Fehlerbehebung beim sicheren IPS-Workflow (Secure Access Decryption and Intrusion Prevention System)

Inhalt

Einleitung

Architektur für sicheren Zugriff

Funktionsüberblick

Entschlüsselungs- und IPS-bezogene Einstellungen in Secure Access

- Entschlüsselung für IPS
- IPS-Einstellungen pro Richtlinie
- Listen nicht entschlüsseln
- Vom System bereitgestellte Liste nicht entschlüsseln
- Einstellungen für Sicherheitsprofile
- IPS-Profile

HTTPS-Datenverkehrsfluss in sicherem Zugriff

Wann ist mit einer Entschlüsselung des Datenverkehrs zu rechnen?

Protokollierung und Berichterstellung für Entschlüsselung und IPS

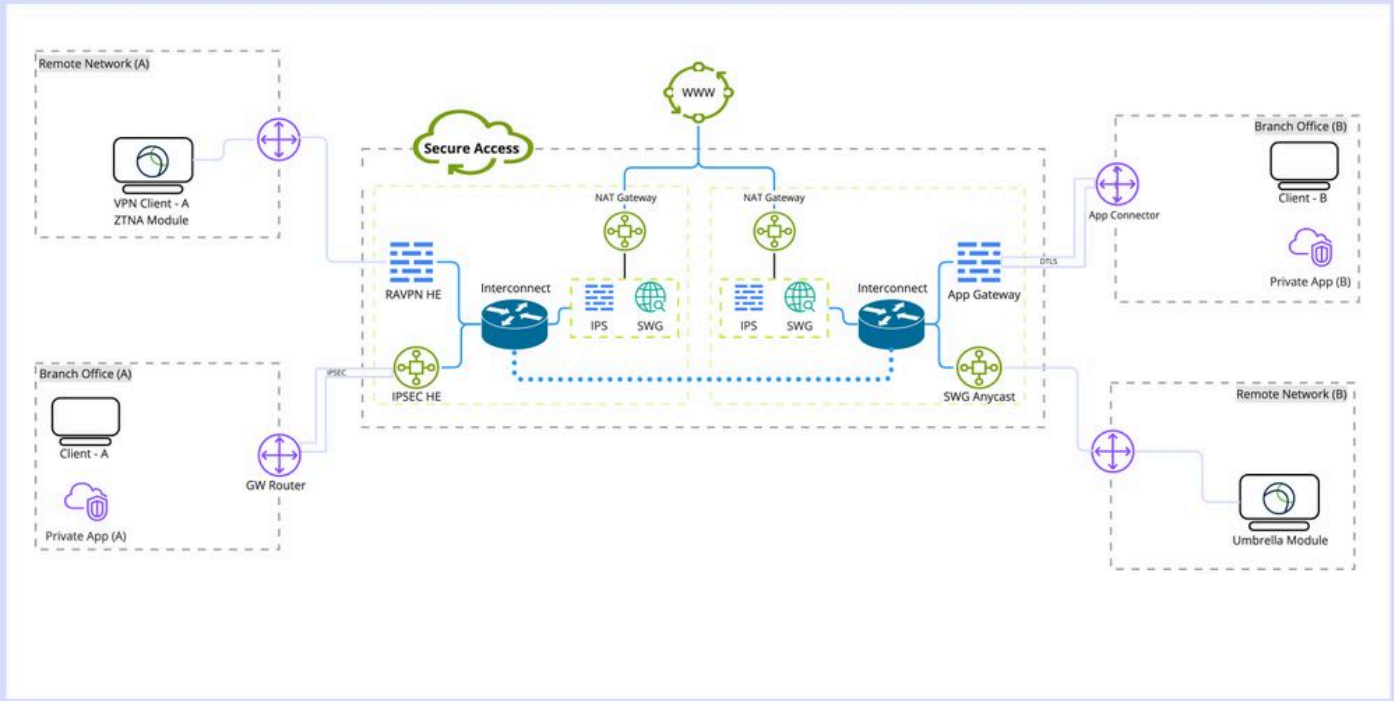
Zugehörige Informationen

Einleitung

In diesem Dokument werden der Workflow für die sichere Zugriffsentschlüsselung und das IPS beschrieben und wichtige Einstellungseigenschaften hervorgehoben.

Architektur für sicheren Zugriff

In dieser Architektur für sicheren Zugriff werden die verschiedenen Dienste von sicherem Zugriff und die verschiedenen Verbindungsmethoden hervorgehoben, die zum Sichern des Netzwerks eingerichtet werden können.



