Troubleshoot Secure Access Decryption and Intrusion Prevention System (IPS) Workflow

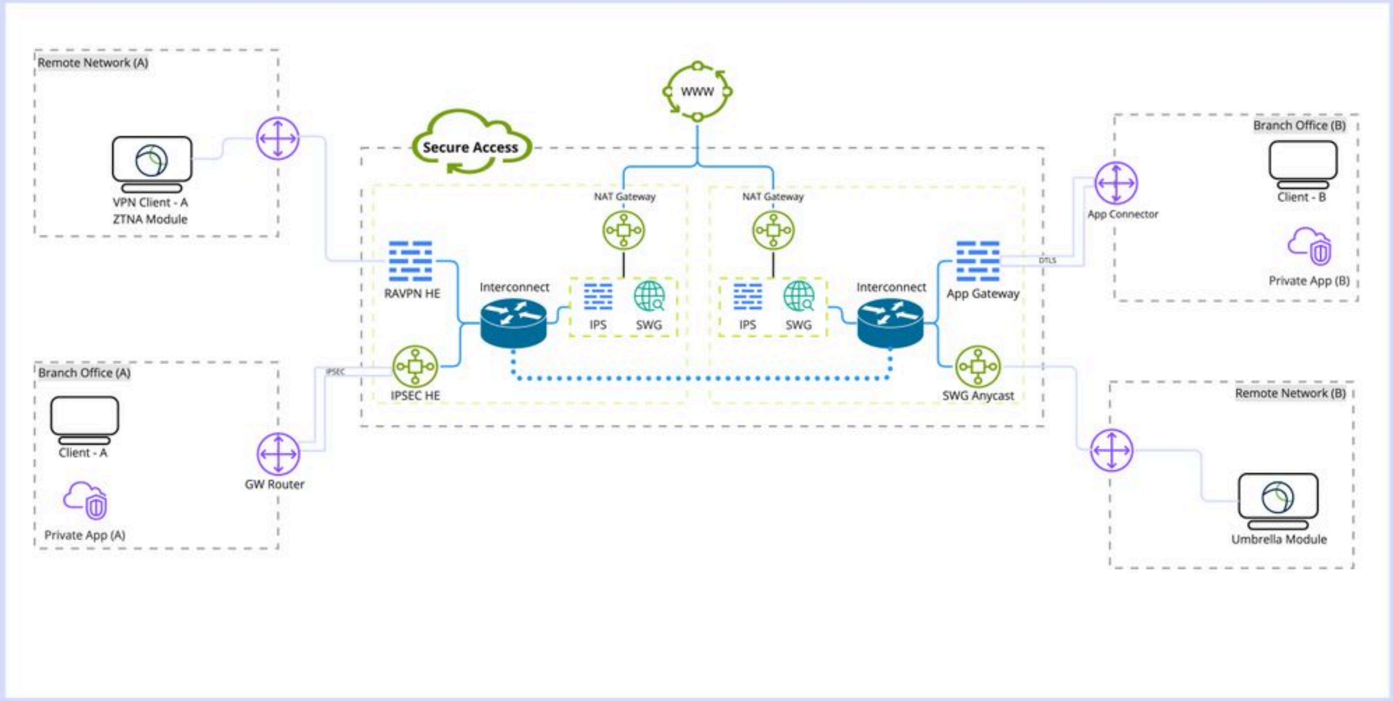
Contents

Introduction

This document describes the Secure Access Decryption and IPS workflow and highlights important settings properties.

Secure Access Architecture

This Secure Access architecture highlights the different services provided by Secure Access and different connection methods that can be established to secure the network.



Secure Access Architecture

Architecture Details:

Terms to be familiar with:

RAVPN HE: Remote Access Virtual Private Network Head End

IPSEC HE: Remote Tunnel Internet Protocol Security (IPSEC) Head End

ZTNA Module: Zero Trust Network Access Module

SWG: Secure Web Gateway

IPS: Intusion Prevention System

NAT Gateway: Network Address Translation Gateway

SWG AnyCast: Secure Web Gateway Anycast ingress point

Deployment Types:

1. Remote Access VPN

2. Remote Access Tunnel

3. Umbrella Roaming Module

4. Application Connector/Application Gateway

5. Zero Trust Module (ZTNA)

Feature Overview

Secure Access provides the capability of doing both Web Decryption and Intrusion Prevention System (IPS) to enhance the applications detection and categorization and provide more details about the traffic. including URL paths, file names, and their application category. and help prevent from zero-day attacks and malwares.

