

# SECURE 64 ✓™

Protecting The Network via A Secure DNS

## DNS Summer Day 2017

Amanda Constant, VP Engineering, Secure64

# Introduction

## **Amanda Constant – Secure64 Vice President of Engineering**

- **MS Computer Science – University of Arizona 1984**
- **33+ years experience in Software Engineering**
- **11 Years at Secure64**
- **Secure64 Representative to DNS OARC**
- **Responsible for all R&D, Current Product Engineering, Product Test, On Call Support Specialists**

Summary	Product name(s)	DNS Cache, DNS Authority, DNS Manager, DNS Guard, DNS Signer, Private Certificate Authority, ENUM Solutions, DNS Analytics, Pipe-Protector, ProVision
	Concept	Highly-secure, always available, set-and-forget DNS, Industry leading innovations on top of DNS as a platform to protect the network and subscribers
	Strengths	Built-in DDoS protection (including PRSD), immune to BIND vulnerabilities, carrier-grade availability, IPv6 and fully automated DNSSEC
	Function	Authority, cache, DNSSEC servers, provisioning, monitoring & management, network protection services
	Format (HW/SW)	Software, virtual appliance, hardware appliance, NFV ready
Performance	Authority server	1M+ Zones
	Cache server	1M+ QPS (HPE DL360 gen9 server with a single Intel® Xeon® Processor E5-2667 v4 (25M Cache, 3.20 GHz), 16GB of RAM, and a two port HP530SFP+ (QLogic 57810S) 10Gb network card.
Price	Pricing model	Cache: QPS-based Authority: Records-based Pay-as-you-Grow
	Minimum upfront cost	From \$7,500
	Running costs	From \$3,000 Annual
Support	Support structure	Japanese language support via Local Partner NSSOL
	CVE response	Japanese language Email Announcement via Local Partner NSSOL
	EOL policy	2 previous generations supported
	Data migration	RFC1035(BIND) formatted zone files translator

Features	Zone data save format		Text file, binary, SQL database	
	Local zone save?		Y	
	PRSD defense?		Y (Rate Limit[Client → Cache], Rate Limit[Cache → Auth], Internal resource monitoring & protection)	
	Cache poisoning defense?		Y Source port randomization; dns-0x20; bailiwick checks; QID, QName,	
	DDoS defense?		Y RRL, Mitigation on: RRTYPE, per IP rates, aggregate rates, response codes, protocols	
	Supported RR Type		All RFC types	
	IPv6 transport support?		Y Including DNS64 and filter-AAAA-on-V4	
	Management	Interface		Web GUI, CLI, REST API
		Integrated management?		Y Manage, monitor, alert/alarm on multiple platforms from a single DNS Manager instance (remote login & command execution)
		Logging?		Query log, command audit logs, negative response logs, blacklist logs
		Query log search?		GUI, CLI
	DNSSEC	Authority	Signature update	Y (automatic)
			Key update	Y (automatic)
			Key update format	ZSK:Pre-Publication, KSK:Double-Rrset
			HSM support	Y – Keys are never in the clear
Cache		Validation	Y	
		TA update	Y (RFC5011 support)	
		NTA support	Y	

# Who We Are

- **Founded by Hewlett Packard veterans in 2002**
- **Based in Denver, Colorado**
- **Built on a foundation of security**
  - **Secure platform for DNS**
  - **Built-in DDoS protection**
  - **Carrier-grade availability**
- **Growing 50-60% annually**
- **Tier-1 ISP and carrier customers**
- **Offices in USA, Europe and Japan**

