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

T-Mobile
verizon
Telefonica
CenturyLink
TELMEX
Sprint
pelephone
media networks
smartfren
movistar
melita
ooredoo
Cellcom
Cnt nos unel
VimpelCom
SingTel

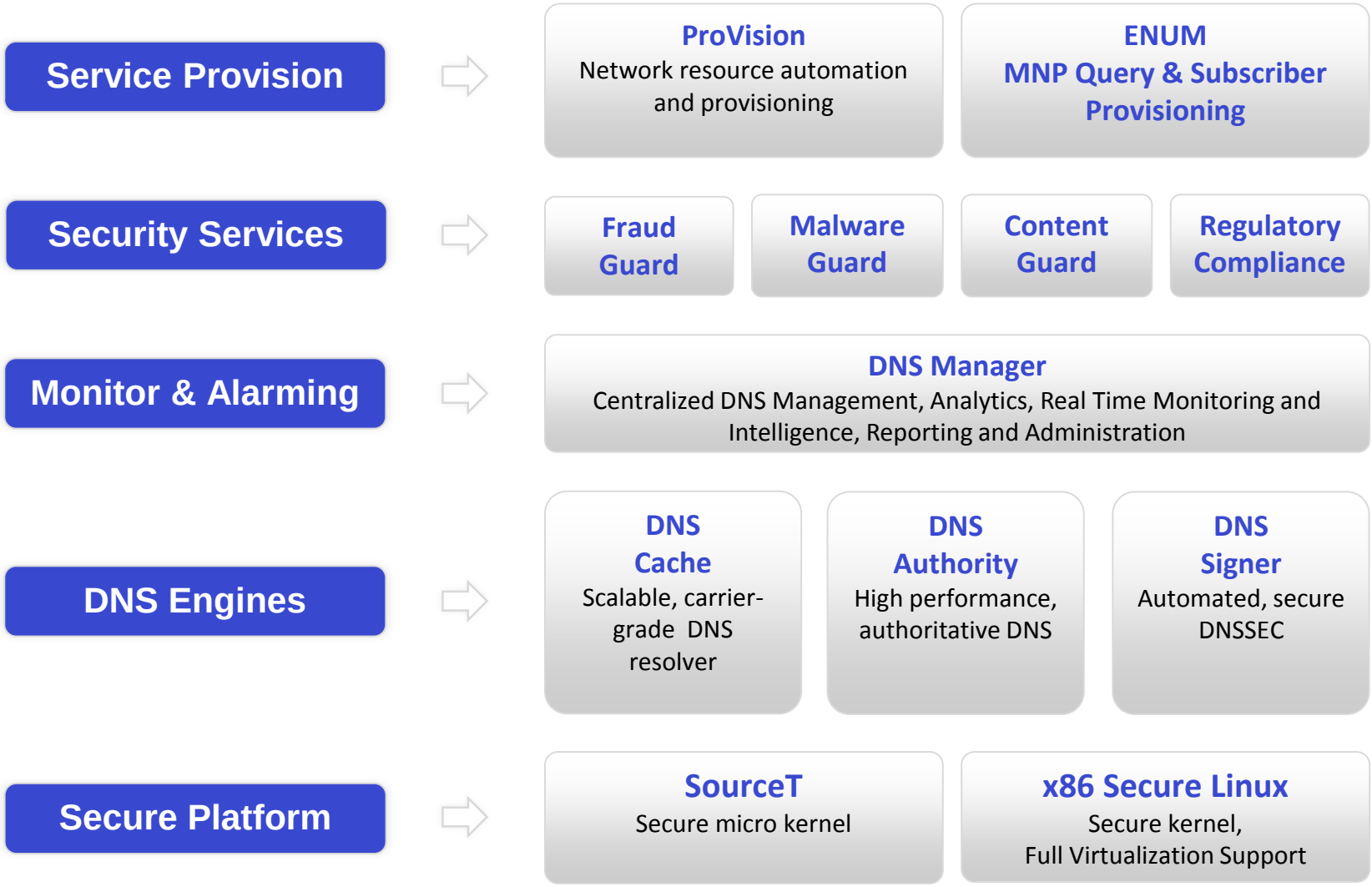
Government / Enterprise

hp
IRS
Ohio OARnet
Federal Retirement Thrift Investment Board — Thrift Savings Plan — 1986
NYC.gov always open
DFAS Defense Finance and Accounting Service
ESnet Energy Sciences Network
NSF
Grupo AVAL