Decryption: In this article the decryption is referred to Decrypting Hyper Text Transfer Protocol (HTTPS) traffic through Secure Web Gateway (SWG) Module. and also Decrypting traffic for IPS inspection.

IPS: Firewall level Intrusion Detection and Prevention System which requires Decryption for traffic in order to perform full functionality.

The Decryption is necessary for multiple Secure Access Features such as Data Loss Prevention (DLP) and Remote Browser Isolation (RBI), File Inspection, file analysis and file type blocking.

Decryption and IPS related settings in Secure Access

This is a quick overview of available Decryption and IPS related settings in Secure Access.

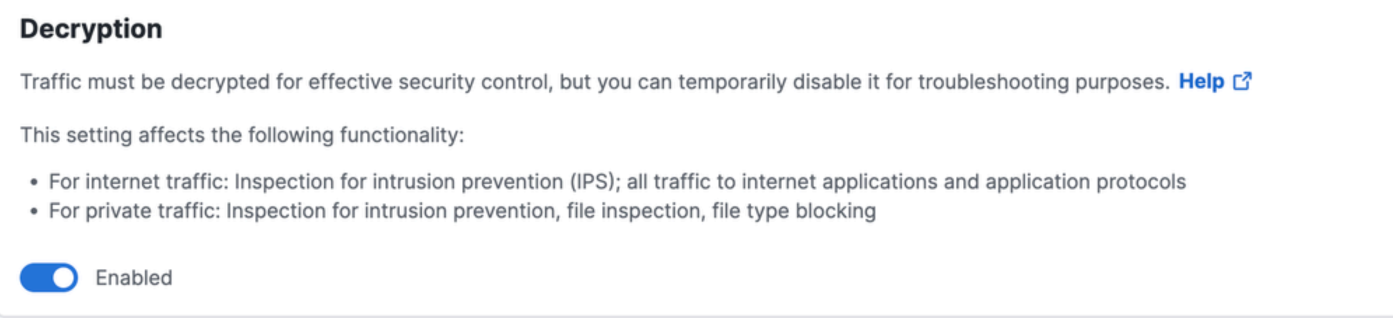
Decryption for IPS

This is a global setting for IPS which is used to disable or enabled IPS engine for all policies.

Properties:

- This option does not affect the Secure Web Gateway Decryption (Web Decryption)
- Disabling and Enabling the IPS per policy is available with limited functionality to only inspect the initial phase of the handshake without inspecting the body of the request.

Configuration: Dashboard -> Secure -> Access Policy -> Rule Defaults and Global Settings -> Global Settings -> Decryption for IPS



Decryption

Traffic must be decrypted for effective security control, but you can temporarily disable it for troubleshooting purposes. Help

This setting affects the following functionality:

- For internet traffic: Inspection for intrusion prevention (IPS); all traffic to internet applications and application protocols
- For private traffic: Inspection for intrusion prevention, file inspection, file type blocking

Enabled

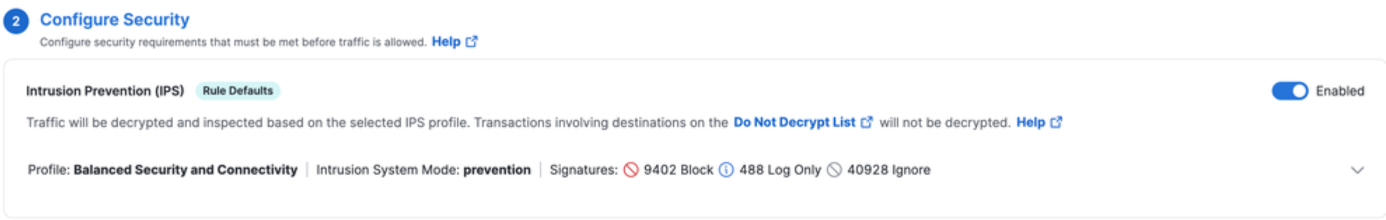
IPS Settings per Policy

This option allows to disable and enable IPS per policy bases.