Architektur für sicheren Zugriff

Architekturdetails:

Begriffe, mit denen Sie vertraut sein müssen:

RAVPN HE: Virtual Private Network Head-End für Remote-Zugriff

IPSEC HE: Remote Tunnel Internet Protocol Security (IPSEC)-Headend

ZTNA-Modul: Netzwerkzugriffsmodul ohne Trust

SWG: Sicheres Web-Gateway

IPS: Intusion Prevention System

NAT-Gateway: Network Address Translation Gateway

SWG AnyCast: sicherer Web-Gateway-Anycast-Eingangspunkt

Bereitstellungsarten:

1. Remote Access-VPN

2. Remote-Zugriffstunnel

3. Umbrella-Roaming-Modul

4. Application Connector/Application Gateway

5. Zero Trust-Modul (ZTNA)

Funktionsüberblick

Secure Access bietet die Möglichkeit, sowohl Webentschlüsselung als auch Intrusion Prevention System (IPS) durchzuführen, um die Erkennung und Kategorisierung von Anwendungen zu verbessern und weitere Details über den Datenverkehr bereitzustellen, einschließlich URL-Pfade, Dateinamen und deren Anwendungskategorie. und um Zero-Day-Angriffe und Malware zu verhindern.

Entschlüsselung: In diesem Artikel wird die Entschlüsselung auf Entschlüsselung von Hyper Text Transfer Protocol (HTTPS)-Datenverkehr über das Secure Web Gateway (SWG)-Modul sowie Entschlüsselung von Datenverkehr für die IPS-Prüfung verwiesen.

IPS: Intrusion Detection and Prevention System auf Firewall-Ebene, das die Entschlüsselung für den Datenverkehr erfordert, um den vollen Funktionsumfang auszuführen.

Die Entschlüsselung ist für mehrere sichere Zugriffsfunktionen erforderlich, z. B. Data Loss Prevention (DLP) und Remote Browser Isolation (RBI), Dateiinspektion, Dateianalyse und Blockierung von Dateitypen.

Entschlüsselungs- und IPS-bezogene Einstellungen in Secure Access

Dies ist eine kurze Übersicht über die verfügbaren Entschlüsselungs- und IPS-bezogenen Einstellungen in Secure Access.

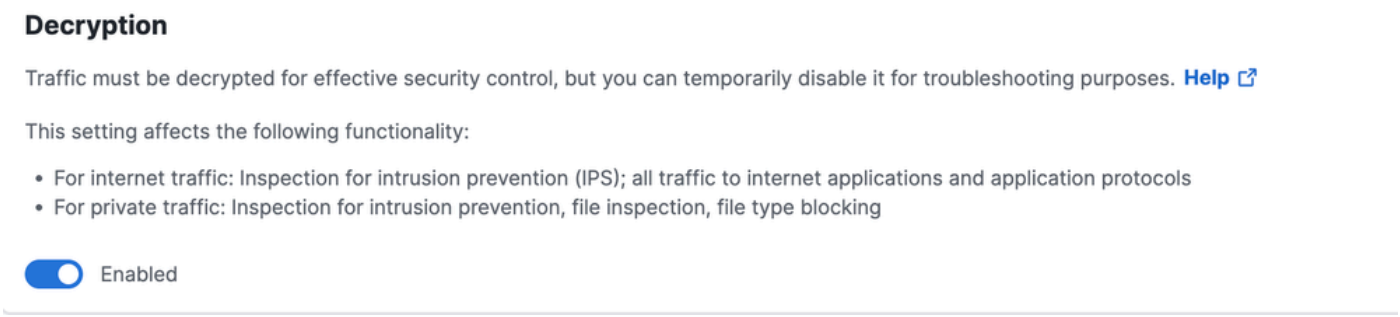
Entschlüsselung für IPS

Dies ist eine globale Einstellung für IPS, mit der die IPS-Engine für alle Richtlinien deaktiviert oder aktiviert wird.

Eigenschaften:

- Diese Option wirkt sich nicht auf die sichere Webgatewayentschlüsselung (Webentschlüsselung) aus.
- Die Deaktivierung und Aktivierung des IPS pro Richtlinie ist mit eingeschränktem Funktionsumfang verfügbar, sodass nur die Anfangsphase des Handshakes ohne Überprüfung des Körpers der Anforderung überprüft werden kann.

Konfiguration: Dashboard -> Sicher -> Zugriffsrichtlinie -> Standardregeln und globale Einstellungen -> Globale Einstellungen -> Entschlüsselung für IPS



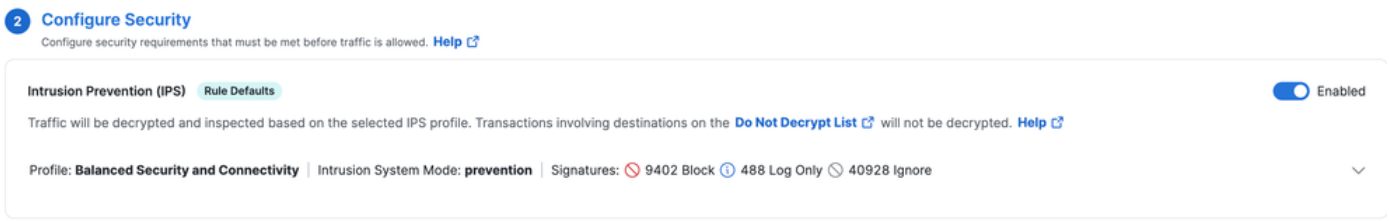
IPS-Einstellungen pro Richtlinie

Mit dieser Option kann IPS für jede Richtlinienbasis deaktiviert und aktiviert werden.

