DNSBOX200

ULTRA-SECURE, HIGH PERFORMANCE DNS/DHCP SERVER

DNSBOX200 is a DNS slave, recursive resolver (DNS cache) and DHCP server for premium performance and security needs.

This is a flexible appliance, which can be licensed for whichever of these 3 services you need.

For the chosen role(s), it will adapt to give you a high performance fit-for-purpose device:

- An adaptive GUI hides features you do not need
- It integrates smoothly with **DNS**BOX300 or **DNS**BOX400 to provide a complete solution
- Equally, it can be deployed standalone to carry out a specific role

Additionally, **DNS**BOX200 can be used as a master for editing authoritative DNS records.

Its advanced design, with roles and services separated, gives you

- Advanced performance
- Advanced security

You get to follow the best practice approach of deploying separate, isolated services, yet only need to pay for and manage one physical server

When you use the authoritative resolver (DNS slave)...

- Isolation from the recursive resolver service means authoritative DNS has another layer of protection, with any possible exposure via more vulnerable DNS caching eliminated
- You have the specialist DNS admin features you need on a slave: granular control and monitoring of your slaved zones; flexible zone transfer options
- Security features include support for DNSSEC signed zones and secure connections with other DNS servers in your architecture

When you use the recursive resolver (DNS cache)...

- Separation of recursive and authoritative resolver roles means extra security and maximum performance
- A purpose-built specialist recursive resolver delivers carrier-grade caching performance, security and control
    - 2.5x performance of BIND
    - Protects against DDoS attacks and cache poisoning

When you use the DHCP server...

- Fully-featured DHCP management software, controlling industry-standard ISC DHCPD, makes configuration easy and accurate
- It is simple to set up DHCP failover to ensure maximum availability of this critical service

DNSBOX200 Benefits

Maximum security

- Separate isolated resolvers: different processes, on different IP addresses and different NICs
- Specialist recursive resolver, purpose-built to protect against DNS cache threats
- Full DNSSEC support
- Secure links to other DNS servers
- Granular control of network traffic to appliance
- **DNS**BOX hardened appliance features

Maximum performance

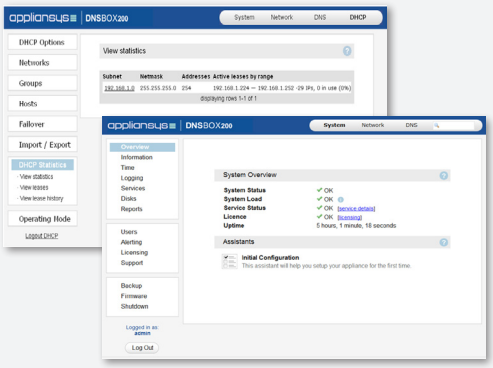
- Dedicated resolvers in own processes run faster
- Specialist DNS cache delivers 2.5x more queries per second than BIND

Supports resilient architectures

- 10x more reliable with solid state storage
- Easy and flexible high availability options for authoritative DNS, recursive DNS and DHCP

Supports advanced IPAM/DNS/DHCP system

- Integrates seamlessly with **DNS**BOX300 and **DNS**BOX400
- Anycast support
- Support for IPv6 and DHCPv6 systems



Three degrees of separation

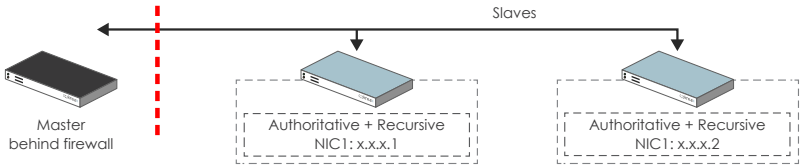
Building DNS Best practice architectures with DNSBOX200

DNSBOX200 helps take DNS Best Practice to an advanced level where security and resilience are even more important than usual.

A principle for DNS Best Practice architectures is separation of roles: within an overall architecture, different servers are deployed, each dedicated to carrying out a specific role. The reasons for this separation of roles are:

- Resilience – putting a server on the LAN in case the WAN connection fails
- Redundancy – eliminating a single point of failure
- Security – keeping services apart if one might expose another to a threat
- Latency and service performance – keeping a service near to its users and dedicating a server to one task rather than several

1. The separation principle starts with the basic master-slave architecture of DNS Best Practice: instead of a single DNS server, a master behind a firewall for security, queries served from at least two slaves for redundancy.



