



The evolving Business needs for DNS

Nigel Ashworth

Solution Architect EMEA



What is DNS “Domain Name
Services”

Your Phone, Address Book for your
business applications

Loose your Phone, Address Book
Is

Loosing your Business
Applications

How important is DNS to the business.



Business Analyst

- What is the Risk to the Business
 - Probable and Likely = High Risk Factor
 - How does this affect the corporate KPI's
- What is the relationship of Brand to DNS services in the Media



Infrastructure / Security Manager

- What attacks can we mitigate
- Are we deploying best practice architectures for the lines of business
- Are we in compliance from vulnerabilities
- How do you measure the value of the service to the business lines



Systems Administrator

- Is Bind the way Forward
- How do we provide mitigation to our existing DNS services
- How do we implement a best practice DNS Firewall
- What types of attack can we mitigate against

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

The evolving Business needs for DNS and its Use Cases

The Use cases that we
commonly deploy with customers

Extend and Improve my
existing DNS

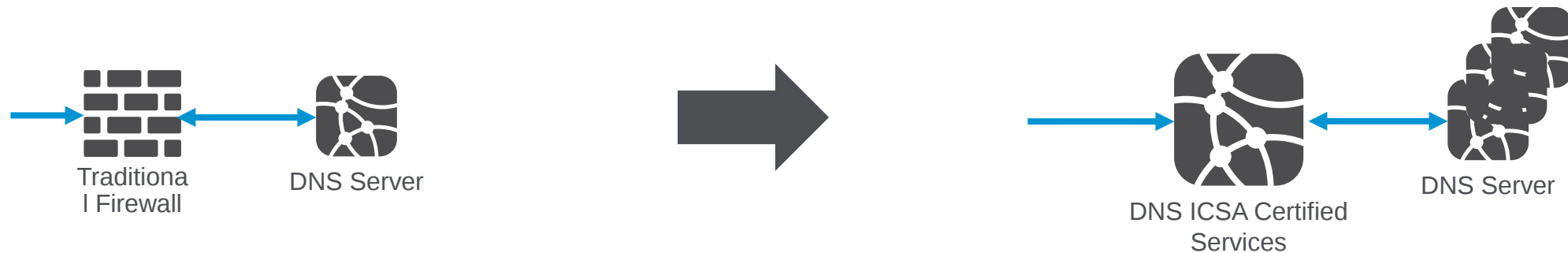


What can I do to Extend and Improve my existing DNS services

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 the traditional firewall limitations