Eigenschaften:

- Diese Option steuert, ob IPS gemäß Richtlinie aktiviert oder deaktiviert wird.
- Diese Option hängt von den IPS-Einstellungen für Entschlüsseln ab. Wenn die globale Option Entschlüsseln für IPS deaktiviert ist, führt dies dazu, dass das Verhalten nur die Anfangsphase des Handshakes überprüft, ohne den Text der Anforderung zu überprüfen.
- Diese Option wirkt sich nicht auf die SWG (Webentschlüsselung) aus

Konfiguration: Dashboard -> Sicher -> Zugriffsrichtlinie -> Richtlinie bearbeiten -> Sicherheit konfigurieren -> Intrusion Prevention (IPS)



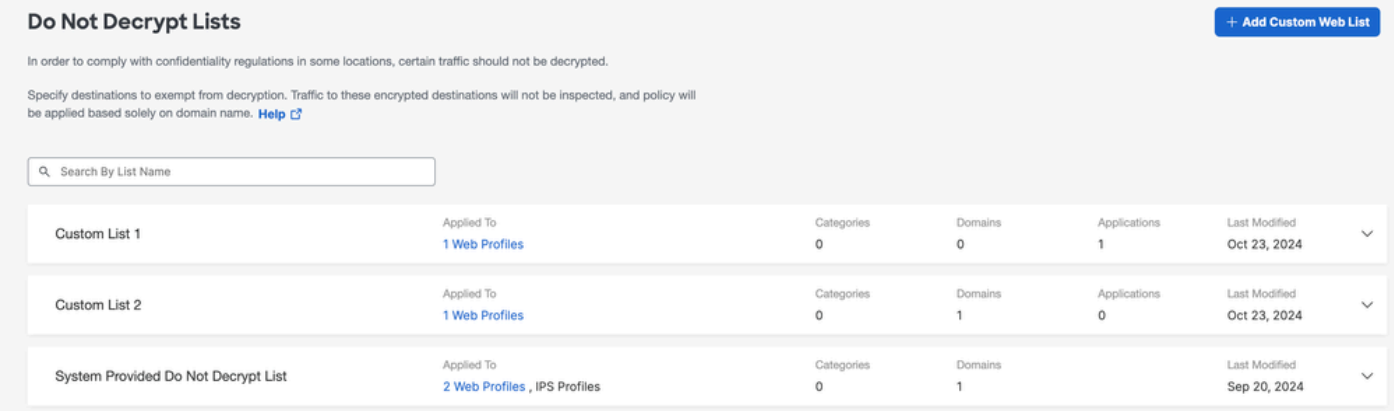
Listen nicht entschlüsseln

Eine Gruppe von Ziellisten, die mit dem Sicherheitsprofil verknüpft werden können, um Domänen oder IP-Adressen vor der Entschlüsselung zu umgehen.

Eigenschaften:

- Umgehung benutzerdefinierter Domänen bei der Webentschlüsselung zulassen
- Diese Liste wirkt sich nur auf die Webentschlüsselung und nicht auf IPS aus, mit Ausnahme der vom System bereitgestellten Liste Nicht entschlüsseln
- Enthält eine (vom System bereitgestellte Liste "Nicht entschlüsseln"), die sowohl die IPS- als auch die Webentschlüsselung umgeht
- Diese Option muss mit Sicherheitsprofilen kombiniert werden, die der Richtlinie hinzugefügt werden.
- Diese Liste kann nur verwendet werden, wenn Entschlüsselung im Sicherheitsprofil aktiviert ist.

Konfiguration: Dashboard -> Sicher -> Listen nicht entschlüsseln



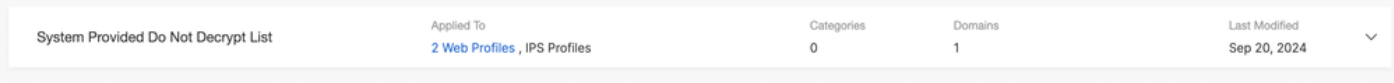
Vom System bereitgestellte Liste nicht entschlüsseln

Teil der Liste "Nicht entschlüsseln" mit zusätzlicher Funktion zum Anwenden von Entschlüsselung und IPS bei sicherem Zugriff.

Eigenschaften:

- Dies ist die einzige benutzerdefinierte Liste "Nicht entschlüsseln", die sich sowohl auf die IPS- als auch die Webentschlüsselung auswirkt
- Es gibt keine Möglichkeit, diese Liste je Richtlinie anzupassen.

