Protect Your DNS Services Against Security Threats
Efficient IP Company Overview

- Americas Headquarters - West Chester, Pennsylvania
- European Headquarters - Paris, France
- First Commercial Release 1998
- Branded EfficientIP In 2004 – Innovative DDI Software Company
  - Unique Advances: Smart DDI, SmartArchitecture™, Hybrid DNS, DNS BLAST,
  - Solution for: BYOD, IP Life Cycle, Unified IP Repository, VLAN Management, Device Management,
  - Compliancy: Integration, WorkFlow Management, and IP Auditing
- Coverage in 60 Plus Countries
- Solid Financial Foundation – Organic Growth & Private Funding
- Full Value Add Services: Hardware Replacement & TAC access 24x7
Today’s Discussion Points

- Applying Best Practices
- Mitigate DNS Malware
- Eliminating Single Point of Failure
- Best Defense is a Great Offense
DNS Security - The storm upon us

+42% Cyber Attacks
+47% DDoS Attacks
+200% DNS Attacks

Symantec: Internet security threat report 2013
Why are DNS Services so Critical?

The Bridge Between Customers and Your Company

Applications & Services

- Online Marketing Web Site
- email
- Website
- Customer Portal

DNS Service

Employees / Customers / Prospects
Why are DNS Services so Critical?

Applications & Services

- Online Marketing Web Site
- email
- Website
- Customer Portal

NO DNS SERVICE = NO BUSINESS

Employees / Customers / Prospects
Apply DNS Best Practices

- Run Up-to-date DNS software version
  - ISC regularly issues updates and patches for BIND
  - Microsoft patches should be applied

- Separate the Functions
  - Authoritative name space should be separate from Caching/Recursive name servers (RFC5358). This aids in preventing Recursive Nameserver Reflection Attacks
  - Authoritative servers should only accept queries they can answer authoritatively and have recursion disabled
  - Apply ACLs to ensure only valid servers are able to initiate zone transfers
Apply DNS Best Practices

- Run DNS Service with Least Privilege
  - Running DNS service as ‘root’ can allow access to file system
  - ✓ Chroot – the name server
  - ✓ Provides minimal rights needed to run service

- Modifying the Zone Data TTLs
  - ✓ Use long TTLs for parent zone for contain “delegation records” (i.e. NS records with associated A or AAAA records)
  - ✓ Set TTLs longer then a typical attack (average attack = 7 hours)
Secure Environment With ACLs

- ACLs are used to control what information will be published
- With Data Flow Identification, lock down who will be able to:
  - Allow Query (server and zone level)
  - Allow Query Cache (server level)
  - Allow Transfer (server and zone levels)
  - Allow Update (zone level)
  - Blackhole (server level)
- Use secure identity
  - Only allow specific Hosts, Networks, or TSIG (Transaction Signature) keys
  - For TSIG, manage all keys centrally to ensure integrity
Architecture Designs for Best Practice

- Automated, Template driven service architecture deployment based on RFC and industry best practice
  - Built-in HIGH Availability
  - Error Free Automated Architecture Configurations
  - Security Best Practice Enforcement
  - Ability to move Point of Recovery and Reduce Time of Recovery

Reduce Complexity: Manage Architectures rather than servers
Automate your Deployment and Management
Best practices enforcement
Protect Against DNS Based Malware

- DNS Firewall or a Response Policy Zone (RPZ)
  - Filters for DNS queries to malicious sites
  - Protects against the initial infection
  - Block communications with Command & Control Servers
  - Help identify infected client workstations

Forbidden Requests are BLOCKED!
(DNS Firewall contains list of malicious domains)
Policies of DNS Firewall

- **Policy Driven RPZ Rules**
  - REDIRECT to Walled Garden or Honeypot
  - NODATA Response to DNS queries
  - NXDOMAIN or Denial of Existence Response
  - PASSTHRU that allows response but tracks

- **Updating Malicious Black List**
  - Filter by creating Resource Records (A, AAAA, Cnames) for each domain or IP address
  - Automatic Data Feed from external source for anti-spam, anti-phishing and anti-malware security database
Bind is the Most Popular & Widely Deployed DNS Engine

• Very flexible with the most comprehensive integration of RFCs
• De facto a “standard”

Security Risks

• Most popular is the most targeted DNS server for hackers
• Numerous security vulnerabilities
• Authoritative and recursive are not separated
Eliminating Single Point of Failure

- Deploy Hybrid DNS Architecture: 3 DNS Engines in One Deployment
  - Including:
    - ISC BIND for Authoritative and Caching DNS
    - NLnetLAB NSD for Authoritative DNS ONLY
    - NLnetLAB Unbound Caching ONLY
- Ability to Switch DNS Engines ON-Demand
Deploy a Hybrid DNS Technology

Hybrid DNS Engine Offers:

- Mitigate zero day vulnerabilities
- Baffle DNS attackers with multiple engines within the same architecture
- Deployment Agility and Security Risk management
- Eliminate single point of failure
- Immediate remediation of security threats
Performance Needs to Mitigate DNS DDoS Attacks:
- 36.75% were at 1 Million qps
- Attacks in 2014 scaled to 400Gb/s

63% of all DNS DDoS Attacks Are Above 1M QPS
Typical Deployment Solutions

- **High TCO: Complex Deployment & Management**
- **Vulnerable to Cache Poisoning**
- **Risky: Denied Valid DNS Requests**
- **Not Scalable: Individual Server Crash**

DNS Operation Analysis and Research Center’s Fall Workshops conference, October 5th - 6th, Phoenix, Arizona (USA)

“request filtering does not mitigate DDoS attacks because it leaves legitimate requests unanswered.”

https://www.dns-oarc.net/
Best Way to Mitigate

The Most Secure Solution is to Always Answer ALL DNS Queries!

Response Rate

Linux 3.11.0-13-generic, Root server, Intel 10GbE, (2013-12-10)

Queries per second

Response Rate [%]

BIND 10.1.1.0  BIND 9.9.4  Knot DNS 1.4-dev  Knot DNS 1.3.2  NSD 3.2.16
NSD 4.0.1  PowerDNS 3.1  YADIFA 1.0.3-2880  DNS Blast
DNS Blast

Million QPS
World’s Fastest DNS Caching Appliance
Mitigating DoS & DDoS Attacks

- DNS Blast Benefits
  - Simple Design and Architecture
  - Requires LESS: Management, Energy, Cooling, Floor Space
  - Scalable and Cost Effective
    - 17 million qps with just 1 appliance and 2 network adapters
CONCLUSION

- Always Apply Best Practices
- Architect for Redundancy and Security
- Implement a DNS Firewall
- Eliminate Single Point of Failures
- Increase and Ensure Performance
THANK YOU!

Stop by the booth to ENTER & WIN: