أستكشاف أخطاء سير عمل نظام منع التسلل (IPS) وفك تشفير الوصول الآمن وإصلاحها

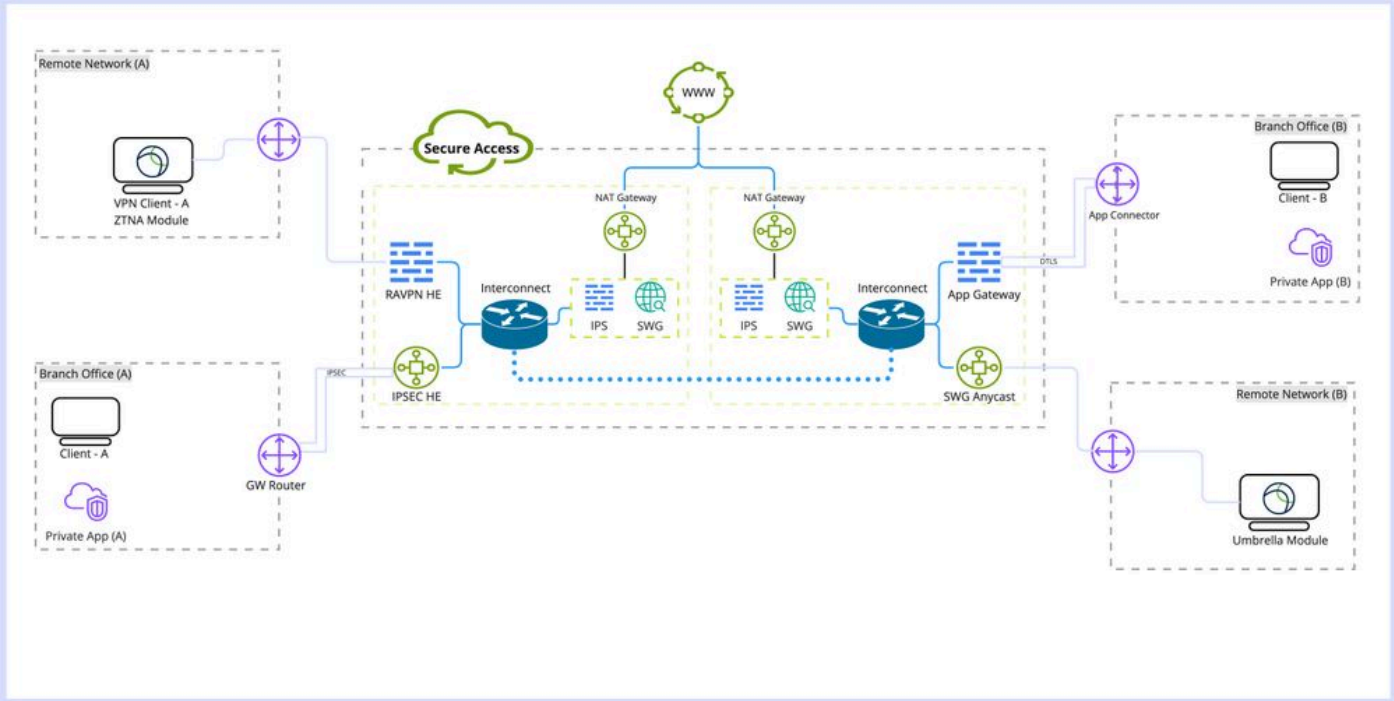
المحتويات

المقدمة

يصف هذا المستند فك تشفير الوصول الآمن وسير عمل IPS ويبرز خصائص الإعدادات المهمة.

بنية الوصول الآمن

تلقي بنية Secure Access هذه الضوء على الخدمات المختلفة التي يوفرها Secure Access وأساليب الاتصال المختلفة التي يمكن إنشاؤها لتأمين الشبكة.



بنية الوصول الآمن

تفاصيل البنية:

المصطلحات التي يجب أن تكون مألوفة:

RAVPN HE: نهاية رأس شبكة الوصول عن بعد الخاصة الظاهرية

IPSec HE: نهاية رأس أمان بروتوكول إنترنت النفق البعيد (IPSec)

الوحدة النمطية ZTNA: الوحدة النمطية Zero Trust Network Access Module

SWG: بوابة الويب الآمنة

IPS: نظام منع الحدس

عبارة NAT: عبارة ترجمة عنوان الشبكة

SWG AnyCast: نقطة مدخل AnyCast لبوابة الويب الآمنة

أنواع النشر:

1. شبكة VPN للوصول عن بعد

2. نفق الوصول عن بعد

3. وحدة التجوال Umbrella

4. موصل التطبيق/بوابة التطبيق

5. نموذج الثقة صفر (ZTNA)

نظرة عامة على الميزة

يوفر "الوصول الآمن" إمكانية تنفيذ كل من "نظام فك تشفير الويب" و"نظام منع التسلل" (IPS) لتحسين اكتشاف التطبيقات وتصنيفها وتوفير مزيد من التفاصيل حول حركة المرور. بما في ذلك مسارات URL وأسماء الملفات وفئة التطبيقات الخاصة بها. والمساعدة على منع الهجمات التي لا تستغرق سوى يوم واحد والبرامج الضارة.

