Secure DNS connection with Windows Server 2008 R2 DNSSEC

In this tutorial we will introduce general knowledge about DNSSEC and the reasons why securing DNS infrastructure is important to your organization.

Network Management **- In this tutorial we will introduce general knowledge about DNSSEC and the reasons why securing DNS infrastructure is important to your organization** .

With the rise of IPv6, accessing computers via DNS domain names will be more important than ever. Some people who have been working with IPv4 for many years find that they can easily remember the number of IPv4 addresses by a four-digit system separated by dots, while the IPv6 address space is too large and formatted. Hexa is too complicated, so only a few people can remember these complicated IP addresses on their networks. Each IPv6 address has 128 bits - 4 times the length of the IPv4 address. This is a way to provide a larger address space for the growing number of hosts on the Internet, but it also makes it more difficult to remember addresses.

Problem: The insecure nature of DNS databases

Because of the increasing dependence on DNS, we will need a way to ensure that all entries in the DNS database are accurate and reliable - and one of the most effective ways for us to do so. That is to ensure that our DNS databases are secure. Until recently, however, DNS was still known as an insecure system, with a series of assumptions made to provide a basic level of security.

Because of this insecure nature, there have been many instances where trust has been violated and DNS servers are hijacked (redirecting DNS name resolution to fake DNS servers), the fake DNS and DNS cache records, making users believe that they are connecting to valid websites but in fact they are connecting to websites that contain malicious content or may collect information. by *pharming* (redirect the traffic of a website to another website). Pharming is similar to phishing, but instead of using a link in an email, users access it by using the correct URL of the legitimate site and they think it is safe. However, the DNS record has been changed and redirected to the fake URL, the pharming site.

Solution: Windows Server 2008 R2 DNSSEC

One solution you can use on your local network to secure your DNS environment is to use Windows Server 2008 R2 DNSSEC. DNSSEC is a collection of extensions that can improve the security of DNS protocols. These extensions will add reliability, integrity of the data and the ability to reject authenticated DNS. The solution also adds new records to DNS, such as DNSKEY, RRSIGN, NSEC and DS.

How does DNSSEC work?

What DNSSEC does is allow all records in the DNS database to be signed in the same way as the method used to communicate email. When a DNS client issues a query to the DNS server, it returns the digital signatures of the record. The client will have the CA public key that has signed DNS records, then can decrypt the hashed values ??(signatures) and validate responses. To do this, the DNS client and server are configured to use *trust anchors* . *T rust anchor* is a pre-configured public key associated with certain DNS zones.

DNS databases are available for both file-based areas (not Active Directory integration) and integrated ones, replication is also available to other authoritative DNS servers for the currently available talk about.

Windows 2008 R2 and Windows 7 DNS clients are configured, default, invalid. In this case, the DNS client will allow the DNS server to perform validation based on its behavior and the DNS client is able to accept DNSSEC responses sent back from the DNSSEC DNS server. . The DNS client itself is also configured to use the Name Resolution Policy Table (NRPT) to determine how to interact with the DNS server. For example, if the NRPT indicates that the DNS client needs to secure the connection between the client and the DNS server, then the certificate authentication will be executed on the query. If security negotiation fails, there is definitely a problem in name resolution, and the name query attempt will fail. By default, when the client returns a DNS query for the application that created the request, it will only return this information if the DNS server has validated the information.

Ensure valid results

There are two methods used to ensure that the results of the DNS query are valid. First, you need to make sure that DNS servers that have your DNS clients connected are actually DNS servers that you want DNS clients to connect to - they're not DNS servers that attack. or fake is sending fake responses. IPsec is an effective way to ensure the identity of the DNS server. DNSSEC uses SSL to confirm that the connection is secure. The DNS server will authenticate itself through a certificate signed by a trusted publisher (such as your own PKI).

Note that if you have an IPsec server and enforce domain isolation, you must remove TCP and UDP ports 53 in the policy. Otherwise, IPsec policy will be used instead of certificate-based authentication. This will cause the client to fail to validate the certificate from the DNS server and the secure connection will not be established.

Area signed

DNSSEC will sign the zones, use the offline signing action with the dnscmd.exe tool. This method results in the signed regional file. The signed zone file contains RRSIG, DNSKEY, DNS and NSEC resource records for that region. After a region has been signed, it needs to be reloaded using the dnscmd.exe tool or DNS manager console.

One restriction in signing zones is that dynamic updates will be disabled. Windows Server 2008 R2 only allows DNSSEC for static areas. This area must be signed every time a change occurs to the region, which may limit the utility of DNSSEC in many environments.

Role of Anchor Trust

The trust anchor is mentioned above. DNSKEY resource records are used to support trust anchors. A valid DNS server must have at least one trust anchor. Trust anchors also apply only to the area they are assigned. If the DNS server has several areas, then we need to use a lot of trust anchors.

The DNSSEC enabled DNS server will perform validation on the name in a client query as long as the trust anchor is appropriate for that region. The client does not need to know DNSSEC for validation to take place, so DNS clients that do not activate DNSSEC (non-DNSSEC) can still use this DNS server to identify names on the local network.

NSEC / NSEC3

NSEC and NSEC3 are methods that can be used to provide the ability to deny the existence of authenticated DNS records. NSEC3 is an improvement based on the original NSEC specification to allow you to prevent 'zone walking', which allows an attacker to retrieve all names in the DNS zone. This is a useful tool that attackers can use to scout your network. This capability is not available in Windows Server 2008 R2, as it only supports NSEC integration.

However, there are limited support for NSEC3:

- Windows Server 2008 R2 can host an area with NSEC with NSEC3 authorization. However, NSEC3 subdomains are not hosted on Windows DNS servers.
- Windows Server 2008 R2 can be an unrecognized DNS server configured with a trust anchor for an area that has been signed with NSEC and has NSEC3 subdomains.
- Windows 7 clients can use non-Microsoft DNS servers to identify DNS names when the server knows about NSEC3.
- When a zone is signed to NSEC, you can configure the Name Resolution Policy Table so that it does not require regional validation. When you do this, the DNS server will not perform validation and will return a response with Active Directory.

Deploy DNSSEC

To deploy DNSSEC, you need to do the following steps:

- Learn the key concepts of DNSSEC
- Upgrade DNS server to Windows Server 2008 R2
- Re-evaluate signed requests, select a lock release mechanism and identify secure computers and DNSSEC protected areas.

- Create and backup keys for your regions. Confirm that DNS will still work and respond to queries after signing the zone.
- Your trust anchor distribution for all unrecognized servers will perform DNS validation with DNSSEC.
- Deploy IPsec certificates and policies for DNS servers
- Configure NRPT settings and deploy IPsec policies for clients.

Conclude

In this article we have provided you with a high level overview of DNSSEC and some of the reasons for securing DNS infrastructure are so important for your organization. Windows Server 2008 R2 introduces a number of new features that can ensure your DNS infrastructure becomes safer than ever through use in conjunction with signed DNS zones, secure SSL connections. for trusted DNS servers, IPsec authentication and encryption. In the following article, we will present DNSSEC solution at a more detailed level and introduce in detail about new resource records, server signing and client interaction that takes place between client and machine. host DNSSEC.