

Was ist VRRP?

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Wie implementiert der VPN 3000-Konzentrator VRRP?](#)

[Konfigurieren von VRRP](#)

[Synchronisieren der Konfigurationen](#)

[Zugehörige Informationen](#)

Einführung

Das Virtual Router Redundancy Protocol (VRRP) beseitigt den Single-Point-of-Failure, der in der statischen Standard-Routing-Umgebung entsteht. Der VRRP legt ein Wahlprotokoll fest, das einem der VPN-Konzentratoren in einem LAN die Verantwortung für einen virtuellen Router (ein Concentrator-Cluster der Serie VPN 300) dynamisch zuweist. Der VRRP VPN Concentrator, der die IP-Adresse(n) steuert, die einem virtuellen Router zugeordnet ist, wird als "Primär" bezeichnet und leitet Pakete weiter, die an diese IP-Adressen gesendet werden. Wenn das primäre Gerät nicht mehr verfügbar ist, ersetzt ein Backup-VPN-Konzentrator das primäre Gerät.

Hinweis: Weitere Informationen finden Sie unter "Konfiguration | System | IP-Routing | Redundanz" im [Benutzerhandbuch zur VPN Concentrator Serie 300](#) oder in der Online-Hilfe für diesen Abschnitt des VPN 300 Concentrator Manager finden Sie vollständige Informationen zum VRRP und dessen Konfiguration.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco VPN Concentrator der Serie 3000.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

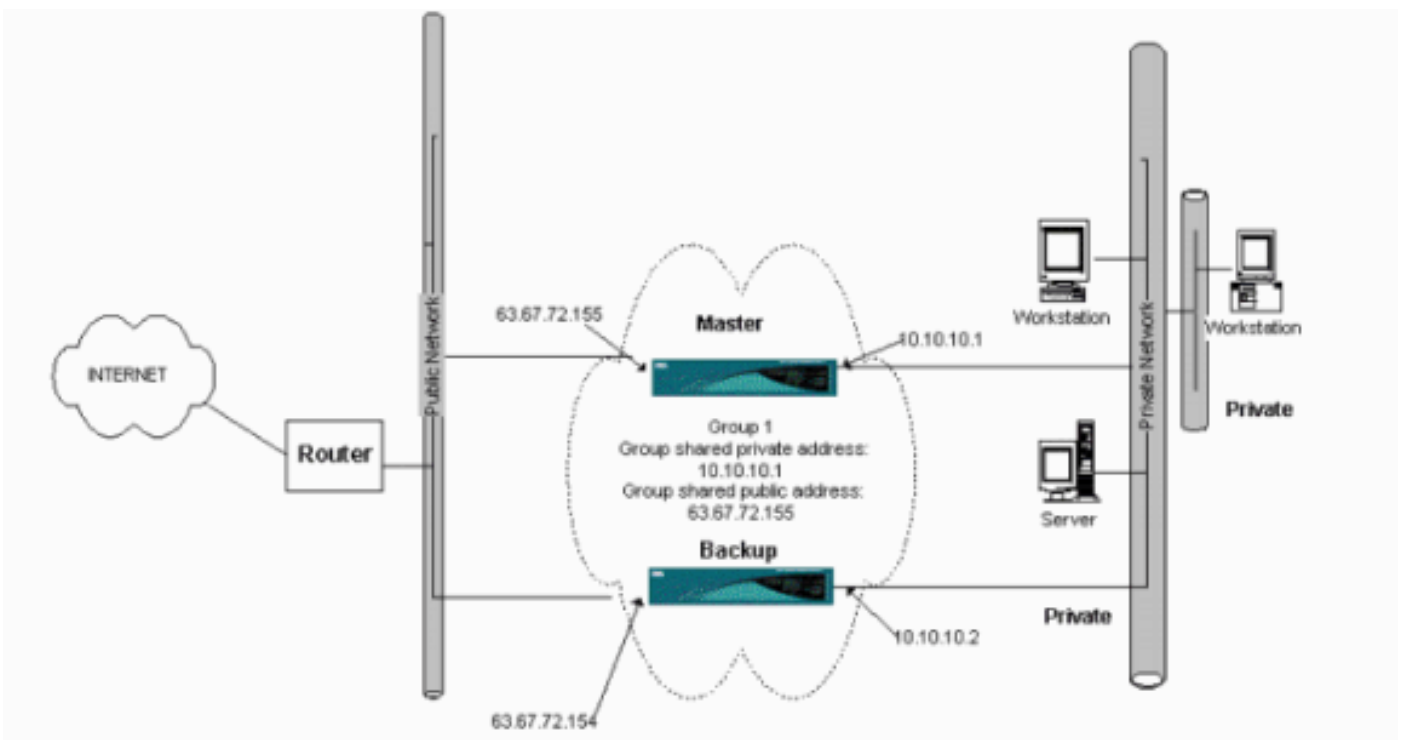
Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Wie implementiert der VPN 3000-Konzentrator VRRP?

