# Site-to-Site-Verbindungen mit überlappenden Subnetzen in Cisco Secure Access

## Inhalt



## Einleitung

In diesem Dokument wird die sich überschneidende Cisco Secure Access-Subnetzlösung beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Access-Administration
- Firewall-/Router-Administration

Cisco empfiehlt Folgendes:

- Administrator-Zugriff auf Cisco Secure Access
- Administratorzugriff auf das IPSec-Headend-Gerät (Firewall oder Router)

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Vorbereitungen

In diesem Beispiel gibt es zwei verschiedene Außenstellen mit demselben IP-Subnetz 192.168.200.0/24, in denen sie über zwei separate IPSec-Tunnel mit Cisco Secure Access verbunden sind.

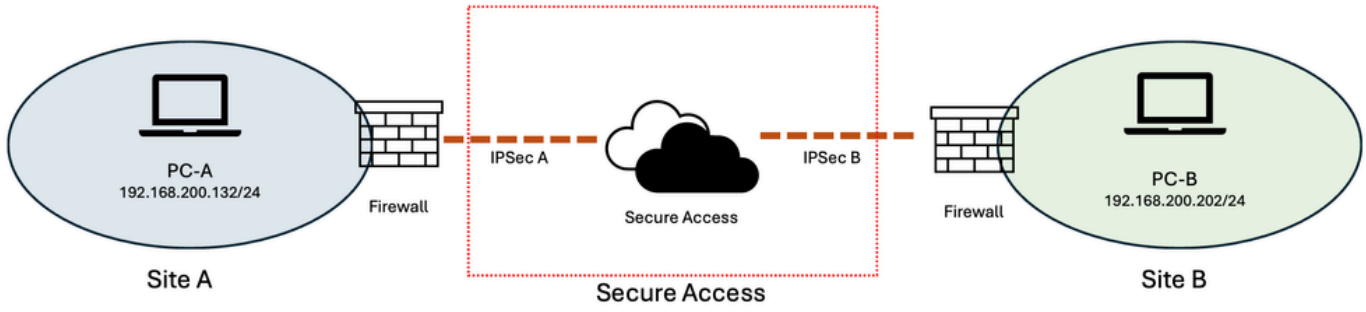


Bild - Netzwerkdiagramm

Das Ziel ist, dass Benutzer von "Standort A" auf die Ressourcen in "Standort B" zugreifen können und umgekehrt.

## Vorbereitung und Planung

Da beide Standorte dasselbe IP-Subnetz verwenden (`192.168.200.0/24`), verhindert der sich überschneidende Adressraum die direkte Kommunikation zwischen den beiden Standorten. Um diese Überlappung zu beheben, werden zwei nicht überlappende virtuelle Subnetze zugewiesen, die die Ressourcen an jedem Standort darstellen.

Für dieses Beispiel:

- Standort A: `10.30.30.0/24`
- Standort B: `10.40.40.0/24`
- Tatsächliches Subnetz an beiden Standorten: `192.168.200.0/24`

Die virtuellen Subnetze stellen eindeutige Adressräume für jeden Standort bereit, während die eigentlichen Ressourcen weiterhin ihre vorhandenen `192.168.200.0/24`-Adressen verwenden.

Wenn ein Benutzer an Standort A auf eine Ressource an Standort B zugreift, greift der Benutzer über das virtuelle Subnetz von Standort B (**`10.40.40.0/24) auf die`** Ressource zu, anstatt direkt den sich überschneidenden `Adressbereich von 192.168.200.0/24` zu verwenden.

Cisco Secure Access bietet eine One-to-One Destination NAT (D-NAT)-Funktion, mit der virtuelle Adressen in die entsprechenden realen Adressen übersetzt werden können. Der D-NAT-Adressbereich hat die gleiche Größe wie das ursprüngliche Subnetz. In diesem Beispiel sind sowohl das virtuelle als auch das tatsächliche Netzwerk `/24`-Subnetze, was eine 1:1-Zuordnung zwischen den virtuellen und den realen IP-Adressen ermöglicht.