Properties:

- This option controls whether IPS is enabled or disabled per policy.
- This option is dependent on Decrypt for IPS settings, if the global Decrypt for IPS option is disabled, it cause the behavior to only inspect the initial phase of the handshake without inspecting the body of the request.
- This option does not affect SWG (Web Decryption)

Configuration: Dashboard -> Secure -> Access Policy ->Edit Policy -> Configure Security -> Intrusion Prevention (IPS)



2 Configure Security

Configure security requirements that must be met before traffic is allowed. Help

Intrusion Prevention (IPS) Rule Defaults — Enabled

Traffic will be decrypted and inspected based on the selected IPS profile. Transactions involving destinations on the Do Not Decrypt List will not be decrypted. Help

Profile: **Balanced Security and Connectivity** | Intrusion System Mode: **prevention** | Signatures: 9402 Block 488 Log Only 40928 Ignore

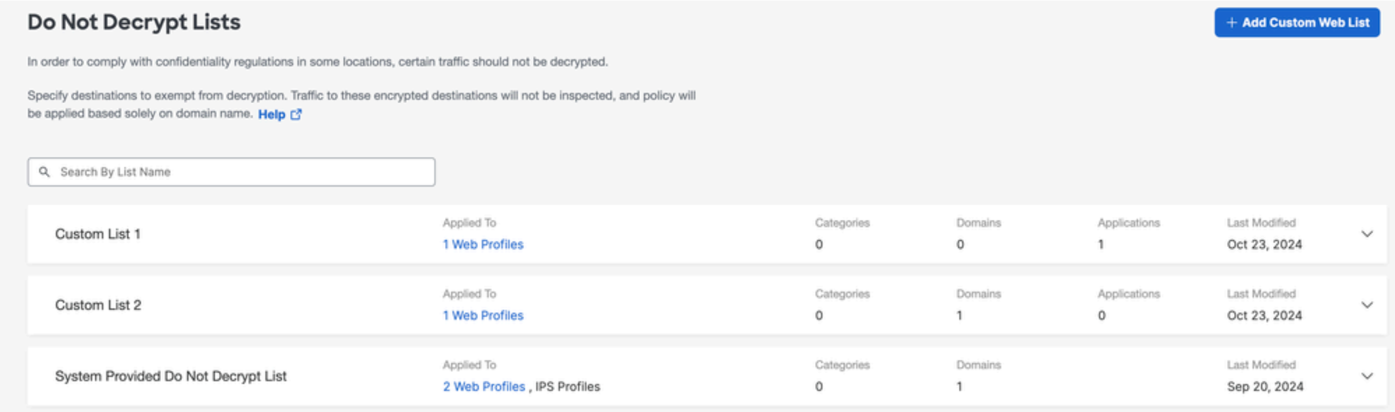
Do Not Decrypt Lists

Set of Destination lists that can be linked to Security Profile to bypass domains or IP addresses from being decrypted.

Properties:

- Allow custom domains to be bypassed Web Decryption
- This list only affects Web Decryption not IPS with exception of System Provided Do Not Decrypt List
- Contains a (System Provided Do Not Decrypt list) that bypass both IPS and Web Decryption
- This Option need to be combined with Security Profiles to be attached to the policy
- This list can be only used if Decryption is enabled in the Security Profile

Configuration: Dashboard -> Secure -> Do Not Decrypt Lists



Do Not Decrypt Lists

In order to comply with confidentiality regulations in some locations, certain traffic should not be decrypted.

Specify destinations to exempt from decryption. Traffic to these encrypted destinations will not be inspected, and policy will be applied based solely on domain name. Help

	Applied To	Categories	Domains	Applications	Last Modified
Custom List 1	1 Web Profiles	0	0	1	Oct 23, 2024
Custom List 2	1 Web Profiles	0	1	0	Oct 23, 2024
System Provided Do Not Decrypt List	2 Web Profiles , IPS Profiles	0	1		Sep 20, 2024

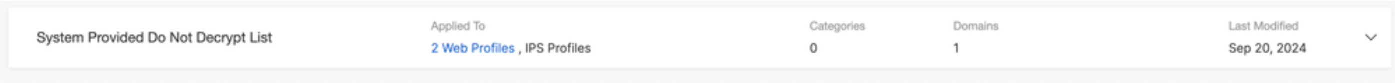
System Provided Do Not Decrypt List

Part of Do Not Decrypt lists, with additional feature of applying on both Decryption and IPS in Secure Access.

Properties:

- This is the only custom Do Not Decrypt list that affects both IPS and Web Decryption
- There's no option to customize this list per policy.

