

**UNCLASSIFIED**

Report Number: C4-050R-00

---

# Guide to Securing Microsoft Windows 2000<sup>®</sup> DNS

**Network Security Evaluations and Tools Division  
of the  
Systems and Network Attack Center (SNAC)**

Author:  
Capt Robin G. Stephens, USAF



Updated: April 9, 2001  
Version 1.0

National Security Agency  
9800 Savage Rd. Suite 6704  
Ft. Meade, MD 20755-6704

[W2Kguides@nsa.gov](mailto:W2Kguides@nsa.gov)

**UNCLASSIFIED**

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of April 9, 2001. See [Microsoft's web page](#) for the latest changes or modifications to the Windows 2000 operating system.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## Acknowledgements

The author would like to acknowledge the authors of the “*Guide to Implementing Windows NT in Secure Network Environments*” and the “*Guide to Securing Microsoft Windows NT Networks*” versions 2.0, 2.1, 3.0, 4.0, and 4.1.

The author would like to acknowledge Paul Bartock and LT. William Billings for their help reviewing the document.

Some parts of this document were drawn from Microsoft copyright materials with their permission.

## Trademark Information

Microsoft, MS-DOS, Windows, Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and Windows 3.1 are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

All other names are registered trademarks or trademarks of their respective companies.

Table of Contents

**Warnings**..... iii

**Acknowledgements** ..... v

**Trademark Information**..... vi

**Table of Contents**..... vii

**Table of Figures** ..... viii

**Table of Tables** ..... ix

**Introduction** ..... 1

*Getting the Most from this Guide* ..... 1

*Commonly Used Names* ..... 2

*About the Guide to Securing Microsoft Windows 2000 DNS*..... 2

**Chapter 1 Securing the Windows 2000 DNS Service** ..... 3

*DNS Server Configurations*..... 3

*Zone Information Security*..... 8

*Controlling Zone Transfers*..... 9

*Router and Firewall Settings* ..... 11

**Appendix A Windows 2000 DNS Server Service Security Configuration Checklist** ..... 13

**Appendix B Windows 2000 DNS Server Security Flowchart**..... 15

**Appendix C Further Information**..... 17

**Appendix D References**..... 19

Table of Figures

Figure 1 DNS with Internet Presence ..... 3  
Figure 2 DNS with Internet Presence and Disconnected Reverse Lookup Zone ..... 5  
Figure 3 DNS with Internet Presence and Secondary Reverse Lookup Zone ..... 5  
Figure 4 DNS with an Internet presence with Forward and Reverse Lookup zone requirements ..... 7  
Figure 5 Zone Types when DNS server is not installed on a Domain Controller ..... 8  
Figure 6 Zone Types when DNS server is installed on a Domain Controller ..... 8  
Figure 7 Zone Transfer ..... 10  
Figure 8 Known Name Servers ..... 11  
Figure 9 DNS Security Flowchart ..... 15



Table of Tables

Table 1 DNS Zone File Security Settings .....	9
Table 2 DNS Registry Security Settings .....	9

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## Introduction

The purpose of this guide is to inform the reader about the available security settings for the Windows 2000 Domain Name System (DNS) Server Service, how to design a secure implementation of the Windows 2000 DNS, and how to properly implement that design. This guide provides step-by-step instructions to perform many of the tasks recommended to secure this service. Because DNS implementations will vary, this document is designed to provide system administrators and network managers the ability to choose appropriate security settings for their environment.

The ***Guide to Securing Microsoft Windows 2000 DNS*** presents detailed information on how to secure this service in a network environment. Although this document assumes the reader will be implementing a Windows 2000 DNS, the network planning sections of this guide hold true for all domain name servers that have the capability for dynamic updates and server records.



**WARNING: This guide does not address security issues for the Microsoft Windows 2000 operating system that are not specifically related to the DNS Server Service and its implementation.**

This document is intended for Windows 2000 network administrators, but should be read by anyone involved or interested in Windows 2000 or network security.

### Getting the Most from this Guide

The following list contains suggestions to successfully secure the Windows 2000 DNS Server Service according to this guide:



**WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.**

- ❑ Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- ❑ Perform pre-configuration recommendations:
  - Perform a complete backup of your system before implementing any of the recommendations in this guide.
  - Ensure that the latest Windows 2000 service pack and hotfixes have been installed. For further information on critical Windows 2000 updates, see the [Windows Update for Windows 2000 web page](#).
- ❑ Configure routers and firewalls to allow the appropriate traffic for the DNS Server.
- ❑ Install the Microsoft Windows 2000 DNS Server Service.
- ❑ Follow the security settings that are appropriate for your environment.