Beispiele:

`10 40 40 202 → 192 168 200 202`

Aus diesem Grund wird eine Anfrage von Standort A, die für `10.40.40.202` bestimmt ist, von D-NAT in `192.168.200.202` übersetzt, sodass die Anfrage die entsprechende Ressource an Standort B erreichen kann, obwohl beide Standorte dasselbe zugrunde liegende IP-Subnetz verwenden.

Mit diesem Ansatz wird effektiv ein virtueller, sich nicht überlappender Adressraum für jeden Standort geschaffen, während die vorhandene IP-Adressierung der Ressourcen erhalten bleibt. Darüber hinaus wird eine konsistente 1:1-Beziehung zwischen den virtuellen und den realen Adressen geschaffen, sodass die Konfiguration einfacher zu verstehen, zu verwalten und Fehler einfacher zu beheben ist.

## Konfigurationsschritte

Aufgrund des aktuellen Designs und der Einschränkungen von Cisco Secure Access ist zur Umsetzung dieses Szenarios eine Konfiguration auf den Headend-Geräten hinter den IPsec-Tunneln und Cisco Secure Access erforderlich.

Das Headend-Gerät ist die Firewall oder der Router, die bzw. der den IPsec-Tunnel zu Cisco

Secure Access herstellt. Neben der Konfiguration von D-NAT in Cisco Secure Access muss die Headend-Firewall auch Source NAT (S-NAT) für den zurückkehrenden Datenverkehr ausführen.

Die Konfiguration besteht daher aus zwei Abschnitten:

1. Konfigurieren von Ziel-NAT (D-NAT) in Cisco Secure Access für jeden Netzwerktunnel separat
2. Konfigurieren von Source NAT (S-NAT) auf den Firewalls, um sicherzustellen, dass der zurückkehrende Datenverkehr in den virtuellen Adressraum zurückübersetzt wird.

## Konfigurieren von Cisco Secure Access

Schritt 1: Navigieren Sie im Cisco Secure Access Management-Portal zu Verbinden > Netzwerkverbindungen, und wählen Sie die Registerkarte Netzwerk-Tunnelgruppen aus.

Phase 2: Bearbeiten Sie die Netzwerk-Tunnelgruppe, die dem IPsec-Tunnel für den Standort zugeordnet ist, der das überlappende Subnetz verwendet.

In diesem Beispiel:

- IPSec-A = Netzwerk-Tunnelgruppe für Standort A
- IPSec-B = Netzwerk-Tunnelgruppe für Standort B

Schritt 3: Klicken Sie auf das Drei-Punkte-Menü neben der gewünschten Netzwerk-Tunnelgruppe, und wählen Sie Bearbeiten aus.

Schritt 4: Wählen Sie im Menü auf der linken Seite die Registerkarte Routing aus, und aktivieren Sie Network Address Translation (NAT), falls diese Option noch nicht aktiviert ist.

Schritt 5: Klicken Sie unter Ziel-NAT-Zuordnungen auf Zuordnungen hinzufügen.

Schritt 6: Mithilfe dieser Tabelle können Sie die D-NAT-Zuordnungen für jede Netzwerk-Tunnelgruppe konfigurieren:

| | Standort A - IPSec-Tunnel | Standort B - IPSec-Tunnel |
|---|---|---|
| Ziel-NAT-1 | Site → Sicherer Zugriff | Site → Sicherer Zugriff |

| | | |
|---|---|---|
| | Ursprüngliche CIDR: 10.40.40.0/24<br>Übersetzte CIDR: 192.168.200.0/24 | Ursprüngliche CIDR: 10.30.30.0/24<br>Übersetzte CIDR: 192.168.200.0/24 |
| Ziel-NAT-2 | Sicherer Zugriff → Site<br>Ursprüngliche CIDR: 192.168.200.0/24<br>Übersetzte CIDR: 10.30.30.0/24 | Sicherer Zugriff → Site<br>Ursprüngliche CIDR: 192.168.200.0/24<br>Übersetzter CIDR: 10.40.40.0/24 |
| |  <br>IPsec-Tunnelstandort A - D-NAT-Konfiguration |  <br>IPsec-Tunnelstandort B - D-NAT-Konfiguration |