فك التشفير: في هذه المقالة يتم الإشارة إلى فك تشفير حركة مرور بروتوكول نقل النص التشعبي (HTTPS) من خلال وحدة عبارة الويب الآمنة (SWG). وكذلك فك تشفير حركة مرور البيانات لتفتيش IPS.

IPS: نظام اكتشاف ومنع الاقتحام على مستوى جدار الحماية الذي يتطلب فك تشفير حركة المرور لتنفيذ الوظائف الكاملة.

يعد فك التشفير ضروريا لميزات الوصول الآمن المتعددة مثل منع فقدان البيانات (DLP) وعزل المستعرض البعيد (RBI) وفحص الملفات وتحليل الملفات وحظر نوع الملفات.

الإعدادات ذات الصلة بفك التشفير و IPS في الوصول الآمن

هذه نظرة عامة سريعة على الإعدادات المتاحة ذات الصلة بفك التشفير و IPS في "الوصول الآمن".

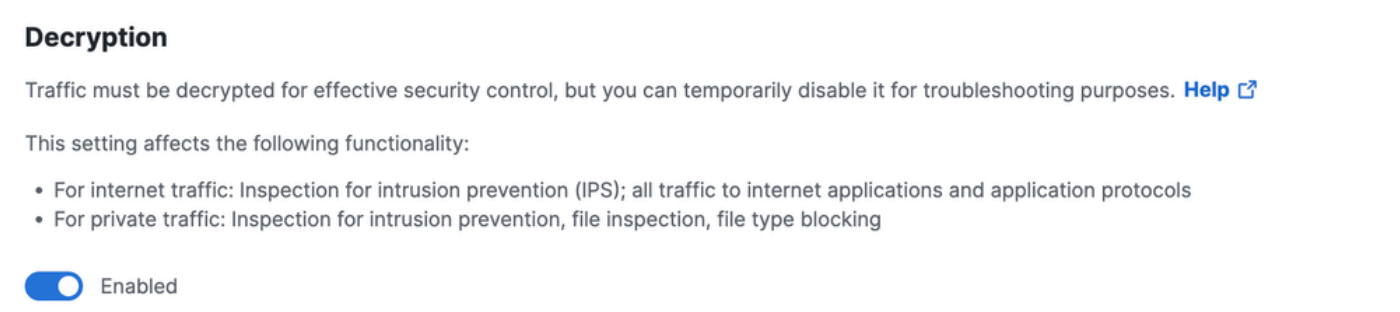
فك تشفير IPS

هذا إعداد عمومي لـ IPS يتم إستخدامه لتعطيل محرك IPS أو تمكينه لكافة النهج.

الخصائص:

- ال يؤثر هذا الخيار على فك تشفير بوابة الويب الآمنة (فك تشفير الويب)
- يتوفر تعطيل IPS وتمكينه لكل نهج مع وظائف محدودة لفحص المرحلة الأولية من المصافحة فقط دون فحص النص الأساسي للطلب.

التكوين: لوحة المعلومات -> Secure -> Access Policy -> Rule Default و Global Settings (إعدادات عامة) -> Decryption لـ IPS



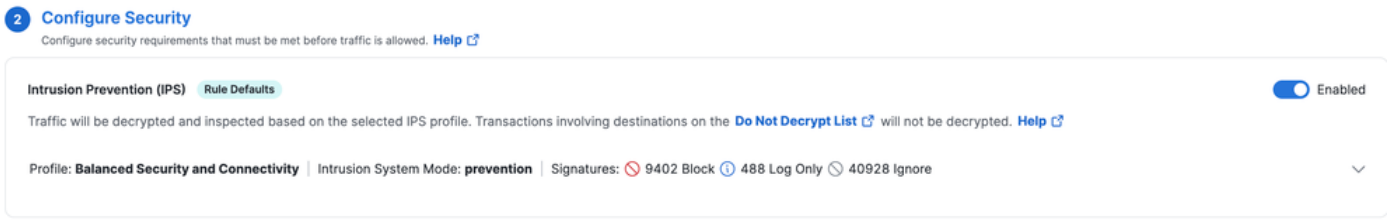
إعدادات IPS لكل نهج

يسمح هذا الخيار بتعطيل IPS وتمكينه لكل قواعد السياسة.

