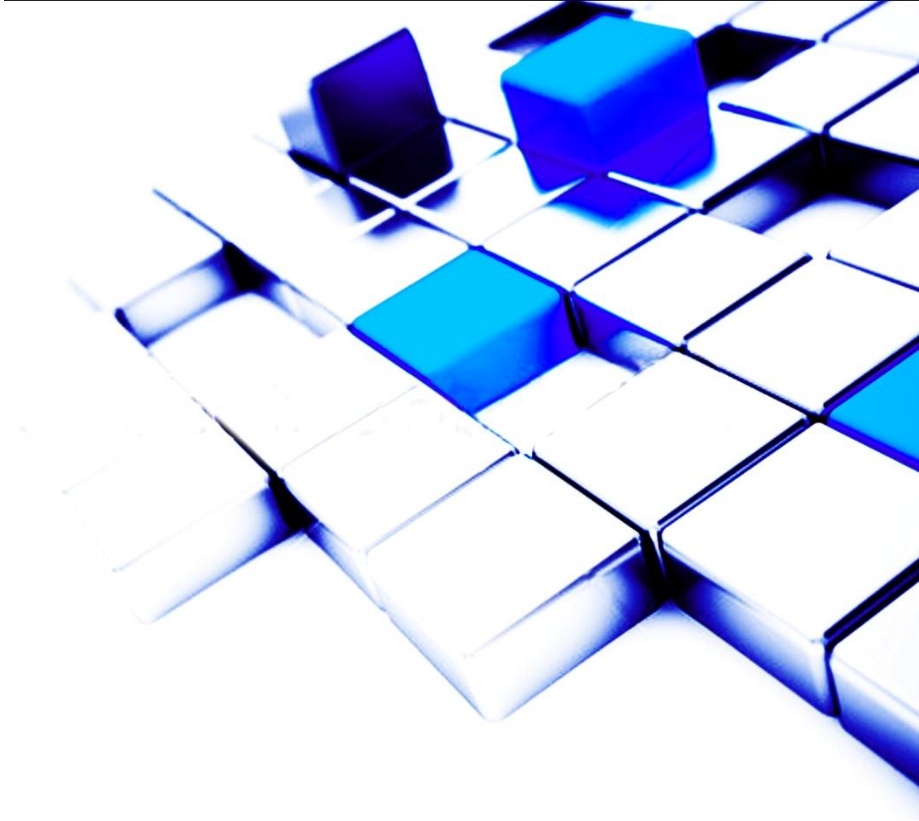
Protecting External DNS servers against attacks



efficient iP™

the global IPAM company

Agenda

- Introduction & Reminders to DNS
- DNS Attacks and Vulnerabilities
- Prevention & Best Practices
- State-of-the-art Stealth DNS SMART Architecture
- DNSSEC