# Key Customers and Verticals

## Communications



## Government / Enterprise



## Internet Infrastructure Automated DNSSEC

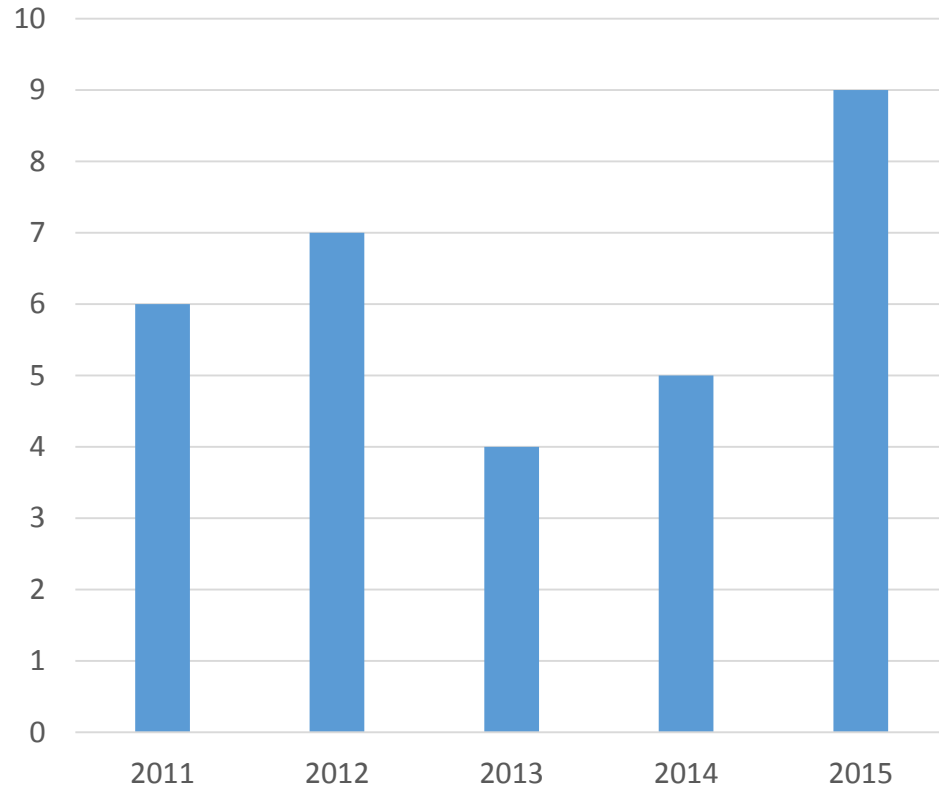


# Secure64 Product Line



# BIND Vulnerabilities – Secure64 is not based on BIND

Critical BIND Security Vulnerabilities Requiring Immediate Patching



Secure64 is not vulnerable to any of these BIND weaknesses

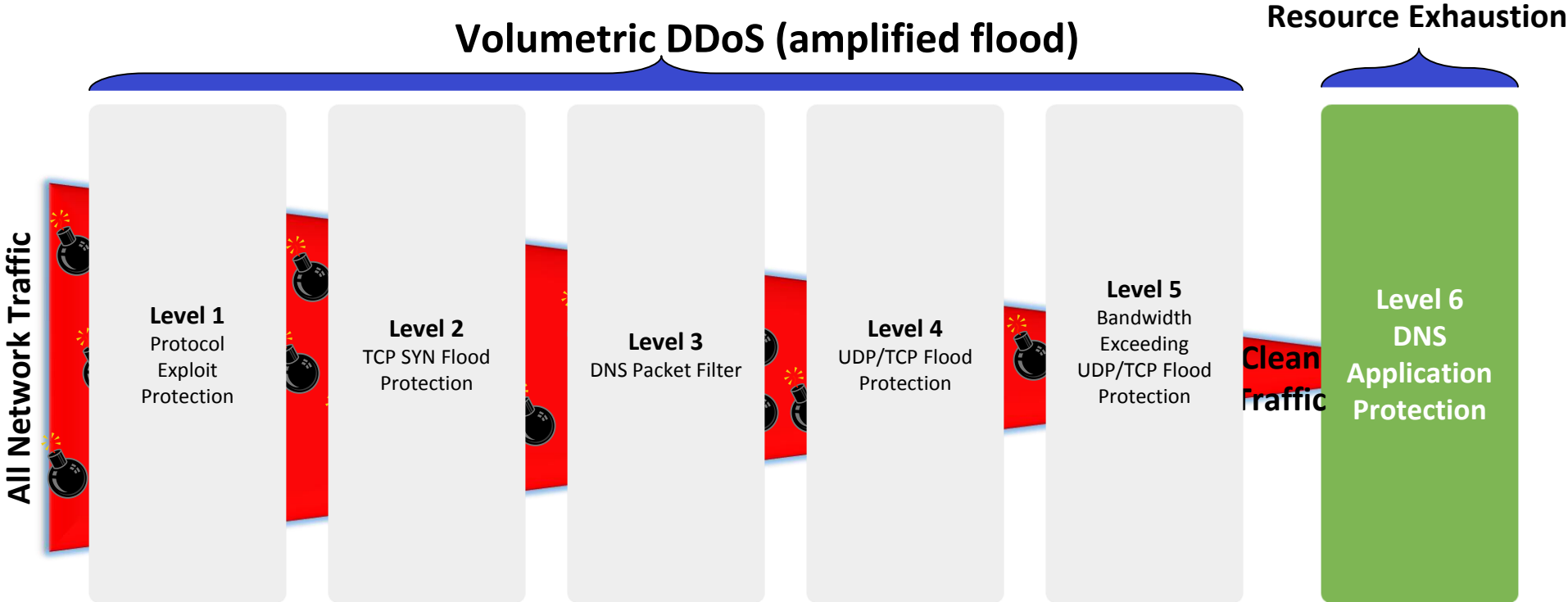
Year	BIND	Secure64	Vulnerability ID	Impact
2016	●	●	<a href="#">CVE-2016-1284</a>	Crash
	●	●	<a href="#">CVE-2016-1285</a>	Crash
	●	●	<a href="#">CVE-2016-1286</a>	Crash
	●	●	<a href="#">CVE-2016-2088</a>	Crash
	●	●	<a href="#">CVE-2016-2775</a>	Crash
	●	●	<a href="#">CVE-2016-2776</a>	Crash
	●	●	<a href="#">CVE-2016-2848</a>	Crash
	●	●	<a href="#">CVE-2016-6170</a>	Crash
	●	●	<a href="#">CVE-2016-8864</a>	Crash
2017	●	●	<a href="#">CVE-2017-3135</a>	Crash
	●	●	<a href="#">CVE-2017-3136</a>	Crash
	●	●	<a href="#">CVE-2017-3137</a>	Crash
	●	●	<a href="#">CVE-2017-3138</a>	Crash

