Probleemoplossing voor Secure Access Decryptie en Inbraakpreventiesysteem (IPS)

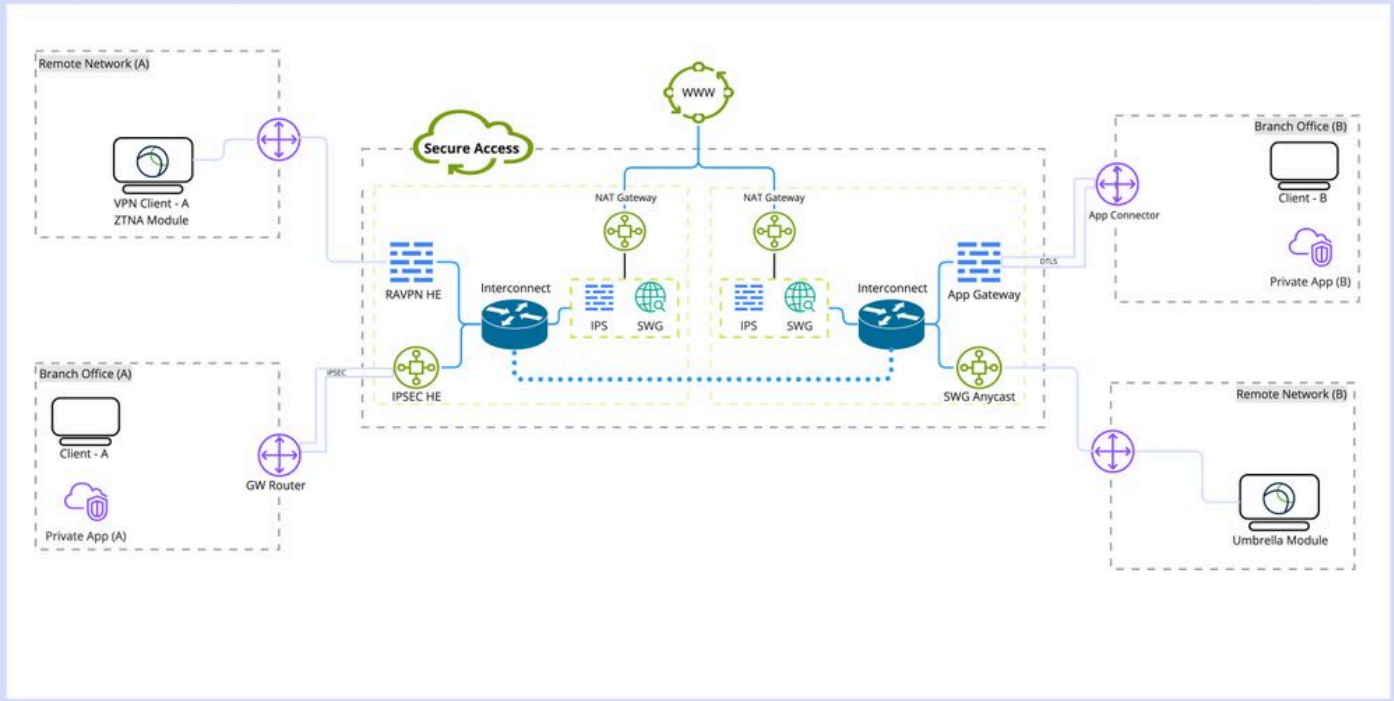
Inhoud

Inleiding

Dit document beschrijft de Secure Access Decryptie en IPS-workflow en markeert belangrijke instellingen en eigenschappen.

Secure Access-architectuur

Deze Secure Access-architectuur benadrukt de verschillende services die worden geleverd door Secure Access en verschillende verbindingsmethoden die kunnen worden ingesteld om het netwerk te beveiligen.



Secure Access-architectuur

Architectuurgegevens:

Termen om bekend te zijn met:

RAVPN HE: Remote Access Virtual Private Network - head-end

IPSEC HE: IPSEC Head-end (Remote Tunnel Internet Protocol Security)

ZTNA-module: netwerktoegangsmodule met nul vertrouwen

SWG: beveiligde webgateway

IPS: inbraakpreventiesysteem

NAT-gateway: gateway voor netwerkadresomzetting

SWG AnyCast: Secure Web Gateway-anycastingtoegangspunt

Implementatietypen:

1. Externe toegang tot VPN

2. Tunnel voor externe toegang

3. Umbrella-roamingmodule

4. Application Connector/Toepassingsgateway

5. Nulvertrouwensmodule (ZTNA)

Overzicht van functies

Secure Access biedt de mogelijkheid om zowel Web Decryption als Inbraakpreventiesysteem (IPS) te doen om de toepassingsdetectie en -categorisering te verbeteren en meer details over het verkeer te bieden. inclusief URL-paden, bestandsnamen en hun toepassingscategorie. en om aanvallen op nul dagen en malwares te voorkomen.