Konfiguration: Dashboard -> Sicher -> Listen nicht entschlüsseln -> Vom System bereitgestellte Liste nicht entschlüsseln



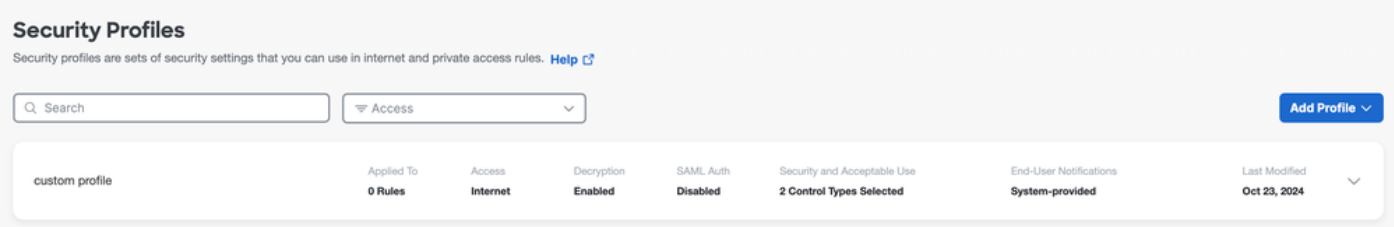
Einstellungen für Sicherheitsprofile

In den Einstellungen für das Sicherheitsprofil können Sie die Webentschlüsselung aktivieren oder deaktivieren, die später mit einer Internetrichtlinie verknüpft werden kann. Wenn Entschlüsselung aktiviert ist, können Sie eine der konfigurierten Listen Nicht entschlüsseln auswählen.

Eigenschaften:

- Steuert mehrere Sicherheitsfunktionen, einschließlich Webentschlüsselung und Listen für die Nicht-Entschlüsselung
- Das Anhängen der vom System bereitgestellten Liste nicht entschlüsseln an das Sicherheitsprofil wirkt sich sowohl auf die Webentschlüsselung als auch auf die IPS-Entschlüsselung aus.

Konfiguration: Dashboard -> Sicher -> Sicherheitsprofile



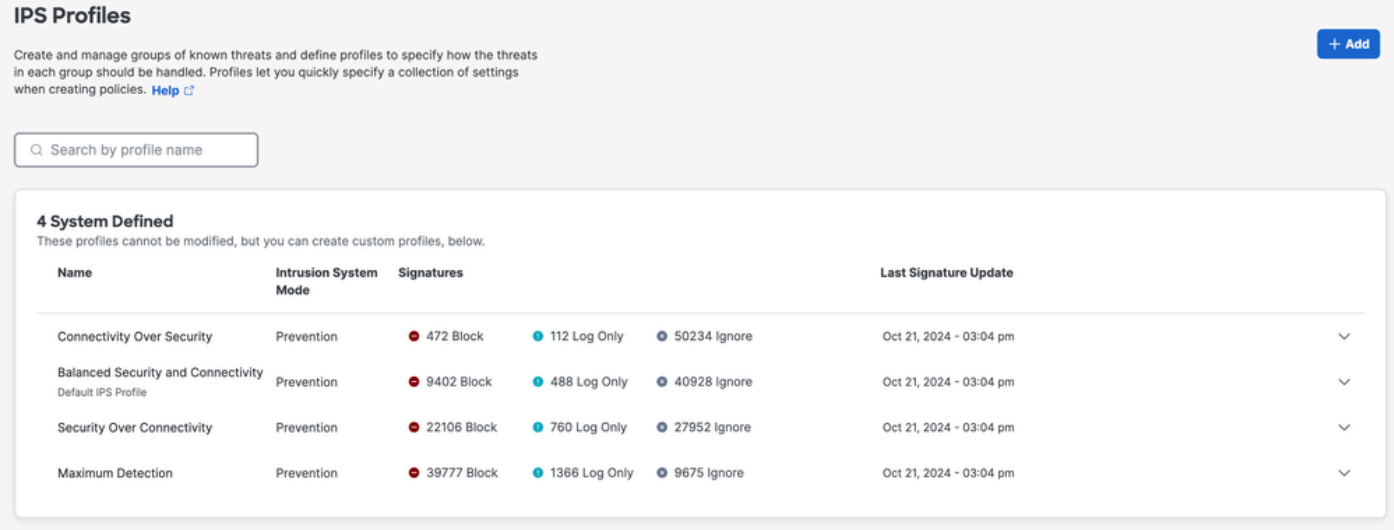
IPS-Profile

Die IPS-Profileinstellungen umfassen vier vordefinierte Hauptsicherheitseinstellungen für das IPS-Profil. Welche Option pro Richtlinieneinstellungen ausgewählt werden kann. Sie haben die Möglichkeit, Ihr eigenes benutzerdefiniertes IPS-Profil zu erstellen, um strengere oder flexiblere Einstellungen zu ermöglichen.

