WNS NetworkShield™ – Technical Overview for IT & Security Teams

1. Executive Summary

WNS NetworkShield™ is a managed DNS security platform designed to add a network-level control point in front of your users, devices, and SaaS applications.

By enforcing security policies at the DNS layer, NetworkShield:
- Blocks access to malicious, suspicious, and non-compliant domains
- Reduces the risk of phishing, credential theft, ransomware, and C2 callbacks
- Provides centralized visibility into DNS traffic across sites and user groups
- Integrates with your existing firewall, VPN, endpoint, and SIEM tooling

WNS delivers NetworkShield as a managed service – you keep control of your network; we own the tuning, threat intelligence, policy maintenance, and reporting.

2. Architecture & Deployment Model

NetworkShield is deployed as either:
- A WNS Secure Appliance (small footprint x86 hardware on-prem)
- A Virtual Appliance (VM) for Hyper-V, VMware, or compatible hypervisors

2.1 DNS Flow

1. Your internal resolvers / DHCP scope / firewall are configured to forward DNS requests to the NetworkShield appliance.
2. NetworkShield acts as a policy-aware recursive DNS resolver:
   - First evaluates the request against local policy and threat feeds.
   - If allowed, forwards the query upstream to trusted resolvers (e.g., DNS-over-TLS/DNSSEC-capable resolvers, depending on configuration).
3. Responses are cached locally to minimize latency and improve performance.

2.2 Redundancy & High Availability

Typical deployment options:
- Primary + Secondary Appliances within the same site
- Anycast-style configuration via your firewall/router for failover
- Optionally, a cloud-based failover resolver (WNS-managed) if on-prem appliance is unreachable

We work with your network team to align with your existing HA strategy (VRRP, HSRP, SD-WAN, etc.).

3. Security & Policy Capabilities

3.1 Threat Intelligence

NetworkShield consumes and maintains multiple DNS threat feeds, including:
- Known phishing and brand-impersonation domains
- Malware and ransomware distribution infrastructure
- Command-and-control (C2) and exfiltration domains

- Cryptomining and abuse-related domains
- Disposable / dynamic DNS services frequently used in attacks

Threat feeds are updated automatically on a scheduled basis managed by WNS.

3.2 Policy Categories & Controls

Policies are applied per:
- Network segment (e.g., corporate LAN, guest WiFi, OT network, lab, etc.)
- Site / location
- Optionally user groups (if integrated with directory or captive portal)

Supported policy types include:
- Domain and category blocking
- Custom allow/deny lists
- Block / redirect actions (NXDOMAIN, block page, silent block)

3.3 TLS/DoH Considerations

NetworkShield can be deployed alongside controls that prevent DNS bypass, such as:
- Firewall rules to block outbound port 53 and only allow DNS from authorized resolvers
- Rules to restrict DNS-over-HTTPS to approved upstreams (e.g., your own DoH gateway or none at all)

4. Integration with Existing Infrastructure

4.1 Firewalls & Routers

NetworkShield sits alongside existing firewalls (Fortinet, Cisco, Palo Alto, etc.) and typically integrates by:
- Pointing the firewall’s DNS forwarders at NetworkShield
- Updating DHCP scopes to hand out NetworkShield as primary resolver
- Optionally using policy-based routing for specific VLANs or sites

4.2 Active Directory / Identity

In AD environments, we can:
- Maintain your internal AD DNS for internal zones
- Forward external queries to NetworkShield
- Map requests per subnet/site to logical groups for reporting

If you’re using Azure AD / Entra ID and cloud-first architectures, we can align with your existing identity and perimeter strategy.

4.3 Remote Users & VPN

For remote or hybrid users:
- VPN users can be forced to use NetworkShield as resolver while connected
- Non-VPN users can be supported with agent-based DNS traffic redirection or split-tunnel configurations that route DNS to your central NetworkShield appliances

4.4 Logging & SIEM

NetworkShield logs:
- Timestamp, source IP, destination domain, category, action (allow/block), policy, site/segment

Options:
- Periodic log export (CSV/JSON) for ingestion into your SIEM
- Syslog or API-based integration (depending on environment)
- WNS can also provide summarized monthly reports for management and audit

5. Performance & Reliability

5.1 Latency

In most environments, NetworkShield adds single-digit millisecond latency, often offset by local DNS caching.

We validate:
- Query per second (QPS) capacity requirements
- Peak load patterns (e.g., morning login storms, scheduled updates, etc.)
- Appropriate hardware/VM sizing for your number of users and sites

5.2 Capacity Planning

We size the deployment based on:
- Number of users
- Number of active network segments / VLANs
- Remote user count
- Expected DNS QPS

6. Management & Operations

6.1 WNS-Managed Service

Your internal IT team retains control over business decisions, while WNS:
- Manages threat feed configuration and updates
- Tunes policies based on your risk tolerance and feedback
- Handles whitelisting/blacklisting requests
- Monitors appliance health and updates
- Produces periodic security and usage reports

6.2 Change Management

Process typically includes:
- Initial policy design workshop
- Staged rollout (monitor-only mode on certain segments first)
- Documented change requests for new policies, whitelists, and new segments/sites

7. Use Cases & Scenarios

7.1 Phishing & Credential Theft
- Block DNS resolution of domains used for fake Microsoft 365, Google Workspace, VPN portals, banking, and payroll systems.

7.2 Ransomware & C2 Communication
- DNS calls to known command-and-control and exfiltration domains are blocked.

7.3 Guest & BYOD Networks
- Apply stricter security policy (and optional content filtering) to guest WiFi and BYOD segments.

7.4 Distributed / Multi-Site Environments
- Use multiple appliances across branches or a central instance with VPN/SD-WAN.

8. Compliance & Governance

NetworkShield can assist with:
- Demonstrating technical controls for security frameworks (e.g., CIS, NIST, ISO27001, PCI-DSS elements around DNS and malicious site protection).
- Providing evidence for audits (reports on blocked malicious domains, policy definitions, and change logs).
- Supporting internal security policy (acceptable use, segmentation, least privilege).

9. Typical Implementation Timeline

1. Discovery
2. Design & sizing
3. Deployment
4. Pilot / monitoring mode (optional)
5. Full enforcement
6. Monthly / quarterly reviews

10. Who Should Be Involved on Your Side

For the smoothest deployment, we recommend including:
- Network engineer / architect
- Systems engineer (DNS, AD, DHCP, VPN)
- Security lead / CISO / vCISO
- IT manager / operations