Site-to-site connectiviteit met overlappende subnetten in Cisco Secure Access

Inhoud

Inleiding

In dit document wordt de overlappende subnetoplossing van Cisco Secure Access beschreven.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beheer van Cisco Secure Access.
- Firewall/routerbeheer.

Cisco raadt u aan om:

- Administratieve toegang tot Cisco Secure Access.
- Administratieve toegang tot het IPSec Headend-apparaat (firewall of router)

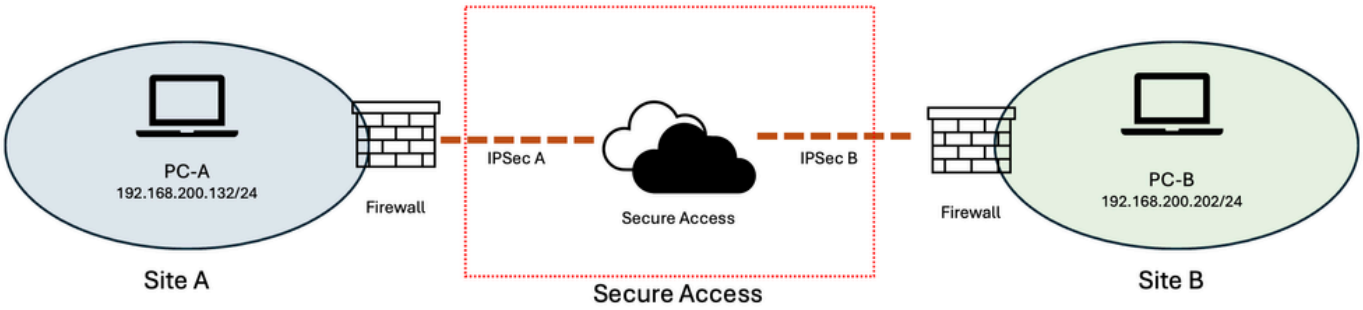
Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Voordat u begint

In dit voorbeeld zijn er twee verschillende filiaalsites met hetzelfde IP-subnet 192.168.200.0/24, waarin ze zijn verbonden met de Cisco Secure Access via twee afzonderlijke IPSec Tunnel.



Afbeelding - Netwerkdiagram

Het doel is dat gebruikers van "Site A" toegang hebben tot de bronnen in "Site B" en andersom.

Voorbereiding en planning

Omdat beide sites hetzelfde IP-subnet gebruiken (`192.168.200.0/24`), voorkomt de overlappende adresruimte directe communicatie tussen de twee sites. Om deze overlapping op te lossen, worden twee niet-overlappende virtuele subnetten toegewezen om de bronnen op elke site weer te geven.

Voor dit voorbeeld:

- Site A: `10.30.30.0/24`

- Site B: `10.40.40.0/24`
- Werkelijk subnet op beide sites: `192.168.200.0/24`

De virtuele subnetten bieden unieke adresruimten voor elke site, terwijl de werkelijke bronnen hun bestaande `192.168.200.0/24`-adressen blijven gebruiken.

Wanneer een gebruiker van site A toegang heeft tot een bron op site B, krijgt de gebruiker toegang tot de bron via het virtuele subnet van site B (**`10.40.40.0/24`**) in plaats van rechtstreeks de overlappende 192.168.200.0/24 `adresruimte te gebruiken.`

Cisco Secure Access biedt een One-to-One Destination NAT (D-NAT)-functie die de virtuele adressen kan vertalen naar de corresponderende echte adressen. Het D-NAT-adresbereik heeft dezelfde grootte als het oorspronkelijke subnet. In dit voorbeeld zijn zowel de virtuele als de werkelijke netwerken `24/`subnetten, die een één-op-één-toewijzing tussen de virtuele en echte IP-adressen bieden.

Voorbeeld:

`10.40.40.202 → 192.168.200.202`

Daarom wordt een verzoek van Site A bestemd voor `10.40.40.202` door D-NAT vertaald naar `192.168.200.202`, waardoor het verzoek de overeenkomstige bron op Site B kan bereiken, ondanks dat beide sites hetzelfde onderliggende IP-subnet gebruiken.

Deze aanpak creëert effectief een virtuele, niet-overlappende adresruimte voor elke site met behoud van het bestaande IP-adres van de bronnen. Het biedt ook een consistente één-op-één relatie tussen de virtuele en echte adressen, waardoor de configuratie gemakkelijker te begrijpen, beheren en oplossen van problemen.

Configuratiestappen

Vanwege het huidige ontwerp en de beperkingen van Cisco Secure Access, vereist het bereiken van dit scenario configuratie op zowel de headendapparaten achter de IPsec-tunnels als Cisco Secure Access.