Introduction & Reminders to DNS

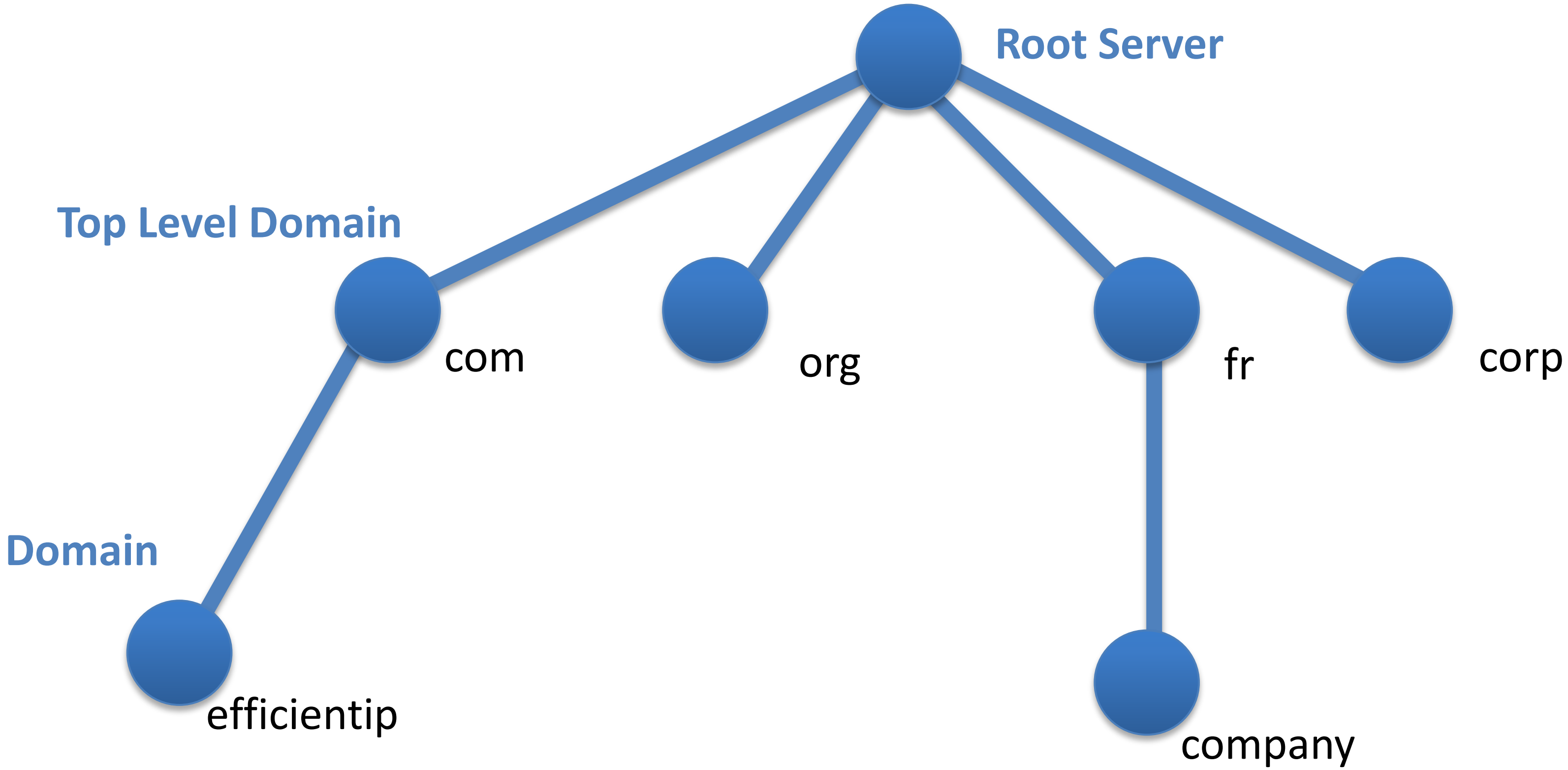
Why is DNS is so critical ?

DNS is a nice target for hackers

- All Internet applications rely on DNS
- DNS is invisible to end users
- DNS is considered as reliable and highly available
- DNS is concentrated on one or two servers, and can be cached on almost every Internet DNS servers.

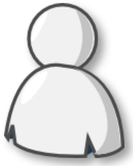
Internet DNS Architecture

The Domain Name System is a hierarchical and distributed database



Internet DNS Architecture

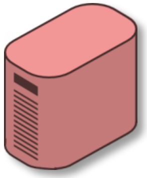
- Components
  - Stub Resolver (client)
  - DNS Recursive Resolver
  - Caching Name Server
  - Authoritative Name Server



