Présentation de VRRP

Contenu

Introduction

Le Virtual Router Redundancy Protocol (VRRP) élimine le point de panne unique inhérent à l'environnement routé par défaut statique. Le VRRP spécifie un protocole d'élection qui assigne dynamiquement la responsabilité d'un routeur virtuel (un cluster de concentrateurs de la gamme VPN 3000). Le concentrateur VRRP VPN qui contrôle l'adresse IP associée à un routeur virtuel s'appelle le maître et transmet les paquets envoyés à ces adresses IP. Quand le maître devient indisponible, un concentrateur VPN de remplacement le remplace.

Remarque: Référez-vous à « configuration | Système | IP ROUTING | Redondance » dans le Guide de l'utilisateur des concentrateurs VPN Cisco 3000 ou à l'aide en ligne de VPN 3000 Concentrator Manager pour des informations complètes sur le VRRP et comment le configurer.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations de ce document sont basées sur le Concentrateur VPN Cisco 3000.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Comment le concentrateur VPN 3000 met-il en œuvre le VRRP ?

1. Les concentrateurs VPN redondants sont identifiés par groupe.
2. Un seul maître est choisi pour le groupe.
3. Un ou plusieurs concentrateurs VPN peuvent remplacer le maître du groupe.
4. Le maître communique son état aux périphériques de remplacement.
5. Si le maître ne communique pas son état, le VRRP essaie chaque périphérique de remplacement par ordre de priorité. Le périphérique de remplacement assume le rôle de maître.**Remarque:** Le VRRP active la redondance pour les connexions en tunnel seulement. Par conséquent, si un basculement de VRRP se produit, le périphérique de remplacement écoute les protocoles et le trafic en mode tunnel. L'envoi d'un ping au concentrateur VPN ne fonctionne pas. Les concentrateurs VPN participants doivent avoir des configurations identiques. Les adresses virtuelles configurées pour le VRRP doivent correspondre à celles configurées sur les adresses d'interface du maître.

Configuration de VRRP

Le VRRP est configuré sur les interfaces publiques et privées dans cette configuration. Le VRRP s'applique seulement aux configurations où deux concentrateurs VPN ou plus fonctionnent en parallèle. Tous les concentrateurs VPN participants ont un utilisateur, un groupe et des paramètres LAN-LAN identiques. Si le maître échoue, celui qui le remplace commence par servir le trafic auparavant géré par le maître. Ce passage se produit en 3 à 10 secondes. Alors que les connexions client IPsec et de protocole de tunnellisation point à point (PPTP) sont déconnectées pendant cette transition, les utilisateurs n'ont qu'à se reconnecter sans changer l'adresse de destination de leur profil de connexion. Dans une connexion LAN-LAN, ce passage est transparent.

Cette procédure montre comment mettre en œuvre cet exemple de configuration.

Sur les systèmes maîtres et de remplacement :

1. Sélectionnez **Configuration > System > IP Routing > Redundancy**. Changez seulement ces paramètres. Laissez tous les autres paramètres dans leur état par défaut :Entrez un mot de passe (au maximum 8 caractères) dans le champ Group Password.Entrez les adresses IP dans le champ Group Shared Addresses (1 privée) des systèmes maîtres et de tous les systèmes de remplacement. Pour cet exemple, l'adresse est 10.10.10.1.Entrez les adresses IP dans le champ Group Shared Addresses (2 publiques) des systèmes maîtres et de tous les systèmes de remplacement. Pour cet exemple, l'adresse est 63.67.72.155.
2. Revenez aux fenêtres **Configuration > System > IP Routing > Redundancy** sur toutes les unités et cochez **Enable VRRP**.**Remarque:** Si vous avez configuré l'équilibrage de charge entre les deux concentrateurs VPN avant et que vous configurez le VRRP sur eux, veillez à effectuer la configuration du pool d'adresses IP. Si vous utilisez le même pool IP qu'avant, vous devez les changer. C'est nécessaire parce que le trafic provenant d'un pool IP dans un scénario d'équilibrage de charge est acheminé vers seulement un des concentrateurs VPN.

Synchronisation des configurations

Cette procédure montre comment synchroniser la configuration entre le maître et l'esclave en effectuant un équilibrage de charge ou un principal en un secondaire avec un protocole VRRP.

1. Dans Master ou Primary, sélectionnez **Administration > File Management** et cliquez sur **View** depuis la ligne CONFIG.
2. Quand le navigateur Web s'ouvre avec la configuration, mettez en surbrillance la configuration et copiez-la (cntrl-a, cntrl-c).
3. Collez la configuration dans WordPad.
4. Sélectionnez **Edit > Replace** et entrez l'adresse IP de l'interface publique du maître ou du principal dans le champ Find What field. Dans le champ Replace With, entrez l'adresse IP que vous prévoyez d'assigner à l'esclave ou au remplaçant.Faites la même chose pour l'IP privé et l'interface externe si vous la configurez.
5. Enregistrez le fichier et donnez-lui un nom de votre choix. Cependant, vérifiez que vous l'enregistrez comme « document texte » (par exemple, synconfig.txt).Vous *ne pouvez pas* enregistrer en .doc (la valeur par défaut) puis changer l'extension plus tard. En effet, le format est enregistré et le concentrateur VPN n'accepte que du texte.
6. Allez à l'esclave ou au secondaire et sélectionnez **Administration > File Management > File Upload**.
7. Entrez **config.bak dans** le fichier dans le champ VPN 3000 Concentrator et recherchez le fichier enregistré sur votre PC (synconfig.txt). Cliquez ensuite sur Upload.Le concentrateur VPN le télécharge et change automatiquement synconfig.txt en config.bak.
8. Sélectionnez **Administration > File Management > Swap Configuration Files** et cliquez sur **OK** pour que le concentrateur VPN démarre avec le fichier de configuration téléchargé.
9. Une fois redirigé vers la fenêtre System Reboot, laissez les configurations par défaut et cliquez sur **Apply**.Lorsqu'il apparaît, il a la même configuration que le maître ou le principal excepté les adresses que vous avez précédemment changées.**Remarque:** N'oubliez pas de changer les paramètres dans la fenêtre Load Balancing ou Redundancy (VRRP). Sélectionnez **Configuration > System > IP Routing > Redundancy**.**Remarque:** Alternativement, sélectionnez **Configuration > System > Load Balancing**.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems