Secure Access Decryption and Intrusion Prevention System(IPS) 워크플로 문제 해결

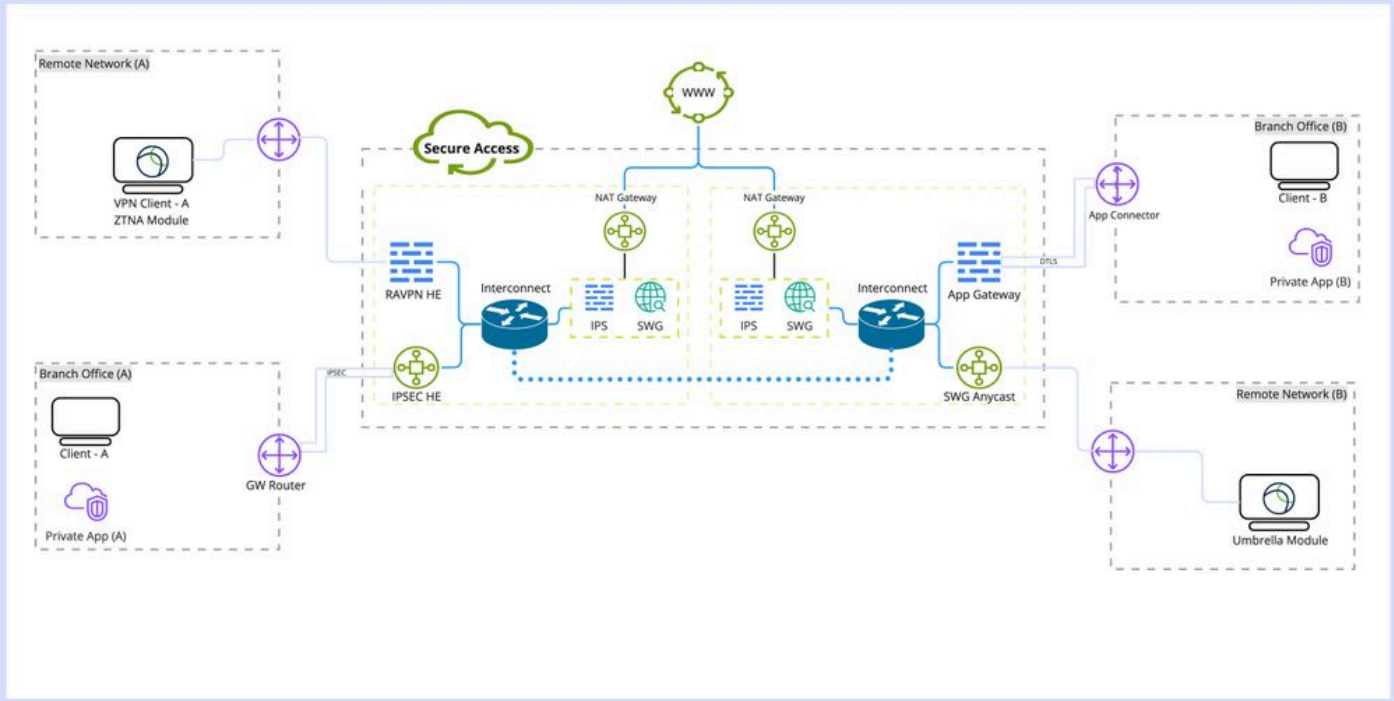
목차

소개

이 문서에서는 Secure Access Decryption and IPS 워크플로에 대해 설명하고 중요한 설정 속성을 강조 표시합니다.

보안 액세스 아키텍처

이 Secure Access 아키텍처는 Secure Access가 제공하는 다양한 서비스와 네트워크 보안을 위해 설정할 수 있는 다양한 연결 방법을 강조합니다.



보안 액세스 아키텍처

아키텍처 세부사항:

숙지해야 할 용어:

RAVPN HE: 원격 액세스 Virtual Private Network 헤드 엔드

IPSEC HE: IPSEC(Remote Tunnel Internet Protocol Security) 헤드 엔드

ZTNA 모듈: 제로 트러스트 네트워크 액세스 모듈

SWG: 보안 웹 게이트웨이

IPS: 침입 방지 시스템

NAT 게이트웨이: 네트워크 주소 변환 게이트웨이

SWG AnyCast: Secure Web Gateway Anycast 인그레스 포인트

구축 유형:

1. 원격 액세스 VPN

2. 원격 액세스 터널

3. Umbrella 로밍 모듈

4. 애플리케이션 커넥터/애플리케이션 게이트웨이

5. ZTNA(제로 트러스트 모듈)

기능 개요

Secure Access는 웹 암호 해독 및 IPS(Intrusion Prevention System)를 모두 수행하여 애플리케이션 탐지 및 범주화를 향상하고, URL 경로, 파일 이름, 해당 애플리케이션 범주 등 트래픽에 대한 세부 정보를 제공하며, 제로 데이 공격 및 악성코드 방지를 지원합니다.

