



A Quick Guide to

# Deploying DNS Appliances

Whitepaper

**Published By:**

ApplianSys Limited  
University of Warwick Science Park  
Business Innovation Centre  
Binley Business Park  
Coventry, CV3 2TX

Copyright © 2009 ApplianSys Ltd. All Rights Reserved. No part of the contents of this document may be reproduced or transmitted in any form or by any means electronic or otherwise without the written permission of ApplianSys Ltd.

## CONTENTS

<b>INTRODUCTION.....</b>	<b>2</b>
<b>THE IMPORTANCE OF RELIABLE DNS .....</b>	<b>2</b>
Causes of failure .....	2
<b>THE OPTIONS FOR MANAGING DNS .....</b>	<b>3</b>
Hosted DNS .....	3
Windows DNS .....	3
Open source BIND on Linux servers .....	4
Dedicated DNS server appliance .....	5
<b>CHOOSING AN APPLIANCE .....</b>	<b>6</b>
Reliability & recovery .....	6
Distributed administration.....	6
Dedicated Slaves .....	6
Integrating IP Address Management (IPAM) .....	6
<b>DEPLOYMENT CHECKLIST .....</b>	<b>7</b>
STEP 1: Start with an audit.....	7
STEP 2: Sizing an orthodox architecture.....	8
STEP 3: Plan the physical and logical configuration of the new DNS appliances. ....	9
STEP 4: Permissions .....	9
STEP 5: Testing .....	9
<b>CONCLUSIONS .....</b>	<b>9</b>

## INTRODUCTION

**DNS is critical to your organization. It's the telephone directory for your network - translating names to IP addresses and vice versa. However, with more applications such as email, Instant Messaging, Voice over IP etc relying on the service, it's become more complicated and difficult to administer.**

In this paper we will look at:

- The importance of reliable DNS
- Options available for managing DNS
- What to look for in an appliance
- And finally, a checklist for sizing and deploying an appliance solution

## THE IMPORTANCE OF RELIABLE DNS

DNS failures are costly. If you sell products over the web your traffic could be worth thousands of pounds per second, DNS failure has a very significant impact on your profitability. But you don't have to be an online retailer to appreciate the impact. If you stop and think about it, what does it cost you if potential customers or channel partners can't use your website? What does it cost if internal users can't use the Internet to send emails? Imagine what would happen if your organisation has a DNS outage.

Management can't review critical financial data from branch offices, production can't order parts via supplier procurement portals, sales teams can't access the latest pricing on network shares, marketing can't get onto eBay!

In addition to immediate 'one-off' interruptions, DNS failures can produce delayed effects. Applications can run for hours or days, only to fail when an IP lease or a DNS address TTL or "time to live" expires. This leads to failures that are difficult to find and fix.

### Causes of failure

There are a number of reasons why DNS can fail:

- Weak solution architecture – becoming more complicated over time, many architectures tend to be surrounded by customized scripts compensating for weaknesses in the platform
- Poor configuration – servers set up incorrectly in the first place
- Input errors – errors that creep in when administering DNS can take web sites down for hours or even days at a time because corrections are not picked up by downstream servers until the TTL of the incorrect entries expire
- Malicious attack - DNS servers are universally accessible by design and so are prone to being hacked. The risk of hacking is increased by the tendency to keep DNS servers fairly static because no one dares to touch them. This leads to administrators using outdated software for which known vulnerabilities have been published and patched, but not implemented

## THE OPTIONS FOR MANAGING DNS

### Hosted DNS

Outsourcing DNS management to a third party is one of the first options organizations consider. The reasons given are all very compelling, no hardware or software to maintain, and no need to employ DNS experts.

The problems with outsourcing usually revolve around 'control'. You're relying on a third party to make changes for you and depending on how often you do this you may find waiting for every update is 'part of the service'. What's more, changes are often billable. So, the more you change, the more you pay.

