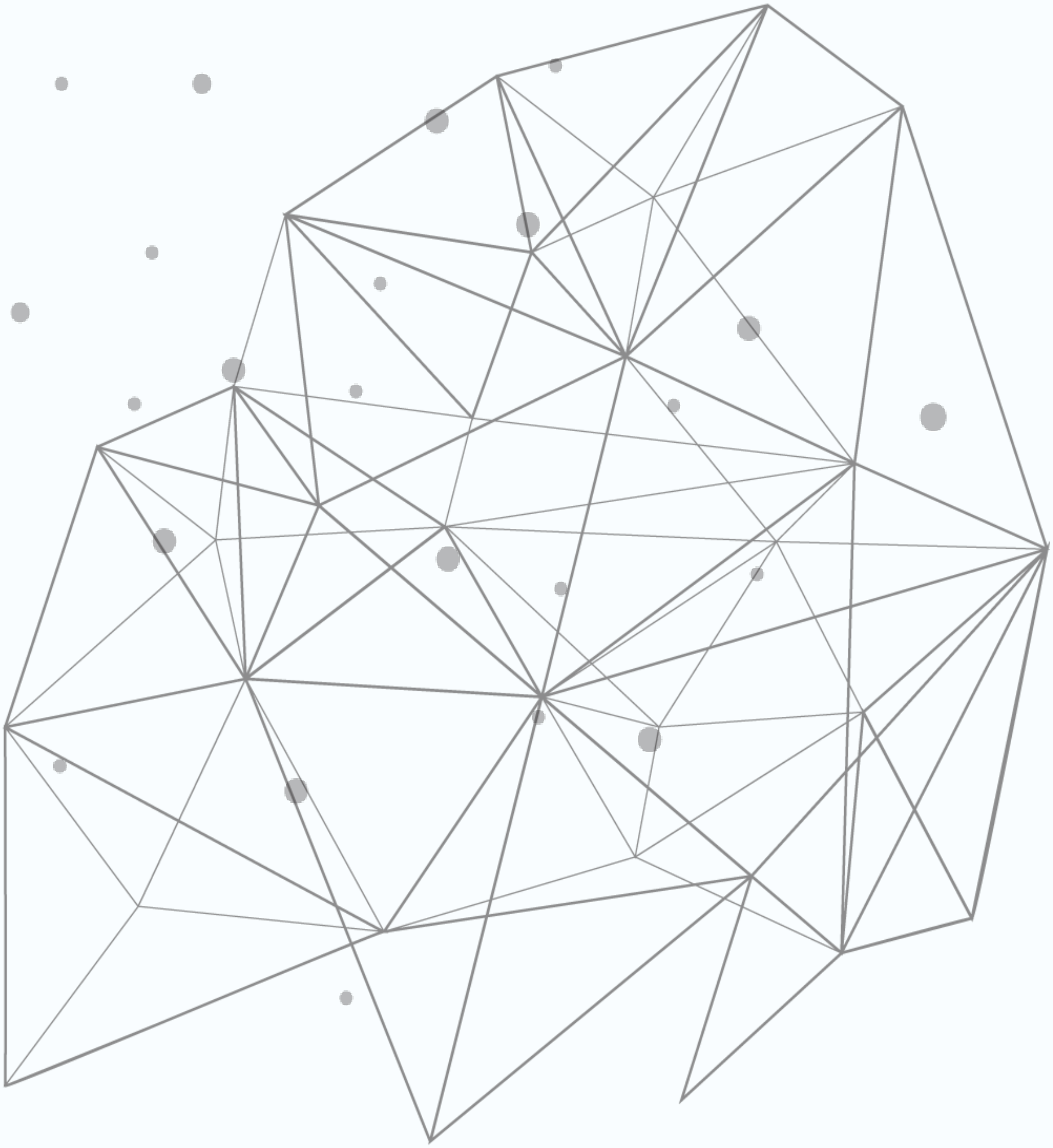
TCPWAVE DDI

Enterprise DNS Best Practices



October 2020

1 INTRODUCTION

To ensure the users efficiently execute the DDI tasks, and its optimal protection while using the TCPWave DDI application, we recommend the end-users to strongly adopt and implement the following DDI best practices that effectively manage your enterprise-grade solutions.

2 Architecture Recommendations

- **Placement**
  - **Recursive DNS**: Ensuring enterprises deploy, dedicated recursive DNS for all the outbound DNS traffic originating from Proxy, DMZ servers, and internal users. Implementing recursive Query ACL from authorized subnet and IP addresses.
  - **External DNS**:
    - **Stealth Primary**: Always implement stealth primary with multi-master mode for any unauthorized access. Should not appear in NS records to avoid any attempts of the DNS query. Restricted zone transfer to specific secondary authoritative DNS servers. Ensuring recursion disabled.
    - **Secondary**: Exposed to the internet for the user's DNS resolution. Restricted and encrypted zone transfers from stealth primary authoritative. Ensuring recursion disabled.
  - **Internal DNS**:
    - **Stealth Primary**: Always implement stealth primary with multi-master mode for any unauthorized access. Should not appear in NS records to avoid any attempts of the DNS query. Restricted zone transfer to specific secondary authoritative DNS servers. Ensuring recursion disabled.
    - **Secondary**: Exposed to the internet for the user's DNS resolution. Restricted and encrypted zone transfers from stealth primary authoritative. Ensuring recursion disabled in a proxy environment. In case recursion is allowed for direct application access like O365, it should be implemented with the necessary access list.
- **Security**
  - Access control list should be implemented queries and recursion on all DNS servers.
  - Rate Limiting: ensuring query rate limiting to avoid any DDoS event.

- Response Rate limiting: It should be implemented on recursive DNS for cache poisoning mitigation.
- DNS tunneling: It should be implemented on recursive DNS to avoid data breach and tunneling activities
- Query Logging: DNS query logging and reporting will provide traffic snapshots and helps in early detection/forensics of security incidents.
- High Availability: All the DNS servers should be deployed in HA.
- Encrypted: Zone transfers
- Encrypted DNS queries from internal clients with DNS over TLS.

3 Other Security Recommendations

- Built in TACACS+/LDAP/AD/RADIUS/SAML Authentication.
- Encrypted DNS and DHCP updates from the management to the remotes.
- Dual DNS engines: BIND/NSD DNS engine for the authoritative DNS appliances.
- Dual DNS engines: BIND/Unbound for the DNS cache appliances.
- SSH authentication using TACACS+/AD.
- No functional accounts at the operating system level with an interactive password.
- Hardened operating system.
- Web-based central patch management.
- Support for streaming logs into Splunk/SIEM.
- Security logs in the CEF format.
- Built-in Employee Entitlement Review System (EERS) integration.
- Granular auditing and reporting.
- Built-in fault management and configuration assurance engines.
- Ability to send SNMP traps to third party fault management systems.
- Ability to undo an object/subnet/scope/zone CRUD operation.
- SSL certificate support for the web interface, communication with the remotes.
- SSL certificate support for executing REST API calls from Automation systems.
- Web-based Disaster Recovery/High Availability management.
- Granular Permissions model.
- Segregation of duties supports that meets the TCPWave Information Security standards.
- Use standard and strong encryption algorithms.
- Prevention of cross-site scripting attacks and command-line injection attacks.
- Allow DDNS updates from trusted sources.
- Audit and syslog reports

Contact the TCPWave Sales Team

TCPWave

7H, Vyshnavi Cynosure, Gachibowli, Hyderabad, Telangana - 500032