암호 해독: 이 문서에서는 암호 해독을 SWG(Secure Web Gateway) 모듈을 통한 HTTPS(Hyper Text Transfer Protocol) 트래픽 해독 및 IPS 검사를 위한 트래픽 해독이라고도 합니다.

IPS: 완벽한 기능을 수행하려면 트래픽에 대한 암호 해독이 필요한 방화벽 수준의 침입 탐지 및 방지 시스템

DLP(Data Loss Prevention) 및 RBI(Remote Browser Isolation), 파일 검사, 파일 분석 및 파일 유형 차단과 같은 여러 보안 액세스 기능에 암호 해독이 필요합니다.

Secure Access의 암호 해독 및 IPS 관련 설정

Secure Access에서 사용 가능한 암호 해독 및 IPS 관련 설정을 간략하게 설명합니다.

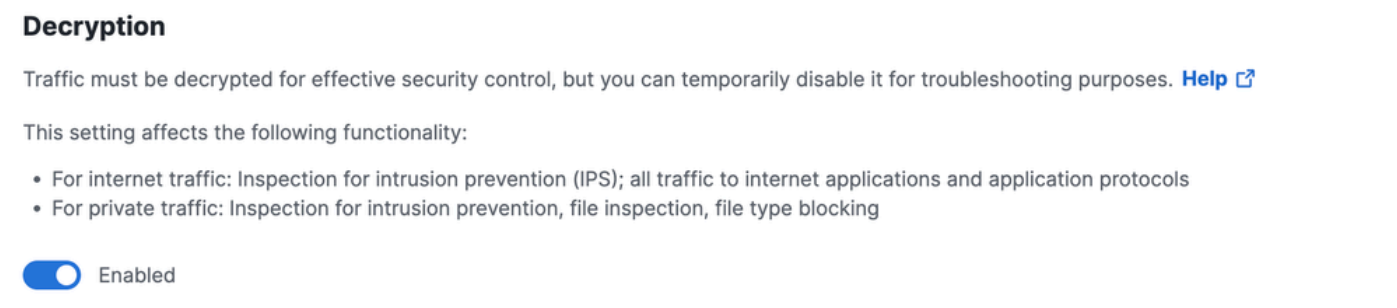
IPS 암호 해독

모든 정책에 대해 IPS 엔진을 비활성화하거나 활성화하는 데 사용되는 IPS에 대한 전역 설정입니다.

속성:

- 이 옵션은 보안 웹 게이트웨이 암호 해독(웹 암호 해독)에는 영향을 주지 않습니다
- 제한적으로 정책당 IPS 비활성화 및 활성화를 사용할 수 있으며 요청의 본문을 검사하지 않고 핸드셰이크의 초기 단계만 검사할 수 있습니다.

설정: 대시보드 -> 보안 -> 액세스 정책 -> 규칙 기본값 및 전역 설정 -> 전역 설정 -> IPS 암호 해독



정책당 IPS 설정

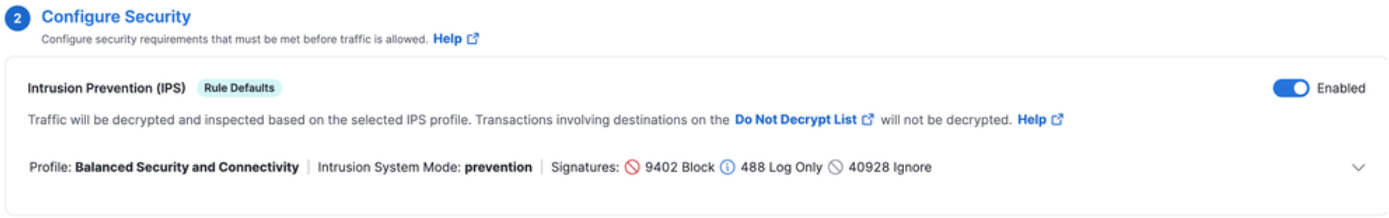
이 옵션을 사용하면 정책 기반별로 IPS를 비활성화하고 활성화할 수 있습니다.

속성:

- 이 옵션은 정책별로 IPS의 활성화 여부를 제어합니다.