Configuration: Dashboard -> Secure -> Do Not Decrypt Lists -> System Provided Do Not Decrypt List



	Applied To	Categories	Domains	Last Modified
System Provided Do Not Decrypt List	2 Web Profiles , IPS Profiles	0	1	Sep 20, 2024

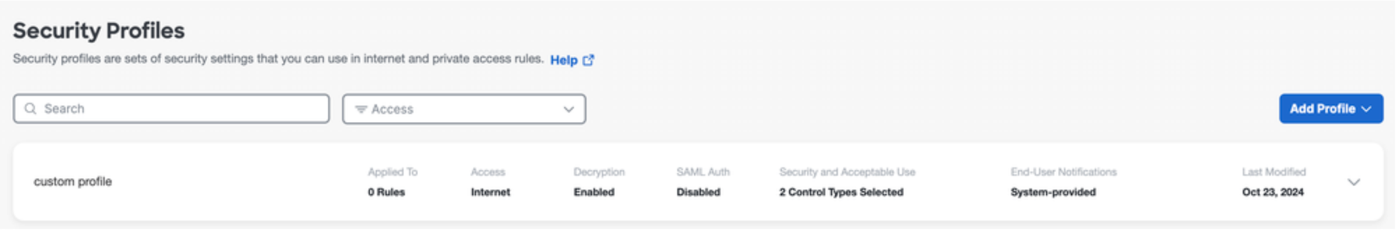
Security Profile Settings

In Security Profile settings you can select Enabling or Disabling Web Decryption which can be later associated with an Internet Policy. If Decryption is enabled, you have the option to select one of the Do Not Decrypt lists configured.

Properties:

- Controls several security features including Web Decryption and Do Not Decrypt Lists
- Attaching System Provided Do Not Decrypt List to the security profile affects both Web Decryption and IPS Decryption

Configuration: Dashboard -> Secure -> Security Profiles



Security Profiles

Security profiles are sets of security settings that you can use in internet and private access rules. Help

	Applied To	Access	Decryption	SAML Auth	Security and Acceptable Use	End-User Notifications	Last Modified
custom profile	0 Rules	Internet	Enabled	Disabled	2 Control Types Selected	System-provided	Oct 23, 2024

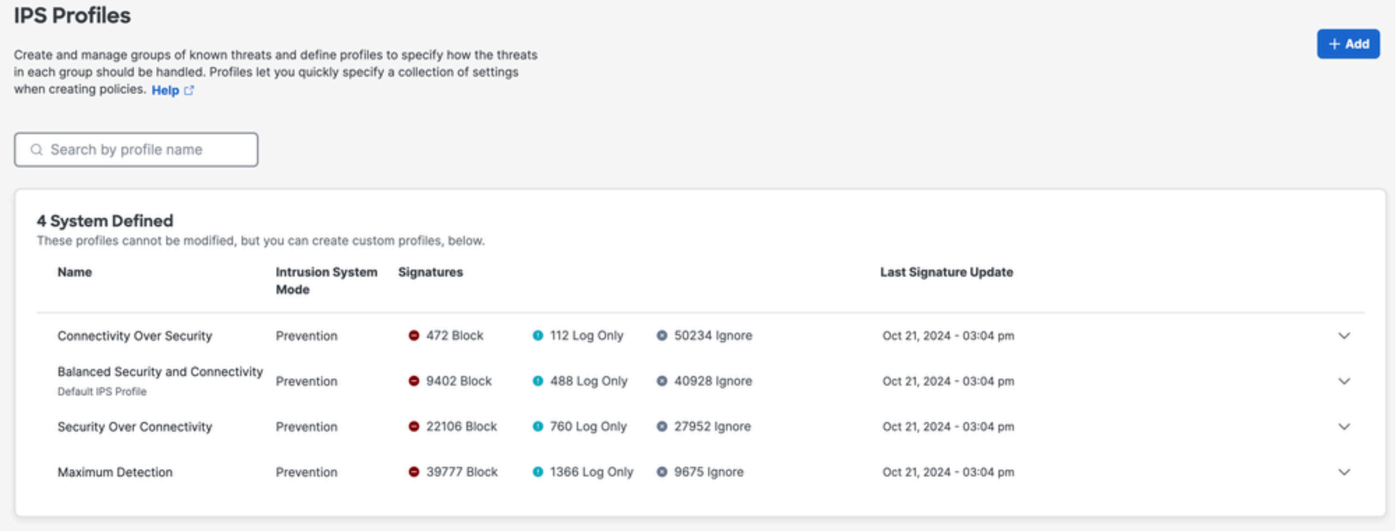
IPS Profiles

IPS Profiles settings include four main pre-defined Security Settings for the IPS Profile. Which can be selected per Policy settings. You have the option to create your own custom IPS profile for more strict or flexible settings.

Properties:

- Contains four pre-defined security levels profiles for IPS
- Custom IPS profile can be created

Configuration: Dashboard -> Secure -> IPS Profiles



IPS Profiles

Create and manage groups of known threats and define profiles to specify how the threats in each group should be handled. Profiles let you quickly specify a collection of settings when creating policies. Help

4 System Defined

These profiles cannot be modified, but you can create custom profiles, below.