Het kopapparaat is de firewall of router die de IPsec-tunnel naar Cisco Secure Access tot stand brengt. Naast het configureren van D-NAT in Cisco Secure Access, moet de headendfirewall ook Source NAT (S-NAT) uitvoeren voor het retourverkeer.

De configuratie bestaat daarom uit twee secties:

1. Bestemming NAT (D-NAT) configureren in Cisco Secure Access voor elke netwerktunnel afzonderlijk.
2. Het configureren van Source NAT (S-NAT) op de firewalls om ervoor te zorgen dat retourverkeer wordt terugvertaald naar de virtuele adresruimte.

Cisco Secure Access configureren

Stap 1: Navigeer vanuit het Cisco Secure Access-beheerportaal naar Verbinding > Netwerkverbindingen en selecteer het tabblad Netwerktunnelgroepen.

Stap 2: Bewerk de netwerktunnelgroep die is gekoppeld aan de IPsec-tunnel voor de site die het overlappende subnet gebruikt.

In dit voorbeeld:

- IPSec-A = Netwerktunnelgroep voor site A
- IPSec-B = Netwerktunnelgroep voor site B

Stap 3: Klik op het driepuntmenu naast de gewenste Netwerktunnelgroep en selecteer Bewerken.

Stap 4: Selecteer in het linkermenu het tabblad Routering en schakel Network Address Translation (NAT) in als dit nog niet is ingeschakeld.

Stap 5: Onder Bestemming NAT Toewijzingen, klikt u op Toewijzingen toevoegen.

Stap 6: Gebruik deze tabel om de D-NAT-toewijzingen voor elke netwerktunnelgroep te configureren:

	Site A - IPSec-tunnel	Site B - IPSec-tunnel
Bestemming NAT-1	Site → Veilige toegang Oorspronkelijke CIDR: 10.40.40.0/24 Vertaald: CIDR 192.168.200.0/24	Site → Veilige toegang Oorspronkelijke CIDR: 10.30.30.0/24 Vertaald: CIDR 192.168.200.0/24

Bestemming NAT-2	Veilige toegang → Site Oorspronkelijke CIDR: 192.168.200.0/24 Vertaald CIDR: 10.30.30.0/24	Veilige toegang → Site Oorspronkelijke CIDR: 192.168.200.0/24 Vertaald CIDR: 10.40.40.0/24
	 IPsec Tunnel Site A - D-NAT-configuratie	 IPsec Tunnel Site B - D-NAT-configuratie

Opmerking: Nadat u de instellingen voor elke netwerktunnelgroep hebt geconfigureerd, klikt u op Opslaan. Wanneer het bevestigingsvenster verschijnt, voert u UPDATE in om de wijziging te bevestigen. Herhaal dezelfde procedure voor de andere netwerktunnelgroep

De firewall configureren

De firewallconfiguratie is vereist vanwege een huidige beperking in de verwerking van overlappende IP-subnetten achter Network Tunnel Groups.

Wanneer Cisco Secure Access D-NAT uitvoert op een binnenkomend pakket, wordt het vertaalde bestemmingsadres gebruikt om het pakket aan de bestemmingsbron te leveren. De overeenkomstige omgekeerde vertaling wordt echter niet automatisch uitgevoerd voor het retourverkeer in dit overlappende subnetscenario.

Als gevolg hiervan moet het retourverkeer handmatig op de firewall worden opgeslagen.

De belangrijkste vereiste is dat de bestemmingsserver het retourverkeer ziet met behulp van het virtuele IP-adres waartoe de client oorspronkelijk toegang had, in plaats van het werkelijke IP-adres van de server.

Voorbeeld

Ga uit van het volgende:

- Site A-client: `192.168.200.132`
- Website B-webserver: `192.168.200.202`
- Site B virtueel subnet: `10.40.40.0/24`

- Virtueel adres van de webserver: `10.40.40.202`

De client op site A heeft toegang tot de site B-webserver via `https://10.40.40.202`

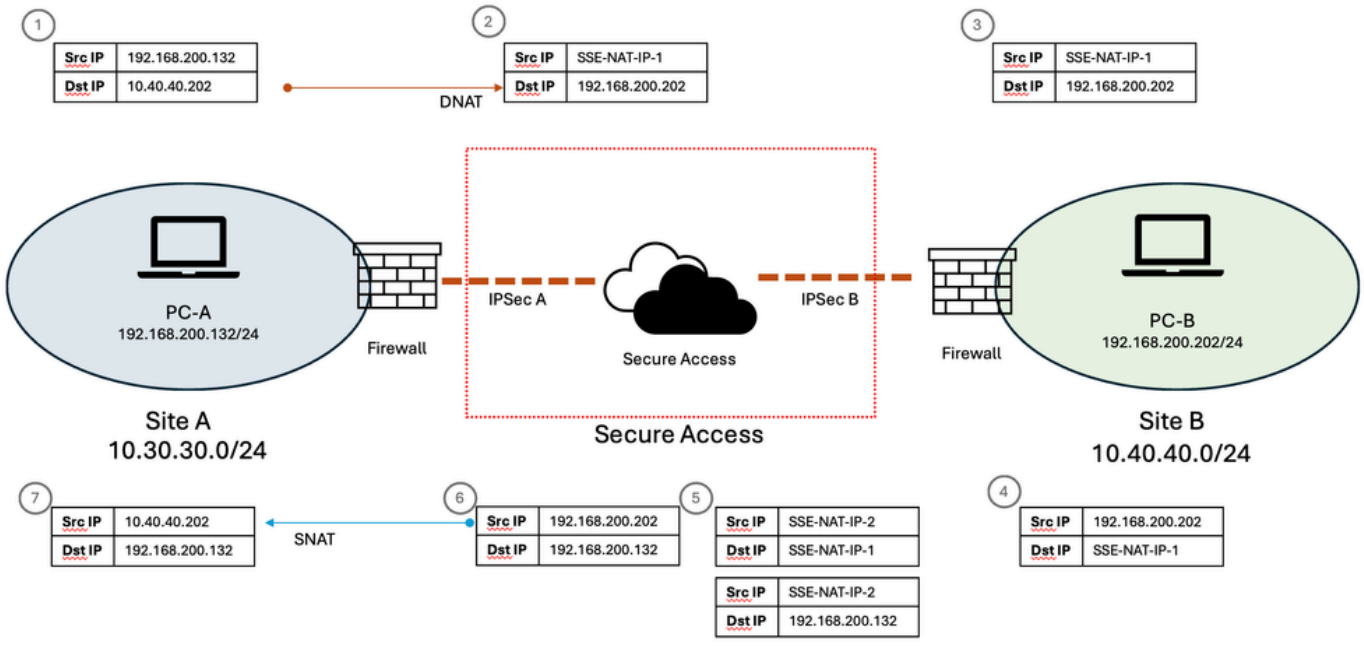
Cisco Secure Access voert de D-NAT `10.40.40.202 → 192.168.200.202 uit`

Het pakket bereikt vervolgens de webserver op `192.168.200.202`.

Het probleem doet zich voor bij het retourverkeer. Zonder extra NAT op de firewall genereert de webserver de respons met Bron: `192.168.200.202`

De client heeft echter de verbinding met Bestemming gestart: `10.40.40.202`

Daarom moet het retourverkeer worden vertaald, zodat het bronadres dat aan de klant wordt gepresenteerd overeenkomt met het virtuele adres`192.168.200.202 → 10.40.40.202`



Afbeelding - Netwerkstroom

Om dit te bereiken, voert de firewall Source NAT uit op verkeer dat naar de Network Tunnel Group vertrekt.

Voor dit voorbeeld is de vereiste toewijzing `192.168.200.0/24 → 10.40.40.0/24`

Dit creëert de omgekeerde één-op-één relatie tussen de echte adressen en hun bijbehorende

virtuele adressen.

Eén-op-één SNAT

Als de firewall één-op-één Source NAT voor het gehele subnet ondersteunt, kan één NAT-regel het volledige `/24`-adresbereik vertegenwoordigen.

Voorbeeld:

werkelijke bron	Vertaalde bron
`192.168.200.0/24`	`10.40.40.0/24`

Dit resulteert in mappings zoals `192.168.200.202 → 10.40.40.202` en `192.168.200.203 → 10.40.40.203`

Dezelfde één-op-één relatie geldt voor het hele subnet.

Firewalls zonder één-op-één SNAT

Als de firewall geen één-op-één Source NAT voor het gehele subnet ondersteunt, moet elke vereiste toewijzing afzonderlijk worden geconfigureerd.

Bijvoorbeeld voor de webserver:

- Bron: IP: `192.168.200.202`
- Broninterface: Netwerktunnelgroep
- Verkeersrichting: Inbound
- Vertaalde bron IP: `10.40.40.202`

De resulterende vertaling is `192.168.200.202 → 10.40.40.202`

Dezelfde aanpak kan worden toegepast op elke bron die toegang via het virtuele subnet vereist.

Dit zorgt ervoor dat in beide richtingen van de communicatie het virtuele adresschema wordt gehandhaafd en dat de client de respons ontvangt van hetzelfde virtuele IP-adres dat hij heeft gebruikt bij het tot stand brengen van de verbinding.

Gerelateerde informatie

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

Cisco Secure Access Network Tunnel Group-configuratie en routeringsreferentie:
https://securitydocs.cisco.com/docs/csa/olh/118900.dita

Cisco Secure Access-handleiding voor probleemoplossing en verzameling van basisgegevens:
https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.