Eigenschaften:

- Enthält vier vordefinierte Sicherheitsebenenprofile für IPS
- Erstellung eines benutzerdefinierten IPS-Profils möglich

Konfiguration: Dashboard -> Sicher -> IPS-Profile

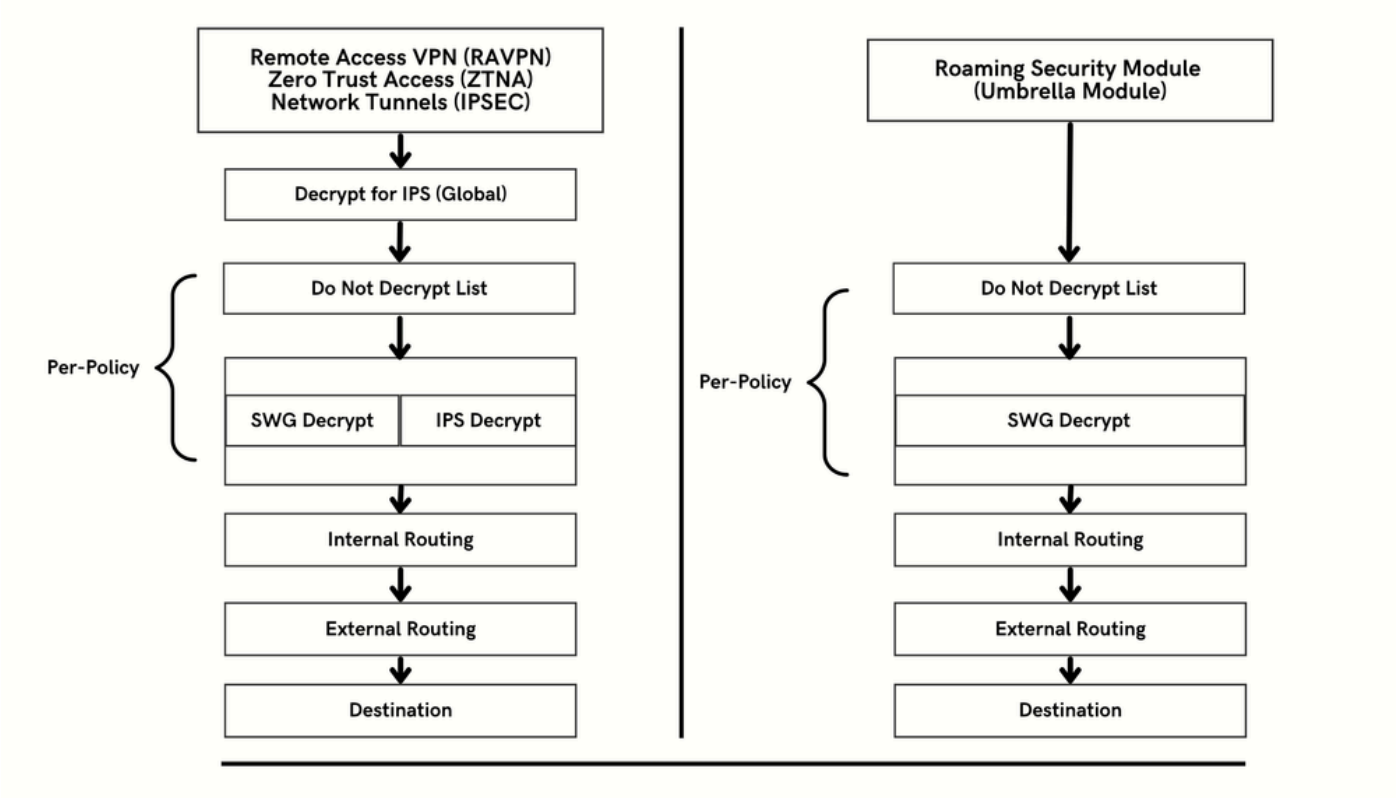


HTTPS-Datenverkehrsfluss in sicherem Zugriff

Je nach Verbindungsmethode gibt es für den sicheren Zugriff unterschiedliche Datenverkehrspfade.

