Global Service Loadbalancing & DNSSEC

Ralf Brünig
Field Systems Engineer
r.bruenig@f5.com
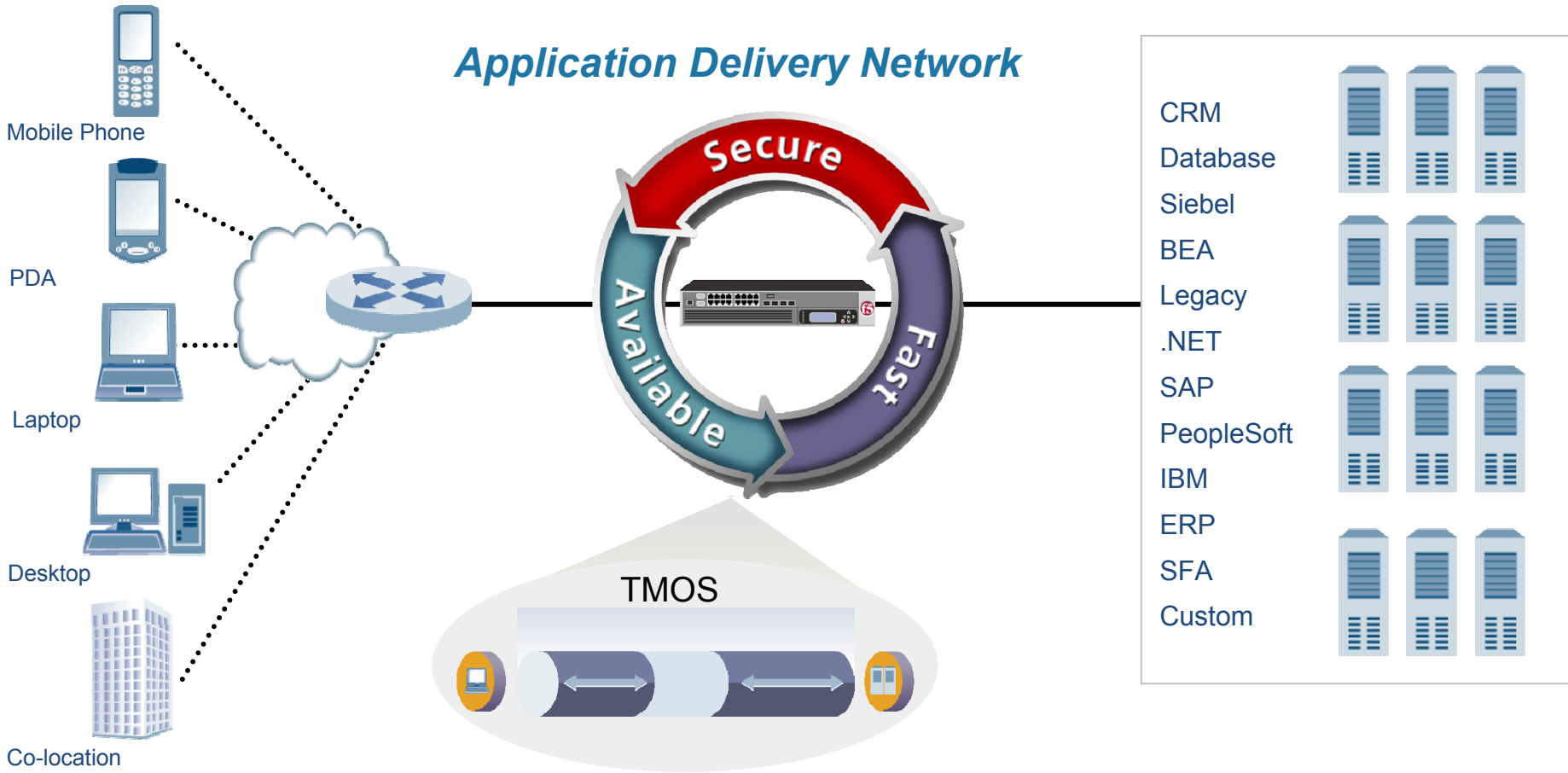
f5 ® IT agility. Your way.

