Solucionar problemas do fluxo de trabalho do Secure Access Decryption and Intrusion Prevention System (IPS)

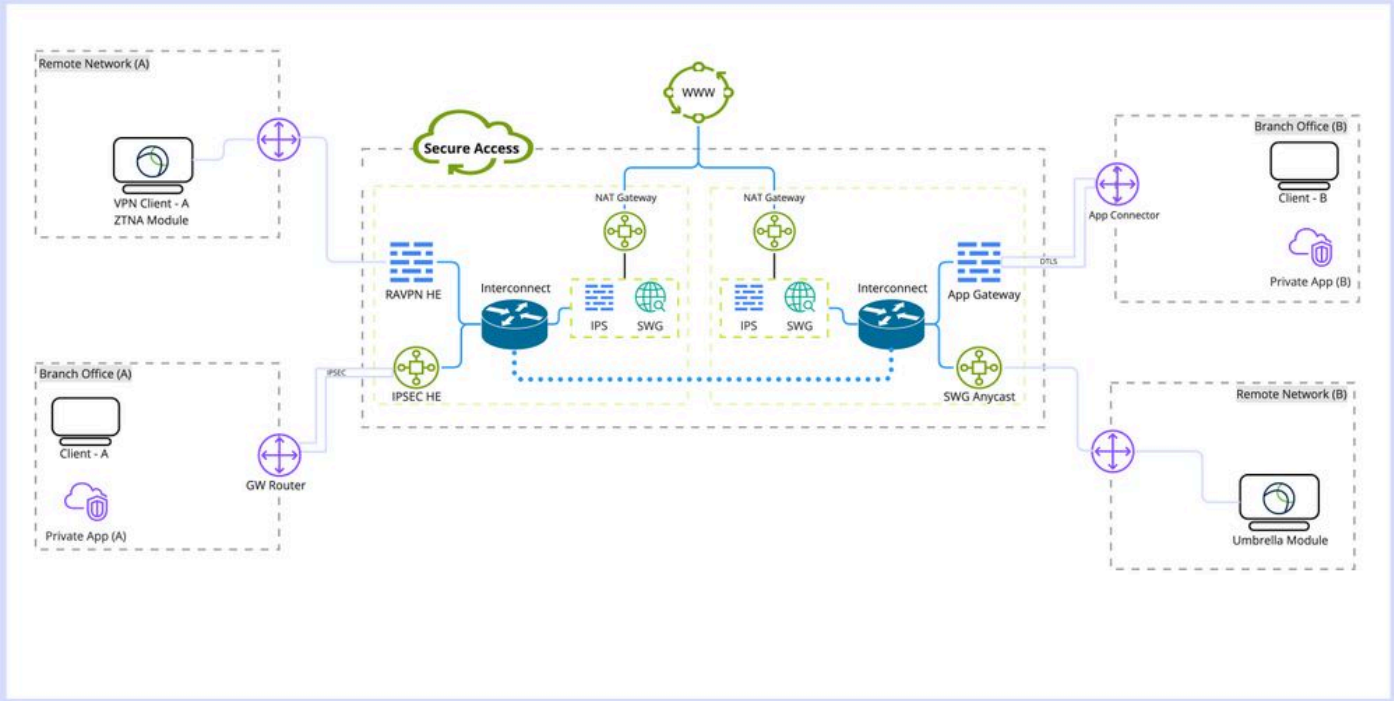
Contents

Introdução

Este documento descreve a Descriptografia de Acesso Seguro e o fluxo de trabalho de IPS e destaca as propriedades importantes das configurações.

Arquitetura de acesso seguro

Essa arquitetura de acesso seguro destaca os diferentes serviços fornecidos pelo acesso seguro e os diferentes métodos de conexão que podem ser estabelecidos para proteger a rede.



