Harness Your Internet Activity

Vantio AuthServe

Enabling Efficiency and Service Differentiation

Ralf Weber
October 13, 2014

Vantio AuthServe Authoritative DNS

Proven High-performance

- Tested with up to 1 Billion resource records per server
- Supports ~260kQPS
- 30K DDNS updates/sec
  - 3.5k write operations

Industry-leading DNS Security

- Completely new development over other choices: Based on lessons from writing BIND 8/9
- Superior security: Zero CVEs in ten year history
- Automated DNSSEC lifecycle management with event notifications

Always-on Service

- In-service configuration updates (no restart)
- Multimastering (dual active masters mirror DNS updates)

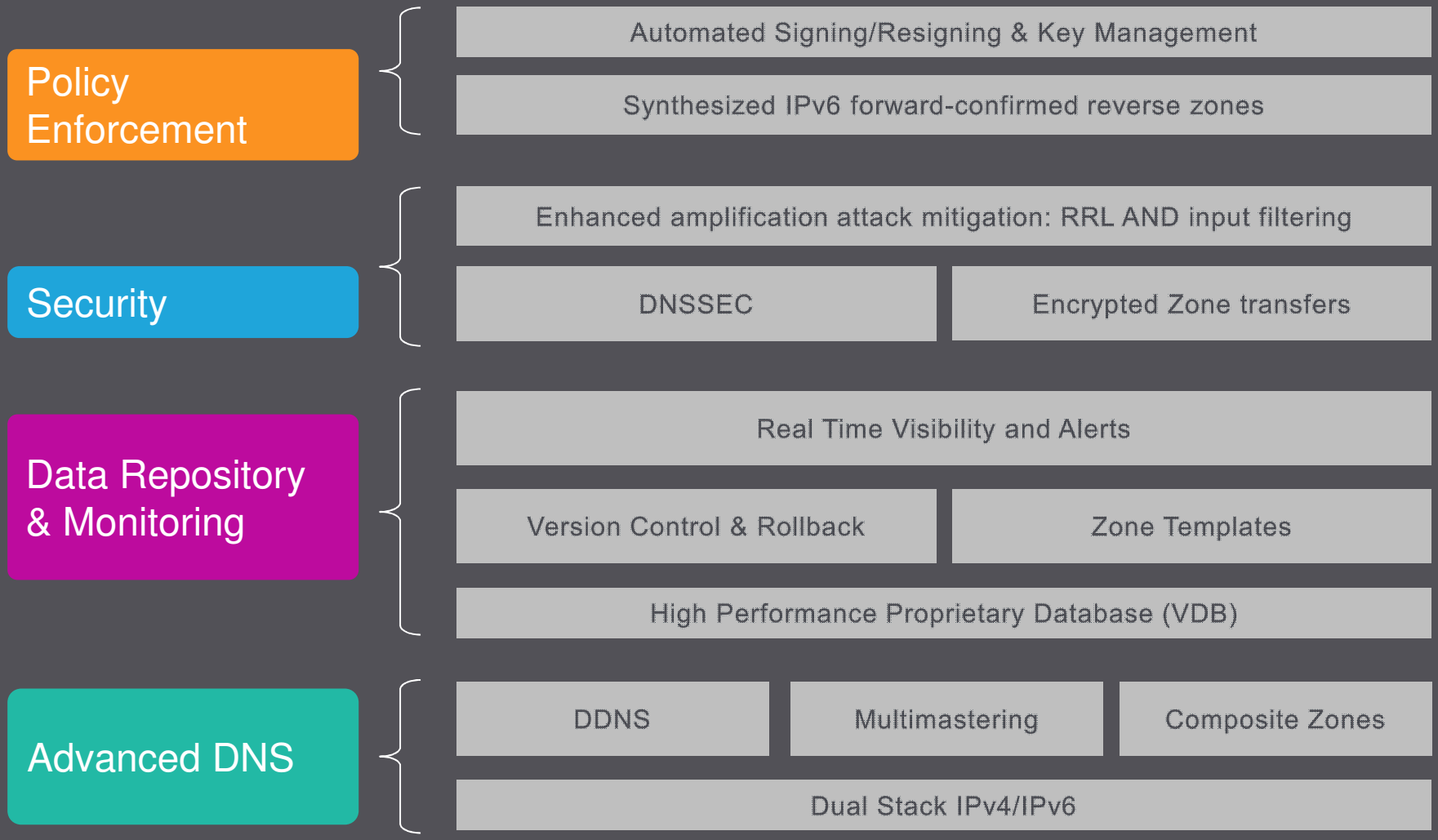
Extensible & Easy to Use

- C, Java, Perl, Python, SOAP/XML management APIs
- Zone configuration templates
- Zone versioning, rollback, diffs

