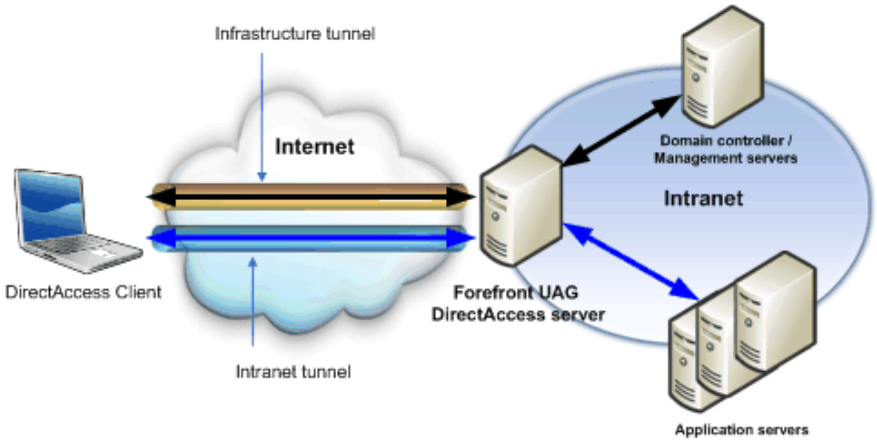
Introduction to UAG DirectAccess - Part 3: NAT64 / DNS64

In this section, I will show you some of the key techniques in deploying DirectAccess in that there is no need to upgrade the network infrastructure to IPv6.

In this section, I will show you some of the key techniques in deploying DirectAccess in that there is no need to upgrade the network infrastructure to IPv6.

In Part 1 of this series, I talked about DirectAccess and explained how DirectAccess works. Part two is a detailed introduction to IPv6 transition techniques to allow DirectAccess clients and servers to communicate with each other in the internal network as well as the IPv4 Internet. It introduced how the DirectAccess client uses the Name Resolution Policy Table (NRPT) to determine if the domain is resolved by internal DNS servers and the domain is resolved by a DNS server outside the Internet.



In this article, I will show you some of the key techniques in deploying DirectAccess in that there is no need to upgrade the network infrastructure to IPv6. This issue is especially important because most networks now have 'IPv4 only' and 'IPv6 capable' clients and servers. In addition, devices that support IPv4 (or IPv4 resources for short) are still more popular than 'IPv6 capable' devices. This is the reality of the network environment in most companies today, and UAG DirectAccess will allow access to IPv4 resources on that network.

Solution: NAT64 / DNS64

UAG DirectAccess manages the problem by executing two techniques that are not available for the Windows DirectAccess solution:

- NAT64
- DNS64

These two techniques allow the DirectAccess client to always use IPv6 'language' with the UAG DirectAccess server to connect to 'IPv4 only' resources on the intranet.

When the DirectAccess client sends requests to access resources by using the complete name or domain name FQDN, it first references the Name Resolution Policy Table (NRPT) table. If there is a match on the table and there is no exception rule for the domain then the client sends a domain resolution request to the IPv6 (6to4) address of the UAG DirectAccess server. If the label name is required, the DirectAccess client's DNS client component will append the DNS suffix as configured on the NIC or through Group Policy.

When the UAG DirectAccess server receives this request, it sends a request to the DNS servers configured on the internal interface in order of the listed server. DNS query requests will be for both IPv4 Host (A) and IPv6 Quad A (AAAA) records. If the DNS server responds to the UAG DirectAccess server with a Quad A record, it will respond to this record with the DirectAccess client and the DirectAccess client will connect to the IPv6 address included in the Quad A response via the DirectAccess IPsec tunnel. .

However, if the DNS server responds to the UAG DirectAccess server with an IPv4 Host (A) record, the DirectAccess client on the Internet will experience problems, because the DirectAccess client can only communicate via IPv6. To solve the problem, the DNS64 component of the UAG DirectAccess server will map the domain name to IPv6 only and then declare the U64 DirectAccess server's NAT64 component between the IPv6 address and the IPv4 address.