Arquitetura de acesso seguro

Detalhes da arquitetura:

Termos com os quais se familiarizar:

RAVPN HE: Central da Rede Virtual Privada de Acesso Remoto

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

Módulo ZTNA: Módulo de Acesso à Rede Zero Trust

SWG: Gateway da Web seguro

IPS: Sistema de prevenção de invasão

Gateway NAT: Gateway de conversão de endereço de rede

SWG AnyCast: ponto de entrada Secure Web Gateway Anycast

Tipos de Implantação:

1. VPN de acesso remoto

2. Túnel de acesso remoto

3. Módulo Umbrella Roaming

4. Conector de Aplicativos/Gateway de Aplicativos

5. Módulo Zero Trust (ZTNA)

Visão geral do recurso

O Secure Access oferece a capacidade de executar o Web Decryption and Intrusion Prevention System (IPS) para aprimorar a detecção e a categorização de aplicativos, além de fornecer mais detalhes sobre o tráfego, incluindo caminhos de URL, nomes de arquivos e suas categorias de aplicativos, e ajudar a evitar ataques de dia zero e malware.

Descriptografia: neste artigo, a descriptografia é chamada de Descriptografando o tráfego do protocolo HTTPS por meio do módulo SWG (Secure Web Gateway) e também Descriptografando o tráfego para inspeção de IPS.

IPS: Sistema de Detecção e Prevenção de Intrusão no nível do firewall que requer Descriptografia para tráfego para executar a funcionalidade completa.

A decodificação é necessária para vários recursos de acesso seguro, como prevenção de perda de dados (DLP) e isolamento de navegador remoto (RBI), inspeção de arquivos, análise de arquivos e bloqueio de tipos de arquivos.

Configurações relacionadas a decodificação e IPS no Secure Access

Esta é uma visão geral rápida das configurações relacionadas a decodificação e IPS disponíveis no Secure Access.

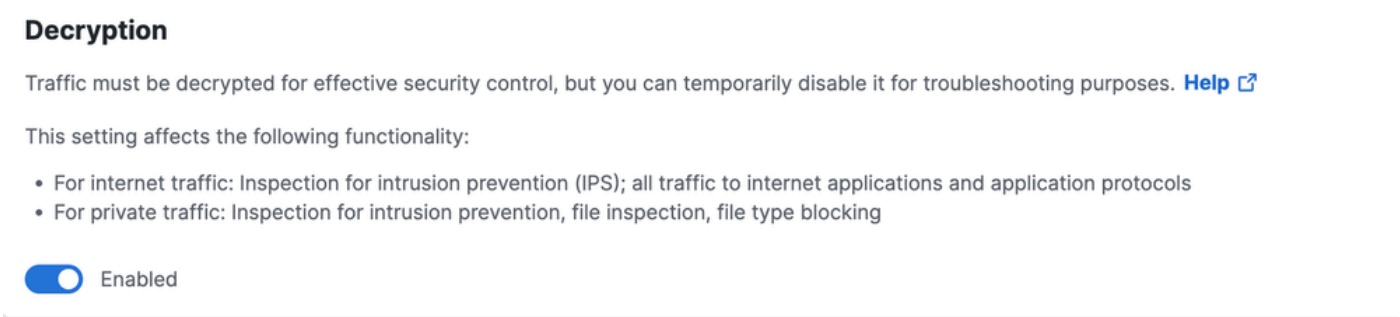
Descriptografia para IPS

Esta é uma configuração global do IPS que é usada para desabilitar ou habilitar o mecanismo IPS para todas as políticas.

Propriedades:

- Essa opção não afeta a Descriptografia segura do gateway da Web (Descriptografia da Web)
- Desativar e ativar o IPS por política está disponível com funcionalidade limitada para inspecionar apenas a fase inicial do handshake sem inspecionar o corpo da solicitação.

Configuração: Painel -> Seguro -> Política de acesso -> Padrões de regra e Configurações globais -> Configurações globais -> Descriptografia para IPS



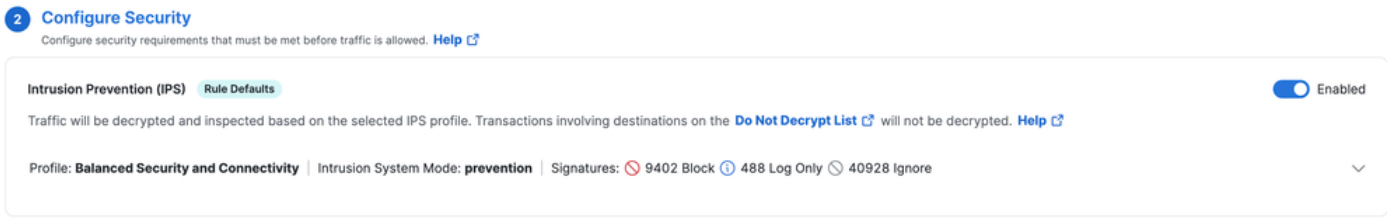
Configurações de IPS por política

Essa opção permite desativar e ativar o IPS por bases de política.