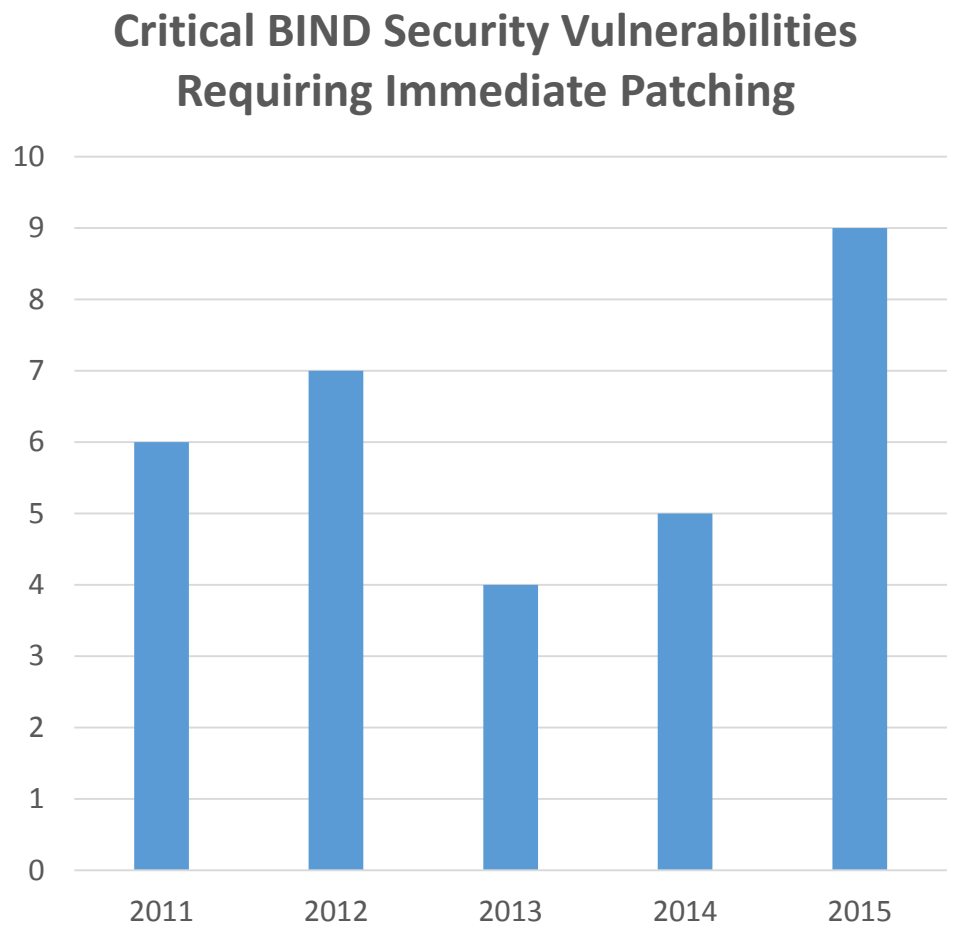
Internet Infrastructure Automated DNSSEC

RIPE NCC
APNIC
.hk
.fi domain name
Afilias
ARIN American Registry for Internet Numbers

