SIG-beleid configureren voor externe toegang voor gebruikers van Secure Connect

Inhoud

Inleiding

In dit document wordt beschreven hoe u SIG-beleid kunt maken voor externe toegang voor gebruikers van Secure Connect.

Overzicht

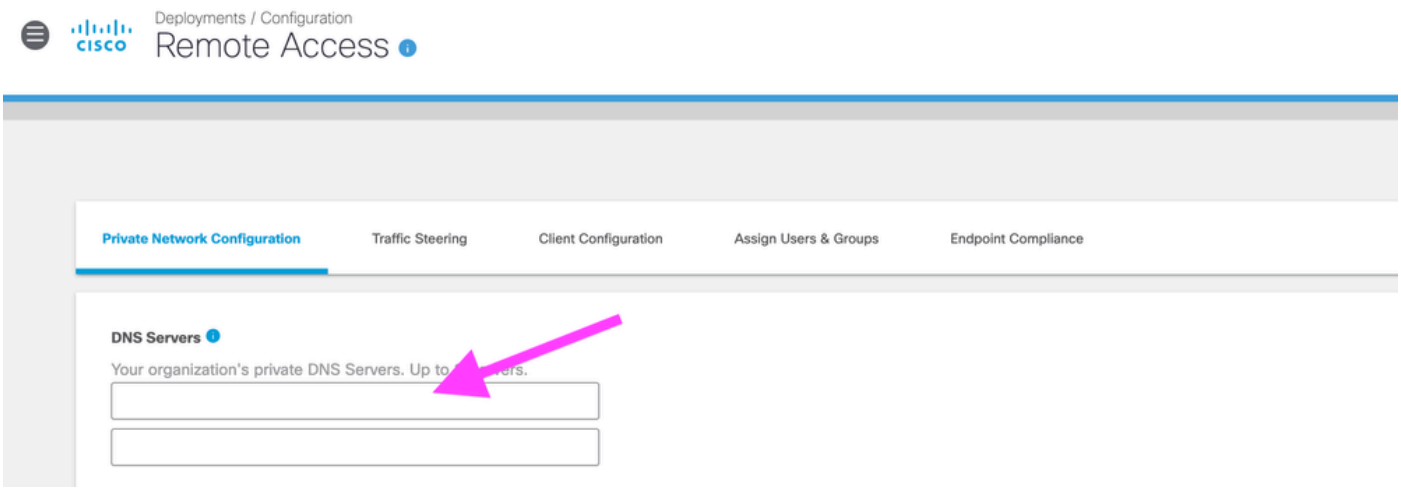
Dit artikel in de Kennisbank is van toepassing op klanten die gebruikmaken van het Secure Connect-pakket dat de functionaliteit voor externe toegang (VPNaaS) in Umbrella bevat.

Beheerders kunnen beleidsregels voor Umbrella Firewall, Web en Gegevensverlies configureren voor zwervende gebruikers die via AnyConnect zijn verbonden met Externe toegang.

DNS-beleid

Het is mogelijk om DNS-query's te verzenden naar Umbrella resolvers (bijv. 208.67.222.222) via de AnyConnect Remote Access VPN-verbinding. Dit maakt echter geen identificatie, beleid of rapportage van DNS-verkeer op het Umbrella-dashboard mogelijk.

- Dit biedt alleen DNS-resolutie en wordt daarom meestal niet aanbevolen.
- Het gebruik van externe DNS-resolvers in uw VPN DNS-configuratie voorkomt het oplossen van interne DNS-zones.

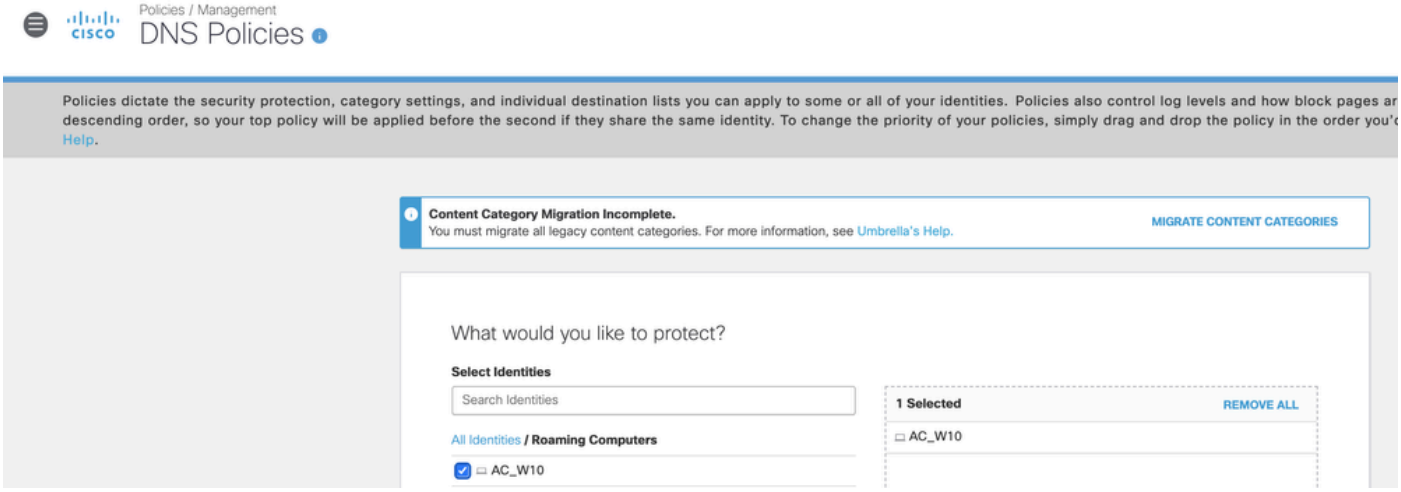


4410210378004

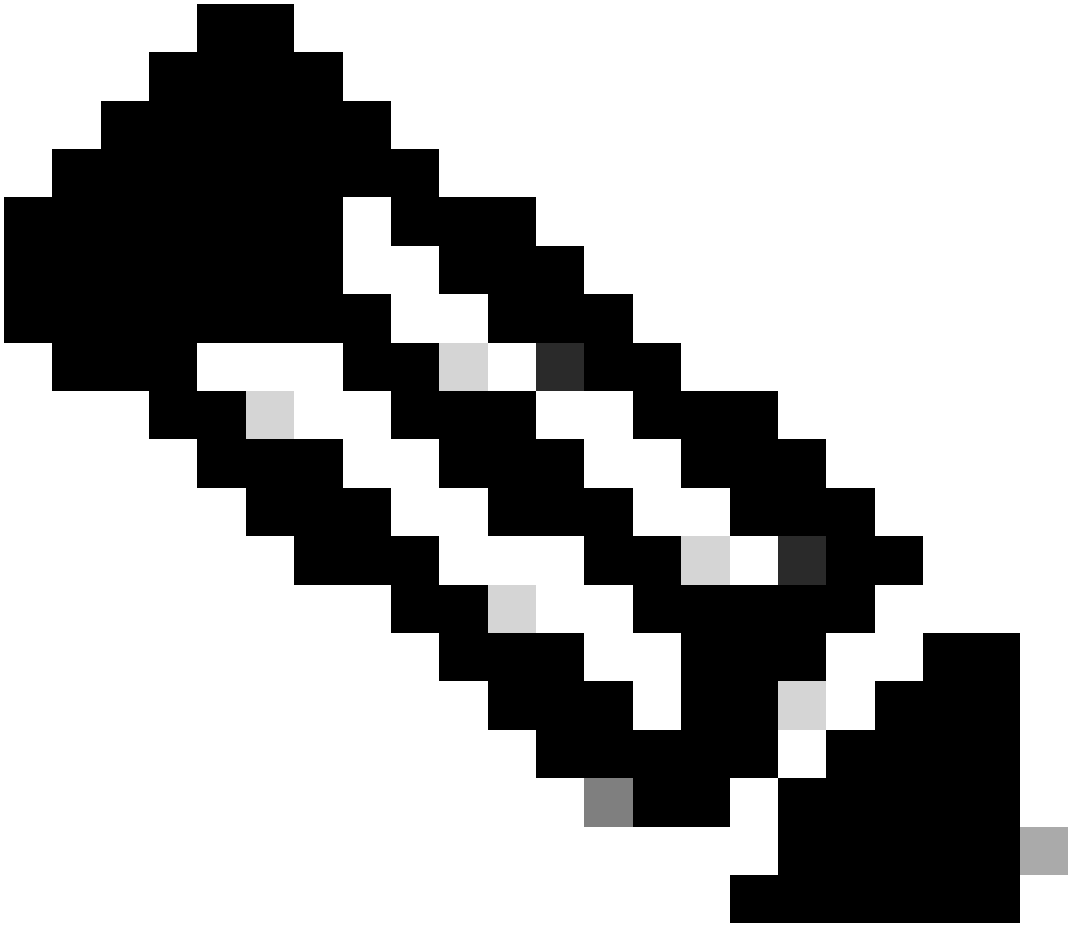
Om identiteit, beleid en rapportage voor DNS-query's toe te voegen, moet een van de drie methoden worden overwogen:

- (Aanbevolen) - Implementeer de overkoepelende AnyConnect-roamingmodule (van Implementaties > Roamingcomputers). Extern DNS-verkeer wordt rechtstreeks naar Umbrella verzonden met de identiteit "Roaming Computer" toegepast. Deze module ondersteunt ook optionele gebruikersidentificatie voor AD.
- Verkeer doorsturen van uw on-premise DNS-server naar Umbrella en verkeer identificeren met behulp van een Network identity. Alle gebruikers ontvangen hetzelfde beleid/dezelfde identiteit en er is geen gedetailleerde gebruikersrapportage.
- Gebruik een Umbrella Virtual Appliance op uw lokale netwerk om verkeer door te sturen naar Umbrella. DNS-query's kunnen worden geïdentificeerd aan de hand van hun interne VPN-pool (IP-adres). AD-integratie kan worden toegevoegd: hiervoor moeten aanvullende on-premise onderdelen worden geïnstalleerd.

In dit voorbeeld wordt getoond hoe een DNS-beleid kan worden geconfigureerd (Beleid > DNS-beleid) voor een individuele AnyConnect-client. Dit is alleen mogelijk wanneer de overkoepelende AnyConnect-roamingmodule wordt geïmplementeerd:



4410210455444



Opmerking: wanneer u de overkoepelende module voor AnyConnect gebruikt, kan DNS-verkeer optioneel binnen of buiten de tunnel worden verzonden, afhankelijk van uw gesplitste tunnelconfiguratie.

Firewallbeleid

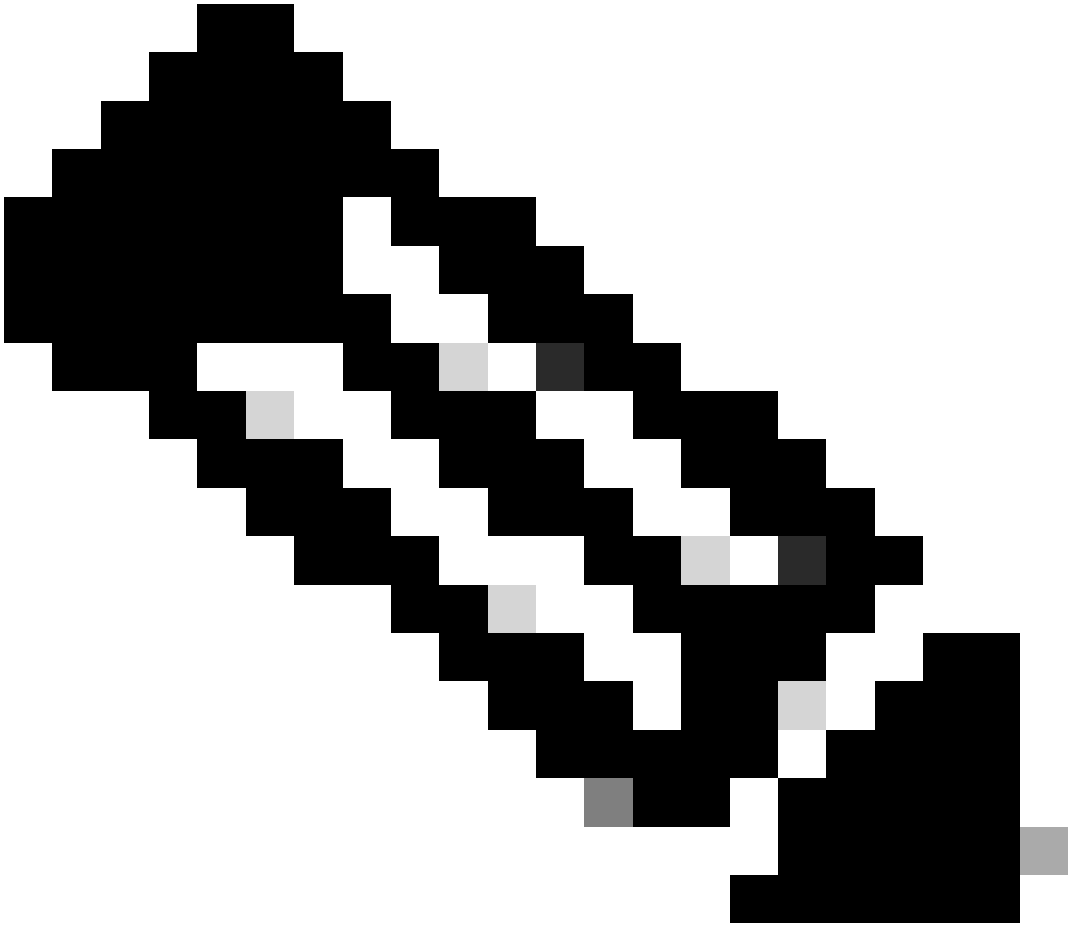
Het firewallbeleid is van toepassing op het verkeer tussen de clients voor externe toegang (AnyConnect) en het internet. Configureer regels in 'Implementaties > Firewallbeleid' volgens de documentatie die u hier vindt: Firewall beheren.

De standaardfirewallregel is van toepassing op clients voor externe toegang. Als u een specifiek beleid maakt voor gebruikers van Externe toegang, kunt u optioneel kiezen om een nieuw firewallbeleid te maken en "Externe toegang of id:<ID>" als brontunnelidentiteit selecteren. Hetzelfde firewallbeleid is van toepassing op alle gebruikers van externe toegang.

- Firewallbeleid wordt niet gebruikt om de toegang tussen RA-clients en privé-/filiaalnetwerken te regelen. Dit moet worden gecontroleerd met on-premise firewalls.

- Zoals alle Umbrella Firewall-regels, regelen deze regels uitgaande verbindingen voor Remote Access-clients. Inkomende verbindingen zijn nooit toegestaan.
- Het bron-IP-adres voor Remote Access-clients wordt altijd dynamisch toegewezen vanuit de VPN-pool.
    - Het maken van regels voor een specifieke computer met behulp van "Bron-IP" wordt niet aanbevolen omdat het IP dynamisch opnieuw wordt toegewezen
    - Het maken van regels die van invloed zijn op gebruikers van een specifiek datacenter voor externe toegang is mogelijk met behulp van een "Source CIDR" - bereik. Elk datacenter biedt een ander VPN-poolbereik dat is geconfigureerd op de pagina 'Implementaties > Externe toegang'.

