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

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Avant de commencer

Préparation et planification

Configuration Steps

- Configuration de Cisco Secure Access

Autres informations utiles

Introduction

Ce document décrit la solution de sous-réseau qui se chevauche dans Cisco Secure Access.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration de Cisco Secure Access

Cisco vous recommande d'avoir :

- Accès administratif à Cisco Secure Access

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, deux filiales utilisent le même sous-réseau IP, 192.168.200.0/24, et sont connectées à Cisco Secure Access via deux tunnels IPsec distincts.

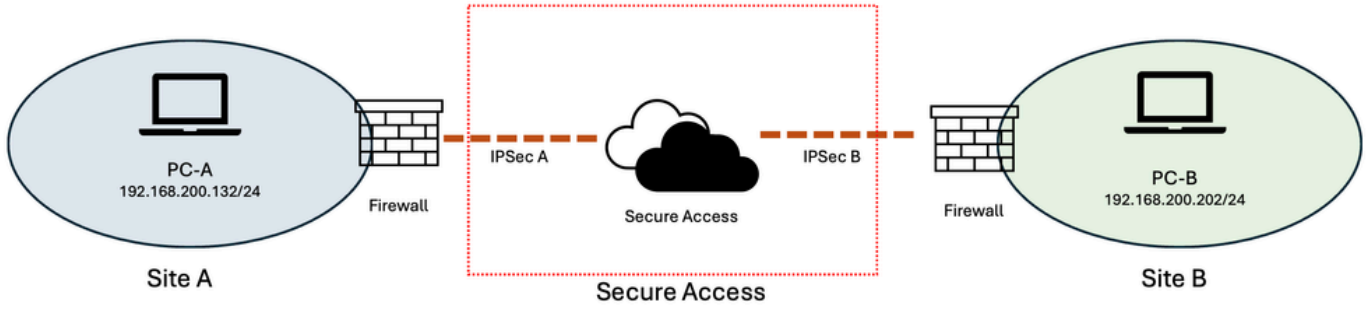


Image - Diagramme de réseau

L'objectif est que les utilisateurs du site A puissent accéder aux ressources du site B, et vice versa.

Préparation et planification

Étant donné que les deux sites utilisent le même sous-réseau IP (192.168.200.0/24), le chevauchement de l'espace d'adressage 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 du site B, il y accède via le sous-réseau virtuel du site B (10.40.40.0/24) plutôt que directement à l'aide de l'espace d'adressage 192.168.200.0/24 qui se chevauche.

Cisco Secure Access fournit une fonction 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, ce qui permet 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

La configuration se compose donc de deux sections :

1. Configuration de la destination NAT (D-NAT) dans Cisco Secure Access pour un tunnel réseau. (Dans cet exemple, Site B)
2. Configuration du routage statique dans Cisco Secure Access pour un autre tunnel réseau (dans cet exemple, le site A)

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: Pour le site B, configurez les mappages NAT de destination,

Étape 4-1 : Dans le menu de gauche, sélectionnez l'onglet Routing et activez Network Address Translation (NAT) s'il n'est pas déjà activé.

Étape 4-2 : Sous Mappages NAT de destination, cliquez sur Ajouter des mappages.

Étape 4-3 : Utilisez ce tableau pour configurer les mappages D-NAT pour le groupe de tunnels réseau.

Étape 4-4 : Enregistrez les modifications.

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

---

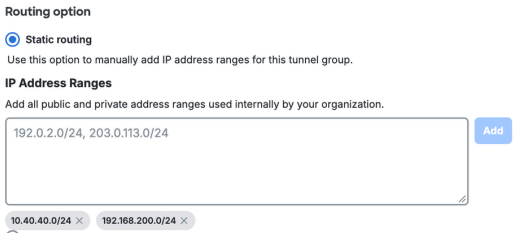
Étape 5: Pour le site A, configurez le routage statique,

Étape 5-1 : Dans le menu de gauche, sélectionnez l'onglet Routing et activez le routage statique s'il n'est pas déjà activé.

Étape 5-2 : Entrez les sous-réseaux et le sous-réseau virtuel dans la section Plages d'adresses IP.

Étape 5-3 : Utilisez cette table pour configurer le routage du groupe de tunnels réseau.

Étape 5-4 : Enregistrez les modifications.

	Site A - Tunnel IPsec	Site B - Tunnel IPsec
Destination NAT-1	S/O	Site → Accès sécurisé CIDR d'origine :192.168.200.0/24 CIDR traduit : 10.40.40.0/24
NAT-2 de destination	S/O	Accès sécurisé → Site CIDR d'origine : 192.168.200.0/24 CIDR traduit : 10.30.30.0/24
Routage	Plages d'adresses IP : 10.40.40.0/24 192.168.200.0/24	S/O
	 Site de tunnel IPsec A - Configuration du routage statique	 Site de tunnel IPsec B - Configuration D-NAT

Autres informations utiles

Mappage NAT d'accès sécurisé Cisco / Configuration du groupe de tunnels réseau

Guide de référence de configuration et de routage du groupe de tunnels Cisco Secure Access

Guide de dépannage et de collecte de données de base de Cisco Secure Access

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.