



donjonet.

Version 1.2

Donjonet is a gateway-level network security solution that extends a sphere of security around all connected IT-assets, constantly safeguarding the enterprise from in-bound cyber threats. Donjonet offers fault-tolerant deployment architecture and provides manageability at all levels such as SD-WAN, VPN, LAN, vLAN, traffic shaping, user-groups, IP-groups, captive portal etc. In addition, it provides a wide range of configuration options to granularly manage content and access rights and to implement simple DLP rules.

With the confluence of several functionalities, Donjonet provides a seamlessly unified security gateway experience to its users.

CONNECT

Choose diverse connectivity for branch offices. Donjonet Unified Gateway provides seamless, technology agnostic multi-ISP connectivity options with auto link failover, QoS and metering.

SECURE

De-risking Access

The UTM features of Unified Gateway include inline AntiVirus engine for HTTP, FTP and email access with Anti-SPAM engine for emails. Strong security measures like Stateful Packet Inspection and Intrusion Detection System keep intruders and hackers out. Site to site and nomadic VPN, using SSL or IPSec allow remote users access relevant resources without any risk of data theft.

Dynamic Content Filtering

Proxies enable restricted web access, bandwidth restrictions on upload and download and blocking of categorized websites. Coupled with built-in user management, authenticated access can be enabled only to trusted users.

Authentication

User authentication via LDAP, external Active Directory and group management ensure that only privileged users can access external sites and resources.

MANAGE

Detailed Usage Data

The Unified Gateway provides a comprehensive view of WAN usage, on a per application or host basis. For example, browsing, email or SAP usage per user can be categorized and scheduled reports can be sent to the network administrator. The period of storage of usage data on the appliance is fully configurable.

Monitoring

The built-in monitoring and management server can proactively monitor its network, business applications and connected network devices to generate reports that pinpoint either a bandwidth problem or an unauthorized user access to the Internet. Statistics are collected on the network devices like routers, switches, servers, network links, hosts, and other network devices using SNMP protocol. The administrator can analyze collected data traffic to prioritize business critical applications over other traffic to meet the SLA requirement.

Configuration

The integrated dashboard view of all monitored nodes and services presents a comprehensive picture of the network. The intuitive GUI helps the administrator configure complex network options remotely using a browser.

KEY FEATURES

- ❖ STATEFUL FIREWALL
- ❖ IDS / IPS
- ❖ SD-WAN WITH FAILOVER AND LOAD BALANCING
- ❖ VPN
- ❖ TRAFFIC SHAPER
- ❖ WEB PROXY
- ❖ WEB PROXY AUTO-DISCOVERY (WPAD/PAC)
- ❖ EDGE AV
- ❖ CAPTIVE PORTAL
- ❖ HIGH AVAILABILITY (FAILOVER)
- ❖ USAGE REPORTING
- ❖ TROUBLESHOOTING TOOLS
- ❖ CONFIGURATION BACKUP / RESTORE
- ❖ OPTIONAL: EMAIL WITH ANTI-VIRUS & ANTI-SPAM



SYSTEM REQUIREMENTS

Donjonet can be installed on any work-station, server-class hardware or network appliances
The solution comes bundled with its own operating system, FreeBSD.

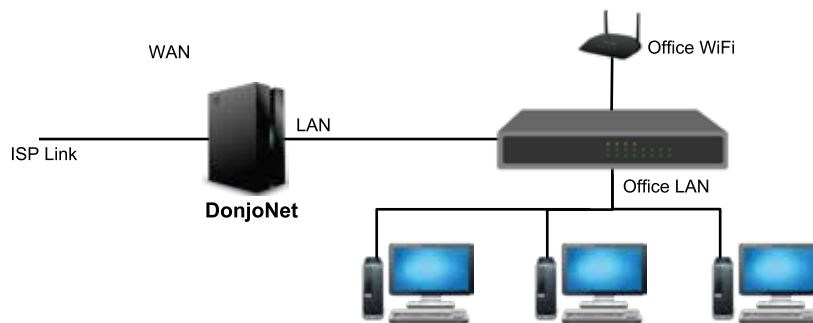
Minimum Hardware Requirements

Processor 1.5 GHz dual core or equivalent
Memory 2 GB
LAN Ports 2 No.s
Hard Disk 40 GB