F5's Integrated Solution

Users

The F5 Solution
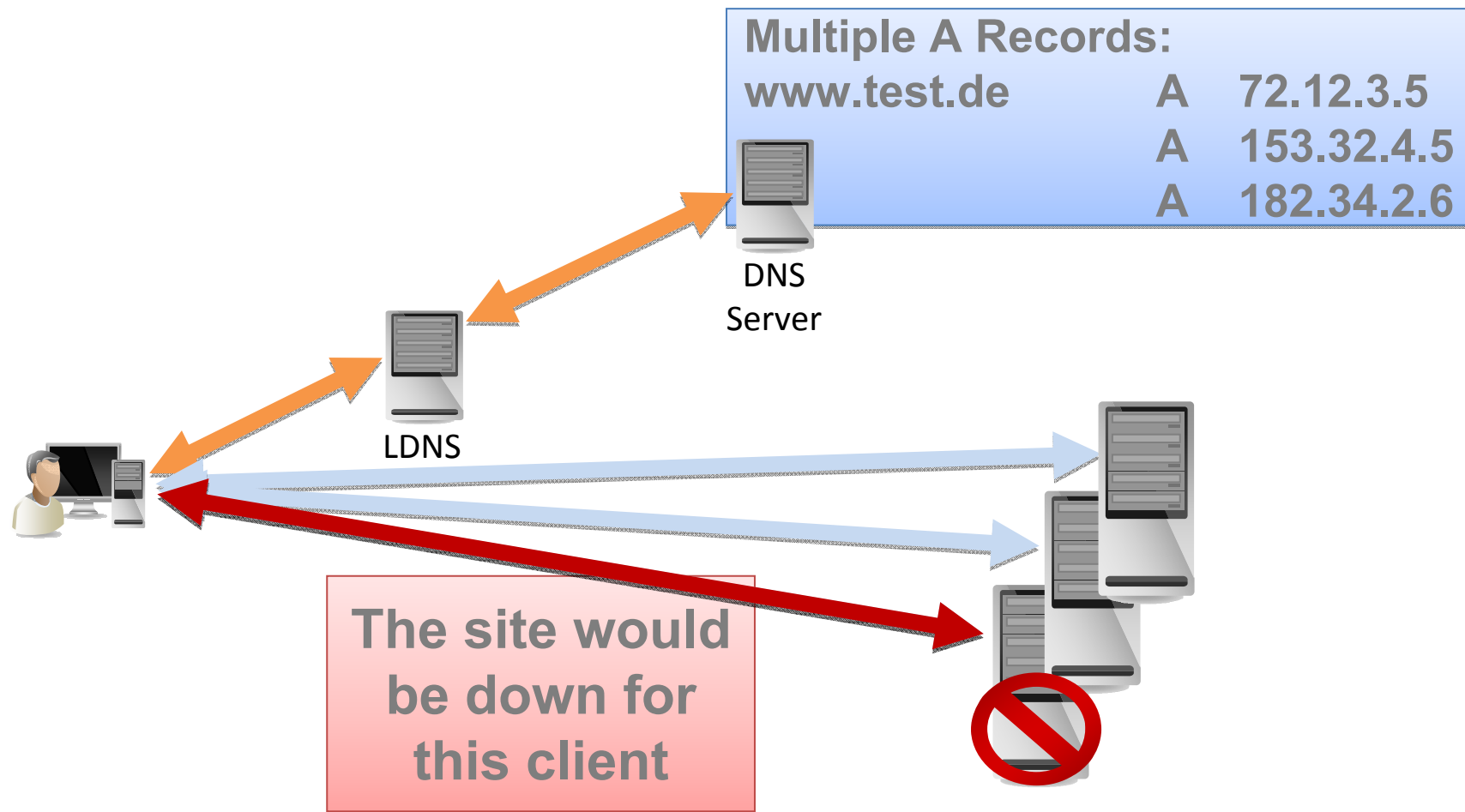
Applications

Application Delivery Network

Mobile Phone

PDA

Laptop

Desktop

Co-location

Secure

Available

Fast

TMOS

CRM
Database
Siebel
BEA
Legacy
.NET
SAP
PeopleSoft
IBM
ERP
SFA
Custom

Global Service Loadbalancing (GSLB)

Global Service Loadbalancing with bind
Multiple A record → Round Robin

Multiple A Records:

www.test.de	A	72.12.3.5
	A	153.32.4.5
	A	182.34.2.6

DNS
Server

LDNS

The site would
be down for
this client

Global Service Loadbalancing
Monitoring

- **ICMP**
- **TCP**
- **UDP**
- **HTTP**
- **HTTPS**
- **FTP**
- **SNMP**
- **IMAP**
- **POP3**
- **SMTP**
- **LDAP**
- **RADIUS**
- **MSSQL**
- **Oracle**
- **...**

Multiple A Records:

www.test.de	A	72.12.3.5
	A	153.32.4.5
	A	~~182.34.2.6~~

GSLB

This server would be taken out of the load balancing
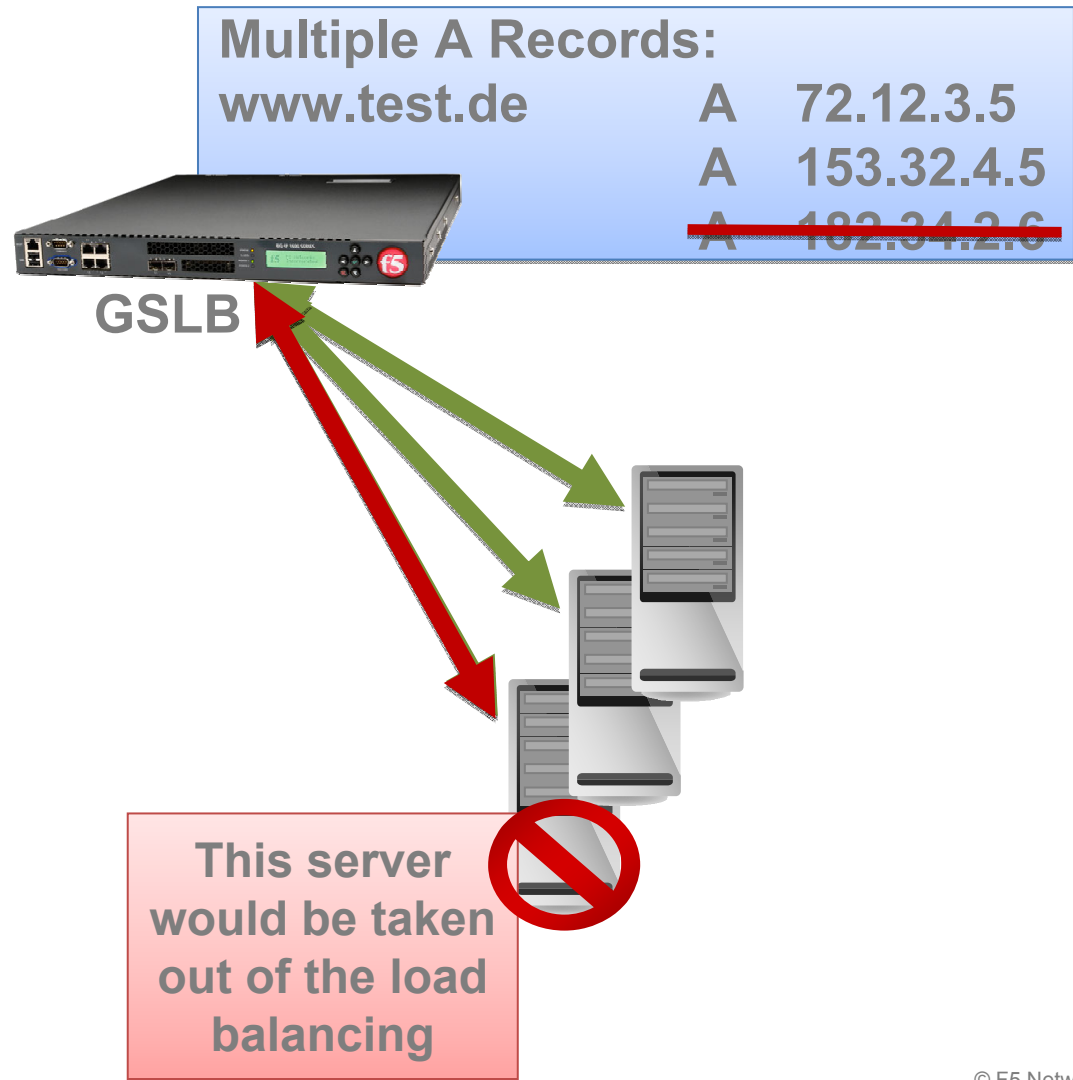
Global Service Loadbalancing
Load Balancing Method
→ The Art of selecting the right server

