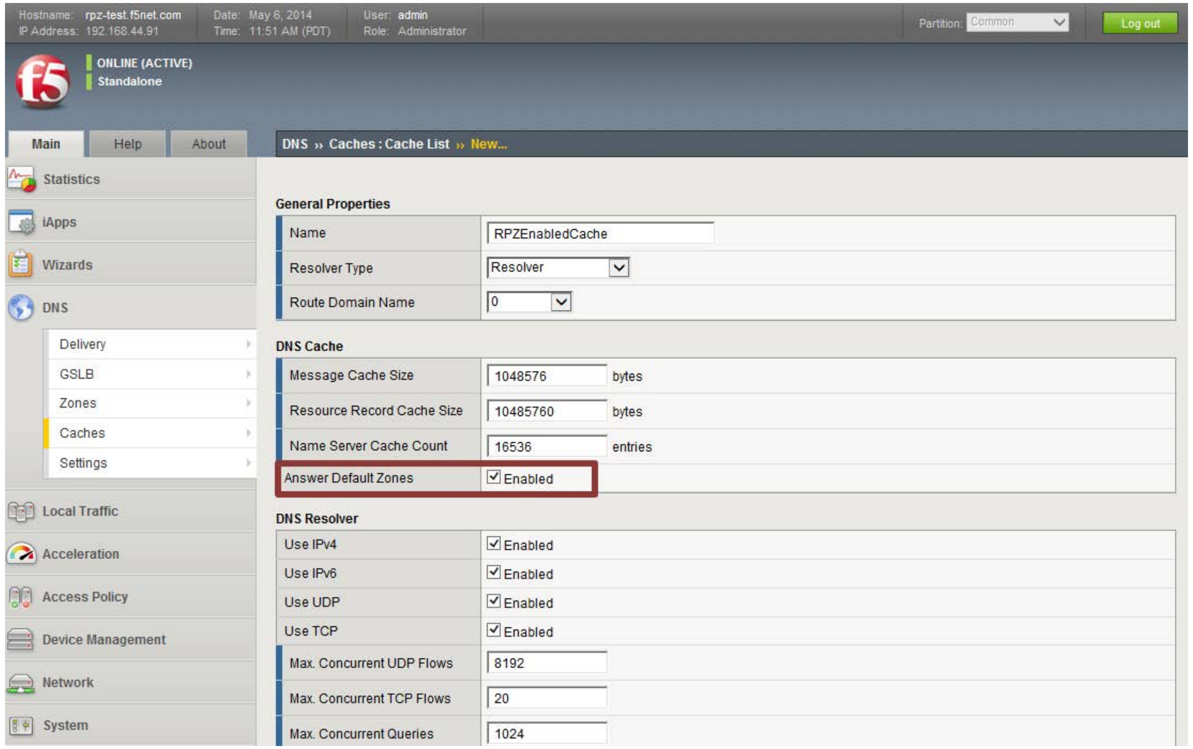
Define what action is requested when there is an RPZ Match.

NXDOMAIN or Walled Garden.

Walled Garden requires a local zone record to be created.

Response Policy Zones

Configuration continued



Hostname: rpz-test.f5net.com
IP Address: 192.168.44.91
Date: May 6, 2014
Time: 11:51 AM (PDT)
User: admin
Role: Administrator

DNS » Caches : Cache List » New...

General Properties

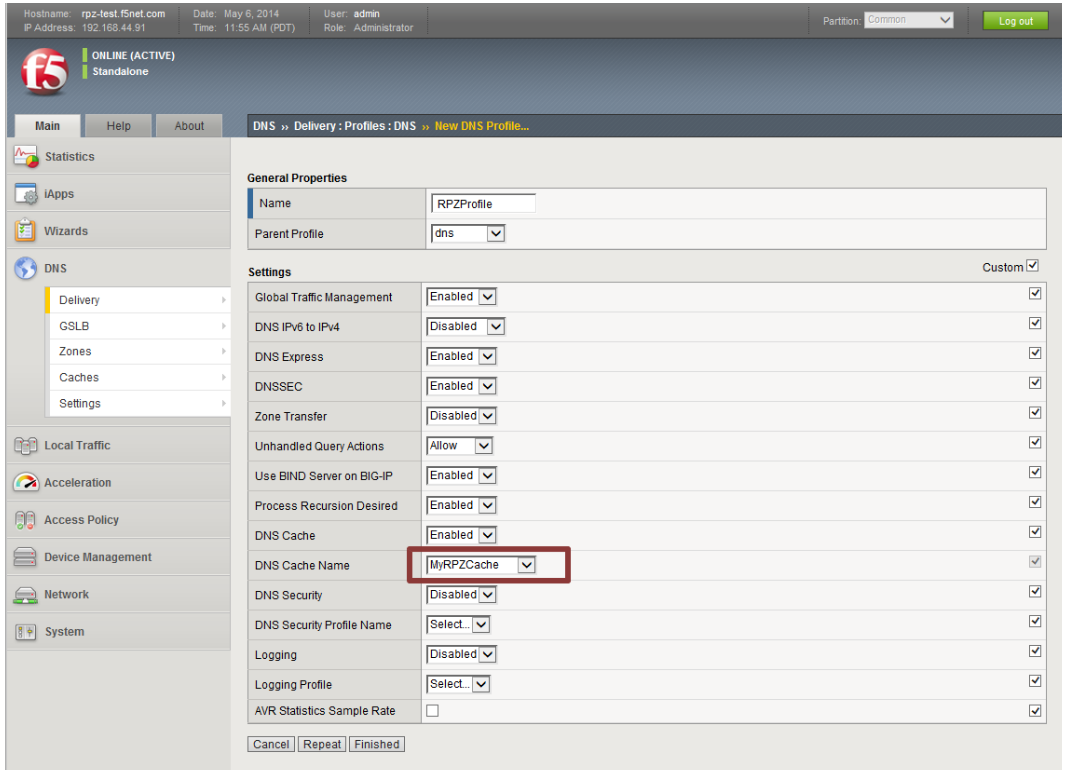
Name	RPZEnabledCache
Resolver Type	Resolver
Route Domain Name	0