4409322341524



Opmerking: identificatie per gebruiker is niet beschikbaar voor firewallbeleid.

Webbeleid

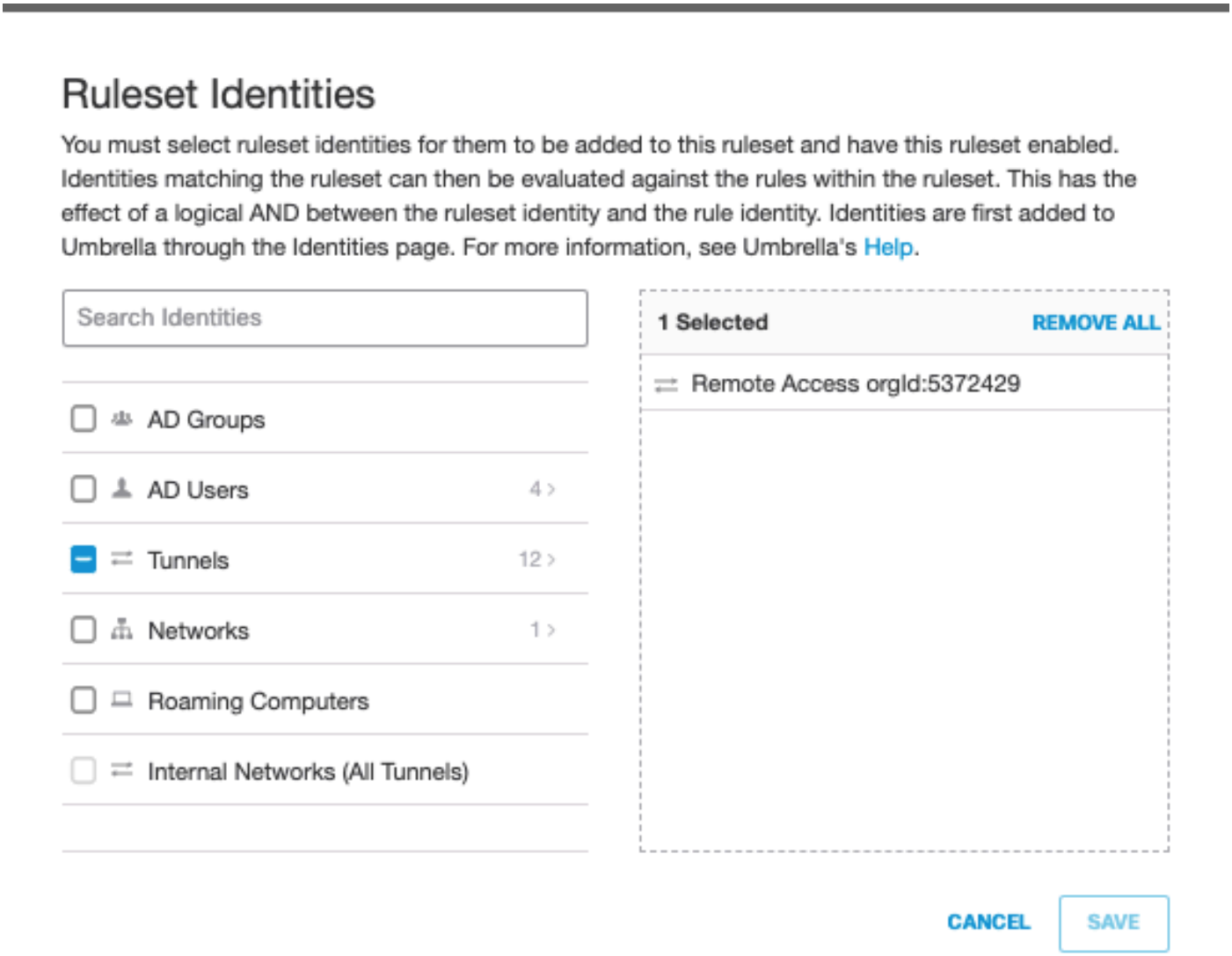
Het webbeleid is van toepassing op verkeer tussen de clients voor externe toegang (AnyConnect) en internet. Configureer regels in 'Implementaties > Webbeleid' zoals in de documentatie hier te vinden is: Webbeleid beheren.

