安全访问解密和入侵防御系统(IPS)工作流程故障排除

目录

[简介](#)

[安全访问架构](#)

[功能概述](#)

[安全访问中的解密和IPS相关设置](#)

- [IPS解密](#)
- [每个策略的IPS设置](#)
- [不解密列表](#)
- [系统提供的不解密列表](#)
- [安全配置文件设置](#)
- [IPS配置文件](#)

[安全访问中的HTTPS流量](#)

[预期何时解密流量](#)

[解密与IPS相关的日志记录和报告](#)

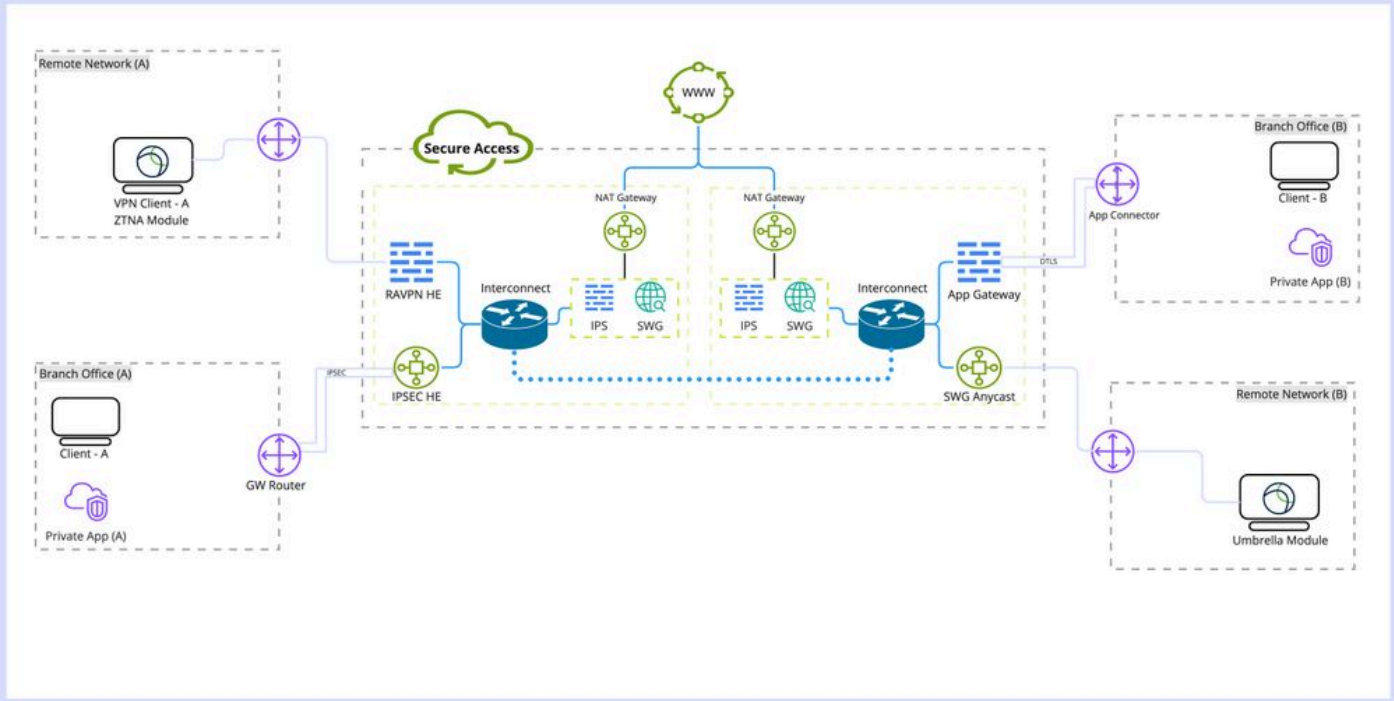
[相关信息](#)

简介

本文档介绍安全访问解密和IPS工作流程并突出显示重要设置属性。

安全访问架构

此安全访问架构重点介绍了安全访问提供的不同服务以及可建立以保护网络的不同连接方法。



安全访问架构

架构详细信息：

要熟悉的术语：

RAVPN HE：远程访问虚拟专用网络前端

IPSEC HE：远程隧道互联网协议安全(IPSEC)前端

ZTNA模块：零信任网络接入模块

SWG：安全Web网关

IPS：入侵防御系统

NAT网关：网络地址转换网关

SWG AnyCast：安全网关任播入口点

部署类型：

1. 远程访问VPN

2. 远程访问隧道

3. Umbrella漫游模块

4. 应用连接器/应用网关

5. 零信任模块(ZTNA)