Propriedades:

- Esta opção controla se o IPS é habilitado ou desabilitado por política.
- Essa opção depende das configurações de Descriptografar para IPS. Se a opção global Descriptografar para IPS estiver desativada, isso fará com que o comportamento inspecione apenas a fase inicial do handshake sem inspecionar o corpo da solicitação.
- Essa opção não afeta o SWG (Descriptografia da Web)

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



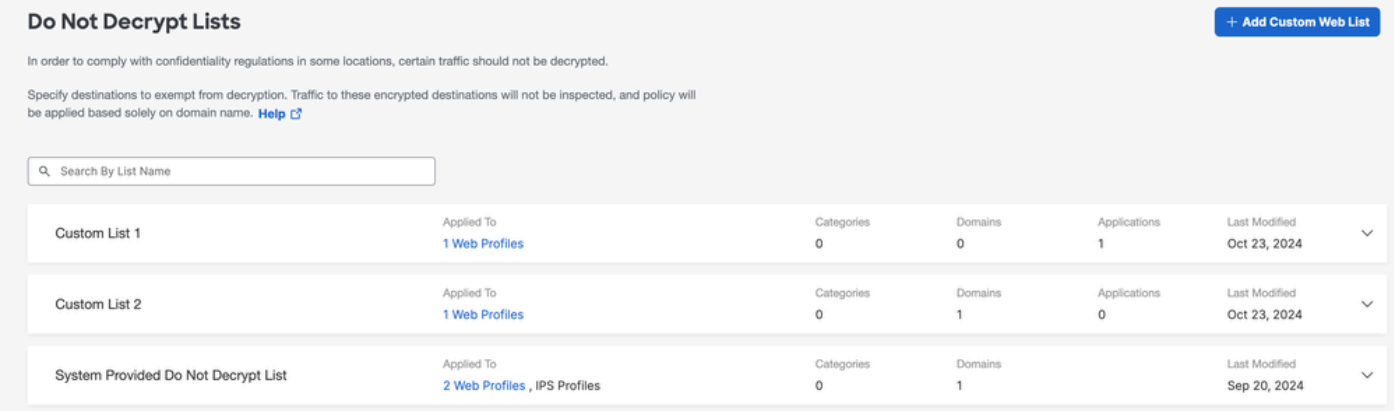
Não descriptografar listas

Conjunto de listas de destino que podem ser vinculadas ao perfil de segurança para ignorar domínios ou endereços IP de serem descriptografados.

Propriedades:

- Permitir que domínios personalizados sejam ignorados Descriptografia da Web
- Esta lista afeta somente a Descriptografia da Web, não o IPS, com exceção da Lista Não Descriptografar Fornecida pelo Sistema
- Contém uma (lista Não descriptografar fornecida pelo sistema) que ignora a descriptografia de IPS e da Web
- Esta opção precisa ser combinada com os perfis de segurança a serem anexados à política
- Esta lista só pode ser usada se Descriptografia estiver habilitada no Perfil de Segurança

Configuração: Painel -> Seguro -> Não descriptografar listas



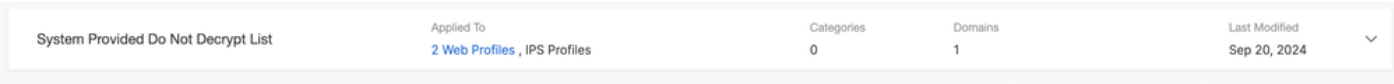
Lista Não Descriptografar Fornecida Pelo Sistema

Parte das listas Não descriptografar, com recurso adicional de aplicação em Descriptografia e IPS no acesso seguro.

Propriedades:

- Esta é a única lista Não descriptografar personalizada que afeta o IPS e a descriptografia da Web
- Não há opção de personalizar essa lista por política.