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

Cache Offload

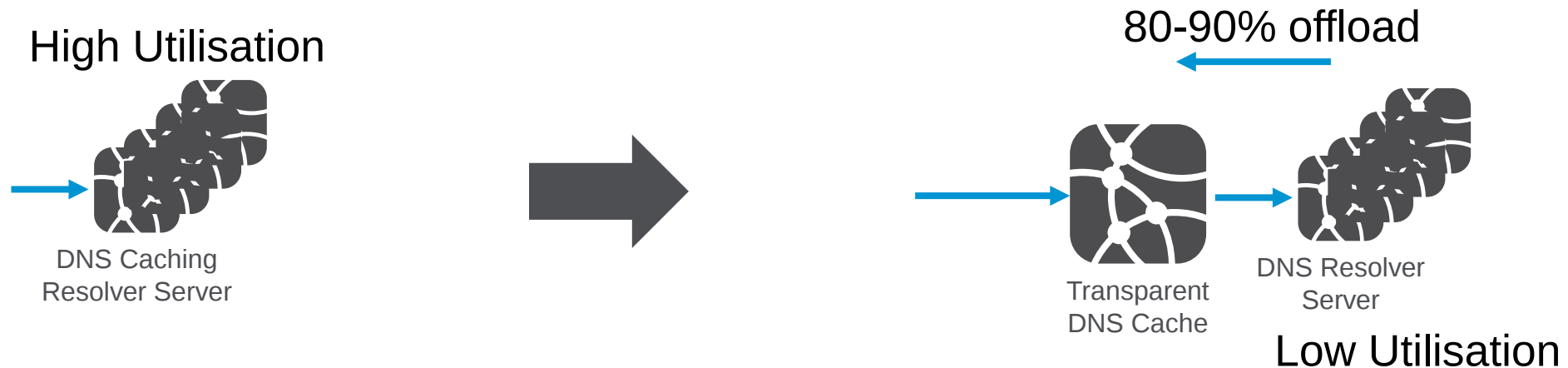


Transparent Cache Offload

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

Per Subscriber Management



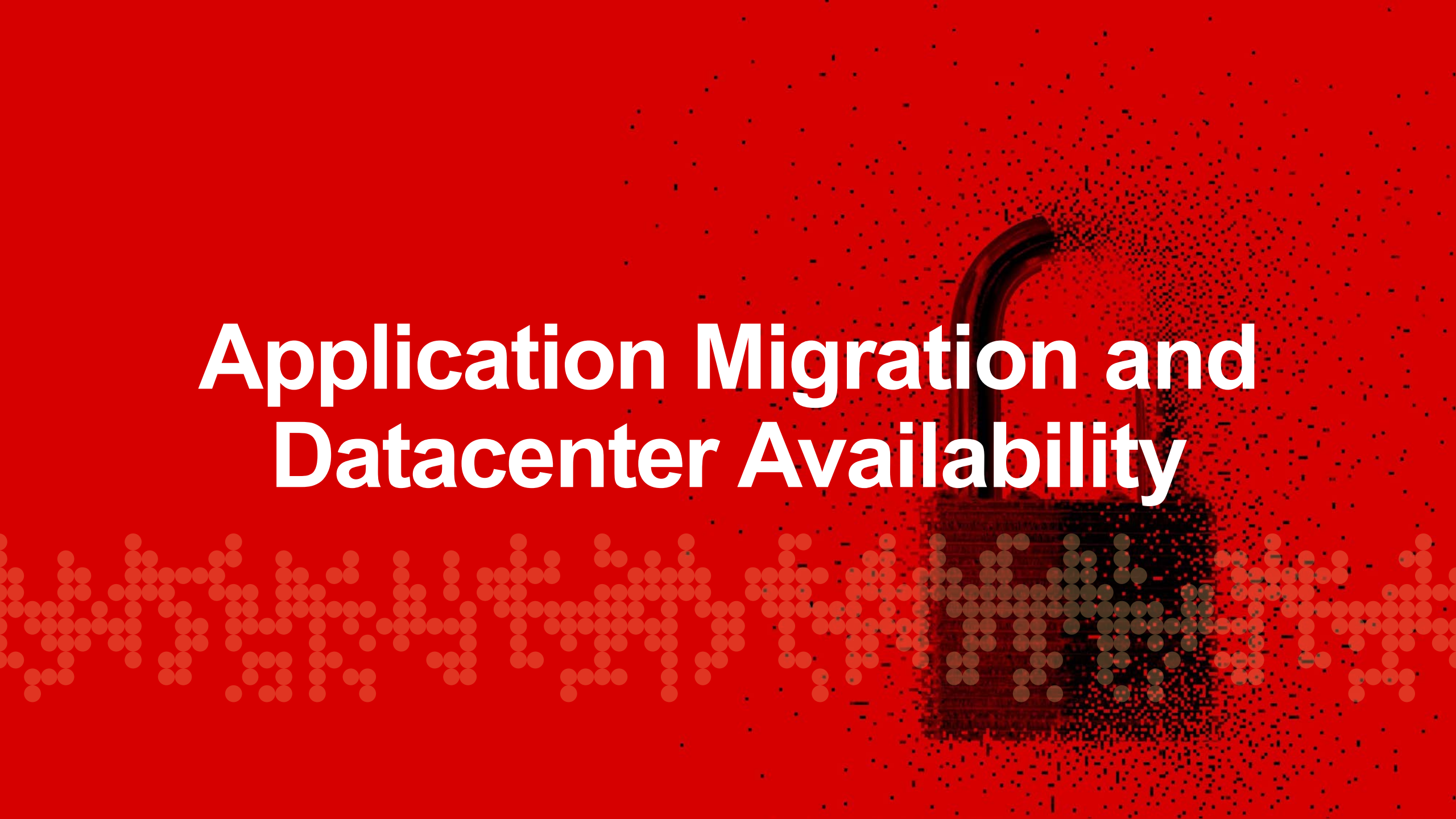
Per Subscriber Management

As an option to remove web sites that are categorised as unsuitable viewing
Identify unsuitable categories by governmental and industry classified (by age / content)
Alert / quarantine / block users by user account attributes or by provided user lists



- Increases security for vulnerable users and open up revenue opportunities