● Vulnerable      ● Not vulnerable

Secure64 is not vulnerable to any of these BIND weaknesses



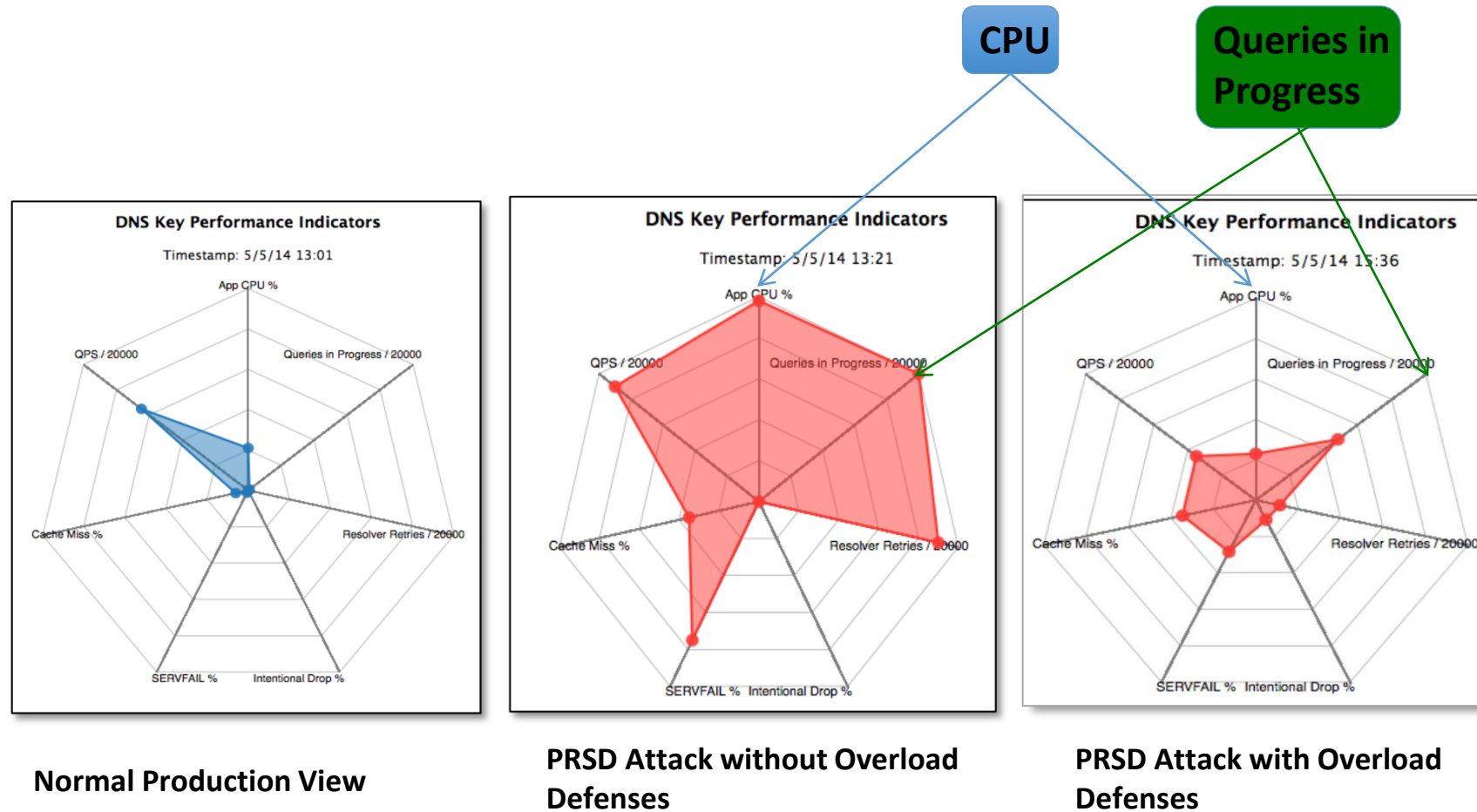
# Secure64 Built-In Defenses



“The Secure64 software was subjected to a number of attacks known to be disruptive to servers, and ignored the attacks, delivering information as requested up to the saturation point of the Gigabit connection used.”

