Global Information Assurance Certification Paper

Hardening Microsoft DNS on NT4.0 sp6a with overview of Split DNS architecture
Clif Sevachko
February 8, 2001 v1.04

> … `Would you tell me, please, which way I ought to go from here?'
> `That depends a good deal on where you want to get to,' said the Cat.
> `I don't much care where--' said Alice.
> `Then it doesn't matter which way you go,' said the Cat. [1]

I encourage the reader to review **DNS Security** by Jeff Holland, July 23, 2000, **DNSSec and BIND9** by Vivian Burns, November 11, 2000 and **DNS Overview with a discussion of DNS Spoofing** by Sinéad Hanley, November 6, 2000.

My basic assumption is that you have a security plan and policy that permits you to perform the following. And that you are familiar in the concept of Defense-in-Depth, have a working knowledge of DNS and are familiar with NT, its registry and editing tools. I have included a network diagram to illustrate the concepts but will focus mainly on the internal DNS server configurations and registry settings.

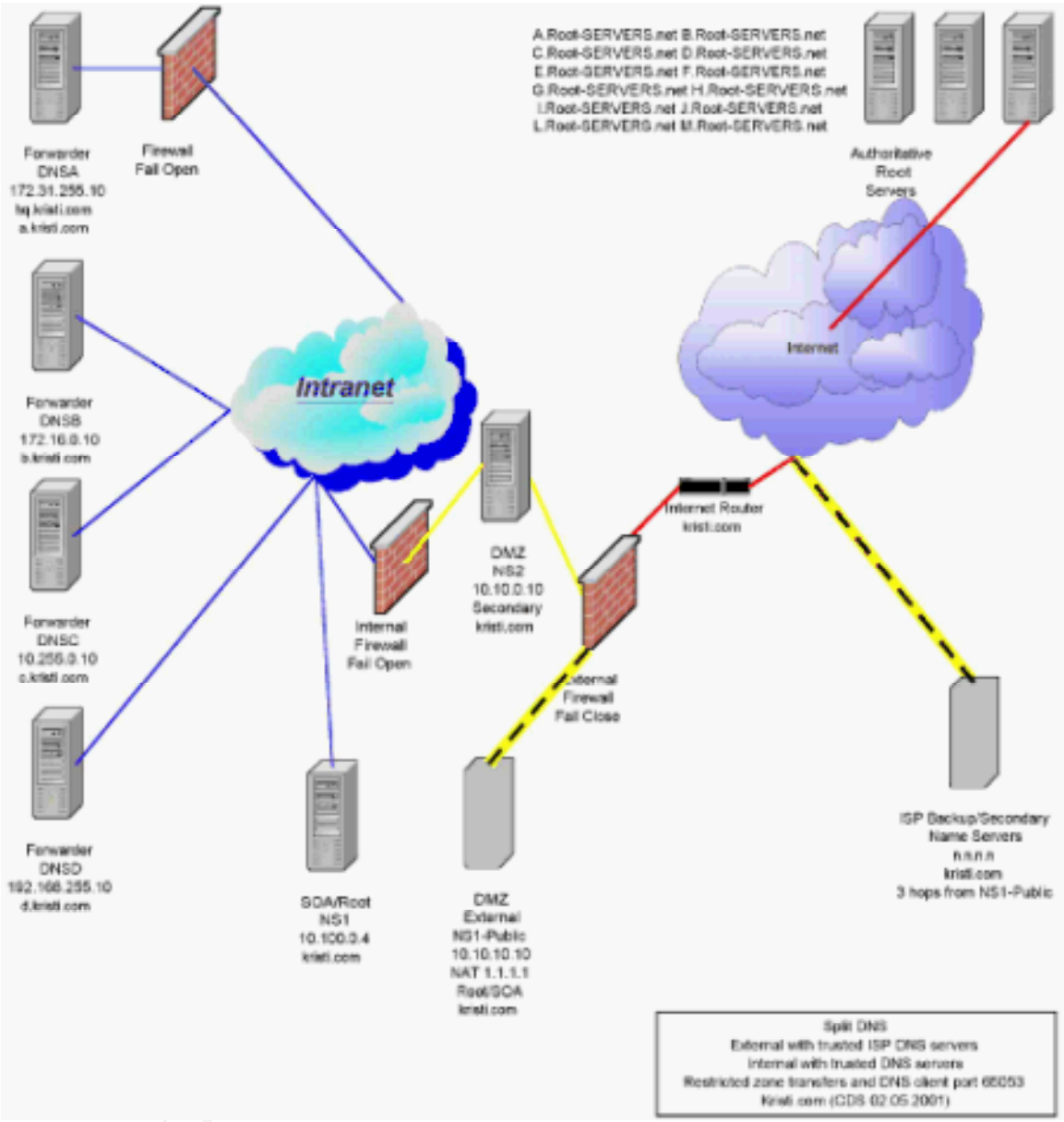
The task is to secure DNS for **kristi.com**, a software design, development and consulting company. They are geographically distributed, connected by an Intranet, connected to the Internet and have a registered domain name. Their External DNS SOA, NS1-Public, is a dedicated NT server in their corporate DMZ. Their external secondary DNS are the name servers of their ISP. The lockdown steps applied to the internal servers have been applied to the External DNS server and firewall policies adjusted to enable allowed zone transfers and queries.

