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.

Mucho-a-uno, la solución lo más comúnmente posible implementada NAT, asocia a varias direcciones privadas a un solo direccionamiento del routable (público); esto también se conoce como Port Address Translation (PAT). La asociación se implementa en el nivel del puerto. La solución de la PALMADITA crea un problema para el tráfico IPSec que no utiliza ninguna puertos.

prerrequisitos

Requisitos

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
- Versión de Cliente Cisco VPN 3000 2.1.3 y posterior

- Cliente Cisco VPN 3000 y concentrador versión 3.6.1 y posterior para el 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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Carga útil de seguridad encapsulada

El protocolo 50 (Encapsulating Security Payload [ESP]) dirige cifrado/los paquetes encapsulados de IPSec. La mayoría de los dispositivos PAT no funcionan con el ESP puesto que se han programado para trabajar solamente con el Transmission Control Protocol (TCP), el User Datagram Protocol (UDP), y el Internet Control Message Protocol (ICMP). Además, los dispositivos PAT no pueden asociar los índices múltiples del parámetro de seguridad (SPI). El modo transparente NAT en el VPN 3000 Client soluciona este problema encapsulando el ESP dentro del UDP y enviándolo a un puerto negociado. El nombre del atributo a activar en el concentrador VPN 3000 es IPSec con el NAT.

Un nuevo protocolo NAT-T que es una norma de IETF (aún en la etapa del PROYECTO a partir de la escritura este artículo) también encapsula los paquetes IPsec en el UDP, pero lo trabaja en el puerto 4500. Ese puerto no es configurable.

¿Cómo funciona el modo transparente de NAT?

El modo transparente del IPSec que activa en el concentrador VPN crea las reglas de filtro no visible y las aplica al Filtro público. El número del puerto configurado entonces se pasa al cliente VPN transparente cuando el cliente VPN conecta. En el costado entrante, el tráfico entrante UDP de ese puerto pasa directamente al IPSec para procesar. El tráfico es desencriptado y decapsulated, y entonces ruteado normalmente. En el lado de salida, el IPSec cifra, encapsula y después aplica un encabezado UDP (si está configurado tan). Las reglas para filtros de tiempo de ejecución se desactivan y se borran del filtro apropiado bajo tres condiciones: cuando el IPSec sobre el UDP se inhabilita para un grupo, cuando borran al grupo, o cuando el IPSec activo más reciente sobre UDP SA en ese puerto se borra. El Keepalives se envía para evitar que un dispositivo NAT cierre la correlación de puertos debido a la inactividad.

