DATA SHEET

Secure64® DNS TunnelGuard™

Block bandwidth piracy &
stop data exfiltration

KEY BENEFITS

- Prevents the loss of revenue from bandwidth piracy
- Prevents theft of sensitive information via the DNS
- Enables regulatory compliance
- Protects your brand

KEY FEATURES

- Detects & blocks common DNS tunneling software
- On-box behavioral analysis
- Engages instantly to block tunnels in real time
- Customizable blocking and whitelists
- Captures tunnel metrics for reporting

In countries where data plans are limited, service providers face loss of revenue from subscribers that use DNS tunneling software to bypass data limits. DNS tunnels allow users to access the internet utilizing the unmetered DNS protocol without paying for the data they use.

Additionally, DNS tunneling software can be used by attackers to exfiltrate stolen data, which can be country or corporate secrets.

In some countries, service providers are required to prevent the exfiltration of data.

Secure64 DNS TunnelGuard is part of a family of DNS-based security services that protect the network and its users. DNS TunnelGuard is an on-box security service that uses sophisticated and proprietary technology to detect and automatically block the most common DNS tunnels, including Iodine, dns2tcp, dnscat2, oxymanDNS and others, with a high degree of accuracy, and minimal impact on DNS performance. TunnelGuard analyzes and detects tunnels on the DNS Cache server itself, resulting in much faster detection, blocking tunnels before they have a chance to cause harm.

DNS TunnelGuard also captures information on tunnel activity, which is retrieved by DNS Manager and used to generate insightful reports.

DNS Tunnel Guard is offered on both Secure64 platforms – Itanium/SourceT and on the x86 line.

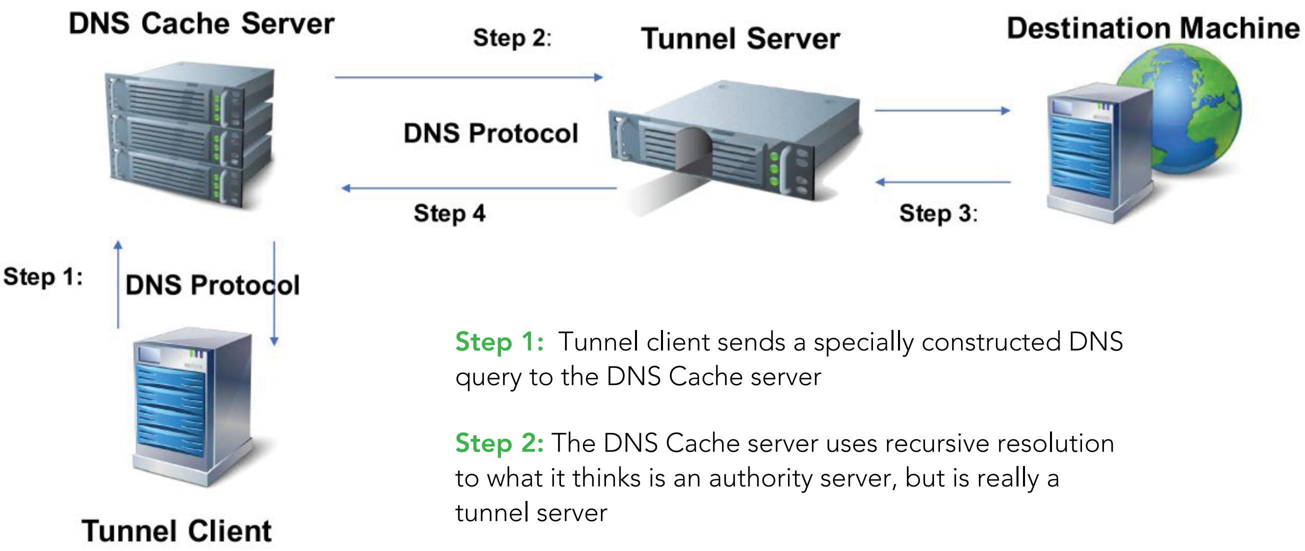
DATA SHEET

Secure64® DNS TunnelGuard™

Block bandwidth piracy &
stop data exfiltration

DNS Tunneling Detection

The operational environment in which DNS tunneling will typically be deployed complies with the following:



Step 1: Tunnel client sends a specially constructed DNS query to the DNS Cache server

Step 2: The DNS Cache server uses recursive resolution to what it thinks is an authority server, but is really a tunnel server

Step 3: Tunnel server talks to a destination machine to either send file content for exfiltration or to a web server for free internet browsing

Step 4: Tunnel server responds with DNS packet, which Cache server returns to tunnel client

Learn more about Secure64 DNS Solutions at **www.secure64.com**