## Commonly Used Names

Throughout this guide the network name “test.gov” and the subnet 192.168.0 will be used in the examples, screenshots, and listings.



**WARNING:** It is extremely important to replace “test.gov” and 192.168.0 with the appropriate network name and subnet for the networks being secured. These names are not real networks and have been used for demonstration purposes only.

## About the Guide to Securing Microsoft Windows 2000 DNS

This document consists of the following chapters:

**Chapter 1, “Securing the Windows 2000 DNS Server Service,”** recommends security settings for individual DNS servers and describes how to use the Microsoft Management Console to implement these settings for the DNS Service.

**Appendix A, “Windows 2000 DNS Server Service Security Configuration Checklist,”** contains a checklist to use when configuring a Windows 2000 DNS Server Service with following the recommendations in this guide.

**Appendix B, “Windows 2000 DNS Server Security Flowchart,”** contains a flowchart to help the reader design a secure DNS implementation.

**Appendix C, “Further Information,”** contains a list of the hyperlinks used throughout this guide.

**Appendix D, “References,”** contains a list of resources cited.

## Securing the Windows 2000 DNS Service

The Microsoft Windows 2000 DNS Service has several features that help provide a more secure DNS environment. These features cover the functionality of the server and the security of the file critical to the service.

### DNS Server Configurations

There are several deployment methods for DNS in a Windows 2000 environment. These methods are defined by the operational requirements of the organizations implementing DNS.

#### DNS in an Enclosed Environment

This type of DNS scheme only requires securing the DNS servers and operating systems. It is recommended that the External Router and Firewall block all DNS traffic (UDP and TCP port 53). Since this guide assumes that the servers will be configured for a Windows 2000 domain, it is recommended to make the DNS zones Active Directory Integrated and only allow zone transfers to servers listed in the **Name Servers** tab as discussed below.

#### DNS with an Internet Presence

Many environments require a connection to the Internet. To function correctly, a DNS server is required to provide addresses for clients. It is recommended to separate the External DNS server from the DNS servers that are being utilized for the Windows 2000 domain. This configuration is shown in **Figure 1**.

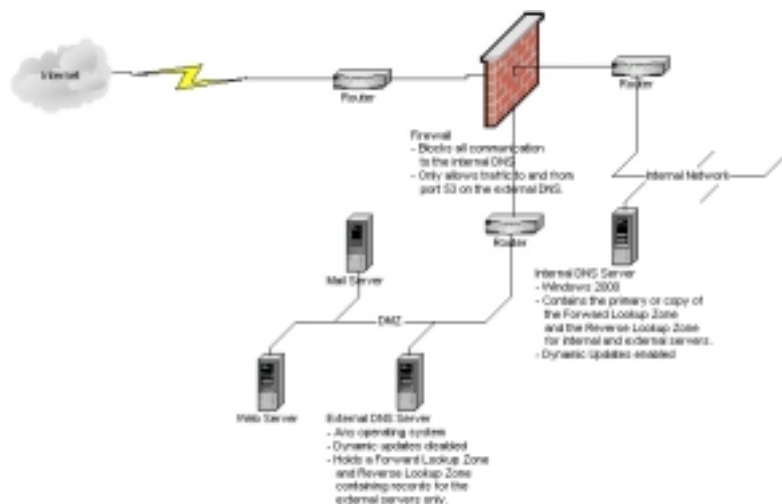


Figure 1 DNS with Internet Presence

Further security recommendations for this configuration include:

- Use Active Directory Integrated DNS servers internally.
- Perform zone transfers on Internal DNS servers to servers listed in the **Name Servers** tab as discussed below.
- Secure the zone transfer on the external servers to a specific list of servers, or no servers, as described in Controlling Zone Transfers. If several servers are used within one DNS domain then controlling the zone transfers by using the **Name Servers** tab, as discussed below, is recommended.
- Secure the file system and registry as described in Zone File and Registry Security below.
- Disable all unnecessary services on External DNS servers
- Disable dynamic updates on External DNS servers.