Secure64 Product Line



BIND Vulnerabilities – Secure64 is not based on BIND



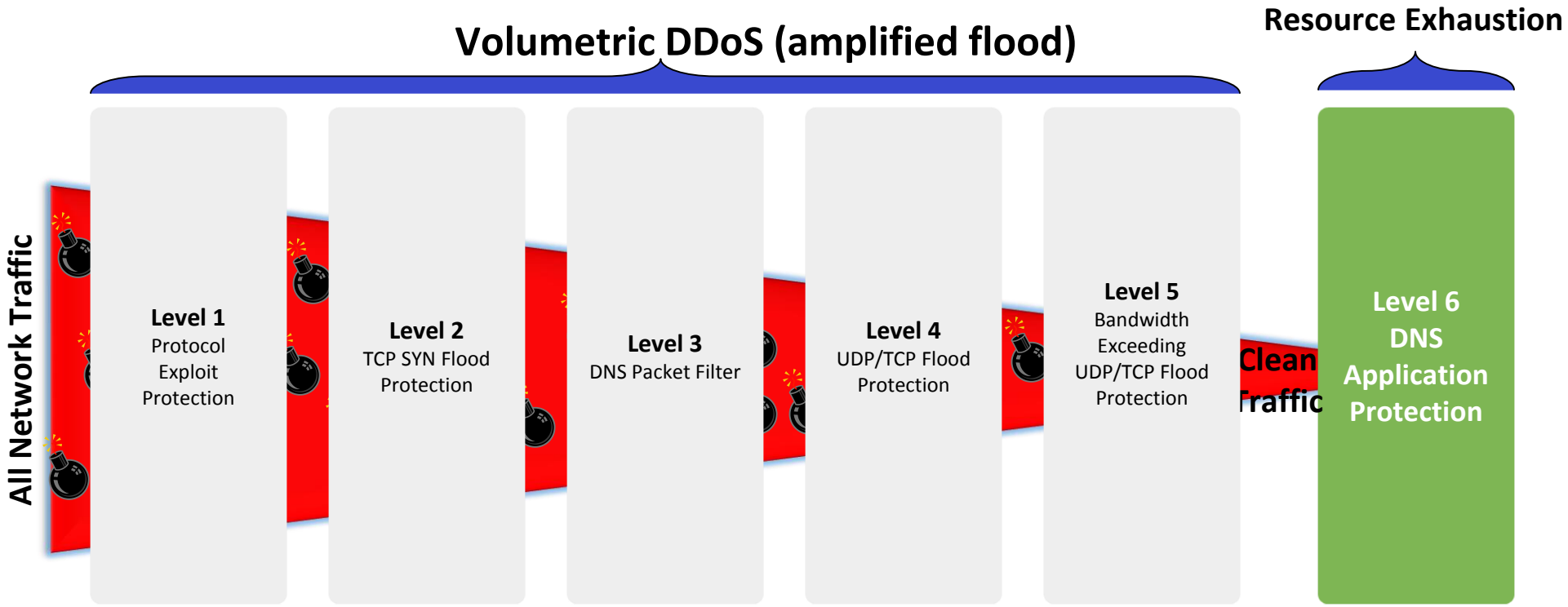
Secure64 is not vulnerable to any of these BIND weaknesses

Year	BIND	Secure64	Vulnerability ID	Impact
2016	●	●	CVE-2016-1284	Crash
	●	●	CVE-2016-1285	Crash
	●	●	CVE-2016-1286	Crash
	●	●	CVE-2016-2088	Crash
	●	●	CVE-2016-2775	Crash
	●	●	CVE-2016-2776	Crash
	●	●	CVE-2016-2848	Crash
	●	●	CVE-2016-6170	Crash
	●	●	CVE-2016-8864	Crash
2017	●	●	CVE-2017-3135	Crash
	●	●	CVE-2017-3136	Crash
	●	●	CVE-2017-3137	Crash
	●	●	CVE-2017-3138	Crash