Any **kristi.com** site may have a design, development, and test area/domain 'behind' it. Policy states only corporate DNS servers may traverse the Intranet and query the Internet. Procedurally this can be done with NT DNS and protect the rest of the corporation from 'rogue' DNS servers by applying some configuration and registry changes.

First, we review our firewall policies. Any internal DNS server should be able to perform a zone transfer and/or query with any other. For fault tolerance, I allow any of these servers to query the Internet directly using a specified port, for example, 35353/udp (0x8A19), 61053/udp (0xee7d), or 65053/udp (0xFE1D). This should only occur if none of the listed forwarders are reachable.

---

[1] Lewis Carroll, Pseudonym of Charles Lutwidge Dodgson , Alice's Adventures in Wonderland, 1865, URL:
http://www.literature.org/authors/carroll-lewis/alices-adventures-in-wonderland/chapter-06.html
Home URL: http://www.lewiscarroll.org/carroll.html
http://wsrv.clas.virginia.edu/~bhs2u/carroll/cd-pic.html

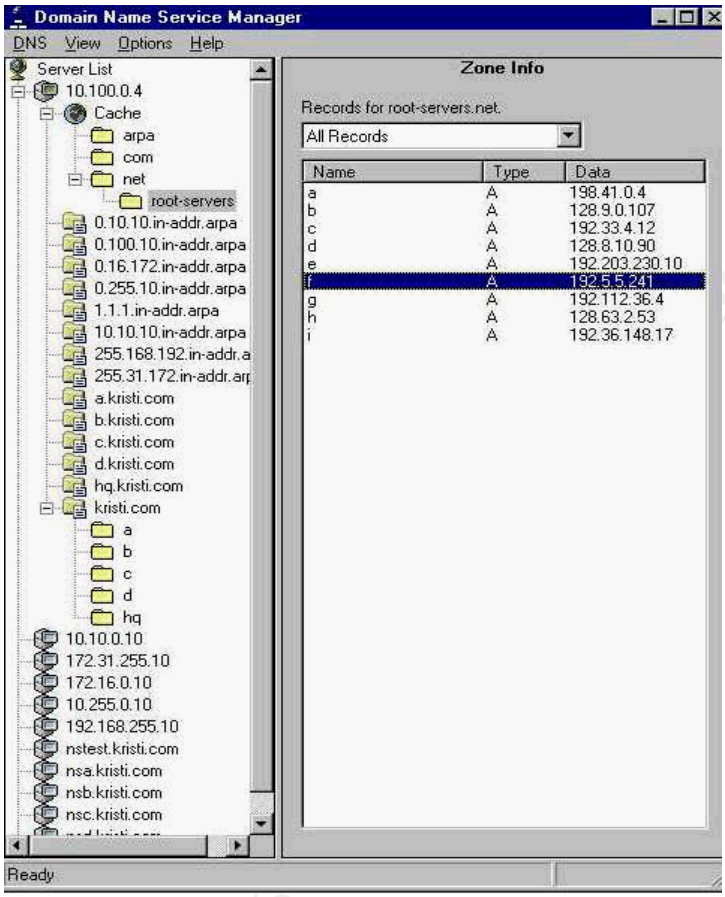