Resolver

- **Round Robin**
- **Ratio**
- **Global Availability**
- **Topology**
- **Round Trip Time**
- **Packet Rate**
- **...**
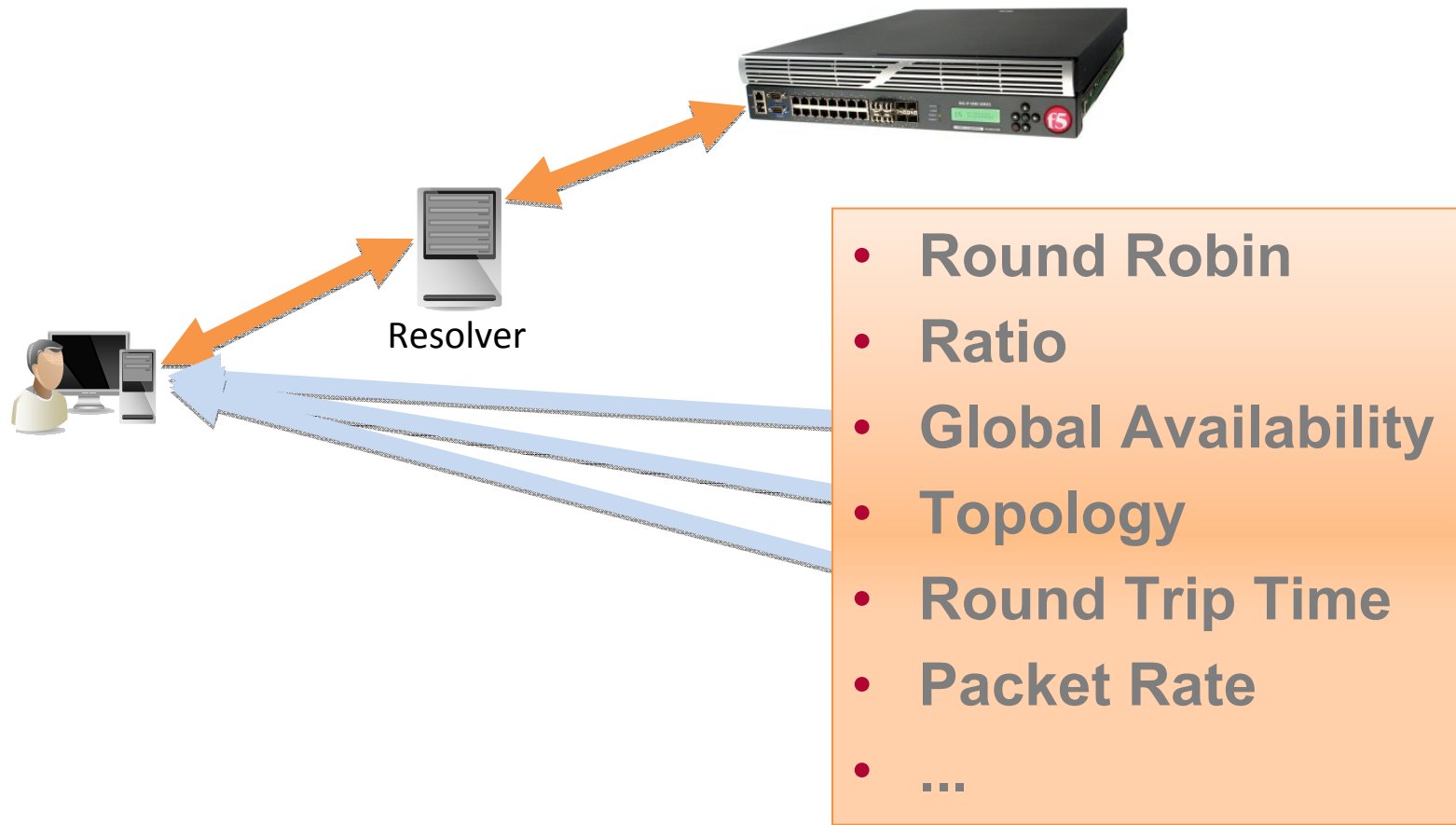
Directing Users to the Best Site

