Dépannage du workflow du système de décodage et de prévention des intrusions (IPS) à accès sécurisé

Table des matières

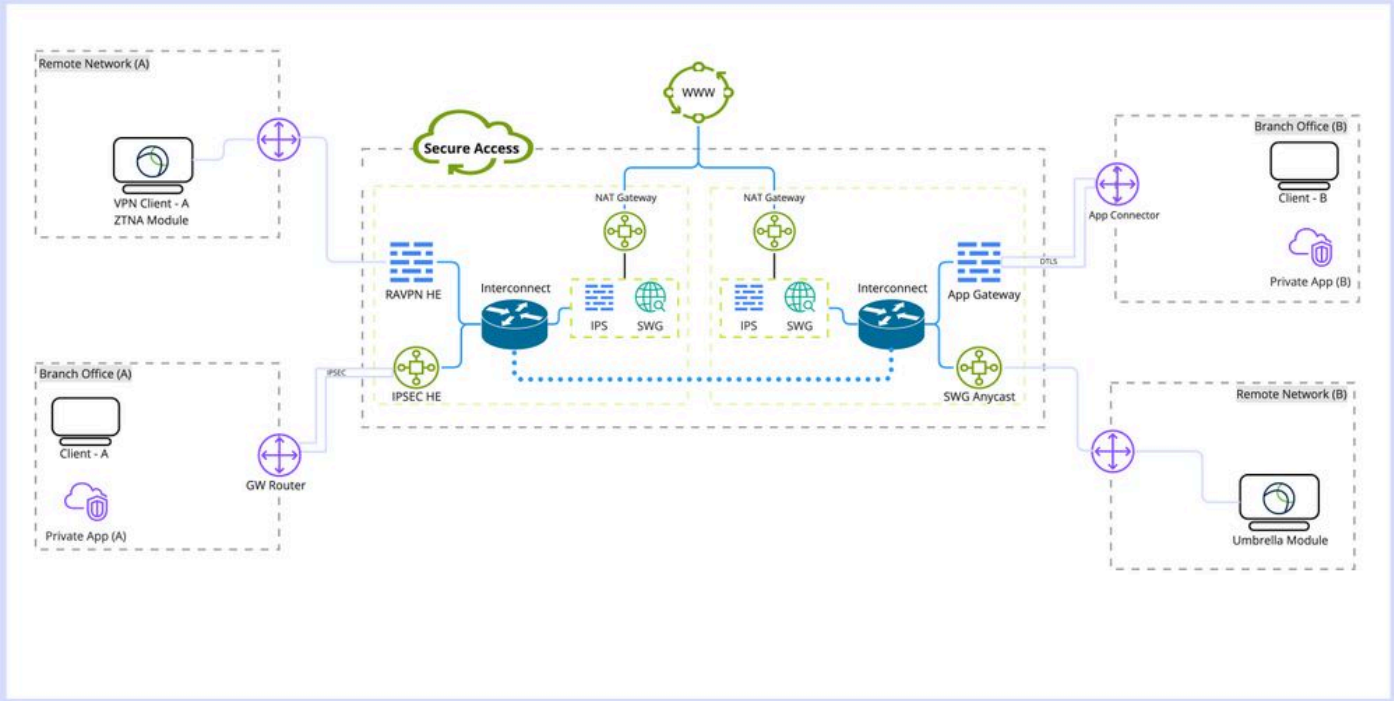
- Introduction
- Architecture d'accès sécurisé
- Présentation des fonctionnalités
- Paramètres relatifs au décodage et à IPS dans Secure Access
  - Déchiffrement pour IPS
  - Paramètres IPS par stratégie
  - Ne pas déchiffrer les listes
  - Liste Ne Pas Déchiffrer Fournie Par Le Système
  - Paramètres du profil de sécurité
  - Profils IPS
- Flux de trafic HTTPS dans l'accès sécurisé
- Quand attendre le décodage du trafic
- Déchiffrement et consignation et création de rapports liés à IPS
- Informations connexes

Introduction

Ce document décrit le flux de travail Secure Access Decryption et IPS et met en évidence les propriétés importantes des paramètres.

Architecture d'accès sécurisé

Cette architecture d'accès sécurisé met en évidence les différents services fournis par l'accès sécurisé et les différentes méthodes de connexion pouvant être établies pour sécuriser le réseau.