Decryptie: In dit artikel wordt de decryptie verwezen naar HTTPS-verkeer (Decrypting Hyper Text Transfer Protocol) via Secure Web Gateway (SWG)-module. en naar IPS-inspectie: decryptie van verkeer.

IPS: Inbraakdetectiesysteem op firewallniveau dat decryptie voor verkeer vereist om volledige functionaliteit te kunnen uitvoeren.

De decryptie is nodig voor meerdere Secure Access-functies, zoals DLP (Data Loss Prevention) en Remote Browser Isolation (RBI), bestandsinspectie, bestandsanalyse en bestandsblokkering.

Instellingen voor decryptie en IPS in beveiligde toegang

Dit is een snel overzicht van beschikbare instellingen voor decryptie en IPS in Secure Access.

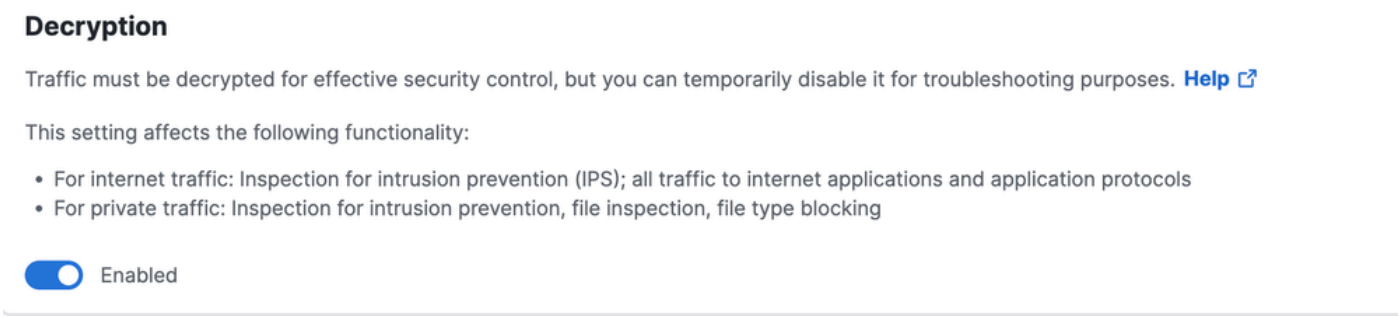
Decryptie voor IPS

Dit is een algemene instelling voor IPS die wordt gebruikt om IPS-engine voor alle beleidsgebieden uit te schakelen of in te schakelen.

Eigenschappen:

- Deze optie heeft geen invloed op de Secure Web Gateway-decryptie (webdecryptie)
- Het uitschakelen en inschakelen van IPS per beleid is beschikbaar met beperkte functionaliteit om alleen de eerste fase van de handdruk te inspecteren zonder de inhoud van het verzoek te inspecteren.

Configuratie: Dashboard -> Beveiligd -> Toegangsbeleid -> Standaardwaarden en wereldwijde instellingen voor regels -> Wereldwijde instellingen -> Decryptie voor IPS



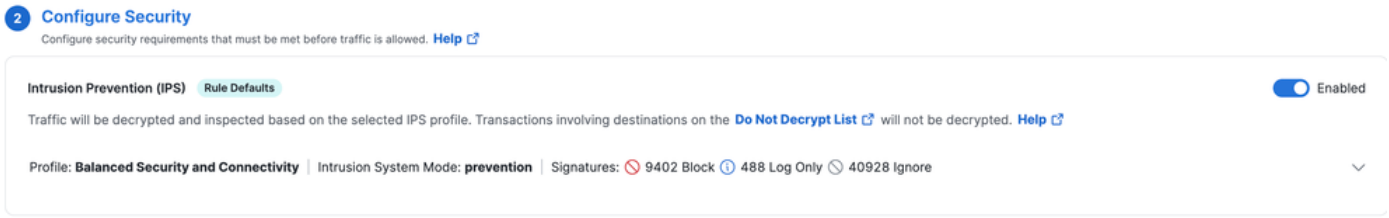
IPS-instellingen per beleid

Met deze optie kunt u IPS per beleidsbasis uitschakelen en inschakelen.