The Corporate servers are:

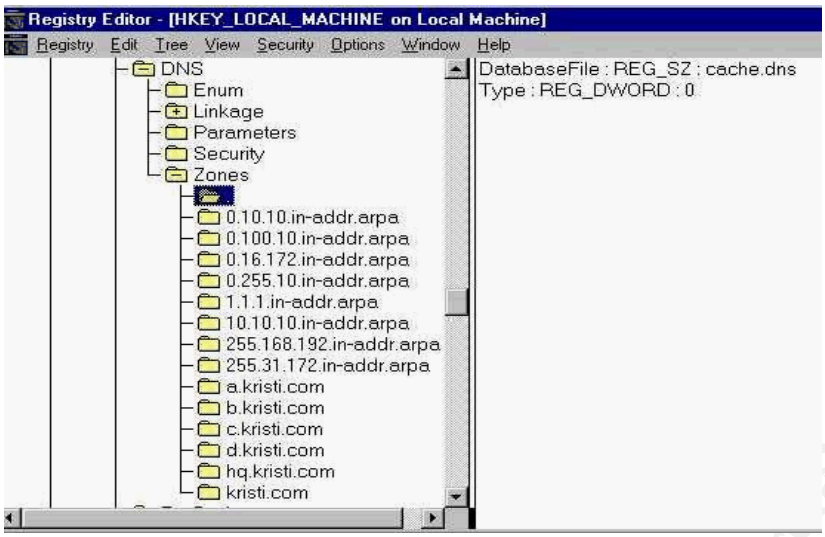
'Internal Root NS1' (10.100.0.4) where the changes and updates are made.
'Internal Secondary NS2' (10.10.0.10) corporate DMZ and queries the Internet.
'Forwarder A' (172.31.255.10) Administrative HQ, no changes, static.
'Forwarder B' (172.16.0.10) Test center, anything goes.
'Forwarder C' (10.255.0.10) Design group, many domain names.
'Forwarder D' (192.168.255.10) 'Don't ask, won't tell', the inexplicable.

Second, we verify that the NT servers have been hardened and sp6a (and appropriate hotfixes been applied). I find WINVER the quickest to determine what the OS thinks it is running. Access to the %SYSTEMROOT%\system32\DNS and the registry keys have been secured and have auditing in place.

Using an account with sufficient administrative privileges we verify what root servers will be used for the servers (Use reference [1], I have found some differences).



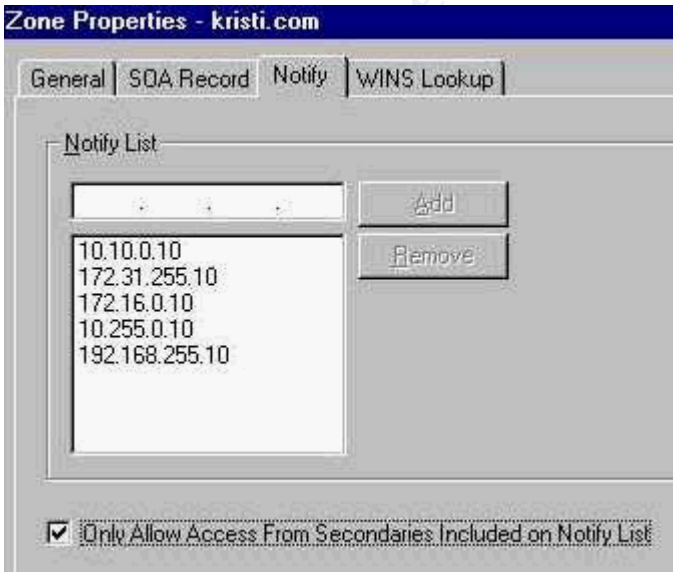
These entries need to be manually changed by editing \%SYSTEMROOT%\system32\DNS\Cache.dns