الخصائص:

- يتحكم هذا الخيار في تمكين IPS أو تعطيله لكل نهج.
- يعتمد هذا الخيار على فك التشفير لإعدادات IPS، إذا تم تعطيل خيار فك التشفير العام لـ IPS، فإنه يتسبب في أن يقوم السلوك بفحص المرحلة الأولية فقط من المصافحة دون فحص متن الطلب.
- لا يؤثر هذا الخيار على SWG (فك تشفير الويب)

التكوين: لوحة المعلومات -> آمنة -> سياسة الوصول ->تحرير السياسة -> تكوين الأمان -> منع التسلل (IPS)



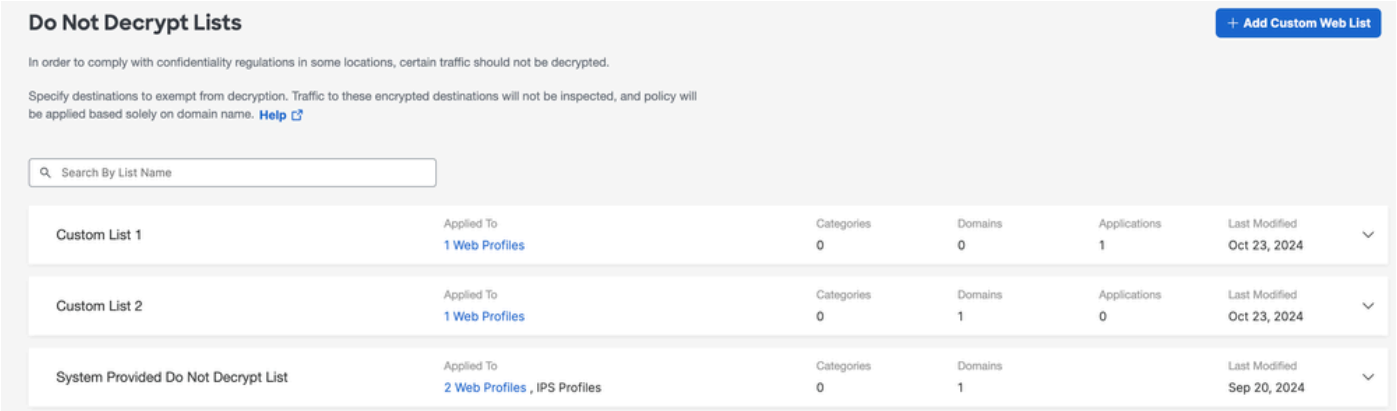
عدم فك تشفير القوائم

مجموعة من قوائم الوجهة التي يمكن ربطها بملف تعريف الأمان إلى مجالات التجاوز أو عناوين IP من أن يتم فك تشفيرها.

الخصائص:

- السماح بتجاوز المجالات المخصصة لفك تشفير ويب
- تؤثر هذه القائمة فقط على فك تشفير الويب وليس IPS باستثناء النظام الذي تم توفيره والا تقوم بفك تشفير القائمة
- يحتوي على (قائمة عدم فك تشفير النظام المتوفرة) التي تتجاوز كلا من IPS وفك تشفير الويب
- يجب دمج هذا الخيار مع توصيفات التأمين لإرفاقها بالسياسة
- يمكن إستخدام هذه القائمة فقط في حالة تمكين فك التشفير في توصيف التأمين

التكوين: لوحة المعلومات -> آمنة -> عدم فك تشفير القوائم



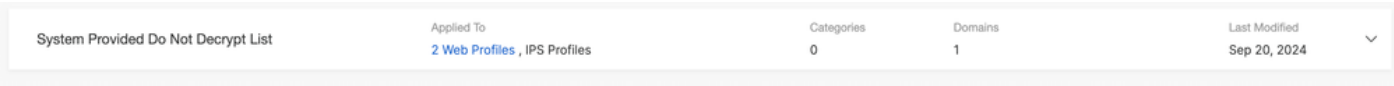
النظام المتوفر لا يتم فك تشفير القائمة

جزء من قواعد عدم فك التشفير، مع ميزة إضافية للتطبيق على كل من فك التشفير و IPS في الوصول الآمن.

الخصائص:

- هذه هي قائمة "عدم فك التشفير" المخصصة الوحيدة التي تؤثر على كل من IPS وفك تشفير الويب
- لا يوجد خيار لتخصيص هذه القائمة لكل نوع.

التكوين: لوحة المعلومات -> آمنة -> عدم فك تشفير القواعد -> النظام المتوفر لا تقوم بفك تشفير القائمة



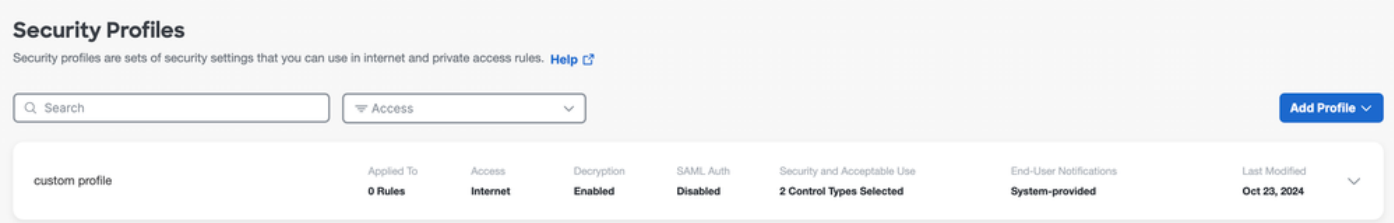
إعدادات توصيف التأمين

في إعدادات توصيف التأمين يمكنك تحديد تمكين أو تعطيل فك تشفير الويب الذي يمكن ربطه فيما بعد بنهج إنترنت. إذا تم تمكين فك التشفير، فلديك الخيار لتحديد إحدى قواعد عدم فك التشفير التي تم تكوينها.