Eigenschappen:

- Deze optie bepaalt of IPS per beleid is ingeschakeld of uitgeschakeld.
- Deze optie is afhankelijk van decrypt voor IPS-instellingen, als de globale optie Decrypt voor IPS uitgeschakeld is, veroorzaakt het dat het gedrag alleen de eerste fase van de handdruk inspecteert zonder de inhoud van het verzoek te inspecteren.
- Deze optie heeft geen invloed op SWG (Web decryption)

Configuratie: Dashboard -> Beveiligd -> Toegangsbeleid ->Bewerkingsbeleid -> Beveiliging configureren -> Inbraakpreventie (IPS)



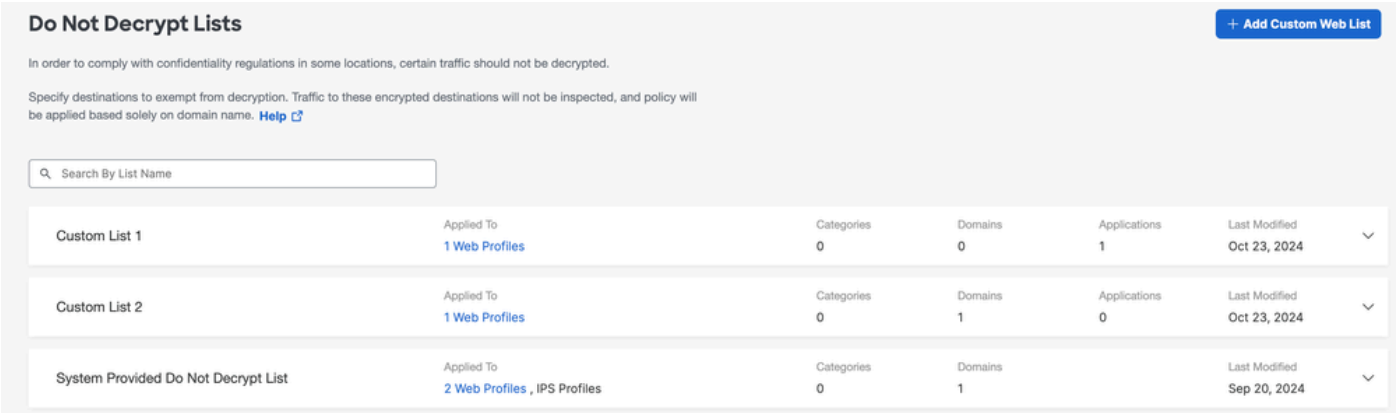
Niet ontsleutelen aan lijsten

Een set van doellijsten die kunnen worden gekoppeld aan een beveiligingsprofiel om te voorkomen dat domeinen of IP-adressen worden gedecodeerd.

Eigenschappen:

- Toestaan dat aangepaste domeinen worden omzeild voor webdecryptie
- Deze lijst heeft alleen invloed op webdecryptie en niet op IPS met uitzondering van het geleverde systeem niet decrypteren
- Bevat een (meegeleverd systeem niet decrypteert lijst) dat zowel IPS als webdecryptie omzeilt
- Deze optie moet worden gecombineerd met beveiligingsprofielen die aan het beleid moeten worden toegevoegd
- Deze lijst kan alleen worden gebruikt als decryptie is ingeschakeld in het beveiligingsprofiel

Configuratie: Dashboard -> Beveiligd -> Niet-decoderen lijsten



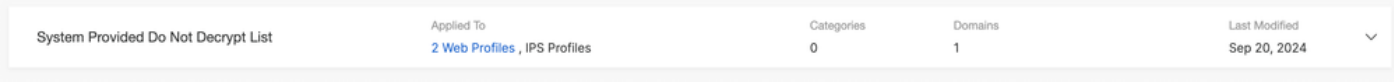
Verstrekt systeem decrypteert geen lijst

Een deel van Do Not Decrypt-lijsten, met extra functie voor het toepassen op zowel Decryptie als IPS in Secure Access.

Eigenschappen:

- Dit is de enige aangepaste lijst Niet ontsleutelen die van invloed is op zowel IPS als webdecryptie
- Deze lijst kan niet per beleid worden aangepast.

Configuratie: Dashboard -> Beveiligd -> Geen coderingslijsten decrypteren -> Verstrekte systeem niet decoderen



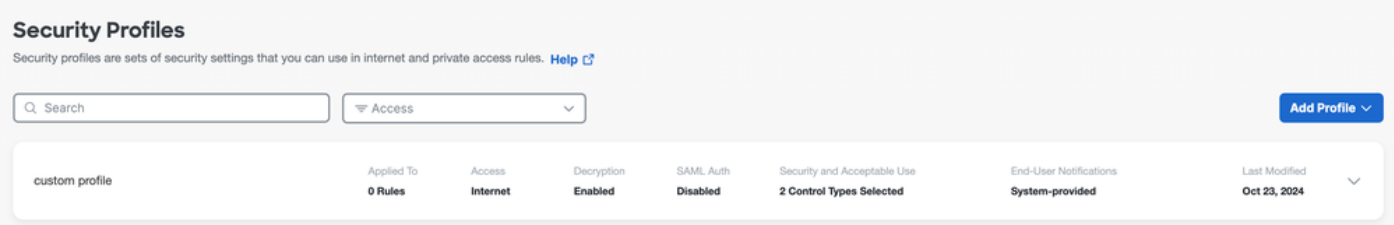
Instellingen beveiligingsprofiel

In de instellingen van het Beveiligingsprofiel kunt u Webdecryptie in- of uitschakelen die later aan een Internetbeleid kan worden gekoppeld. Als de optie Decryptie is ingeschakeld, kunt u een van de geconfigureerde Do Not Decrypt-lijsten selecteren.