Internet name resolution presence can be accomplished by the Internal DNS server or by forwarding queries to the External DNS server. It is recommended to forward queries to the External server. However, if the Internal DNS server supports one part of an Active Directory tree/forest it will need to forward all unresolved queries to the next level of DNS in that tree/forest.

#### DNS with an Internet Presence with Reverse Lookup Requirements

In many government systems, it is necessary to verify that someone is coming from another government system. This verification is commonly accomplished using reverse lookup zones. These zones take an IP address and convert it to a name which can then be checked for the '.mil' or '.gov' extensions. There are two ways to provide this functionality:

1. Add a reverse lookup zone to the external DNS server that contains a list of all the internal network IP addresses. Match each IP address with a fictitious client name with the appropriate extension. This setup will allow the IP address to be verified. Configure the DNS servers as described in the DNS with an Internet Presence section. This configuration is shown in **Figure 2**. It is recommended to use this option because it will limit an attackers ability to correctly map the Protected Network.

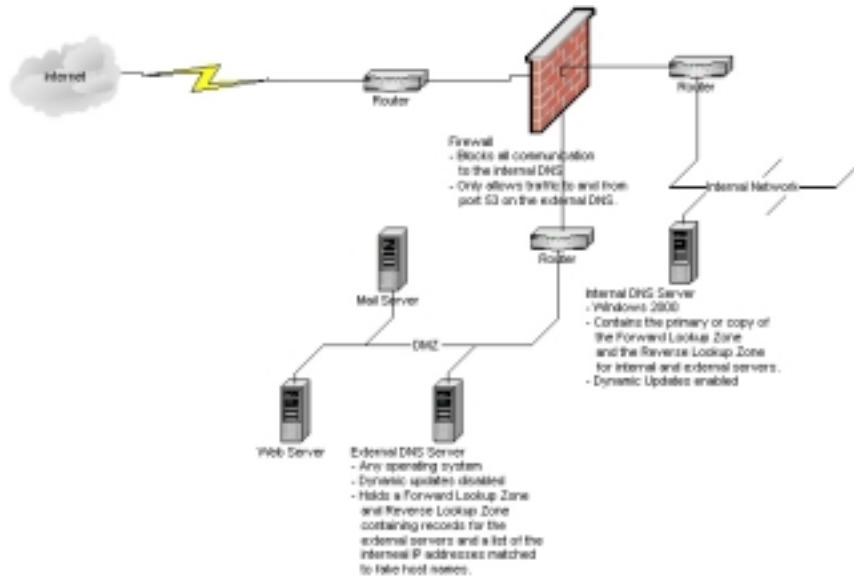


Figure 2 DNS with Internet Presence and Disconnected Reverse Lookup Zone

2. Add a reverse lookup zone to the external DNS server as a secondary zone to the internal network. Add the external server to the list of valid DNS servers to allow zone transfers to on one internal DNS server. Properly configure the router and firewall settings as described in Router and Firewall Settings to allow communication between one External DNS server and one, modified, Internal DNS server. Configure the DNS servers as described in the DNS with an Internet Presence section. Furthermore, it is recommended to not run any other services on the Internal DNS server. This configuration is shown in **Figure 3**. This setting will show the internal server's Start of Authority (SOA) record in the reverse lookup zone.