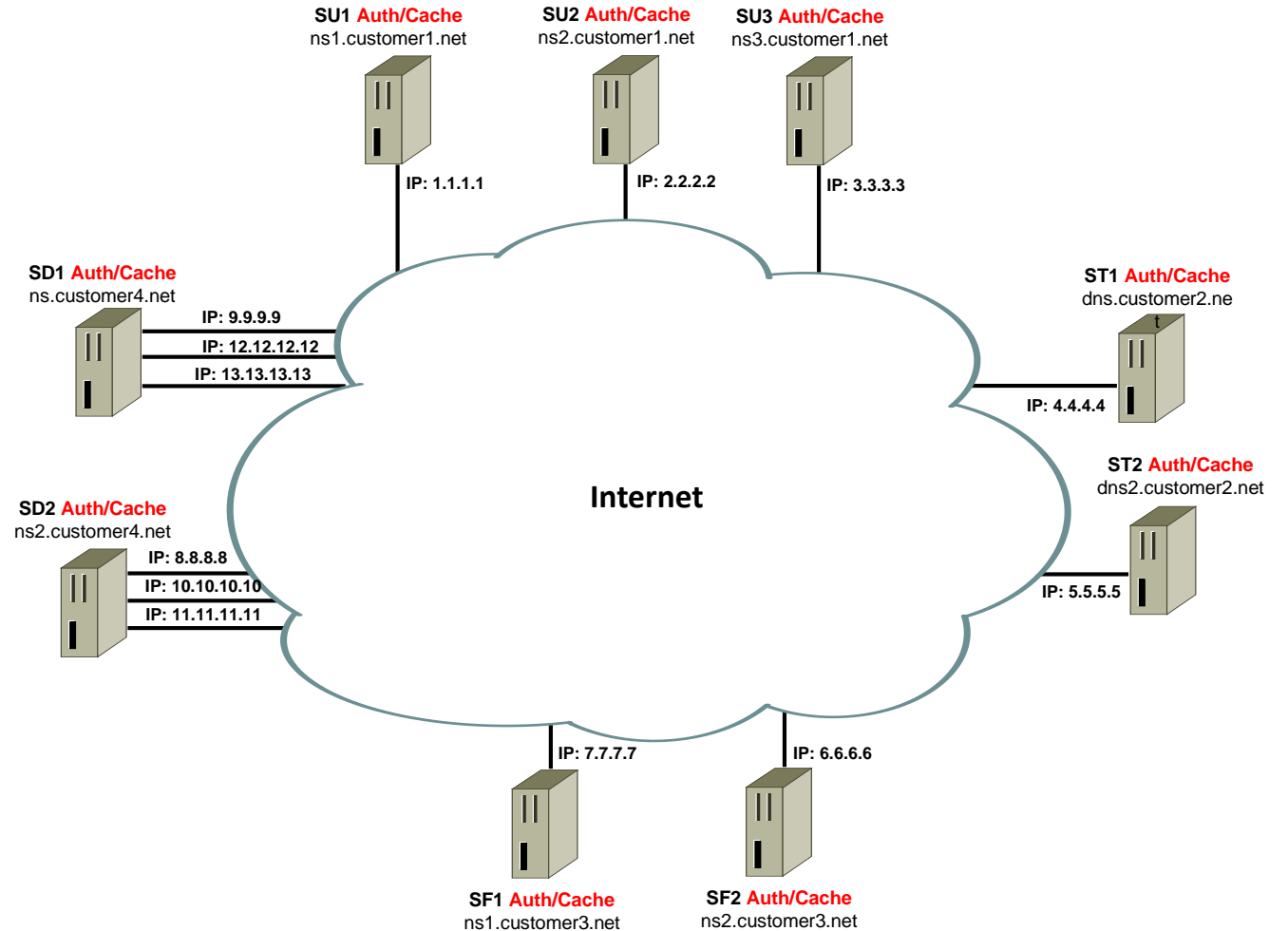


# Overload Defenses in Action vs. PRSD

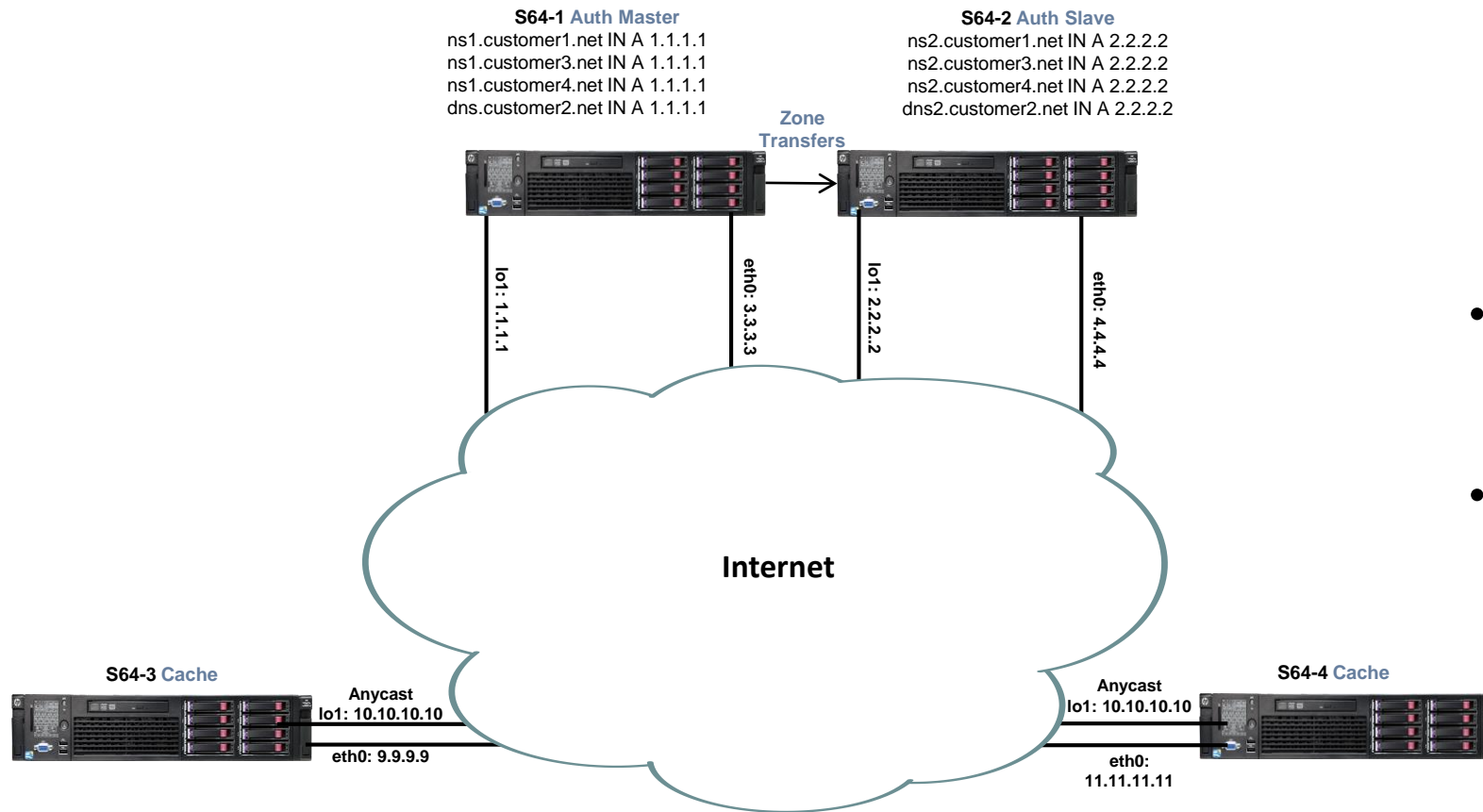


# Consolidating IP Addresses with Anycast Telecom Provider BEFORE

- Security
  - Combined Roles (Auth/Cache)
  - If Cache is attacked, Authority goes down
- IP Space Used
  - 13 unique IP addresses
- Cost
  - 9 BIND servers (power consumption, patching and management)