Eigenschappen:

- Bestuurt verschillende beveiligingsfuncties, waaronder Web Decryptie en Do Not Decrypt Lists
- Op het systeem aangesloten niet-decryptie lijst niet naar het beveiligingsprofiel versleutelen heeft invloed op zowel webdecryptie als IPS-decryptie

Configuratie: Dashboard -> Veilig -> Beveiligingsprofielen



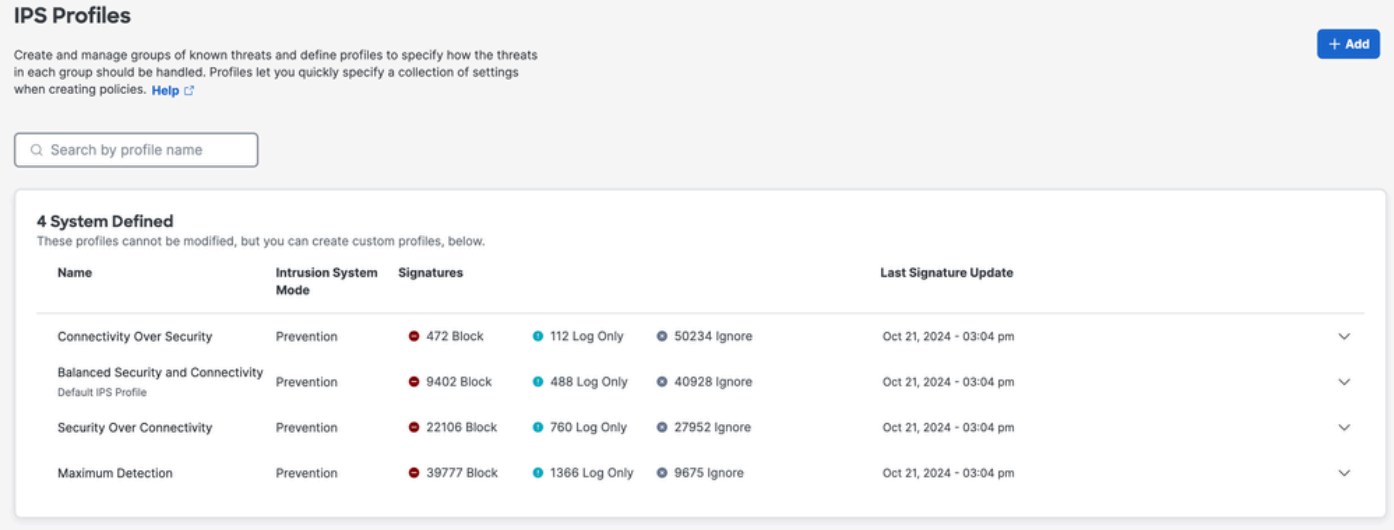
IPS-profielen

De instellingen van IPS-profielen omvatten vier hoofdvooraf gedefinieerde beveiligingsinstellingen voor het IPS-profiel. Welke instellingen kunnen worden geselecteerd per Beleidsinstellingen. U hebt de optie om uw eigen aangepaste IPS-profiel te maken voor striktere of flexibele instellingen.

Eigenschappen:

- Bevat vier vooraf gedefinieerde profielen van beveiligingsniveaus voor IPS
- U kunt een aangepast IPS-profiel maken