1. Redundante VPN-Concentrators werden nach Gruppe identifiziert.
2. Für die Gruppe wird eine primäre Gruppe ausgewählt.
3. Ein oder mehrere VPN-Konzentratoren können Backups des primären Bereichs der Gruppe sein.
4. Das primäre System kommuniziert seinen Zustand mit den Backup-Geräten.
5. Wenn das primäre System seinen Status nicht kommuniziert, versucht das VRRP jede Sicherung in der Rangfolge. Das antwortende Backup übernimmt die Rolle des primären. **Hinweis:** VRRP ermöglicht Redundanz nur für Tunnelverbindungen. Wenn ein VRRP-Failover auftritt, überwacht die Sicherung daher nur Tunnelprotokolle und den Datenverkehr. Das Pingen des VPN-Concentrators funktioniert nicht. Teilnehmer von VPN Concentrators müssen über identische Konfigurationen verfügen. Die für den VRRP konfigurierten virtuellen Adressen müssen mit den für die Schnittstellenadressen des primären Geräts konfigurierten Adressen übereinstimmen.

Konfigurieren von VRRP

VRRP wird in dieser Konfiguration auf den öffentlichen und privaten Schnittstellen konfiguriert. VRRP gilt nur für Konfigurationen, bei denen zwei oder mehr VPN-Konzentratoren parallel betrieben werden. Alle teilnehmenden VPN-Konzentratoren haben identische Benutzer-, Gruppen- und LAN-zu-LAN-Einstellungen. Wenn das primäre Objekt fehlschlägt, beginnt das Backup-Programm, den Datenverkehr zu servicebasiert, der zuvor vom primären Gerät verarbeitet wurde. Dieser Switchover erfolgt in 3 bis 10 Sekunden. Während IPsec- und PPTP-Clientverbindungen (Point-to-Point Tunnel Protocol) während dieser Übergangsphase getrennt werden, müssen Benutzer nur eine erneute Verbindung herstellen, ohne die Zieladresse ihres Verbindungsprofils zu ändern. Bei einer LAN-zu-LAN-Verbindung erfolgt der Switchover nahtlos.



In diesem Verfahren wird veranschaulicht, wie diese Beispielkonfiguration implementiert wird.

Auf den primären und Backup-Systemen:

1. Wählen Sie **Konfiguration > System > IP Routing > Redundanz** aus. Ändern Sie nur diese Parameter. Behalten Sie alle anderen Parameter im Standardzustand bei: Geben Sie im Feld Group Password (Gruppenkennwort) ein Kennwort (maximal 8 Zeichen) ein. Geben Sie die IP-Adressen in der Gruppe "Gemeinsam genutzte Adressen" (1 privat) von Primär- und allen Backup-Systemen ein. In diesem Beispiel lautet die Adresse 10.10.10.1. Geben Sie die IP-Adressen in der Gruppe "Gemeinsam genutzte Adressen" (2 öffentliche Adressen) von Primär- und allen Backup-Systemen ein. In diesem Beispiel lautet die Adresse 63.67.72.155.
2. Wechseln Sie in allen Einheiten zurück zu den Fenstern **Konfiguration > System > IP Routing > Redundanz**, und aktivieren Sie **Enable VRRP**. **Hinweis:** Wenn Sie zuvor Load Balancing zwischen den beiden VPN-Concentrators konfiguriert haben und VRRP für diese konfiguriert haben, achten Sie darauf, dass Sie die Konfiguration des IP-Adresspools übernehmen. Wenn Sie denselben IP-Pool wie zuvor verwenden, müssen Sie ihn ändern. Dies ist erforderlich, da der Datenverkehr von einem IP-Pool in einem Lastenausgleichsszenario nur an einen der VPN-Konzentratoren geleitet wird.

Synchronisieren der Konfigurationen

Dieses Verfahren zeigt, wie die Konfiguration von Primär zu Sekundär synchronisiert wird, indem entweder Load Balancing durchgeführt wird oder von Primär zu Sekundär bei VRRP.

1. Wählen Sie unter Primär die Option **Administration > File Management** aus, und klicken Sie in der Reihe CONFIG auf **View (Ansicht)**.

Administration | File Management Tuesday, 01 June 2004 15:09:20
Refresh

This screen lets you manage files on the VPN 3000 Concentrator. Select a file from the list and click the appropriate **Action**, or choose an action from the list below.

- [Swap Config File](#) -- swap the backup and boot configuration files.
- [TFTP Transfer](#) -- transfer files via TFTP.
- [File Upload](#) -- send a file via HTTP.
- [XML Export](#) -- export the configuration to an XML file.

