Conectividad de sitio a sitio con superposición de subredes en Cisco Secure Access

Contenido

Introducción

Este documento describe la solución de subred superpuesta de Cisco Secure Access.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración de Cisco Secure Access.
- Administración de firewall/router.

Cisco recomienda que tenga:

- Acceso administrativo a Cisco Secure Access.
- Acceso administrativo al dispositivo de cabecera IPSec (firewall o router)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antes de comenzar

En este ejemplo hay dos sitios de sucursal diferentes con la misma subred IP 192.168.200.0/24, en los que están conectados a Cisco Secure Access a través de dos túneles IPSec independientes.

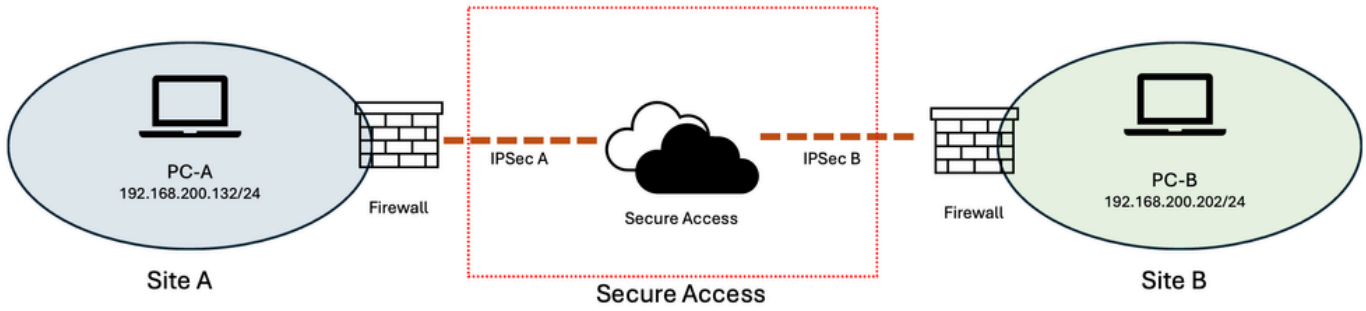

Imagen - Diagrama de red

El objetivo es que los usuarios del "Sitio A" puedan acceder a los recursos del "Sitio B" y viceversa.

Preparación y planificación

Debido a que ambos sitios utilizan la misma subred IP (`192.168.200.0/24`), el espacio de dirección superpuesto impide la comunicación directa entre los dos sitios. Para resolver este solapamiento, se asignan dos subredes virtuales que no se solapan para representar los recursos de cada sitio.

Para este ejemplo:

- Sitio A: `10.30.30.0/24`
- Sitio B: `10.40.40.0/24`
- Subred real en ambos sitios: `192.168.200.0/24`

Las subredes virtuales proporcionan espacios de direcciones únicos para cada sitio mientras que los recursos reales siguen utilizando sus direcciones `192.168.200.0/24` existentes.

Cuando un usuario del Sitio A accede a un recurso ubicado en el Sitio B, el usuario accede al recurso a través de la subred virtual del Sitio B (**`10.40.40.0/24`**) en lugar de utilizar directamente el espacio de direcciones 192.168.200.0/24 superpuesto.

Cisco Secure Access proporciona una función NAT de destino uno a uno (D-NAT) que puede traducir las direcciones virtuales a las direcciones reales correspondientes. El rango de direcciones D-NAT tiene el mismo tamaño que la subred original. En este ejemplo, tanto las redes virtuales como las reales son subredes `/24`, lo que proporciona una asignación uno a uno entre las direcciones IP virtuales y reales.

Por ejemplo:

`10.40.40.202` → `192.168.200.202`

Por lo tanto, una solicitud del Sitio A destinada a `10.40.40.202` es traducida por D-NAT a `192.168.200.202`, lo que permite que la solicitud llegue al recurso correspondiente en el Sitio B a pesar de que ambos sitios usen la misma subred IP subyacente.

Este enfoque crea de forma eficaz un espacio de direcciones virtual y no superpuesto para cada sitio, a la vez que conserva el direccionamiento IP existente de los recursos. También proporciona una relación uno a uno coherente entre las direcciones virtual y real, lo que facilita la comprensión, la gestión y la resolución de problemas de la configuración.

Configuration Steps

Debido al diseño actual y a las limitaciones de Cisco Secure Access, para lograr este escenario es necesario configurar tanto los dispositivos de cabecera detrás de los túneles IPsec como Cisco Secure Access.