*“On average we would make up to 6 changes a day to the DNS records and would send an email to the DNS administrators requesting any additions, updates or deletions. The main problem was our dependency on the suppliers’ schedule: nothing happened immediately and we would have to spend a lot of time and effort to confirm changes were applied.”*

Director of Network Services,  
**National Association of Home Builders**

### Windows DNS

DNS and DHCP services come bundled with Microsoft Windows server software. For Network Managers unfamiliar with or just not interested in learning BIND, it's usually the default choice. Although this solution is fairly cheap initially (unless you consider it as a portion of Microsoft's overall set-up, upgrade, and licensing fees for networking software), it only offers basic functionality.

In addition to serious reliability and scalability concerns associated with these implementations, network administrators have to constantly monitor and implement security updates and patches in order to keep the system up-to-date and secure from intruders.

*“In an advisory this morning borrowing language used during previous statements about completely different exploits, Microsoft's Security Response Center team confirmed that it has seen at least one new wave of attacks based on proof-of-concept code impacting its DNS server software in Windows Server-based systems.”*

Scott M. Fulton,  
**Microsoft DNS Server Attacks Continue,**  
betanews.com, April 17, 2007

## Open source BIND on Linux servers

BIND is a very popular choice, and rightly so, it does a great job and is of course free. Install it on a Linux server and you've got yourself a very powerful DNS solution.

However, common complaints of BIND are that it's not easy to administer. It needs a high degree of expertise and the skills needed don't come cheap. If senior technicians are occupied with administering DNS, they aren't able to add value on other projects that may be more important.

Many DNS failures result from simple, innocent errors inside a DNS record. Even experienced operators can make mistakes. The main public editing tools used with BIND require the expertise of specialist UNIX/NT technicians and are subject to serious errors. Moreover, because all the data is in one very big file, editing plain BIND files is very time consuming.

In addition to administration, both BIND and the server Operating Systems need to be patched on a regular basis.

*“When looking for a solution, we wanted to find something that would do the job without taking up our time, and that would also eliminate human error in the process. We knew that setting up and looking after DNS servers takes up a lot of time, and they're particularly prone to errors.”*

Network Manager,  
**CMPI**

*“The setup of our network held up the whole IT department. Each time a new PC arrived on campus, the helpdesk team had to wait for the infrastructure team...It made the whole process slower than it needed to be.”*

Network and Telecommunications Manager,  
**London Business School**

## Dedicated DNS server appliance

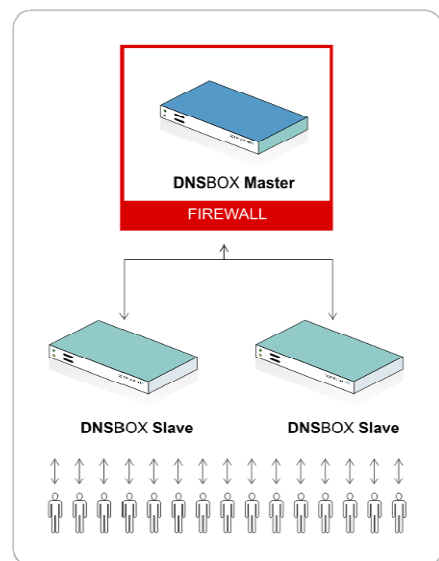
Server appliances are one of the latest developments in DNS management. Wrapping hardware, operating system and support features around specialised management software, server appliances are simpler, with less to manage and less to worry about.

Most vendors incorporate accepted DNS best practice into their solutions. Such as:

- Running a mixture of DNS management software. This is usually BIND, running in a 'jailed' environment, surrounded by commercial software to add input validation and automation.
- Disabling unused ports, eliminating unnecessary applications from the OS and including on-box firewalls to isolate the appliances from non-relevant traffic and possible exploits.
- Supporting solution architectures that increase redundancy, which is better than hardening single servers.
- Support for DNS 'views'. This allows the administration of an unlimited number of discrete copies of the same zone(s), eg 'Internal' and 'External' views could be present that represent different copies of the same zone to different slaves.

