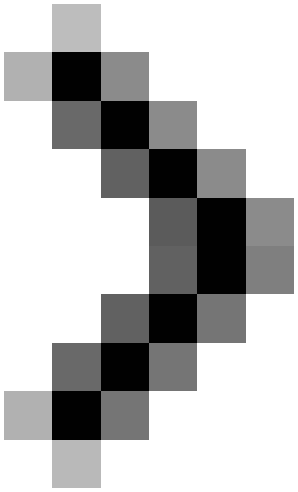
DNS protection for Windows (Part 2)

In the previous section of this article we have introduced you to some basic security concepts about DNS. One of the security concepts is integrated DNS Active Directory and establishes a more secure DNS environment with DHCP communication.



DNS protection for Windows (Part 1)

Derek Melber

In the previous section of this article we have introduced you to some basic security concepts about DNS. One of the security concepts is integrated DNS Active Directory and establishes a more secure DNS environment with DHCP communication. There are also several powerful configurations and allow you to easily create a DNS environment. Don't stop here! because that is just the surface of the DNS environment security issue. In each section of this article we will dive deeper into DNS and how DNS databases are secured, especially with communication with DNS servers. DNS servers must communicate to upgrade the database to another DNS server. This communication can be a good solution for an attacker to hack into these exposed

weaknesses. If you take precautions and set up secure DNS configurations, exposing the vulnerability may be reduced.

Move area

When it comes to DNS zones, you have to understand that there are different types of zones that can be set up within the DNS environment. Although we need to focus on some possible areas, I still give a list of all the areas you can set up in DNS.

1. Active Directory integrated Zone
2. Primary Zone
3. Secondary Zone
4. Stub Zone

In the previous section, we introduced the Active Directory integration zone. In this section, we will discuss Active Directory integrated area functions as a primary area. The reason for this problem: the main entry (Active Directory integrated area) is the zone for writing DNS databases. Secondary areas do not do this but they only receive updates from the primary DNS zone. Upgrades from the primary area to the secondary zone are called zone transfers.

The zone movement interface is quite clear through your options, which can be seen in Figure 1. You can allow any DNS server to receive the contents of the key zone or restrict it. so that only a certain DNS number can be selected. Obviously, for security purposes, you will want to limit the scope of DNS servers that are allowed to receive IP addresses and domains of all computers in your organization.

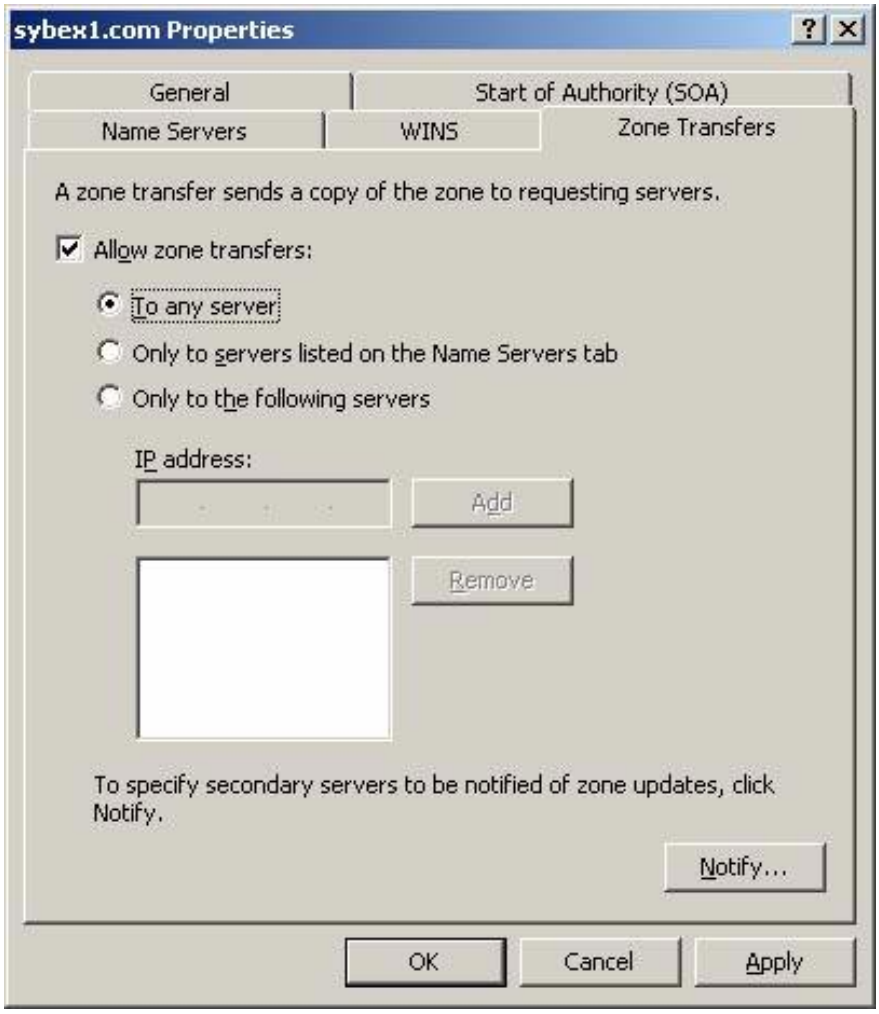


Figure 1: Zone migration interface for Windows DNS

Secure zone migration

You can also change the concept of securing DNS zone transfers to a different level. Making DNS safer is not a radical concept, most companies today implement additional configurations to protect their DNS zone transfers. There are several options to protect DNS and zone transfers. However, the key to the problem is how to set up the DNS environment.