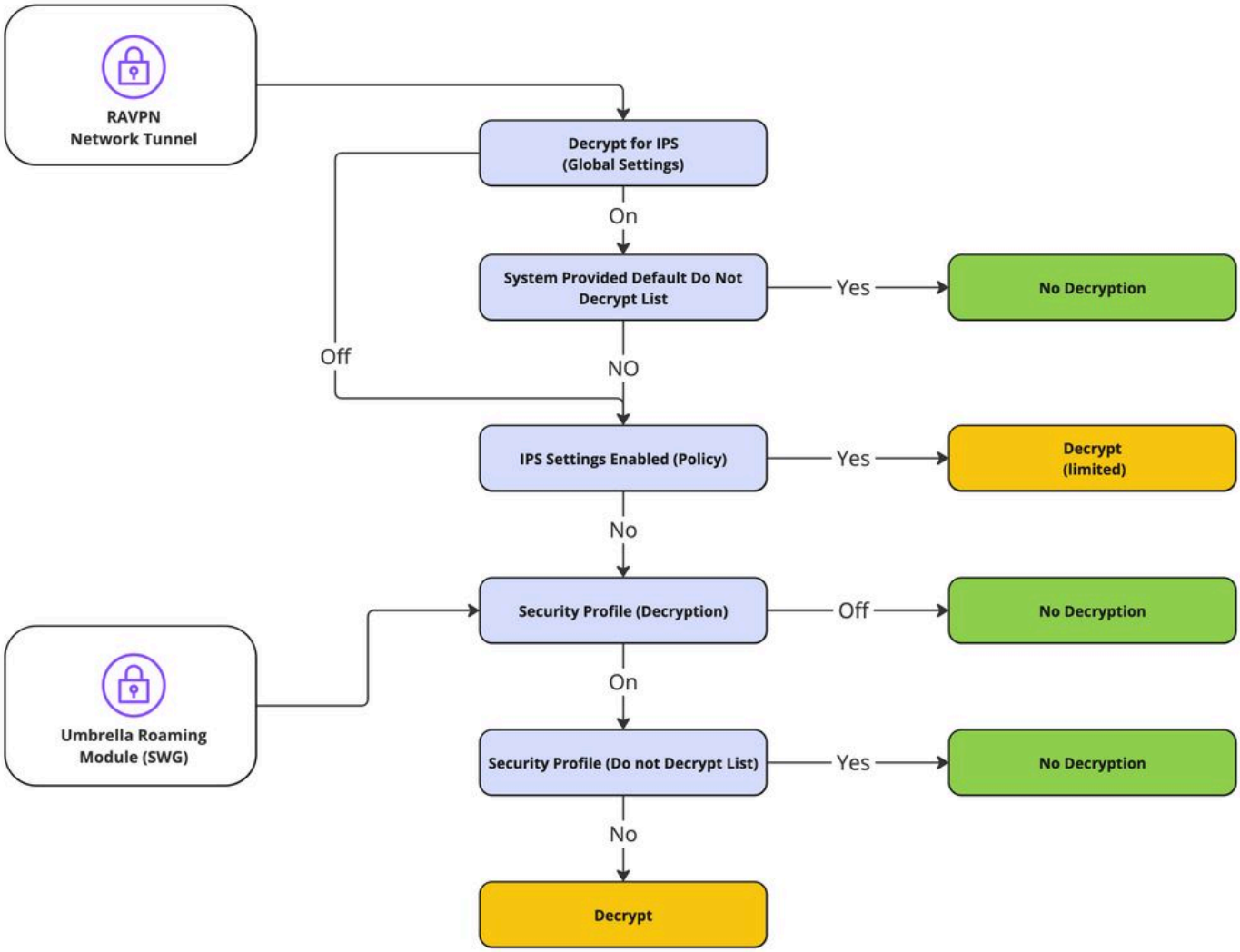
Die Komponenten Remote Access VPN (RAVPN) und Zero Trust Access (ZTNA) sind identisch.

Roaming-Sicherheitsmodule (Umbrella Module) haben unterschiedliche Datenverkehrspfade.



Wann ist mit einer Entschlüsselung des Datenverkehrs zu rechnen?

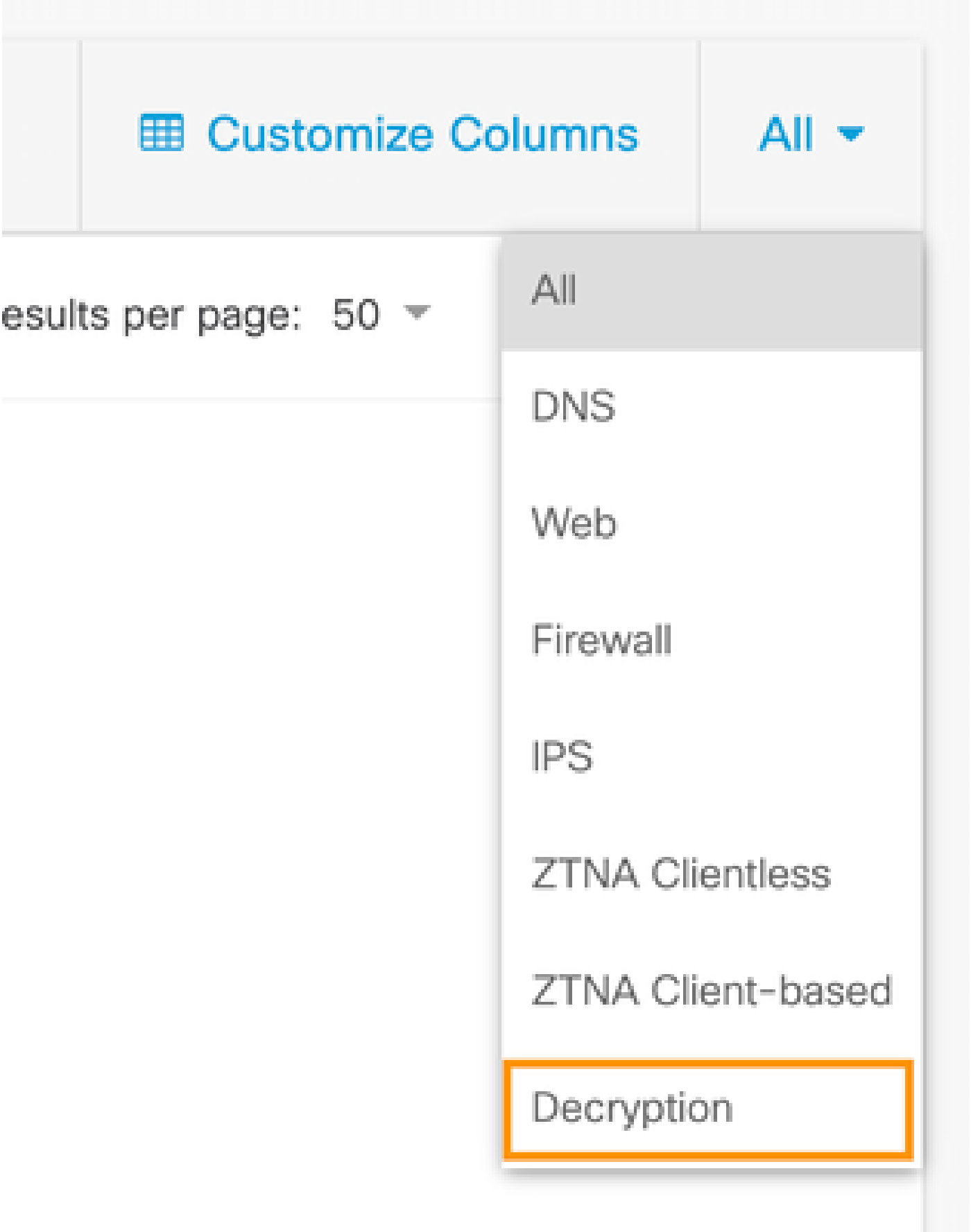
In diesem Abschnitt wird die Kette von Aktionen und ihre führenden Ergebnisse bei Entschlüsselung oder Nichtentschlüsselung ausführlich erläutert.