Architecture d'accès sécurisé

Détails d'architecture :

Termes à connaître :

RAVPN HE : tête de réseau privé virtuel à accès distant

IPSEC HE : tête de réseau IPSEC (Remote Tunnel Internet Protocol Security)

Module ZTNA : module d'accès au réseau Zero Trust

SWG : passerelle Web sécurisée

IPS : système de prévention des intrusions

Passerelle NAT : Passerelle de traduction d'adresses réseau

SWG AnyCast : point d'entrée Anycast Secure Web Gateway

Types de déploiement :

1. VPN d'accès à distance

2. Tunnel d’accès à distance

3. Module d’itinérance Umbrella

4. Connecteur d'application/passerelle d'application

5. ZTNA (Zero Trust Module)

Présentation des fonctionnalités

L'accès sécurisé offre la possibilité d'effectuer à la fois le décryptage Web et le système de prévention des intrusions (IPS) pour améliorer la détection et la catégorisation des applications et fournir plus de détails sur le trafic, y compris les chemins d'URL, les noms de fichiers et leur catégorie d'application. et aide à prévenir les attaques de type « zero-day » et les programmes malveillants.

Décryptage : dans cet article, le décryptage porte sur le décryptage du trafic HTTPS (Hyper Text Transfer Protocol) via le module SWG (Secure Web Gateway). et également sur le décryptage du trafic pour l'inspection IPS.

IPS : système de prévention et de détection des intrusions au niveau du pare-feu qui nécessite un décodage pour le trafic afin d'exécuter toutes les fonctionnalités.

Le déchiffrement est nécessaire pour plusieurs fonctionnalités d'accès sécurisé, telles que la prévention de perte de données (DLP) et l'isolation du navigateur distant (RBI), l'inspection des fichiers, l'analyse des fichiers et le blocage des types de fichiers.

Paramètres relatifs au décodage et à IPS dans Secure Access

Il s'agit d'une présentation rapide des paramètres disponibles relatifs au décryptage et à l'IPS dans Secure Access.

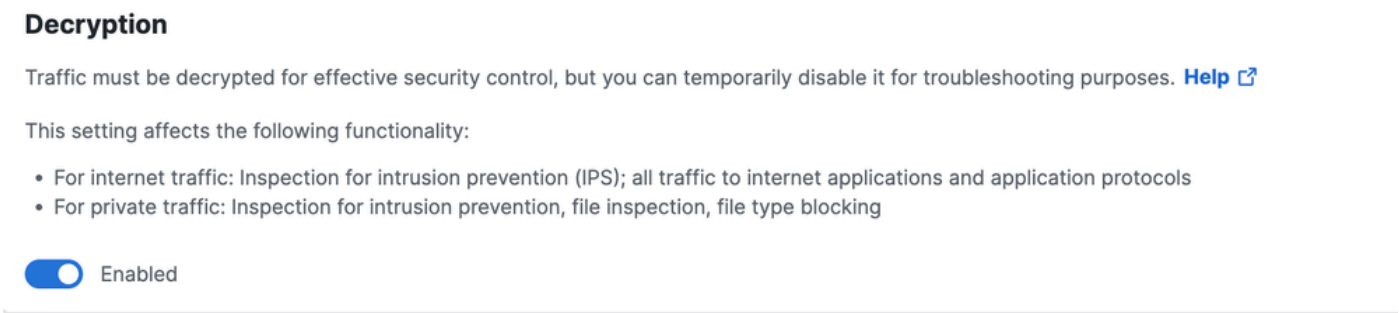
Déchiffrement pour IPS

Il s'agit d'un paramètre global pour IPS qui est utilisé pour désactiver ou activer le moteur IPS pour toutes les stratégies.

Propriétés :

- Cette option n'affecte pas le décodage de la passerelle Web sécurisée (décodage Web)
- La désactivation et l'activation de l'IPS par stratégie sont disponibles avec des fonctionnalités limitées pour inspecter uniquement la phase initiale de la connexion sans inspecter le corps de la requête.

Configuration: Tableau de bord -> Sécurisé -> Stratégie d'accès -> Paramètres généraux et par défaut des règles -> Paramètres généraux -> Déchiffrement pour IPS



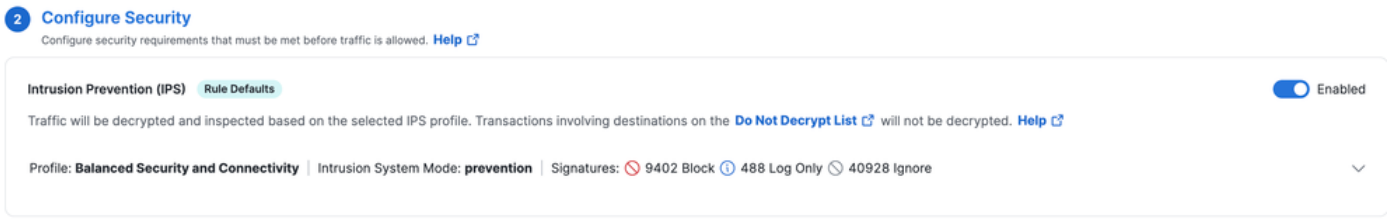
Paramètres IPS par stratégie

Cette option permet de désactiver et d'activer IPS par base de stratégie.