Configuratie: Dashboard -> Beveiligd -> IPS-profielen

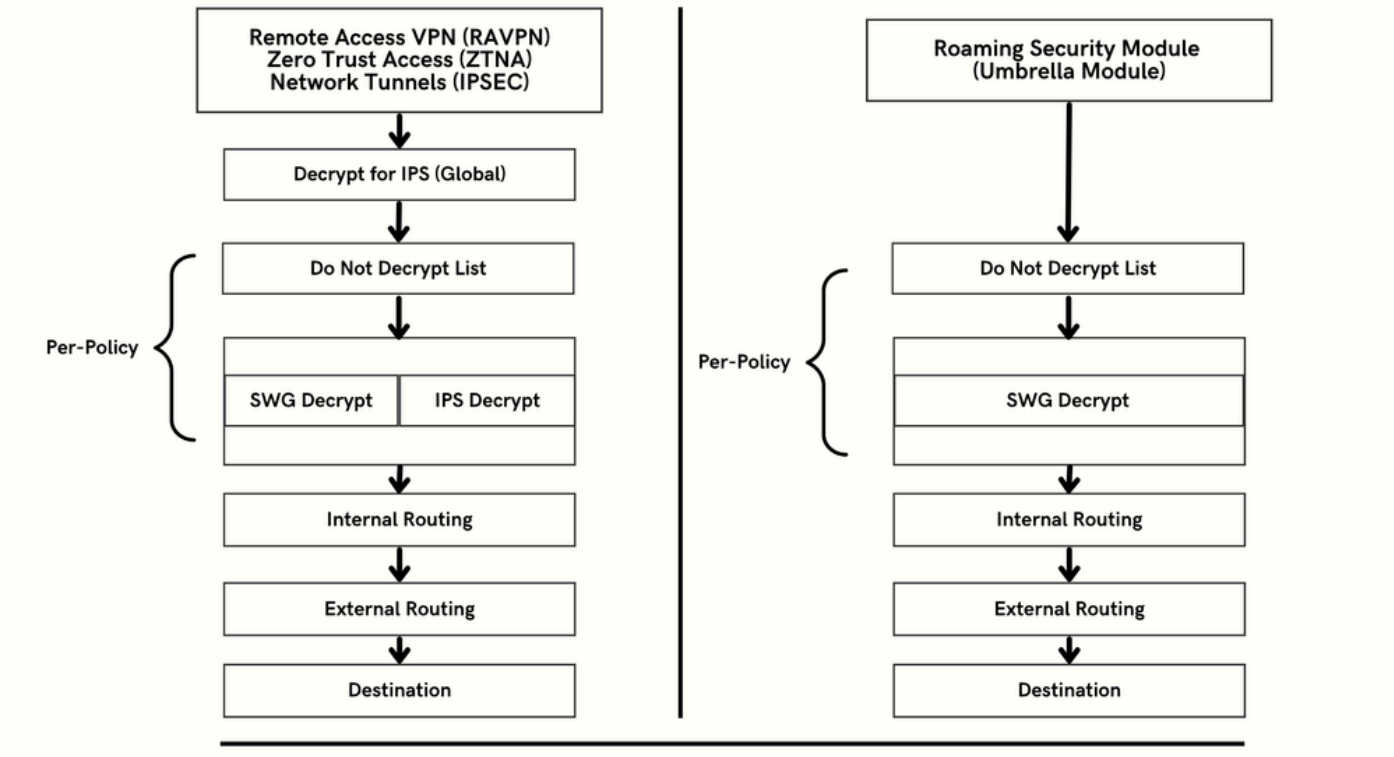


HTTP-verkeersstroom in beveiligde toegang

Secure Access heeft verschillende verkeerspaden op basis van de verbindingsmethode.

Remote Access VPN (RAVPN) en Zero Trust Access (ZTNA) delen dezelfde componenten.

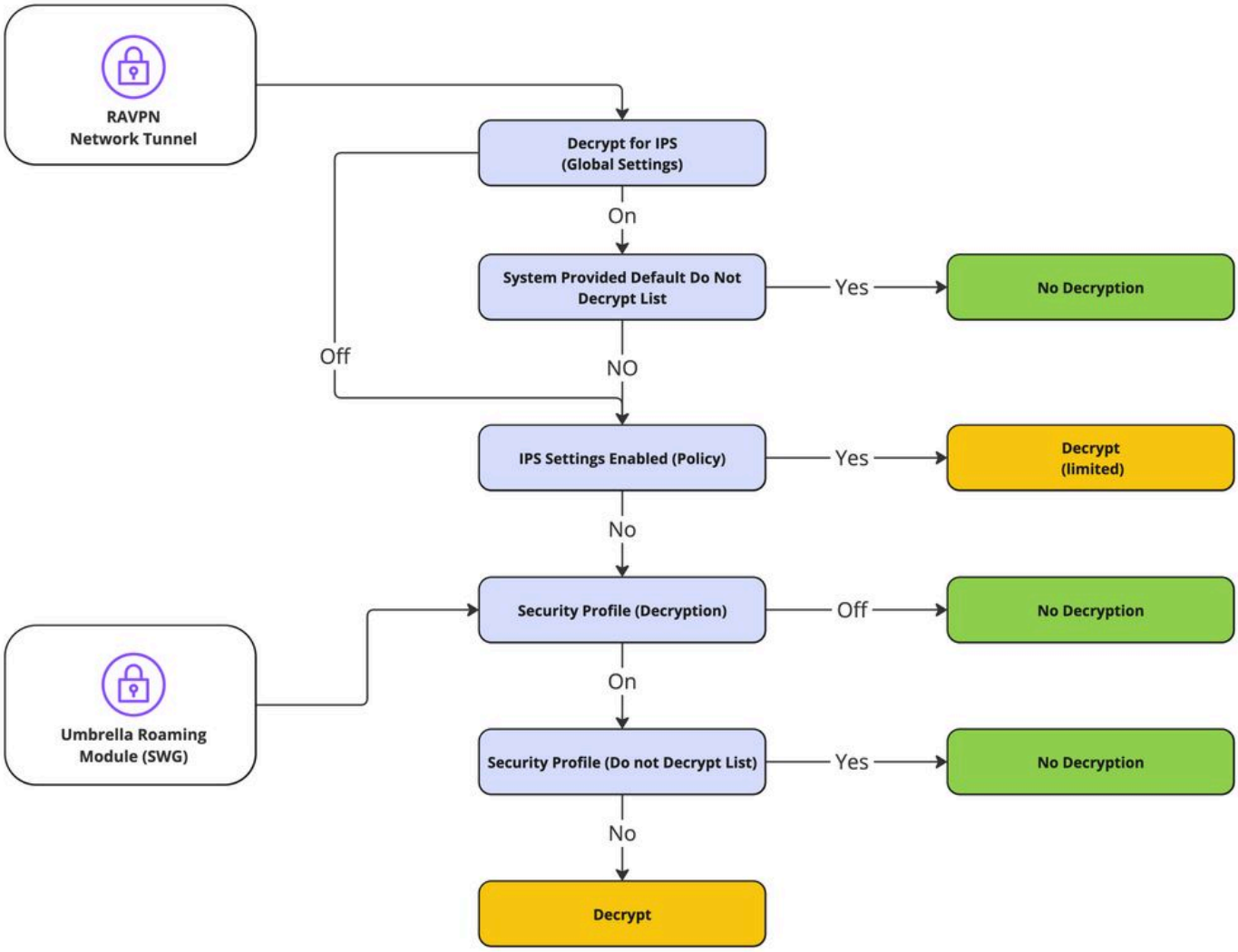
Roamingbeveiligingsmodule (Umbrella Module) heeft een ander verkeerspad.