الخصائص:

- التحكم في العديد من ميزات الأمان بما في ذلك فك تشفير الويب وعدم فك تشفير القواعد
- يؤثر النظام المرفق الموفر على كل من فك تشفير الويب وفك تشفير IPS في قائمة ملف تعريف الأمان

التكوين: لوحة المعلومات -> آمنة -> ملفات تعريف الأمان



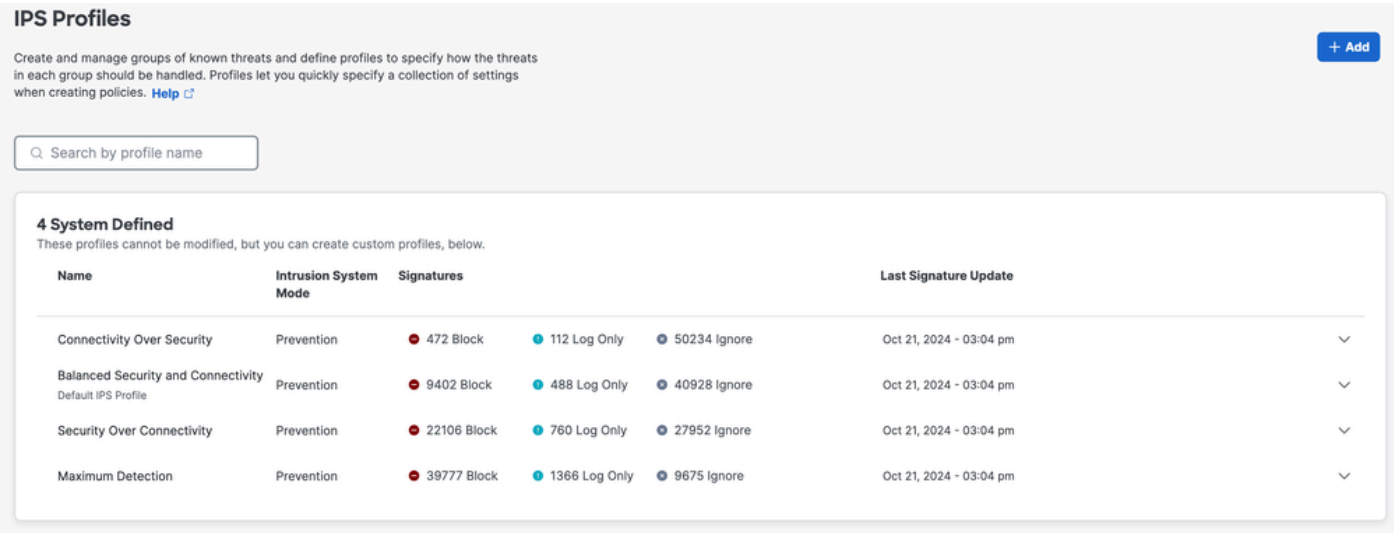
توصيفات IPS

تتضمن إعدادات توصيفات IPS أربعة إعدادات تأمين أساسية معرفة مسبقا لتوصيف IPS. ما يمكن تحديده لكل إعدادات النهج. لديك الخيار لإنشاء ملف تعريف IPS المخصص من أجل إعدادات أكثر صرامة أو مرونة.

الخصائص:

- يحتوي على أربعة توصيفات لمستويات أمان محددة مسبقا ل IPS
- يمكن إنشاء ملف تعريف IPS المخصص