DNS Cache

Message Cache Size	1048576 bytes
Resource Record Cache Size	10485760 bytes
Name Server Cache Count	16536 entries
Answer Default Zones	☑ Enabled

DNS Resolver

Use IPv4	☑ Enabled
Use IPv6	☑ Enabled
Use UDP	☑ Enabled
Use TCP	☑ Enabled
Max. Concurrent UDP Flows	8192
Max. Concurrent TCP Flows	20
Max. Concurrent Queries	1024



Hostname: rpz-test.f5net.com
IP Address: 192.168.44.91
Date: May 6, 2014
Time: 11:55 AM (PDT)
User: admin
Role: Administrator

DNS » Delivery : Profiles : DNS » New DNS Profile...

General Properties

Name	RPZProfile
Parent Profile	dns

Settings

		Custom ☑
Global Traffic Management	Enabled	☑
DNS IPv6 to IPv4	Disabled	☑
DNS Express	Enabled	☑
DNSSEC	Enabled	☑
Zone Transfer	Disabled	☑
Unhandled Query Actions	Allow	☑
Use BIND Server on BIG-IP	Enabled	☑
Process Recursion Desired	Enabled	☑
DNS Cache	Enabled	☑
DNS Cache Name	MyRPZCache	☑
DNS Security	Disabled	☑
DNS Security Profile Name	Select...	☑
Logging	Disabled	☑
Logging Profile	Select...	☑
AVR Statistics Sample Rate	□	☑

Cancel | Repeat | Finished

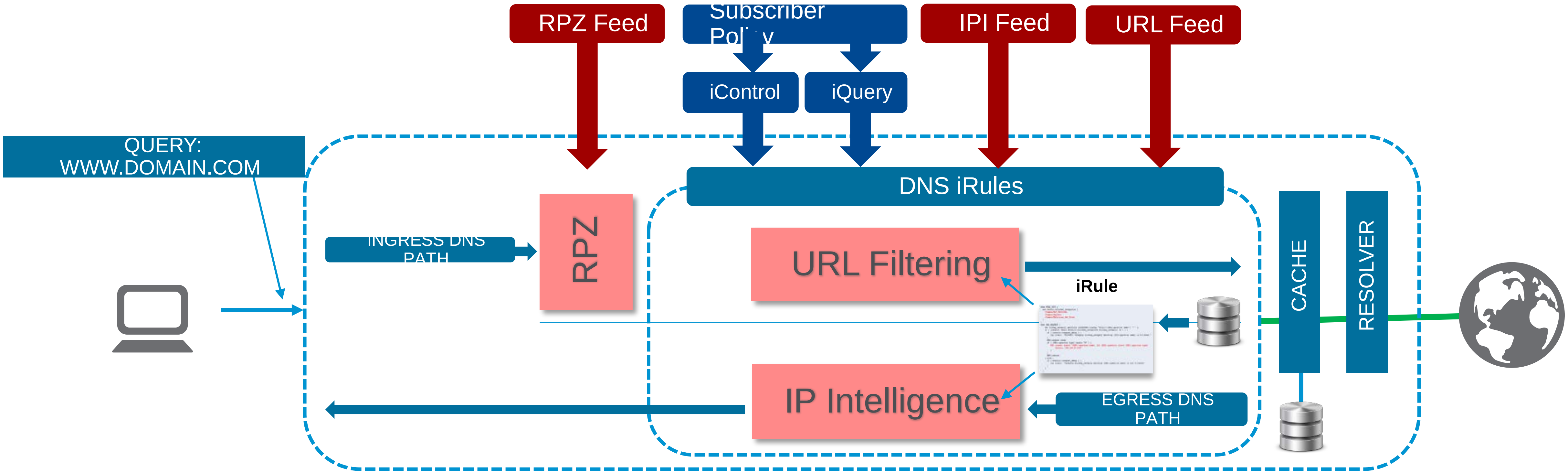
Create a new cache and enable the Answer Default Zones.

Create a new DNS profile and reference the RPZ enabled cache.

Don’t forget to ensure DNS Express is enabled. It is used to host the DNS RPZ Zone.