Wanneer kan worden verwacht dat verkeer wordt gedecrypteerd

In dit gedeelte wordt de keten van acties en de belangrijkste resultaten van decryptie of niet-

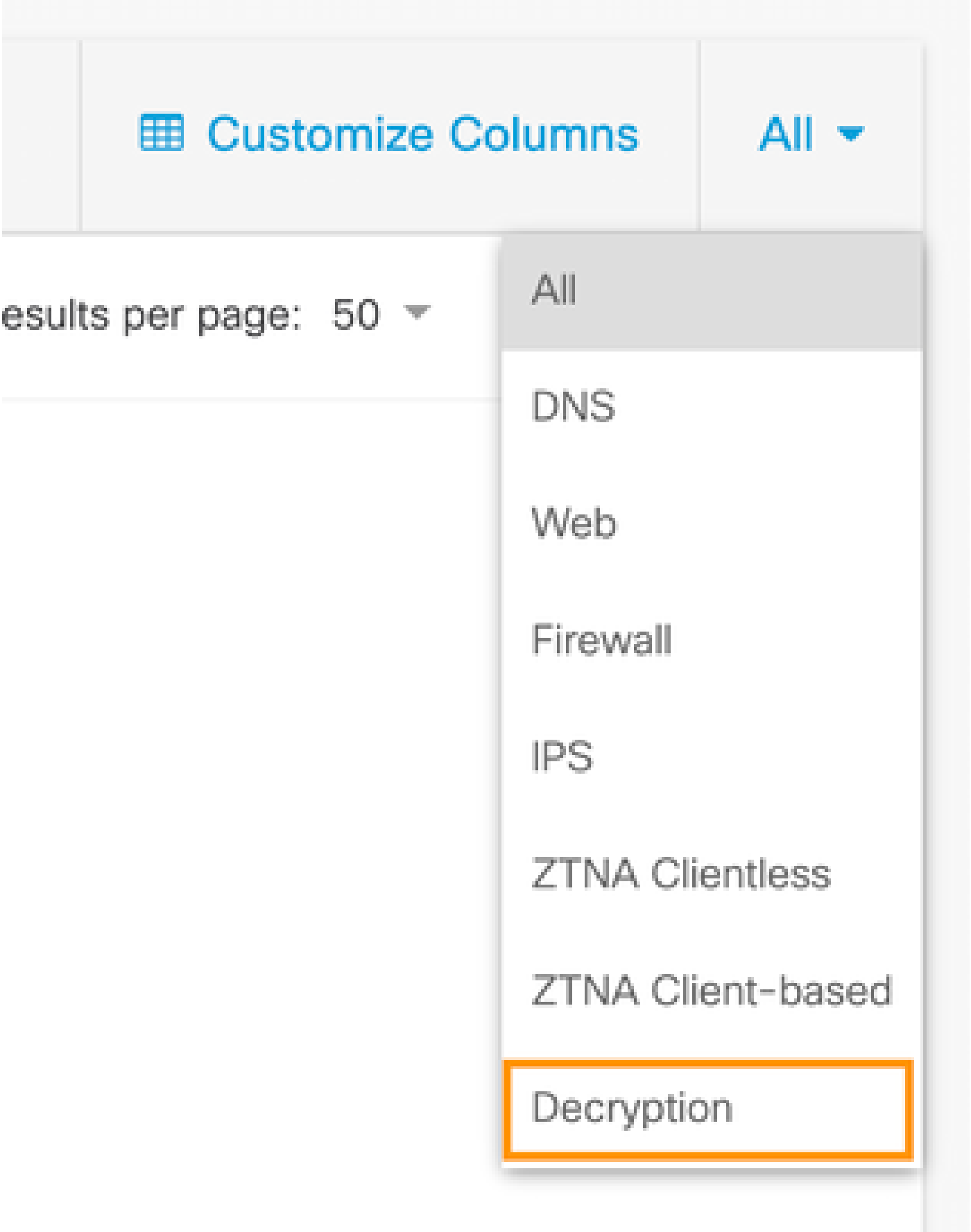
decryptie uitvoerig toegelicht.