Large social networking site needs state-level control
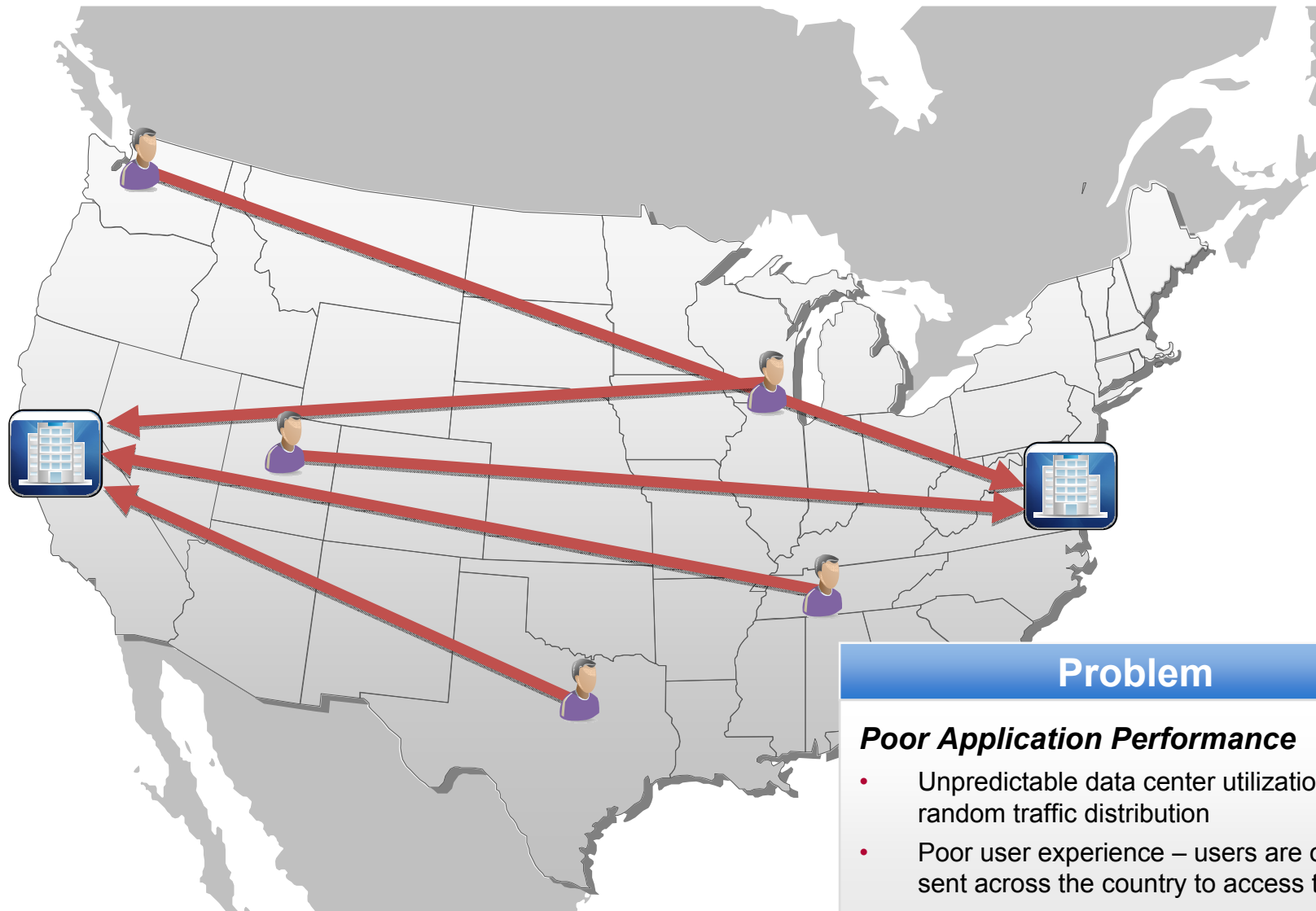
Problem