التكوين: لوحة المعلومات -> آمنة -> توصيفات IPS

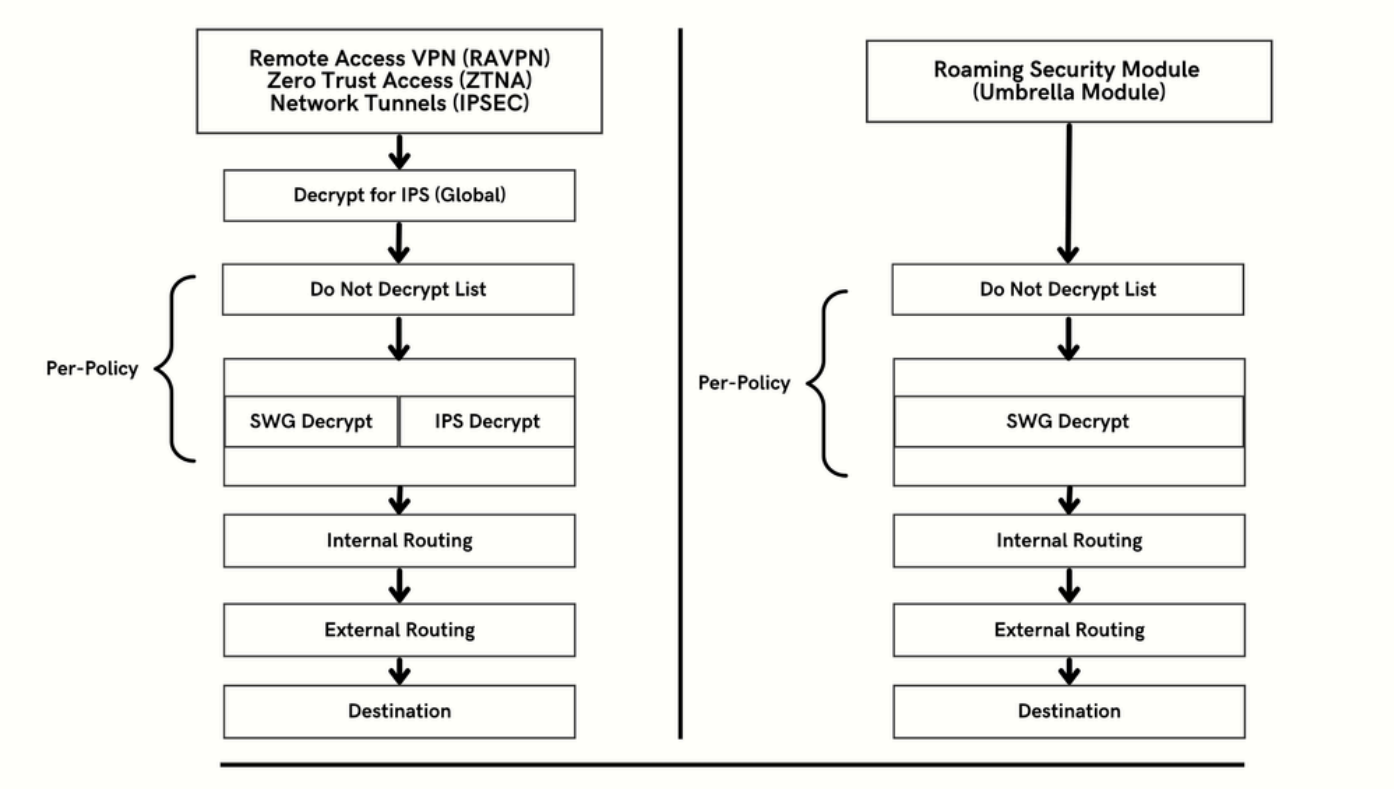


تدفق حركة مرور بيانات HTTPS في الوصول الآمن

يحتوي Secure Access على مسارات حركة مرور مختلفة استنادا إلى طريقة الاتصال.