Total: 12336KB, Used: 208KB, Free: 12128KB

| Filename | Size (bytes) | Date/Time | Actions |
|-------------|--------------|---------------------|------------------------|
| CONFIG.BAK | 35500 | 04/23/2004 13:49:24 | [View Delete Copy] |
| CONFIG | 33920 | 05/27/2004 19:22:46 | [View Delete Copy] |
| SAVELOG.TXT | 8018 | 05/27/2004 19:21:32 | [View Delete Copy] |

- Wenn der Webbrowser mit der Konfiguration geöffnet wird, markieren und kopieren Sie die Konfiguration (Strg-a, Strg-c).
- Fügen Sie die Konfiguration in WordPad ein.
- Wählen Sie **Bearbeiten > Ersetzen**, und geben Sie die IP-Adresse der öffentlichen Schnittstelle Primär im Feld Suchen nach ein. Geben Sie im Feld Ersetzen durch die IP-Adresse ein, die Sie für die Sekundäre oder Sicherung zuweisen möchten. Führen Sie das Gleiche für die private IP-Adresse und die externe Schnittstelle aus, wenn Sie diese konfiguriert haben.
- Speichern Sie die Datei, und geben Sie einen Namen, den Sie auswählen. Stellen Sie jedoch sicher, dass Sie das Dokument als "Textdokument" speichern (z. B. synconfig.txt). Sie *können nicht* als .doc (die Standardeinstellung) speichern und die Erweiterung später ändern. Der Grund hierfür ist, dass das Format gespeichert wird und der VPN Concentrator nur Text akzeptiert.
- Wählen Sie in der Sekundären Registerkarte **Administration > File Management > File Upload** aus.

Administration | File Management | File Upload

This section lets you upload files to your VPN 3000 Concentrator. Type in the name of the destination file on the VPN 3000 Concentrator, and the name of the file on your workstation. **Please wait for the operation to finish.**

File on the VPN 3000 Concentrator

Local File


- Geben Sie **config.bak** in das Feld Datei des VPN 3000 Concentrator ein, und navigieren Sie zur gespeicherten Datei auf Ihrem PC (synconfig.txt). Klicken Sie anschließend auf **Hochladen**. Der VPN-Concentrator lädt diesen hoch und ändert die Datei synconfig.txt automatisch in config.bak.

8. Wählen Sie **Administration > File Management > Swap Configuration Files** und klicken Sie auf **OK**, damit der VPN Concentrator mit der hochgeladenen Konfigurationsdatei bootet.


Administration | File Management | Swap Configuration Files

Every time the active configuration is saved, a backup is made of the config file. By clicking OK, you can swap the backup config file with the boot config file. To reload the boot configuration, you must then reboot the device. **You will be sent to the System Reboot screen after the config files have been swapped.**

9. Wenn Sie zum Fenster Systemneustart umgeleitet wurden, lassen Sie die Standardeinstellungen unverändert, und klicken Sie auf **Übernehmen**.

Administration | System Reboot Save Needed 

This section presents reboot options.

 If you reboot, the browser may appear to hang as the device is rebooted.

Action

- Reboot
- Shutdown without automatic reboot
- Cancel a scheduled reboot/shutdown

Configuration

- Save the active configuration at time of reboot
- Reboot without saving the active configuration
- Reboot ignoring the configuration file

When to Reboot/Shutdown

- Now
- Delayed by minutes
- At time (24 hour clock)
- Wait for sessions to terminate (don't allow new sessions)

Nach der Aktivierung hat sie dieselbe Konfiguration wie die primäre Adresse, mit Ausnahme der zuvor geänderten Adressen. **Hinweis:** Ändern Sie im Fenster Load Balancing or Redundancy (VRRP) die Parameter. Wählen Sie **Konfiguration > System > IP-Routing > Redundanz** aus.

Configuration | System | IP Routing | Redundancy

Configure the Virtual Router Redundancy Protocol (VRRP) for your system. **All interfaces that you want to configure VRRP on should already be configured.** If you later configure an additional interface, you need to revisit this screen.

Enable VRRP Check to enable VRRP.
 Group ID Enter the Group ID for this set of redundant routers.
 Group Password Enter the shared group password, or leave blank for no password.
 Role Select the Role for this system within the group.
 Advertisement Interval Enter the Advertisement interval (seconds).

Group Shared Addresses

1 (Private)
 2 (Public)
 3 (External)

Hinweis: Sie können auch **Configuration > System > Load Balancing** auswählen.

Configuration | System | Load Balancing

Configure Load Balancing. All devices in the cluster must share an identical **Cluster Configuration**. **Note: the public and private filters need to have the VCA In and VCA Out filter rules added. These filter rules may need to be modified if the VPN Virtual Cluster UDP Port is modified.**

Cluster Configuration

VPN Virtual Cluster IP Address Enter the cluster's virtual IP address.
 VPN Virtual Cluster UDP Port Enter the cluster's UDP port.
 Encryption Check to enable IPsec encryption between cluster devices.
 IPsec Shared Secret Enter the IPsec Shared secret in the cluster.
 Verify Shared Secret Re-enter the IPsec Shared secret in the cluster.

Device Configuration

Load Balancing Enable Check to enable load balancing for this device.
 Priority Enter the priority of this device. The range is from 1 to 10.
 NAT Assigned IP Address Enter the IP address that this device's IP address is translated to by NAT. Enter 0.0.0.0 if NAT is not being used, or the device is not behind a firewall using NAT.

Zugehörige Informationen

- [Support-Seite für Cisco VPN Concentrator der Serie 3000](#)
- [IPsec-Aushandlung/IKE-Protokolle](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)