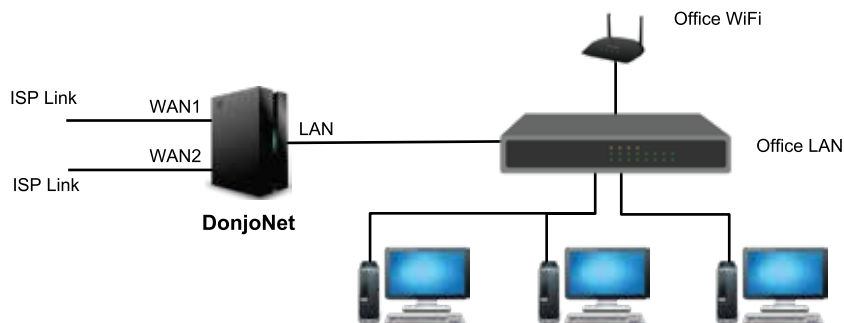
This configuration can handle up to 150 concurrent users.
For your specific requirements, please contact sales@perforsys.in for hardware sizing.

SAMPLE DEPLOYMENT SCHEMATICS

Single WAN

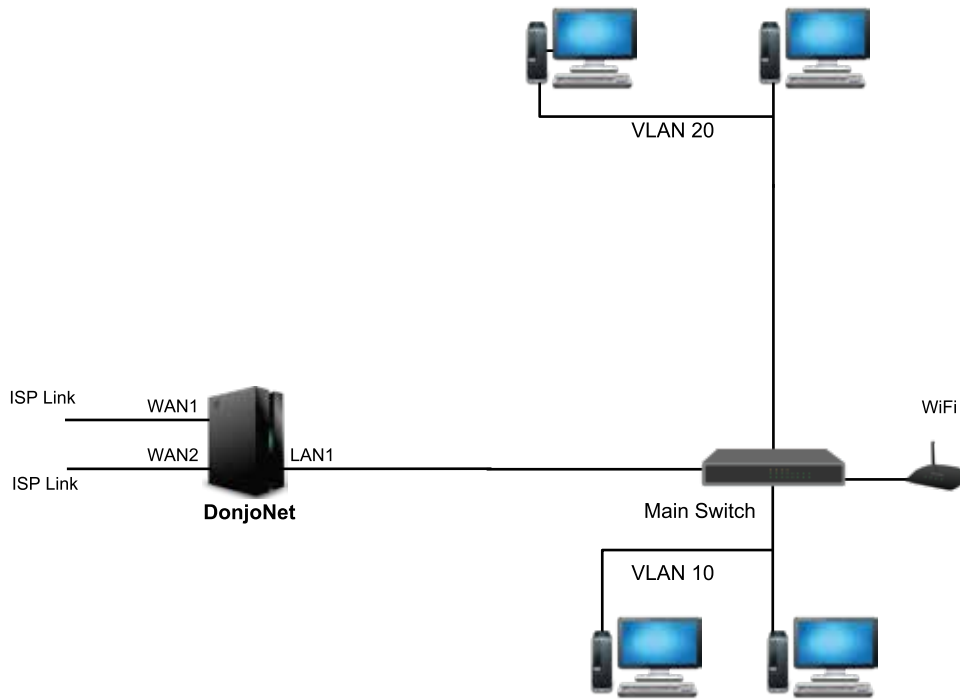


Multi WAN

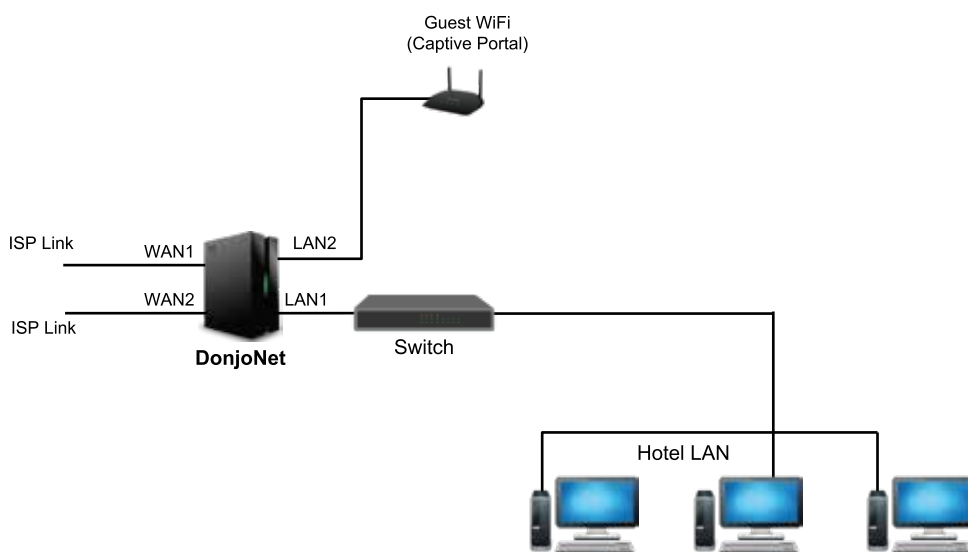


Note: Donjonet supports HA configuration. As an alternative to Donjonet workstation (above), a network appliance or a server hardware could also be used.