- 이 옵션은 Decrypt for IPS 설정에 따라 달라집니다. 전역 Decrypt for IPS 옵션이 비활성화된 경우 동작은 요청의 본문을 검사하지 않고 핸드셰이크의 초기 단계만 검사합니다.
- 이 옵션은 SWG(웹 암호 해독)에 영향을 주지 않습니다

구성: 대시보드 -> 보안 -> 액세스 정책 -> 정책 편집 -> 보안 구성 -> 침입 방지(IPS)



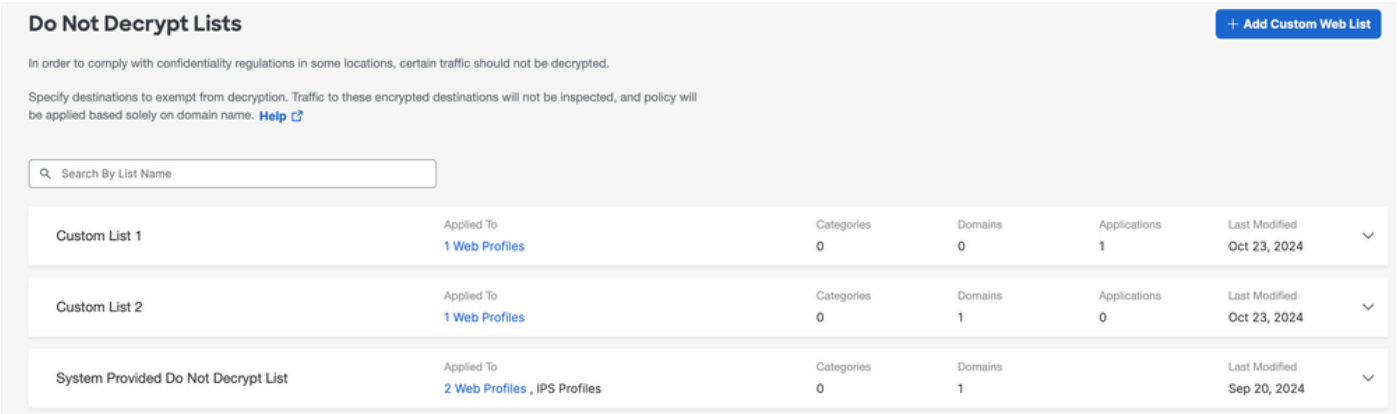
목록 해독 안 함

도메인 또는 IP 주소의 암호 해독을 우회하기 위해 보안 프로필에 연결할 수 있는 대상 목록 집합입니다.

속성:

- 사용자 지정 도메인이 웹 암호 해독을 우회하도록 허용
- 이 목록은 IPS가 아닌 웹 암호 해독에만 적용됩니다. 단, 제공된 시스템 암호 해독 안 함 목록은 예외입니다.
- IPS 및 웹 암호 해독을 모두 우회하는 (시스템 제공 암호 해독 안 함 목록) 포함
- 이 옵션은 보안 프로필과 함께 정책에 연결해야 합니다
- 이 목록은 보안 프로필에서 암호 해독이 활성화된 경우에만 사용할 수 있습니다

구성: Dashboard(대시보드) -> Secure(보안) -> Do Not Decrypt Lists(목록 해독 안 함)



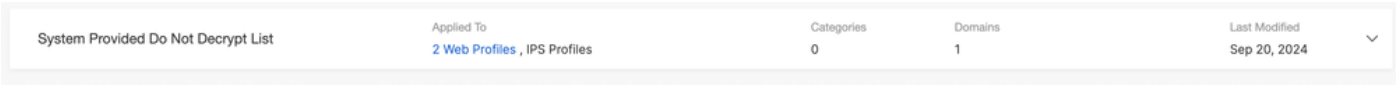
시스템에서 제공한 Do Not Decrypt 목록

Do Not Decrypt(암호 해독 안 함) 목록의 일부이며, Secure Access에서 암호 해독 및 IPS에 모두 적용하는 추가 기능이 있습니다.

속성:

- 이 목록은 IPS 및 웹 암호 해독 모두에 영향을 미치는 유일한 사용자 지정 Do Not Decrypt 목록입니다
- 정책별로 이 목록을 사용자 지정할 수 있는 옵션은 없습니다.

구성: Dashboard(대시보드) -> Secure(보안) -> Do Not Decrypt Lists(목록 해독 안 함) -> System Provided Do Not Decrypt List(시스템 제공 목록 해독 안 함)



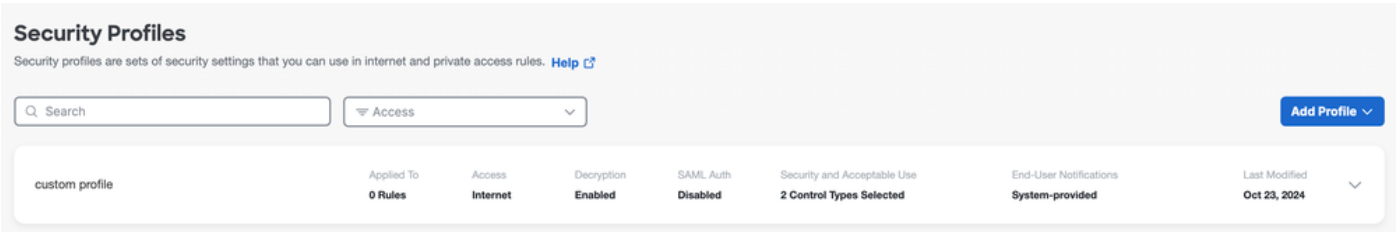
보안 프로파일 설정

보안 프로파일 설정에서 나중에 인터넷 정책과 연결할 수 있는 웹 암호 해독 활성화 또는 비활성화를 선택할 수 있습니다. Decryption(해독)이 활성화된 경우 Do Not Decrypt(해독 안 함) 목록 중 하나를 선택할 수 있습니다.