● Vulnerable ● Not vulnerable

Secure64 is not vulnerable to any of these BIND weaknesses

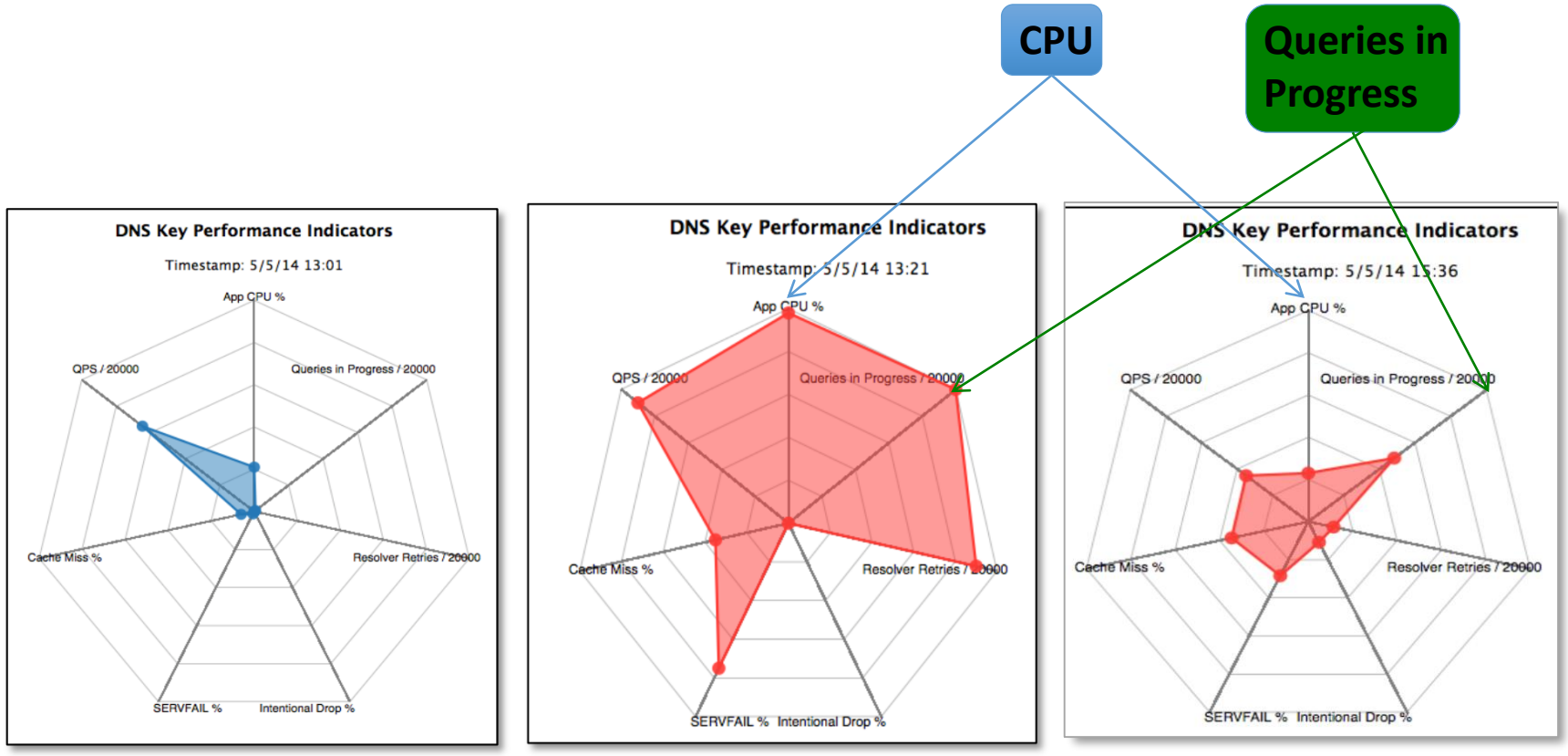
Secure64 Built-In Defenses



"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."

EXTREMELABS, INC.