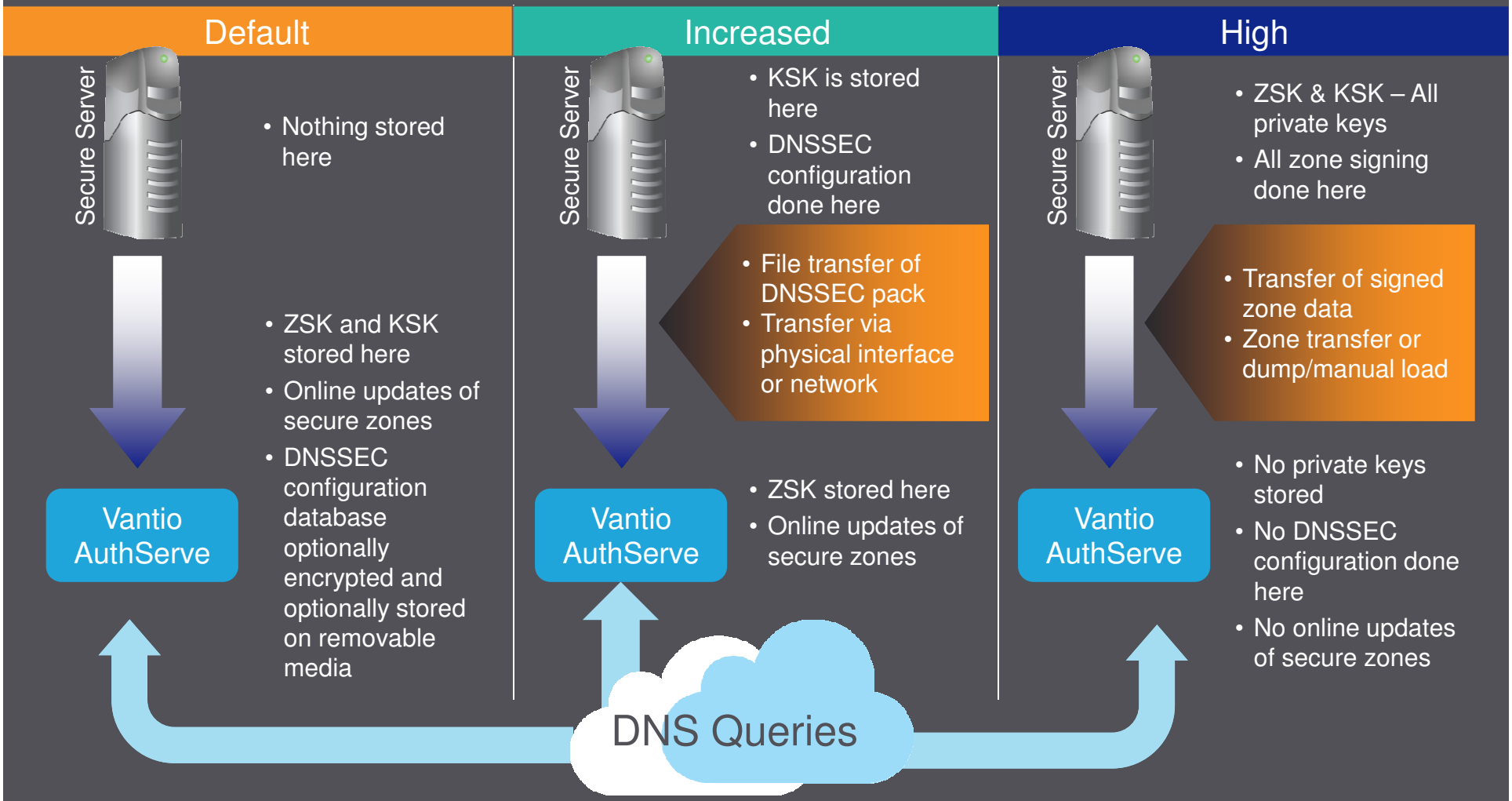
Network Visibility & Event Awareness

- Detailed analytical data of DNS queries
- Threshold-based alerting (SNMP, Syslog)

Unique Combination of Capabilities



DNSSEC Security Options



Complete DNSSEC Automation

CHALLENGES	NOMINUM SOLUTION
Key Administration • Manual key generation (many steps and utilities) • Manual tracking and scheduling for expired keys (zsk & ksk)	**DNSSEC Packs** • Administrative bundle that automates DNSSEC lifecycle: 1. Automatically signs and resigns zones 2. Automates key rollover (e.g. update every 60 days) based on policy 3. Manages publication of DNSSEC signed data • DNSSEC becomes transparent
Managing Signing Of Zones • Manually signing a large number of zones is impractical	
Updating Zones When Data Changes • Manual zone file re-signing when records are added, changed or deleted from a zone	
Signing/Resigning Zones Is Cpu-intensive	• Query response performance not affected by signing operations • Separate, dedicated CPUs used for signing operations (i.e. signing/resigning zones)
Database Size • Can grow by 6x… or more	• Performance of database not affected by increase in size