속성:

- 웹 암호 해독 및 Do Not Decrypt 목록을 비롯한 여러 보안 기능을 제어합니다.
- 제공된 Do Not Decrypt List를 보안 프로파일에 연결하는 것은 웹 암호 해독 및 IPS 암호 해독 모두에 영향을 미칩니다

구성: 대시보드 -> 보안 -> 보안 프로파일



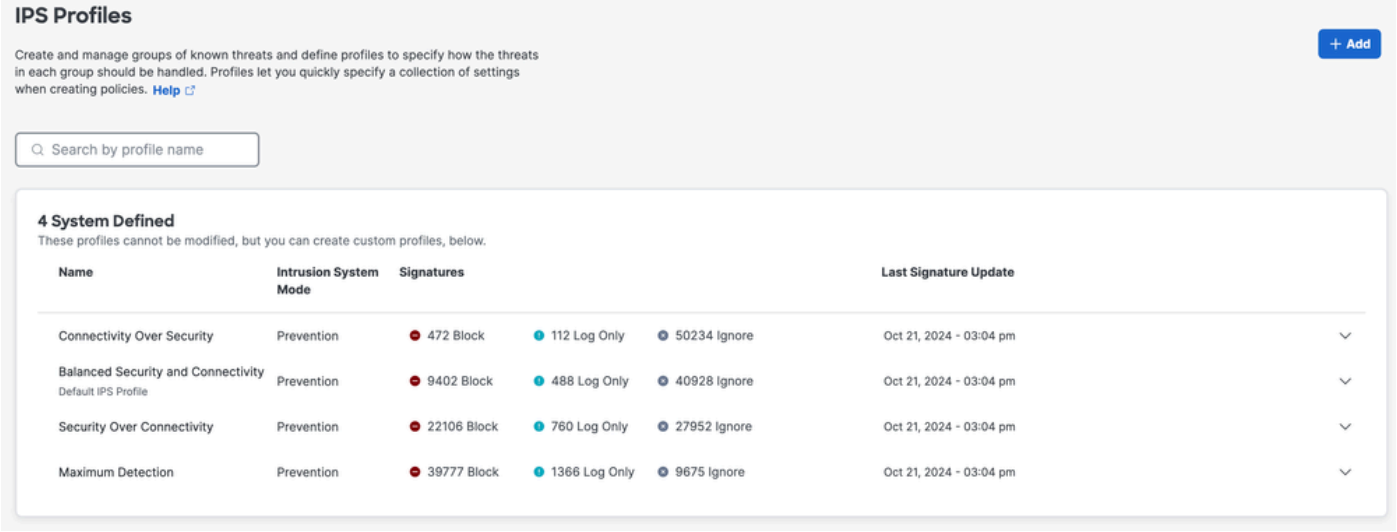
IPS 프로필

IPS 프로필 설정에는 IPS 프로필에 대한 4가지 기본 사전 정의 보안 설정이 포함됩니다. 정책 설정별로 선택할 수 있습니다. 더 엄격하거나 유연한 설정을 위해 사용자 지정 IPS 프로필을 직접 만들 수 있습니다.

속성:

- IPS에 대해 사전 정의된 4개의 보안 레벨 프로파일 포함
- 맞춤형 IPS 프로필 생성 가능

구성: 대시보드 -> 보안 -> IPS 프로파일

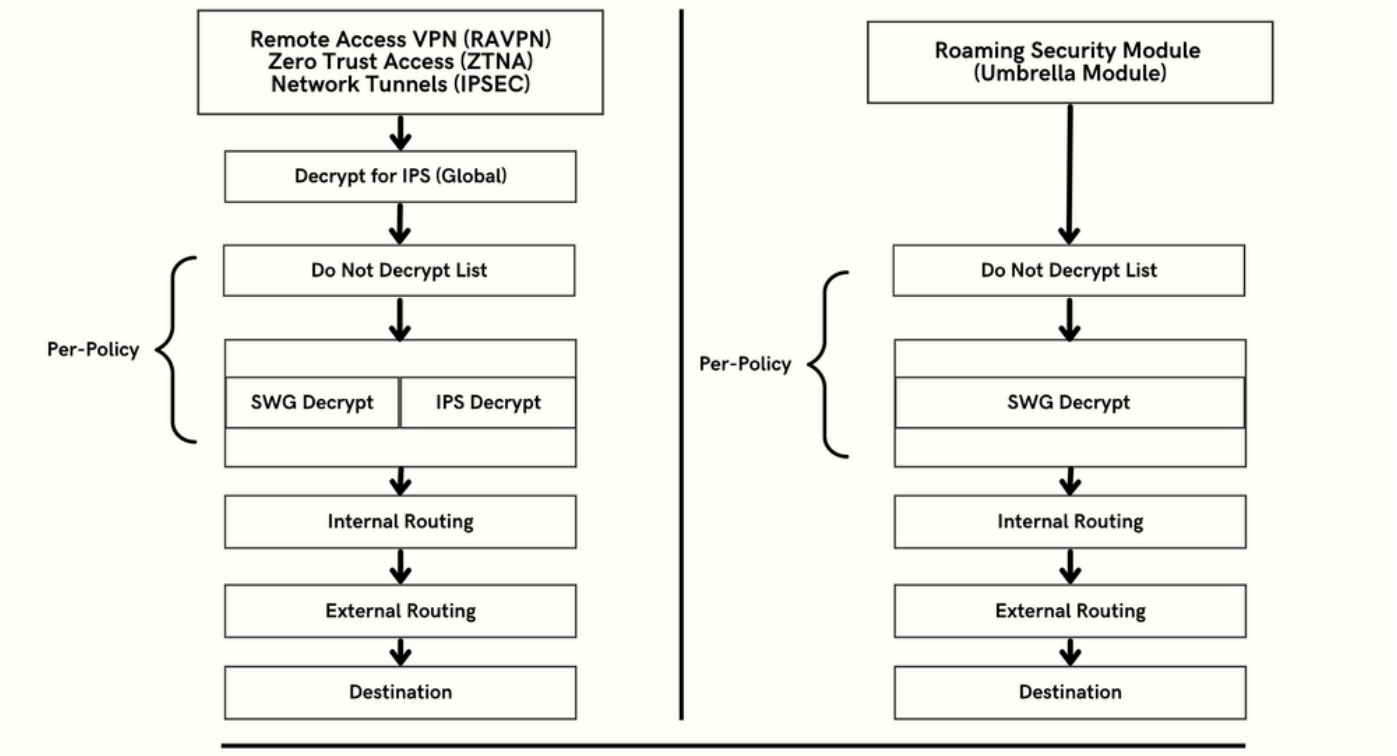


보안 액세스의 HTTPS 트래픽 흐름

Secure Access는 연결 방법에 따라 트래픽 경로가 다릅니다.

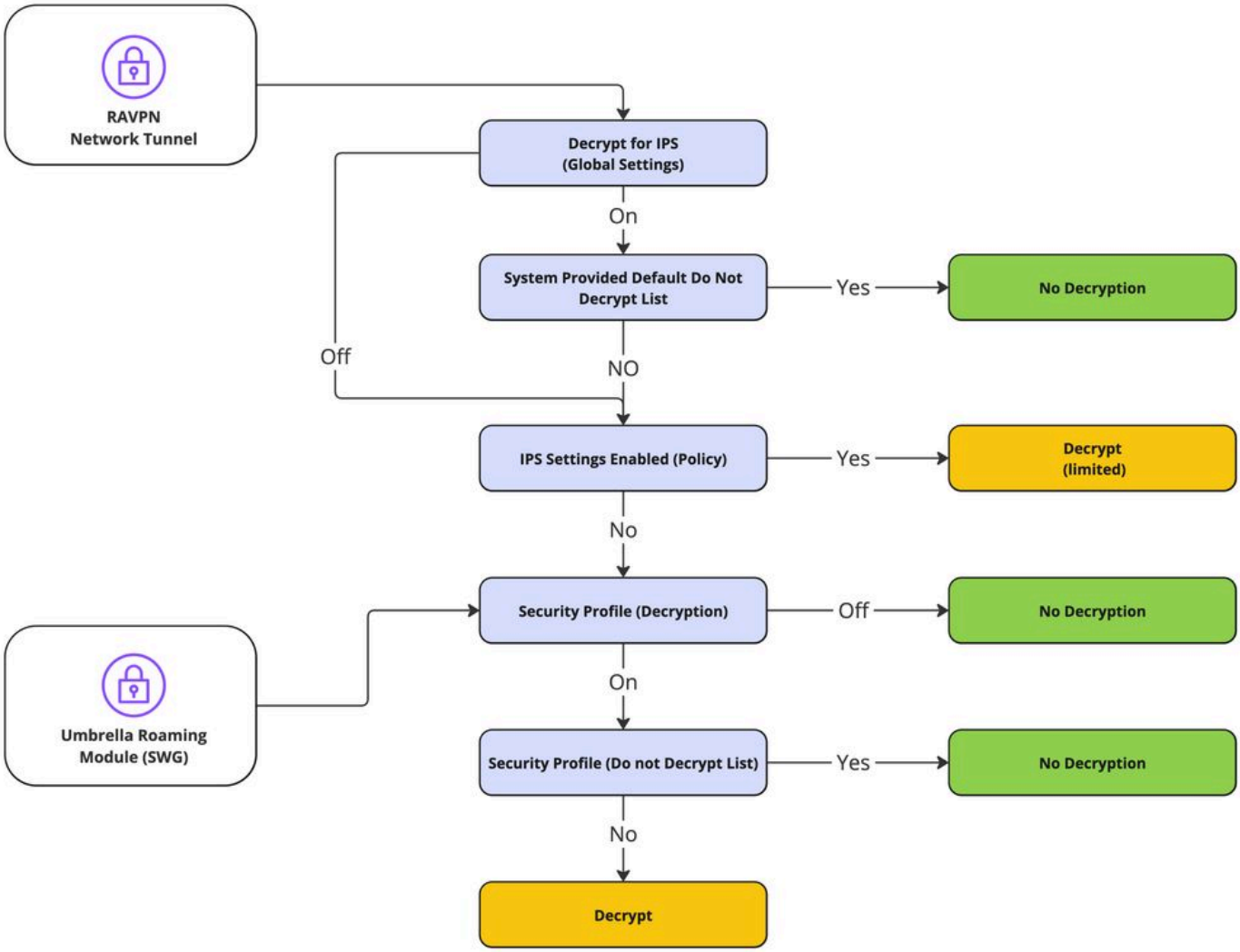
RAVPN(Remote Access VPN) 및 ZTNA(Zero Trust Access)는 동일한 구성 요소를 공유합니다.