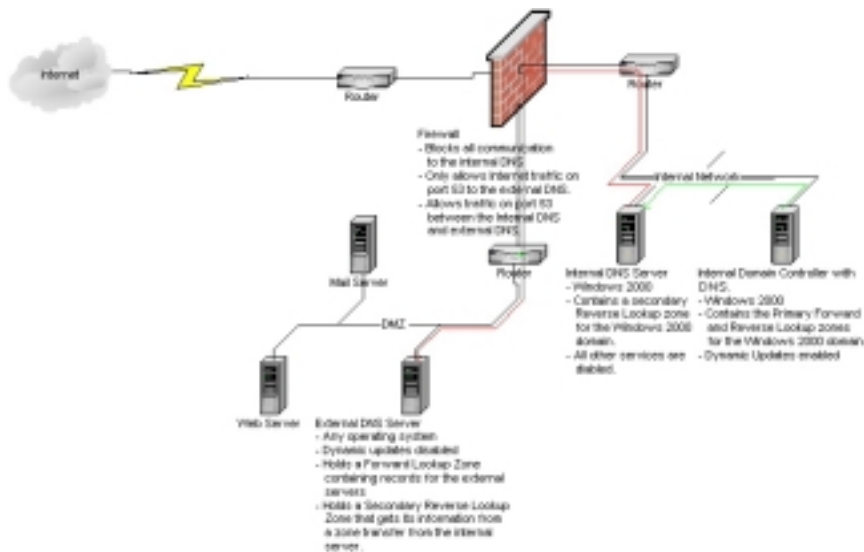


Figure 3 DNS with Internet Presence and Secondary Reverse Lookup Zone

## DNS with Internet Presence with Forward and Reverse Lookup Zone Requirements

This configuration is not recommended but may exist if a Windows 2000 forest or tree is linked across the Internet. If the server records are exposed to the Internet, external attackers will be able to completely map the internal network by querying the DNS server. There are several ways to approach this issue including:

1. Use a secure tunneling protocol between sites to secure zone transfers and protect the internal DNS server records and use one of the other DNS schemes mentioned above for the external servers. This configuration is shown in **Figure 4** (Good).
2. Add only the specific server records that are required for the network to function in the external DNS servers (Worse).
3. Configure one external DNS server's forward and reverse lookup zones to be secondary zones of one internal DNS server's zones (Worst).

As noted at the end of each option, the solutions are labeled with a degree of projected vulnerability. No matter how it occurs, there will always be a higher risk that an attacker has access to your DNS records if DNS zones are transferred over the Internet.