Propriétés :

- Cette option détermine si IPS est activé ou désactivé par stratégie.
- Cette option dépend des paramètres Decrypt for IPS. Si l'option globale Decrypt for IPS est désactivée, le comportement n'inspecte que la phase initiale de la connexion sans inspecter le corps de la requête.
- Cette option n'affecte pas SWG (Web Decryption)

Configuration : Tableau de bord -> Sécurisé -> Stratégie d'accès ->Modifier la stratégie -> Configurer la sécurité -> Prévention des intrusions (IPS)



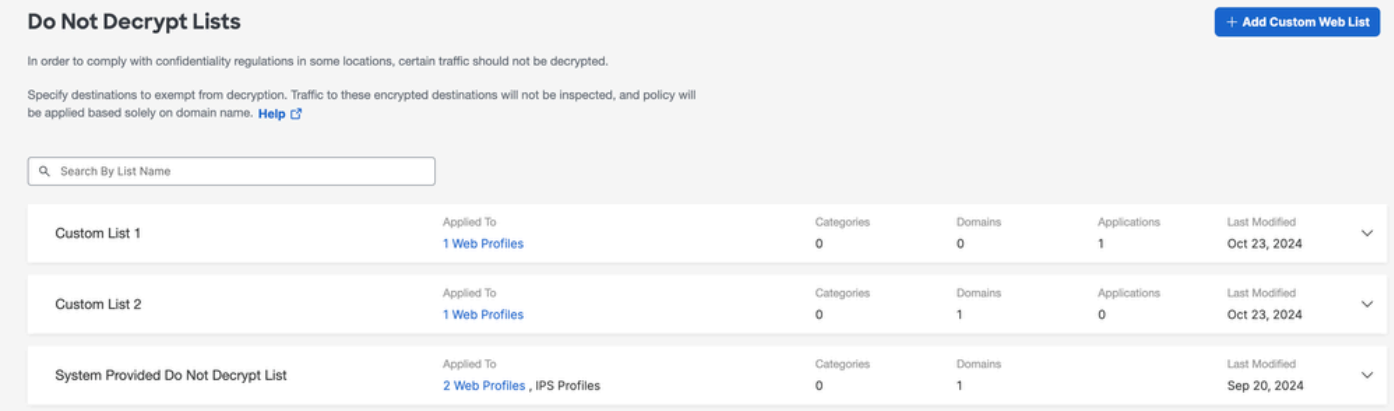
Ne pas déchiffrer les listes

Ensemble de listes de destinations pouvant être liées au profil de sécurité pour éviter le déchiffrement des domaines ou des adresses IP.

Propriétés :

- Autoriser le contournement du décodage Web des domaines personnalisés
- Cette liste affecte uniquement le décodage Web et non IPS, à l'exception de la liste de non-décodage fournie par le système
- Contient une liste (Ne pas déchiffrer fournie par le système) qui contourne à la fois IPS et le déchiffrement Web
- Cette option doit être associée à des profils de sécurité à joindre à la stratégie
- Cette liste ne peut être utilisée que si le décodage est activé dans le profil de sécurité

Configuration : Tableau de bord -> Sécurisé -> Ne pas déchiffrer les listes



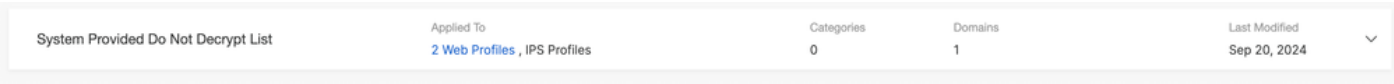
Liste Ne Pas Déchiffrer Fournie Par Le Système

Fait partie des listes Ne pas déchiffrer, avec une fonctionnalité supplémentaire d'application sur le déchiffrement et IPS dans Secure Access.

Propriétés :

- Il s'agit de la seule liste personnalisée Ne pas déchiffrer qui affecte à la fois IPS et le déchiffrement Web
- Il n'existe aucune option permettant de personnaliser cette liste par stratégie.

Configuration : Tableau de bord -> Sécurisé -> Ne pas déchiffrer les listes -> Liste fournie par le système



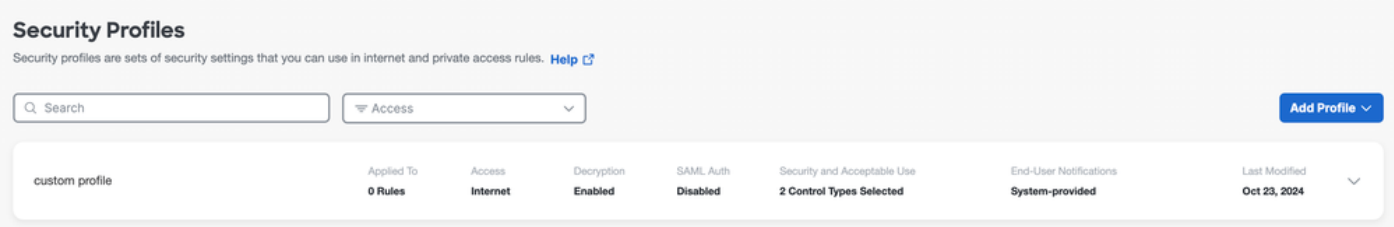
Paramètres du profil de sécurité

Dans les paramètres du profil de sécurité, vous pouvez sélectionner l'option Activation ou Désactivation du décryptage Web qui peut être associée ultérieurement à une stratégie Internet. Si le déchiffrement est activé, vous avez la possibilité de sélectionner l'une des listes Ne pas déchiffrer configurées.