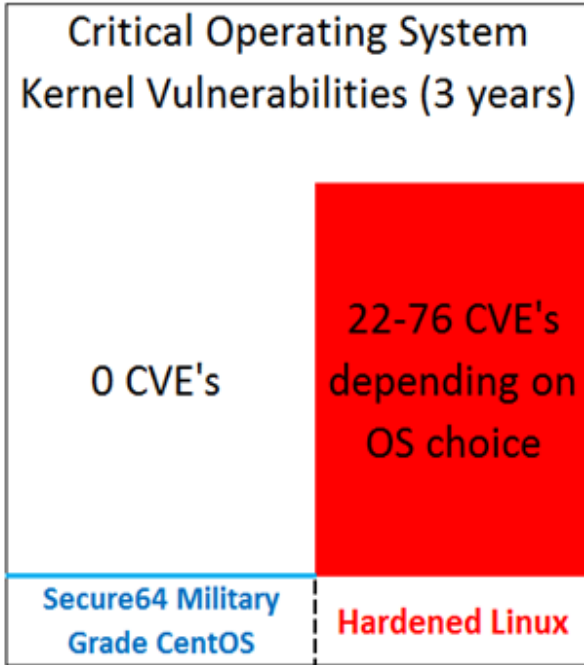


# Consolidating IP Addresses with Anycast Telecom Provider AFTER



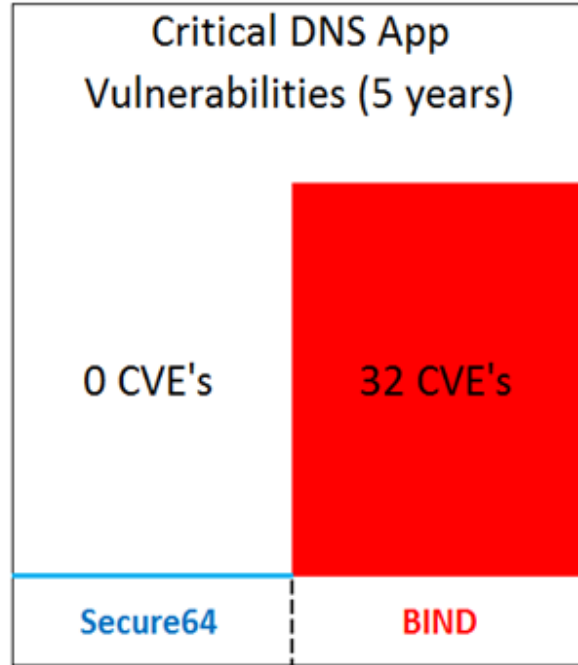
- Security
  - Separate Cache DNS and Authority DNS
  - Remove BIND vulnerabilities from network
- IP Space Used
  - 7 unique IP addresses (vs. 13)
- Cost
  - 4 Secure64 DNS servers (vs. 9)
  - Less power consumption
  - Centralized management with DNS Manager
  - No CVE Patching

# Secure64 – Benchmark Leader



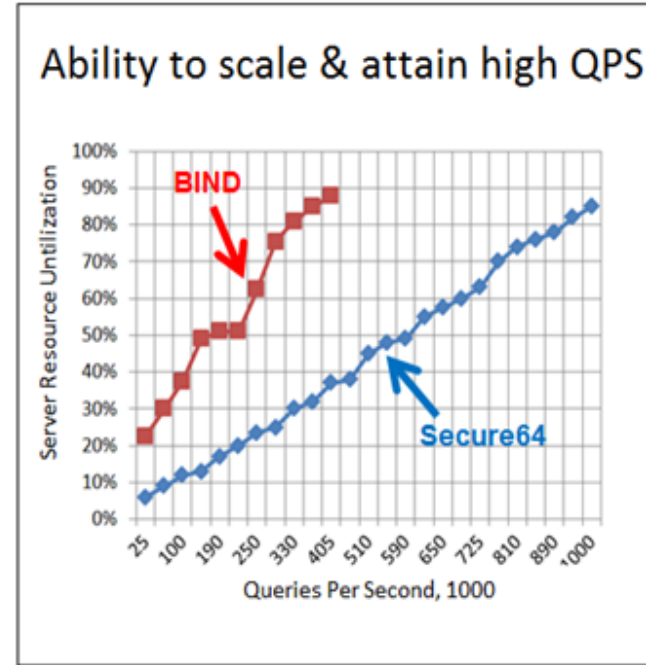
Source: NIST and other sources, 2014-16

NIST



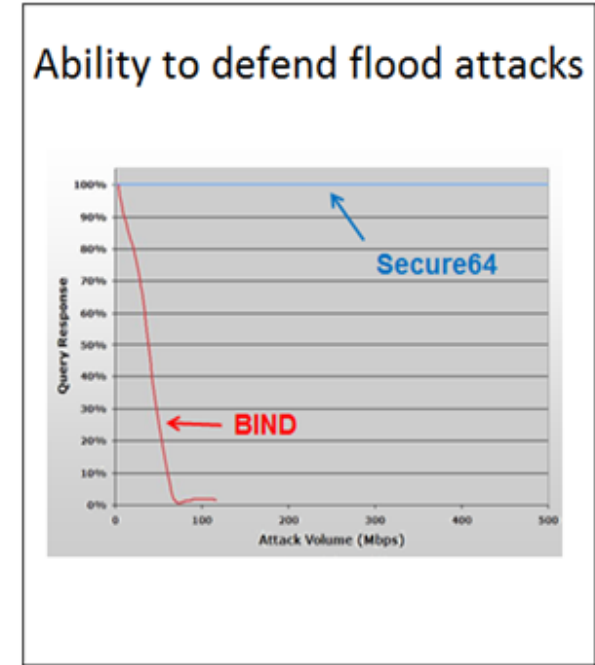
Source: NIST published data, 2012-16

NIST



Source: Farsight Lab & Secure64 Lab

FARSIGHT



Source: Extreme Labs, California

EXTREME LABS, INC.