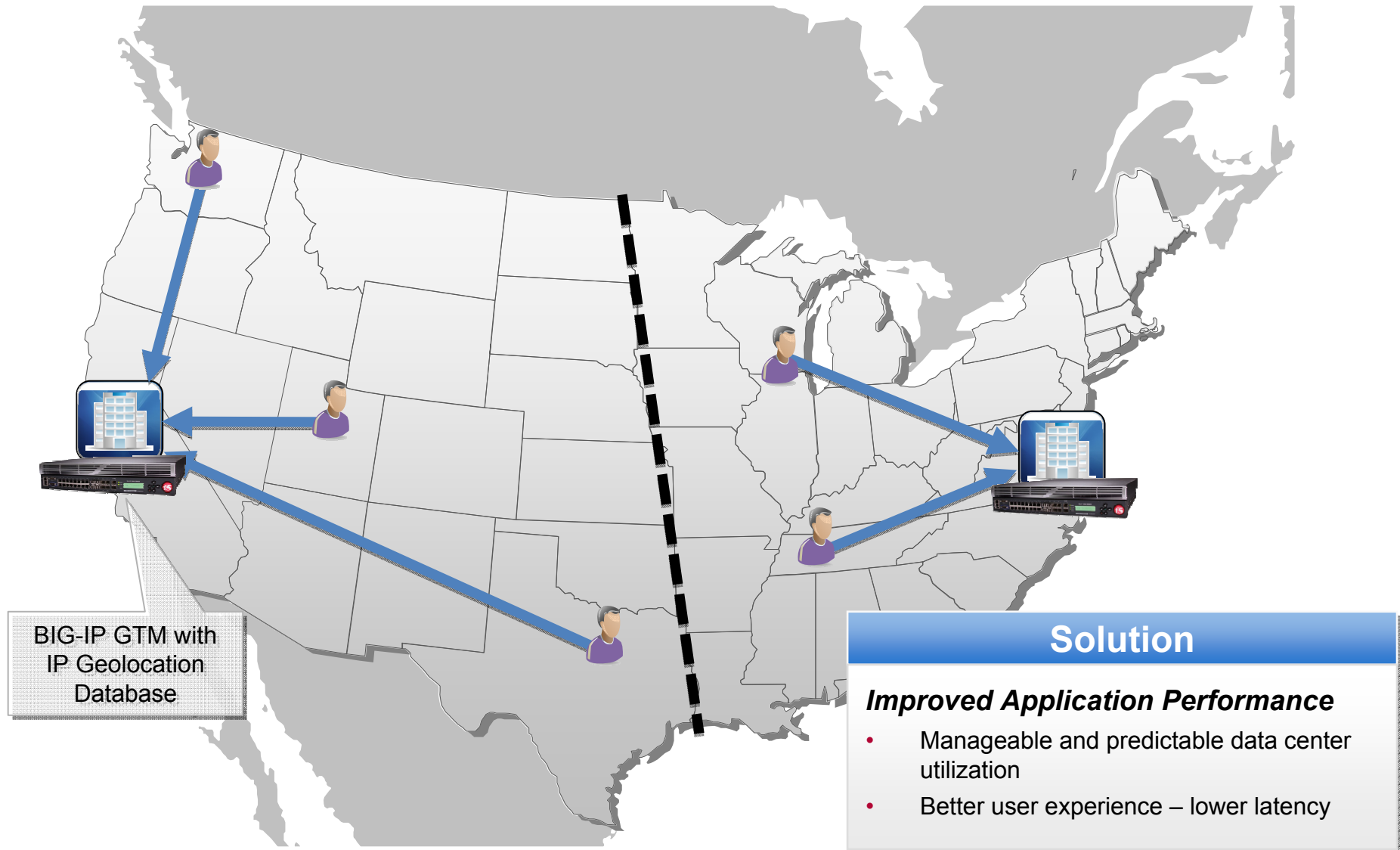### *Poor Application Performance*

- Unpredictable data center utilization – random traffic distribution
- Poor user experience – users are often sent across the country to access the site
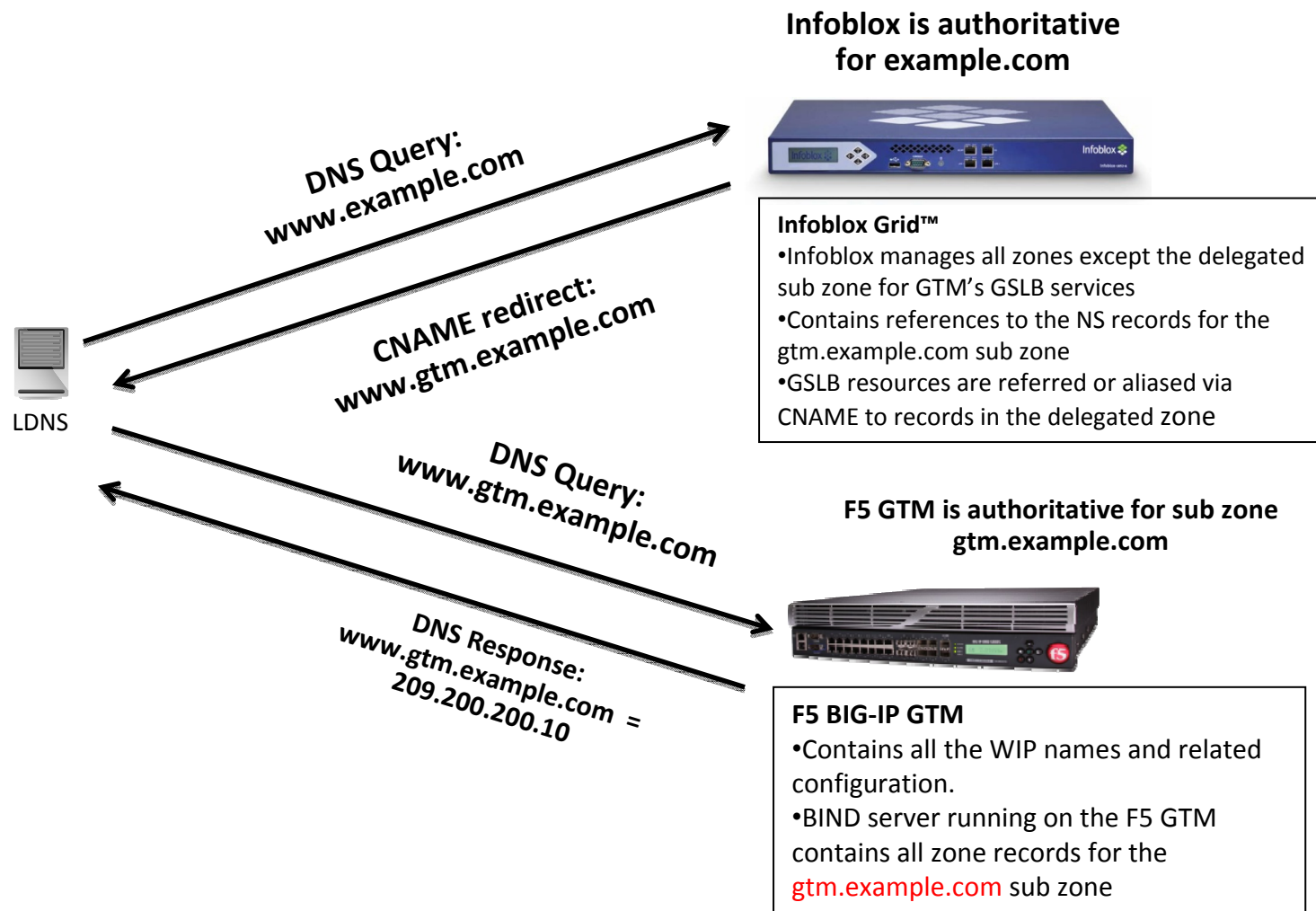
Directing Users to the Best Site
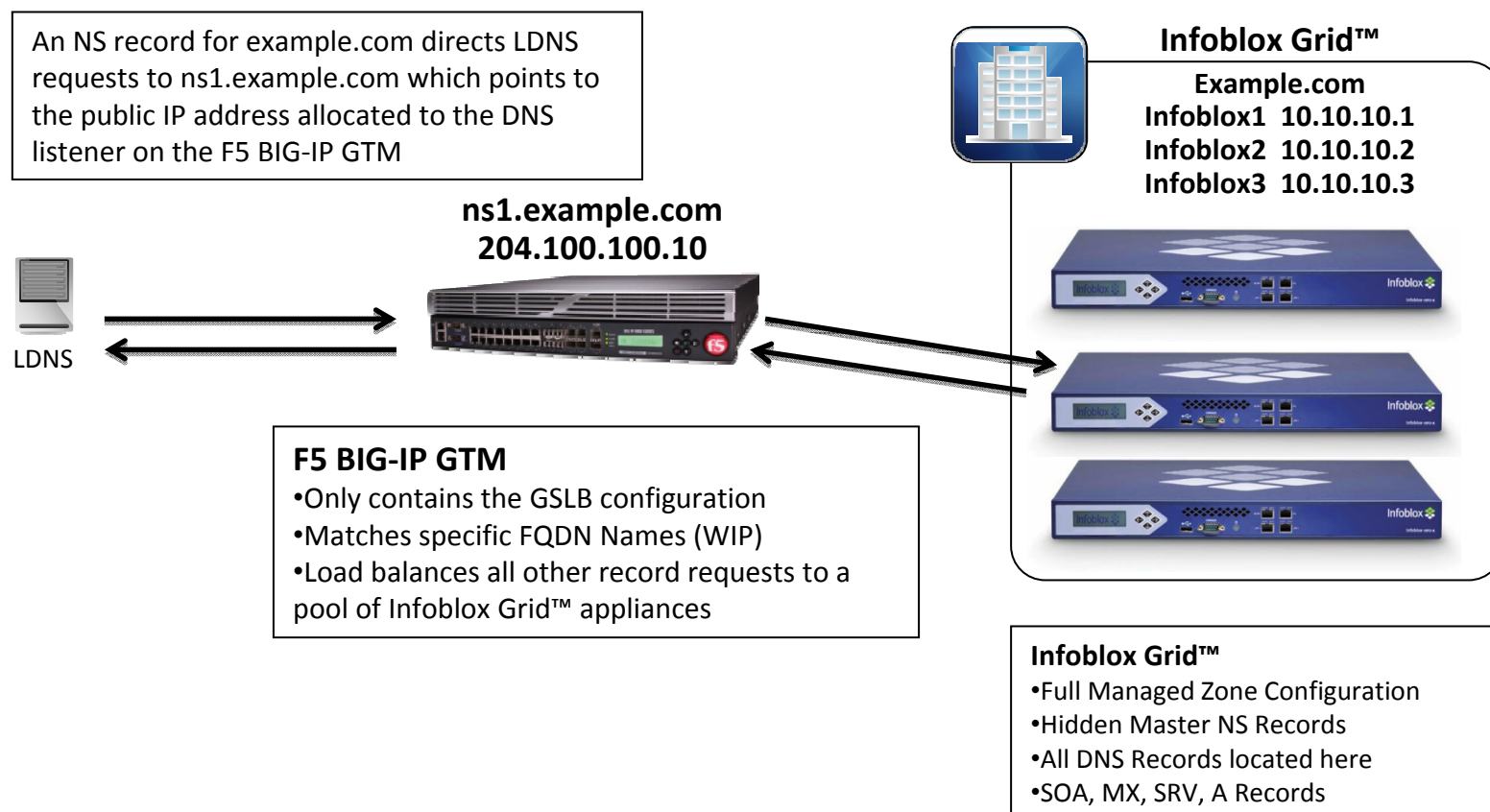
State level control improves end user experience

BIG-IP GTM with IP Geolocation Database

Solution

Improved Application Performance

- Manageable and predictable data center utilization
- Better user experience – lower latency

Integration Architectures
Delegation

Infoblox is authoritative for example.com

DNS Query:
www.example.com

CNAME redirect:
www.gtm.example.com

LDNS

DNS Query:
www.gtm.example.com

DNS Response:
www.gtm.example.com =
209.200.200.10

Infoblox Grid™
- Infoblox manages all zones except the delegated sub zone for GTM's GSLB services
- Contains references to the NS records for the gtm.example.com sub zone
- GSLB resources are referred or aliased via CNAME to records in the delegated zone

F5 GTM is authoritative for sub zone gtm.example.com

F5 BIG-IP GTM
- Contains all the WIP names and related configuration.
- BIND server running on the F5 GTM contains all zone records for the gtm.example.com sub zone

Integration Architectures
Authoritative Screening

An NS record for example.com directs LDNS requests to ns1.example.com which points to the public IP address allocated to the DNS listener on the F5 BIG-IP GTM

Infoblox Grid™

Example.com
Infoblox1 10.10.10.1
Infoblox2 10.10.10.2
Infoblox3 10.10.10.3

ns1.example.com
204.100.100.10

LDNS

F5 BIG-IP GTM
•Only contains the GSLB configuration
•Matches specific FQDN Names (WIP)
•Load balances all other record requests to a pool of Infoblox Grid™ appliances