- Het webbeleid wordt niet gebruikt om de toegang tussen RA-clients en private/branch-webservers te beheren. Het webbeleid is alleen van toepassing op externe websites.

Het standaardwebbeleid is van toepassing op clients voor externe toegang. We raden echter aan een nieuwe regelset te maken om beveiligingsinstellingen specifiek voor Remote Access-clients te definiëren. Bij het definiëren van de Ruleset identiteiten kiest u Externe toegang of id:<ID> uit de lijst met tunnels. Hetzelfde webbeleid is van toepassing op alle gebruikers van externe toegang.

Na het maken van een regelset is het mogelijk om een webregel toe te voegen die de

filterinstellingen voor inhoudscategorieën en toepassingsinstellingen definieert.



4409322363924

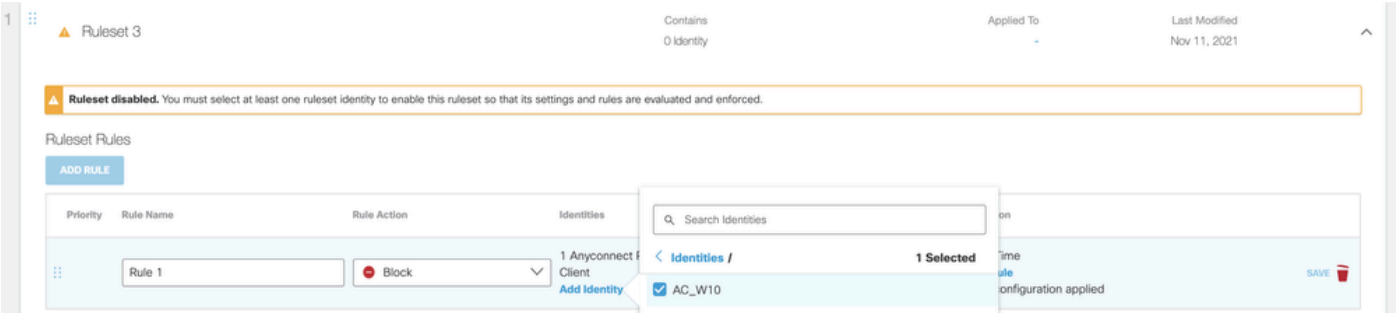
Identificatie van webgebruiker

Het verkeer voor externe toegang kan standaard niet per gebruiker of groep worden beheerd. Hetzelfde beleid is van toepassing op al het RA-verkeer op basis van de identiteit "Remote Access orgid". Als u gebruikers-/groepsidentificatie wilt toevoegen, hebt u twee opties:

- Installeer onze AnyConnect Umbrella Roaming Security-module en schakel de functie SWG Agent in. De agent verzendt webverkeer rechtstreeks naar Umbrella SWG met de identiteit "Roaming Computer" toegepast. Deze module ondersteunt ook optionele gebruikersidentificatie voor AD.
- Schakel SAML in de webregelset in die van invloed is op uw identiteit voor 'Externe toegang'. Na verbinding te hebben gemaakt met externe toegang, wordt RA-gebruikers gevraagd om zich een tweede keer te verifiëren via SAML bij het genereren van webbrowserverkeer.