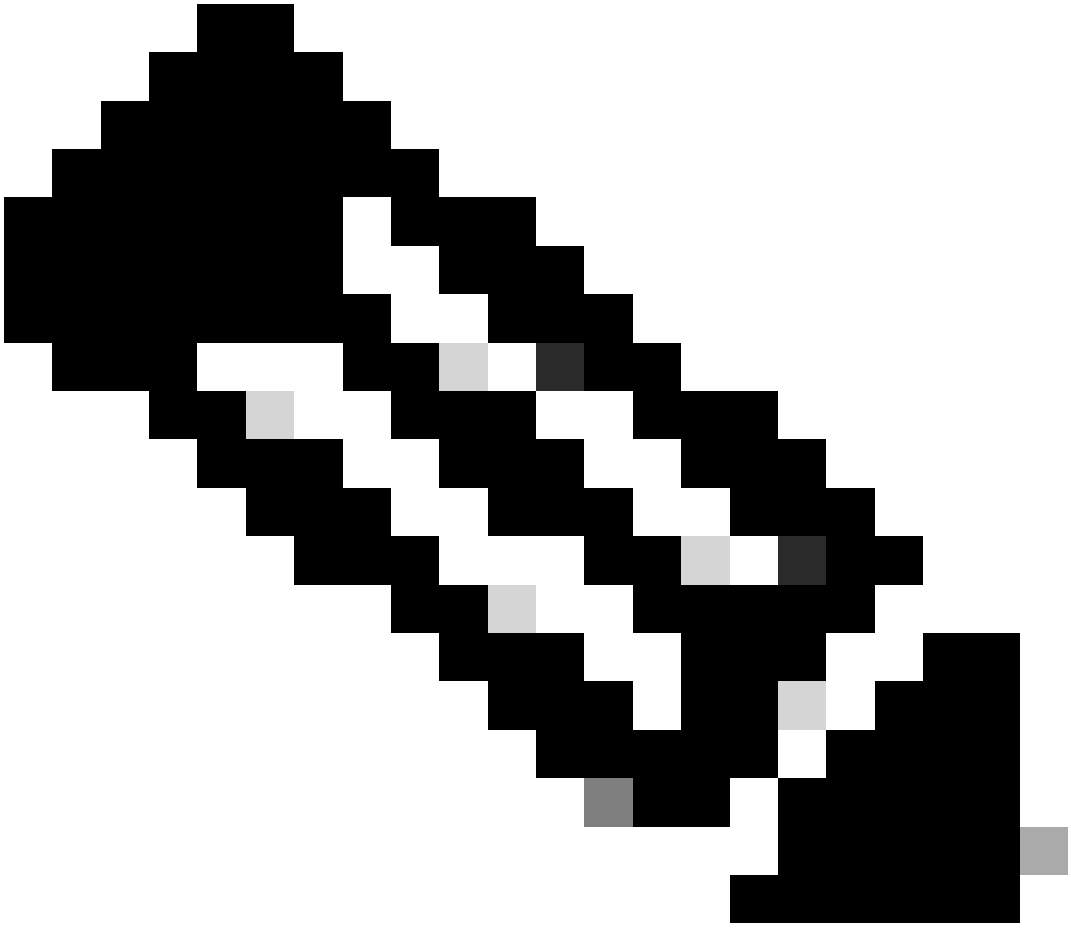


Entschlüsselungsablauf

Protokollierung und Berichterstellung für Entschlüsselung und IPS

Secure Access umfasst einen neuen Berichtsbereich (Entschlüsselung), auf den über Dashboard -> Überwachung -> Aktivitätssuche -> Zu Entschlüsselung wechseln zugegriffen werden kann.