功能概述

安全访问能够执行Web解密和入侵防御系统(IPS)来增强应用检测和分类，并提供有关流量的更多详细信息，包括URL路径、文件名及其应用类别，并帮助防止零日攻击和恶意软件。

解密：在本文中，解密是指通过安全网络网关(SWG)模块解密超文本传输协议(HTTPS)流量，以及解密流量以进行IPS检查。

IPS：防火墙级别的入侵检测和防御系统，需要解密流量才能执行完整功能。

解密对于多个安全访问功能(例如防数据丢失(DLP)和远程浏览器隔离(RBI)、文件检查、文件分析和文件类型阻止)是必要的。

安全访问中的解密和IPS相关设置

这是安全访问中可用的解密和IPS相关设置的快速概述。

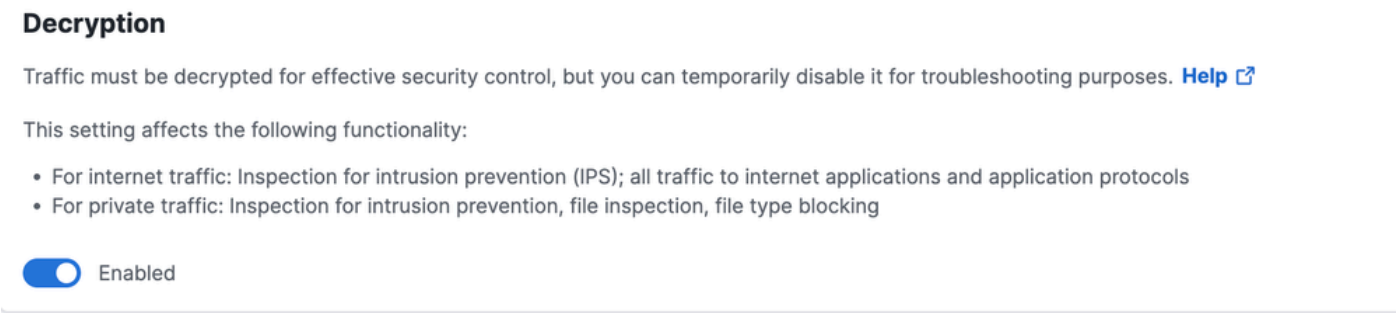
IPS解密

这是IPS的全局设置，用于禁用或启用所有策略的IPS引擎。

属性：

- 此选项不影响安全网关解密（Web解密）
- 禁用和启用每个策略的IPS功能有限，只能检查握手的初始阶段，而不检查请求正文。

配置: 控制面板->安全->访问策略->规则默认值和全局设置->全局设置->IPS解密



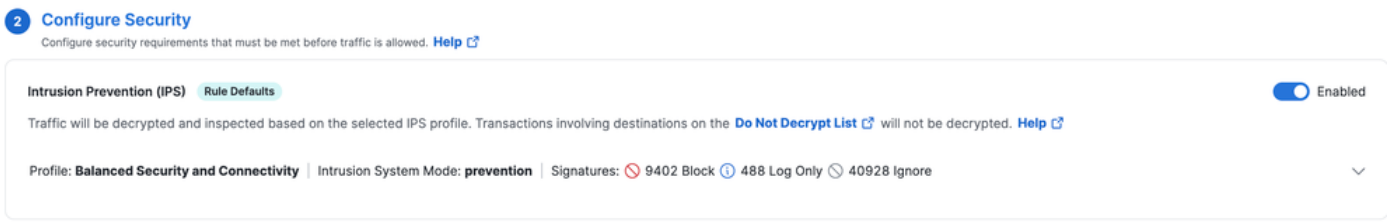
每个策略的IPS设置

此选项允许禁用和启用每个策略库的IPS。

属性：

- 此选项控制每个策略是启用还是禁用IPS。
- 此选项取决于Decrypt for IPS设置，如果全局的Decrypt for IPS选项被禁用，则行为将仅检查握手的初始阶段，而不检查请求正文。
- 此选项不会影响SWG（Web解密）

配置：控制面板->安全->访问策略->编辑策略->配置安全->入侵防御(IPS)