로밍 보안 모듈(Umbrella 모듈)의 트래픽 경로가 다릅니다.



트래픽이 해독될 것으로 예상하는 시기

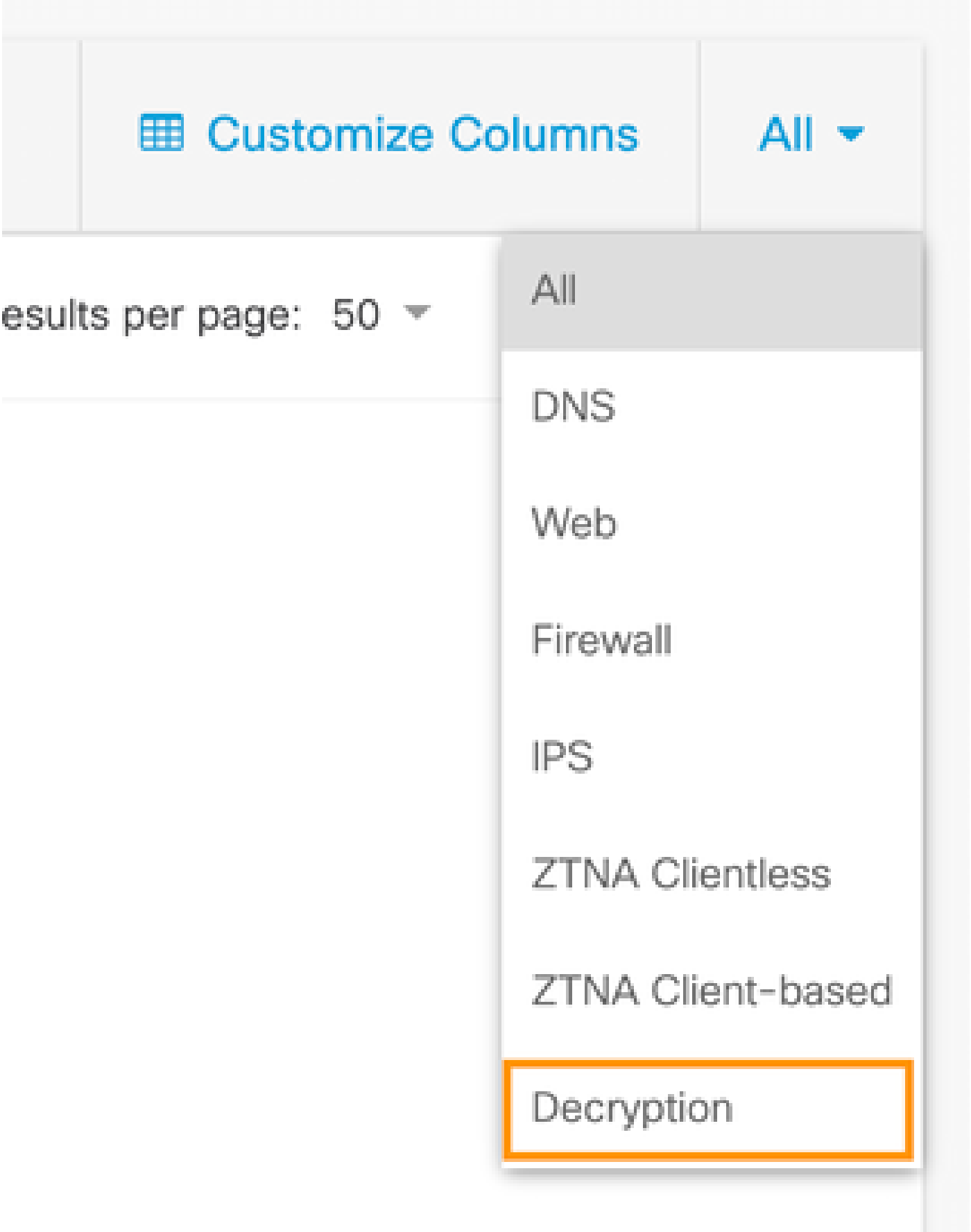
이 섹션에서는 작업의 체인 및 암호 해독의 선행 결과 또는 암호 해독이 없는 결과에 대해 자세히 설명합니다.