Use Case – ISP Layered Client Protection

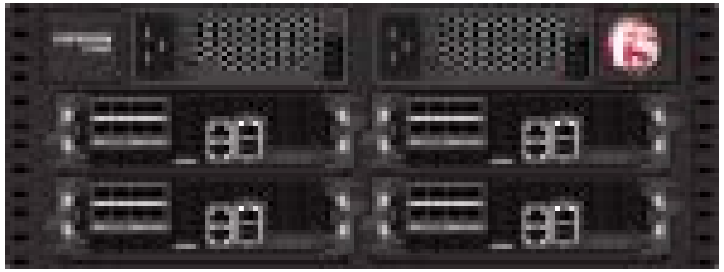
- Response Policy Zones (RPZ) filters out and provides NXDOMAIN / Redirect for know bad doma
- URL Filtering further provides granular policy controls using categories.
- IP Intelligence blocks based on the resolved IP.
  - It can also be used in the data path for other protocols.



Protocol Abuse

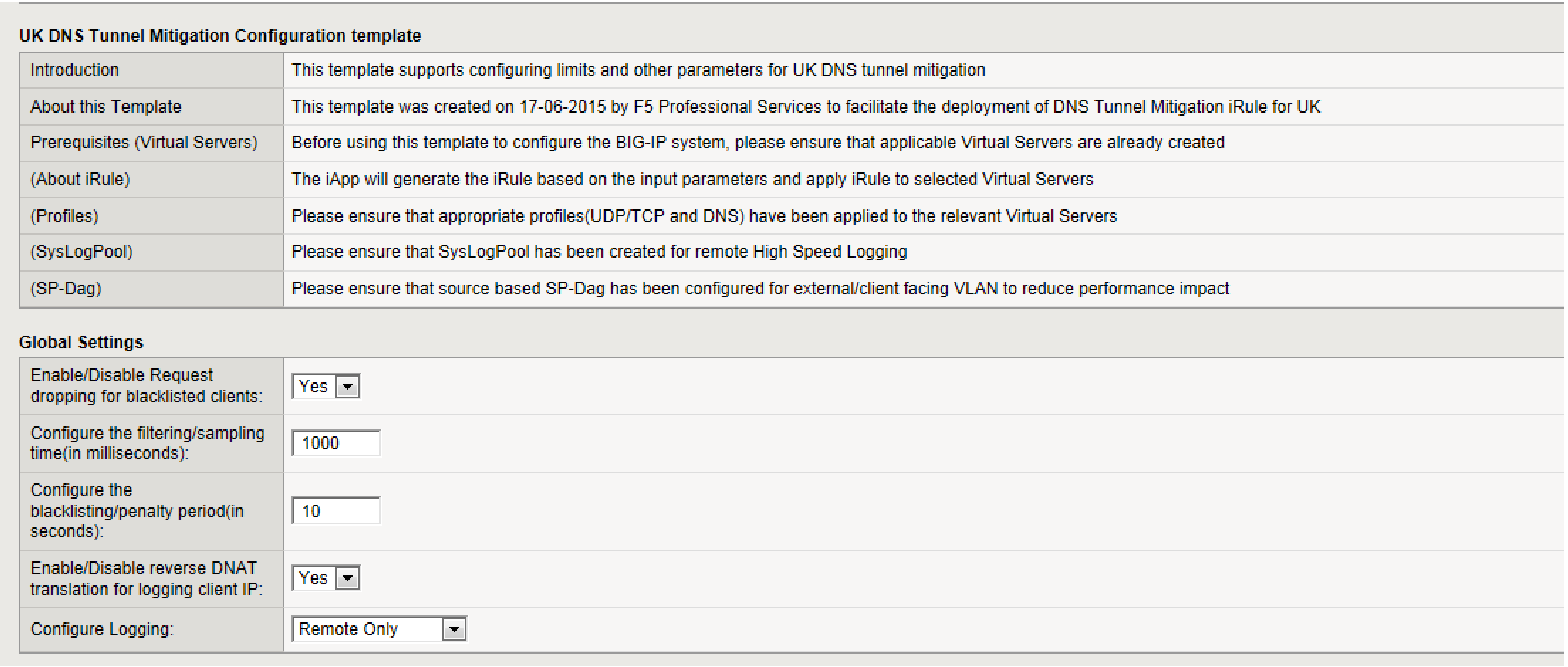
Mitigation of protocol abuse and enforcement

Long host name
Same URL
Random subdomain
Nxdomain response
Long packet response
DPI on packet request?
Packet vs Flow