Propriétés :

- Contrôle plusieurs fonctions de sécurité, notamment le décryptage Web et les listes à ne pas décrypter
- L'association de la liste de non-déchiffrement fournie par le système au profil de sécurité affecte le déchiffrement Web et le déchiffrement IPS

Configuration : Tableau de bord -> Sécurisé -> Profils de sécurité



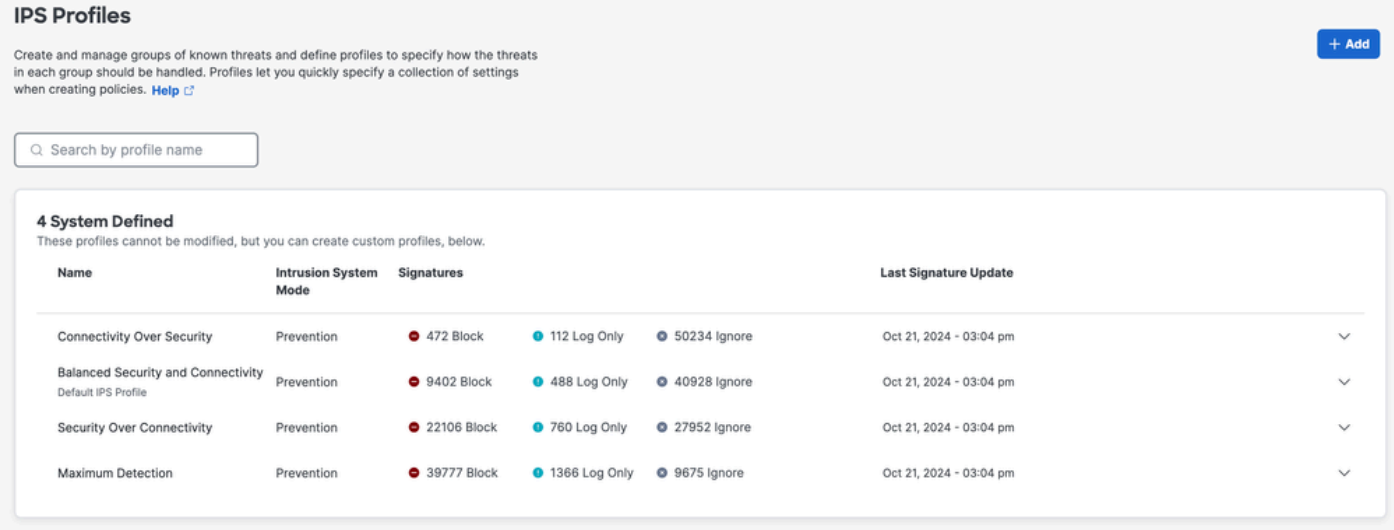
Profils IPS

Les paramètres des profils IPS incluent quatre paramètres de sécurité prédéfinis principaux pour le profil IPS. Lesquels peuvent être sélectionnés en fonction des paramètres de stratégie. Vous avez la possibilité de créer votre propre profil IPS personnalisé pour des paramètres plus stricts ou plus flexibles.

Propriétés :

- Contient quatre profils de niveaux de sécurité prédéfinis pour IPS
- Un profil IPS personnalisé peut être créé