If your account and workstation can access all the servers, these can be all done at one sitting. This can be accomplished by running DNSADMIN and REGEDIT (or REGEDT32). Most of the security and configuration can be done via DNSADMIN. I recommend not showing the automatically created zones. Editing their properties can easily kill the DNS service.

0.in-addr.arpa
127.in-addr.arpa
255.in-addr.arpa

Allowing access only to secondaries is how you lock down zone transfers and nslookup. Adding to the Notify list is how you enable access. This can be applied to each zone.



NS1 is the internal SOA/Root server for **Kristi.com**. NS2 the secondary and normally will be making most of the queries to the Internet. A, B, C and D will forward to NS1, then NS2, then other backup servers. The corporate external root server, NS1-Public could be used as a last resort but since it should have only external addresses for **kristi.com** servers, this may not work as expected and may require some creative routing and firewall policies.

The following registry settings must be done manually via REGEDIT/REGEDT32.

HK_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters

Value: RpcProtocol Type: DWORD Default: 0xffffffff (all) (Suggest 0x1 TCP)
Function: Determine which protocols administrative RPC runs over
Benefit: Administrators must use TCP/IP to administer the service

Value: SendOnNonDnsPort Type: DWORD Default: NoKey (Suggest 0xFE1D {65053})
Function: Determines port on which server sends UDP queries to other DNS servers.
Benefit: Administrators can easily identify, monitor and control forwarding queries.

Value: SecureResponses Type: DWORD Default: NoKey (Non-Secure data kept, set to 1)
Function: Determines whether server attempts to clean up responses to avoid cache pollution.
Benefit: Avoid cache poisoning/pollution.

Value: AddressAnswerLimit Type: DWORD Default: NoKey (Suggest 0x10)
Function: Limits number of A records put in answer to query.
Benefit: Can avoid truncated responses and 53/tcp.

Value: EventLogLevel Type: DWORD Default: NoKey (all) (Suggest 0x4 unless log filling up)
Function: Determines level of logging to event log
0 – none, 1 – Error, 2- Warning, 4 - All
Benefit: Administrators can reduce logging to avoid DoS because of log entries.

Value: LogLevel Type: DWORD Default: NoKey (Suggest 0x0)
Function: Determines level of logging to file (Dns.log).
Benefit: Administrators can log to the packet level if needed.

Value: NoRecursion Type: DWORD Default: NoKey (Do recursion)
Function: Determine whether or not server does recursive lookups.
Benefit: Administrators can control a specific servers behavior.
Block an internal development DNS server and make the client fall back to a secondary server.

Don't forget to stop and start the service for the changes to be in effect.
Net Stop DNS, Net Start DNS

So at this point, we have:

NS1 **10.100.0.4** *(Kristi.com Root/SOA)*
Allow Access to Secondaries
10.10.0.10 (NS2),
172.31.255.10 (A), 172.16.0.10(B), 10.255.0.10 (C), 192.168.255.10 (D)
Forward to:
10.10.0.10 (NS2), 10.10.10.10 (NS1-Public internal address)