## Blacklist & Whitelist editor

Overview Cache Authority Admin

### Blacklist

The Blacklist Node creates blacklist configuration components for caching servers. Define a blacklist feed or file and the caching server action(s) for the blacklisted items.

#### Blacklist Type

Select Local File to manually enter blacklist information. Select Remote Feed to choose a Blacklist Feed. To view or add a Remote Feed, select the **Configure Blacklist Feeds** command.

Local File  Remote Feed

#### Remote Feed

Select the Blacklist Feed to use for this Blacklist node.

Secure64 Malware Feed

Total Entries:	845290
Domain Name Only:	847347
Domain Name with URL:	0
IP Addresses:	1923
Update Frequency:	Every 4 hours
Last Updated:	Apr-10-09-01:44

#### Domain Name Only

Select the action to take for all domains and subdomains in this Blacklist: **Refuse**

#### Domain Name with URL

Select the action to take for all domains associated with URLs in this Blacklist: **Deny**

## Config Editor

Overview Cache Authority Admin

### Identity and Version Denial

**hide-identity:** Refuse id.server and hostname.bind queries.

**hide-version:** If set to yes, the server refuses version.server and version.bind queries. If not defined, the default is no.

**identity:** Recommended for security purposes. Returns the specified string when queried for id.server.

Set the string to an arbitrary value to mask the server's nodename. If not defined, the default is the name as set up by the nodename command.

**version:** Set the version to report for version.server and version.bind queries. If not defined and hide-version is set to no, the default is the system node name.

### Security Hardening items:

harden-glue:

cache.conf

- SERVER clause
  - 1. Comments
  - 2. General Settings
  - 3. Network Settings
  - 4. Interfaces
  - 5. Access Control
  - 6. Cache Sizes
  - 7. DNSSEC
  - 8. Security Settings**
  - 9. Performance Settings
  - 10. Query Logging
  - 11. Local Zones
  - 12. NXDOMAIN Redirect
- Named Cache(s)
- STUB ZONE declarations)
- FORWARD ZONE declarations)
- MERGE ZONE declarations)
- Global INCLUDE Files(s)
- VIEW declaration(s)

## Create Custom Reports

### Reports

#### Monitoring

- Cache Miss Latency
- Average Cache Hit Latency
- Average Cache Miss Latency
- Inbound Query Rate by RRType
- Inbound Query Rate by Validation
- Incoming Queries SRVFAIL Ratio
- Resolver Lookup Rate
- Top Domains or Clients (RTQM)
- Ambient Temp °C

#### Capacity Planning

- Inbound Query Rate by Server
- Total Inbound Query Rate
- IP Packet Rate

## Software updates, version control & rollback

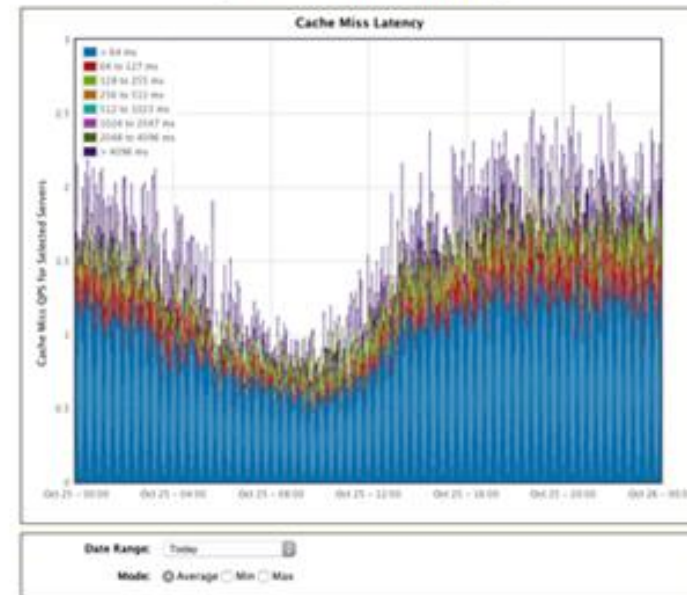
Production

- Authority Cache Servers
  - Lenexa
    - 10.0.0.75 **New node**
    - 10.0.0.76
    - 10.0.0.77
  - Reston
    - 10.0.0.78
    - 10.0.0.79
    - 10.0.0.80
- Authority Master Servers
  - Lenexa
    - 10.0.0.69
    - 10.0.0.70
  - Reston
    - 10.0.0.71
    - 10.0.0.72
- Authority Slave Servers