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



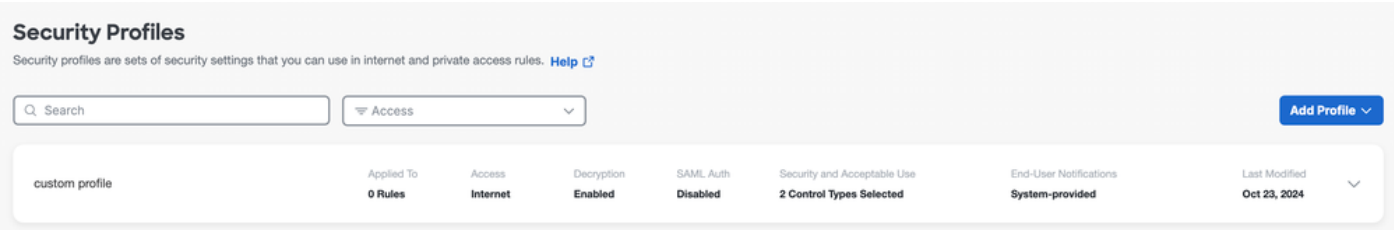
Configurações do perfil de segurança

Nas configurações do perfil de segurança, você pode selecionar Ativando ou Desativando a descriptografia da Web, que pode ser posteriormente associada a uma diretiva da Internet. Se a opção Descriptografia estiver habilitada, você terá a opção de selecionar uma das listas Não descriptografar configuradas.

Propriedades:

- Controla vários recursos de segurança, incluindo Web Decryption e Do Not Decrypt Lists
- A anexação da lista Não descriptografar fornecida pelo sistema ao perfil de segurança afeta a descriptografia da Web e a descriptografia de IPS

Configuração: Painel de controle -> Seguro -> Perfis de segurança



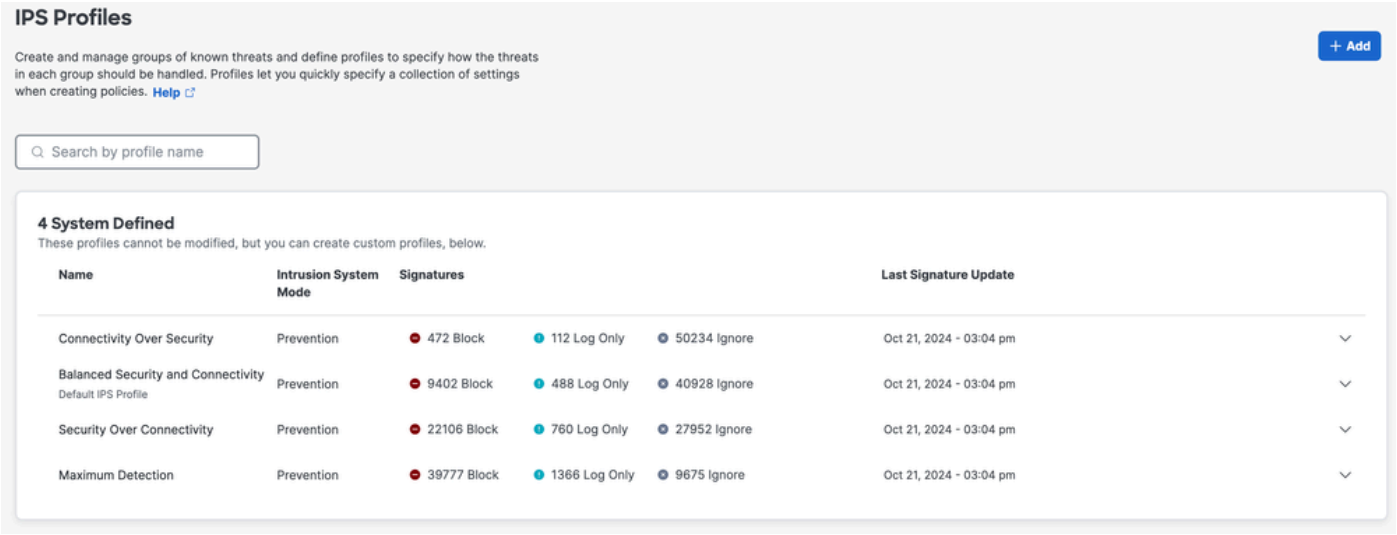
Perfis IPS

As configurações de perfis IPS incluem quatro configurações de segurança principais predefinidas para o perfil IPS. Que pode ser selecionado de acordo com as configurações de política. Você tem a opção de criar seu próprio perfil de IPS personalizado para configurações mais rígidas ou flexíveis.