The orthodox approach to architecting DNS, which adheres to best practice, is a master-slave approach:

- A master is hidden securely behind the firewall.
- A minimum of 2 slaves serve queries, for redundancy.
- The master is used to edit DNS records. It holds the original authoritative records, but does not resolve DNS queries.
- Each slave only carries a copy of zone data, with the original held securely on the master. Data on the slave is not propagated to any other device. If a slave somehow became compromised, any amended DNS data could not infect the entire installation. Any damaging results would be more temporary and more contained than with compromises to the master authoritative data.



**Image 1 - Orthodox Master and Slave Architecture**

## CHOOSING AN APPLIANCE

Not all DNS appliances are the same. When choosing one you should consider the following:

### Reliability & recovery

Whilst appliances offer better reliability than general purpose servers, many still suffer from a common point of failure. Hard drives account for 90% of hardware failures, so using alternative storage media, such as solid state CompactFlash, can make a big difference to reliability. CompactFlash is also more robust in situations where there is a power loss, with no loss of data or settings and immediate reboot.

### Distributed administration

The ability to delegate parts of the DNS management workload to junior administrators or a support helpdesk is a definite bonus. However, look for an appliance that allocates user permissions via groups. A 'User Groups' feature lets a central administrator maintain tight control over the rights of other administrators. If you have multiple DNS administrators it means tasks can be shared in a very efficient, controlled and coordinated way.

### Dedicated Slaves

DNS slaves do a very different job to the master. Using master appliances reconfigured as slaves is more expensive than using dedicated slave appliances because you're paying the overhead of management software you won't use. As well as lowering the cost of the project, dedicated slave give you greater flexibility when architecting a solution. Adding more (lower cost) slaves means you can design in greater redundancy as well offering local name resolution to branch offices.

### Integrating IP Address Management (IPAM)

If you're considering IPAM, look for a solution that overlays IP address management onto your existing DNS /DHCP system without you having to scrap what you already have. Avoid standalone software that can't synchronise with DNS/DHCP data sets, otherwise you'll be adding to your administrative workload, manually synchronising two separate systems.

*“Appliances must be simple, secure, robust, intuitive, and low cost. The ApplianSys DNSBOX delivers - and on every count. The differences between this and other solutions I have tested are like night and day.”*

Senior Network Architect,  
**Warner Bros**

## DEPLOYMENT CHECKLIST

### STEP 1: Start with an audit

- Which zones need to be migrated?  
*This ensures you don't miss any zones in the migration.*
- Which servers currently host each zone?  
*This alerts you to any other services your DNS servers may be providing*
- Are there interactions beyond simple queries that occur with other DNS servers?  
*Do you have dynamic updates from Active Directory or any billing or setup systems? For example, an ISP may want billing systems to be aware of DNS updates, whilst a university may have a system that lets departments or the IT helpdesk request changes to zones. Fewer interactions make the migration easier.*
- Any specific permissions/privileges defined in current DNS server(s) to allow access from other internal or 3rd party DNS servers?  
*For example, parent company DNS by TSIG*
- Any TSIG keys or other forms of security used with 3rd parties that will need to be maintained?
- Do any 3<sup>rd</sup> party organisations have an interest in this DNS infrastructure?  
*E.g. DNS peering arrangements, delegated management permissions, system health monitoring, etc. If so, they should be informed of the planned changes to ensure continuity of service. A recent customer, in addition to replicating its entire DNS infrastructure at a disaster recovery site, also had its DNS mirrored by its ISP as a second layer of protection. The ISP is an example of a 3<sup>rd</sup> party who needs to be kept in the loop.*

## STEP 2: Sizing an orthodox architecture.

More complex architectures retain the master-slave approach, but introduce options like Failover Masters and High Availability Load-Balanced Slave Clustering. These add more redundancy to the inherent redundancy of the master-slave architecture. Massively redundant architectures feature data-centre level redundancy as well.