DNS client

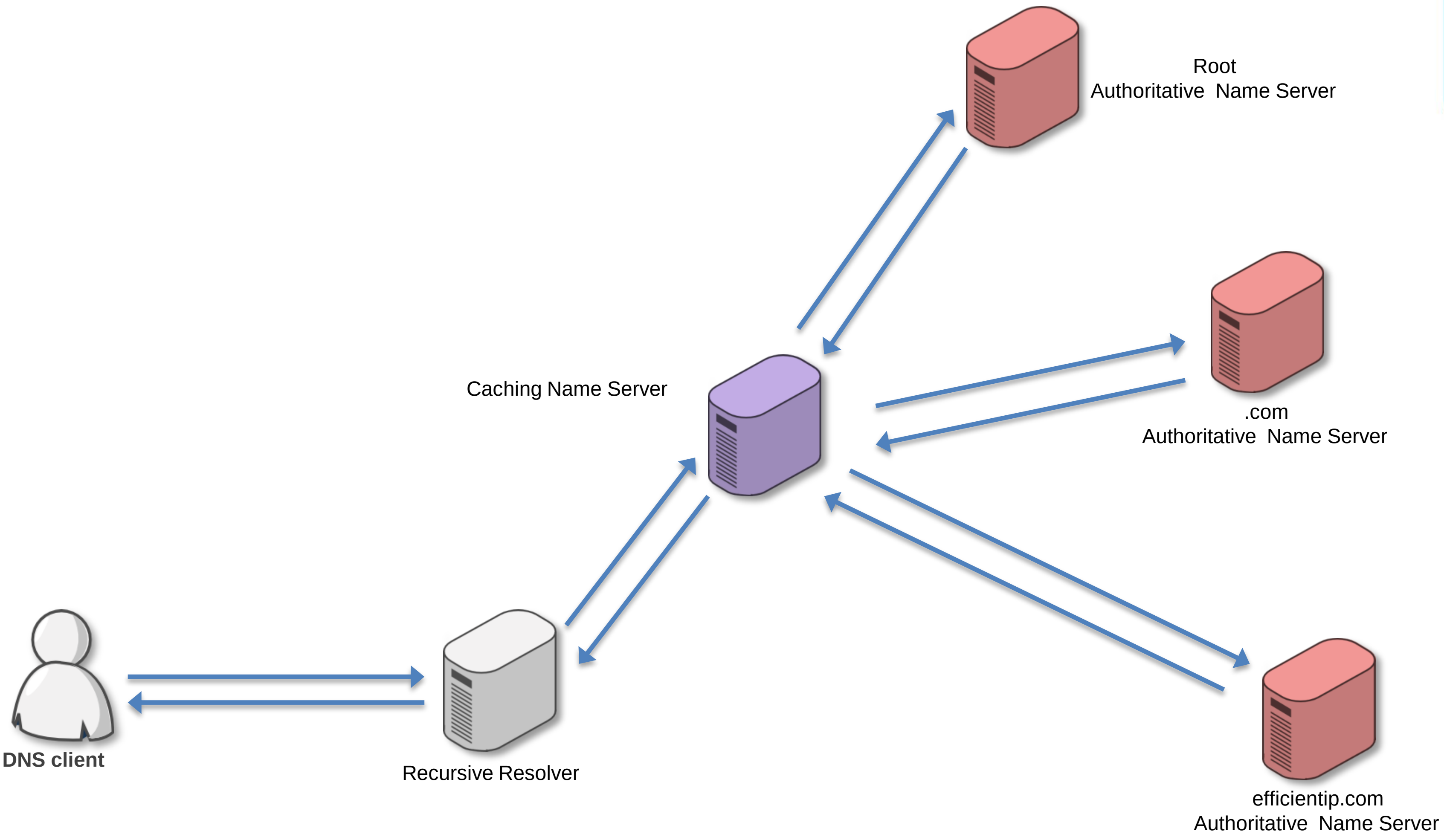
Recursive Resolver

Caching Name Server



Authoritative Name Server

Internet DNS Architecture


Root
Authoritative Name Server
Caching Name Server
.com
Authoritative Name Server
DNS client
Recursive Resolver
efficientip.com
Authoritative Name Server

DNS Attacks and Vulnerabilities

Two ways DNS hacking

- By using the protocol attacks
  - DNS protocol failure and limitation.
- By using the attacks based on the DNS implementation
  - Attacks based on bugs or flaws of the programs (including the DNS engine).
  - Attack based on the OS hosting the DNS server.
  - Attack based on the architecture including the network and the OS.