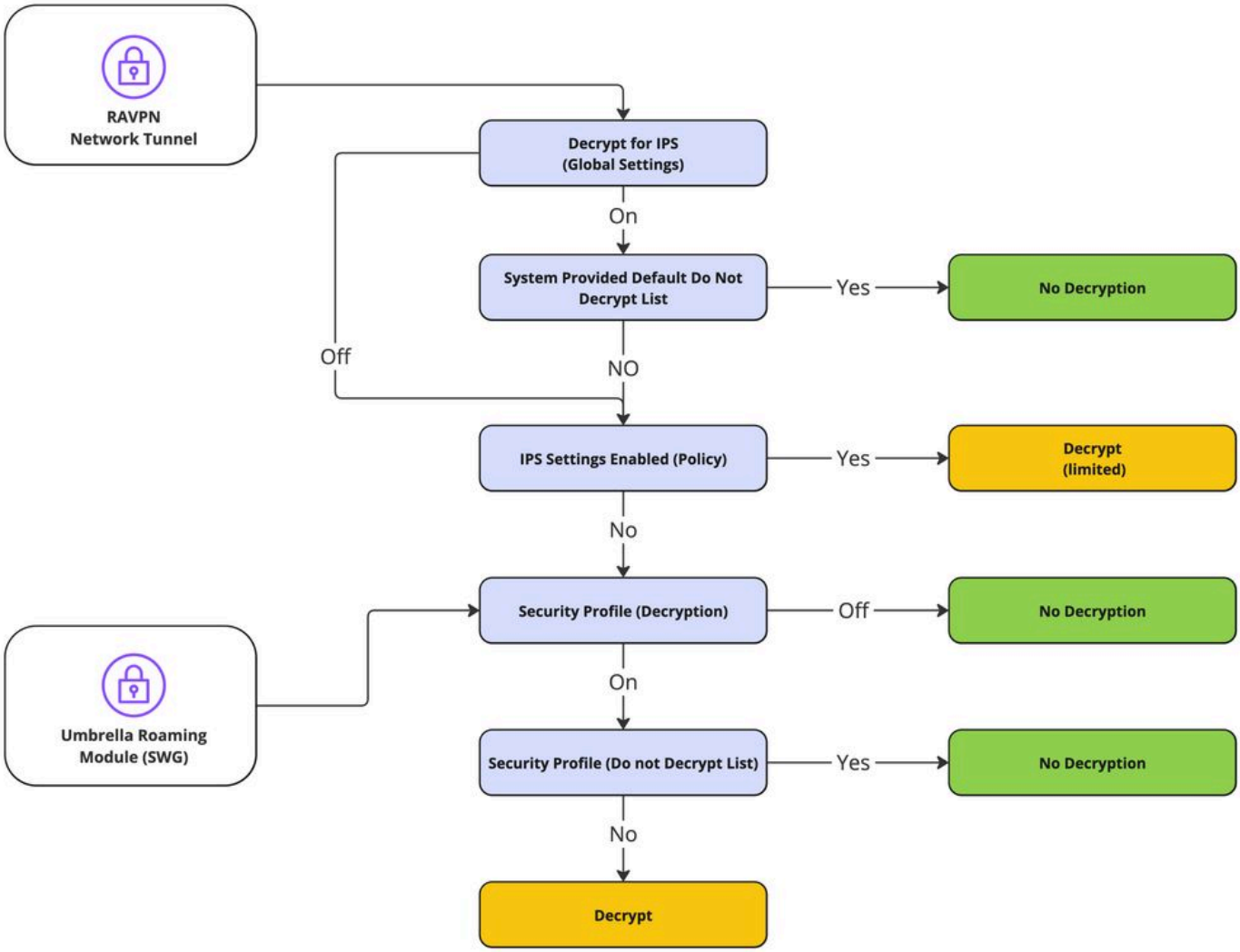
يتشارك كل من Remote Access VPN (RAVPN) و Zero Trust Access (ZTNA) في المكونات نفسها.

تحتوي وحدة أمان التجوال (الوحدة النمطية Umbrella Module) على مسار حركة مرور مختلف.



متى يمكن فك تشفير حركة المرور

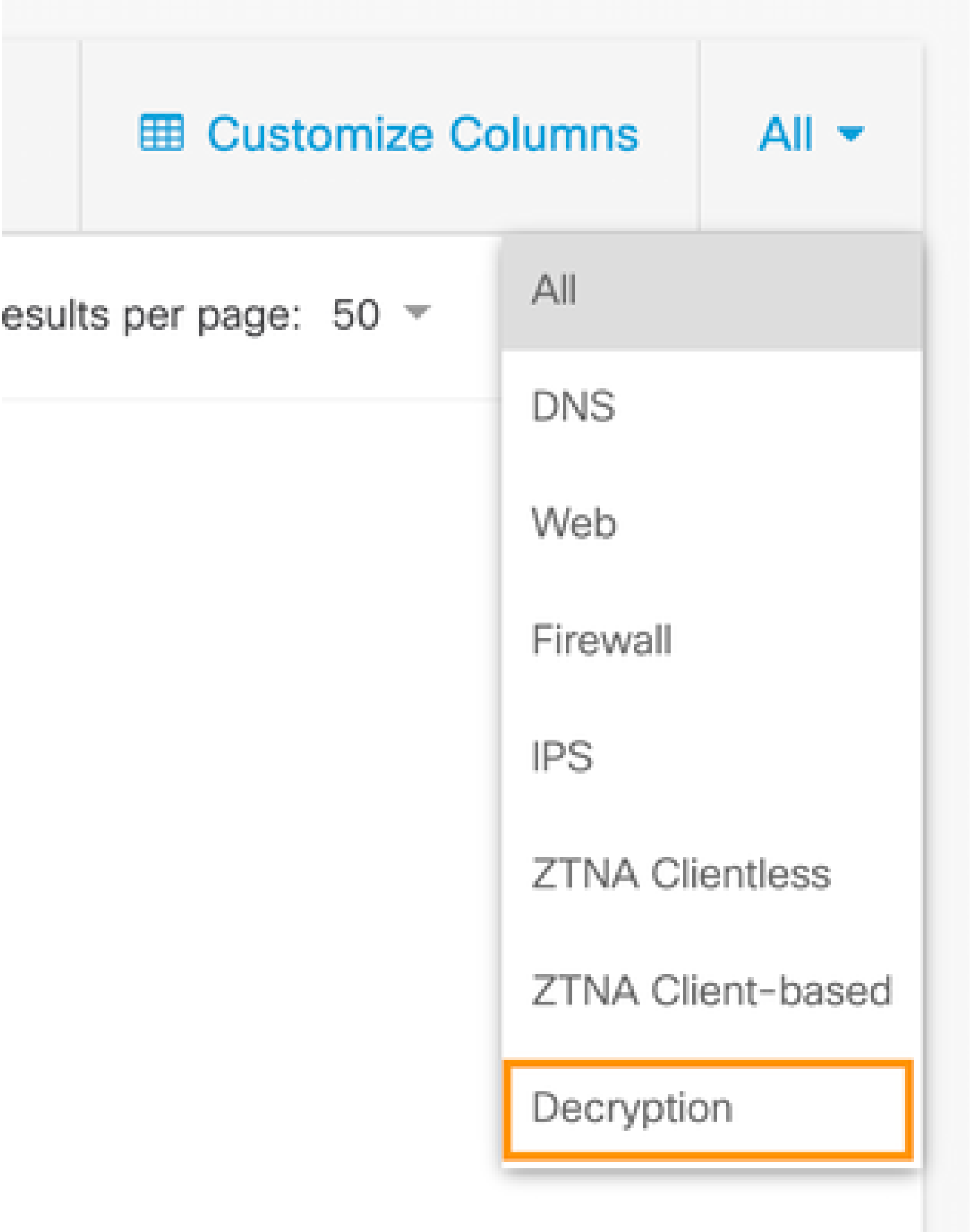
يشرح هذا القسم بالتفصيل سلسلة الإجراءات والنتائج الرئيسية الخاصة بما لفك التشفير أو عدم فك التشفير.