VIPRION 2400 Chassis

Mitigation of protocol abuse and enforcement



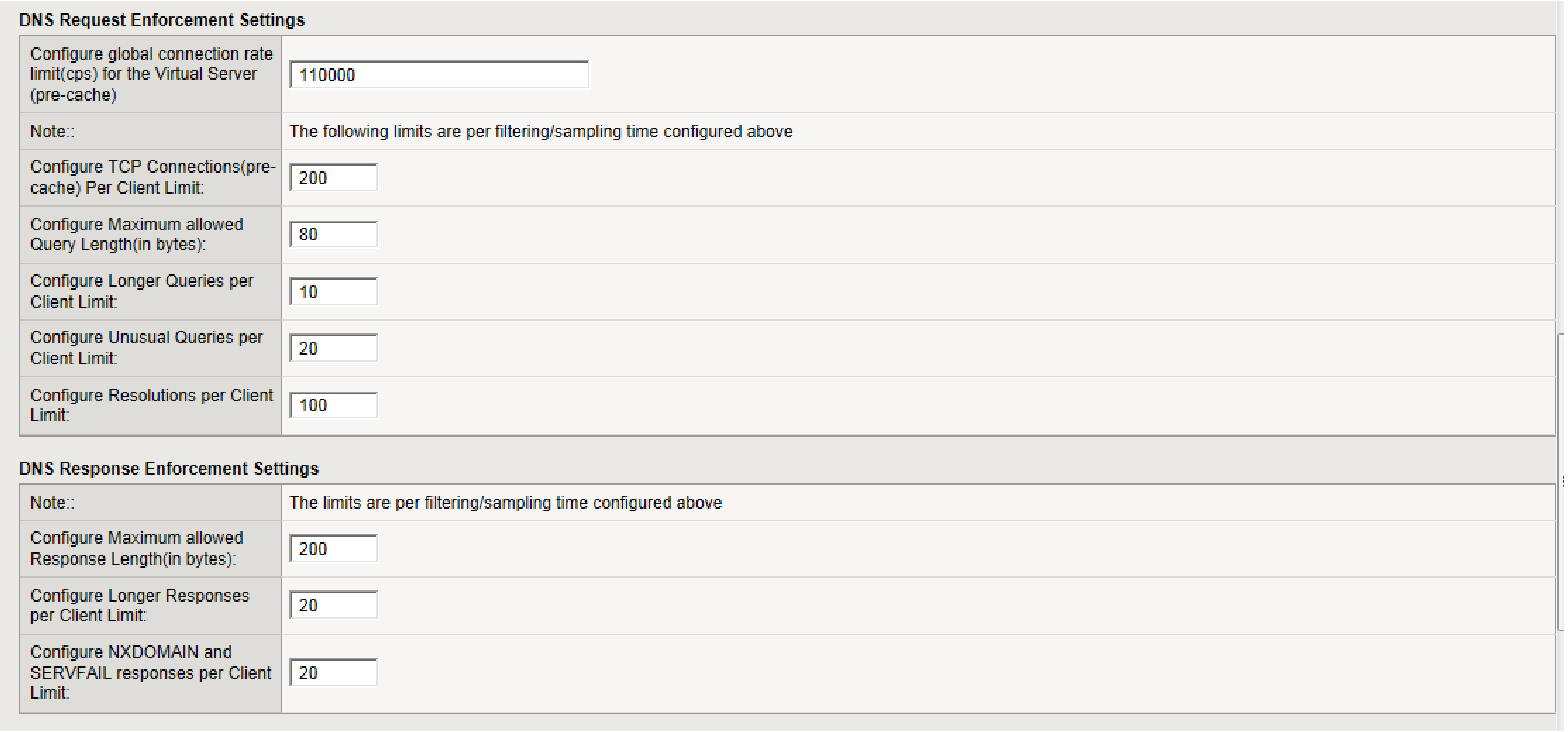
UK DNS Tunnel Mitigation Configuration template

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

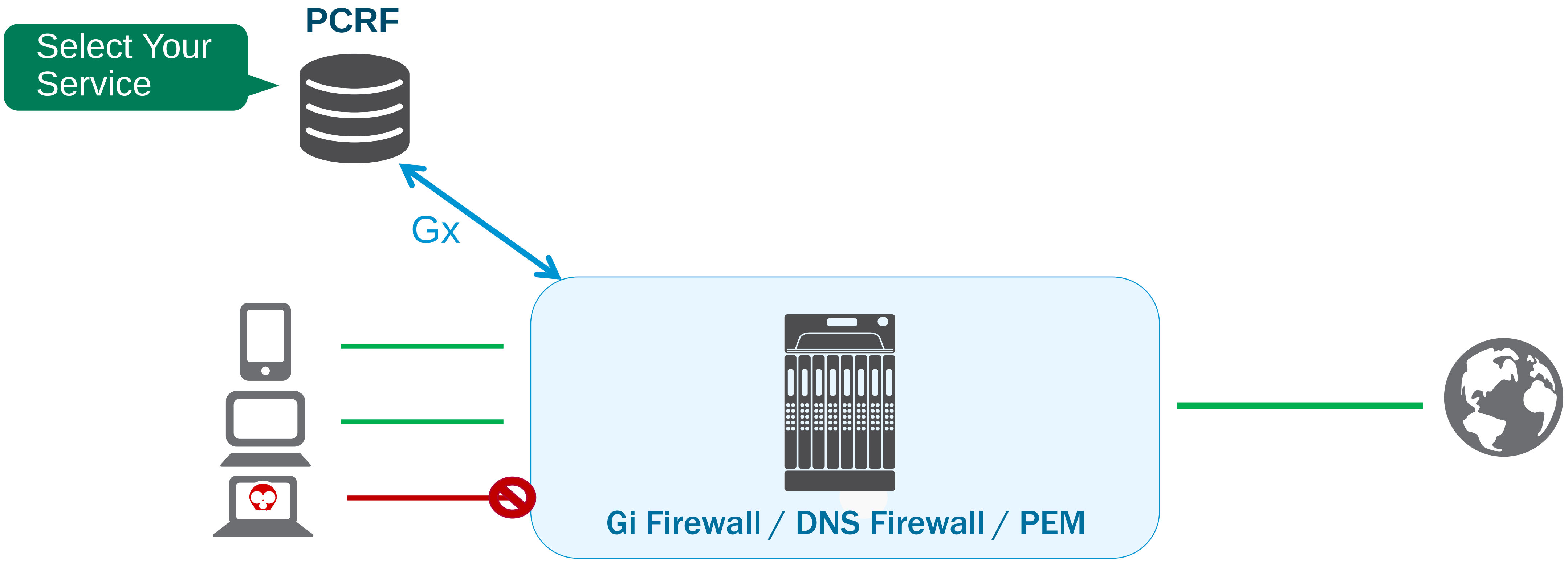
Configure global connection rate limit(cps) for the Virtual Server (pre-cache)	110000
Note::	The following limits are per filtering/sampling time configured above
Configure TCP Connections(pre-cache) Per Client Limit:	200
Configure Maximum allowed Query Length(in bytes):	80
Configure Longer Queries per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