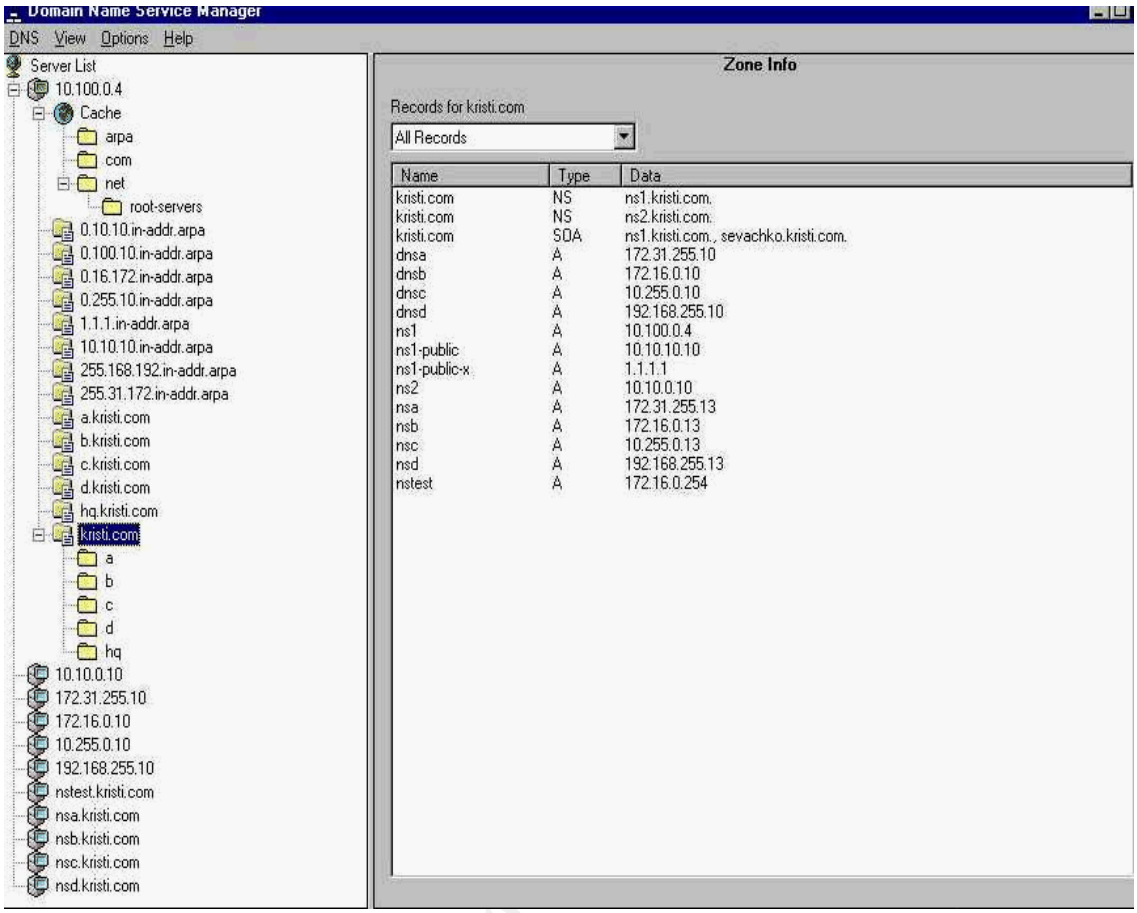
NS2 **10.10.0.10** *(Secondary)*
Allow Access to Secondaries
172.31.255.10 (A), 172.16.0.10(B), 10.255.0.10 (C), 192.168.255.10 (D)

A **172.31.255.10**
Allow Access to Secondaries - None
Forward to:
10.100.0.4 (NS1), 10.10.0.10 (NS2), 172.16.0.10(B),
10.255.0.10 (C), 192.168.255.10 (D) {Possibly 10.10.10.10}

B **172.16.0.10**
Allow Access to Secondaries - None
Forward to:
10.100.0.4 (NS1), 10.10.0.10 (NS2), 172.31.255.10(A),
10.255.0.10 (C), 192.168.255.10 (D) {Possibly 10.10.10.10}

C **10.255.0.10**
Allow Access to Secondaries - None
Forward to:
10.100.0.4 (NS1), 10.10.0.10 (NS2), 172.31.255.10(A),
172.16.0.10 (B), 192.168.255.10 (D) {Possibly 10.10.10.10}