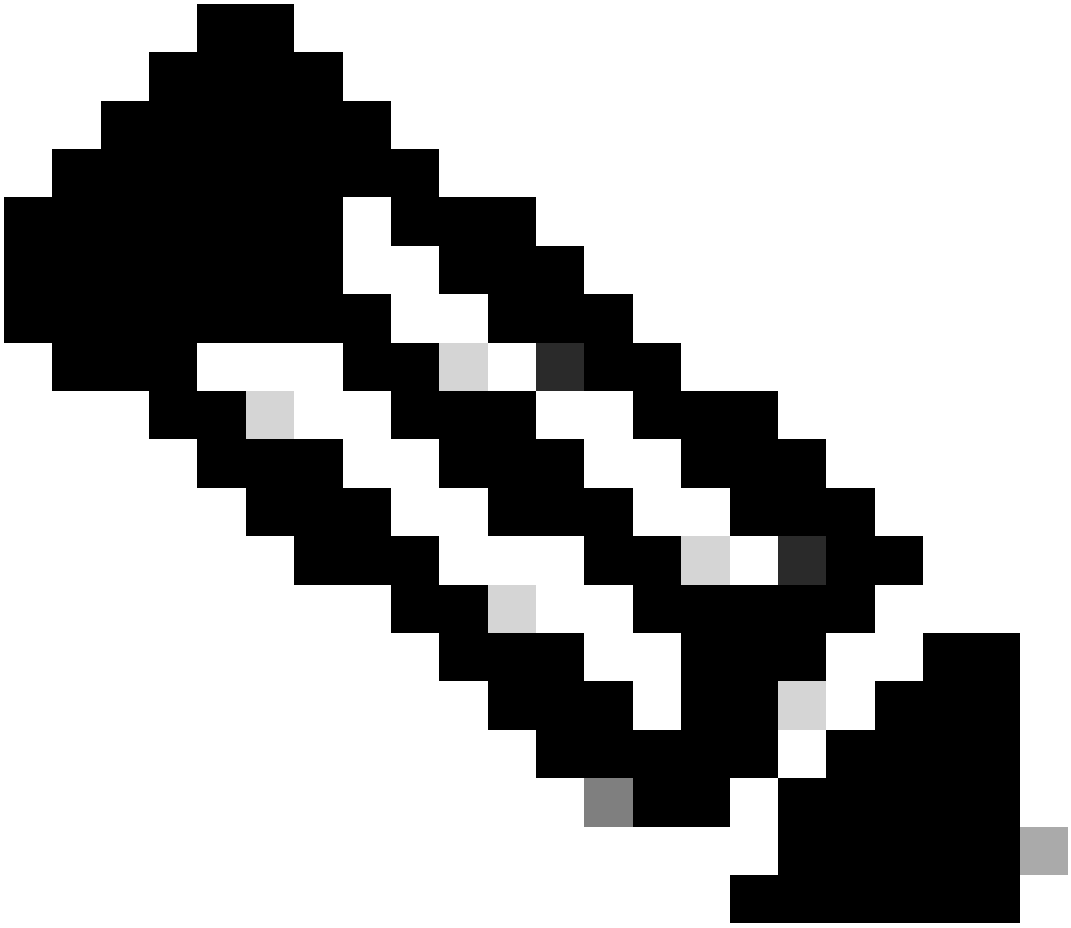


تدفق فك الترميز

إلغاء التشفير والتسجيل وإعداد التقارير ذات الصلة ب IPS

يتضمن Secure Access قسم التقارير الجديد (فك التشفير) الذي يمكن الوصول إليه من خلال لوحة المعلومات -> الشاشة -> البحث عن النشاط -> المحول إلى فك التشفير.