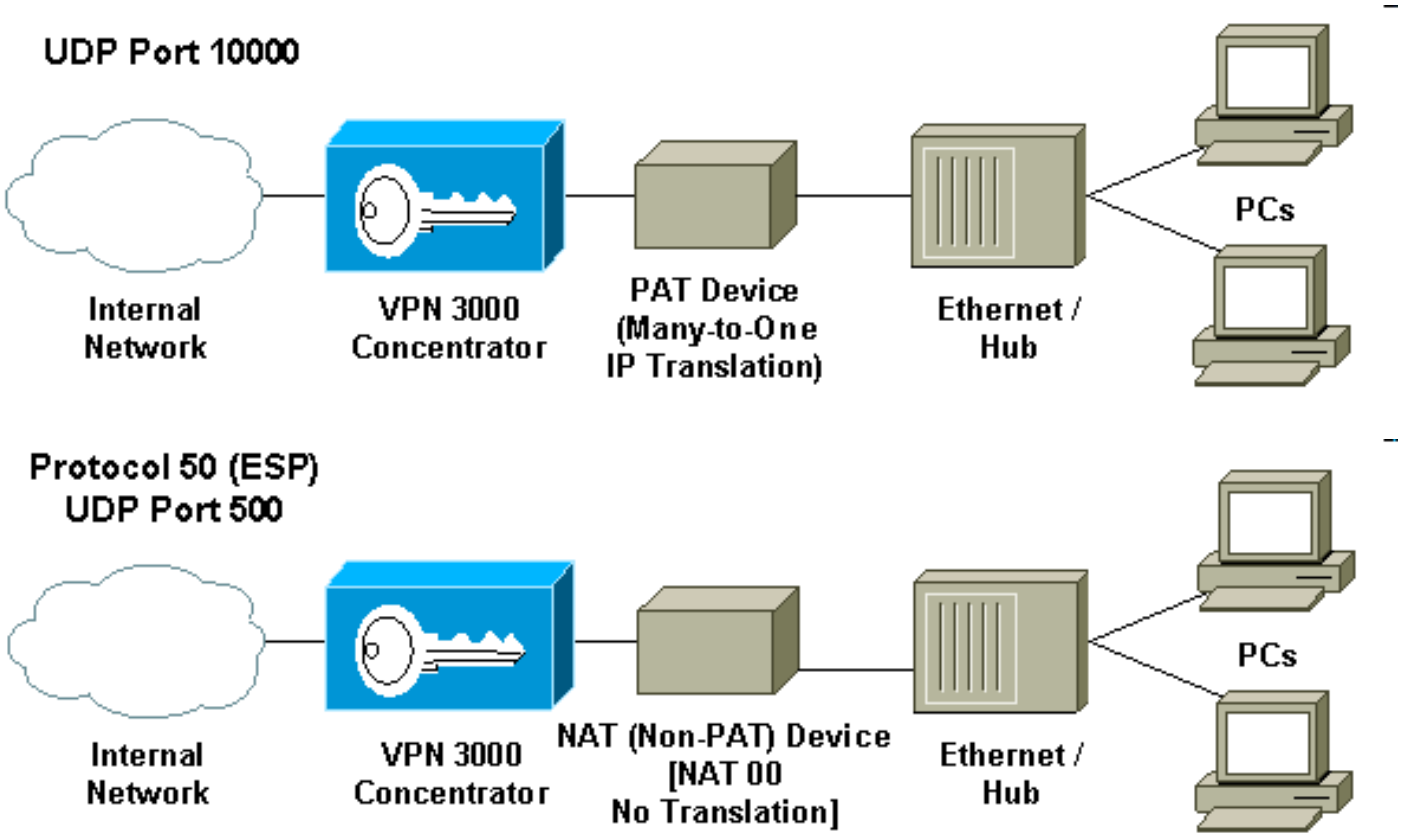
Si el IPSec sobre el NAT-T se habilita en el concentrador VPN, después el cliente VPN Concentrator/VPN utiliza al modo de encapsulación UDP NAT-T. El NAT-T trabaja auto-detectando cualquier dispositivo NAT entre el cliente VPN y el concentrador VPN durante la negociación IKE. Usted debe asegurarse de que el puerto 4500 UDP no esté bloqueado entre el cliente VPN Concentrator/VPN para que el NAT-T trabaje. También, si usted está utilizando una configuración anterior del IPSec/UDP que esté utilizando ya ese puerto, usted debe configurar de nuevo que configuración anterior del IPSec/UDP para utilizar un diverso puerto UDP. Puesto que el NAT-T es un borrador IETF, ayuda al usar los dispositivos de varios proveedores si el otro vendedor implementa este estándar.

El NAT-T trabaja con las conexiones de cliente VPN y las conexiones de LAN a LAN a diferencia

de IPSec sobre el UDP/TCP. También, el Routers de Cisco IOS® y los dispositivos del firewall PIX soportan el NAT-T.

Usted no necesita el IPSec sobre el UDP ser habilitado para tener funcionamiento NAT-T.

Modo transparente de la configuración NAT



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

Nota: El IPSec sobre el UDP se configura en a por la base del grupo, mientras que el IPSec sobre TCP/NAT-T se configura global.

1. IPSec de la configuración sobre el UDP:En el concentrador VPN, seleccione el **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos)**.Para agregar a un grupo, selecto **agregue**. Para modificar un grupo existente, seleccionar lo y el tecleo **se modifica**.Haga clic la lengueta del IPSec, marque el **IPSec con el NAT** y configure el **IPSec a través del puerto NAT UDP**. El puerto predeterminado para el IPSec con el NAT es 10000 (fuente y destino), pero esta configuración puede ser cambiada.
2. IPSec de la configuración sobre el NAT-T y/o IPSec sobre el TCP:En el concentrador VPN seleccione el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec** > la **Transparencia NAT**.Marque el **IPSec sobre el NAT-T y/o casilla de selección TCP**.

Si se habilita todo, utilice esta precedencia:

1. IPSec sobre el TCP.
2. IPSec sobre el NAT-T.

3. IPSec sobre el UDP.

Configuración de Cliente Cisco VPN para utilizar la Transparencia NAT

Para utilizar el IPSec sobre el UDP o el NAT-T que usted necesita habilitar el IPSec sobre el UDP en el 3.6 y posteriores del Cliente Cisco VPN. El puerto UDP es asignado por el concentrador VPN en caso del IPSec sobre el UDP, mientras que para el NAT-T se repara al puerto 4500 UDP.

Para utilizar el IPSec sobre el TCP, usted necesita habilitarlo en el cliente VPN y configurar el puerto que se debe utilizar 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