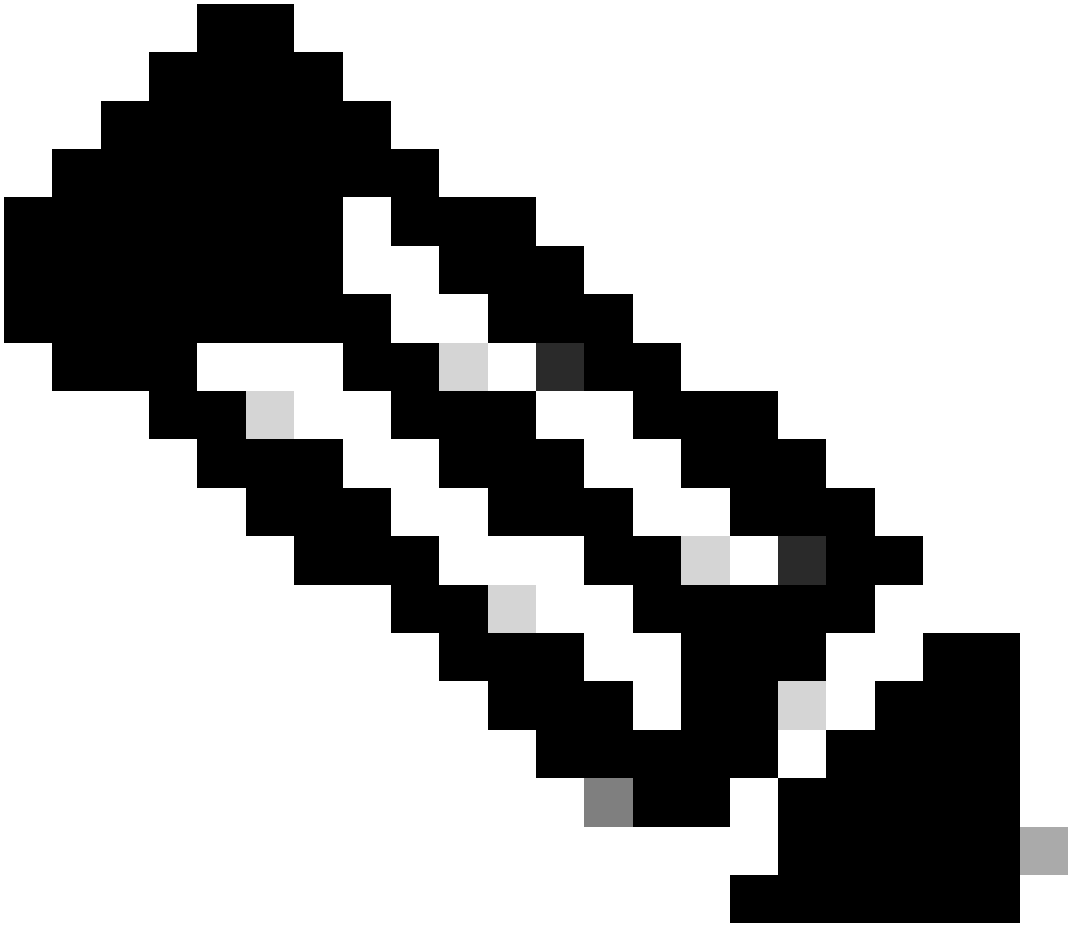


Decryptie Flow

Vastlegging en rapportage in verband met decryptie en IPS

Secure Access bevat nieuwe rapportage-sectie (decryptie) die toegankelijk is via Dashboard -> Monitor -> Zoeken naar activiteiten -> Switch voor decryptie.