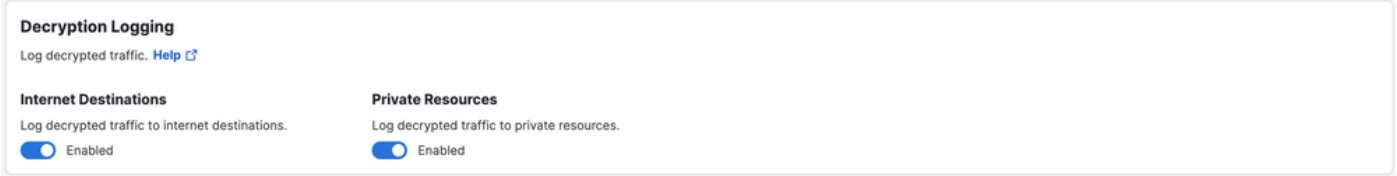

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



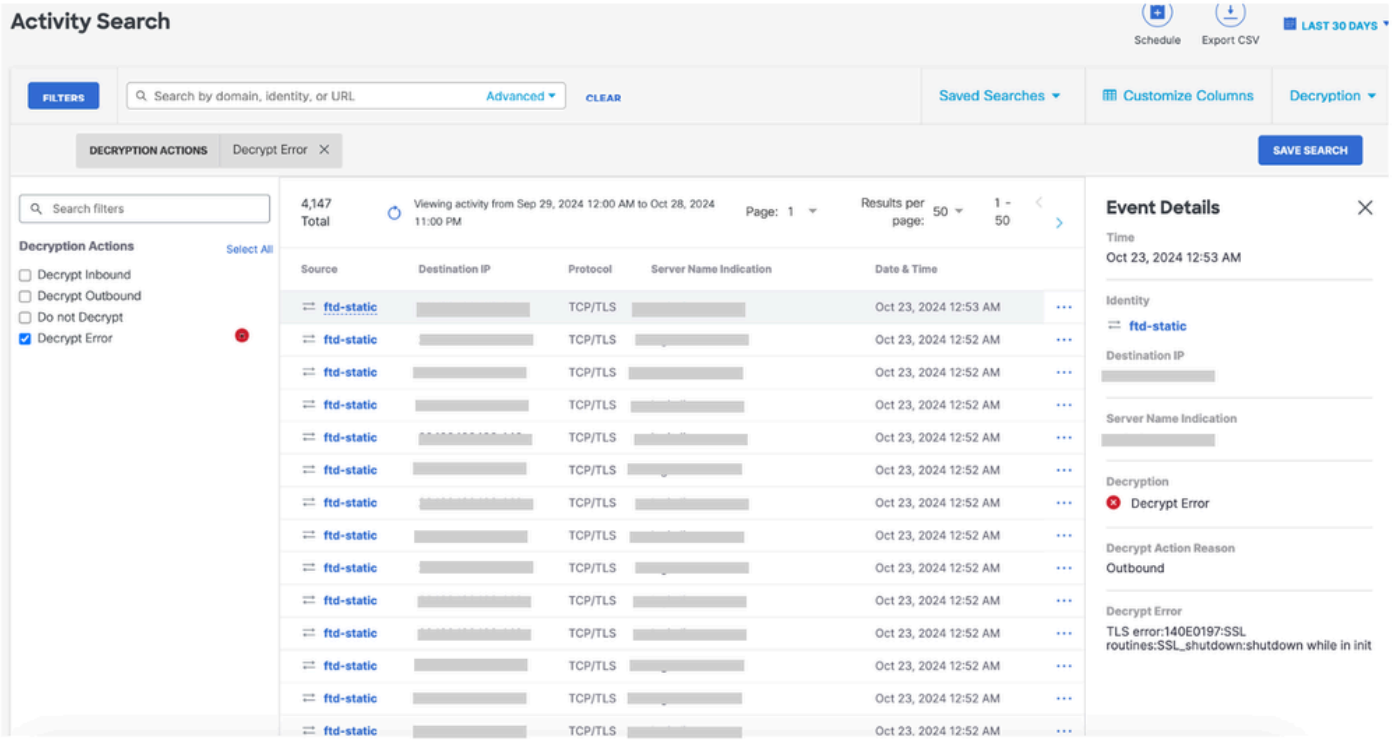
ملاحظة: لتمكين سجلات فك التشفير، يمكن تمكين هذا الإعداد على الإعدادات العمومية:

لوحة المعلومات -> Secure -> Access Policy -> الإعدادات الافتراضية للقواعد والإعدادات العامة -> Global Settings (الإعدادات العامة) -> تسجيل فك التشفير.

إعدادات تسجيل فك التشفير:



مثال لخطأ فك التشفير:



معلومات ذات صلة

- [دليل مستخدم Secure Access]
- [الدعم الفني والتنزيلات - Cisco Systems]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).