Connectivité de site à site avec chevauchement des sous-réseaux dans Cisco Secure Access

Table des matières

Introduction

Ce document décrit la solution de sous-réseau de chevauchement d'accès sécurisé Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration de Cisco Secure Access.
- Administration du pare-feu/routeur.

Cisco vous recommande d'avoir :

- Accès administratif à Cisco Secure Access.
- Accès administratif au périphérique de tête de réseau IPSec (pare-feu ou routeur)

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Avant de commencer

Dans cet exemple, il existe deux sites de filiale différents avec le même sous-réseau IP 192.168.200.0/24, dans lesquels ils sont connectés à Cisco Secure Access via deux tunnels IPSec distincts.

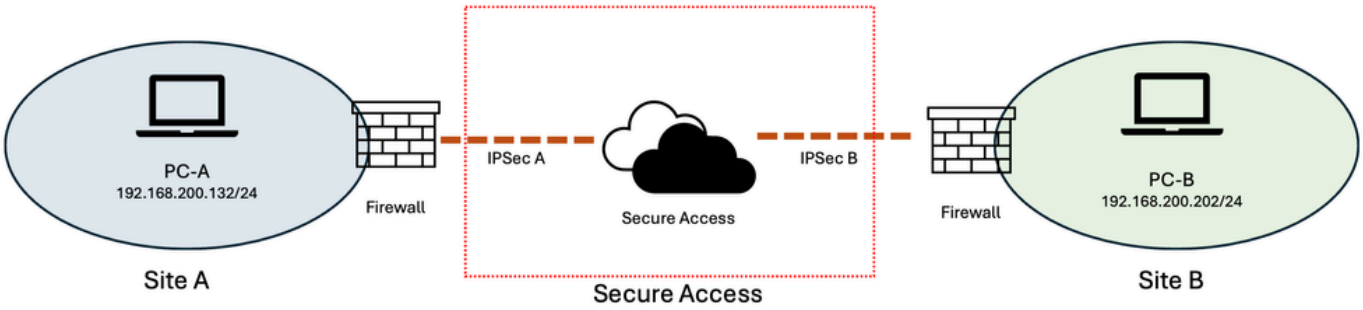


Image - Diagramme de réseau

L'objectif est que les utilisateurs du « Site A » puissent accéder aux ressources du « Site B » et vice versa.

Préparation et planification

Les deux sites utilisant le même sous-réseau IP (`192.168.200.0/24`), l’espace d’adressage qui se chevauche empêche la communication directe entre les deux sites. Pour résoudre ce chevauchement, deux sous-réseaux virtuels sans chevauchement sont affectés pour représenter les ressources de chaque site.

Pour cet exemple :

- Site A : `10.30.30.0/24`

- Site B : `10.40.40.0/24`
- Sous-réseau réel sur les deux sites : `192.168.200.0/24`

Les sous-réseaux virtuels fournissent des espaces d'adressage uniques pour chaque site, tandis que les ressources réelles continuent d'utiliser leurs adresses `192`.168.200.0/24 existantes.

Lorsqu'un utilisateur du site A accède à une ressource située sur le site B, il accède à la ressource par le sous-réseau virtuel du site B (**`10.40.40.0/24`**) plutôt qu'en utilisant directement l'`espace d'adressage 192.168.200.0/24` qui se chevauche.

Cisco Secure Access fournit une fonctionnalité NAT de destination un à un (D-NAT) qui peut traduire les adresses virtuelles en adresses réelles correspondantes. La plage d'adresses D-NAT a la même taille que le sous-réseau d'origine. Dans cet exemple, les réseaux virtuels et réels sont tous deux des sous-réseaux `/24`, fournissant un mappage un-à-un entre les adresses IP virtuelles et réelles.

Exemple :

`10.40.40.202` → `192.168.200.202`

Par conséquent, une requête du site A destinée à `10.40.40.202` est traduite par D-NAT en `192.168.200.202`, permettant à la requête d'atteindre la ressource correspondante au site B malgré que les deux sites utilisent le même sous-réseau IP sous-jacent.

Cette approche crée efficacement un espace d'adressage virtuel sans chevauchement pour chaque site tout en préservant l'adressage IP existant des ressources. Il fournit également une relation univoque et cohérente entre les adresses virtuelles et les adresses réelles, ce qui facilite la compréhension, la gestion et le dépannage de la configuration.

Configuration Steps

En raison de la conception actuelle et des limites de Cisco Secure Access, la réalisation de ce scénario nécessite une configuration sur les périphériques de tête de réseau derrière les tunnels IPsec et Cisco Secure Access.

Le périphérique de tête de réseau est le pare-feu ou le routeur qui établit le tunnel IPsec vers Cisco Secure Access. Outre la configuration de D-NAT dans Cisco Secure Access, le pare-feu de tête de réseau doit également exécuter la NAT source (S-NAT) pour le trafic de retour.

