Configuración del modo transparente de NAT para IPSec en el concentrador VPN 3000

Contenido

Introducción

La Traducción de Dirección de Red (NAT) fue desarrollada para abordar el problema del agotamiento del espacio de direcciones para Internet Protocol Version 4 (IPV4). Hoy, en las redes de usuarios domésticos y oficinas pequeñas se utiliza NAT como alternativa a la compra de direcciones registradas. Las sociedades implementan NAT sola o con un firewall para proteger sus recursos internos.

La solución NAT de varios a uno, la más implementada, asigna varias direcciones privadas a una única dirección enrutable (pública); esto también se conoce como Traducción de direcciones de puerto (PAT). La asociación se implementa a nivel de puerto. La solución PAT crea un problema para el tráfico IPSec que no utiliza ningún puerto.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Concentrador Cisco VPN 3000

- Cisco VPN 3000 Client Release 2.1.3 y posterior
- Cisco VPN 3000 Client and Concentrator Release 3.6.1 y posterior para NAT-T

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Carga útil de seguridad encapsulada

El protocolo 50 (Carga de seguridad de encapsulación [ESP]) gestiona los paquetes cifrados/encapsulados de IPSec. La mayoría de los dispositivos PAT no funcionan con ESP, ya que se han programado para funcionar únicamente con el protocolo de control de transmisión (TCP), el protocolo de datagramas de usuario (UDP) y el protocolo de mensajes de control de Internet (ICMP). Además, los dispositivos PAT no pueden asignar varios índices de parámetros de seguridad (SPI). El modo transparente NAT en el cliente VPN 3000 resuelve este problema encapsulando ESP dentro de UDP y enviándolo a un puerto negociado. El nombre del atributo que se activará en el concentrador VPN 3000 es IPSec a través de NAT.

Un nuevo protocolo NAT-T que es un estándar IETF (todavía en la etapa DRAFT al escribir este artículo) también encapsula paquetes IPSec en UDP, pero funciona en el puerto 4500. Ese puerto no es configurable.

¿Cómo funciona el modo transparente de NAT?

Al activar el modo transparente de IPSec en el concentrador VPN, se crean reglas de filtro no visibles y se aplican al filtro público. El número de puerto configurado se pasa al cliente VPN de forma transparente cuando el cliente VPN se conecta. En el lado entrante, el tráfico entrante UDP de ese puerto pasa directamente a IPSec para su procesamiento. El tráfico se descifra y desencapsula y, a continuación, se enruta normalmente. En el lado saliente, IPSec cifra, encapsula y, a continuación, aplica un encabezado UDP (si está configurado). Las reglas de filtrado en tiempo de ejecución se desactivan y eliminan del filtro adecuado en tres condiciones: cuando IPSec sobre UDP está desactivado para un grupo, cuando se elimina el grupo o cuando se elimina el último IPSec activo sobre UDP SA en ese puerto. Las señales de mantenimiento se envían para evitar que un dispositivo NAT cierre la asignación de puertos debido a la inactividad.