Configuration : Tableau de bord -> Sécurisé -> Profils IPS

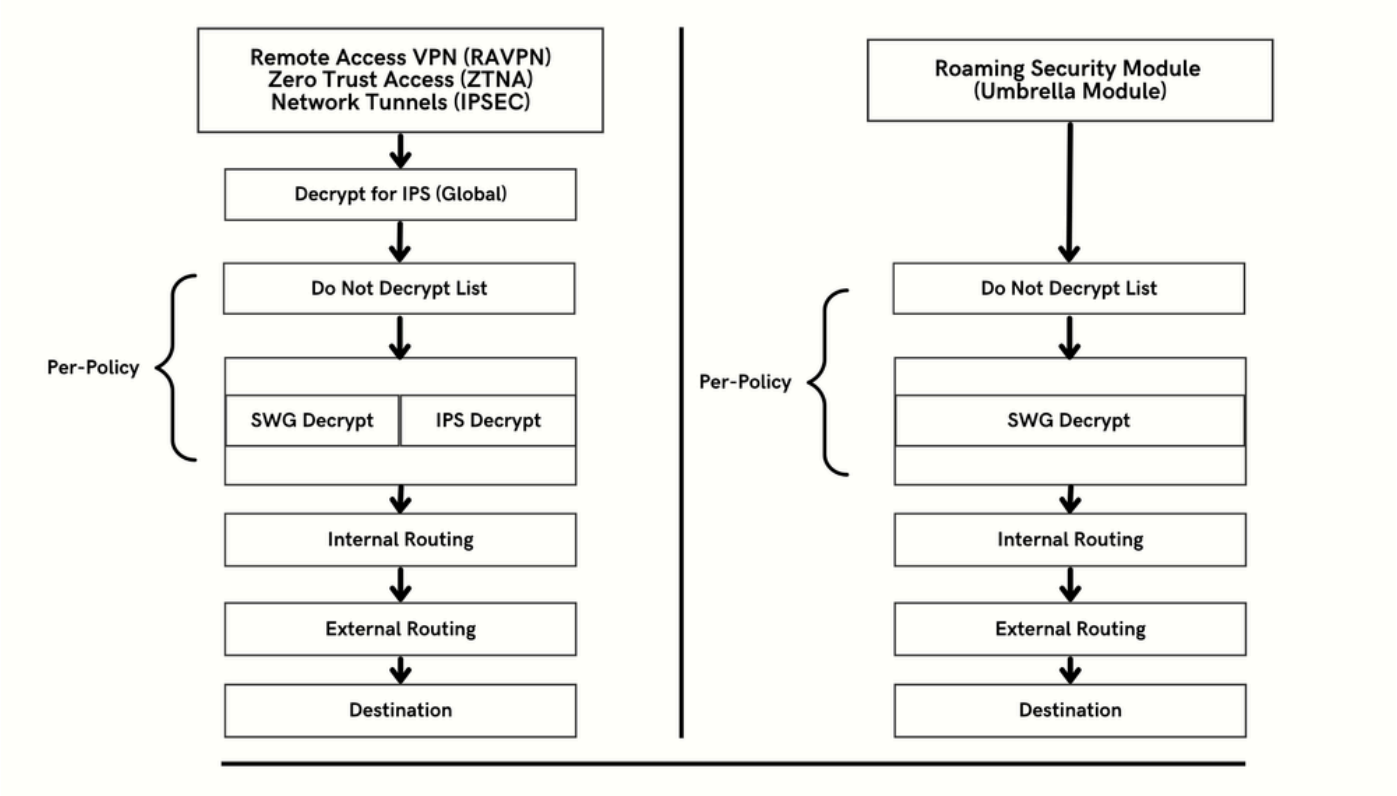


Flux de trafic HTTPS dans l'accès sécurisé

Secure Access a différents chemins de trafic basés sur la méthode de connexion.