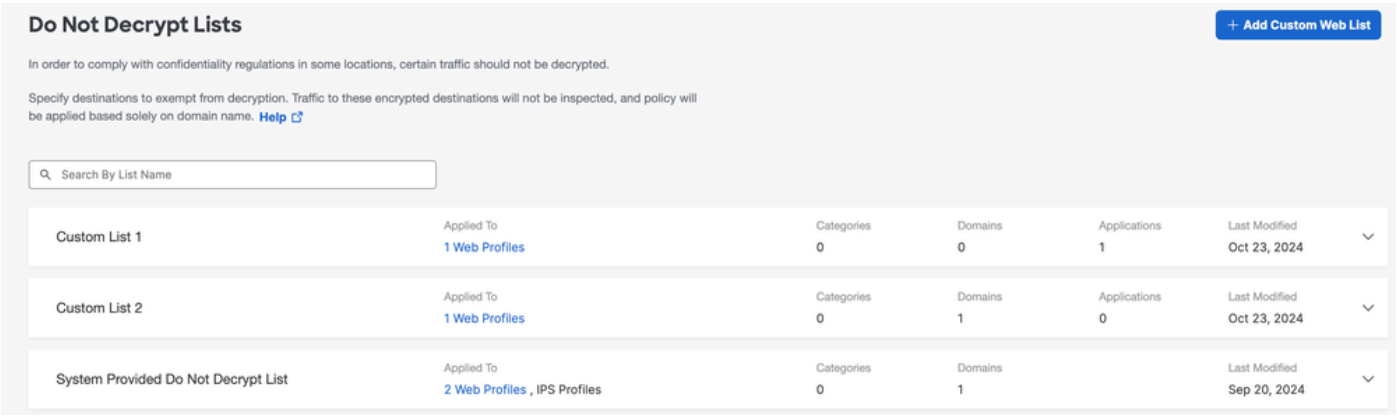
不解密列表

可链接到安全配置文件以绕过域或IP地址解密的目标列表集。

属性：

- 允许绕过自定义域的Web解密
- 此列表仅影响Web解密而非IPS，系统提供的不解密列表除外
- 包含同时绕过IPS和Web解密的（系统提供的不解密列表）
- 此选项需要与要附加到策略的安全配置文件结合使用
- 只有在安全配置文件中启用了解密时，才能使用此列表

配置：控制面板(Dashboard) ->安全(Secure) ->不解密列表(Do Not Decrypt Lists)



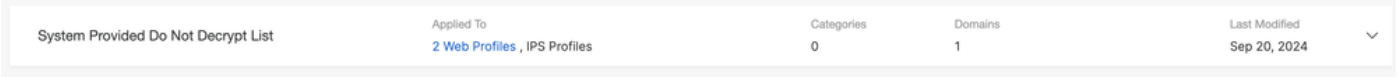
系统提供的不解密列表

“不解密”列表的一部分，具有应用于安全访问中的解密和IPS的附加功能。

属性：

- 这是影响IPS和Web解密的唯一自定义“不解密”列表
- 没有根据策略自定义此列表的选项。

配置：控制面板->安全->不解密列表->系统提供的不解密列表



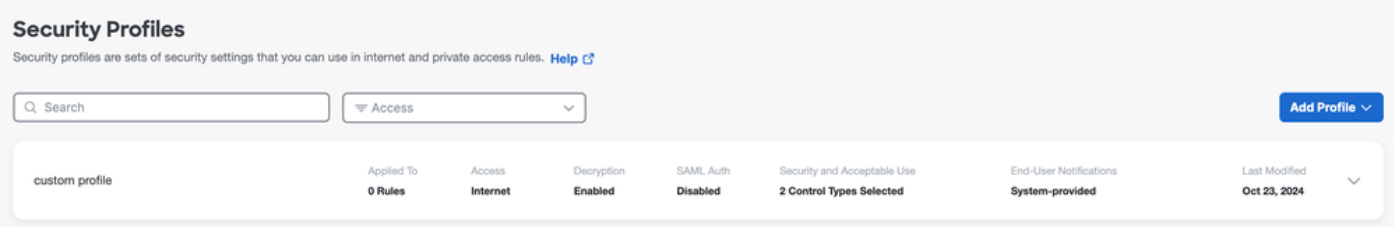
安全配置文件设置

在“安全配置文件”(Security Profile)设置中，您可以选择启用或禁用Web解密(Enable or Disabling Web Decryption)，稍后可将其与Internet策略相关联。如果启用解密(Decryption)，您可以选择已配置的“不解密”(Do Not Decrypt)列表之一。

属性：

- 控制多个安全功能，包括Web解密和Do Not Decrypt列表
- 将系统提供的不解密列表附加到安全配置文件会影响Web解密和IPS解密

配置：控制面板(Dashboard) ->安全(Secure) ->安全配置文件(Security Profiles)