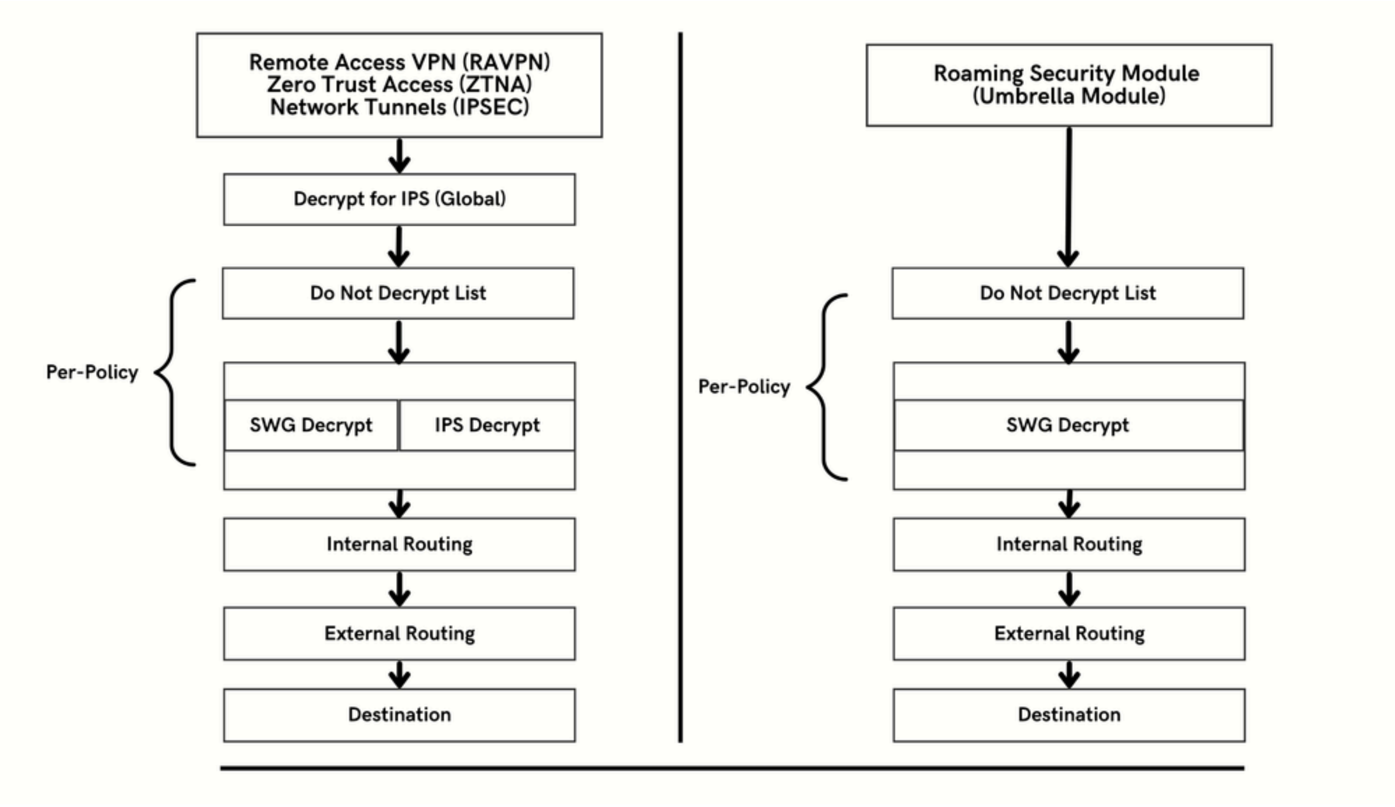
Name	Intrusion System Mode	Signatures			Last Signature Update
Connectivity Over Security	Prevention	472 Block	112 Log Only	50234 Ignore	Oct 21, 2024 - 03:04 pm
Balanced Security and Connectivity Default IPS Profile	Prevention	9402 Block	488 Log Only	40928 Ignore	Oct 21, 2024 - 03:04 pm
Security Over Connectivity	Prevention	22106 Block	760 Log Only	27952 Ignore	Oct 21, 2024 - 03:04 pm
Maximum Detection	Prevention	39777 Block	1366 Log Only	9675 Ignore	Oct 21, 2024 - 03:04 pm

HTTPS Traffic Flow in Secure Access

Secure Access have different traffic paths based on the connection method.