Propriedades:

- Contém quatro perfis de níveis de segurança predefinidos para IPS
- O perfil IPS personalizado pode ser criado

Configuração: Painel de controle -> Seguro -> Perfis IPS

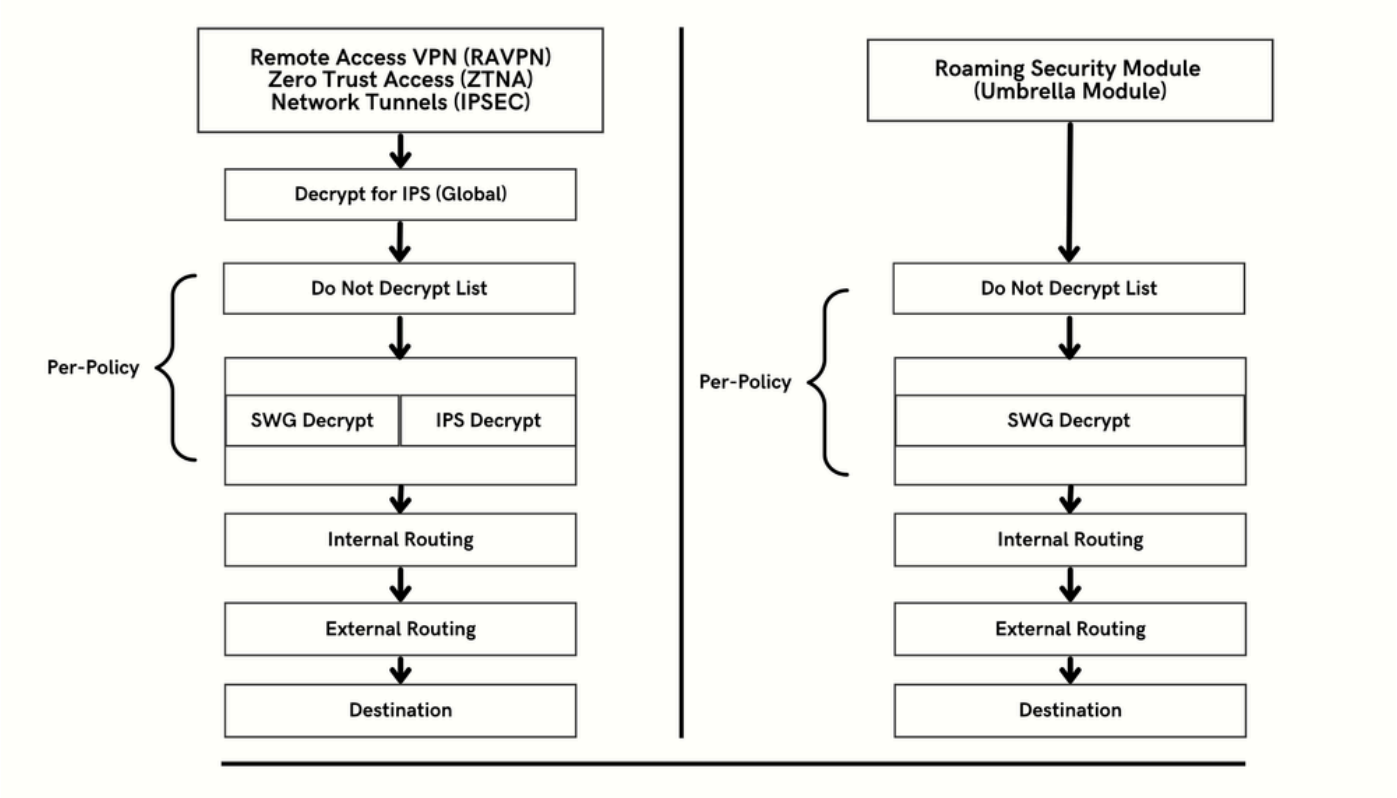


Fluxo de tráfego HTTPS em acesso seguro

O acesso seguro tem diferentes caminhos de tráfego com base no método de conexão.