La configuration se compose donc de deux sections :

1. Configuration de la destination NAT (D-NAT) dans Cisco Secure Access pour chaque tunnel réseau séparément.
2. Configuration de la NAT source (S-NAT) sur les pare-feu pour garantir que le trafic de retour est retraduit vers l'espace d'adressage virtuel.

Configuration de Cisco Secure Access

Étape 1: Dans le portail de gestion Cisco Secure Access, naviguez jusqu'à Connect > Network Connections et sélectionnez l'onglet Network Tunnel Groups.

Étape 2: Modifiez le groupe de tunnels réseau associé au tunnel IPsec pour le site qui utilise le sous-réseau en chevauchement.

Dans cet exemple :

- IPSec-A = groupe de tunnels réseau pour le site A
- IPSec-B = groupe de tunnels réseau pour le site B

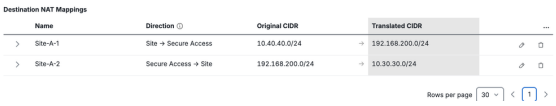
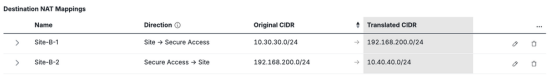
Étape 3: Cliquez sur le menu à trois points en regard du groupe de tunnels réseau requis et sélectionnez Edit.

Étape 4: Dans le menu de gauche, sélectionnez l'onglet Routing et activez Network Address Translation (NAT) s'il n'est pas déjà activé.

Étape 5: Sous Mappages NAT de destination, cliquez sur Ajouter des mappages.

Étape 6: Utilisez ce tableau pour configurer les mappages D-NAT pour chaque groupe de tunnels réseau :

	Site A - Tunnel IPSec	Site B - Tunnel IPSec
Destination NAT-1	Site → Accès sécurisé CIDR d'origine : 10.40.40.0/24 CIDR traduit : 192.168.200.0/24	Site → Accès sécurisé CIDR d'origine : 10.30.30.0/24 CIDR traduit : 192.168.200.0/24

NAT-2 de destination	Accès sécurisé → Site CIDR d'origine : 192.168.200.0/24 CIDR traduit : 10.30.30.0/24	Accès sécurisé → Site CIDR d'origine : 192.168.200.0/24 CIDR traduit : 10.40.40.0/24
	 Site de tunnel IPsec A - Configuration D-NAT	 Site de tunnel IPsec B - Configuration D-NAT

Remarque : Après avoir configuré les paramètres de chaque groupe de tunnels réseau, cliquez sur Save. Lorsque la fenêtre de confirmation apparaît, saisissez UPDATE pour confirmer la modification. Répétez la même procédure pour l'autre groupe de tunnels réseau

Configuration du pare-feu

La configuration du pare-feu est requise en raison d'une limitation actuelle dans la gestion des sous-réseaux IP qui se chevauchent derrière les groupes de tunnels réseau.

Lorsque Cisco Secure Access exécute D-NAT sur un paquet entrant, l'adresse de destination traduite est utilisée pour acheminer le paquet vers la ressource de destination. Cependant, la traduction inverse correspondante n'est pas exécutée automatiquement pour le trafic de retour dans ce scénario de chevauchement de sous-réseaux.

Par conséquent, le trafic de retour doit être envoyé manuellement par NAT source sur le pare-feu.

La condition essentielle est que le serveur de destination voie le trafic de retour en utilisant l'adresse IP virtuelle à laquelle le client a accédé à l'origine, plutôt que l'adresse IP réelle du serveur.

Exemple

Supposons ce qui suit :

- Client du site A : `192.168.200.132`
- Serveur Web du site B : `192.168.200.202`
- Sous-réseau virtuel du site B : `10.40.40.0/24`
- Adresse virtuelle du serveur Web : `10.40.40.202`

Le client du site A accède au serveur Web du site B à l'aide de https://10.40.40.202

Cisco Secure Access exécute la D-NAT `10.40.40.202 → 192.168.200.202`

Le paquet atteint ensuite le serveur Web à l'adresse `192.168.200.202`.