Overload Defenses in Action vs. PRSD



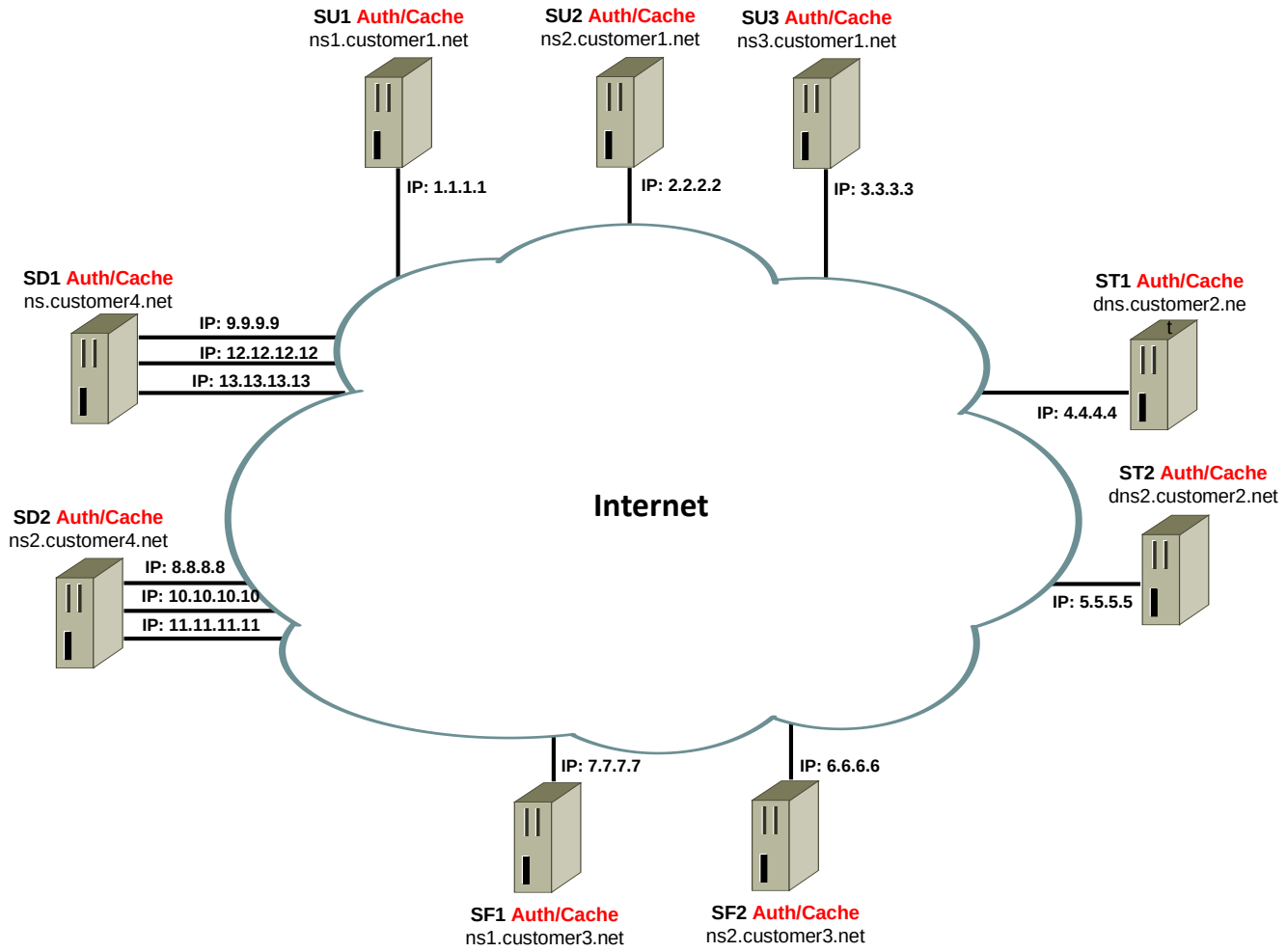
Normal Production View

PRSD Attack without Overload Defenses

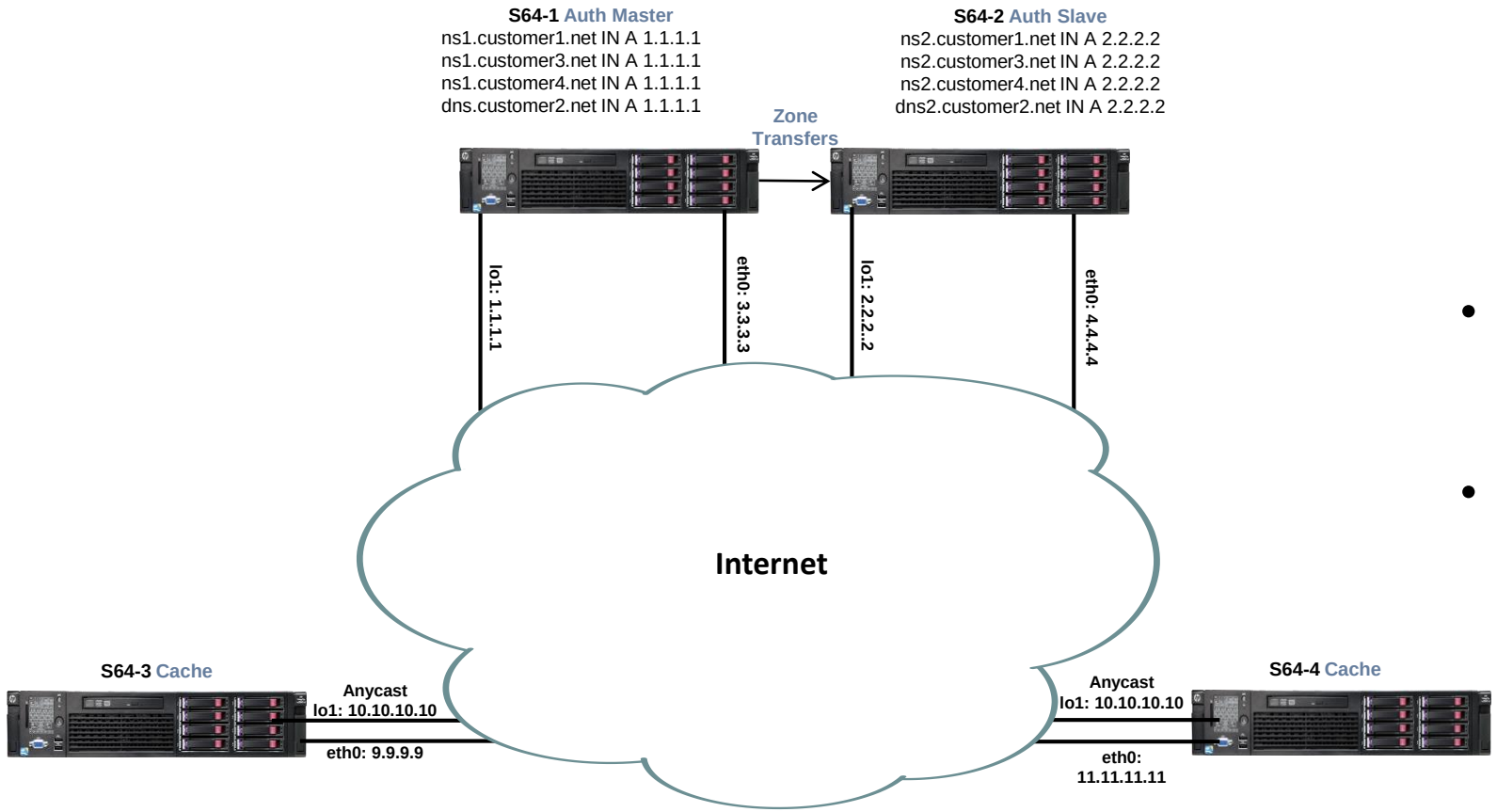
PRSD Attack with Overload Defenses

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)

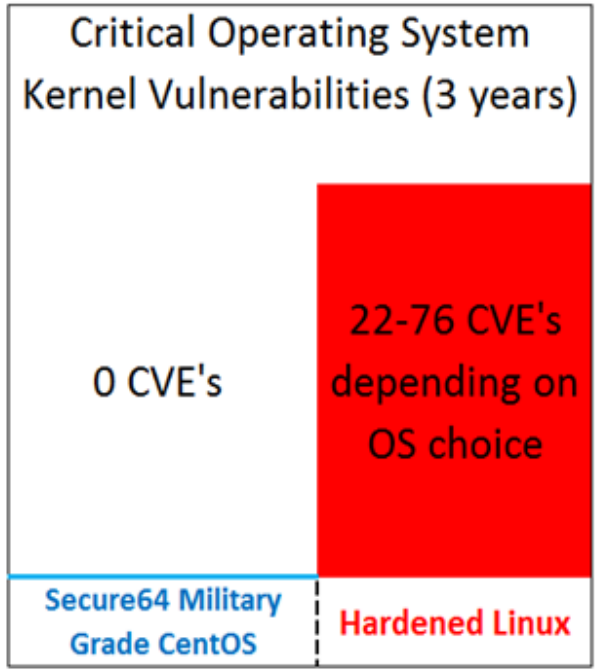


Consolidating IP Addresses with Anycast Telecom Provider AFTER