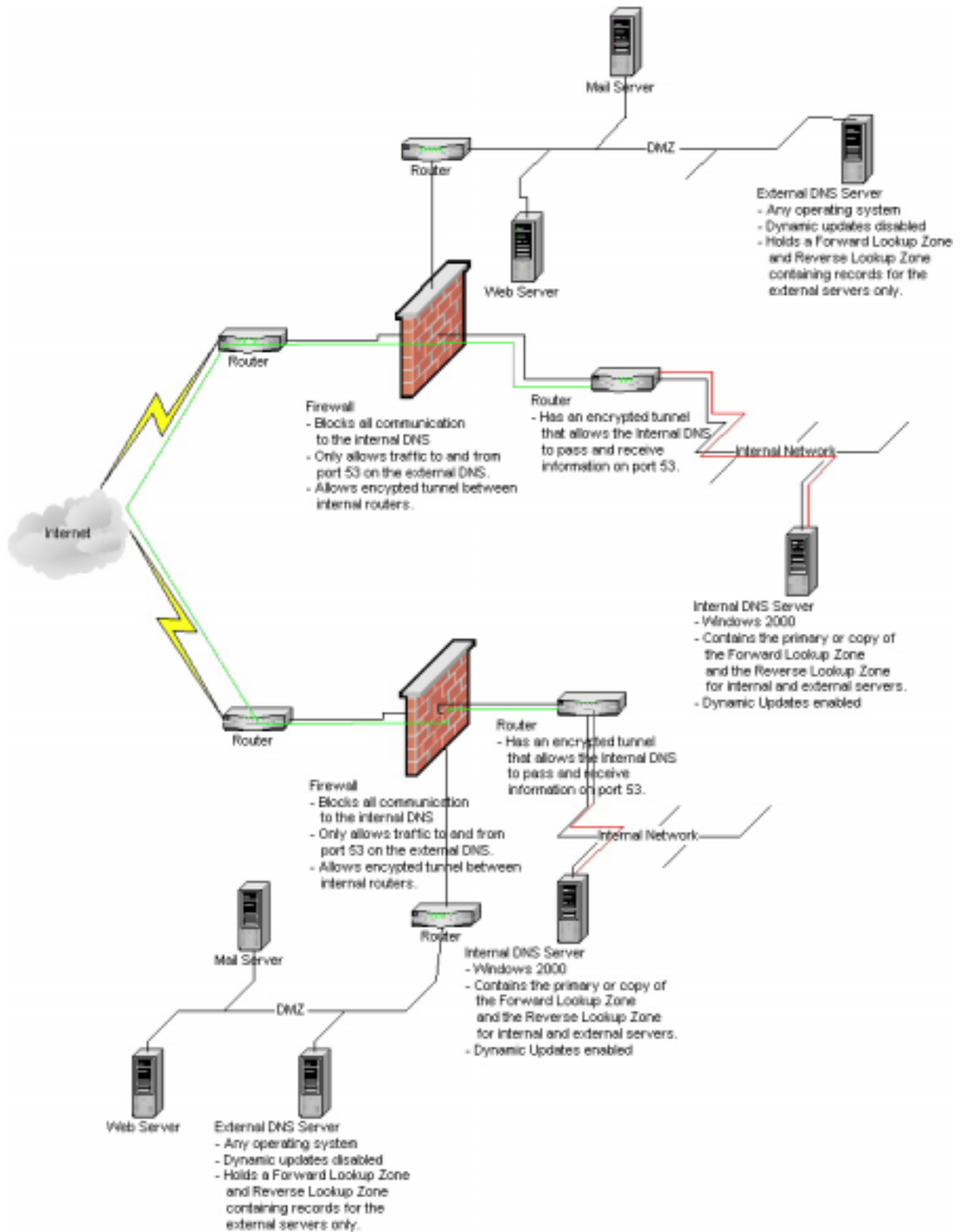


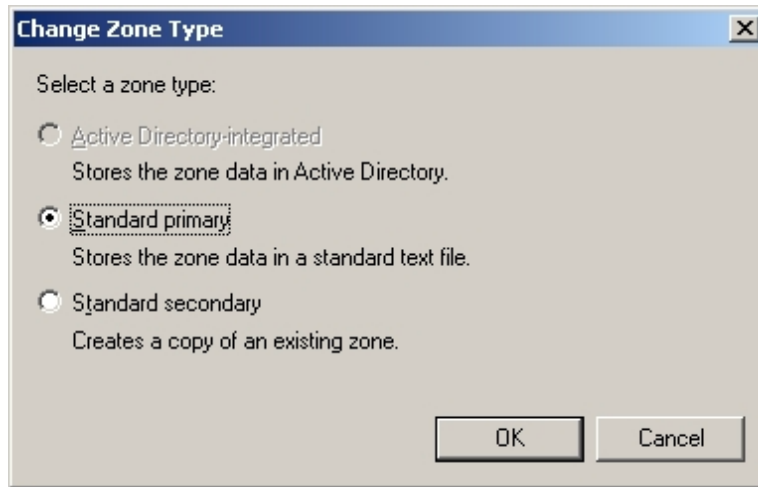
Figure 4 DNS with Internet Presence with Forward and Reverse Lookup Zone Requirements

## Zone Information Security

It is recommended to secure the location of the zone information a DNS server uses. This information is stored in the Windows 2000 Active Directory or in files stored on the hard drive.

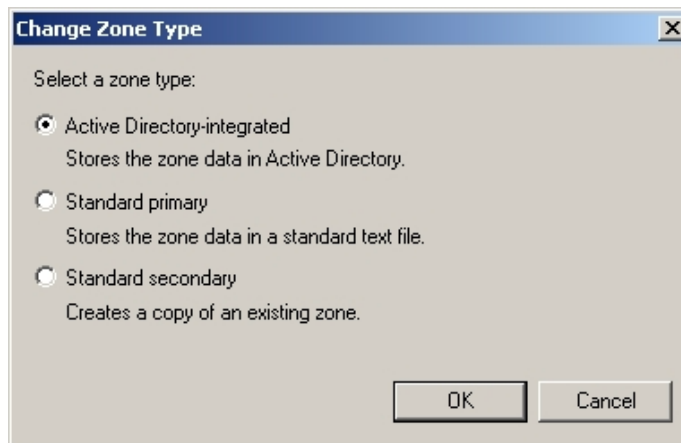
### Converting to an Active Directory Integrated Server

It is possible to convert a DNS zone to an Active Directory Integrated Zone. This action requires the DNS server to be on a Windows 2000 Domain Controller. If the DNS server is not located on a domain controller this option will be grayed out as shown in **Figure 5**.



**Figure 5 Zone Types when DNS server is not installed on a Domain Controller**


If the server is on a Windows 2000 Domain Controller, the zone types include the Active Directory integrated zone. These options are shown in **Figure 6**. This zone type offers many advantages to the DNS server and is recommended. Some of these options include the zone information being stored, replicated, and secured in the Active Directory. If this feature is used a “Only secure updates” option is enabled for Dynamic Updates. This option is recommended when allowing dynamic updates, which is a necessary feature for a Windows 2000 Domain.