- Maintains responses and performance for users
- Reduces unwanted content and brand association to sites

Application Migration and Datacenter Availability

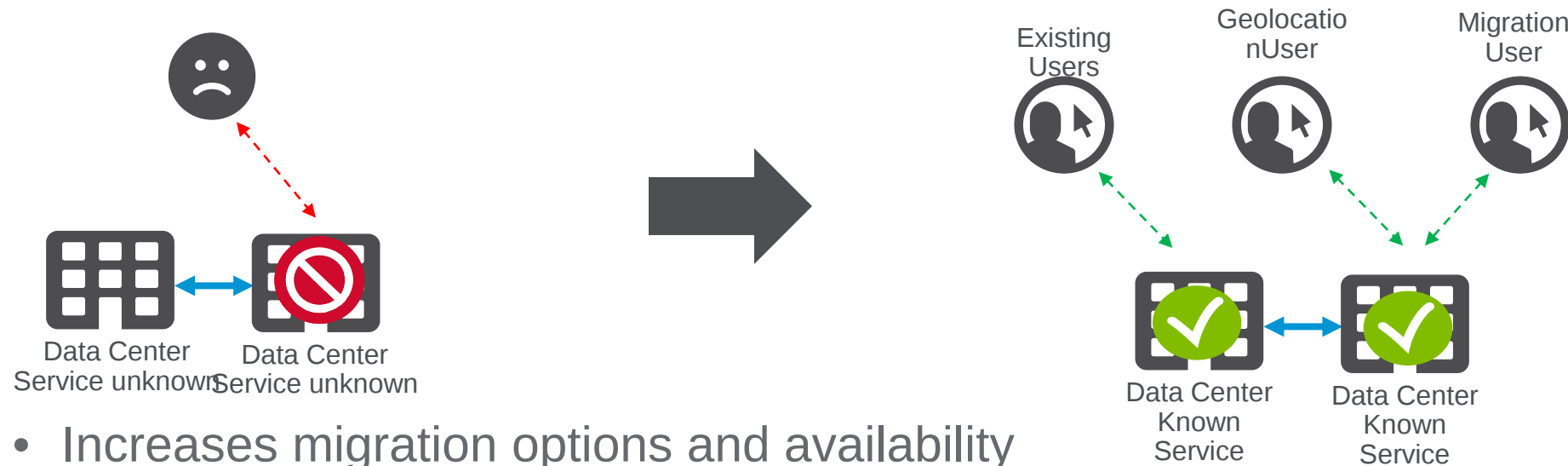


Application Migration and Datacenter Availability

To move services from one datacentre another without impacting user experience

Health management of services for migration

Pre test, group or Geolocation migration and No big bang migration,



- Increases migration options and availability
- Maintains all Services whilst migrating
- Reduces migration risk to the business

