

Configuración del DNS dividido y dinámico en el concentrador VPN 3000 de Cisco

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Convenciones](#)

[Configuración de DNS y DDNS divididos](#)

[DNS dividido](#)

[DDNS](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Dividir el Sistema de nombres de dominio (DNS) permite consultas DNS para que ciertos nombres de dominio sean resueltos por los servidores DNS internos sobre el túnel VPN, mientras todas las otras consultas DNS son resueltas por el servidor DNS del Proveedor del servicio de Internet (ISP). Durante la negociación inicial del túnel se “empuja” una lista de nombres de dominio interno al VPN Client. El cliente VPN luego determina si las búsquedas de DNS deben enviarse a través del túnel encriptación o enviarse al ISP sin cifrar. El DNS dividido sólo se usa en entornos de tunelización dividida, ya que el tráfico se envía a Internet sobre el túnel encriptación y no encriptación.

DNS dinámica (DDNS) permite el registro automático de los nombres de host VPN Client en un servidor DNS ante una negociación exitosa de la conexión VPN. Cuando un cliente VPN inicia una conexión, el nombre del host local se envía al concentrador, que a su vez lo reenvía al servidor ubicado centralmente en el Protocolo de configuración dinámica de host (DHCP) para la asignación de la dirección. Si el servidor DHCP soporta DDNS, entonces la dirección y el nombre de host asignados son introducidos automáticamente. La asignación de la dirección DHCP es un requisito para el funcionamiento de DDNS, pero no funciona con agrupaciones de direcciones locales.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

Componentes Utilizados

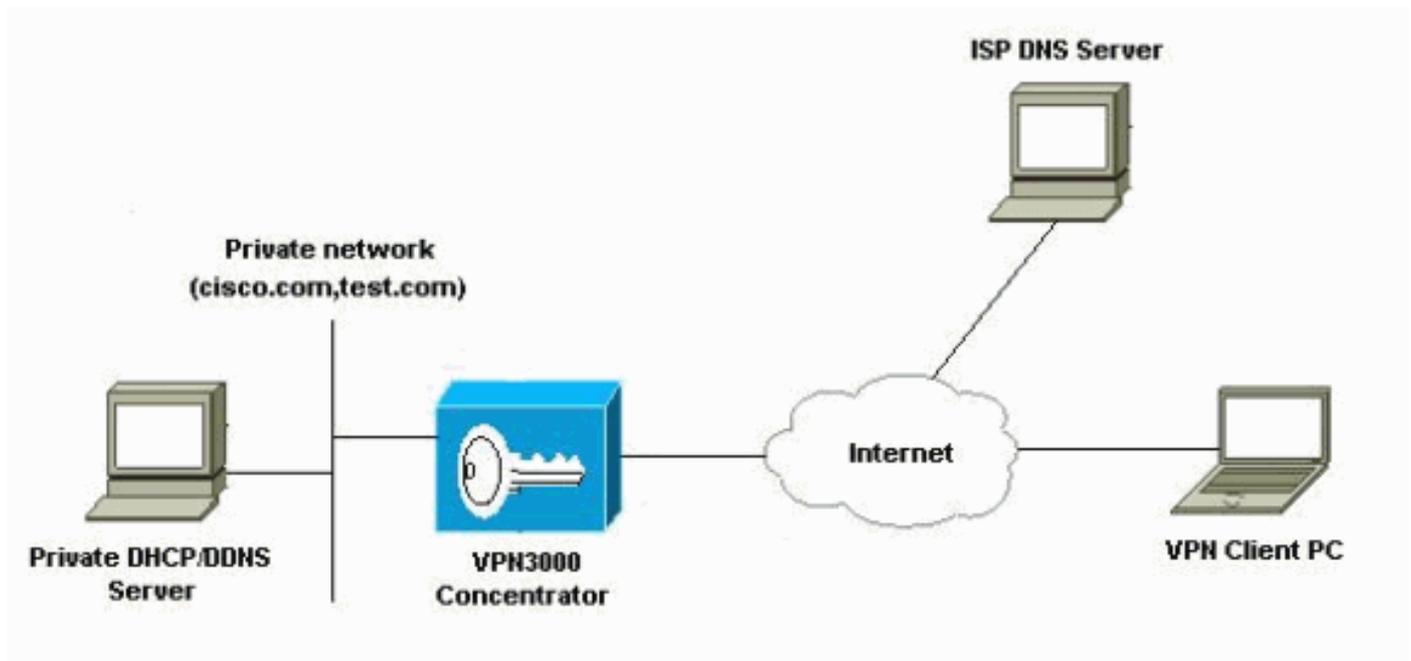
Tanto los DDNS como los DNS divididos se introdujeron en la versión 3.6 del concentrador y del código de cliente. Debe ejecutar al menos estas versiones para activar y configurar esta función. Todas las configuraciones en este documento fueron desarrolladas y probadas usando estas versiones de software y hardware.

- Concentrador Cisco VPN 3000 versión 3.6.7.A
- Cliente Cisco VPN versión 3.6.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

Configuración de DNS y DDNS divididos

DNS dividido

En esta sección encontrará la información para configurar las funciones descritas en este documento. Los parámetros de DNS dividido se configuran dentro de los parámetros de grupo del Concentrador VPN 3000 de Cisco. Por tanto, no es necesario configurar el cliente.

1. En User Management (Administración de usuarios) > Sección Groups (Grupos) de la GUI,

seleccione el grupo adecuado y luego Modify Group (Modificar grupo).

2. En la ficha General, introduzca hasta dos servidores internos DNS que transmitirá al

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.

cliente.

3. En la ficha Client Config (Config. del cliente), configure la tunelización dividida, el nombre de dominio predeterminado y la lista de dominio de DNS

