Protect Your DNS Services Against Security Threats
Data Connectors San Francisco 2016
EfficientIP Company Overview

• Americas Headquarters - West Chester, Pennsylvania
• European Headquarters - Paris, France
• APAC Headquarters - Singapore
• Coverage in 110+ countries
• First commercial release in 1998
• Branded EfficientIP in 2004 - Innovative DDI (DNS-DHCP-IPAM) software company
  • Unique advances: Smart DDI, SmartArchitecture™, Hybrid DNS Engine, DNS Blast
  • Solutions for: BYOD, IP life cycle, unified IP repository, VLAN management, device management
  • Compliance: Integration, workflow management, and IP auditing
• Solid financial foundation - organic growth and private funding
• Full value-add services: hardware replacement and TAC access 24x7
Today’s Discussion Points

- Applying best practices
- Mitigating DNS malware
- Eliminating single point of failure (SPOF)
- The best defense is a great offense
DNS Security - The Storm Is Upon Us

Akamai 2016 Q1 State of the Internet Security Report

- +38% Cyber Security Attacks
- +125% DDoS Attacks
- +200% DNS Attacks
Recent Stats

Stats don’t lie- various types of attacks are on the rise and only getting worse...

DNS Attacks Experienced -Past 12 Months-

- NX DOMAIN ATTACKS: 6.50%
- DNS WATER TORTURE: 5.8%
- DNS-BASED MALWARE: 16.20%
- DNS TUNNELLING: 10.70%
- ZERO-DAY VULNERABILITIES: 13.10%
- DNS AMPLIFICATION: 15.70%
- DOS/DDOS ATTACKS: 21.80%
- CACHE POISONING: 18.90%

10.8% of businesses worldwide incurred attack damages between $1-5 million

SOURCE: 2016 EfficientIP DNS Security Survey, of 1,000 global respondents
Why Are DNS Services So Critical?

Applications & Services

- Employees / Customers / Prospects / Students
- VoIP
- https://

DNS Service
Why Are DNS Services So Critical?

Applications & Services

NO DNS SERVICE = NO BUSINESS

Employees / Customers / Prospects / Students
DNS Best Practices

• Run up-to-date DNS software versions
  • 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) - aids in preventing recursive name server 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
DNS Best Practices cont.

- Run DNS service through user account with minimal privileges
  - 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 to contain ‘delegation records’ (i.e. NS records with associated A or AAAA records)
  - Set TTLs longer than a typical attack (average attack = 7 hours)
Secure Environments 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

---

DNS Master - Slave

Stealth DNS

DNS Farm
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
  - Blocks communications with Command & Control servers
  - Helps 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 queries

• Updating malicious blacklist
  • 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
Single DNS Engine: Strengths & Weaknesses

• BIND is the most popular and widely deployed DNS engine
  • Very flexible with the most comprehensive integration of RFCs
  • De facto a ’standard’

• Security risks
  • Most popular also makes it the most targeted DNS server for hackers
  • Numerous security vulnerabilities
  • Authoritative and recursive functions are not separated
Eliminating Single Point Of Failure

- Deploy Hybrid DNS architecture - three DNS engines in one deployment, including:
  - ISC BIND for authoritative and caching DNS
  - NLnetLAB NSD for authoritative DNS only
  - NLnetLAB Unbound caching only

- Hybrid architecture allows for the ability to switch DNS engines on demand
Deploy A Hybrid DNS Technology

• Hybrid DNS engine features
  • Mitigate zero-day vulnerabilities
  • Baffle attackers with multiple engines within the same architecture
  • Deployment agility and security risk management
  • Eliminate single point of failure (SPOF)
  • Immediate remediation of security threats
DDoS DNS Attacks On The Rise

Existing DNS solutions are not enough to mitigate DDoS attacks!

- Average DNS server handles 100K QPS* before severe degradation begins

49% of DNS DDoS Attacks Are Above 1 Million QPS

*QPS= DNS queries per second

SOURCE: Arbor Networks 2016 Worldwide Infrastructure Security Report

SOURCE: 2016 EfficientIP DNS Security Survey
DDoS DNS Attacks On The Rise cont.