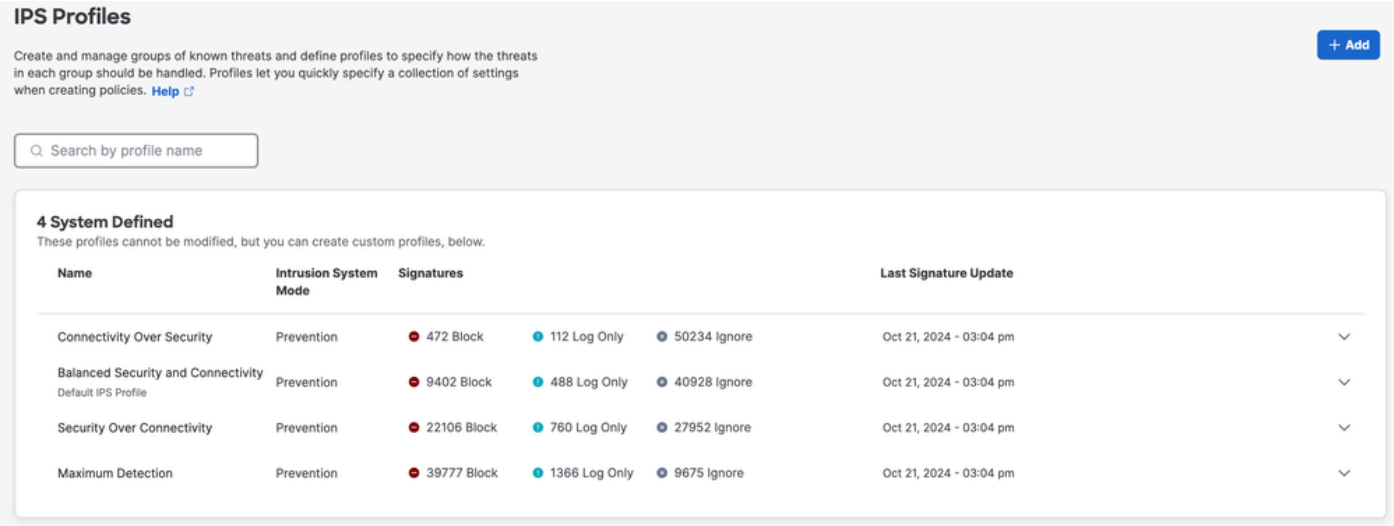
IPS配置文件

IPS配置文件设置包括四个主要的IPS配置文件预定义安全设置。可按策略设置进行选择。您可以选择创建自己的自定义IPS配置文件，以进行更严格或灵活的设置。

属性：

- 包含四个适用于IPS的预定义安全级别配置文件
- 可以创建自定义IPS配置文件

配置：控制面板->安全-> IPS配置文件