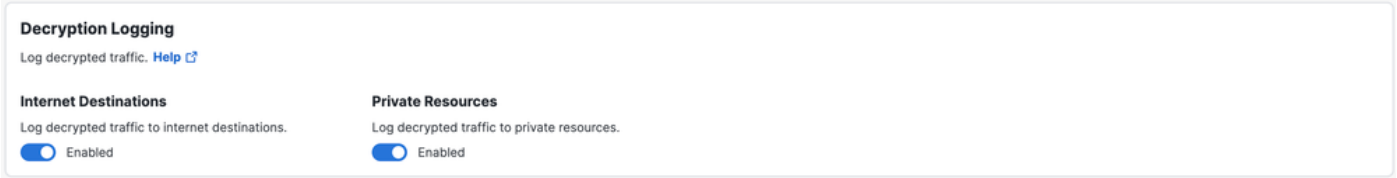

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



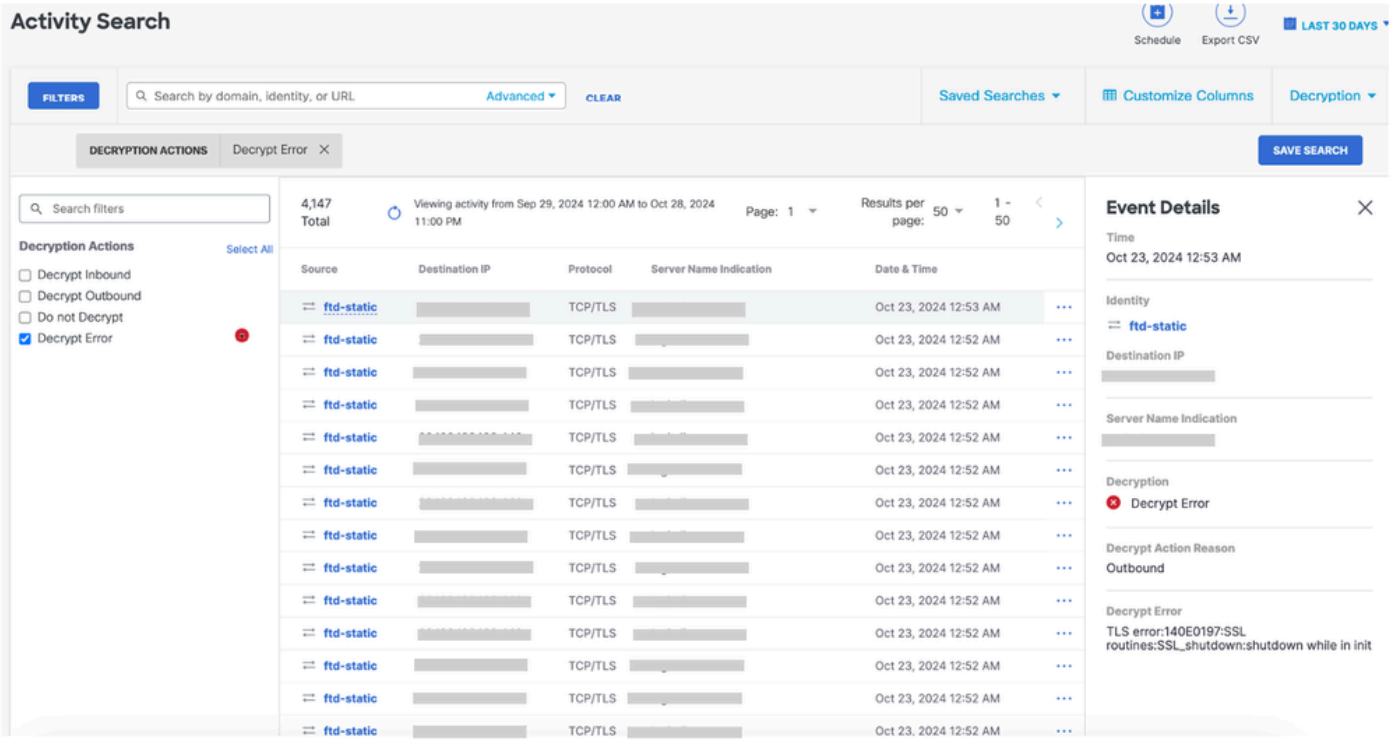
Hinweis: Um Entschlüsselungsprotokolle zu aktivieren, kann diese Einstellung in den globalen Einstellungen aktiviert werden:

Dashboard -> Sicher -> Zugriffsrichtlinie -> Regelstandardwerte und globale Einstellungen -> Globale Einstellungen -> Entschlüsselungsprotokollierung.

Einstellungen für die Entschlüsselungsprotokollierung:



Beispiel für einen Entschlüsselungsfehler:



Zugehörige Informationen

- Benutzerhandbuch zu Secure Access
- Technischer Support und Downloads – Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.