Parental Control
Per-Subscriber DNS-Based
Security Services

Per-Subscriber DNS-Based Security Services

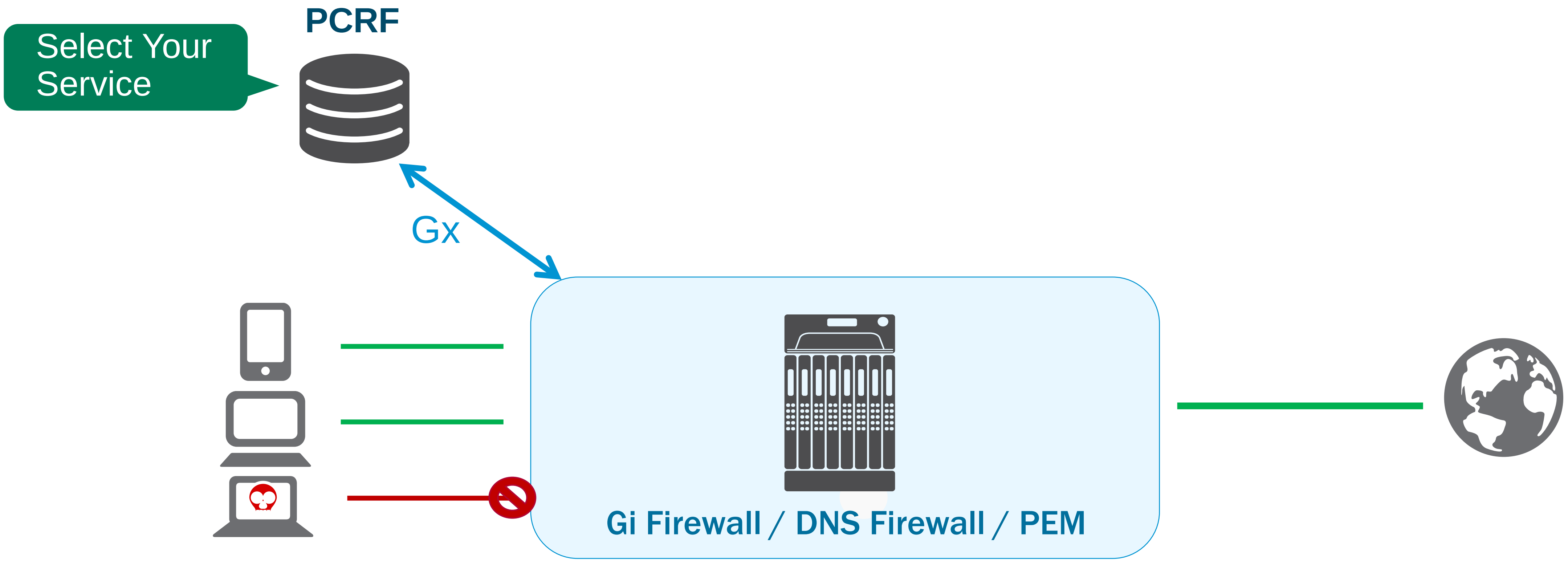


- Increases security for vulnerable users and open up revenue opportunities

- Maintains responses and performance for users

Reduces unwanted content and brand association to sites

Per-Subscriber DNS-Based Security Services

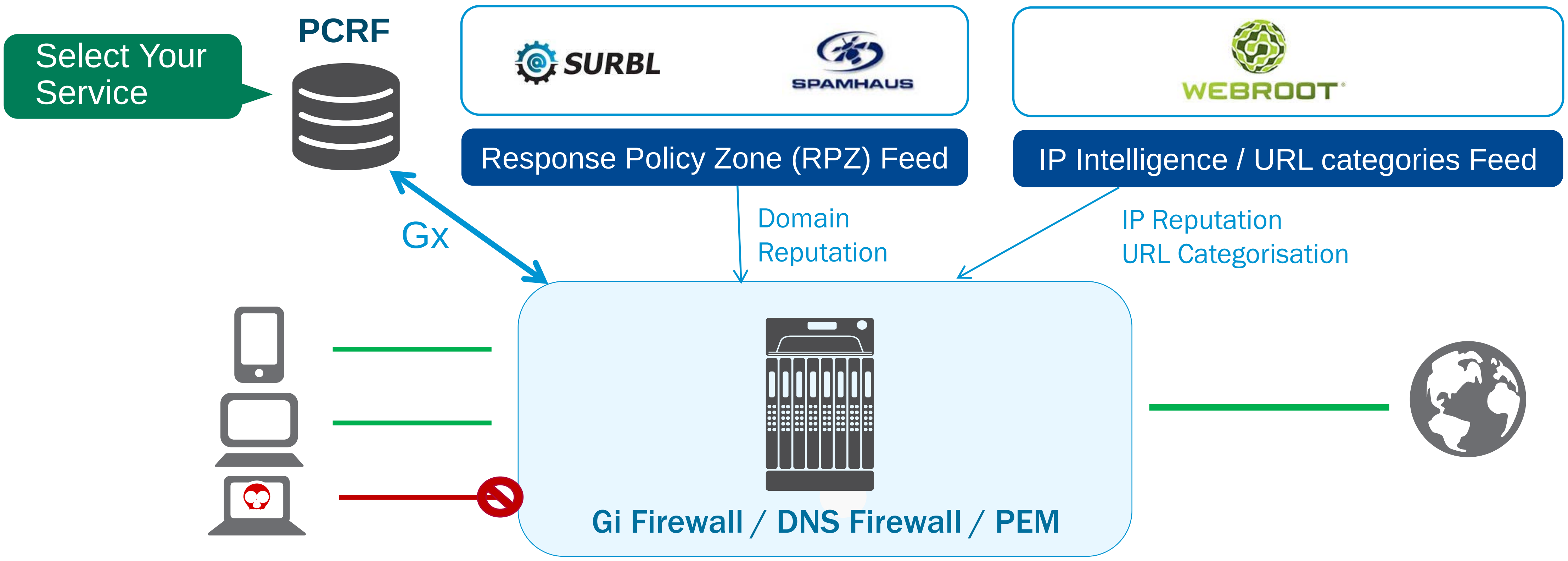


- Front end existing DNS services
- PEM

- Front end and Secure DNS services
- PEM + AFM

- DNS response + Security + Parental control
- PEM + AFM + DNS

Per-Subscriber DNS + URL Security Services



Select Your Service

PCRF

Gx

Response Policy Zone (RPZ) Feed

Domain Reputation

IP Intelligence / URL categories Feed

IP Reputation
URL Categorisation