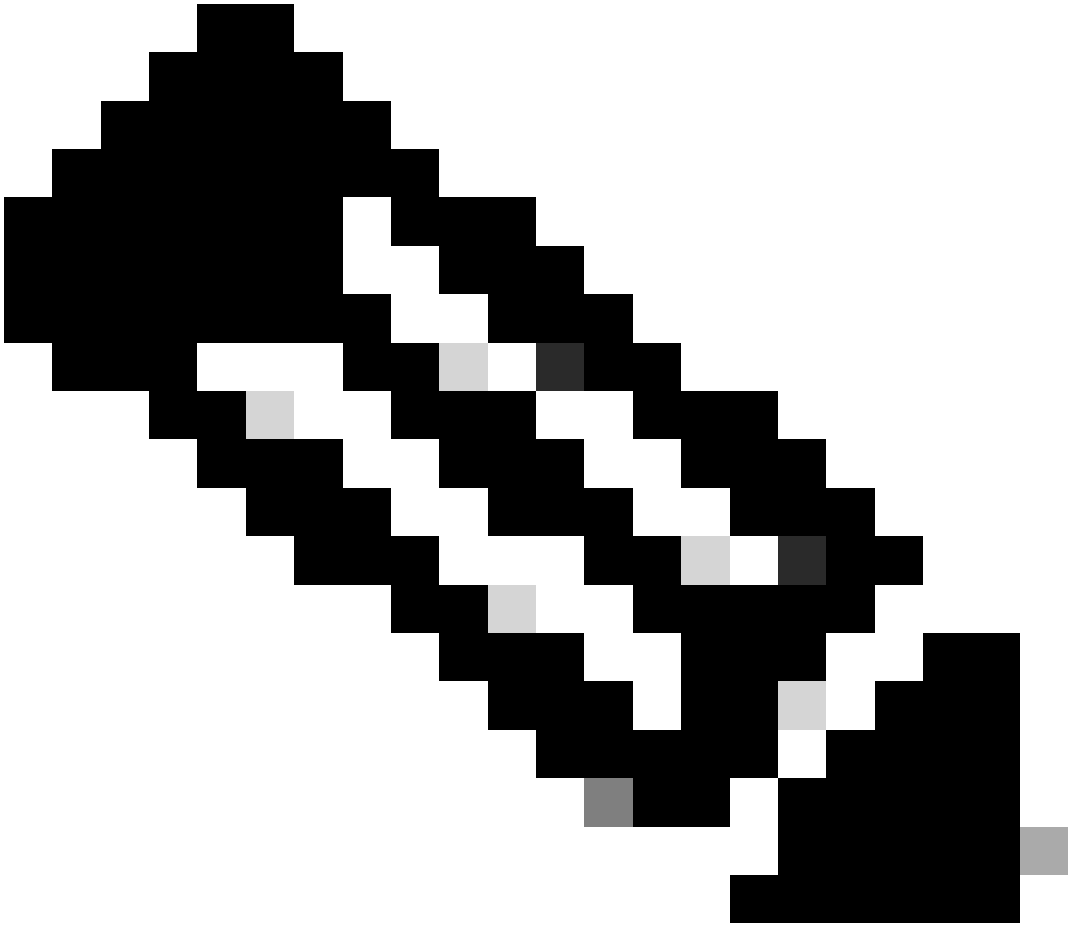


암호 해독 흐름

암호 해독 및 IPS 관련 로깅 및 보고

Secure Access에는 Dashboard(대시보드) -> Monitor(모니터) -> Activity Search(활동 검색) -> Switch to Decryption(암호 해독으로 전환)을 통해 액세스할 수 있는 새 보고 섹션(암호 해독)이 포함되어 있습니다.