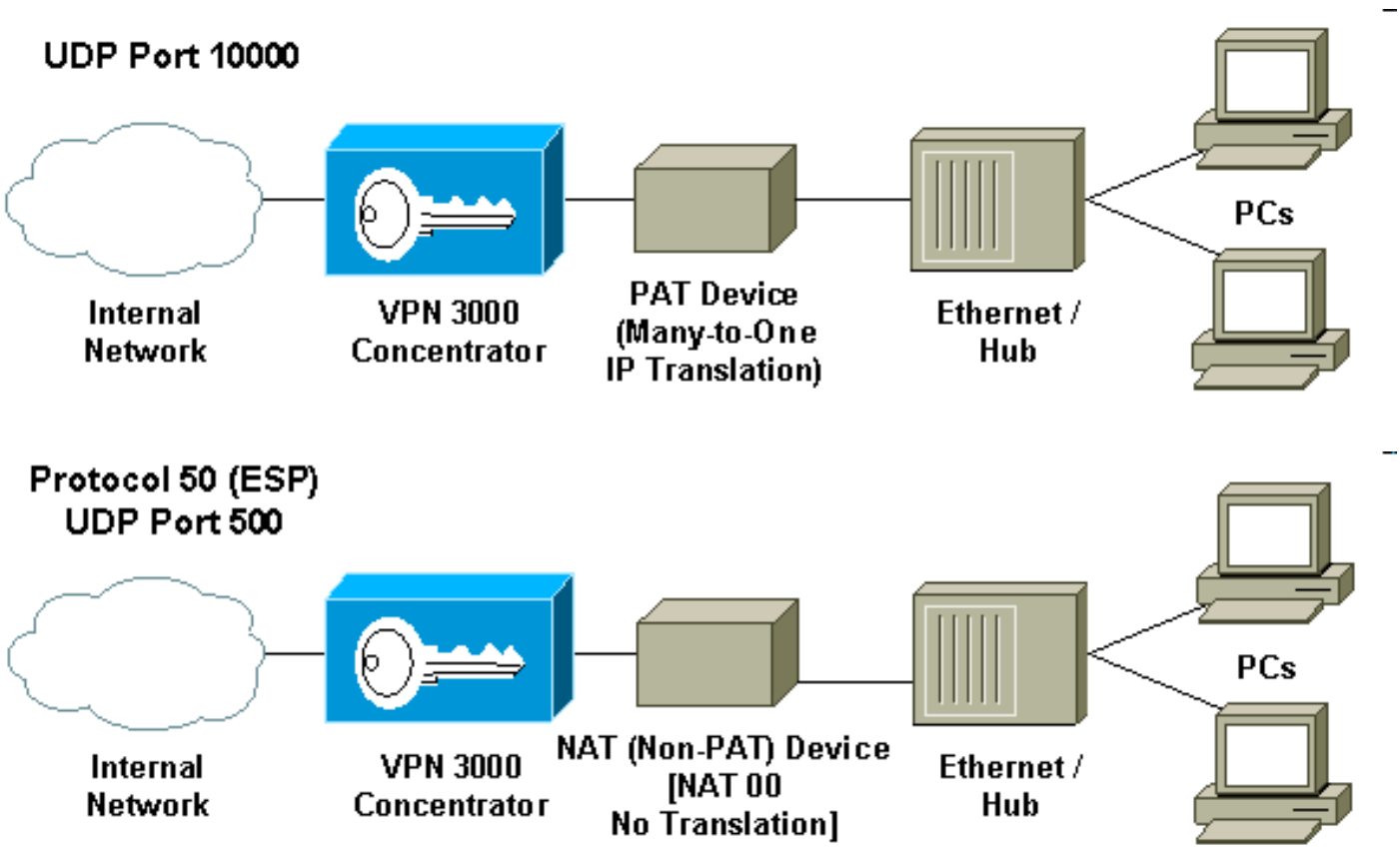
Si IPSec sobre NAT-T está habilitado en el concentrador VPN, el concentrador VPN/cliente VPN utiliza el modo NAT-T de encapsulación UDP. NAT-T funciona mediante la detección automática de cualquier dispositivo NAT entre el cliente VPN y el concentrador VPN durante la negociación IKE. Debe asegurarse de que el puerto UDP 4500 no esté bloqueado entre el VPN Concentrator/VPN Client para que NAT-T funcione. Además, si utiliza una configuración

IPSec/UDP anterior que ya esté utilizando ese puerto, debe volver a configurar esa configuración IPSec/UDP anterior para utilizar un puerto UDP diferente. Dado que NAT-T es un borrador de IETF, ayuda al utilizar dispositivos de varios proveedores si el otro proveedor implementa este estándar.

NAT-T funciona con las conexiones VPN Client y las conexiones de LAN a LAN a diferencia de IPSec sobre UDP/TCP. Además, los routers Cisco IOS® y los dispositivos de firewall PIX admiten NAT-T.

No necesita que IPSec sobre UDP esté habilitado para que NAT-T funcione.

Configurar el modo transparente de NAT



Utilice el siguiente procedimiento para configurar el modo transparente de NAT en el concentrador VPN.

Nota: IPSec sobre UDP se configura por grupo, mientras que IPSec sobre TCP/ NAT-T se configura globalmente.

1. Configuración de IPSec sobre UDP:

    a. En el Concentrador VPN, seleccione Configuration > User Management > Groups.

    b. Para agregar un grupo, seleccione Add. Para modificar un grupo existente, selecciónelo y haga clic en Modificar.

c. Haga clic en la ficha IPSec, verifique IPSec a través de NAT y configure IPSec a través del puerto UDP de NAT. El puerto predeterminado para IPSec a través de NAT es 10000 (origen y destino), pero esta configuración se puede cambiar.

2. Configuración de IPSec sobre NAT-T o IPSec sobre TCP:

   a. En el concentrador VPN, seleccione Configuration > System > Tunneling Protocols > IPSec > NAT Transparency.

   b. Marque la casilla de verificación IPSec sobre NAT-T y/o TCP.

Si todo está habilitado, utilice esta prioridad:

1. IPSec sobre TCP.
2. IPSec sobre NAT-T.
3. IPSec sobre UDP.

Configuración de Cisco VPN Client para Utilizar la Transparencia NAT

Para utilizar IPSec sobre UDP o NAT-T, debe habilitar IPSec sobre UDP en Cisco VPN Client 3.6 y posterior. El puerto UDP es asignado por el concentrador VPN en el caso de IPSec sobre UDP, mientras que para NAT-T es fijo al puerto UDP 4500.

Para utilizar IPSec sobre TCP, debe activarlo en el cliente VPN y configurar el puerto que debe utilizarse manualmente.

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).