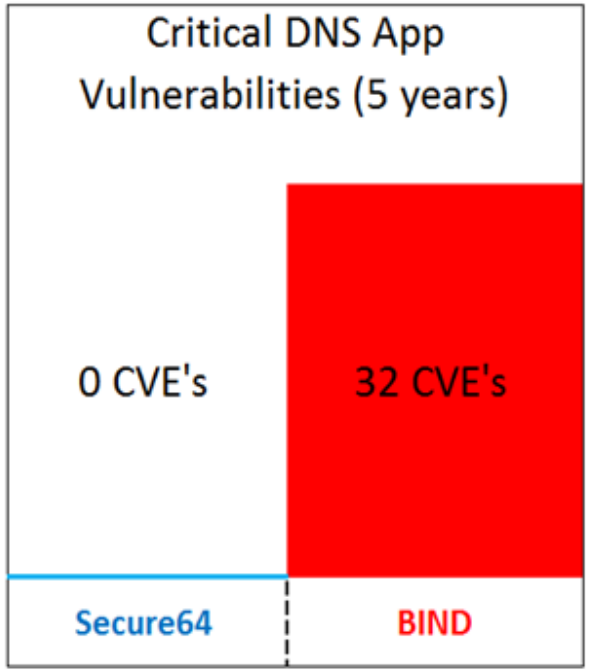
- Security
  - Separate Cache DNS and Authority DNS
  - Remove BIND vulnerabilities from network
- IP Space Used
  - 7 unique IP addresses (vs. 13)
- Cost
  - 4 Secure64 DNS servers (vs. 9)
  - Less power consumption
  - Centralized management with DNS Manager
  - No CVE Patching