Opmerking: wanneer u de overkoepelende module voor AnyConnect gebruikt, kan SWG-verkeer optioneel binnen of buiten de tunnel worden verzonden, afhankelijk van uw gesplitste tunnelconfiguratie.

In dit voorbeeld wordt getoond hoe een DNS-beleid kan worden geconfigureerd (Beleid > DNS-beleid) voor een individuele AnyConnect-client. Dit is alleen mogelijk wanneer de overkoepelende AnyConnect-roamingmodule wordt geïmplementeerd:

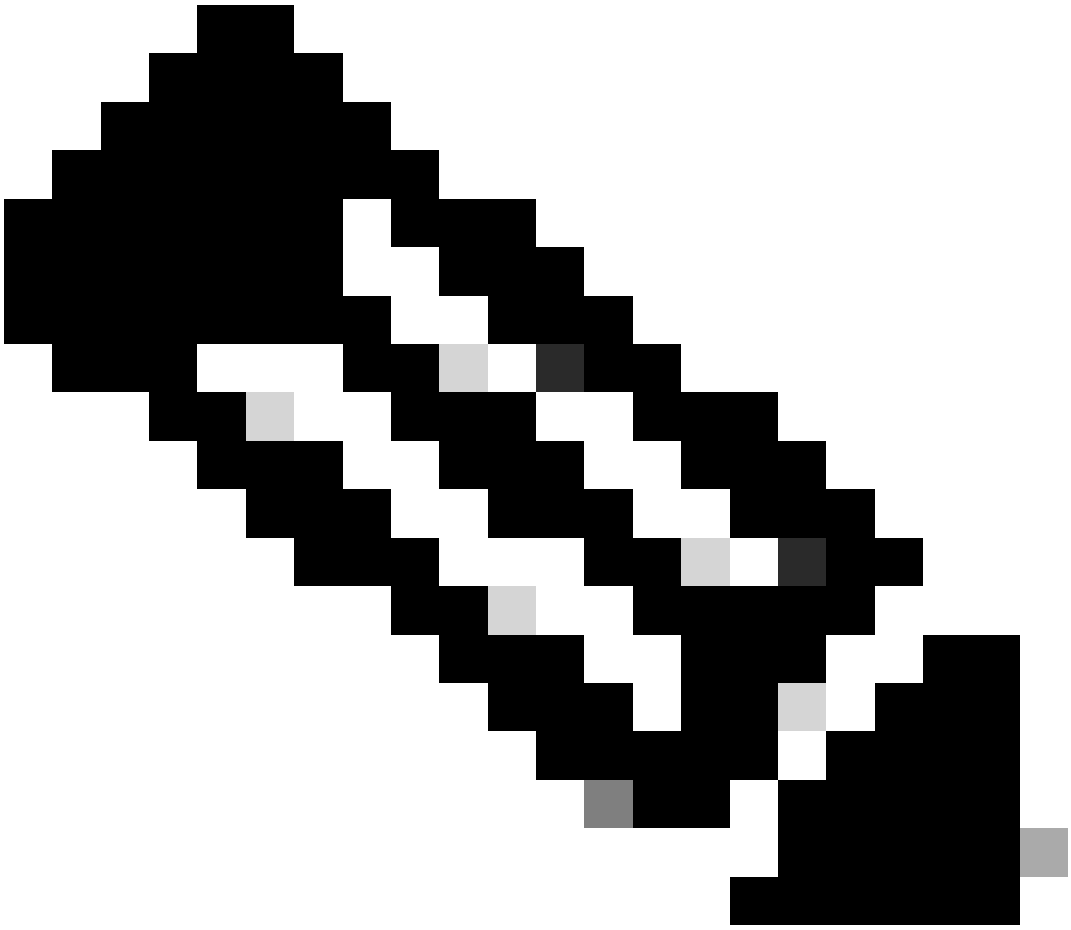


4410210499476

DLP-beleid

Het beleid voor gegevensverlies is van toepassing op het verkeer tussen de clients voor externe toegang (AnyConnect) en het internet. Configureer de regels in 'Implementaties > Beleid ter voorkoming van gegevensverlies', zoals in de documentatie die u hier vindt: Beleid voor gegevensbescherming beheren.

