Introduction

Split Domain Name System (DNS) allows DNS queries for certain domain names to be resolved to internal DNS servers over the VPN tunnel, while all the other DNS queries are resolved to the Internet Service Provider's (ISP) DNS servers. A list of internal domain names is "pushed" to the VPN Client during initial tunnel negotiation. The VPN Client then determines whether DNS queries should be sent over the encrypted tunnel or sent unencrypted to the ISP. Split DNS is only used in split-tunneling environments, since traffic is sent both over the encrypted tunnel and unencrypted to the Internet.

Dynamic DNS (DDNS) allows automatic registration of VPN Client host names into a DNS server upon successful negotiation of the VPN connection. When a VPN Client initiates a connection, the local host name is sent to the concentrator, which in turn forwards this onto the centrally located Dynamic Host Configuration Protocol (DHCP) server for the address allocation. If the DHCP server supports DDNS, then the allocated address and host name are entered automatically. DHCP address allocation is a requirement for DDNS to function, but does not work with local address pools.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

Both split DNS and DDNS were introduced in version 3.6 of both concentrator and client code. You must run at least these versions to enable and configure this feature. All the configurations in this document were developed and tested using these software and hardware versions.

- Cisco VPN 3000 Concentrator Version 3.6.7.A
- Cisco VPN Client Version 3.6.1
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

**Network Diagram**

This document uses this network setup:

![Network Diagram](image-url)

**Conventions**

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

**Configuring Split DNS and DDNS**

**Split DNS**

In this section, you are presented with the information to configure the features described in this document. Split DNS parameters are configured under the group parameters on the Cisco VPN 3000 Concentrator. Therefore, no configuration on the client is necessary.

1. Under the **User Management > Groups** section of the GUI, select the appropriate group, and select **Modify Group**.
2. Under the General tab, enter up to two internal DNS servers to be passed down to the client.
3. Under the Client Config tab, configure split tunneling, the default domain name, and the split DNS domain list.
After the tunnel is successfully negotiated using the above parameters, any reference to hosts with fully qualified domain names in the Cisco.com or Test.com domains results in a DNS query being sent over the tunnel to 192.168.1.1. DNS queries for hosts in any other domain are sent unencrypted to the DNS servers provided by DHCP at the initial PC boot up time.

**Note:** The split tunnel list called "192.168 Network" contains the 192.168.0.0/16 network. This is necessary so that the DNS requests to the internal DNS server of 192.168.1.1 will be encrypted.
DDNS

DDNS requires that the DHCP address assignment is configured on the VPN Concentrator. Therefore, no configuration on the client is necessary. During the initial tunnel negotiation, the client sends its host name to the concentrator, and the concentrator uses this in its DHCP request packet when requesting an address for the client. It is up to the DHCP server to dynamically add this host name into the DDNS server. Windows 2000 DHCP servers support this functionality.

1. To configure DHCP address allocation for VPN Clients on the VPN Concentrator, under Configuration > System > Servers > DHCP, add the DHCP servers IP address. Ensure that DHCP is enabled globally on the concentrator under Configuration > System > IP Routing > DHCP Parameters.

Note: This is enabled by default.

2. Under Configuration > System > Address Management > Assignment, check the option to allocate addresses from a DHCP server.

<table>
<thead>
<tr>
<th>Use Client Address</th>
<th>Check to use the IP address supplied by the client. This can be overridden by user/group configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Address from Authentication Server</td>
<td>Check to use an IP address retrieved from an authentication server for the client.</td>
</tr>
<tr>
<td>Use DHCP</td>
<td>Check to use DHCP to obtain an IP address for the client.</td>
</tr>
<tr>
<td>Use Address Pools</td>
<td>Check to use internal address pool configuration to obtain an IP address for the client.</td>
</tr>
</tbody>
</table>

Verify

The Log Viewer included with the VPN Client can be used to ensure the correct parameters are being sent down from the VPN Concentrator. Under Options > Filters, set the Internet Key Exchange (IKE) log class to High. After the tunnel is successfully negotiated, the following messages (or your network–specific equivalent) should be present in the log.

34 11:43:38.069 03/07/03 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 192.168.1.50

35 11:43:38.069 03/07/03 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 192.168.1.1

38 11:43:38.069 03/07/03 Sev=Info/5 IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG.Unity.SplitInclude (# of split_nets), value = 0x00000001

39 11:43:38.069 03/07/03 Sev=Info/5 IKE/0x6300000F
SPLIT_NET #1
subnet = 192.168.0.0
mask = 255.255.0.0
protocol = 0
src port = 0
dest port=0

40 11:43:38.069 03/07/03 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG.Unity.DEFDOMAIN: , value = cisco.com

41 11:43:38.069 03/07/03 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG.Unity.SplitDNS_name: , value = cisco.com,test.com

The above parameters are defined as follows:
• INTERNAL_IPV4_ADDRESS – IP address allocated to VPN Client connection
• INTERNAL_IPV4_DNS(1) – Internal DNS server
• MODECFG.Unity_SPLIT_INCLUDE – Number of networks in the split tunnel list
• SPLIT_NET #n – Details of each split tunnel network passed down to client
• MODECFG.Unity_DEFDOMAIN – Default domain name
• MODECFG.Unity_SPLITDNS_NAME – List of internal domains to be sent to INTERNAL_IPV4_DNS

Troubleshoot

There is currently no specific troubleshooting information available for this configuration. For additional troubleshooting information, refer to Troubleshooting Connection Problems on the VPN 3000 Concentrator.

Related Information

• VPN 3000 Concentrator Configuration Guide
• Cisco VPN 3000 Series Concentrator Support Page
• Cisco VPN 3000 Series Client Support Page
• IPSec Support Page
• Technical Support – Cisco Systems