DNSSEC Enhancements

Managing Signed Zones (DNSSEC) As Easy As Managing Unsigned Zones (DNS)

- DNSSEC only visible as high-level policies (simple commands)
- No external tools (complete integration)

Supports offline, online, secondary, command line signing modes

- Offers deployment architecture flexibility with minimal impact.
- Allows slave servers to sign zones
- Allows management applications to sign zones

Superior Performance

- Takes advantage of multi-core architectures to sign zones online,
- No impact on 'fast path' query handling

Operational Focus

- Logging and events notification of key rollovers etc.
- Possible to integrate with network monitoring systems

Maximum automation

- Server automatically manages key lifecycles
- Eliminates error prone manual processes

Multimastering

Risks with Single Master Approach

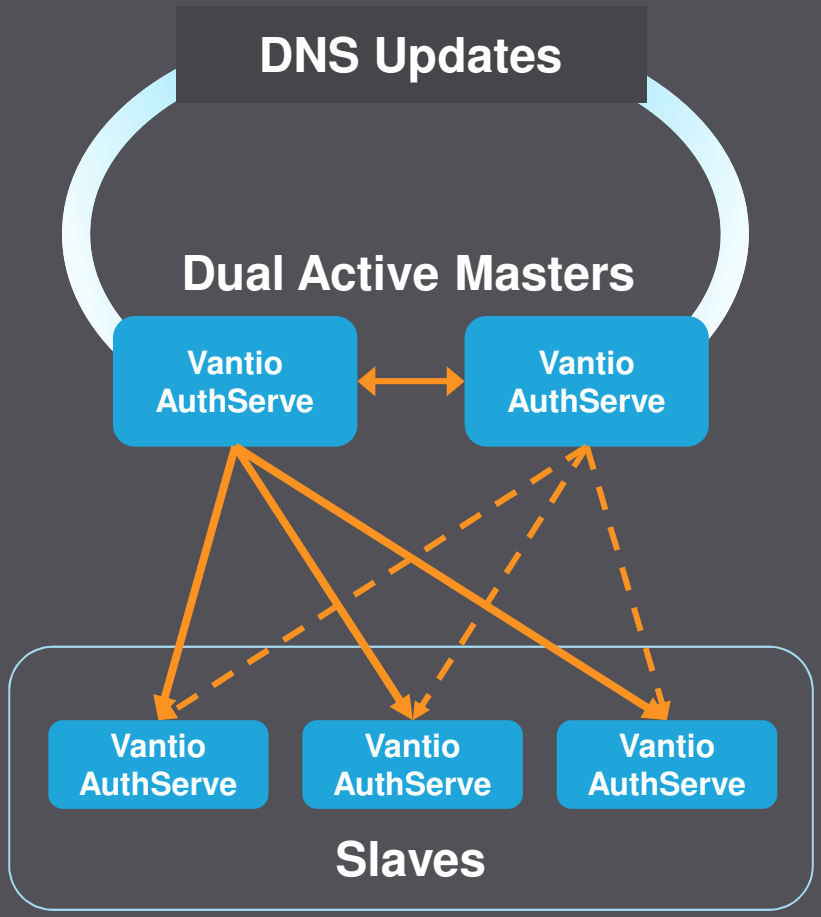
- Changes cannot be made when master fails
- Catastrophic in dynamic environments

Nominum Multimastering Advantages

- Complete data and service availability
  - During catastrophic events
  - During planned and unplanned maintenance windows
- Automatic healing after network changes
- Geographic redundancy
- Mirrored DNS updates
  - Automatic zone data propagation
  - Updates performed regardless of availability
  - No proprietary connections between masters
- Ease of configuration
  - No manual (human) conflict resolution
  - Automatic, rapid zone data convergence

Multimastering Use Cases Include

- Dynamic environments needing reliability such as data centers, VoIP, M2M, etc.



Flexibility and Extensibility

Focus on Data Management at Every Level

- In Service Configuration updates (no restart)
- Auto-generated reverse records for IPv6 and matching AAAA forward records

Management APIs

- Controls the software and overall DNS systems via command channel
- Communicates system information out of Vantio AuthServe via event channel

Zone Configuration Templates

- Replication of large amounts of information without manual entry
- Does not store redundant information
- Provides pointers to common zone files