Le problème se produit avec le trafic de retour. Sans NAT supplémentaire sur le pare-feu, le serveur Web génère la réponse avec Source : `192.168.200.202`

Cependant, le client a initié la connexion à Destination : `10.40.40.202`

Par conséquent, le trafic de retour doit être traduit de sorte que l'adresse source présentée au client corresponde à l'adresse virtuelle`192.168.200.202 → 10.40.40.202`

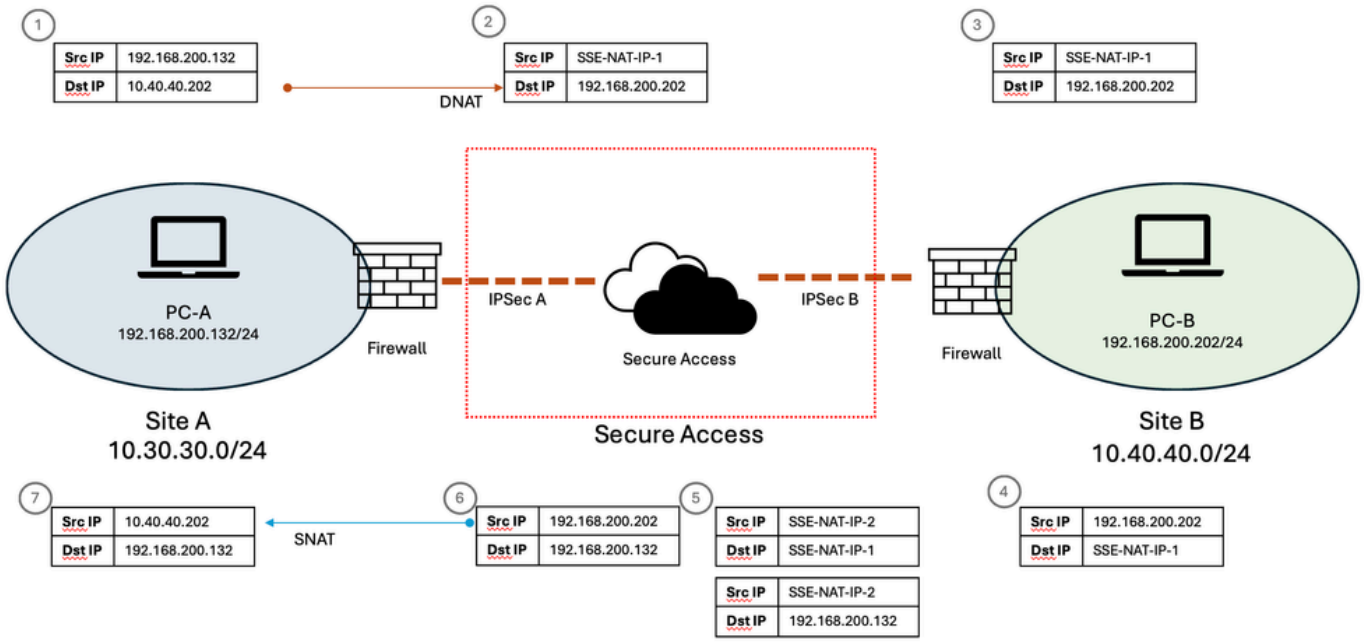


Image - Flux réseau

Pour ce faire, le pare-feu exécute la fonction NAT source sur le trafic sortant vers le groupe de tunnels réseau.

Pour cet exemple, le mappage requis est`192.168.200.0/24 → 10.40.40.0/24`

Cela crée la relation inverse un à un entre les adresses réelles et leurs adresses virtuelles correspondantes.

SNAT un à un

Si le pare-feu prend en charge la NAT source un-à-un pour l'ensemble du sous-réseau, une seule règle NAT peut représenter la plage d'adresses `/24` complète.

Exemple :

Source réelle	Source traduite
`192.168.200.0/24`	`10.40.40.0/24`

Il en résulte des mappages tels que `192.168.200.202 → 10.40.40.202` et `192.168.200.203 → 10.40.40.203`

La même relation un-à-un s'applique à l'ensemble du sous-réseau.

Pare-feu sans SNAT un à un

Si le pare-feu ne prend pas en charge la NAT source un-à-un pour l'ensemble du sous-réseau, chaque mappage requis doit être configuré individuellement.

Par exemple, pour le serveur Web :

- Adresse IP source: `192.168.200.202`
- Interface source : Groupe de tunnels réseau
- Direction du trafic : Entrant
- Adresse IP source traduite : `10.40.40.202`

La traduction obtenue est `192.168.200.202 → 10.40.40.202`

La même approche peut être appliquée à chaque ressource qui nécessite un accès via le sous-réseau virtuel.

Cela garantit que les deux directions de la communication conservent le schéma d’adressage virtuel et que le client reçoit la réponse de la même adresse IP virtuelle qu’il a utilisée lors de l’établissement de la connexion.

Informations connexes

Mappage NAT d'accès sécurisé Cisco / Configuration du groupe de tunnels réseau :
https://securitydocs.cisco.com/docs/csa/olh/168842.dita

Référence de configuration et de routage du groupe de tunnels réseau Cisco Secure Access :
https://securitydocs.cisco.com/docs/csa/olh/118900.dita

Guide de dépannage et de collecte de données de base de Cisco Secure Access :
https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.