Configuring NAT Transparent Mode for IPSec on the VPN 3000 Concentrator

Document ID: 5753

Contents

Introduction

Network Address Translation (NAT) was developed to address the problem of Internet Protocol Version 4 (IPV4) running out of address space. Today, home users and small office networks use NAT as an alternative to buying registered addresses. Corporations implement NAT alone or with a firewall to protect their internal resources.

Many−to−one, the most commonly implemented NAT solution, maps several private addresses to one single routable (public) address; this is also known as Port Address Translation (PAT). The association is implemented at the port level. The PAT solution creates a problem for IPSec traffic that does not use any ports.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco VPN 3000 Concentrator
- Cisco VPN 3000 Client Release 2.1.3 and later
- Cisco VPN 3000 Client and Concentrator Release 3.6.1 and later for NAT−T

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.

Encapsulating Security Payload

Protocol 50 (Encapsulating Security Payload [ESP]) handles the encrypted/encapsulated packets of IPSec. Most PAT devices do not work with ESP since they have been programmed to work only with Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). In addition, PAT devices are unable to map multiple security parameter indexes (SPIs). The NAT transparent mode in the VPN 3000 Client solves this problem by encapsulating ESP within UDP and sending it to a negotiated port. The name of the attribute to activate on the VPN 3000 Concentrator is IPSec through NAT.

A new protocol NAT−T which is an IETF standard (still in the DRAFT stage as of the writing this article) also encapsulates IPSec packets in UDP, but it works on port 4500. That port is not configurable.

How Does NAT Transparent Mode Work?

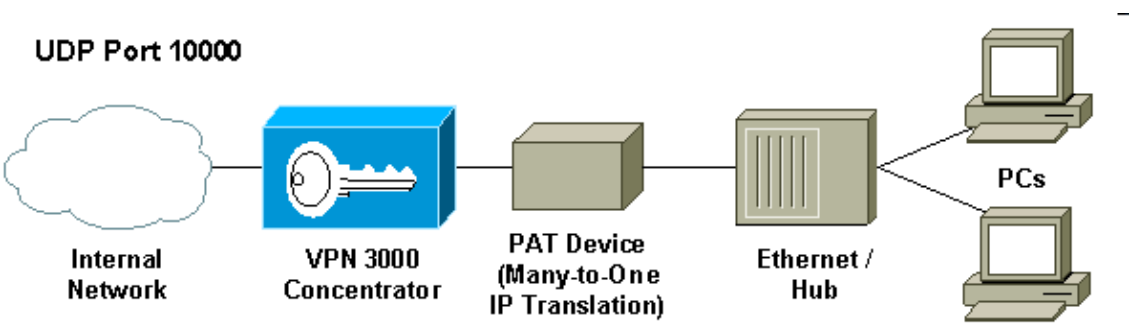
Activating IPSec transparent mode on the VPN Concentrator creates non−visible filter rules and applies them to the public filter. The configured port number is then passed to the VPN Client transparently when the VPN Client connects. On the inbound side, UDP inbound traffic from that port passes directly to IPSec for processing. Traffic is decrypted and decapsulated, and then routed normally. On the outbound side, IPSec encrypts, encapsulates and then applies a UDP header (if so configured). The runtime filter rules are deactivated and deleted from the appropriate filter under three conditions: when IPSec over UDP is disabled for a group, when the group is deleted, or when the last active IPSec over UDP SA on that port is deleted. Keepalives are sent to prevent a NAT device from closing the port mapping due to inactivity.

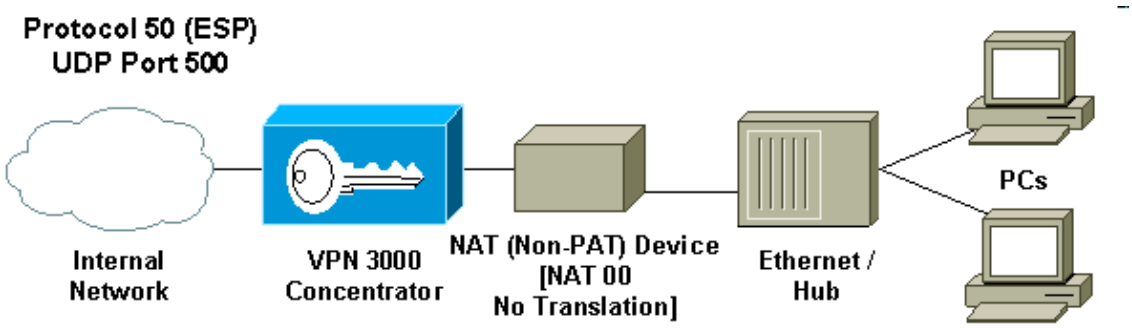
If IPSec over NAT−T is enabled on the VPN Concentrator, then the VPN Concentrator/VPN Client uses NAT−T mode of UDP encapsulation. NAT−T works by auto−detecting any NAT device between the VPN Client and VPN Concentrator during IKE negotiation. You must ensure that UDP port 4500 is not blocked between the VPN Concentrator/VPN Client for NAT−T to work. Also, if you are using a previous IPSec/UDP configuration that is already using that port, you must reconfigure that earlier IPSec/UDP configuration to use a different UDP port. Since NAT−T is an IETF draft, it helps when using multivendor devices if the other vendor implements this standard.

NAT−T works with both VPN Client connections and LAN−to−LAN connections unlike IPSec over UDP/TCP. Also, Cisco IOS® routers and the PIX firewall devices support NAT−T.

You do not need IPSec over UDP to be enabled to have NAT−T working.

Configure NAT Transparent Mode





Use the following procedure to configure NAT transparent mode on the VPN Concentrator.

Note: IPSec over UDP is configured on a per group basis, while IPSec over TCP/ NAT−T is configured globally.

1. Configure IPSec over UDP:
    a. On the VPN Concentrator, select **Configuration > User Management > Groups**.
    b. To add a group, select **Add**. To modify an existing group, select it and click **Modify**.
    c. Click the IPSec tab, check **IPSec through NAT** and configure the **IPSec through NAT UDP Port**. The default port for IPSec through NAT is 10000 (source and destination), but this setting may be changed.
2. Configure IPSec over NAT−T and/or IPSec over TCP:
    a. On the VPN Concentrator select **Configuration** > **System** > **Tunneling Protocols** > **IPSec** > **NAT Transparency**.
    b. Check the **IPSec over NAT−T and/or TCP** check box.

If everything is enabled, use this precedence:

1. IPSec over TCP.
2. IPSec over NAT−T.
3. IPSec over UDP.

Cisco VPN Client Configuration to Use NAT Transparency

To use IPSec over UDP or NAT−T you need to enable IPSec over UDP on Cisco VPN Client 3.6 and later. The UDP port is assigned by the VPN Concentrator in case of IPSec over UDP, while for NAT−T it is fixed to UDP port 4500.

To use IPSec over TCP, you need to enable it on the VPN Client and configure the port that should be used manually.

Related Information

- **Cisco VPN 3000 Series Concentrator Support Page**
- **Cisco VPN 3000 Series Client Support Page**
- **IPSec Support Page**
- **Technical Support − Cisco Systems**

Updated: Jan 14, 2008 Document ID: 5753