Mitigating against CVE's and Bind

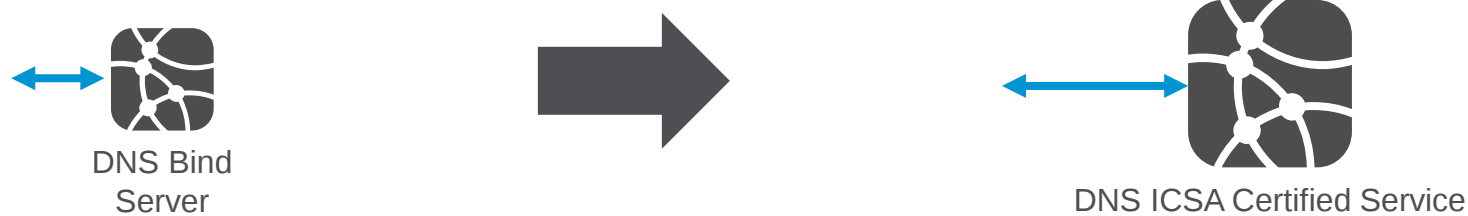


Mitigating against CVE's and Bind

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



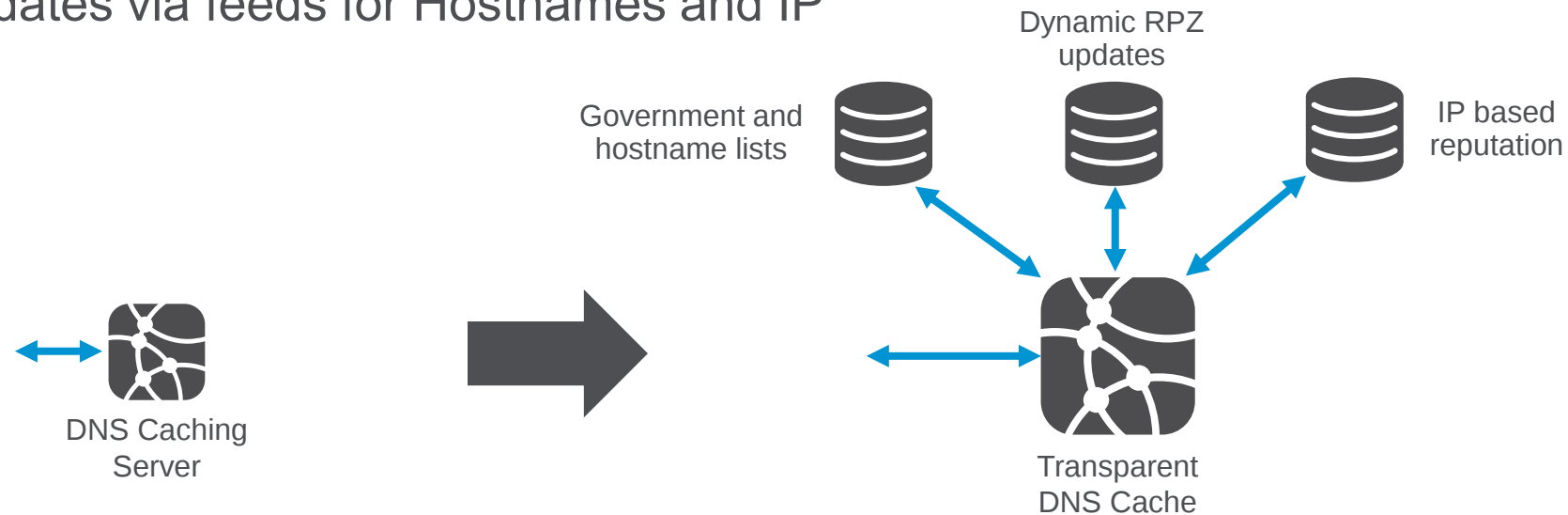
- Increases security, scale and certification
- Maintains features of existing deployments
- Reduces OPEX by removing vulnerability due to the Bind CVE's