El dispositivo de cabecera es el firewall o router que establece el túnel IPsec a Cisco Secure Access. Además de configurar D-NAT en Cisco Secure Access, el firewall de cabecera también

debe realizar la NAT de origen (S-NAT) para el tráfico de retorno.

Por lo tanto, la configuración consta de dos secciones:

1. Configuración de NAT de destino (D-NAT) en Cisco Secure Access para cada túnel de red por separado.
2. Configuración de NAT de origen (S-NAT) en los firewalls para garantizar que el tráfico de retorno se traduce de nuevo al espacio de direcciones virtuales.

Configuración de Cisco Secure Access

Paso 1: Desde el portal de administración de Cisco Secure Access, navegue hasta Connect > Network Connections y seleccione la pestaña Network Tunnel Groups.

Paso 2: Edite el grupo de túnel de red asociado con el túnel IPsec para el sitio que utiliza la subred superpuesta.

En este ejemplo:

- IPSec-A = Grupo de túnel de red para el sitio A
- IPSec-B = Grupo de túnel de red para el Sitio B

Paso 3: Haga clic en el menú de tres puntos junto al grupo de túnel de red requerido y seleccione Edit.

Paso 4: En el menú de la izquierda, seleccione la ficha Routing y active la Traducción de direcciones de red (NAT) si aún no está activada.

Paso 5: En Asignaciones NAT de destino, haga clic en Agregar asignaciones.

Paso 6: Utilice esta tabla para configurar las asignaciones D-NAT para cada grupo de túnel de red:

	Sitio A: túnel IPSec	Sitio B: túnel IPSec
NAT-1 de destino	Sitio → Acceso seguro CIDR original: 10.40.40.0/24	Sitio → Acceso seguro CIDR original: 10.30.30.0/24

	CIDR traducido: 192.168.200.0/24	CIDR traducido: 192.168.200.0/24
NAT-2 de destino	Sitio de Secure Access → CIDR original: 192.168.200.0/24 CIDR traducido: 10.30.30.0/24	Sitio de Secure Access → CIDR original: 192.168.200.0/24 CIDR traducido: 10.40.40.0/24
	 Configuración del Sitio A del Túnel IPsec - D-NAT	 Configuración del Sitio B del Túnel IPsec - D-NAT

Nota: Después de configurar los parámetros para cada grupo de túnel de red, haga clic en Save. Cuando aparezca la ventana de confirmación, introduzca UPDATE para confirmar el cambio. Repita el mismo procedimiento para el otro grupo de túnel de red

Configuración del firewall

La configuración del firewall es necesaria debido a una limitación actual en el manejo de subredes IP superpuestas detrás de los grupos de túnel de red.

Cuando Cisco Secure Access ejecuta D-NAT en un paquete entrante, la dirección de destino traducida se utiliza para entregar el paquete al recurso de destino. Sin embargo, la traducción inversa correspondiente no se realiza automáticamente para el tráfico de retorno en este escenario de subred superpuesta.

Como resultado, el tráfico de retorno debe ser NAT de origen manual en el firewall.

El requisito clave es que el servidor de destino vea el tráfico de retorno usando la dirección IP virtual a la que el cliente accedió originalmente, en lugar de la dirección IP real del servidor.

Ejemplo:

Suponga lo siguiente:

- Cliente del sitio A: `192.168.200.132`
- Servidor web del sitio B: `192.168.200.202`
- Subred virtual del sitio B: `10.40.40.0/24`

- Dirección virtual del servidor web: `10.40.40.202`

El cliente del sitio A accede al servidor web del sitio B mediante `https://10.40.40.202`

Cisco Secure Access ejecuta el D-NAT `10.40.40.202` → `192.168.200.202`

Luego, el paquete llega al servidor web en `192.168.200.202`.

El problema ocurre con el tráfico de retorno. Sin NAT adicional en el firewall, el servidor web genera la respuesta con Source: `192.168.200.202`

Sin embargo, el cliente inició la conexión con el Destino: `10.40.40.202`

Por lo tanto, el tráfico de retorno debe traducirse de modo que la dirección de origen presentada al cliente corresponda a la dirección virtual`192.168.200.202` → `10.40.40.202`

