

DHCP Relay Feature on the VPN 3000 Concentrator Configuration Example

Document ID: 26581

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how to configure the Dynamic Host Configuration Protocol (DHCP) relay feature introduced in Cisco VPN 3000 Concentrator version 3.6. With this feature enabled, a VPN Concentrator can relay the DHCP message between the DHCP client on the side of its public or external interface and the DHCP server behind its private interface.

This example shows how to apply the DHCP Relay feature in a wireless LAN (WLAN) and VPN environment. The wireless client first associates with a wireless Access Point (AP) located in front of a VPN Concentrator and gets an IP address via DHCP. Then the wireless client can launch a VPN connection to the VPN Concentrator to secure its access to internal network resources; see [Configuring Automatic VPN Initiation on Cisco VPN Client in a Wireless LAN Environment](#) for details. The client gets a private IP address during the Internet Key Exchange (IKE) negotiation via DHCP. Using the DHCP Relay feature saves the cost of maintaining a separate DHCP server at the public side of the VPN Concentrator to allocate IP addresses for the wireless clients when they associate with the wireless AP.

Note: One possible misleading use of the DHCP feature is that Cisco VPN Concentrator can support being a DHCP relay agent. The Cisco VPN Concentrator cannot act as a DHCP relay agent. It can only act as a pass through device. The Cisco VPN Concentrator can be configured to use a DHCP server in which it can proxy arp on behalf of the VPN Clients for an IP address assignment.

Prerequisites

Requirements

Before attempting this configuration, ensure that you meet these requirements:

- Cisco VPN Client administration
- Cisco VPN Concentrator administration

Components Used

The information in this document is based on these software and hardware versions:

- Cisco VPN 3000 Concentrator with version 3.6
- Cisco Aironet 340 AP
- Cisco VPN Client version 3.6
- CNR is used as the DHCP server

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.

Conventions

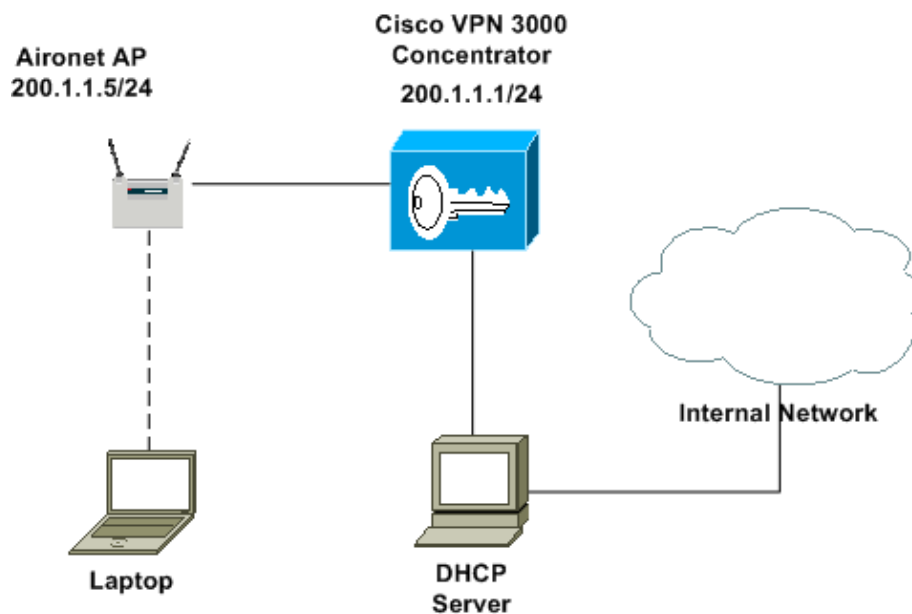
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses the network setup shown in the diagram below.



The IP address of the DHCP server is 10.1.1.253. On the DHCP server, a scope with IP address ranging from 200.1.1.50 to 200.1.1.250 is created from the Wireless clients.

Configurations

Use this procedure to configure a VPN Concentrator for DHCP relay:

1. From the VPN Concentrator console, select **Configuration > System > IP Routing > DHCP Relay**. Select the **Enabled** check box to activate DHCP relay, and enter the forwarding IP address and subnet mask.

In this example, the DHCP message sent from the DHCP client is relayed to the DHCP server at 10.1.1.253.

Configuration | System | IP Routing | DHCP Relay

Configure DHCP Relay (Dynamic Host Configuration Protocol) parameters.

To enable DHCP Relay, you must also assign proper rules to filters in the **Configuration | Policy Management | Traffic Management | Filters** screen.

Enabled Check to enable DHCP Relay.

DHCP Info Transmission Broadcast to all interfaces.

Forward to Enter the network/host address.

Enter the subnet mask.

2. From the VPN Concentrator console, select **Configuration > Policy Management > Traffic Management > Assign Rules to Filter**. In the resulting screen (shown below), move the **DHCP In** and **DHCP Out** rules from Available Rules to Current Rules in Filter.

Configuration | Policy Management | Traffic Management | Assign Rules to Filter

Save

Add, remove, prioritize, and configure rules that apply to a filter.

Filter Name: Public (Default)

Select an **Available Rule** and click **Add** to apply it to this filter.
 Select a **Current Rule in Filter** and click **Remove**, **Move Up**, **Move Down**, or **Assign SA to Rule** as appropriate.
 Select an **Available Rule**, then select a **Current Rule in Filter**, and click **Insert Above** to add the available rule above the current rule.