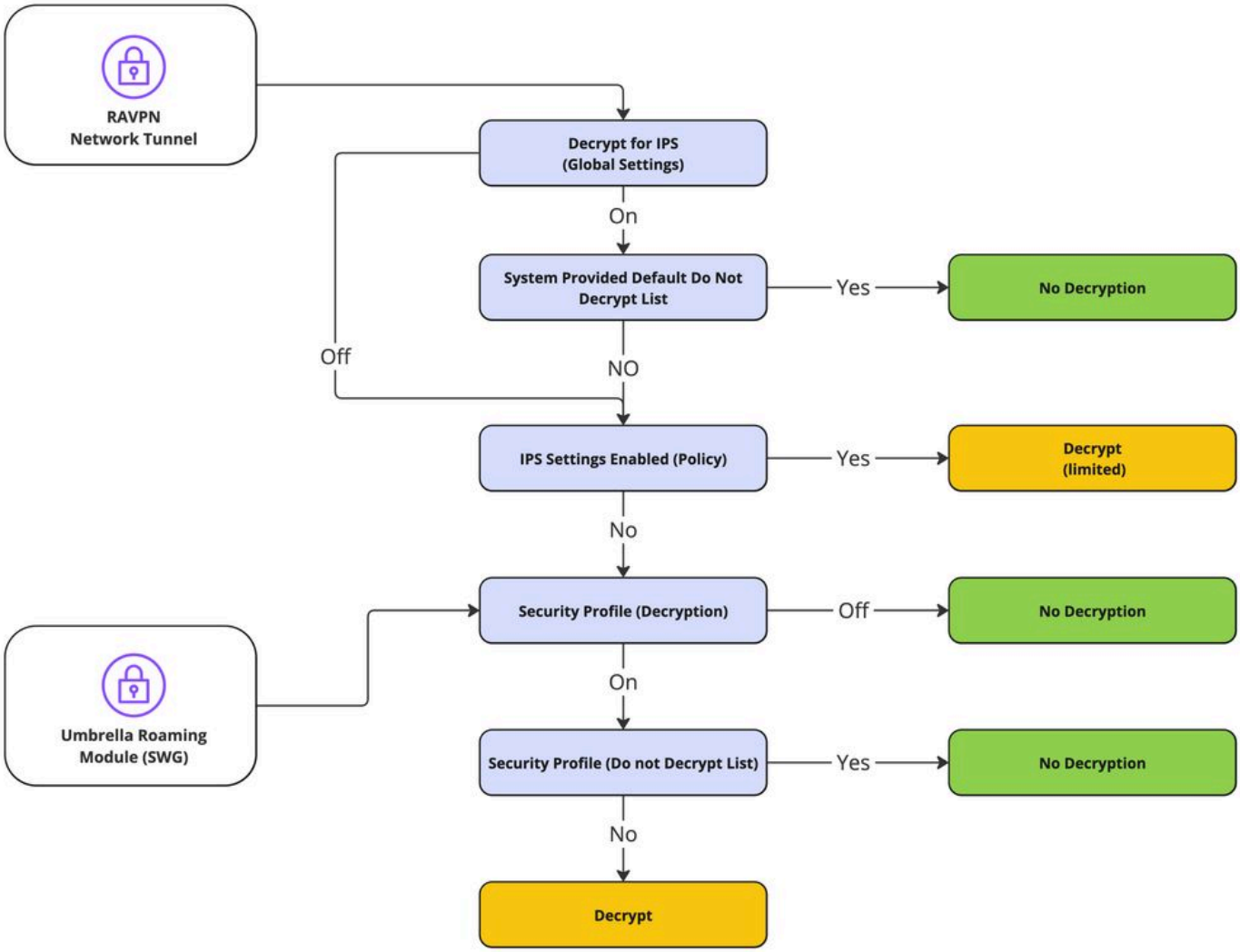
Les réseaux privés virtuels d'accès à distance (RAVPN) et ZTNA (Zero Trust Access) partagent les mêmes composants.

Les modules de sécurité d'itinérance (Umbrella Module) ont des chemins de trafic différents.



Quand attendre le décodage du trafic

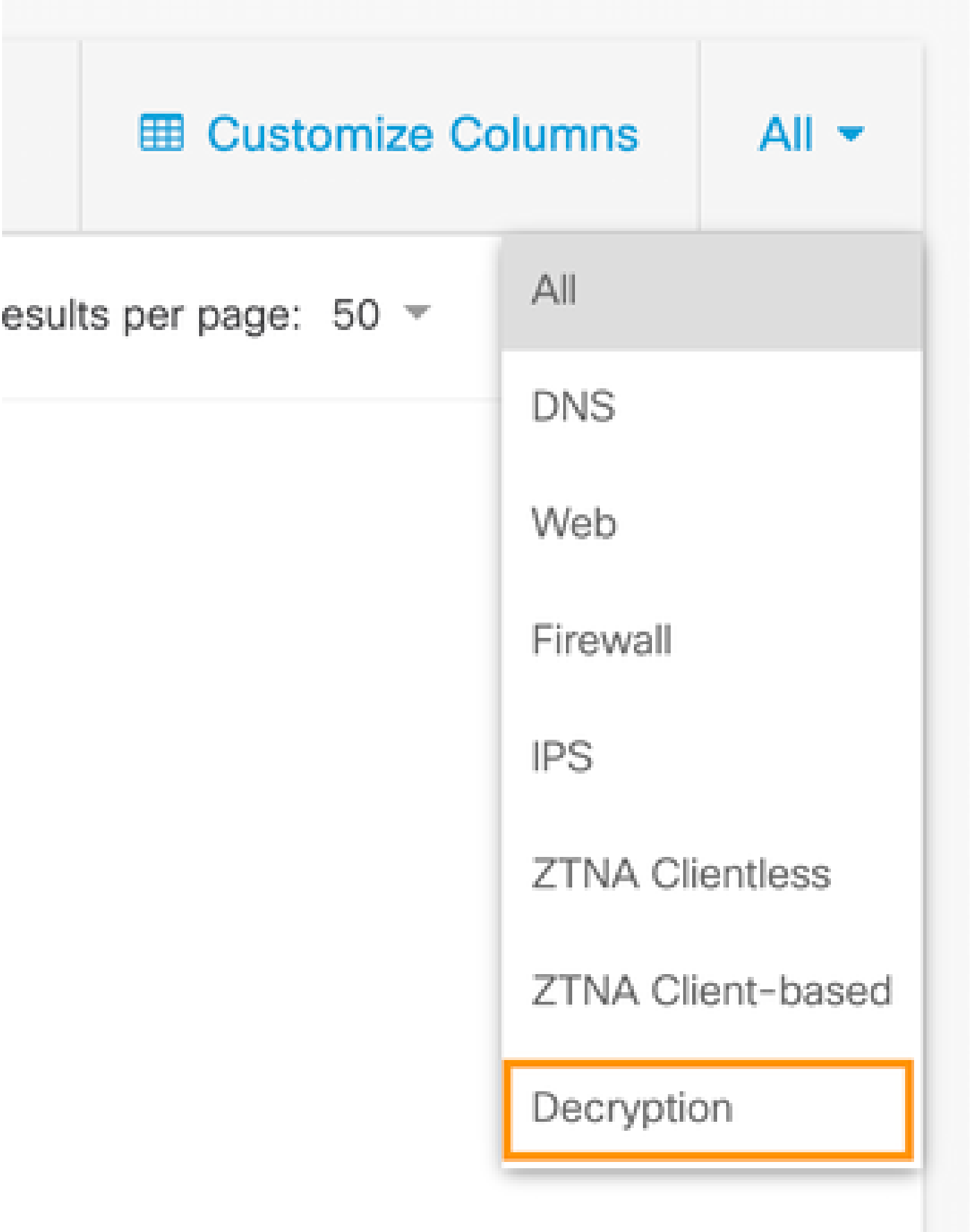
Cette section explique en détail la chaîne d'actions et leurs principaux résultats de décryptage ou d'absence de décryptage.