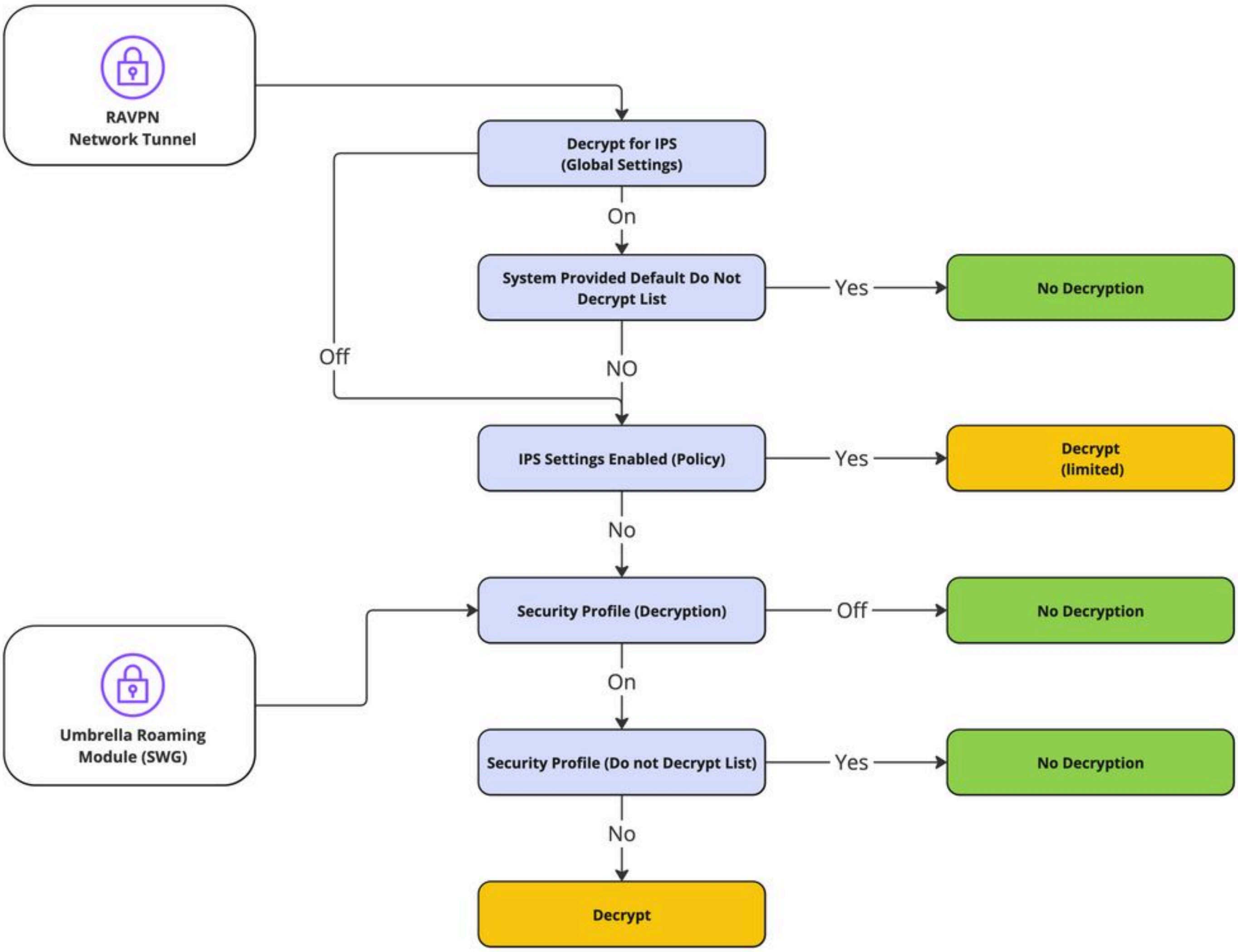
Remote Access VPN (RAVPN) and Zero Trust Access (ZTNA) shares the same components.

Roaming Security Module (Umbrella Module) have different traffic path.