Cache Security



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

Authoritative DNS

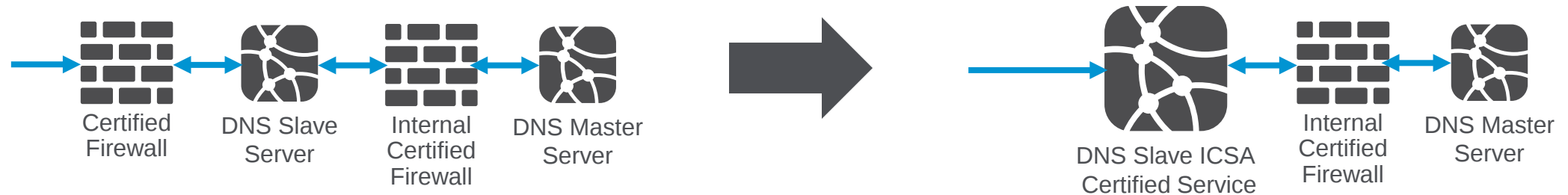


Authoritative DNS

When under attack Traditional Firewalls do not provide security and fail before the DNS servers

Remove Bind services and complement with scalable High speed slave

Implement security certification / compliance and consolidate



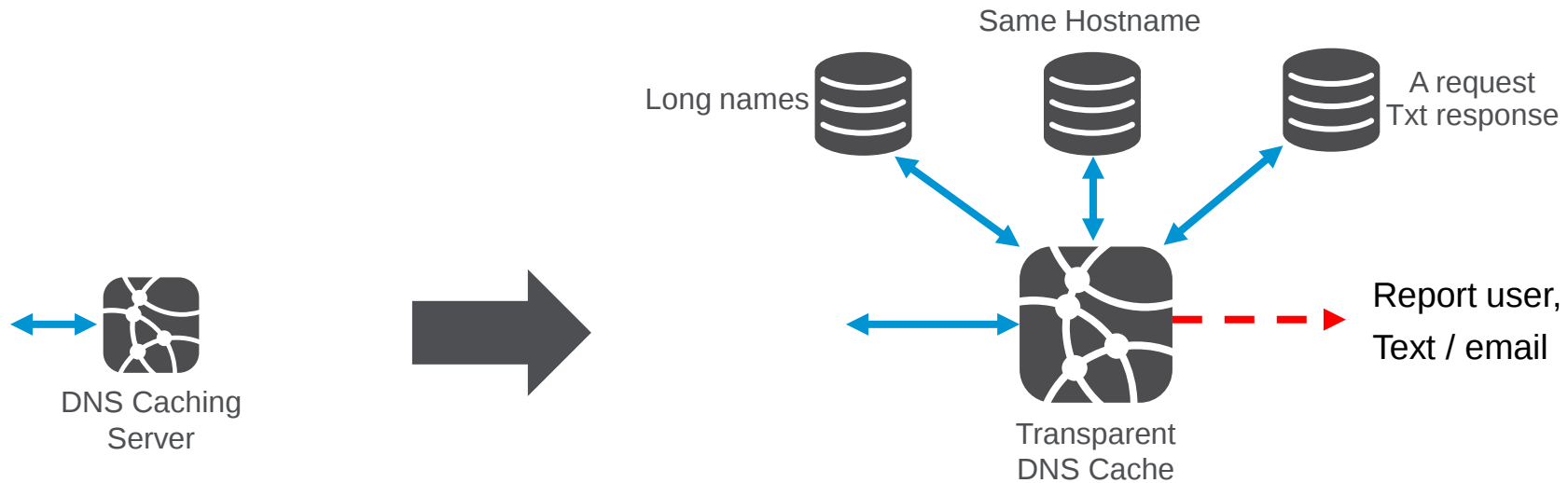
- Increases availability when under attack, and massive scalability
- Maintains all current DNS Master configurations and processes
- Removes single point of failure

Protocol and tunneling abuse



Protocol and tunneling abuse

Take charge of users / applications that would take advantage of the DNS protocol
Identify DNS requests that do not match the RFC's, or are streams
Alert / Quarantine / Block / Report users that are abusing the DNS protocol



- Increases revenue by removing free loaders
- Maintains valid users traffic
- Reduces abuse and reports violations,