**Figure 6 Zone Types when DNS Server is Installed on a Domain Controller**

## Zone File and Registry Security

If the DNS server is not storing its records in the Windows 2000 Active Directory, it is recommended to secure the DNS zone files. The recommended file security settings are listed in **Table 1**.

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS
<p><b>%SystemDirectory%\DNS</b> folder, subfolders, and files</p> <p>Directory that contains the DNS zone files.</p>  <p><b>Note: The Administrators group will have to be added to the file permissions if files must be manually edited.</b></p>	System	Full Control

**Table 1 DNS Zone File Security Settings**

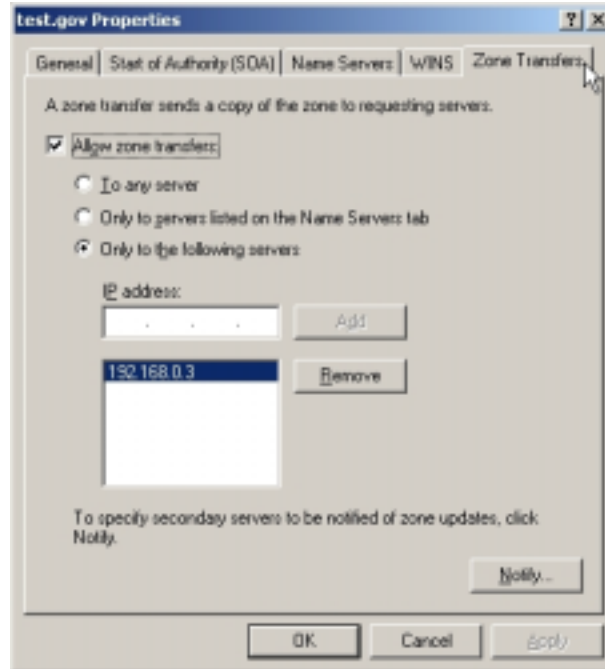
It is recommended that all DNS servers have the registry secured as listed in the following table. These settings will help prevent unauthorized users from identifying or modifying the location of the zone files.

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DNS	Administrator System	Full Control Full Control

**Table 2 DNS Registry Security Settings**

## Controlling Zone Transfers

The ability to control zone transfers is extremely important when securing DNS servers. In Windows 2000 modifying the access lists available for each individual zone controls zone transfers. Since zone transfers move all the records for a particular zone from one server to another it is extremely important not to transfer the forward lookup zone on a DNS server that contains Windows 2000 domain information to any server outside the Windows 2000 domain. **Figure 7** shows the four available options for zone transfers. This figure is a screenshot from the forward lookup zone properties of the test.gov DNS zone.



**Figure 7 Zone Transfer**

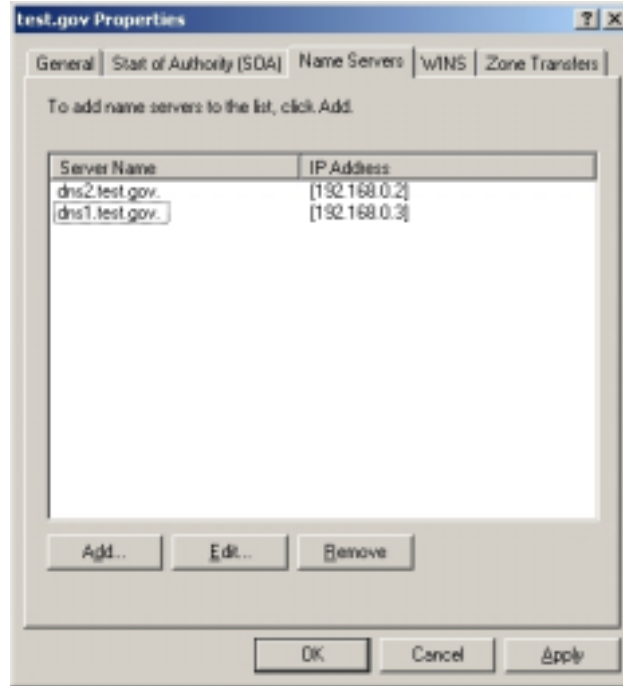
The four options for zone transfers are:

1. Do not allow zone transfers:
 

This option stops a complete zone transfer from occurring. However, this server will still be capable of receiving zone transfers from other DNS servers. Clients will be able to receive DNS query responses from this server. This option is recommended for any DNS server that does not specifically need to allow zone transfers.
2. Allow zone transfers to any server:
 

This option will allow any server or proper command sequence to transfer the DNS zone from the computer. Although this is the default configuration, it is not recommended to use this option on any DNS server.
3. Allow zone transfers to all servers listed in the **Name Servers** property tab:
 

This option uses the **Name Servers** list as represented in Figure 8. Since this list contains all domain servers within the DNS domain, this configuration is recommended when zone transfers will only be done within one domain. For example, when the DNS zone is hosting a Windows 2000 Domain this option would allow the DNS servers within the domain to share their zone information.



**Figure 8 Known Name Servers**

4. Allow zone transfers to a specific list of IP addresses:

This option controls zone transfers through a list of IP addresses as shown in **Figure 7**. This option allows information to be shared with specific servers outside the DNS domain. This configuration is recommended when communicating between protected DNS servers and a DNS server that can be accessed from the Internet. It is recommended to never transfer the forward lookup zone containing active directory records to any server that can be accessed via the Internet.

## Router and Firewall Settings

DNS traffic travels through port 53 (UDP and TCP). Therefore, it is necessary to open these ports on the router and firewall to allow clients and other servers to utilize DNS. UDP port 53 is required for client queries while the TCP port is required for zone transfers. In most cases, it is unnecessary to allow zone transfers outside of the Protected Network so TCP port 53 should be blocked at the Internal, External, Firewall, and DMZ routers. If the DNS is configured to allow reverse lookup zone transfers between the Internal and External DNS servers the Internal Router, Firewall, and DMZ router should allow connections on TCP port 53 between the Internal and External DNS only. If any problem is experienced with Windows 2000 using port 53 for DNS refer to the Microsoft knowledge base article [Q260186](#) for further information.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## Windows 2000 DNS Server Service Security Configuration Checklist

The following is a comprehensive checklist of the suggested configuration settings as outlined in this document. This list can be used as a quick reference guide for experienced system administrators who are already familiar with Windows 2000 and know how to perform these tasks using the Microsoft supplied tool set. For additional information on a specific recommendation, refer to the chapter designator at the end of that item.

1. DNS in an Enclosed Environment
  - 1.1. Disable all unnecessary services
  - 1.2. Block UDP and TCP port 53 at external Routers and Firewalls
  - 1.3. Make DNS zones Active Directory Integrated
  - 1.4. Only zone transfers to servers listed in the Name Servers tab only
2. DNS with an Internet Presence
  - 2.1. Create a separate External DNS to handle Internet DNS requests
    - 2.1.1. Disable all unnecessary services
    - 2.1.2. Set the ACL on %SystemDirectory%\DNS folder, subfolder and files to only allow system full control as shown in **Table 1 DNS Zone File Security Settings**.
    - 2.1.3. Set the ACL on HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\DNS to only allow System Full Control as shown in **Table 2 DNS Registry Security Settings**.
  - 2.2. Secure the Internal DNS
    - 2.2.1. Disable all unnecessary services
    - 2.2.2. Block UDP and TCP port 53 at external routers and firewalls. If using zone transfers, allow TCP port 53 through the external router and firewall between the Internal and External DNS servers only.
    - 2.2.3. Make DNS zones Active Directory Integrated
    - 2.2.4. Only zone transfers to servers listed in the Name Servers tab only. Do not transfer forward lookup zones to External DNS servers and only allow transfers of Reverse Lookup Zones to External DNS servers if absolutely necessary. See **DNS with an Internet Presence with Reverse Lookup Requirements** and **DNS with Internet Presence**

**with Forward and Reverse Lookup Zone Requirements** for more information.

2.2.5. Configure DNS forwarding requirements as follows:

- 2.2.5.1. If the Internal DNS server is part of a larger Windows 2000 forest/tree, forward unresolved DNS requests to the next part of the forest/tree.
- 2.2.5.2. If the Internal DNS server is not part of a larger Windows 2000 forest/tree, forward unresolved DNS requests to the External DNS server. This setting requires UDP port 53 to be open on the external firewall and router between the Internal and External DNS servers.