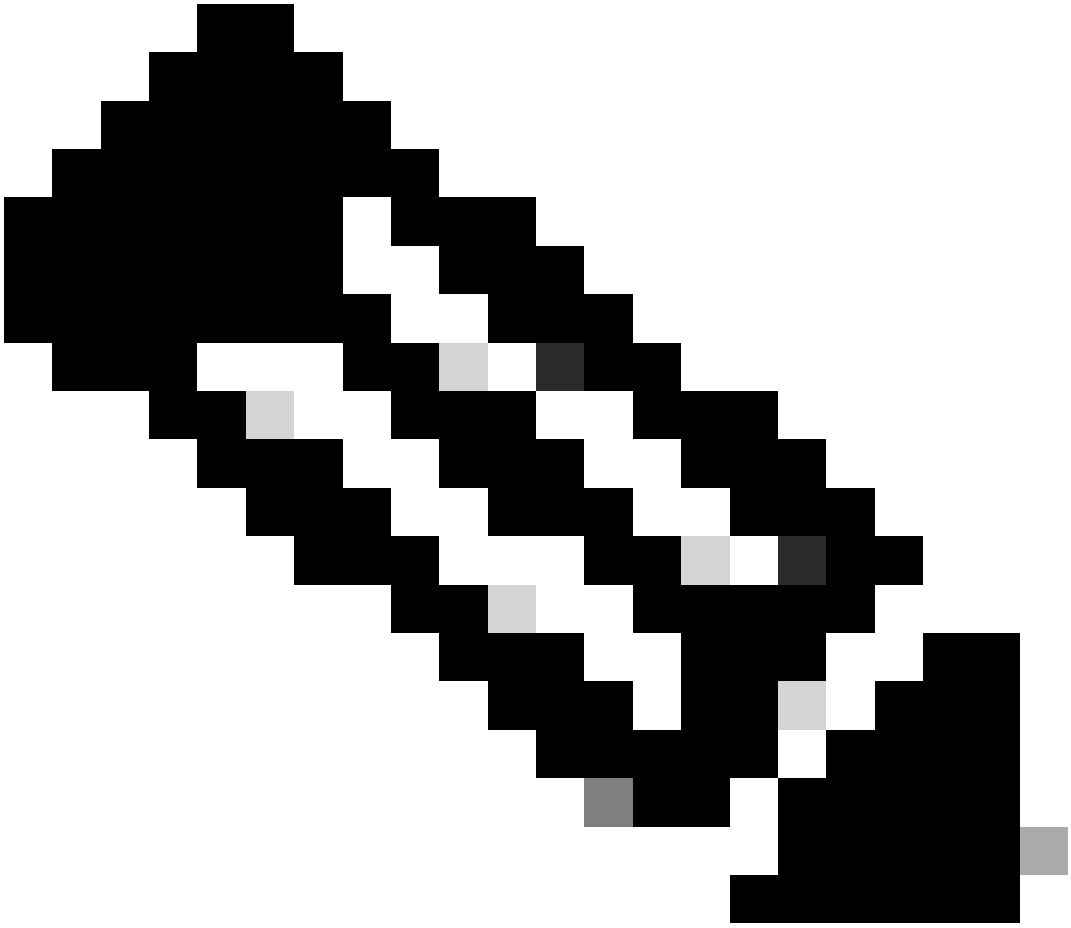


Flux de décodage

Déchiffrement et consignation et création de rapports liés à IPS

L'accès sécurisé inclut une nouvelle section de création de rapports (Décryptage) accessible via Tableau de bord -> Surveillance -> Recherche d'activité -> Passer au décryptage.