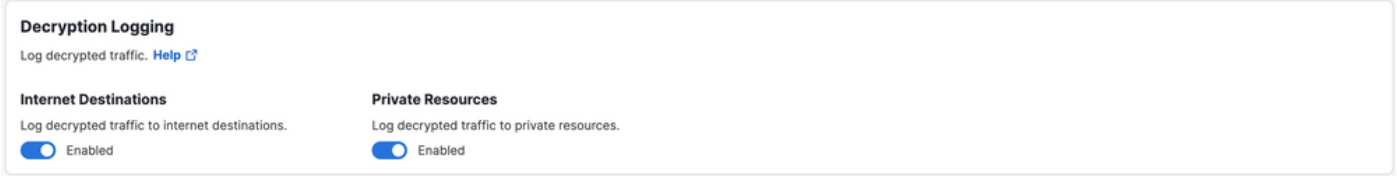

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



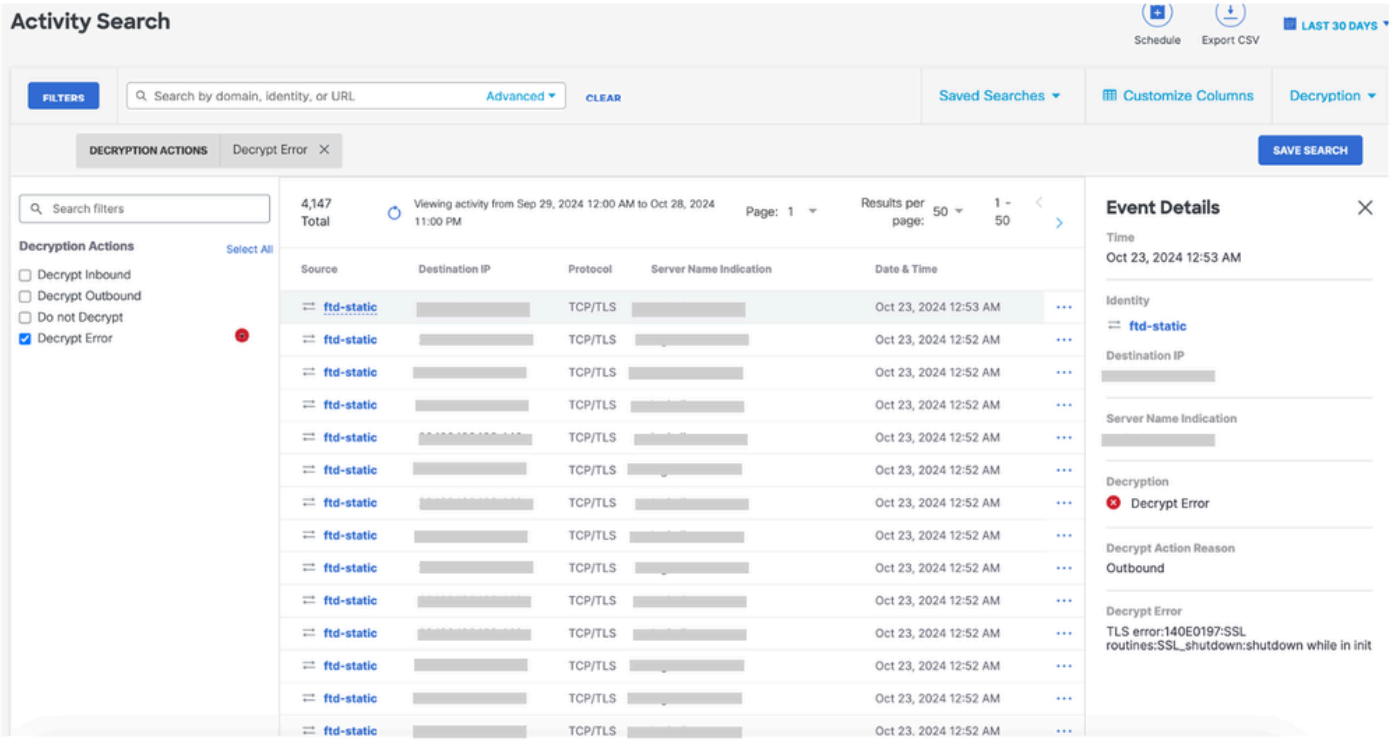
Opmerking: om decryptie logbestanden in te schakelen, kan deze instelling worden ingeschakeld voor wereldwijde instellingen:

Dashboard -> Beveiligd -> Toegangsbeleid -> Standaardwaarden en wereldwijde instellingen voor regels -> Wereldwijde instellingen -> Vastlegging decryptie.

Instellingen voor decryptie-vastlegging:



Voorbeeld van decryptie fout:



Gerelateerde informatie

- [Gebruikershandleiding voor Secure Access]
- [Technische ondersteuning en downloads – Cisco Systems]

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.