Gi Firewall / DNS Firewall / PEM

- Mitigate DNS threats by blocking access to malicious IPs
- Reduce malware and virus infections

- Prevent malware and sites hosting malicious content from ever communicating with a client

- Inhibit the threat at the earliest opportunity – Internet activity starts with a DNS request

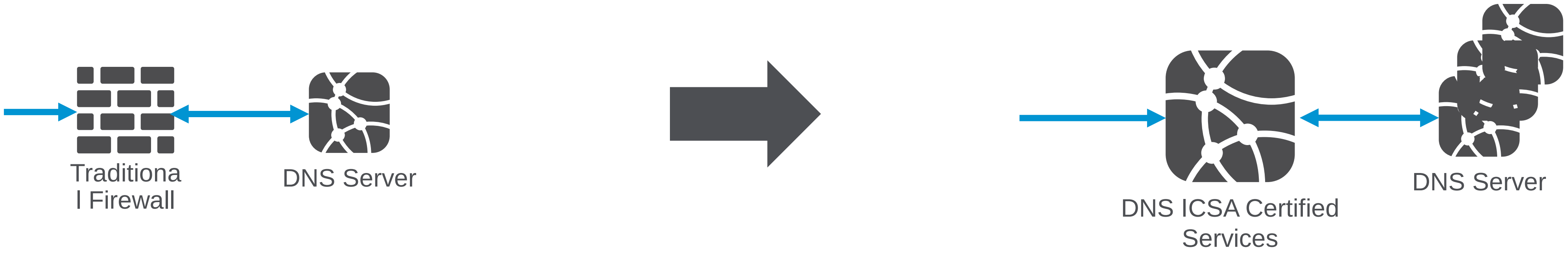
Use cases

What can I do to Extend and Improve my existing DNS services

Traditional scale existing services

Load Balancing extra services to deliver capacity

Complement security with software defined hardware and then look at offload



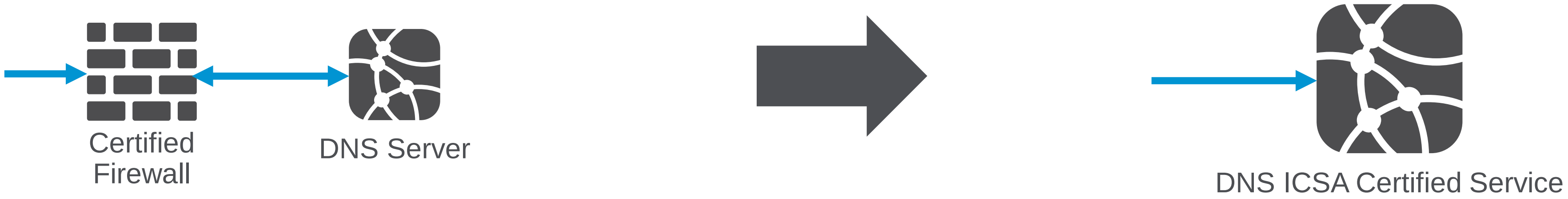
- Increases capacity via scalability
- Maintains all current investment
- Reduces risk of a the traditional firewall limitations