Infoblox Grid™
•Full Managed Zone Configuration
•Hidden Master NS Records
•All DNS Records located here
•SOA, MX, SRV, A Records
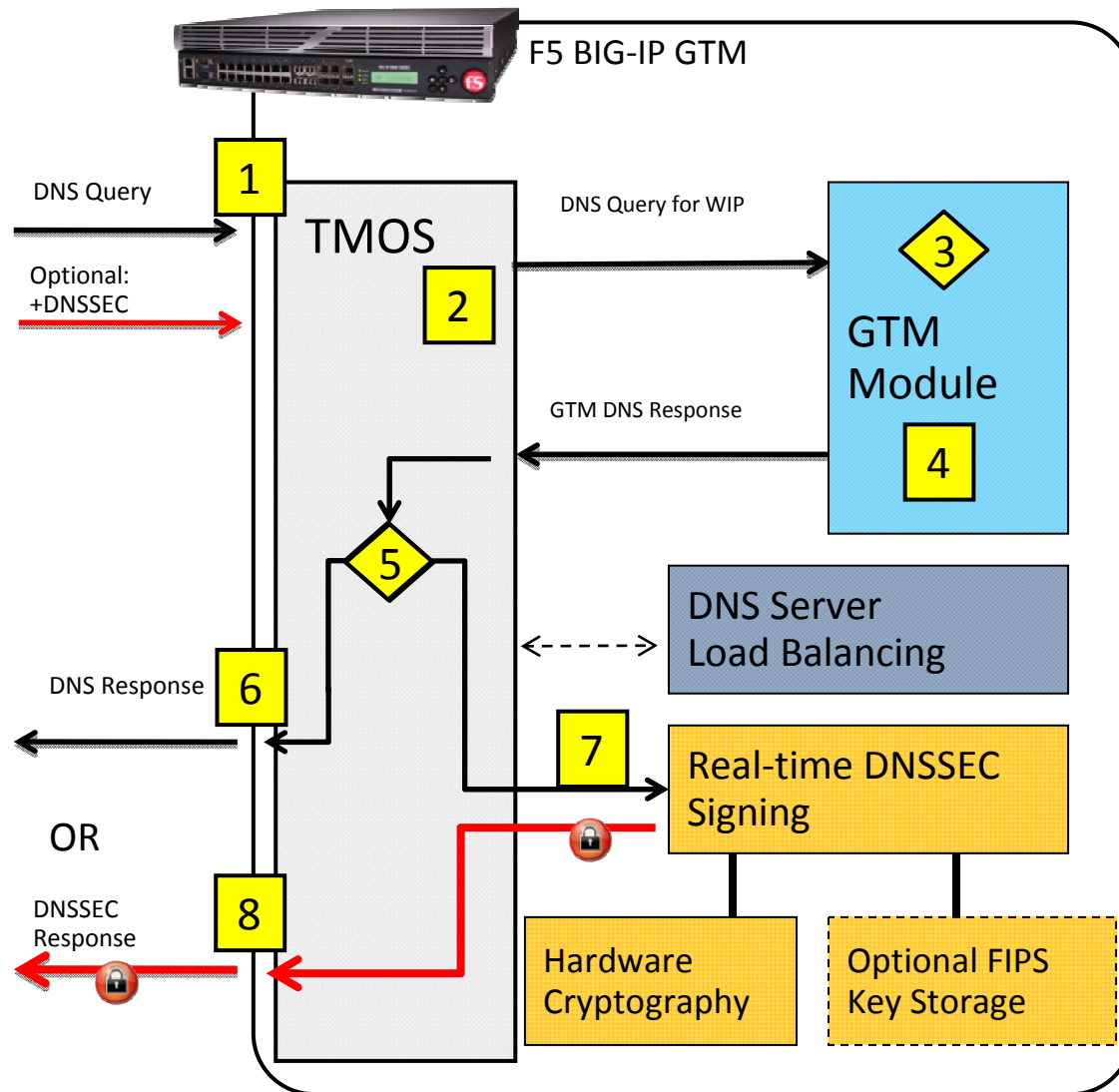
DNSSEC

f5® IT agility. Your way.

How big an issue is this?