# Windows 2000 DNS Server Security Flowchart

The following flowchart was designed to help decide how to use this guide. The various steps indicated in the chart represent

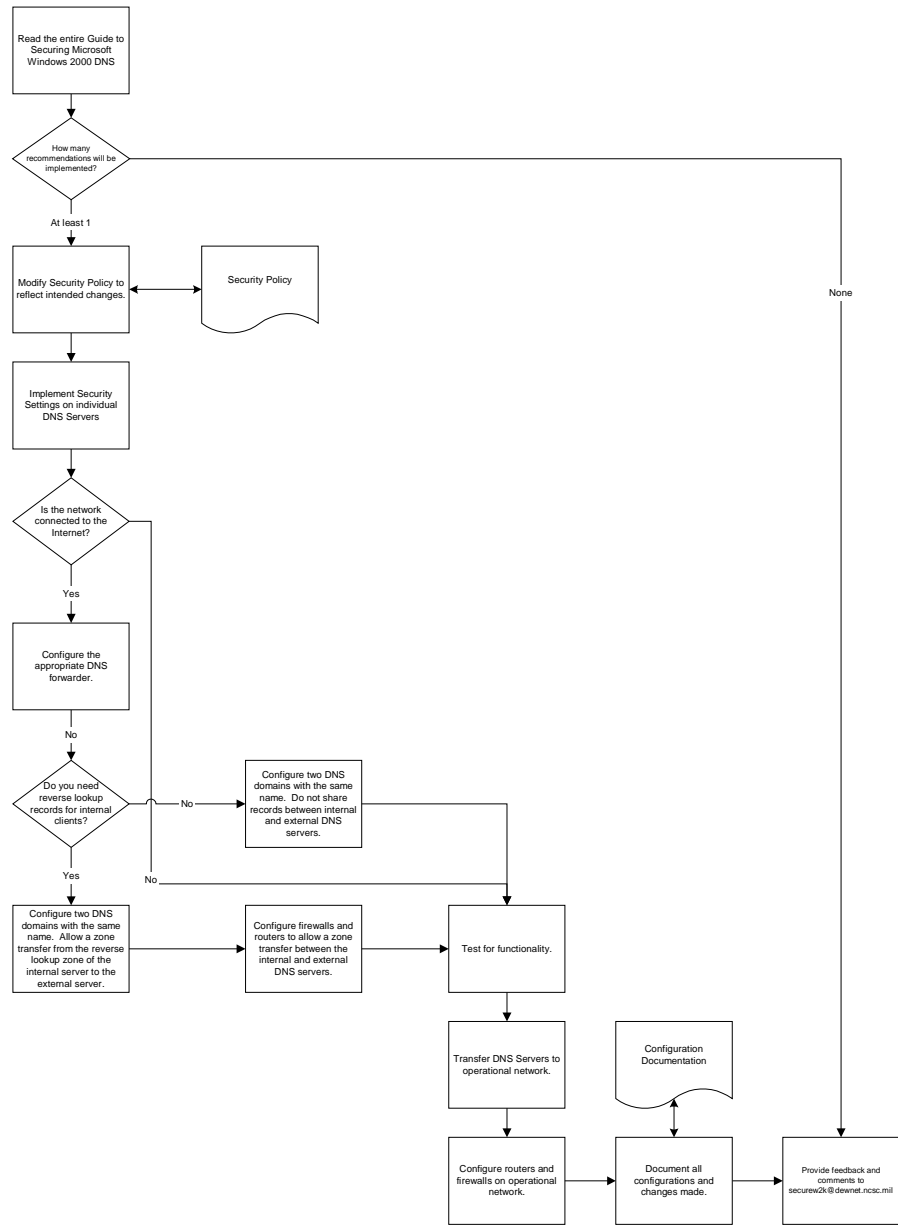


Figure 9 DNS Security Flowchart

Appendix B – Windows 2000  
DNS Server Security Flowchart

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED



---

## Further Information

Albitz, Paul and Cricket Liu, DNS and BIND, O'Reilly & Associates, 1998.

[Microsoft's Web Site.](#)

Microsoft. "DNS Requirements for Deploying Active Directory."  
<http://www.microsoft.com/TechNet/win2000/win2ksrv/dnsreq.asp>

Wong, William, Windows 2000 DNS Server, Osborne/McGraw-Hill, 2000.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

---

## References

Albitz, Paul and Cricket Liu, DNS and BIND, O'Reilly & Associates, 1998.

[Microsoft's Web Site.](#)