The first is to use IPSec or a VPN tunnel between DNS servers to allow encrypted DNS database communications while it is sent across the entire network. IPSec is a very common way of communicating between DNS servers on the same network. If communication between your DNS servers must go through an unsecured network, a VPN will be used. If you use a VPN to protect data through an unprotected network, the way that is commonly used is to use L2TP. L2TP uses a secure encryption algorithm when it is sent over the network.

Another option to protect data when it is sent on the network from one DNS server to another DNS server is to use Active Directory integration. This method requires DNS servers to operate in the same Active Directory domain. It also requires DNS to run on a domain controller. The benefits are significant because the data is saved and replicated through Active Directory replication, besides the data is encrypted when it is sent from the DNS

server to another DNS server. Another benefit from DNS functionality and migration to Active Directory usage is that all communications are authenticated initially. This helps them to protect domain migration, forcing the DNS server to authenticate the Active Directory database before the information is replicated.

Forward (4 types)

There is another way to protect your DNS environment is to use multiple options for forwarding. This can help you maintain the stability of the DNS infrastructure, while ensuring that computers and applications can access the correct server on the network. There is a pair of options for forwarding within a Microsoft DNS environment.

The first is like a standard transition, shown in Figure 2, all requests that do not make sense for the existing DNS server will be sent along with other DNS servers. This is ideal when you have an internal DNS server that is used for all names, Active Directory, etc. This DNS server is configured on all clients. However, this DNS server doesn't care about names in the Internet, so when the DNS server receives a meaningful request to the Internet, the query is forwarded to another DNS server that can resolve it. This is required. This will protect your internal DNS server from having unnecessary unnecessary network outages.

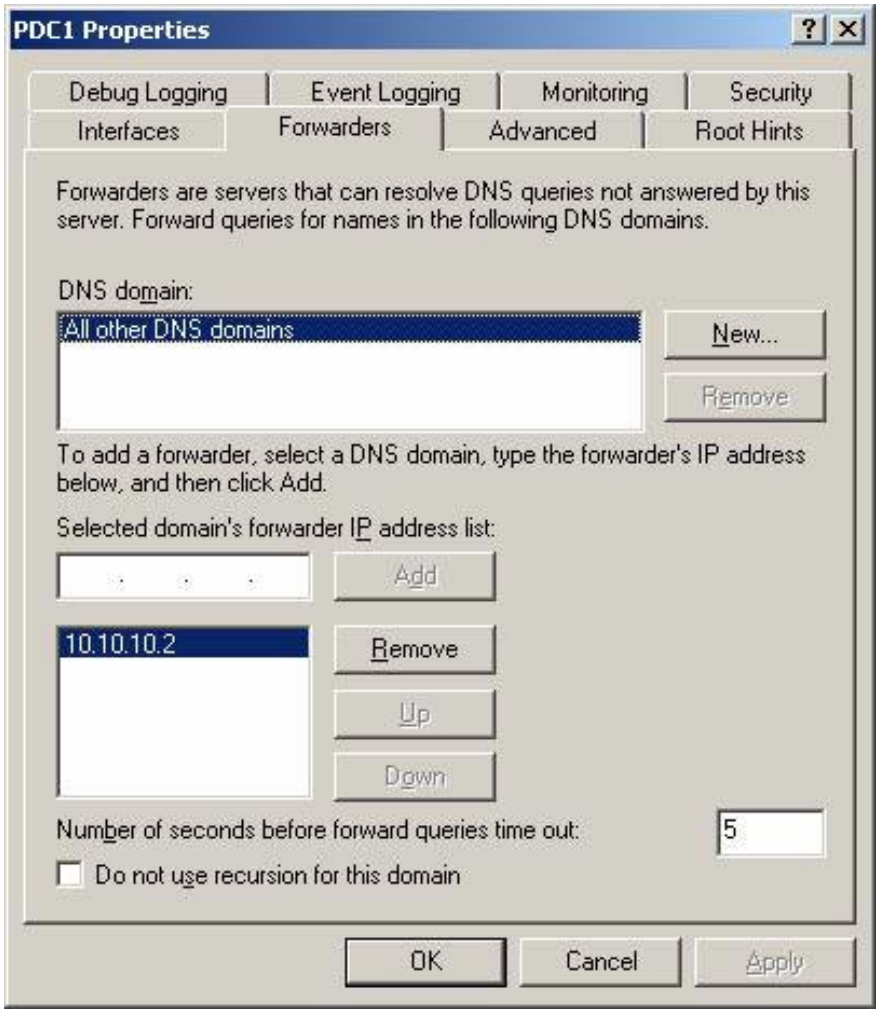


Figure 2: Forwarding to a Windows DNS server

Another option is a forward-looking transition. This can ensure that all requests are redirected to the correct DNS server, which greatly reduces false information and minimal modification. This option is called conditional forwarding, shown in the upper part of Figure 2. They can be used in environments with multiple DNS namespaces inside and you do not want to rely on the Internet or some facilities. Other collaborative DNS infrastructure to resolve names. Here, you simply have a DNS server forwarding requests to another namespace for clients.

Conclude

DNS can be complicated, but when divided into small pieces it is not complicated at all, and can be properly protected. Here, you have seen that DNS can protect the database by configuring with the DSN servers to receive zone transfers. In this situation, your Active Directory and primary zones will have secondary DNS servers so they can communicate with each other. Without this configuration, fake DNS servers can steal all important information on your network. Another step is to make DNS migration safe. Secure DNS servers can be through Active Directory integration, or more sophisticated technologies such as IPSec or VPN tunnels. Finally, controlling your DNS forwarding can ensure that the name resolution becomes more meticulous, more secure, and that protects internal DNS servers from being misguided with inaccurate information. .