Secure64 – Benchmark Leader



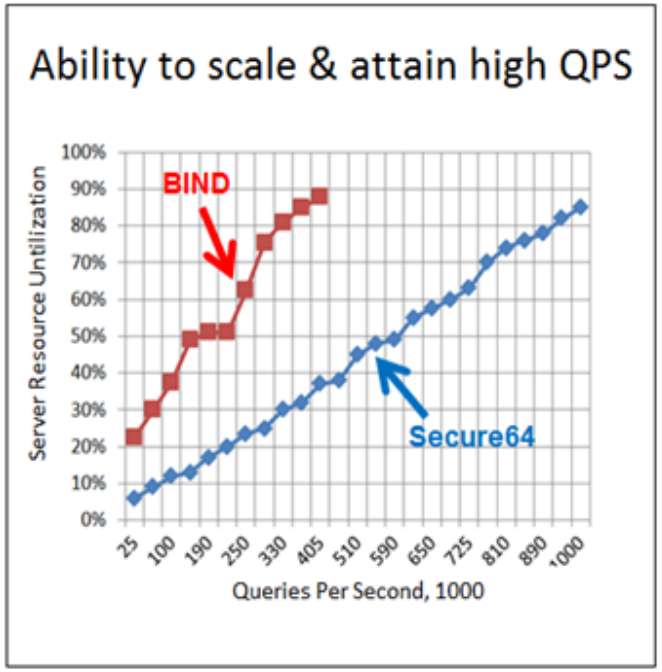
Source: NIST and other sources, 2014-16

NIST



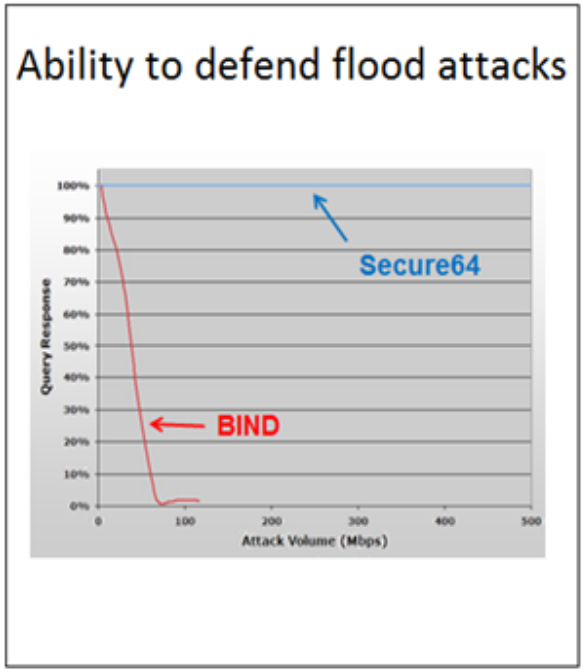
Source: NIST published data, 2012-16

NIST



Source: Farsight Lab & Secure64 Lab

FARSIGHT



Source: Extreme Labs, California

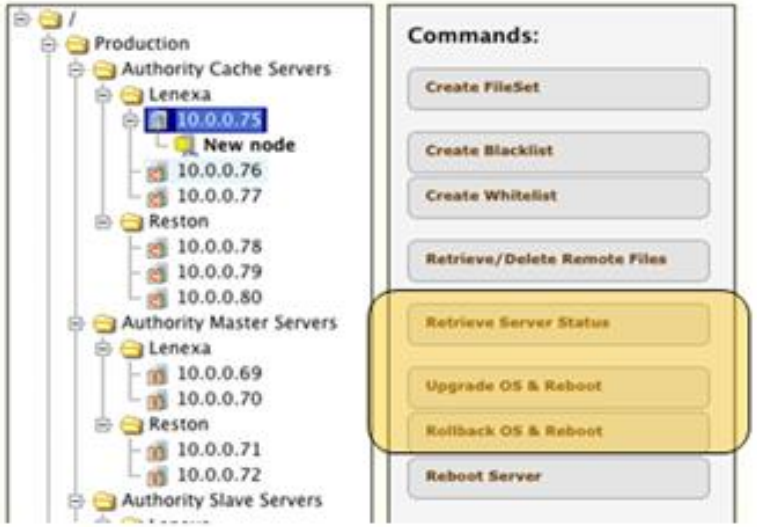
EXTREMELABS, INC.