DNS Attacks & Vulnerabilities

- Denial of Service
  - Harm and block DNS traffic
- Data Modification
  - Query/Request Redirection
  - DNS cache poisoning
  - DNS ID hacking
- Zone Enumeration
- Tunnels

Denial of Service (DoS)

- DNS is an effective DOS attack vector for a few reasons:
  - DNS usually uses the UDP as its transport.
  - Most of autonomous systems allow source-spoofed packets to enter their network.
  - There is a lot of Open DNS Resolvers on the Internet.
- Type of Attacks to block DNS from responding
- Overload the system by using:
  - DNS reflectors, amplification, botnet
  - DDOS, recursive malformed requests, impersonation

Data Modification

- Query/Request Redirection
  - Using Man-In-the-Middle position
  - Break of the chain of trust
- DNS Spoofing
  - forge a fake answer
- DNS ID Hacking
  - succeed in impersonating a DNS server
- DNS Cache Poisoning
  - Sending user to malicious site
  - Famously known with the Kaminsky bug

Zone Enumeration

- Not really considered as an attack
- Most considered as a threat as it allows attackers to gather information
- Precedes an attempt at an attack

Tunnels

- Uses DNS TCP transport mechanism
- DNS TCP is used for
  - Failover transport: switch from UDP to TCP
  - Secondary zone transfer
  - DNSSEC and IPv6 traffic
  - EDNS is often badly supported by customer network
- Attacks use TCP channel to tunnel other protocol and run malicious software

Prevention & Best Practices

Prevention

- Use Best Practices configurations
  - Run software in secure environment
  - Identify data flow
  - ACLs
  - Stealth Architecture
- Enable DNSSEC
- Monitor DNS Traffic
  - Short term analysis (peak detection)
  - Long term analysis (abnormal behavior)

Server Secure Environment

- Running up-to-date software version
- Check that the Operating System is also having all security fixes!
- EfficientIP comes into an appliance format with a single upgrade process that updates:
  - Operating System
  - Services
  - Software

Secure Environment

- Data Flow Identification
- The server that you will be running is:
  - Caching server?
  - Resolver?
  - Authoritative?
- Separate the functions as possible.
- Disabling unwanted features will help into preventing attacks! *A public authoritative server should never be recursive.*

Access Control List

- ACLs are used to control what information will be published
- With Data Flow Identification, you can choose who will be able to:
  - Allow query (server and zone level)
  - Allow query cache (server level)
  - Allow transfer (server and zone level)
  - Allow update (zone level)
  - Blackhole (server level)
  - Negative Cache (zone level)

State-of-the-art Stealth DNS SMART Architecture

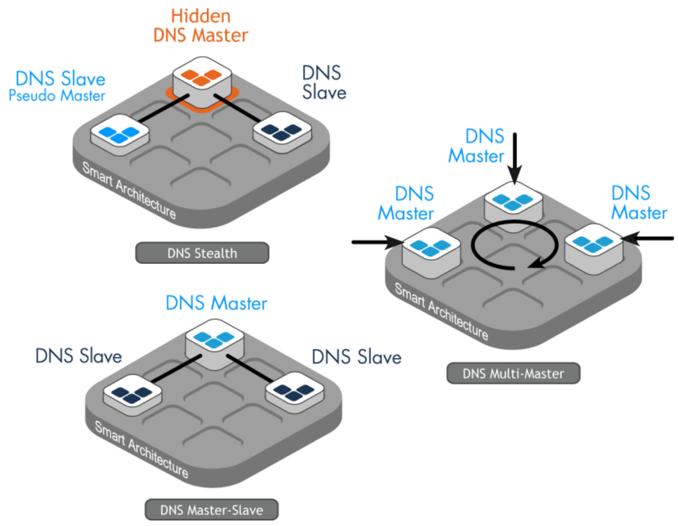
Protecting External DNS Architecture

- Good way to do so is to:
  - Hide information from the Internet: private DNSSEC keys, DNS architecture, flows.
  - Protect Master DNS server against attacks