DDOS protection for existing DNS services

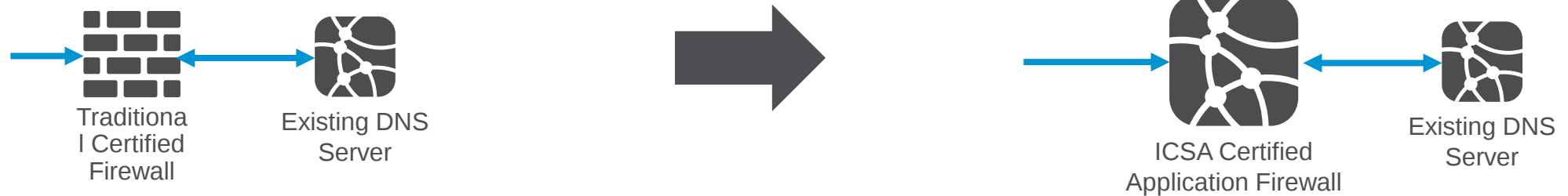
A red padlock with a black handle is positioned on the right side of the image. The background is black with a pattern of red dots of varying sizes, some of which are arranged in a grid-like pattern around the padlock. The text "DDOS protection for existing DNS services" is written in white, bold, sans-serif font across the center of the image.