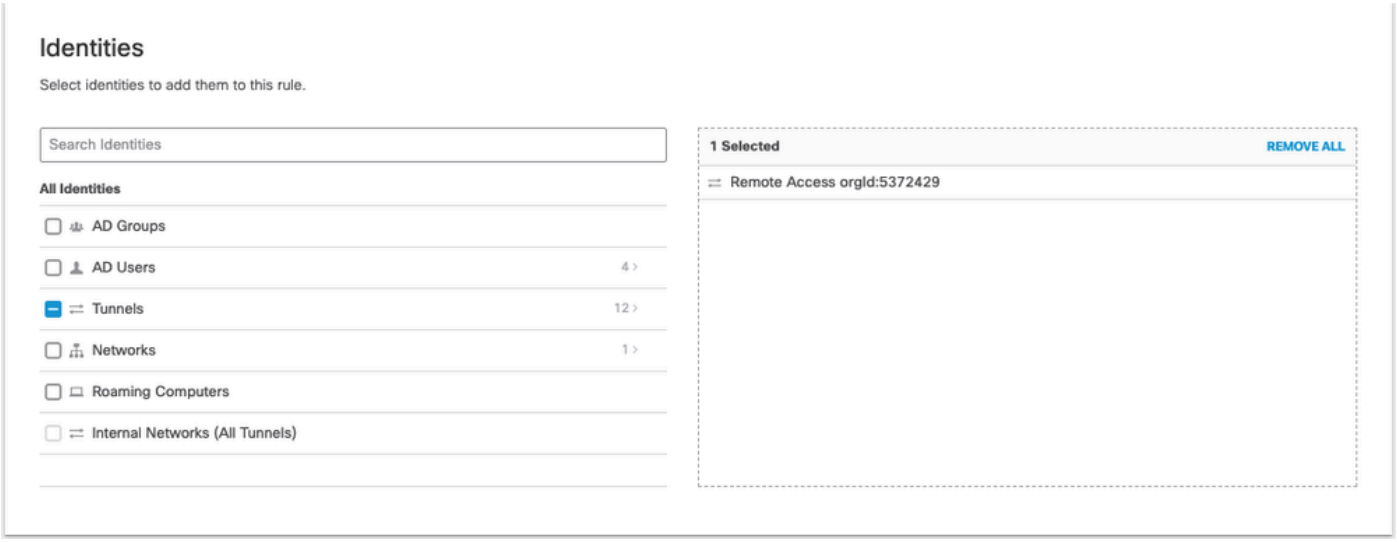
- Het DLP-beleid wordt niet gebruikt om de toegang tussen RA-clients en Private/Branch-webservers te beheren. Het DLP-beleid is alleen van toepassing op verkeer naar externe websites.



Opmerking: als u het DLP-beleid wilt toepassen, moet u eerst een webregelset voor gebruikers met externe toegang hebben gemaakt. De webregelset moet HTTPS-decodering hebben ingeschakeld.

Kies bij het selecteren van identiteiten voor een regel voor gegevensbescherming Externe toegang of id:<ID>. Hetzelfde gegevensbeschermingsbeleid is van toepassing op alle gebruikers.

Als u de DLP-regel wilt voltooien, moet u ook DLP-classificatoren selecteren of definiëren.



4409322428820

DLP-gebruikersidentificatie

DLP krijgt gebruikersidentiteit van de beveiligde webgateway (webbeleid). Raadpleeg het gedeelte Webbeleid voor instructies voor het toevoegen van gebruikersidentificatie.

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.