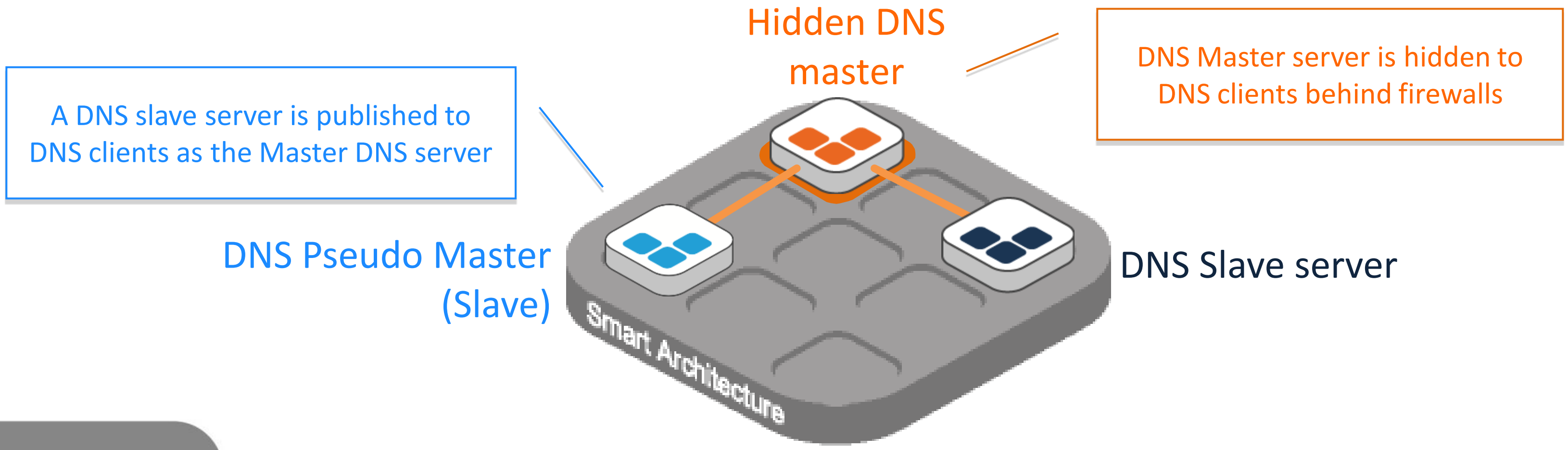
- Answer is: Stealth DNS Architecture

Ease of Deployment

- **Automate DNS architecture deployment**
  - Library of SmartArchitecture DNS templates
  - Automated configuration of all DNS servers according to selected SmartArchitecture
  - Best practices enforcement



- **DNS Stealth: State of the Art Internet DNS architecture**
  - Most secure Internet DNS architecture