Anmerkung: Klicken Sie nach dem Konfigurieren der Einstellungen für jede Netzwerk-Tunnelgruppe auf Speichern. Wenn das Bestätigungsfenster angezeigt wird, geben Sie UPDATE ein, um die Änderung zu bestätigen. Wiederholen Sie den gleichen Vorgang für die andere Netzwerk-Tunnelgruppe.

## Konfigurieren der Firewall

Die Firewall-Konfiguration ist aufgrund einer aktuellen Beschränkung bei der Behandlung sich überlappender IP-Subnetze hinter Netzwerk-Tunnelgruppen erforderlich.

Wenn Cisco Secure Access eine D-NAT für ein eingehendes Paket durchführt, wird die umgewandelte Zieladresse verwendet, um das Paket an die Zielressource zu senden. Die entsprechende umgekehrte Übersetzung wird in diesem überlappenden Subnetz-Szenario jedoch nicht automatisch für den zurückkehrenden Datenverkehr durchgeführt.

Daher muss der zurückkehrende Datenverkehr manuell per Quell-NAT über die Firewall geleitet werden.

Die wichtigste Anforderung besteht darin, dass der Zielserver den zurückfließenden Datenverkehr mithilfe der virtuellen IP-Adresse erkennt, auf die der Client ursprünglich zugegriffen hat, und nicht mithilfe der tatsächlichen IP-Adresse des Servers.

Beispiel

Nehmen wir Folgendes an:

- Standort A-Client: `192.168.200.132`
- Website B-Webserver: `192.168.200.202`
- Virtuelles Subnetz Standort B: `10.40.40.0/24`
- Virtuelle Adresse des Webservers: `10.40.40.202`

Der Client an Standort A greift über `https://10.40.40.202` auf den Webserver von Standort B zu.

Cisco Secure Access führt die D-NAT `10.40.40.202 → 192.168.200.202 aus.`

Das Paket erreicht dann den Webserver unter `192.168.200.202`.

Das Problem tritt beim zurückkehrenden Datenverkehr auf. Ohne zusätzliche NAT auf der Firewall generiert der Webserver die Antwort mit Quelle: `192.168.200.202`

Der Client hat jedoch die Verbindung mit Ziel initiiert: `10.40.40.202`

Daher muss der Rückverkehr so umgerechnet werden, dass die dem Client vorgelegte Quelladresse der virtuellen Adresse`192.168.200.202 → 10.40.40.202` entspricht

