HS

HORIZONSHIELD

Securing Your Digital Future, Today.

INFRASTRUCTURE SERIES · BOOK 10 OF 16

Network Security Guide

Architecture, Defence & Monitoring — 2026

Complete network security guide covering architecture design, firewall strategy, protocol security, intrusion detection, wireless security, and SD-WAN/SASE frameworks — with practical configuration examples.

PROTOCOLS	TOOLS	STANDARD	LEVEL
30+	40+	CIS Controls v8	Intermediate

Contents

NETWORK SECURITY 2026

CHAPTER 01

Network Security Architecture

A well-designed network makes lateral movement expensive and detection easy.

DEFENCE IN DEPTH | SEGMENTATION | DMZ | MONITORING

Defence-in-Depth Network Architecture

Layer	Controls	Purpose	Detection Capability
Internet Edge	Next-gen firewall, DDoS mitigation, DNS filtering	Block known-bad inbound, geo-block, rate limit	Perimeter threat intelligence, flow analysis
DMZ	WAF, reverse proxy, email gateway	Isolate internet-facing services from internal network	Application-layer attack detection
Internal Network	NAC, network IDS/IPS, segmentation	Detect and limit lateral movement between segments	East-west traffic anomaly detection
Server Segment	Host-based firewall, EDR, file integrity monitoring	Protect servers from compromised workstations	Host-based IOC detection
Data/Database Tier	DB firewall, DLP, column-level encryption	Last-resort data protection	Unusual query patterns, bulk extraction detection

```
# Cisco IOS — Basic hardened firewall rules
# Best practice: explicit deny at end, log all denies

ip access-list extended INBOUND-INTERNET
 ! Allow established sessions returning
 permit tcp any any established
 ! Allow HTTPS to DMZ web servers only
 permit tcp any 203.0.113.10 0.0.0.0 eq 443
```

```
 permit tcp any 203.0.113.10 0.0.0.0 eq 80
 ! Block all RFC1918 private IPs from internet (spoofing)
 deny ip 10.0.0.0 0.255.255.255 any log
 deny ip 172.16.0.0 0.15.255.255 any log
 deny ip 192.168.0.0 0.0.255.255 any log
 ! Block BOGON/unallocated addresses
 deny ip 0.0.0.0 0.255.255.255 any log
 ! Explicit deny all with logging
 deny ip any any log

# Default outbound — deny not allow:
ip access-list extended OUTBOUND-INTERNET
 permit tcp 10.0.0.0 0.255.255.255 any eq 443
 permit tcp 10.0.0.0 0.255.255.255 any eq 80
 permit udp 10.0.0.0 0.255.255.255 any eq 53
 permit tcp 10.0.0.0 0.255.255.255 any eq 25  ! SMTP from mail server only
 deny ip any any log  ! Block and log all other outbound
```

LOG EVERYTHING AT THE PERIMETER

A firewall with no logging is a lock with no video camera. You need to know what is being blocked AND what is getting through. Forward firewall logs to SIEM. Alert on: (1) new outbound destination IPs not seen before, (2) connection spikes to single destination, (3) off-hours connections from user workstations, (4) connections to known-malicious IPs or Tor exit nodes.

CHAPTER 03

DNS Security

DNS is both a critical protocol to secure and an invaluable security monitoring data source.

DNSSEC | DNS FILTERING | DNS LOGGING | C2 DETECTION

DNS Security — Configuration & Monitoring

DNS Security Control	Implementation	What It Prevents	Effort
DNS filtering (recursive)	Cloudflare Gateway, Cisco Umbrella, Pi-hole with blocklists	Malware C2 callbacks, phishing domain resolution, botnet communication	LOW — 1 hour to deploy
DNSSEC (authoritative)	Enable on your domain registrar — signs records cryptographically	DNS cache poisoning, DNS spoofing attacks against your domain	MEDIUM — 2 hours, verify with dnssec-debugger.verisignlabs.com
DNS over HTTPS/TLS (recursive)	Configure resolvers to use DoH/DoT to upstream	ISP/attacker interception of DNS queries — query privacy	LOW — configure in router/client
Disable zone transfers	Restrict AXFR/IXFR to authorised secondary NS only	Full domain enumeration via zone transfer	LOW — 30 minutes
Disable recursive DNS on public servers	Separate authoritative and recursive DNS servers	DNS amplification DDoS using your servers	MEDIUM — architecture change

DNS Security Control	Implementation	What It Prevents	Effort
DNS logging & SIEM integration	Forward DNS resolver logs to SIEM	C2 detection, malware identification, data exfiltration via DNS tunnelling	MEDIUM — log forwarding setup

```
# Detect DNS tunnelling (C2 exfiltration via DNS TXT/NULL records)
# Zeek/Bro query: detect unusually long DNS queries (tunnelling uses subdomain encoding)

# Suricata rule for long DNS queries:
alert dns any any -> any 53 (
  msg:"Potential DNS Tunneling - Long Query";
  dns.query; content:"."; pcre:"/^.{50,}$/";
  threshold:type threshold, track by_src, count 10, seconds 60;
  classtype:policy-violation; sid:9000001; rev:1;
)

# Splunk: hunt for DNS tunnelling
index=dns
| eval query_len=len(query)
| where query_len > 50
| stats count avg(query_len) as avg_len by src_ip, dest_ip
| where count > 20 AND avg_len > 40
| sort -count
# High frequency long queries = likely DNS tunnelling or DGA domain generation
```

DNS LOGGING IS ONE OF YOUR MOST VALUABLE SECURITY DATA SOURCES

DNS queries reveal: (1) C2 beaconing — regular interval lookups to unusual domains, (2) DGA malware — pattern of random-looking domain queries, (3) DNS tunnelling — encoded data in long subdomain queries, (4) Phishing — lookups to lookalike domains (microsoft-support.com vs microsoft.com). If you are not logging DNS, you are forensically blind to these attacks.

HS

HORIZONSHIELD

Securing Your Digital Future, Today.

Network Security Guide 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.