For example, suppose the DirectAccess client on the Internet needs to connect to the SRV1.contoso.com domain. It will send the domain query request to the IPv6 address (6to4) of the UAG DirectAccess server via the IPsec tunnel. The UAG DirectAccess server sends IPv4 Host (A) and IPv6 Host (Quad A) requests for the SRV1.contoso.com domain to the DNS server configured on the internal interface. Then the DNS server will only respond to the record with IP address 10.0.0.66. The DNS64 component on the UAG DirectAccess server maps the 10.0.0.66 address to an IPv6 address, such as 2002 :: 0066 (this is an illustration only). The DNS64 component of the UAG DirectAccess server will declare to that NAT64 component that it will forward any requests to the 2002 :: 0066 address to the IP address 10.0.0.66. Session state is also marked so that the response from 10.0.0.66 is forwarded to the DirectAccess client. The UAG DirectAccess server will forward the domain resolution response to SRV1.contoso.com via the IP address 2002 :: 0066 to the DirectAccess client on the Internet and the DirectAccess client will send a connection request to that address.

As you can see, DNS64 / NAT64 acts as an IPv6 / IPv4 protocol compiler, so that the DirectAccess client on the Internet can connect to 'IPv4 only' resources on the intranet. In fact, this means that the client components installed on the DirectAccess client need to be 'IPv6 aware', but the server components do not need to be. This allows to expand the number of DirectAccess client scripts connected to intranet resources.

Limit

However, like all NAT-based solutions, there are some limitations and disadvantages to this solution. The main limitations here are:

- NAT64 / DNS64 will consume CPU and memory resources and thus may negatively affect performance wear on the UAG DirectAccess server.
- NAT64 / DNS64 only works in the 'NAT forwarding' scenario. This means that you cannot 'reverse NAT' from the local network to the DirectAccess client from an IPv4 management station. As a result, it is not possible to initiate a connection from the 'IPv4 only' management station to the DirectAccess client. However, the DirectAccess client can connect to the management station as long as it initiates the connection. If the solution works with this existing connection, you can connect back to the DirectAccess client.
- NAT64 / DNS64 does not have any NAT editors (NAT editors). NAT editors are often used to allow applications to embed network information into their application protocols. For example, the FTP protocol will embed IP address information into its protocol and the OCS client will embed the IPv4 address into the application protocol. This method cannot be applied to NAT64 / DNS64 because there is no NAT editor to help them work.

Here are some problems you may encounter when using the UAG DirectAccess server's NAT64 / DNS64 solution. It should be noted that NAT64 / DNS64 is only used if the server with the application running on it does not support IPv6 or if the application itself does not support IPv6. If the server and application support IPv6, NAT64 / DNS64 will be used and communication from the DirectAccess client to the destination server will be the communication to the ISATAP address assigned to the server on the corporate network.

Note:

An interesting fact about UAG DirectAccess NAT64 / DNS64 is that, the NAT64 component is part of the TMG application installed on the UAG DirectAccess server, while the DNS64 component is part of the UAG code.

Another thing you need to know is that NAT64 / DNS64 allows deploying DirectAccess in organizations that do not require Windows 2008 R2 except on UAG DirectAccess servers. Your entire company may be using Windows Server 2000 domains and resources are hosted on Windows 2000, Windows Server 2003, Windows Server 2008 servers or even non-Microsoft operating systems, the DirectAccess clients. can still connect to that resource. This explains why NAT64 / DNS64 is so important - it allows you to deploy DirectAccess without the cost of upgrading the infrastructure. If you've heard somewhere saying that an IPv6 network is needed before deploying DirectAccess, this is completely wrong; Your network may be IPv4 but can still exploit the benefits of UAG DirectAccess deployment.

Conclude

In this article, I have shown you how the DirectAccess client uses IPv6 to communicate with the DirectAccess server. This requires that the DirectAccess client be able to communicate with resources on the intranet that are not 'IPv6 capable'. And the solution to that problem is UAG NAT64 / DNS64 service. This service can map domain names and addresses of 'IPv4 only' resources to the IPv6 address used by the DirectAccess client. This allows the DirectAccess client to initiate connections to resources on the intranet. However, there are still limitations to NAT64 / DNS64 services, such as resources on the local network that cannot initiate connections to the DirectAccess client. However, because most of the connection cases are done from the client side, the above limitation is not too serious.

Next

In the next part of this series, we will introduce the main infrastructure components needed for the UAG DirectAccess deployment to work. These components include:

- Active Directory Domain Services and Group Policy
- Domain Name Services (DNS)
- Public Key Infrastructure (PKI) and Windows Active Directory Certificate Services
- Network Location Servers
- Server Certificate Revocation List (CRL)
- Windows Firewall with Advanced Security and Network Firewalls
- Remote Access VPN server
- NAP and Smart Card Infrastructure.