

Configuring Split and Dynamic DNS on the Cisco VPN 3000 Concentrator

Document ID: 26405

Introduction

Prerequisites

Requirements

Components Used

Network Diagram

Conventions

Configuring Split DNS and DDNS

Split DNS

DDNS

Verify

Troubleshoot

Related Information

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.

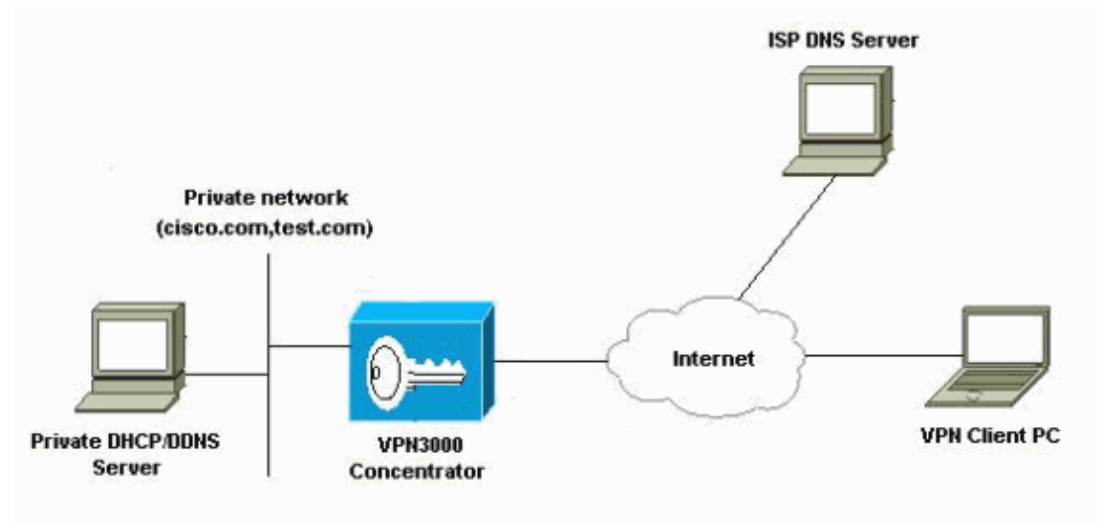
- Cisco VPN 3000 Concentrator Version 3.6.7.A
- Cisco VPN Client Version 3.6.1

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:



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.

Identity General IPsec Client Config Client FW HW Client PPTP/L2TP			
General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS	192.168.1.1	<input type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS	192.168.2.2	<input type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input checked="" type="checkbox"/>	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to remove the realm qualifier of the user name during authentication.

- Under the Client Config tab, configure split tunneling, the default domain name, and the split DNS domain list.

Client Configuration Parameters			
Cisco Client Parameters			
Attribute	Value	Inherit?	Description
Banner		<input checked="" type="checkbox"/>	Enter the banner for this group. Only software clients see the banner.
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to store the password locally.
IPSec over UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPSec over UDP Port	10000	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPSec Backup Servers	Use Client Configured List	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> Select a method to use or disable backup servers. Enter up to 10 IPSec backup server addresses/names starting from high priority to low. Enter each IPSec backup server address/name on a single line.
Microsoft Client Parameters			
Intercept DHCP Configure Message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to use group policy for clients requesting Microsoft DHCP options.
Subnet Mask	255.255.255.255	<input checked="" type="checkbox"/>	Enter the subnet mask for clients requesting Microsoft DHCP options.
Common Client Parameters			
Split Tunneling Policy	<input type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in list to bypass the tunnel <input checked="" type="radio"/> Only tunnel networks in the list	<input type="checkbox"/>	Select the method and network list to be used for Split Tunneling. Tunnel Everything: Send all traffic through the tunnel. Allow the networks in the list to bypass the tunnel: The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE This setting only applies to the Cisco VPN Client. Tunnel networks in the list: Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.
Split Tunneling Network List	192.168 Network	<input type="checkbox"/>	
Default Domain Name	cisco.com	<input type="checkbox"/>	Enter the default domain name given to users of this group.
Split DNS Names	cisco.com,test.com	<input type="checkbox"/>	Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel. The Default Domain Name must be explicitly included in Split DNS Names list if it is to be resolved through the tunnel.

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.

Use Client Address <input type="checkbox"/>	Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
Use Address from Authentication Server <input type="checkbox"/>	Check to use an IP address retrieved from an authentication server for the client.
Use DHCP <input checked="" type="checkbox"/>	Check to use DHCP to obtain an IP address for the client.
Use Address Pools <input type="checkbox"/>	Check to use internal address pool configuration to obtain an IP address for the client.

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_SPLIT_INCLUDE (# of split_nets), value = 0x000000

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**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 14, 2008

Document ID: 26405