Has your organisation been a victim
of a DNS poisoning attack in the past year?
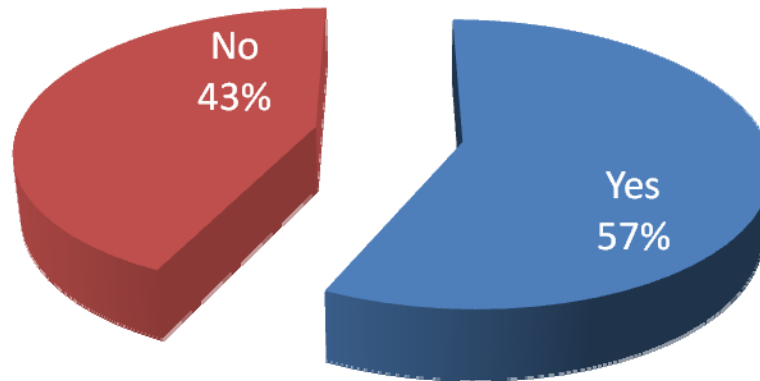
Nearly half of those answering "yes" report
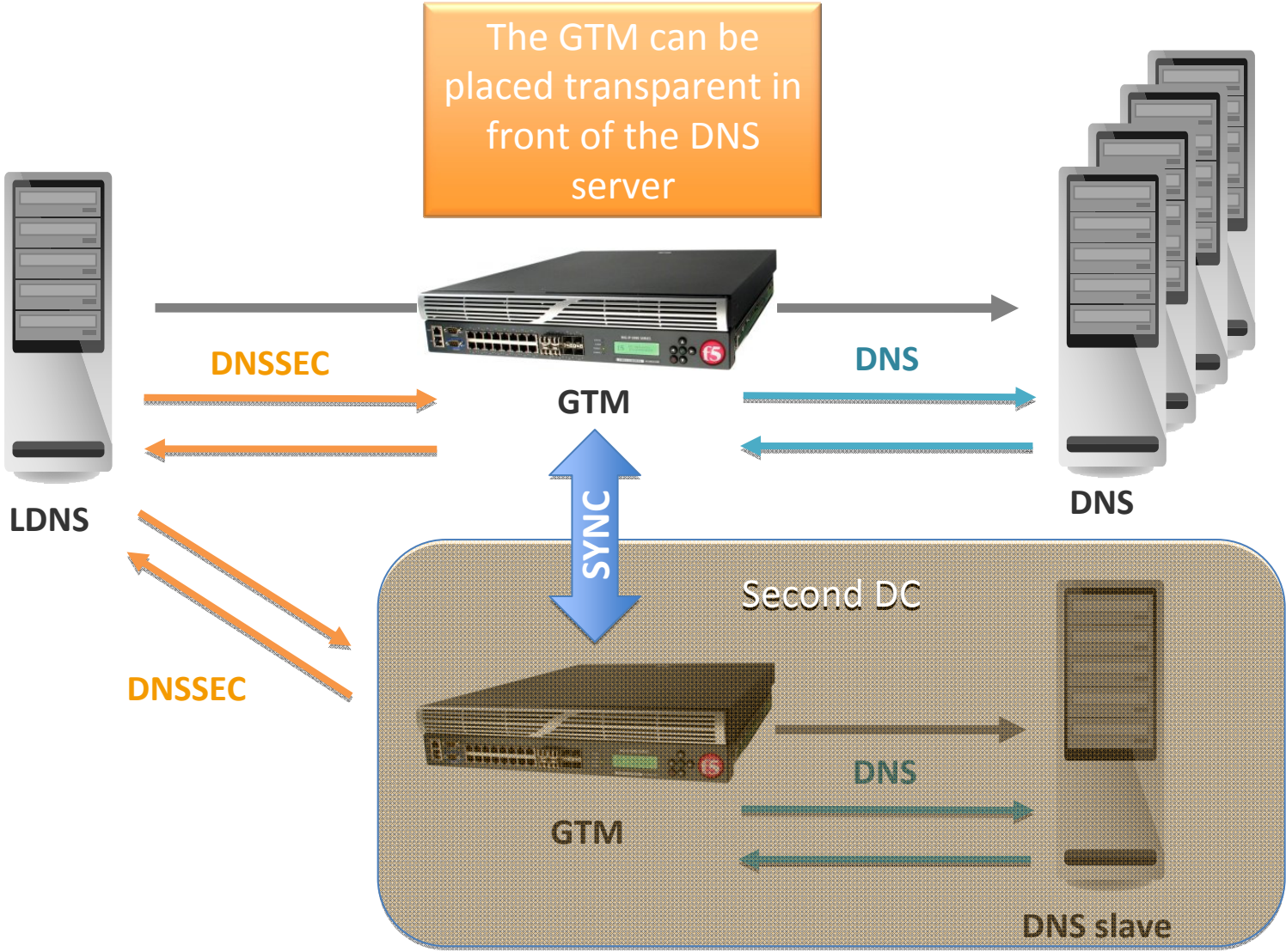monthly occurrences of such attacks

Source: Center for Strategic and International Studies

Solution: Real-time DNSSEC Signing

F5 BIG-IP GTM

TMOS

1 DNS Query

2 Optional: +DNSSEC

DNS Query for WIP

3 GTM Module

GTM DNS Response

4

5

DNS Server Load Balancing

6 DNS Response

7 Real-time DNSSEC Signing

8 OR

DNSSEC Response

Hardware Cryptography

Optional FIPS Key Storage

F5 Patent Pending

Request Processing:

1. TMOS receives request on the DNS listener IP
2. TMOS sends request to GTM module
3. GTM applies GSLB rules
4. GTM returns response
5. TMOS checks if original request included +DNSSEC
6. If a normal DNS request, TMOS responds normally
7. If a DNSSEC request, TMOS signs the response
8. DNSSEC Response

GTM – DNSSEC Integration

The GTM can be placed transparent in front of the DNS server

LDNS

DNSSEC

GTM

DNS

DNS

SYNC

DNSSEC

Second DC

GTM

DNS

DNS slave

F5 DNSSEC Configuration

1. Create the key signing key (KSK)
2. Create the zone signing key (ZSK)
3. Create the DNSSEC zone and assign the KSK and ZSK keys
4. Send public KSK to parent zone authority
5. Repeat step 3 to sign additional DNSSEC zones
6. Key management operations automated by policy

Automatic Key Rollover

Key Expiration Period

Key Rollover Period

Generation 0

Generation 1

Generation 2

overlap

t

Generation 0 Rollover Date @ t_1

Generation 0 Expiration Date @ t_2

Generation 0 reaches its rollover date causing mcpd to create Generation 1. They will necessarily overlap for the difference between Generation 0's rollover and expiration date.

Generation 0 reaches expiration date and is removed from the configuration by mcpd, while Generation 1 carries on.

Links

- http://www.f5.com/solutions/security/dnssec/
- http://www.f5.com/news-press-events/web-media/webcasts/deploying-dnssec.html

- http://devcentral.f5.com/weblogs/dctv/archive/2010/01/11/secure-dns-with-big-ip-v10.1-dnssec.aspx

- http://www.practicesafedns.org/

IT agility. Your way.