

Options for the IPsec Fragmentation Policy in the VPN 3000 Concentrator

Document ID: 69379

Introduction

Prerequisites

Requirements

Components Used

Conventions

Background Information

IPsec Fragmentation Options

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document discusses all the available IPsec fragmentation options in a Cisco VPN 3000 Concentrator. The IPsec fragmentation policy specifies how to treat packets that exceed the MTU setting when tunneling traffic through the public interface.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- IP Fragmentation and Reassembly
- Basic knowledge of the Cisco VPN 3000 Concentrator

Components Used

The information in this document is based on the Cisco VPN 3000 Series Concentrator with version 4.7.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The IPsec Fragmentation Policy feature provides a way to handle cases where a router or Network Address Translation (NAT) device between the VPN Concentrator and the VPN Client rejects or drops IP fragments. For example, a client wants to use FTP **get** from an FTP server behind a VPN Concentrator. The FTP server transmits packets that when encapsulated, exceed the MTU size of the VPN Concentrator on the public interface.

IPsec Fragmentation Options

The fragmentation policy you set here applies to all traffic that travels out of the VPN Concentrator public interface to clients that run VPN Client software version 3.6 or later. The second and third options described here can affect performance. VPN Clients that run software versions earlier than 3.6 or Layer 2 Tunnel Protocol (L2TP) over IPsec clients can use only the "Do not fragment prior to IPsec encapsulation; fragment prior to interface transmission" option. The setting you configure applies to VPN Client software version 3.6 and later. The VPN Concentrator ignores the setting for VPN Clients that run software versions earlier than 3.6 and protocols other than IPsec. For these clients, the "Do not fragment prior to IPsec encapsulation; fragment prior to interface transmission" option applies.

Select **Configuration > Interface > Ethernet > General** to see the various options for IPsec fragmentation under **Public Interface IPsec Fragmentation Policy**.

The screenshot shows the configuration page for Ethernet 1 (Private). The 'General Parameters' section is active, and the 'Public Interface IPsec Fragmentation Policy' is highlighted with a red box. The policy options are:

Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	1.1.1.3	
	Subnet Mask	255.255.254.0	
	Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address	00.90.A4.00.00.A2	The MAC address for this interface.
	Filter	—None—	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500)
	Public Interface IPsec Fragmentation Policy		<input checked="" type="radio"/> Do not fragment prior to IPsec encapsulation; fragment prior to interface transmission <input type="radio"/> Fragment prior to IPsec encapsulation with Path MTU Discovery (ICMP) <input type="radio"/> Fragment prior to IPsec encapsulation without Path MTU Discovery (Clear DF bit)

Buttons: Apply, Cancel

These options determine how the VPN 3000 Concentrator processes these packets:

- Do not fragment prior to IPsec encapsulation; fragment prior to interface transmission** The VPN Concentrator encapsulates all tunneled packets. After encapsulation, the VPN Concentrator fragments packets that exceed the MTU setting before transmitting them through the public interface. This is the default policy for the VPN Concentrator. This option works for situations where fragmented packets are allowed through the tunnel without hindrance. For the FTP example, large packets are encapsulated and then fragmented at the IP layer. Intermediate devices can drop fragments or just out-of-order fragments. Load-balancing devices can introduce out-of-order fragments.
- Fragment prior to IPsec encapsulation with Path MTU Discovery (ICMP)** The VPN Concentrator fragments tunneled packets that exceed the MTU setting during encapsulation. For this

option, the VPN Concentrator drops large packets that have the Do not Fragment (DF) bit set, and sends the "Packet needs to be fragmented but DF is set" ICMP message to the packet's initiator. The ICMP message includes the maximum MTU size allowed. Path MTU Discovery means that an intermediate device (in this case the VPN Concentrator) informs the source of the MTU permitted to reach the destination.

If a large packet does not have the DF bit set, the VPN Concentrator fragments prior to encapsulating. This creates two independent non-fragmented IP packets and transmits them out the public interface. This is the default policy for the VPN 3002 Hardware Client.

- **Fragment prior to IPsec encapsulation without Path MTU Discovery (Clear DF bit)** The VPN Concentrator fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the VPN Concentrator clears the DF bit, fragments the packets, and then encapsulates them. This action creates two independent non-fragmented IP packets leaving the public interface and successfully transmits these packets to the peer site by turning the fragments into complete packets to be reassembled at the peer site. In this example, the VPN Concentrator overrides the MTU and allows fragmentation by clearing the DF bit.

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

- [VPN 3000 Series Concentrator, Release 4.7](#)
- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [IPsec Negotiation/IKE Protocols](#)
- [IP Fragmentation and PMTUD](#)
- [IP Fragmentation and MTU Path Discovery with VPN](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

Updated: Jun 01, 2006

Document ID: 69379