Configuration du DNS partagé et DNS dynamique sur le concentrateur Cisco VPN 3000

Contenu

Introduction

Le Système de noms de domaine (DNS) fendu permet des requêtes DNS pour que certains noms de domaine soient résolus aux serveurs DNS internes au-dessus du tunnel VPN, alors que toutes les autres requêtes DNS sont résolues aux serveurs DNS du fournisseur d'accès Internet (ISP). Une liste de noms de domaine internes « est poussée » au client vpn pendant la négociation initiale de tunnel. Le client vpn détermine alors si des requêtes DNS devraient être envoyées au-dessus du tunnel chiffré ou du décrypté envoyé à l'ISP. Des DN fendus est seulement utilisés dans des environnements de Segmentation de tunnel, puisque le trafic est envoyé au-dessus du tunnel chiffré et décrypté à l'Internet.

Les DN dynamiques (DDNS) permet l'enregistrement automatique des noms d'hôte de client vpn dans un serveur DNS sur la négociation réussie de la connexion VPN. Quand un client vpn initie une connexion, le nom d'hôte local est envoyé au concentrateur, qui consécutivement en avant ceci sur le serveur centralement localisé du protocole DHCP (DHCP) pour l'allocation d'adresse. Si le serveur DHCP prend en charge DDNS, alors l'adresse et le nom d'hôte alloués sont écrits automatiquement. L'allocation d'adresse DHCP est une condition requise pour que DDNS fonctionne, mais ne fonctionne pas avec des groupes d'adresse locale.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

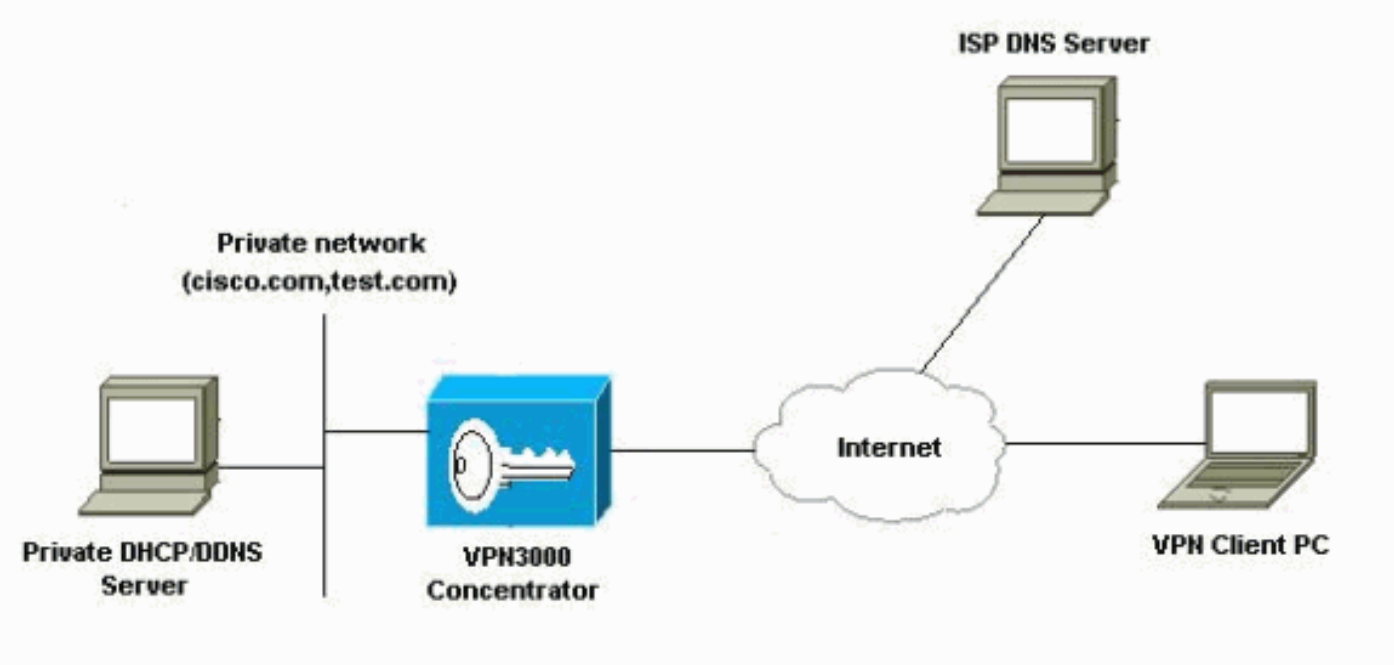
Séparez les DN et DDNS ont été introduits dans la version 3.6 du concentrateur et du code client. Vous devez exécuter au moins ces versions pour activer et configurer cette caractéristique. Toutes les configurations dans ce document ont été développées et testées utilisant des ces le logiciel et les versions de matériel.