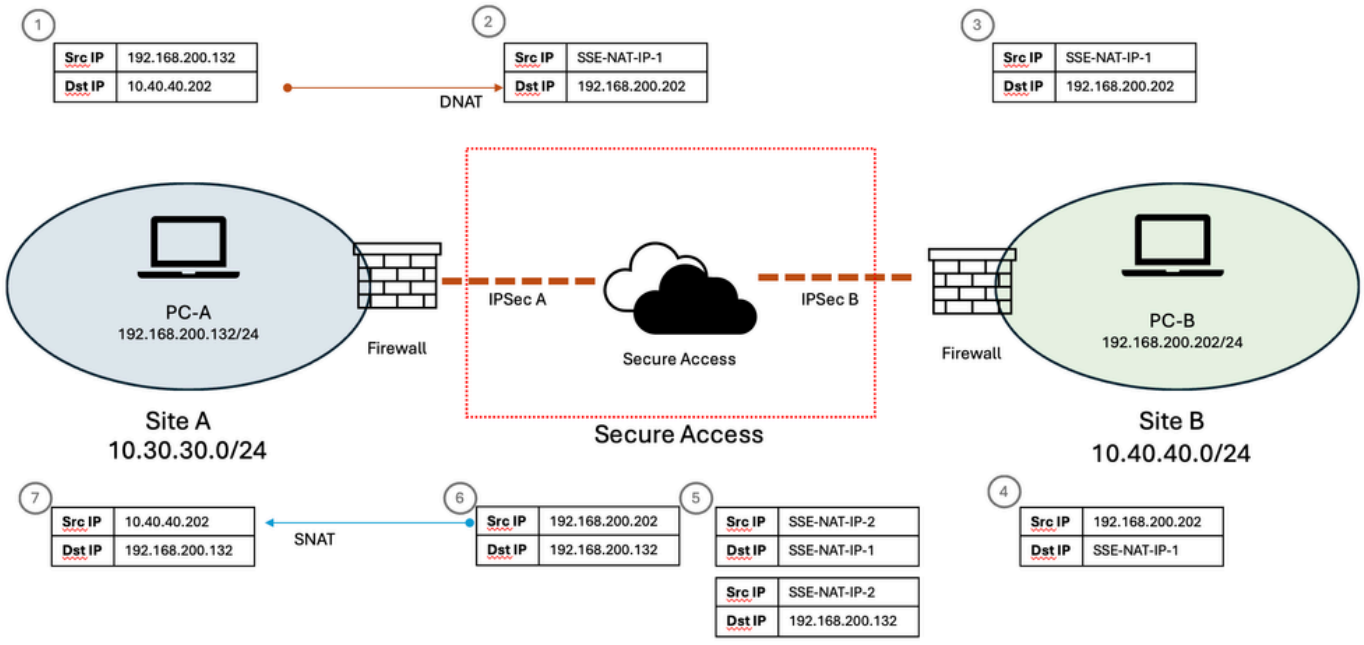


Image - Netzwerkfluss

Zu diesem Zweck führt die Firewall die Quell-NAT für Datenverkehr aus, der in Richtung der Netzwerk-Tunnelgruppe verläuft.

Für dieses Beispiel ist die erforderliche Zuordnung`192.168.200.0/24 → 10.40.40.0/24`

Dadurch entsteht die umgekehrte Eins-zu-Eins-Beziehung zwischen den realen Adressen und den entsprechenden virtuellen Adressen.

One-to-One SNAT

Wenn die Firewall One-to-One Source NAT für das gesamte Subnetz unterstützt, kann eine einzelne NAT-Regel den gesamten `24/24`-Adressbereich repräsentieren.

Beispiele:

| Quelle | Übersetzte Quelle |
|---|---|
| `192.168.200.0/24` | `10.40.40.0/24` |

Daraus ergeben sich Zuordnungen wie `192.168.200.202 → 10.40.40.202` und `192.168.200.203 → 10.40.40.203`

Die gleiche 1:1-Beziehung gilt für das gesamte Subnetz.

Firewalls ohne One-to-One SNAT

Wenn die Firewall keine Eins-zu-Eins-Quell-NAT für das gesamte Subnetz unterstützt, muss jede erforderliche Zuordnung einzeln konfiguriert werden.

Beispiel für einen Webserver:

- Quell-IP: `192.168.200.202`
- Quellschnittstelle: Netzwerk-Tunnelgruppe
- Datenverkehrsrichtung: Eingehend
- Übersetzte Quell-IP: `10.40.40.202`

Die resultierende Übersetzung ist`192.168.200.202 → 10.40.40.202`

Derselbe Ansatz kann auf alle Ressourcen angewendet werden, die Zugriff über das virtuelle Subnetz benötigen.

Dadurch wird sichergestellt, dass beide Kommunikationsrichtungen das virtuelle

Adressierungsschema beibehalten und dass der Client die Antwort von derselben virtuellen IP-Adresse erhält, die er beim Herstellen der Verbindung verwendet hat.

## Zugehörige Informationen

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

Cisco Secure Access Network Tunnel Group-Konfigurations- und Routing-Referenz: https://securitydocs.cisco.com/docs/csa/olh/118900.dita

Cisco Secure Access-Leitfaden zur Fehlerbehebung und Datenerfassung: https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.