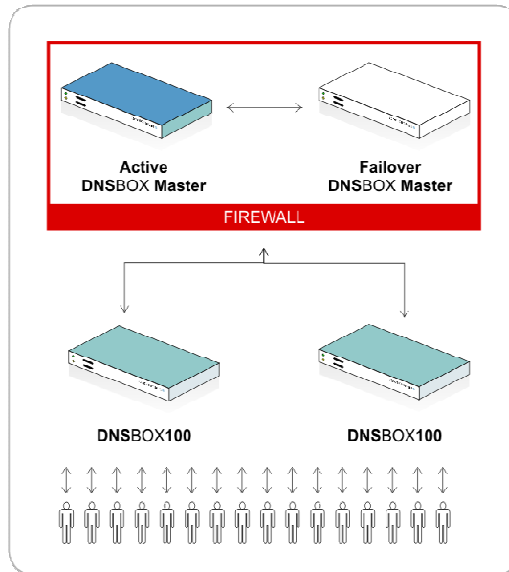


Image 2 - Master (with HA) and Slaves

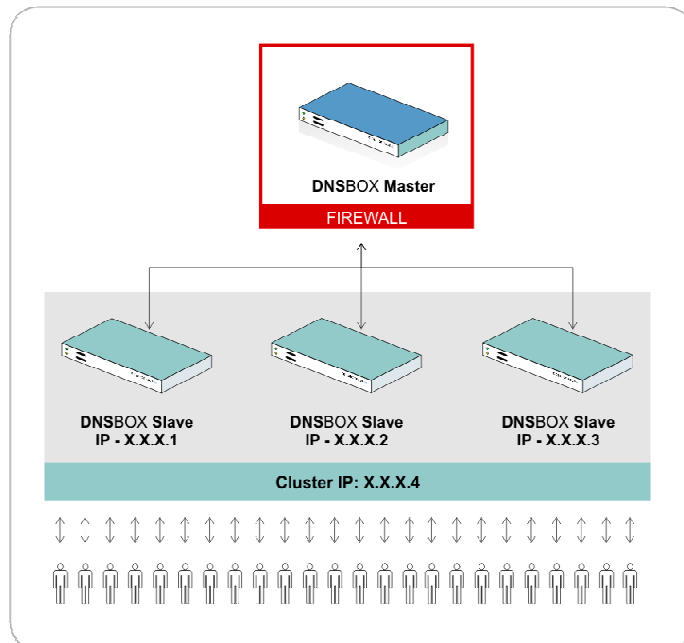


Image 3 - Load balanced Slave cluster

### STEP 3: Plan the physical and logical configuration of the new DNS appliances.

- IP address and hostname decisions should be made now and addresses should be reserved if necessary
- If you plan to cluster your appliances, ensure you have an extra IP & hostname available for each cluster
- If the new appliances will eventually be replacing old DNS servers and taking their IP addresses (to ease transition), assign temporary IP addresses for each unit. Ideally assign a permanent IP to the new master(s) in this instance as they won't be visible from the internet. There's no harm in putting the new master on a new IP address.
- Rack space and switch ports should be provisioned for each unit. Take care to provide as much physical/networking/power separation as possible to guard against network connection/switch/power failure. Note: If the clustering feature is used, each cluster must be configured on the same IP subnet, if the network permits

### STEP 4: Permissions

Once you've fully understood and documented the current architecture fully, contact each legacy DNS hosting provider and request that full zone-transfer permissions (AXFR) are granted to the IP address of the new main master (and only this IP).

### STEP 5: Testing

Build a detailed test-plan to ensure thorough and accurate testing is completed. It's essential that all revenue-generating/business-critical zones are exhaustively checked for completeness and validity. The tests you should run include:

- Validate actual zone data is accurate
- Test zone queries from every interface
- Test zone queries from public/private addresses

## CONCLUSIONS

DNS appliances offer better reliability, security and ease of use than alternative approaches to DNS management. A well designed architecture and co-ordinated rollout ensure you've got a rock solid foundation for future service expansion.