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



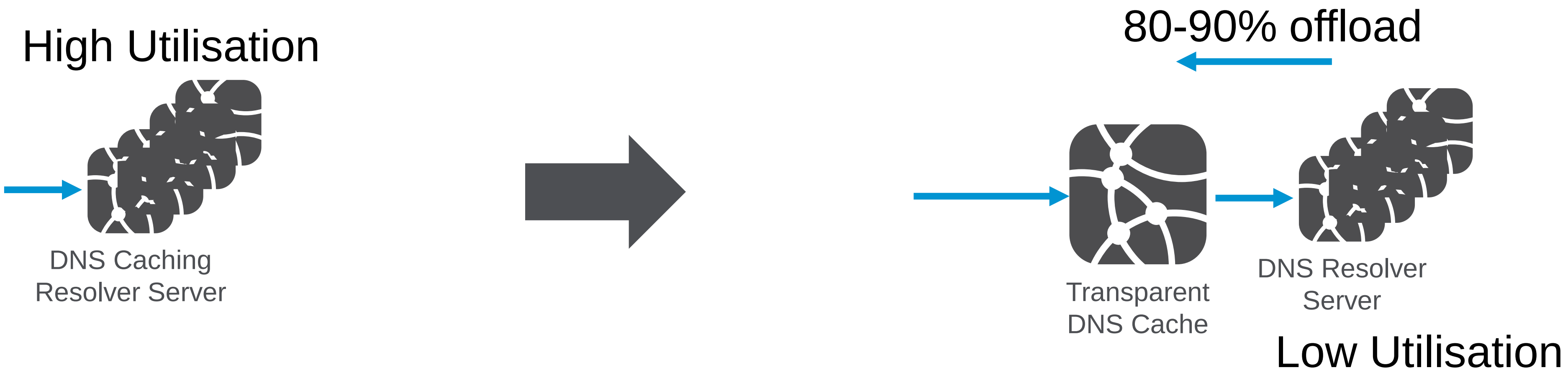
- Increases availability when under attack, and scalability
- Maintains all Security Certifications
- Reduces Vendor and hardware requirements for Capex and Opex

Transparent Cache Offload

Reduce the response time for a DNS resolution

Offload from existing servers

Reduce time to respond for users (local and centralised)



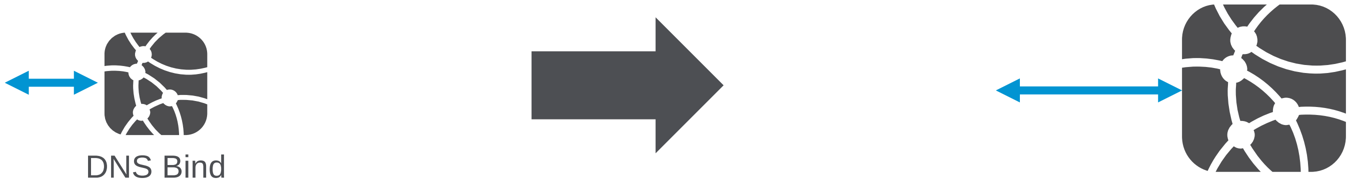
- Increases user experience and scalability
- Maintains all existing hardware and extends the investment on existing hardware
- Reduces migration risk

Mitigating against CVE’s and Bind

Vulnerabilities against Bind are averaging 9-10 per year and do not seem to be slowing down

Where possible remove bind from designs to remove CVE possibilities

Migrate to services that are ICSA certified for security compliance



DNS Bind
Server

DNS ICSA Certified Service

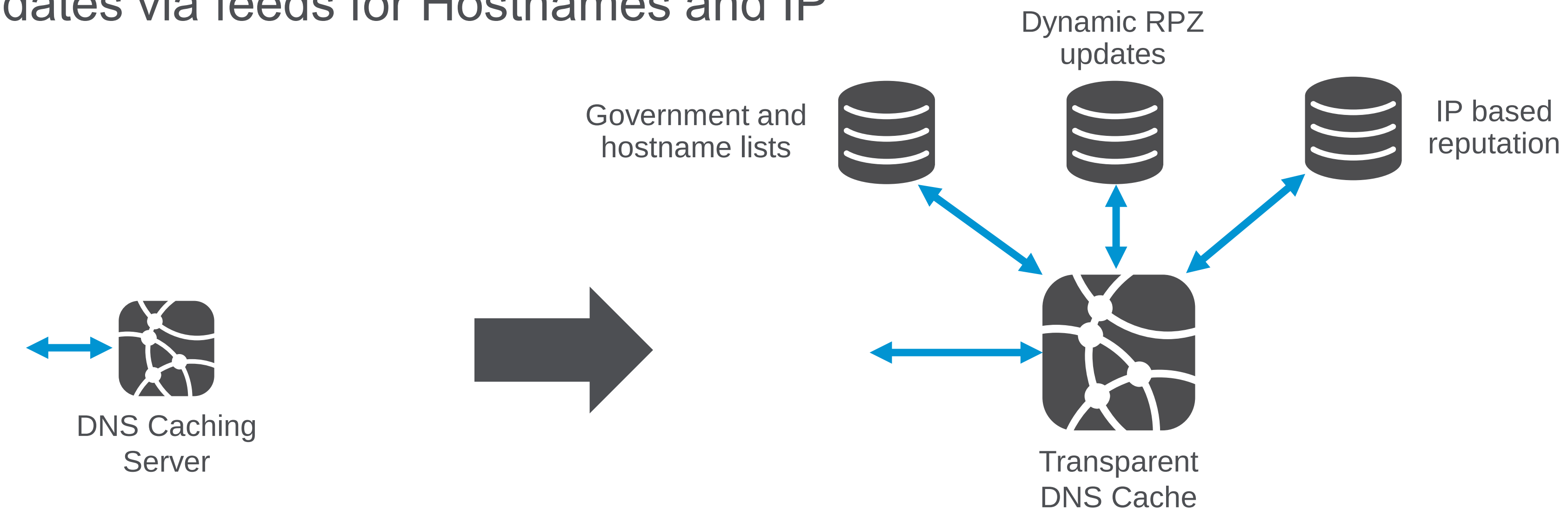
- Increases security, scale and certification
- Maintains features of existing deployments
- Reduces OPEX by removing vulnerability due to the Bind CVE’s