Zone Versioning, Rollback & Diffs

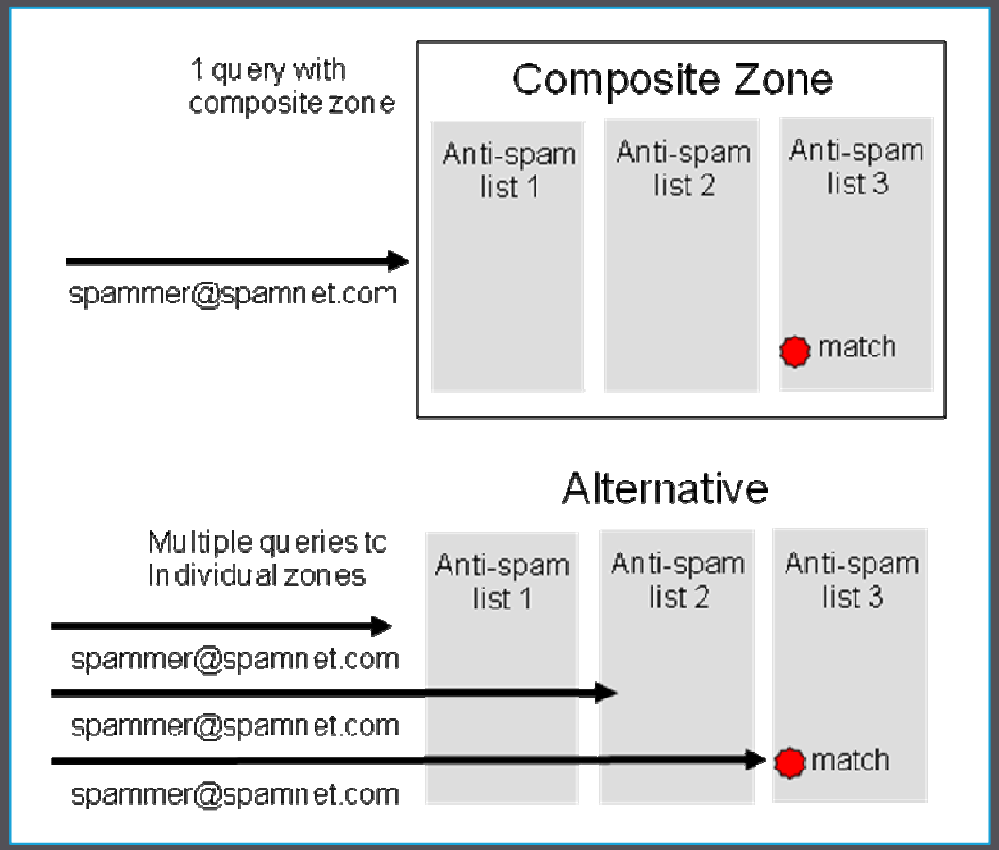
- Complete control over data management
- Reporting and recovery of data to previous states

Web based Graphical User Interface Option

- Centralized server and zone management with audit log
- Role-based access control

Composite Zones

- Patented technology
- Combine entries in multiple zones into a single combined (composite) zone
- Eliminates sequential searching through multiple zones
- Faster lookups for services like ENUM



Real-Time Visibility and Alerts

Real-time logging and statistical analysis of DNS query streams

Key Features

- Simple configuration, data collection over any time horizon
- Integrated data analysis and reporting interface
- Support of real time or offline analysis
- Much less taxing then query logging and network traffic snooping

Use Cases

- Targeted data collection to identify broad trends or pinpoint problems over any time horizon
- Top sources of traffic by provider, or other source
- Top domains queried – evaluate application or resource usage
- Domains queried with DO bit set
- NXDomains – detect cache poisoning attempts, misconfigured client

Amplification Attack Remediation

Input Rate Filtering – Vantio AuthServe Unique Features

- Better granularity to better target attack traffic
  - Filter based on query source IP (client) address
  - Filter based on query type (ANY, RRSIG, DNSKEY, etc.)
  - Filter on domain name
  - Filter on combination of all three
- Important advantages of input rate filtering
  - Protects the authoritative service itself - highly efficient
  - Protects the target of an attack
  - Protects the reputation of the provider/authoritative server

Response Rate Limiting (RRL)

- Rate limits responses (answers) to queries, not questions
- Server prepares responses, then rate limiting is applied
- Server work is wasted, but necessary for some types of queries

Combination of Input Rate Filtering and RRL gives Vantio AuthServe unmatched remediation capabilities

Vantio AuthServe Recent Changes

- Background
  - Rate Limiting (applies to Vantio as well)
  - Incremental improvements
- Features
  - Rate Limiting
    - Filter based on source IP (client) address, query type, domain name, response size, or any combination
    - Response Rate Limiting (RRL)
      - Rate limits responses (answers) to queries, not questions
  - Unique Auto-generated reverse records for IPv6 and matching AAAA forward records
    - Works with DNSSEC
    - Configuration works with zone transfers
  - DNSSEC
    - Slave zones have signing capability; allows for a signing server in middle
    - Remote generation of signing packs
    - Updated logging and events

Harness Your Internet Activity