Blacklist & Whitelist editor

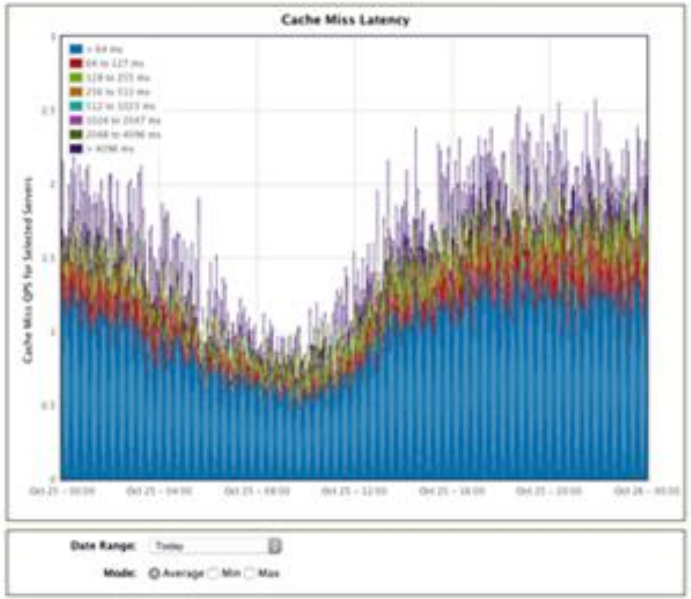
Config Editor

Create Custom Reports

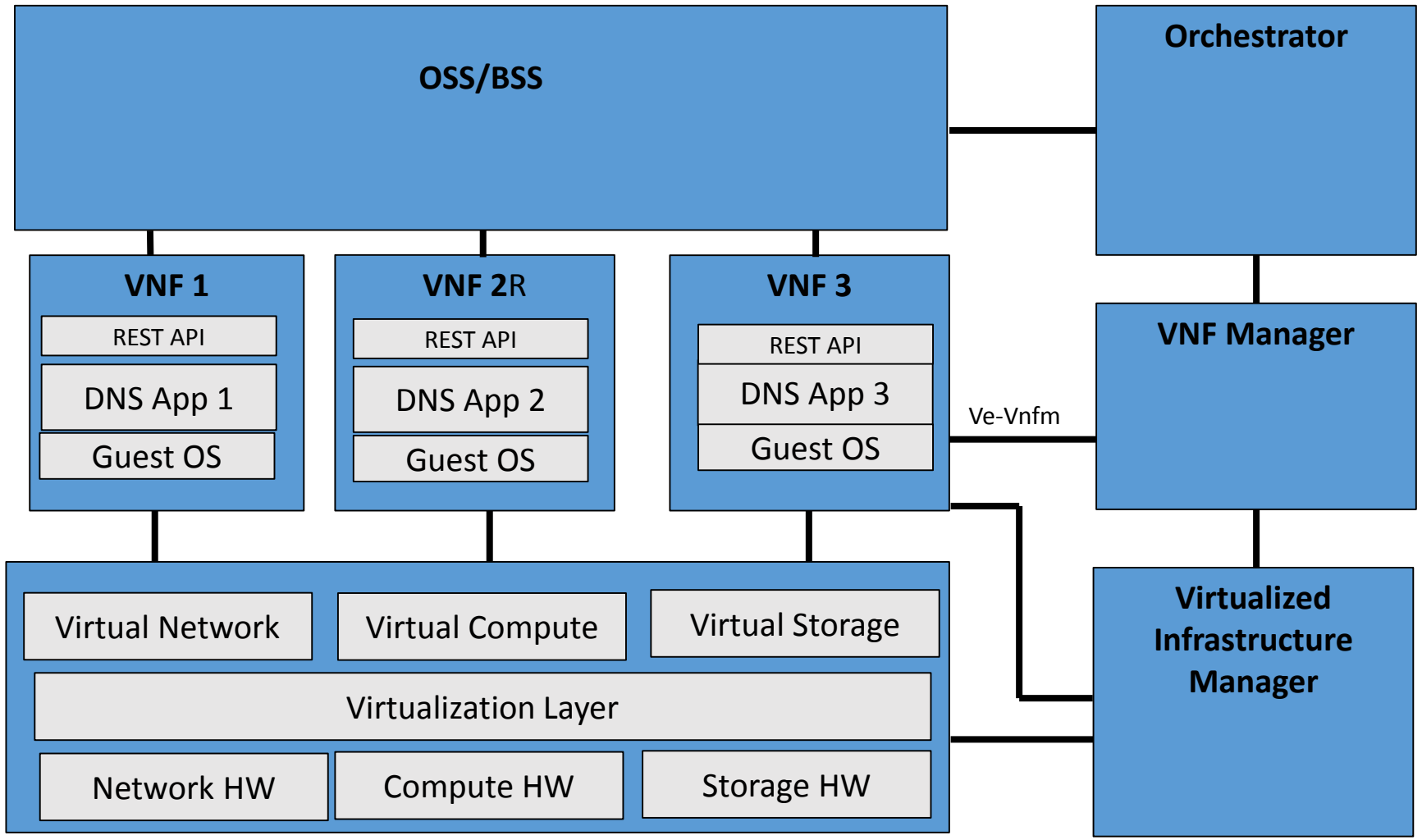
Software updates, version control & rollback



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**

Thank you