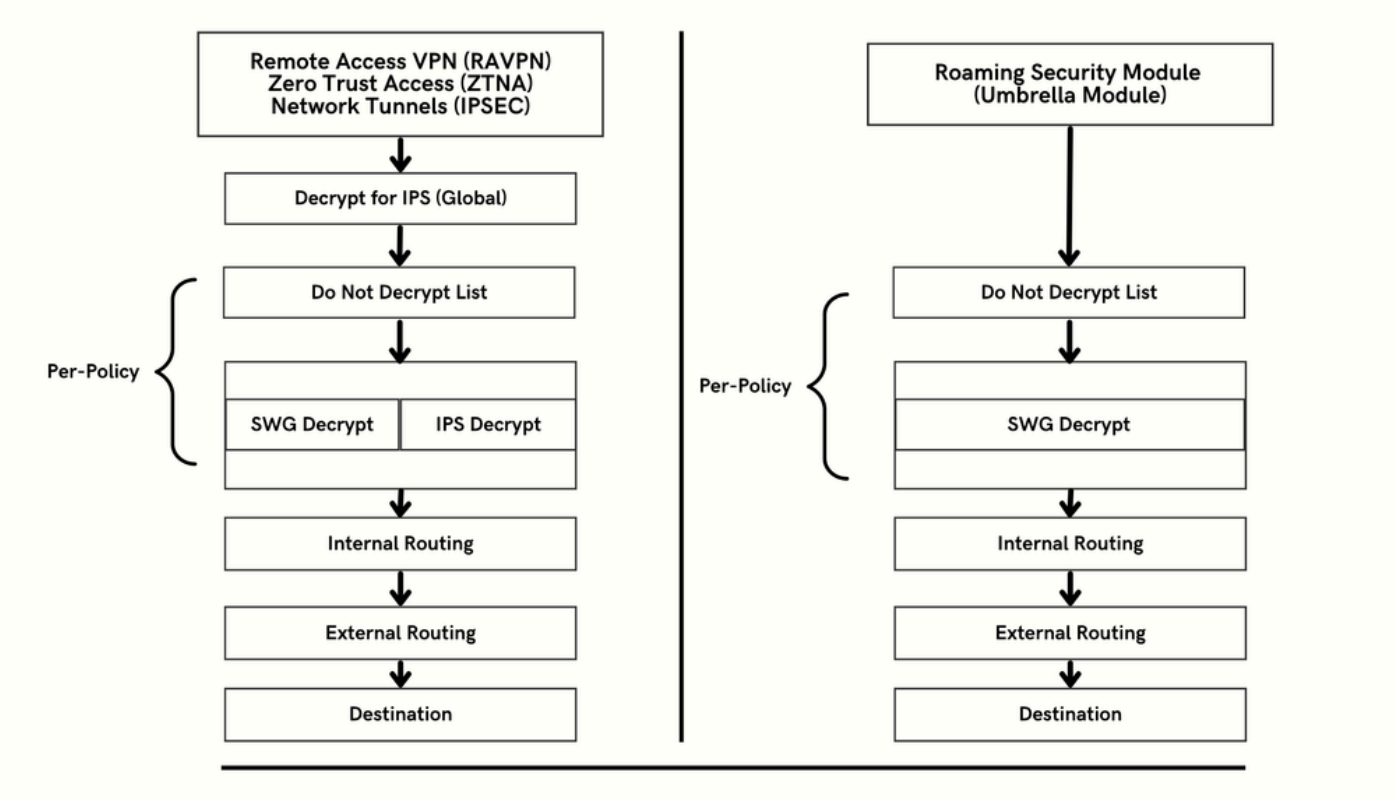


安全访问中的HTTPS流量

根据连接方法，安全访问具有不同的流量路径。

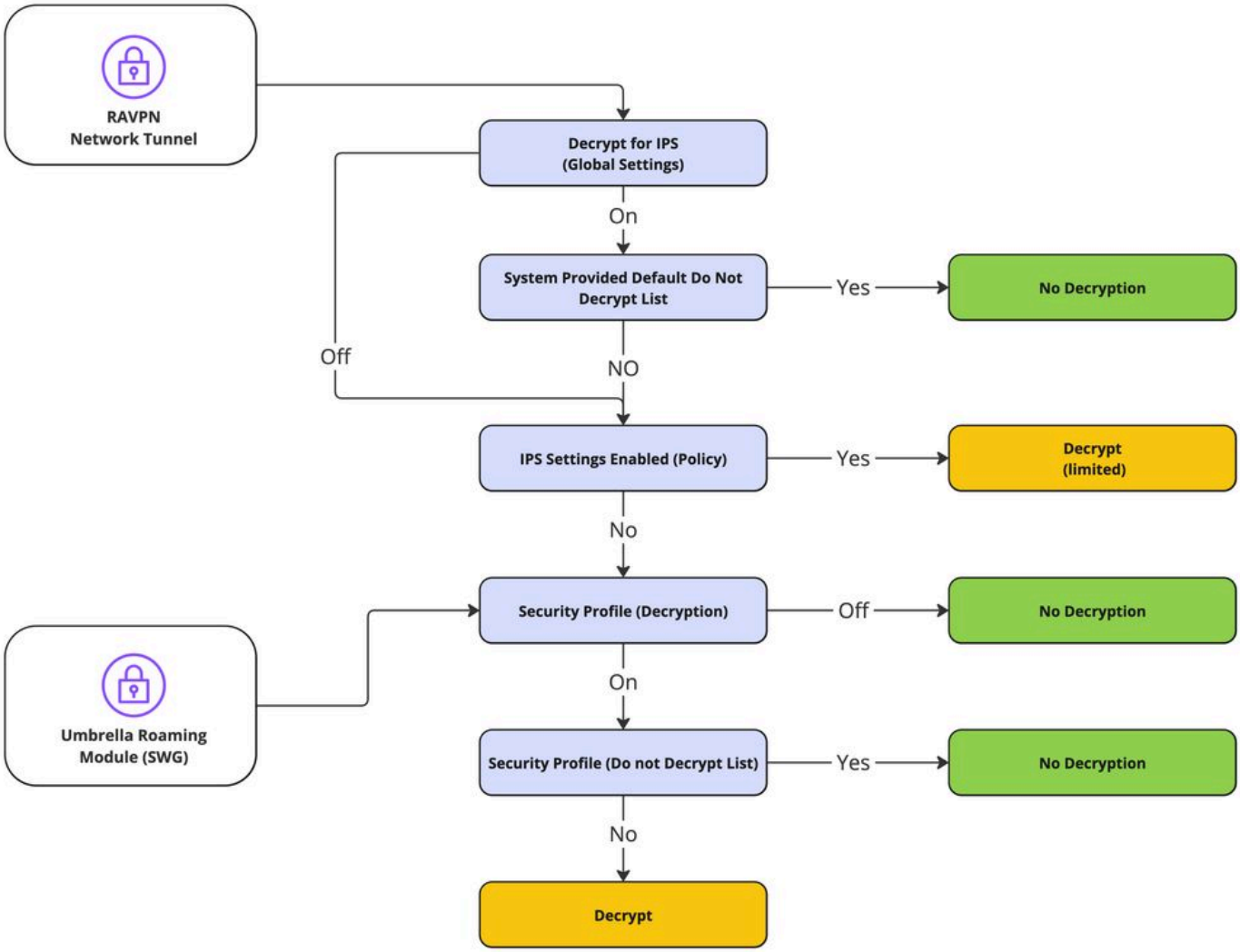
远程访问VPN (RAVPN)和零信任访问(ZTNA)共享相同的组件。

漫游安全模块（Umbrella模块）具有不同的流量路径。



预期何时解密流量