D **192.168.255.10**
Allow Access to Secondaries - None
Forward to:
10.100.0.4 (NS1), 10.10.0.10 (NS2), 172.31.255.10(A),
172.16.0.10(B), 10.255.0.10 (C), {Possibly 10.10.10.10}



I'm in the process of looking under the DNS hood of Windows 2000. At the July DC2000 SANS, Steve Northcutt made a reference to port 445, he called it "…the bridal registry of DNS…". With Active Directory and DDNS, this is appears to be only the tip of the iceberg. I'm keeping my eyes posted hoping someone else generates a write up on re-securing DNS under W2K. And I'm waiting for the results of the next W2K service pack rollout to begin any serious work in this area. Like the Cheshire Cat said, it doesn't matter which way you go if don't know where you are going.

References

[1] Root Domain Servers
ftp://ftp.rs.internic.net/domain/root.zone
ftp://ftp.rs.internic.net/domain/README Last accessed 2 February, 2001

```
A.ROOT-SERVERS.NET. 518400 IN A 198.41.0.4
B.ROOT-SERVERS.NET. 518400 IN A 128.9.0.107
C.ROOT-SERVERS.NET. 518400 IN A 192.33.4.12
D.ROOT-SERVERS.NET. 518400 IN A 128.8.10.90
E.ROOT-SERVERS.NET. 518400 IN A 192.203.230.10
F.ROOT-SERVERS.NET. 518400 IN A 192.5.5.241   (NT default is different)
G.ROOT-SERVERS.NET. 518400 IN A 192.112.36.4
H.ROOT-SERVERS.NET. 518400 IN A 128.63.2.53
I.ROOT-SERVERS.NET. 518400 IN A 192.36.148.17
```

```
J.ROOT-SERVERS.NET. 518400 IN A 198.41.0.10
K.ROOT-SERVERS.NET. 518400 IN A 193.0.14.129
L.ROOT-SERVERS.NET. 518400 IN A 198.32.64.12
M.ROOT-SERVERS.NET. 518400 IN A 202.12.27.33
```


[2] Microsoft Inc, "DNS and Microsoft Windows NT 4.0"
http://www.microsoft.com/ntserver/nts/deployment/planguide/dnswp.asp
http://support.microsoft.com/support/kb/articles/Q164/4/88.asp
Accessed 8 February, 2001

[3] Microsoft Inc, "Microsoft DNS Server Registry Parameters, part 1 of 3"
http://support.microsoft.com/support/kb/articles/Q198/4/08.ASP
Microsoft Inc, "Microsoft DNS Server Registry Parameters, part 2 of 3"
http://support.microsoft.com/support/kb/articles/Q198/4/09.ASP
Microsoft Inc, "Microsoft DNS Server Registry Parameters, part 3 of 3"
http://support.microsoft.com/support/kb/articles/Q198/4/10.ASP
Accessed 8 February, 2001

[4] Microsoft Inc, "Microsoft DNS Server Root Hints"
http://support.microsoft.com/support/kb/articles/Q195/8/11.ASP
Accessed 8 February, 2001

[5] Web sites for testing DNS configuration settings, ARIN registrations, etc.
http://combat.uxn.com, http://www.geektools.com Accessed 8 February, 2001

[7] Microsoft Inc, "SENDPORT DNS Registry Key does not work as expected"
http://support.microsoft.com/support/kb/articles/Q260/1/86.ASP
Accessed 8 February, 2001

[8] Holland, Jeff, "DNS Security", July 23, 2000
http://www.sans.org/infosecFAQ/DNS_sec.htm Accessed 8 February, 2001

[9] Hanley, Sinéad "DNS Overview with discussion of DNS Spoofing", November 6, 2000, :http://www.sans.org/infosecFAQ/DNS.htm Accessed 8 February, 2001

[10] Burns, Vivian, "DNSSec and BIND9", November 11, 2000
http://www.sans.org/infosecFAQ/unix/BIND9.htm Accessed 8 February, 2001