VLAN

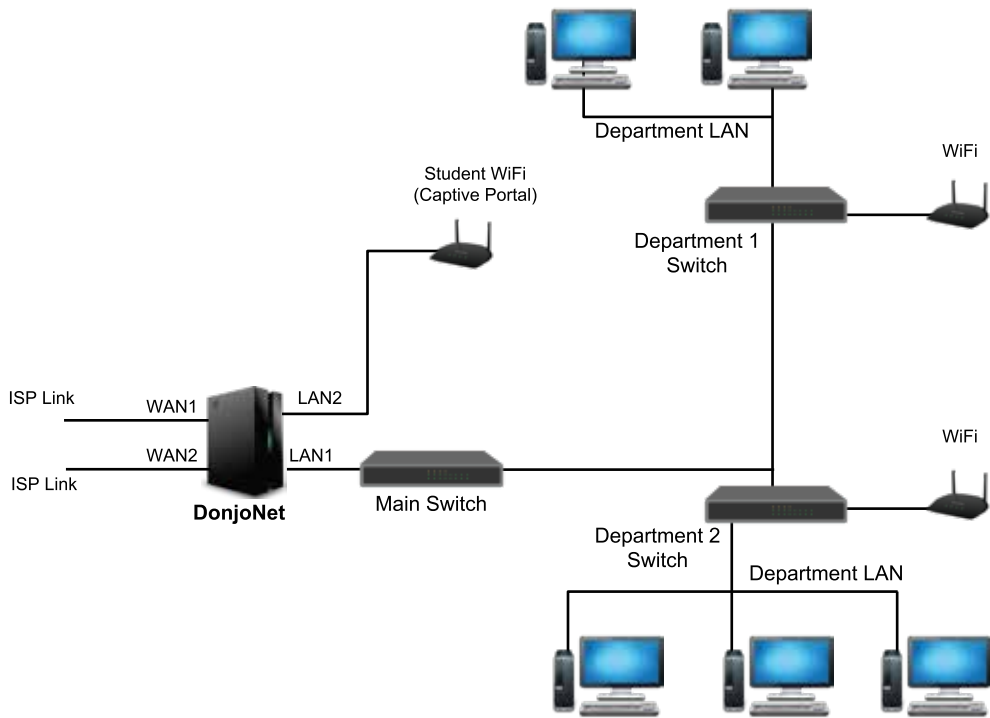


Hospitality

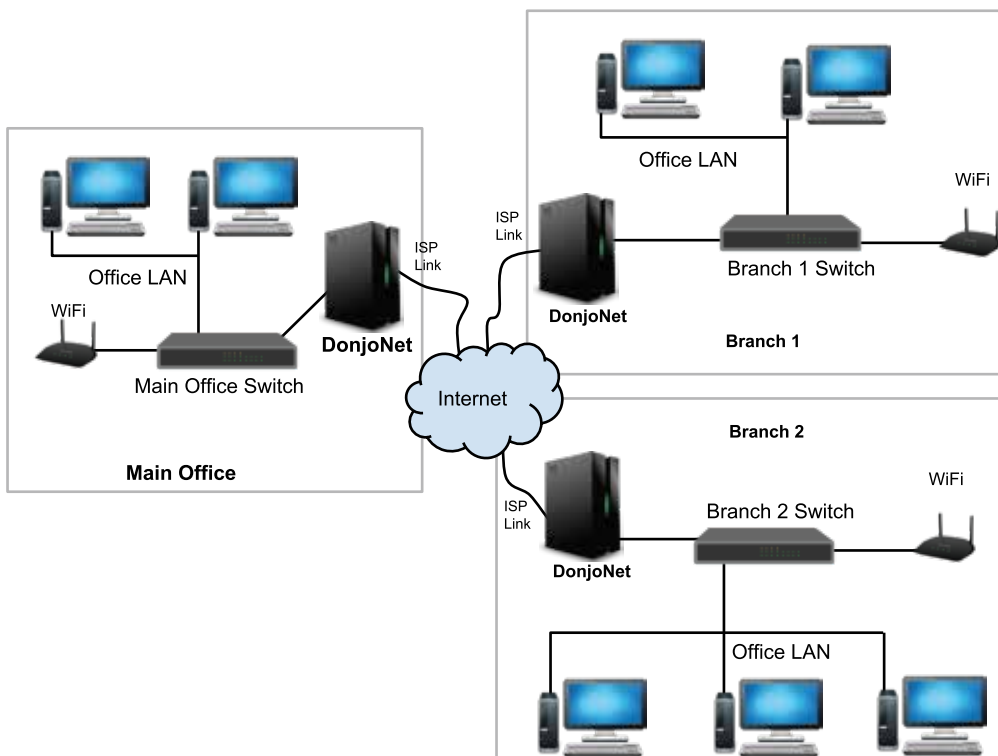


Note: Donjonet supports HA configuration. As an alternative to Donjonet workstation (above), a network appliance or a server hardware could also be used.

SMB/SME



Distributed Enterprise



Note: Donjonet supports HA configuration. As an alternative to Donjonet workstation (above), a network appliance or a server hardware could also be used.

SPECIFICATIONS

Firewall

- Stateful
- Enable / Disble
- Filter by
 - ◇ Source
 - ◇ Target
 - ◇ Protocol
 - ◇ Port
 - ◇ Operating System
- Limit per rule base
- Log traffic

NAT

- Port forwarding
- One to One
- Outbound
- Reflection

DHCP Server

- IPv4 , IPv6
- Supports Relay
- BOOTP

Multi WAN

- Load Balancing
- Failover

Traffic Shaping

- Bandwidth Pipes
- Bandwidth Groups
- Divide Bandwidth

VPN

- IPSec
- OpenVPN
- L2TP

Authentication

- Local
- LDAP
- Radius

802.1Q VLAN support

- Maximum 4096 VLAN's

SNMP

External Monitoring

IGMP Proxy