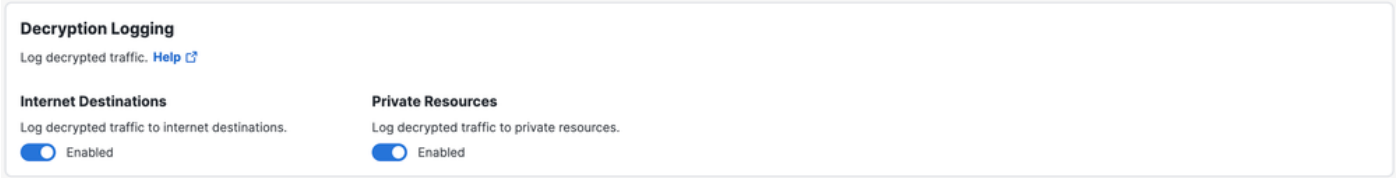

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



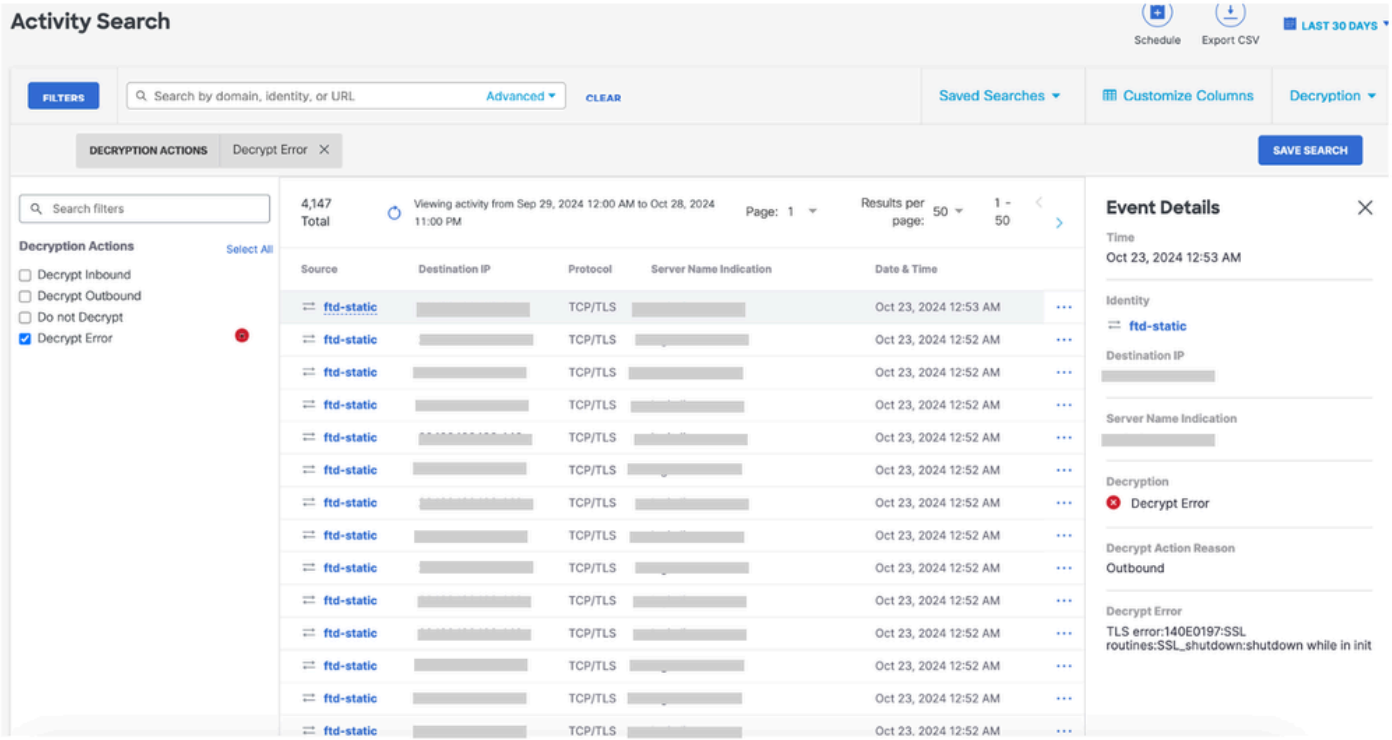
Remarque : pour activer les journaux de déchiffrement, ce paramètre peut être activé sur les paramètres globaux :

Tableau de bord -> Sécurisé -> Stratégie d'accès -> Paramètres par défaut et paramètres globaux -> Paramètres globaux -> Journalisation du décodage.

Paramètres de journalisation du décodage :



Exemple d'erreur de déchiffrement :



Informations connexes

- Guide de l'utilisateur Secure Access
- Assistance technique et téléchargements — Cisco Systems

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.