Current Rules in Filter	Actions	Available Rules
DHCP In (forward/in)	<< Add	RIP In (forward/in)
GRE Out (forward/out)	<< Insert Above	RIP Out (forward/out)
IKE Out (forward/out)	Remove >>	OSPF In (forward/in)
PPTP Out (forward/out)	Move Up	OSPF Out (forward/out)
L2TP Out (forward/out)	Move Down	Any In (forward/in)
ICMP Out (forward/out)	Assign SA to Rule	Any Out (forward/out)
VRRP Out (forward/out)	Done	Incoming HTTPS In (forward/in)
Incoming HTTP Out (forward/out)		Incoming HTTPS Out (forward/out)
Outgoing HTTP Out (forward/out)		LDAP In (forward/in)
VCA Out (forward/out)		LDAP Out (forward/out)
NAT-T Out (forward/out)		Telnet/SSL In (forward/in)
DHCP Out (forward/out)		Telnet/SSL Out (forward/out)

Verify

This section provides information you can use to confirm your configuration is working properly.

An administrator can enable the DHCP and DHCPDBG event classes with severity level 1–9 to verify and troubleshoot the DHCP Relay feature. This event log demonstrates how DHCP messages from the client are relayed by the VPN Concentrator to the DHCP server.

The event log shows that the VPN 3000 Concentrator relays the DHCP Discover messages sent from the wireless client to the DHCP server, and places its public interface IP address in the giaddr (gateway IP address) field. The DHCP server then sends the IP address 200.1.1.52 back to the wireless client.

```
1 01/01/1999 00:05:49.300 SEV=9 DHCPDBG/22 RPT=7
Sockets got data for DHCP sock_rcv_cb: sd 1, buf 0x1e3e000

2 01/01/1999 00:05:49.300 SEV=6 DHCP/77 RPT=7
Relaying DHCP Packet: DHCP Discover

3 01/01/1999 00:05:49.300 SEV=6 DHCP/79 RPT=7
TX:DHCPDISCOVER
ciaddr:0.0.0.0 yiaddr:0.0.0.0 siaddr:0.0.0.0
giaddr:200.1.1.1 chaddr:00.09.E8.62.A3.24

6 01/01/1999 00:05:49.310 SEV=9 DHCPDBG/22 RPT=8
Sockets got data for DHCP sock_rcv_cb: sd 1, buf 0x1d32000

7 01/01/1999 00:05:49.310 SEV=6 DHCP/77 RPT=8
Relaying DHCP Packet: DHCP Offer

8 01/01/1999 00:05:49.310 SEV=6 DHCP/79 RPT=8
TX:DHCPPOFFER
ciaddr:0.0.0.0 yiaddr:200.1.1.52 siaddr:0.0.0.0
giaddr:200.1.1.1 chaddr:00.09.E8.62.A3.24

11 01/01/1999 00:05:49.310 SEV=9 DHCPDBG/22 RPT=9
Sockets got data for DHCP sock_rcv_cb: sd 1, buf 0x1e3e800

12 01/01/1999 00:05:49.310 SEV=6 DHCP/77 RPT=9
Relaying DHCP Packet: DHCP Request

13 01/01/1999 00:05:49.310 SEV=6 DHCP/79 RPT=9
TX:DHCPREQUEST
ciaddr:0.0.0.0 yiaddr:0.0.0.0 siaddr:0.0.0.0
giaddr:200.1.1.1 chaddr:00.09.E8.62.A3.24

16 01/01/1999 00:05:49.340 SEV=9 DHCPDBG/22 RPT=10
Sockets got data for DHCP sock_rcv_cb: sd 1, buf 0x1d32800

17 01/01/1999 00:05:49.340 SEV=6 DHCP/77 RPT=10
Relaying DHCP Packet: DHCP Ack

18 01/01/1999 00:05:49.340 SEV=6 DHCP/79 RPT=10
TX:DHCPACK
ciaddr:0.0.0.0 yiaddr:200.1.1.52 siaddr:0.0.0.0
giaddr:200.1.1.1 chaddr:00.09.E8.62.A3.24

21 01/01/1999 00:05:51.710 SEV=9 DHCPDBG/16 RPT=22
DHCP task: Periodic timer expired (ticks 22)

22 01/01/1999 00:05:51.710 SEV=9 DHCPDBG/29 RPT=22
DHCP poll timeouts routine entered
```

```
23 01/01/1999 00:05:51.710 SEV=9 DHCPDBG/30 RPT=22
DHCP poll stats: callbacks 0, active CBs 0, total CBs 0

24 01/01/1999 00:06:06.710 SEV=9 DHCPDBG/16 RPT=23
DHCP task: Periodic timer expired (ticks 23)

25 01/01/1999 00:06:06.710 SEV=9 DHCPDBG/29 RPT=23
DHCP poll timeouts routine entered

26 01/01/1999 00:06:06.710 SEV=9 DHCPDBG/30 RPT=23
DHCP poll stats: callbacks 0, active CBs 0, total CBs 0
```

Troubleshoot

An administrator can enable the DHCP and DHCPDBG event classes with severity level 1–9 to verify and troubleshoot the DHCP Relay feature.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [Configuring Automatic VPN Initiation on Cisco VPN Client in a Wireless LAN Environment](#)
- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3000 Series Client Support Page](#)
- [IPSec Support Page](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 24, 2007

Document ID: 26581