Multicast Routing

Intrusion Detection & Prevention

- Inline
- Rulesets
 - ◇ SSL Blacklists
 - ◇ Feodo Tracker
- SSL Fingerprinting
- Automate updates

Captive Portal

- Guest Network
- Hotel Wifi
- School/College Wifi
- Custom Login Theme
- Zones
- Filtering
- Voucher Management
- Reporting

Reporting

- Network Usage
 - ◇ LAN
 - ◇ WAN
 - ◇ VPN
- Web Proxy Usage
- Live Monitoring

Modern User Interface

- Dashboard
- Widgets
- Live Traffic
- Live Logs

Dynamic DNS

- List
- Custom
- RFC 2136

DNS Forwarder

- Supports Overrides
- DNS Server
 - Overrides
 - Access Control

DNS Filter

- OpenDNS Support

High Availability

- Automatic Failover
- Firewall Sync
- Configuration Sync

Web Proxy

- Supports multiple interfaces
- Caching
- User Groups
 - ◇ LDAP/Authentication
 - ◇ IP Based
- Blacklists
- Traffic Management
- Antivirus
- WPAD/PAC

Troubleshooting

- Firewall Tables
- Open Sockets
- Ping
- Packet Capture
- DNS Lookups
- NDP Table
- ARP Table
- Port Test
- Traceroute
- Logs