Transparent Cache Security

Filters DNS requests and responses

Government and categorised lists removed

Dynamic updates via feeds for Hostnames and IP



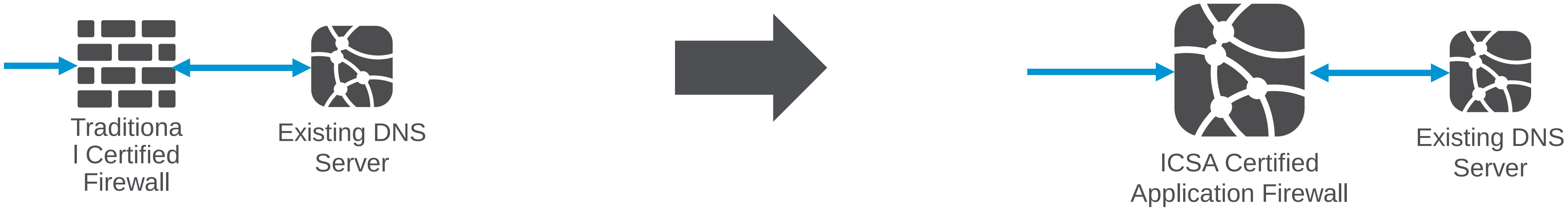
- Increases security from bad sites
- Maintains throughput and users experience while filtering
- Reduces footprint to the internet as part of attacks being logged

DDOS protection for existing DNS services

Provide DDOS hardware protection to existing DNS infrastructure

Provide DDOS hardware vector protection to DNS protocol

Use software defined hardware to maintain security certification



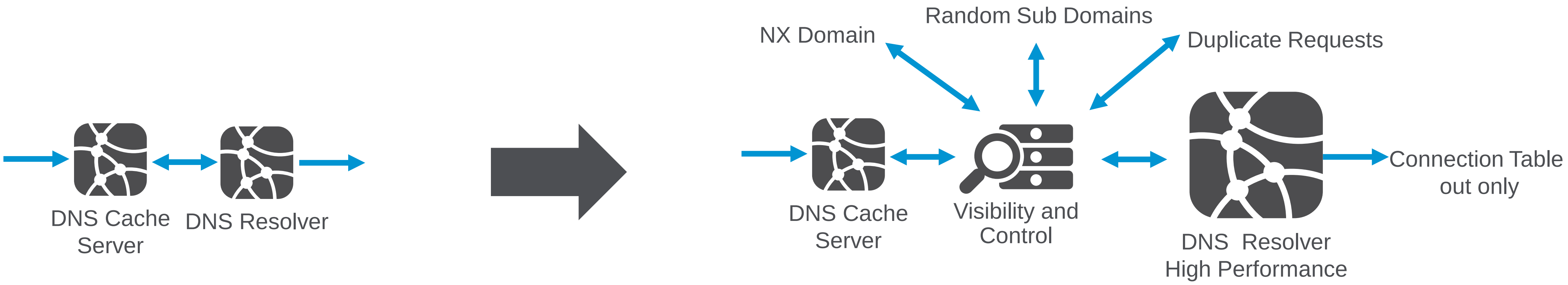
- Increases availability when under DDOS attack
- Maintains all Security Certifications
- Reduces single Point of failure and scrubs the common DNS attacks

DNS Resolver Performance and Security

Maximise cache hit ratio and protect the queue to the Resolver

Remove attacks and queue filling requests

Log users, Rate limit and quarantine on invalid requests



- Increases Performance for the Resolver (for valid requests)
- Maintains all existing deployment Architecture
- Reduces attacks internal and from external sources to increase up time,

Summary

Scaling and securing the DNS Cache/Resolver infrastructure

- Extend and Improve my existing DNS
- DNS Firewalling rather than a Firewall for a DNS server
- Transparent Cache Offload
- Per-Subscriber DNS-Based Security Services
- Mitigating against CVE’s and Bind
- Transparent Cache Security
- Protocol and tunneling abuse
- DDOS protection for existing DNS services
- DNS Resolver Performance and Security

Next Steps: Ensure Life blood to DNS Services

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