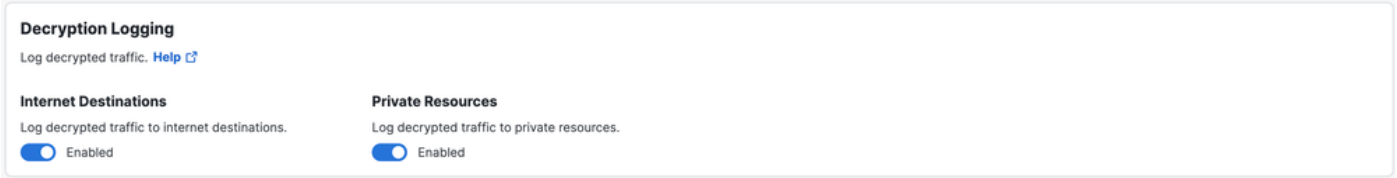

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



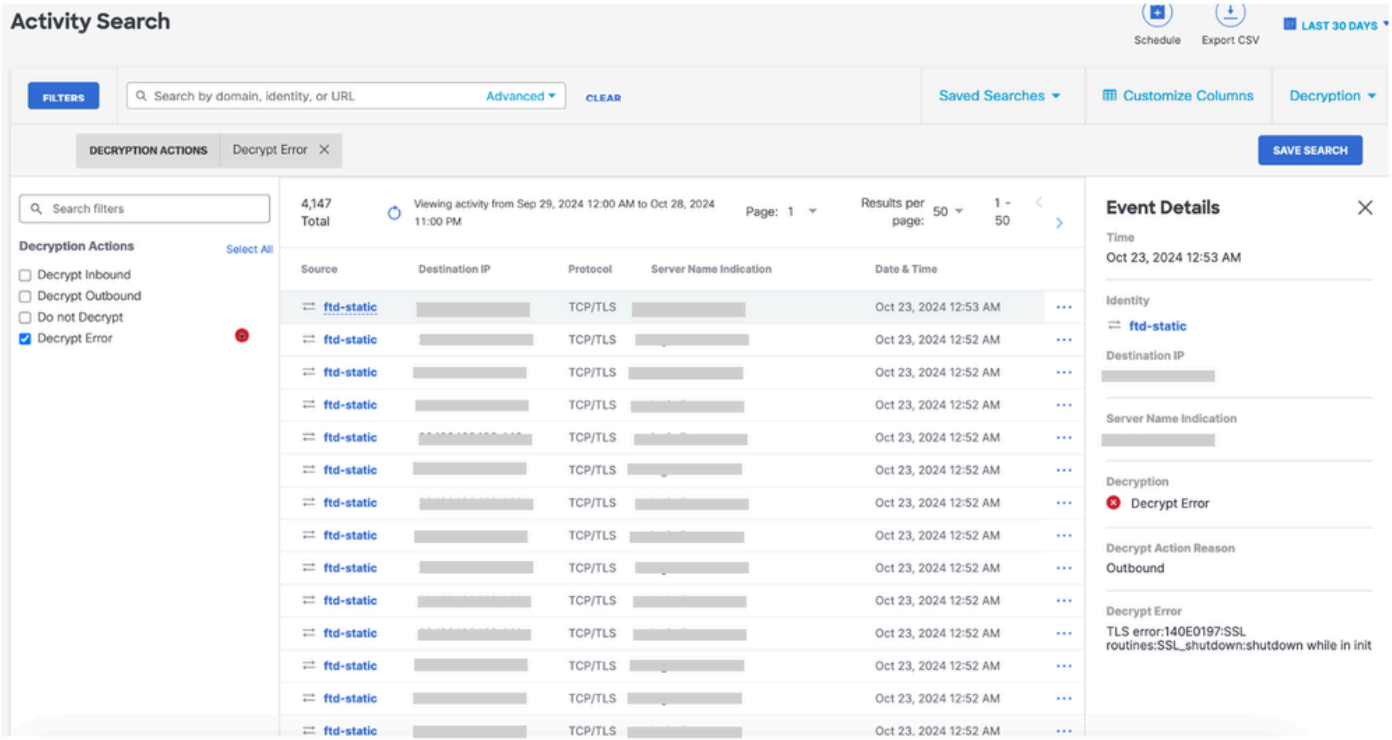
참고: 암호 해독 로그를 사용하려면 전역 설정에서 이 설정을 사용하도록 설정할 수 있습니다.

대시보드 -> 보안 -> 액세스 정책 -> 규칙 기본값 및 전역 설정 -> 전역 설정 -> 암호 해독 로깅.

암호 해독 로깅 설정:



암호 해독 오류의 예:



관련 정보

- [Secure Access 사용 설명서]
- [기술 지원 및 다운로드 - Cisco Systems]

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.