A DNS slave server is published to DNS clients as the Master DNS server

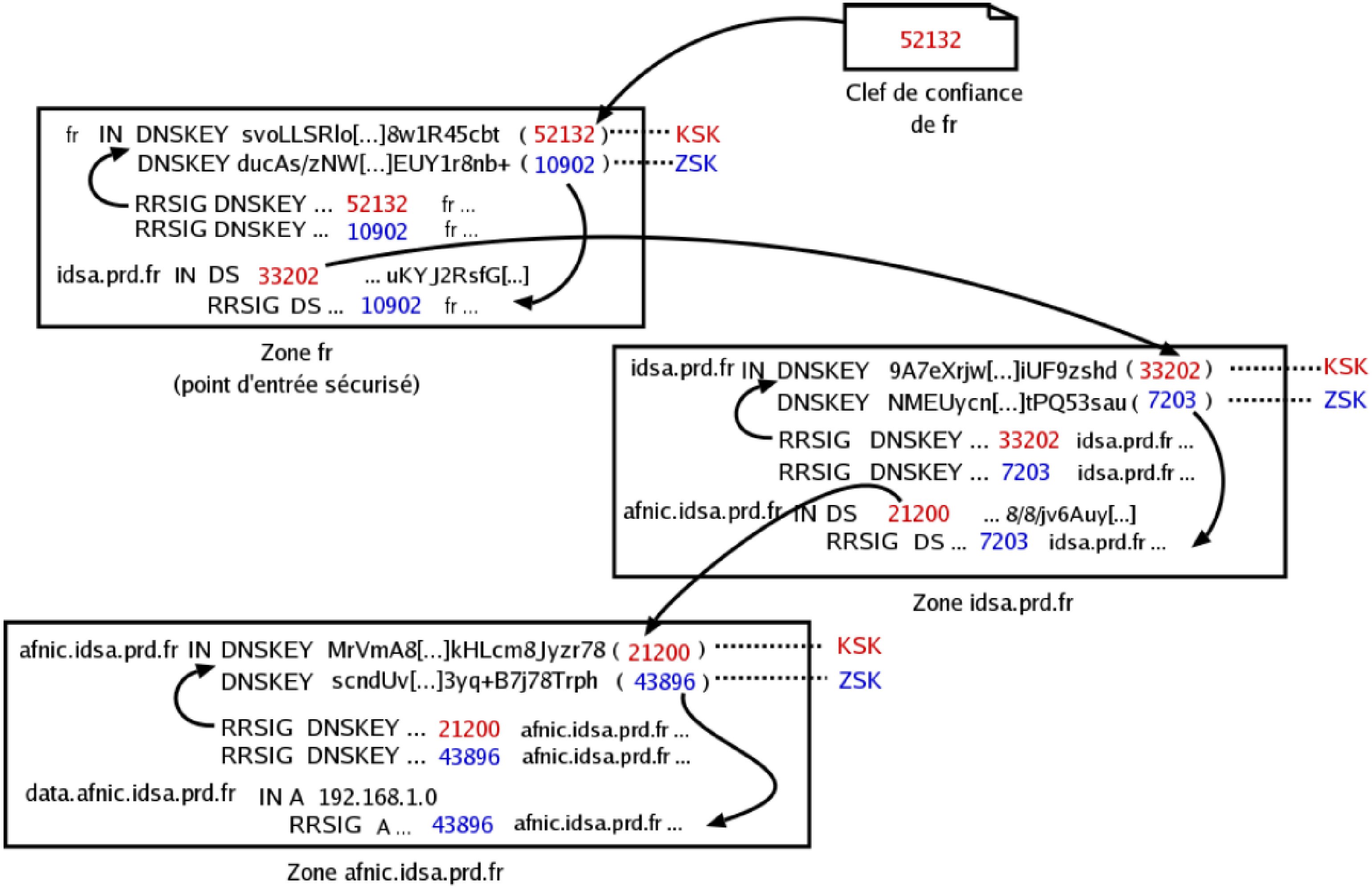
DNS Master server is hidden to DNS clients behind firewalls

DNSSEC

DNSSEC

- DNSSEC is used to protect against query/request redirection
- DNSSEC creates a chain of trust between the client and the authoritative server
- Based on key exchange inside specific signed resource records

DNSSEC



52132

Clef de confiance
de fr

fr IN DNSKEY svoLLSRlo[...]8w1R45cbt (52132) KSK
DNSKEY ducAs/zNW[...]EUY1r8nb+ (10902) ZSK
RRSIG DNSKEY ... 52132 fr ...
RRSIG DNSKEY ... 10902 fr ...
idsa.prd.fr IN DS 33202 ... uKYJ2RsfG[...]
RRSIG DS ... 10902 fr ...

Zone fr
(point d'entrée sécurisé)

idsa.prd.fr IN DNSKEY 9A7eXrjw[...]iUF9zshd (33202) KSK
DNSKEY NMEUycn[...]tPQ53sau (7203) ZSK
RRSIG DNSKEY ... 33202 idsa.prd.fr ...
RRSIG DNSKEY ... 7203 idsa.prd.fr ...
afnic.idsa.prd.fr IN DS 21200 ... 8/8/jv6Auy[...]
RRSIG DS ... 7203 idsa.prd.fr ...

Zone idsa.prd.fr

afnic.idsa.prd.fr IN DNSKEY MrVmA8[...]kHLcm8Jyzr78 (21200) KSK
DNSKEY scndUv[...]3yq+B7j78Trph (43896) ZSK
RRSIG DNSKEY ... 21200 afnic.idsa.prd.fr ...
RRSIG DNSKEY ... 43896 afnic.idsa.prd.fr ...
data.afnic.idsa.prd.fr IN A 192.168.1.0
RRSIG A ... 43896 afnic.idsa.prd.fr ...

Zone afnic.idsa.prd.fr

- Automatic signature of zones
- KSK and ZSK key creation
- Automatic NSEC3 resource records creation
- Rollover management of keys
- Global DNSSEC validation checking

EfficientIP solutions

Please feel free to contact us for more information or a presentation of EfficientIP solutions:

By email: info@efficientip.com

Or via our website: www.efficientip.com