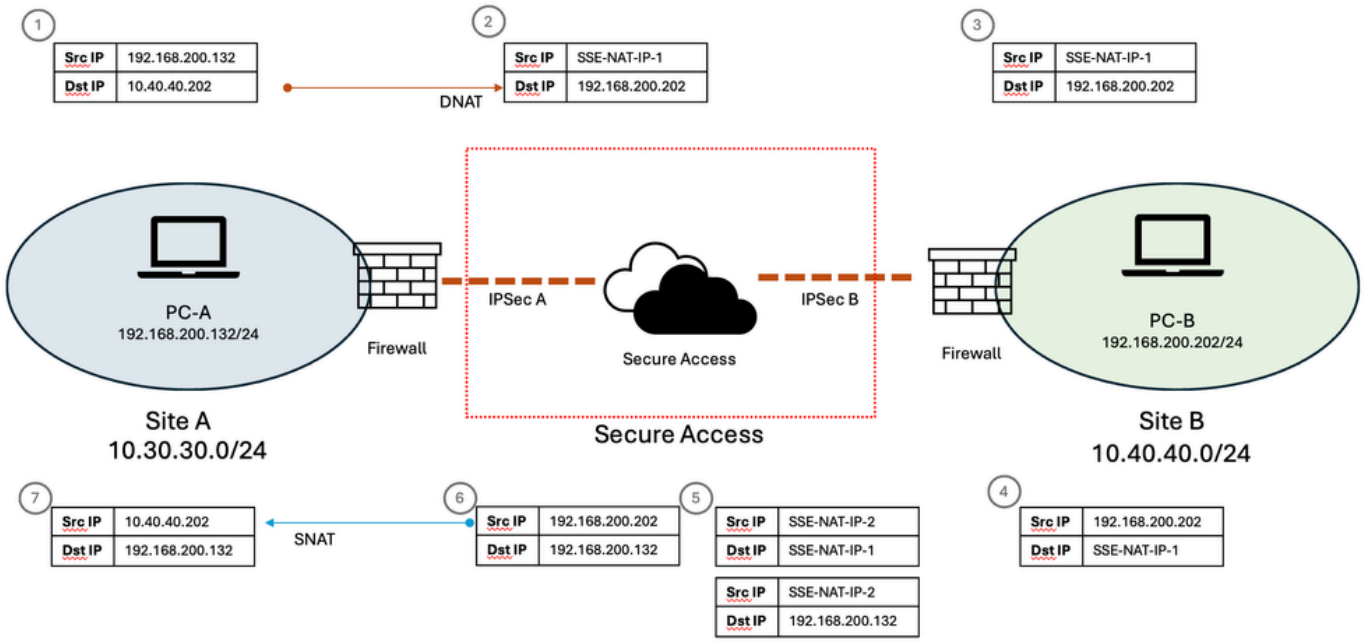

Imagen - Flujo de red

Para lograr esto, el firewall realiza la NAT de origen en el tráfico que sale hacia el grupo de túnel de red.

Para este ejemplo, la asignación necesaria es`192.168.200.0/24` → `10.40.40.0/24`

Esto crea la relación inversa uno a uno entre las direcciones reales y sus direcciones virtuales

correspondientes.

SNAT de uno a uno

Si el firewall soporta NAT de origen uno a uno para toda la subred, una sola regla NAT puede representar el rango de direcciones `/24` completo.

Por ejemplo:

Fuente real	Origen traducido
`192.168.200.0/24`	`10.40.40.0/24`

Esto da como resultado mapeos como `192.168.200.202 → 10.40.40.202` y `192.168.200.203 → 10.40.40.203`

La misma relación uno a uno se aplica a toda la subred.

Firewalls sin SNAT de uno a uno

Si el firewall no admite NAT de origen uno a uno para toda la subred, cada asignación necesaria debe configurarse individualmente.

Por ejemplo, para el servidor Web:

- IP de origen: `192.168.200.202`
- Interfaz de origen: Grupo de túnel de red
- Dirección del tráfico: Entrante
- IP de origen traducida: `10.40.40.202`

La traducción resultante es`192.168.200.202 → 10.40.40.202`

Se puede aplicar el mismo enfoque a cada recurso que requiera acceso a través de la subred virtual.

Esto garantiza que ambas direcciones de la comunicación mantengan el esquema de direccionamiento virtual y que el cliente reciba la respuesta de la misma dirección IP virtual que utilizó al establecer la conexión.

Información Relacionada

Configuración de Cisco Secure Access NAT Mapping/Network Tunnel Group : https://securitydocs.cisco.com/docs/csa/olh/168842.dita

Configuración de Cisco Secure Access Network Tunnel Group y referencia de routing: https://securitydocs.cisco.com/docs/csa/olh/118900.dita

Guía de recopilación de datos básicos y resolución de problemas de Cisco Secure Access: https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

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).