**Targets of Application-Layer Attacks**

- 78% DNS
- 75% HTTP
- 47% HTTPS
- 25% SMTP
- 19% SIP/VOIP
- 8% IRC
- 7% Other
- 6% Not applicable

**SOURCE:** Arbor Networks 2016 Worldwide Infrastructure Security Report
Multiple DNS Targets For Many Objectives

- Business Downtime
- Embezzlement of Money
- Intellectual Property Theft
- Customer Data Theft
- Damaged Reputation
- Password Stealing

- Volumetric
- Stealth
- Exploits
Detecting DNS Tunnelling

• Use Case: How to detect an attempt of DNS tunnelling?
  • Some will make use of the recursive DNS of an organization as a relay to query a remote authoritative DNS
  • Remote authoritative DNS is the accomplice → used to encapsulate the HTML pages content in the answers of the queries
  "Like getting internet access from a hotel room without paying the access fees"

Client capable of sending the internet access requests via the DNS queries and to reassemble the HTML content carried in the DNS answers

Recursive DNS used as a ‘carrier’ for the internet access request/responses

Server capable of interpreting the requests and cutting the HTML pages into slices for transport in the DNS answers
Detecting DNS Tunnelling cont.

- Use Case: How to detect an attempt of DNS tunnelling?
  - The transfer of the HTML pages will result in a high cumulated size of the answers returned by the DNS
  - Can be detected by sorting the statistics using the column ‘miss-A-sz’

DNS Blast> **show clients order=miss-A-sz**

**MOST USED CLIENTS ENTRIES:**

<table>
<thead>
<tr>
<th>Query</th>
<th>Client IP</th>
<th>Last-used</th>
<th>C-hit</th>
<th>C-miss</th>
<th>hit-Q-sz</th>
<th>miss-Q-sz</th>
<th>hit-A-sz</th>
<th>miss-A-sz</th>
</tr>
</thead>
<tbody>
<tr>
<td>1595k</td>
<td>10.0.200.1</td>
<td>291</td>
<td>229135</td>
<td>1366k</td>
<td>9800kB</td>
<td>58598kB</td>
<td>25229kB</td>
<td>123MB</td>
</tr>
<tr>
<td>178993</td>
<td>10.0.22.22</td>
<td>283</td>
<td>2587</td>
<td>176406</td>
<td>110kB</td>
<td>8808kB</td>
<td>237kB</td>
<td>2911kB</td>
</tr>
<tr>
<td>188165</td>
<td>10.0.30.44</td>
<td>14</td>
<td>136191</td>
<td>51974</td>
<td>4919kB</td>
<td>1987kB</td>
<td>31346kB</td>
<td>12089kB</td>
</tr>
<tr>
<td>69981</td>
<td>10.0.0.43</td>
<td>7</td>
<td>23536</td>
<td>46445</td>
<td>949kB</td>
<td>1885kB</td>
<td>2119kB</td>
<td>4162kB</td>
</tr>
<tr>
<td>54381</td>
<td>10.0.30.221</td>
<td>22</td>
<td>11979</td>
<td>42402</td>
<td>442kB</td>
<td>1670kB</td>
<td>1262kB</td>
<td>5347kB</td>
</tr>
<tr>
<td>51034</td>
<td>10.0.30.222</td>
<td>28</td>
<td>18955</td>
<td>32079</td>
<td>693kB</td>
<td>1245kB</td>
<td>4950kB</td>
<td>9346kB</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Typical Deployment Solutions

- High TCO: complex deployment & management
- Vulnerable to cache poisoning
- Risky: denied valid DNS requests
- Not scalable: individual server crash

"Request filtering does not mitigate DDoS attacks because it leaves legitimate requests unanswered."

DNS cluster and load balancing diagram.
The 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)

Response Rate [%]

Queries per second

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 Solution

• Benefits for mitigating DoS and DDoS attacks
  • Transactional inspection of DNS queries
  • Simple design and architecture
  • Requires less: management, energy, cooling, floor space
  • Scalable and cost-effective

17 million QPS with just one appliance and two network adapters
DNS Guardian Solution

- Adaptive DNS security
- Inside-DNS transaction analysis for accurate attack detection
  - Global and per IP statistics (cache & recursive)
- Volumetric, stealth & exploit attack detection
  - Tunnelling, RQName attacks, phantom attacks, anomalies
- Graduated protection with smart countermeasures
  - Block the attack source IPs
  - Quarantine suspected attack source IPs
  - Patented Rescue Mode: ensure service continuity even if the attack source is unidentifiable
Conclusion

- Always apply best practices
- Create architecture for redundancy and security
- Implement a DNS firewall
- Eliminate single point of failure
- Increase and ensure performance
Thank You!

-- Stop by our booth with any questions --

Confidential-Property of EfficientIP - All rights reserved-Copyright © 2016