When to Expect Traffic to be Decrypted

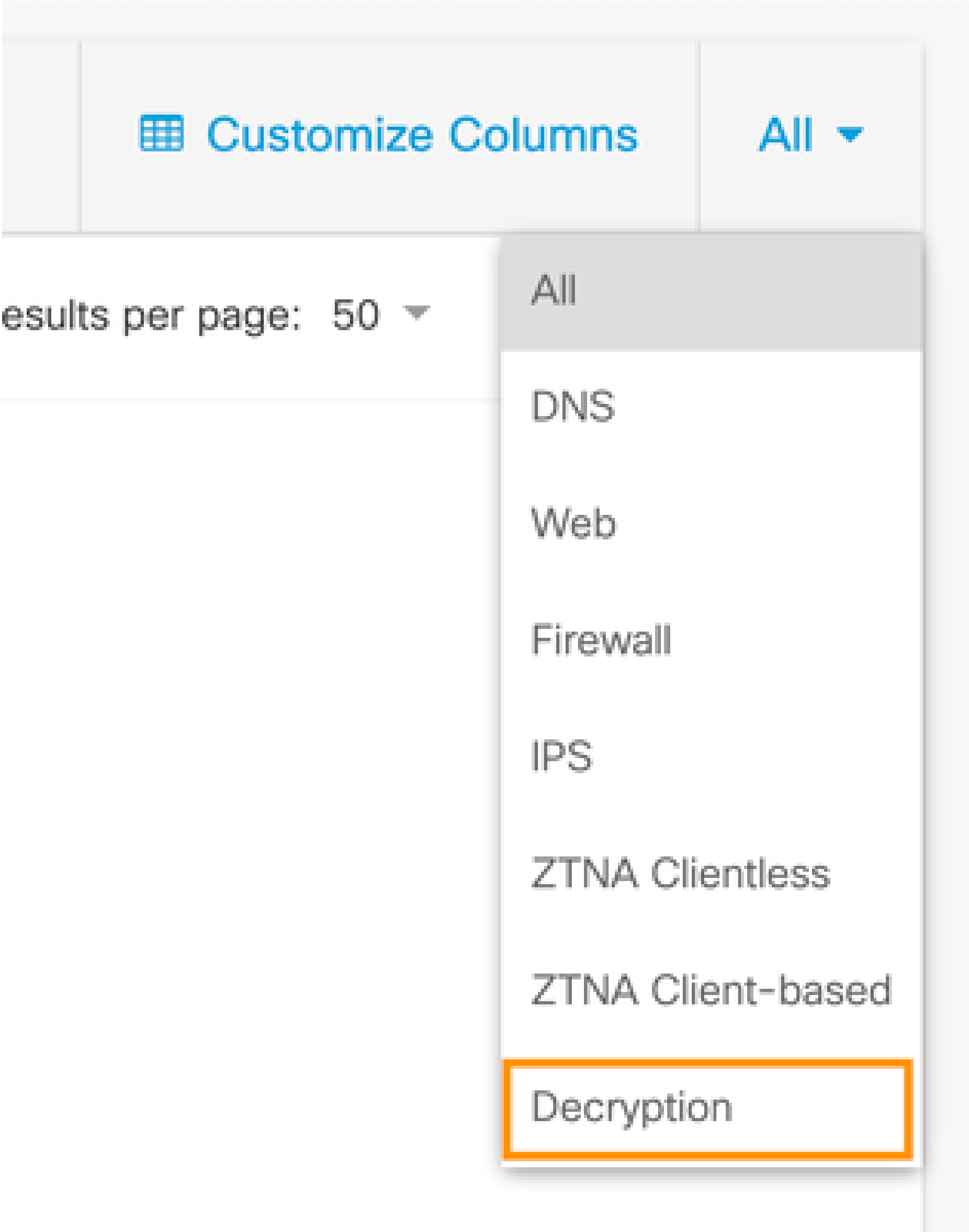
This section explains in detail the chain of actions and their leading results of decryption or no decryption.



Decryption Flow

Decryption and IPS related Logging and Reporting

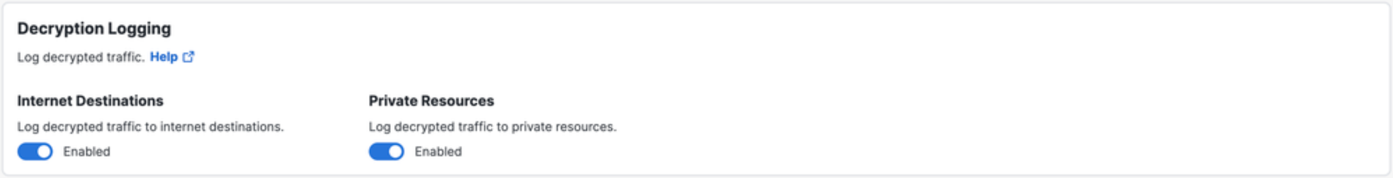
Secure Access includes new reporting section (Decryption) which can be accessed through **Dashboard -> Monitor -> Activity Search -> Switch to Decryption.**


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

Note: To Enable Decryption Logs, this setting can be enabled on global settings:

Dashboard -> Secure -> Access Policy -> Rule Defaults and Global Settings -> Global Settings -> Decryption Logging.