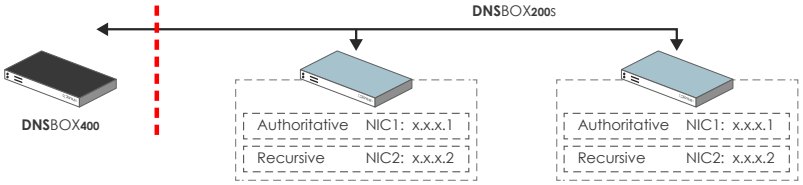
Typically, this scenario might see BIND on each slave server, acting as both an authoritative slave and a DNS cache (recursive resolver).

In advanced cases, the separation principle goes further. Authoritative and cache roles are split onto separate servers. The main reason for this is security – isolating the authoritative resolver from more vulnerable DNS cache.

Other common examples of separation of roles include separating different DNS Views onto different DNS slaves, and decentralising DHCP to multiple smaller subnets.

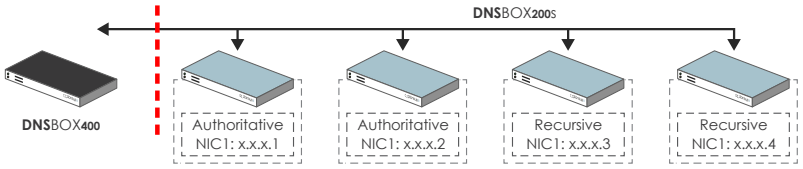
The downside of continuing to apply the separation principle is an increased number of servers to manage and increased cost.

2. With **DNS**BOX200, you have a neat solution to this. If you want to separate services for increased security or performance, you can do so while still needing just one physical server.



Each service runs as completely independently in its own “sandbox”, a secure chroot, held on a RAMdisk. Each can be served from a separate IP address and over a different NIC.

3. With **DNS**BOX200 you can have it either way. If you want to separate roles to different physical devices, **DNS**BOX200 is still a neat solution. When you deploy it for just one service – authoritative DNS, DNS cache or DHCP – you have a fit-for-purpose cost-effective solution.



- You only pay for the service you need
- The GUI hides features you don’t need so they don’t get in your way
- Each service uses software specialised for that particular service

DNSBOX200 - Key Features

Authoritative DNS slave

- Managed BIND resolver, with support for TSIG and IP secured zone transfers
- Delete zones, force updates, display zone files
- Full support for DNSSEC signed zones
- Compatible with any standards-compliant DNS Server
- Regular zone backups from master
- IPv6 support

DNS cache

- High performance recursive resolver Unbound, with support for forward zones and global forwarding
- Optimised DNSSEC validation
- Denial of Service (DoS) protection
- Cache poisoning protection - max randomness for query ID and port, case preservation, response scrubbing, access control
- High Availability Load Balanced clustering

DHCP Server

- Easy DHCP configuration with automated validation and custom configuration
- Reports on live & historic DHCP usage
- Automated DHCP failover replicates data to a secondary active unit
- DHCPv6 support

Easy appliance management

- Secure, easy to use web interface
- Simple, safe upgrades: firmware update with option to rollback to previous version
- Graphical performance and system health reports
- Email, SMS and SNMP alerts
- Output to remote Syslog server
- Can be managed seamlessly from **DNS**BOX300/400
- Unlimited simultaneous administrators

Appliance Security & reliability

- Each service runs in its own process in a ‘sandbox’ - secure chroot, held on RAMdisk
- Each service can be served from separate IP address over a separate NIC.
- Hardened ApplianSys Linux OS. Read only, compressed firmware. Integral firewall
- AES encrypted IPSEC to other **DNS**BOXes
- TSIG secured transfers to 3rd party DNS servers
- Granular control of user access, only over secure SSH/SSL links
- Dual CompactFlash - program and data

Technical Specifications

	DNSBOX210	**DNS**BOX220	**DNS**BOX230
Authoritative (QpS)	12,000		32,000
Ethernet (NICs)	2 x 10/100/1000		
Flash Storage	1 x OS, 1 x data		
DHCP Storage	SSD		
Dimensions	19” (482.6mm) x 1.75” (44.45mm) x 10” (254mm)	19” (482.6mm) x 1.75” x (44.45mm) x 17” (432mm)	