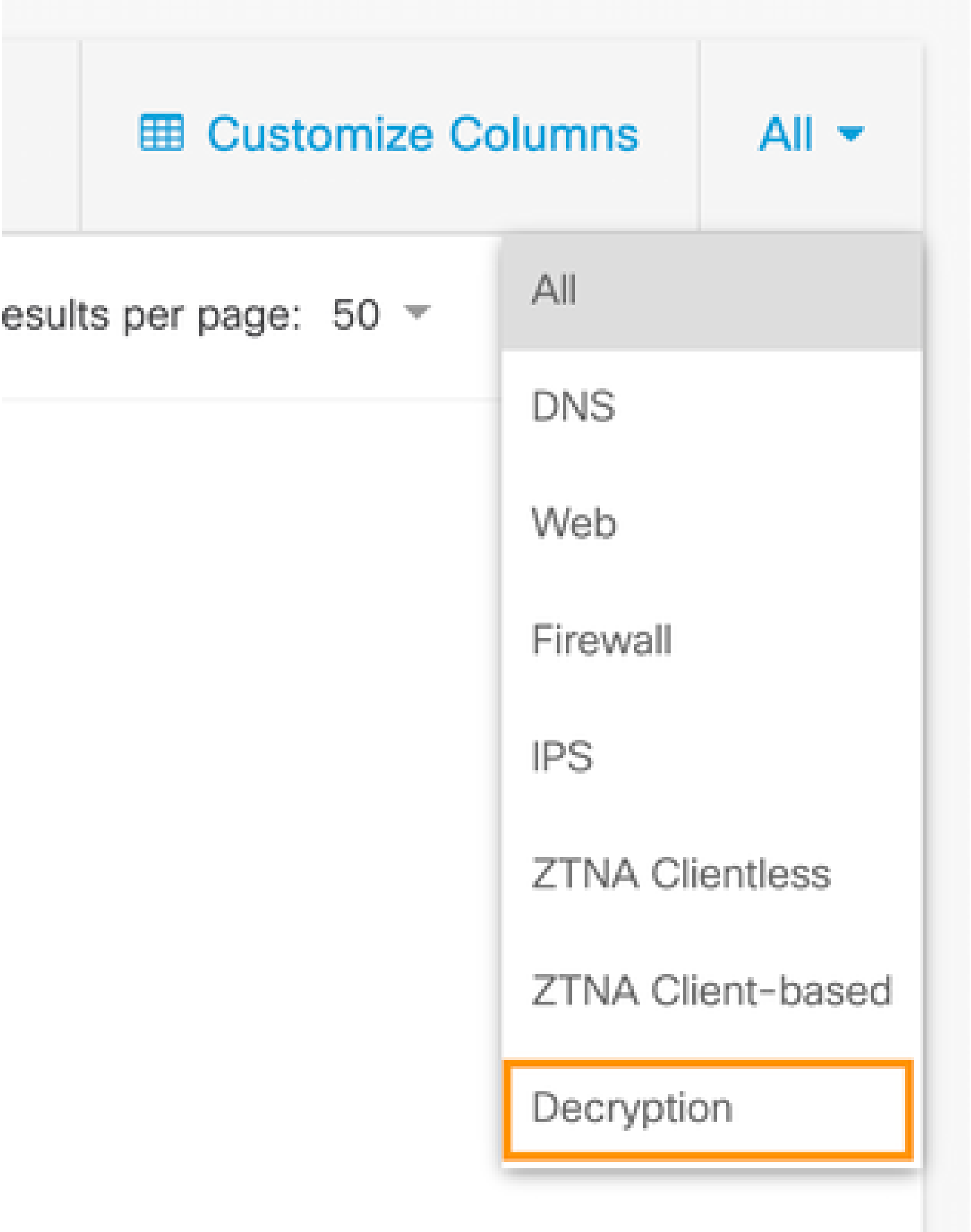
本节详细解释操作链及其解密或不解密的主要结果。

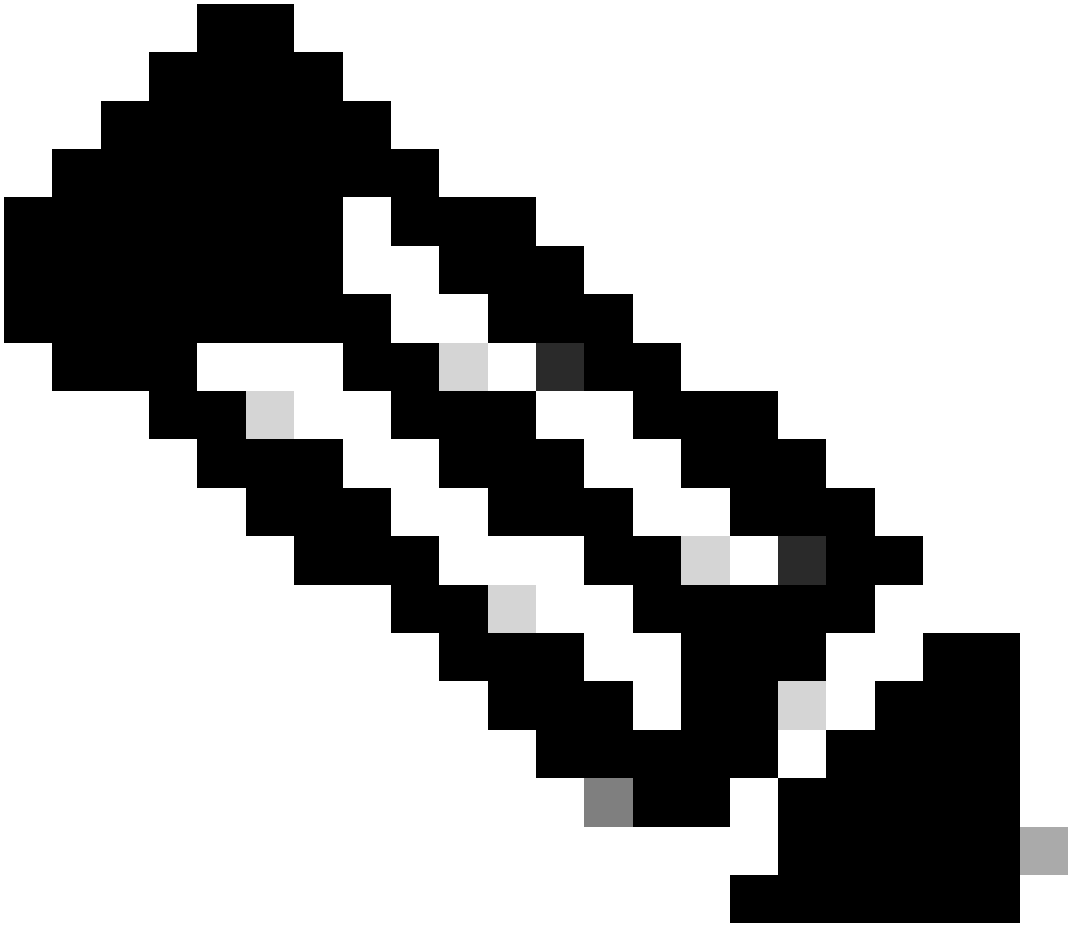


解密流程

解密与IPS相关的日志记录和报告

安全访问包括新的报告部分（解密），可通过控制面板->监控->活动搜索->切换到解密访问。

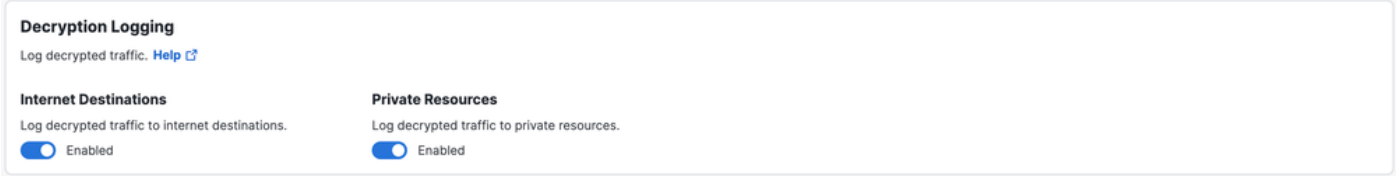