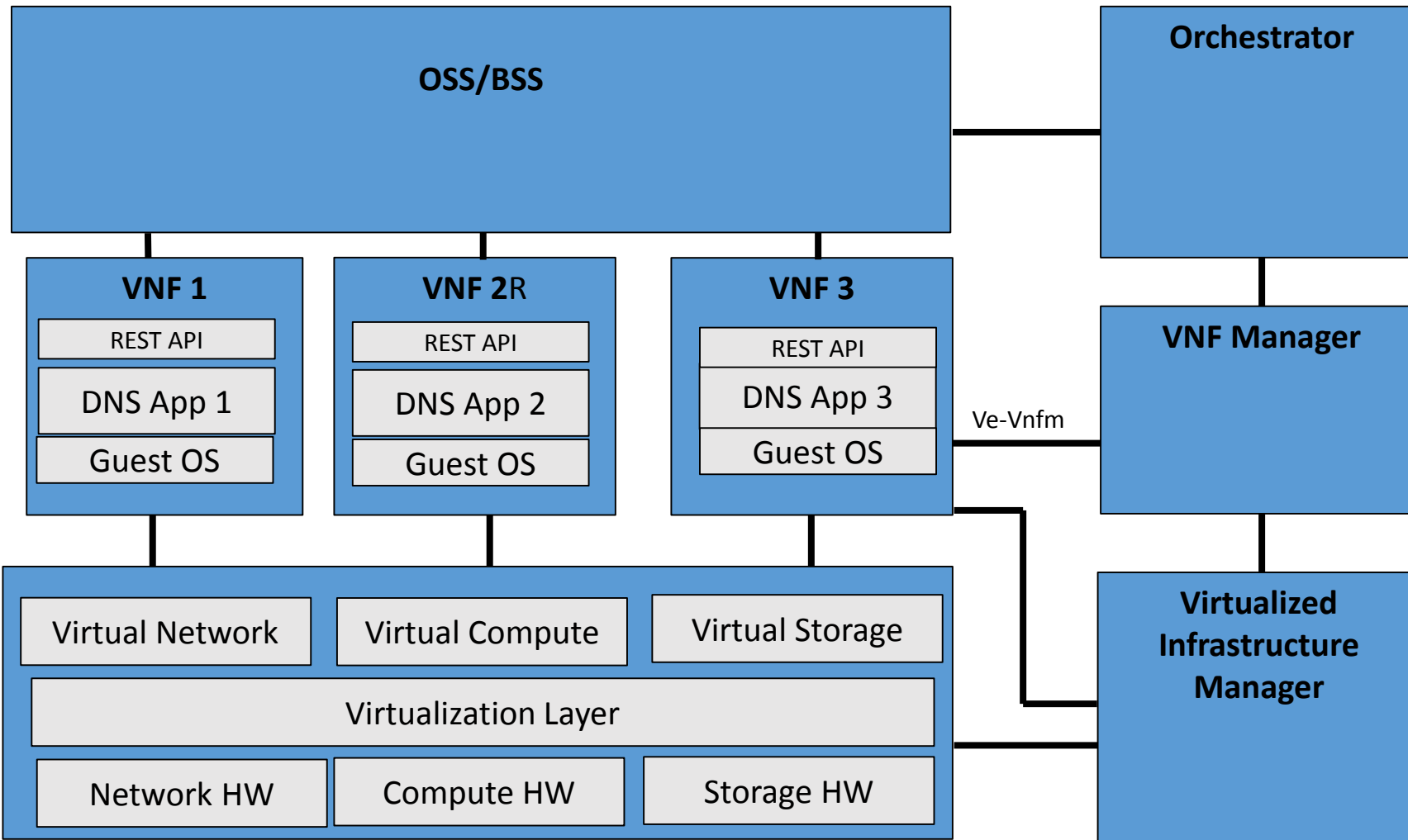
### Commands:

- Create FileSet
- Create Blacklist
- Create Whitelist
- Retrieve/Delete Remote Files
- Retrieve Server Status
- Upgrade OS & Reboot
- Rollback OS & Reboot
- Reboot Server

## Drill Down Graphs



# Deployment Model – Network Function Virtualization



Ve-Vnfm automatically:

- Configures
- Monitors
- Controls
- Provisions

Benefit	
Maximizes performance	
Reduces CAPEX	✓
Reduces HW OPEX	✓
Reduces SW OPEX	✓
Accelerates time to market	✓
Increases agility & flexibility	✓

# Secure64 in Summary

- **Not vulnerable to BIND CVEs**
- **Built in DDoS protection, including PRSD & overload attacks**
- **Carrier-grade availability**
- **IPv6 compatible**
- **Fully automated DNSSEC**
- **Network security innovations utilizing a secure DNS**
- **Simplified DNS architecture reduces operational costs**
- **NFV Ready**



**SECURE 64**  **TM**

Thank you