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

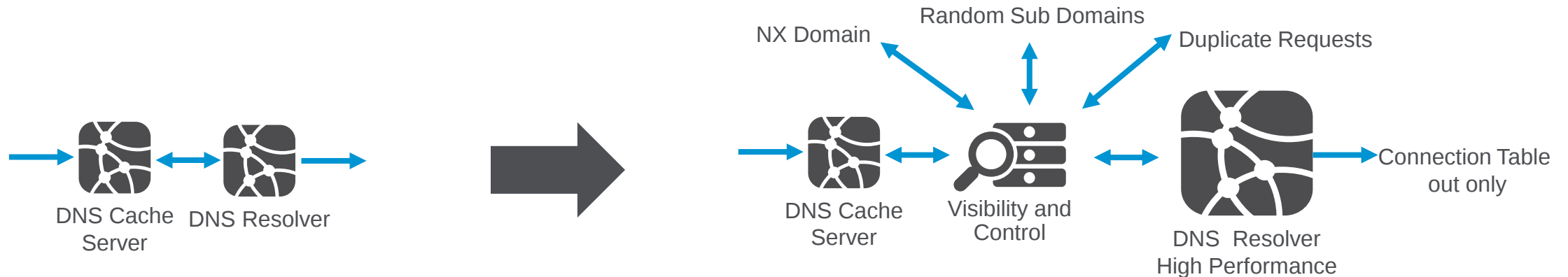


DNS Resolver Performance and Security

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,

GGSN and PGW availability

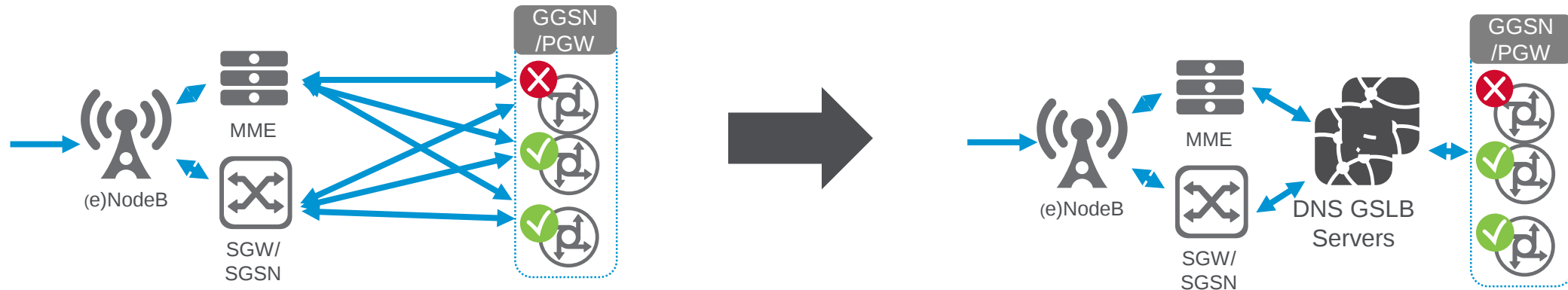


GGSN and PGW availability

Dynamically choose gateways based on availability

Monitor the Health of gateways

Gateway selection based on location and availability

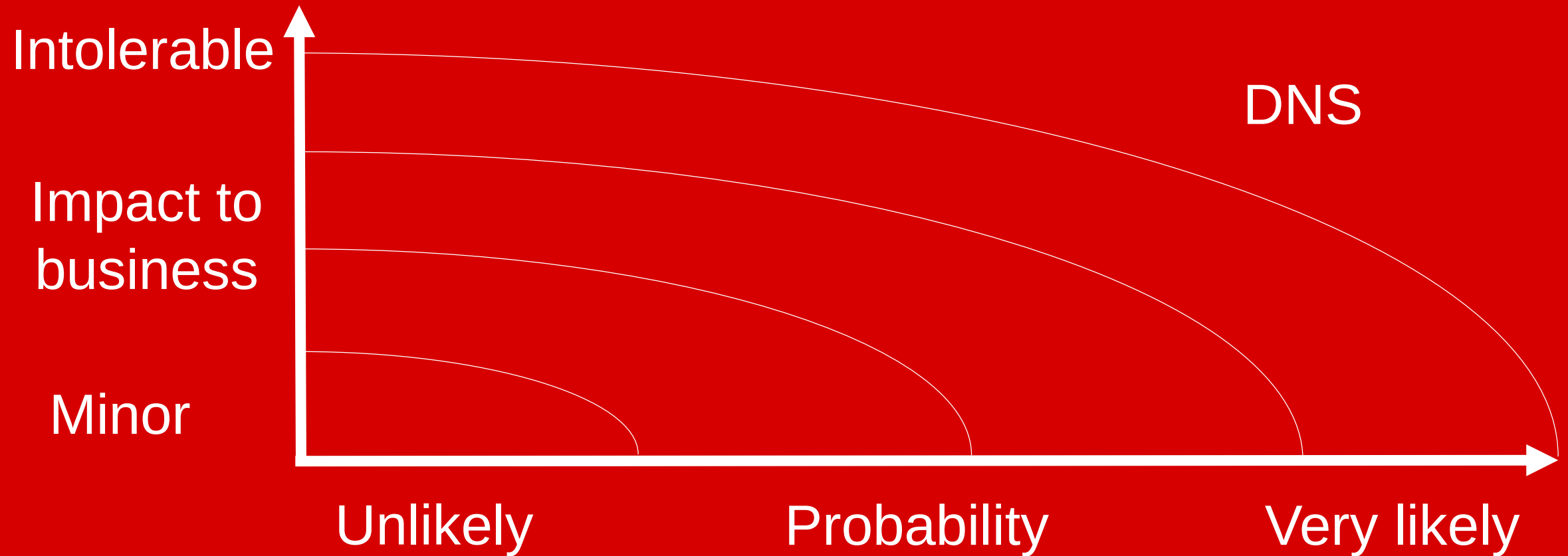


- Increases availability and scalability for gateway services
- Maintains all current DNS configurations
- Removes single point of failure and manual configurations

Use Cases:

- Extend and Improve my existing DNS
- DNS Firewalling rather than a Firewall for a DNS server
- Transparent Cache Offload
- Per Subscriber Management
- Application Migration and Datacenter Availability
- Mitigating against CVE's and Bind
- Transparent Cache Security
- Authoritative DNS
- Protocol and tunneling abuse
- DDOS protection for existing DNS services
- DNS Resolver Performance and Security
- GGSN and PGW availability

DNS Risk Management



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

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