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



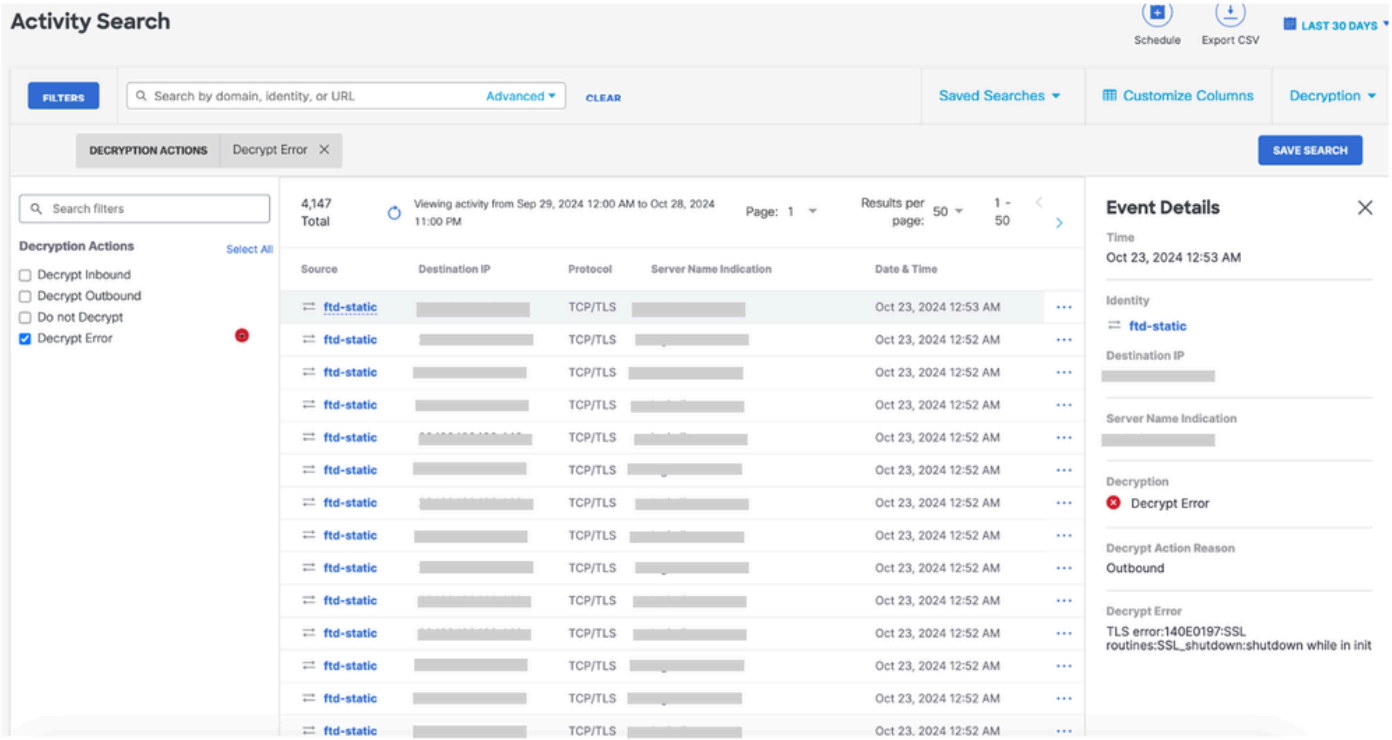
注意：要启用解密日志，可以在全局设置中启用此设置：

控制面板(Dashboard) ->安全(Secure) ->访问策略(Access Policy) ->规则默认值和全局设置(Rule Defaults and Global Settings) ->全局设置(Global Settings) ->解密日志记录(Decryption Logging)。

解密日志记录设置：



解密错误示例：



相关信息

- 安全访问用户指南
- 技术支持和下载 - 思科系统公司

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。