Decryption Logging Settings:



Decryption Logging

Log decrypted traffic. Help

Internet Destinations

Log decrypted traffic to internet destinations.

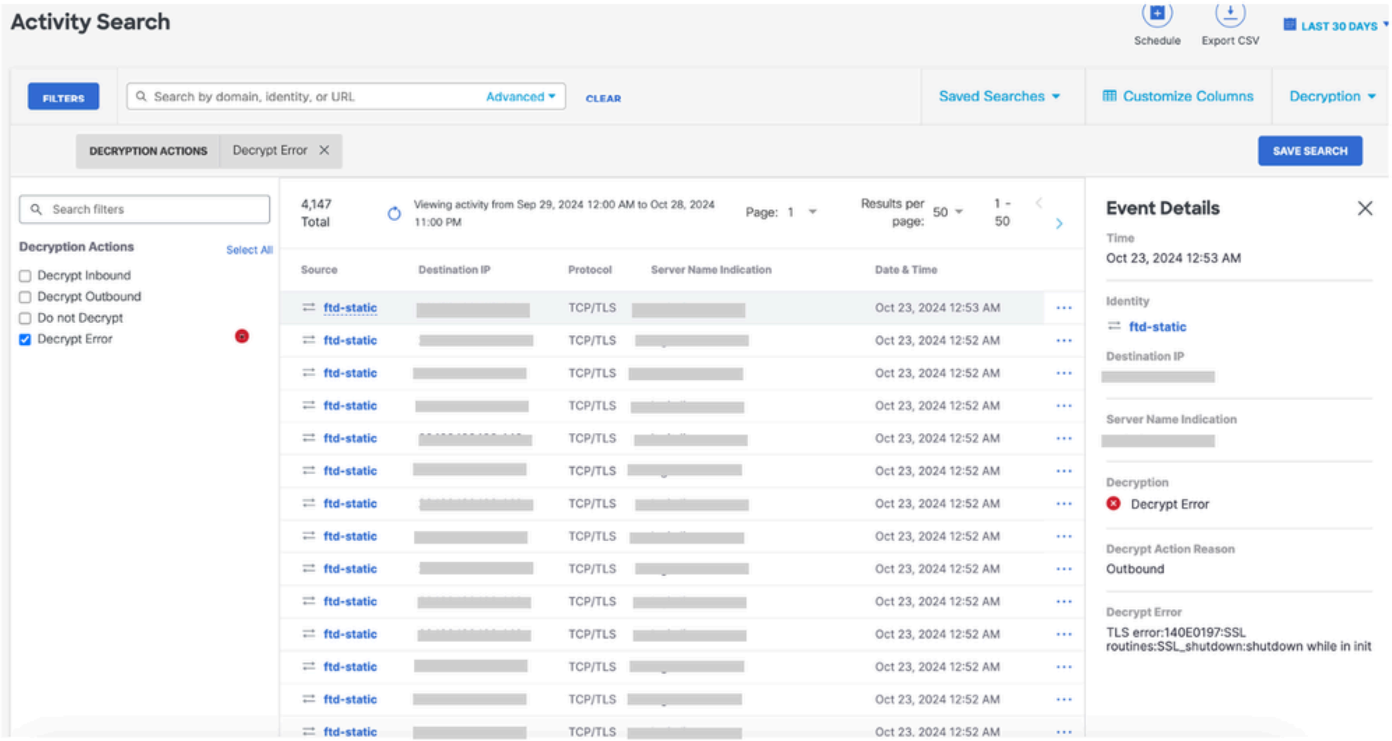
Enabled

Private Resources

Log decrypted traffic to private resources.

Enabled

Example of Decryption Error:



Decryption Actions — Select All

- ☐ Decrypt Inbound
- ☐ Decrypt Outbound
- ☐ Do not Decrypt
- ☑ Decrypt Error

4,147 Total

Viewing activity from Sep 29, 2024 12:00 AM to Oct 28, 2024 11:00 PM

Page: 1 — Results per page: 50 — 1 - 50

Source	Destination IP	Protocol	Server Name Indication	Date & Time
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:53 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM
ftd-static	[redacted]	TCP/TLS	[redacted]	Oct 23, 2024 12:52 AM

Event Details

Time: Oct 23, 2024 12:53 AM

Identity: ftd-static

Destination IP: [redacted]

Server Name Indication: [redacted]

Decryption: Decrypt Error

Decrypt Action Reason: Outbound

Decrypt Error: TLS error:140E0197:SSL routines:SSL_shutdown:shutdown while in init

Related Information

- [Secure Access User Guide]
- [Technical Support & Downloads - Cisco Systems]