- Version 3.6.7.A de concentrateur de Cisco VPN 3000
- Version 3.6.1 de Client VPN Cisco

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

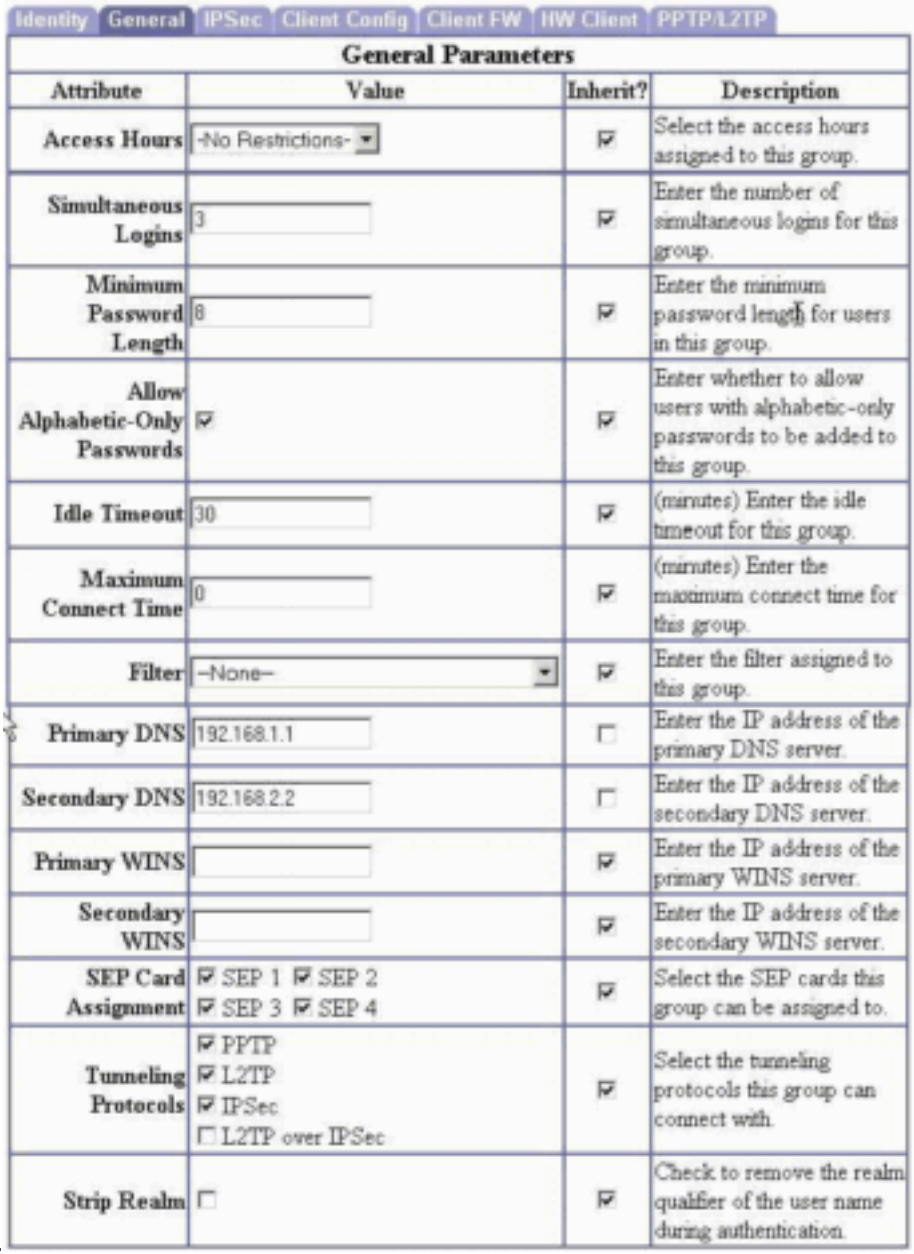
Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurer les DN fendus et le DDNS

DN fendus

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document. Des paramètres fendus de DN sont configurés sous les paramètres de groupe sur le concentrateur de Cisco VPN 3000. Par conséquent, aucune configuration sur le client n'est nécessaire.

1. Sous la section de **gestion des utilisateurs** > de **groupes du** GUI, sélectionnez le groupe approprié, et choisi **modifiez le groupe**.
2. Sous l'onglet Général, présentez jusqu'à deux serveurs DNS internes à passer vers le bas au client.



Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters

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

3. Sous l'onglet de config de client, configurez la Segmentation de tunnel, le nom de domaine par défaut, et le domain list fendu de