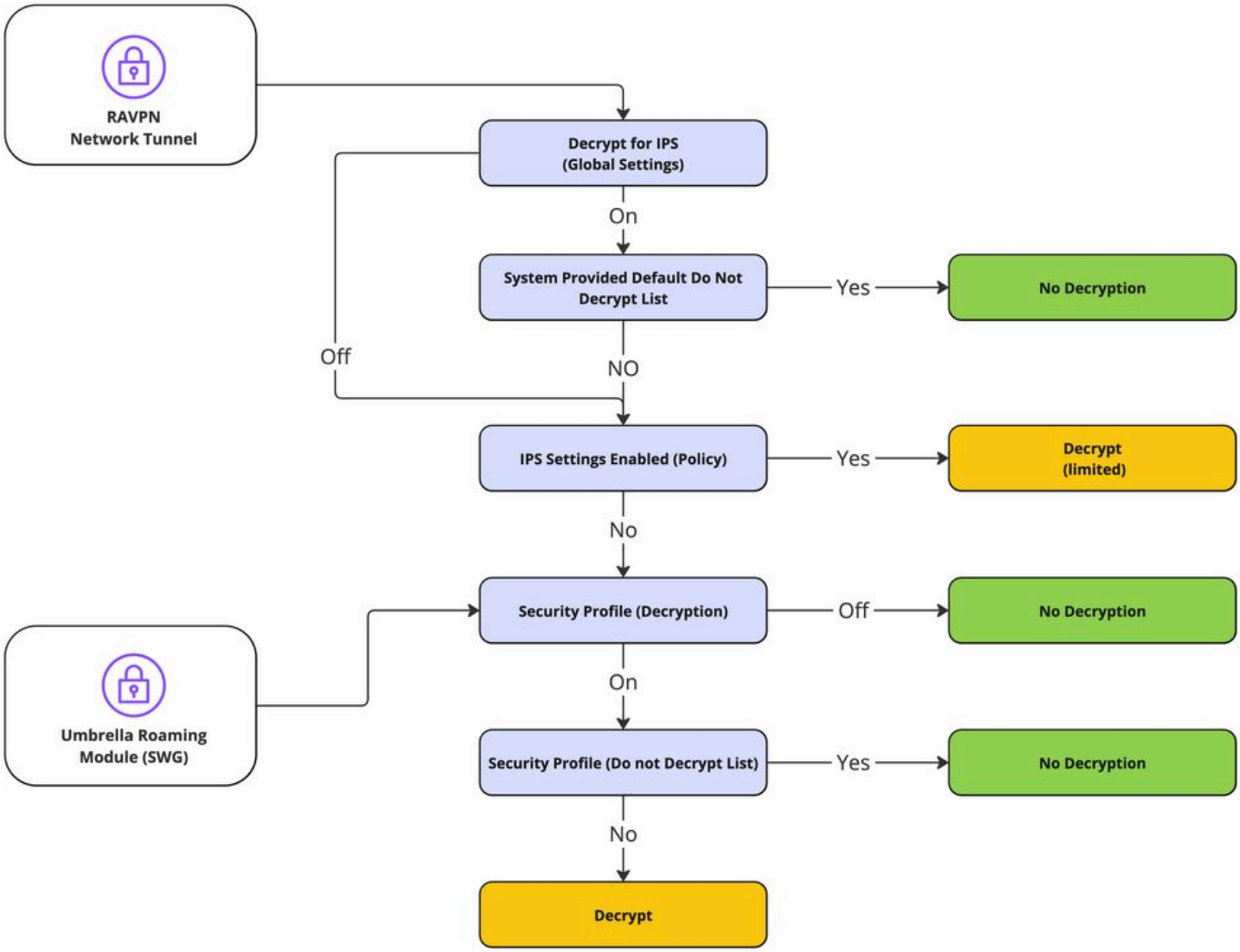
A VPN de acesso remoto (RAVPN) e o acesso zero confiável (ZTNA) compartilham os mesmos componentes.

O módulo de segurança de roaming (módulo Umbrella) tem um caminho de tráfego diferente.



Quando esperar que o tráfego seja descriptografado

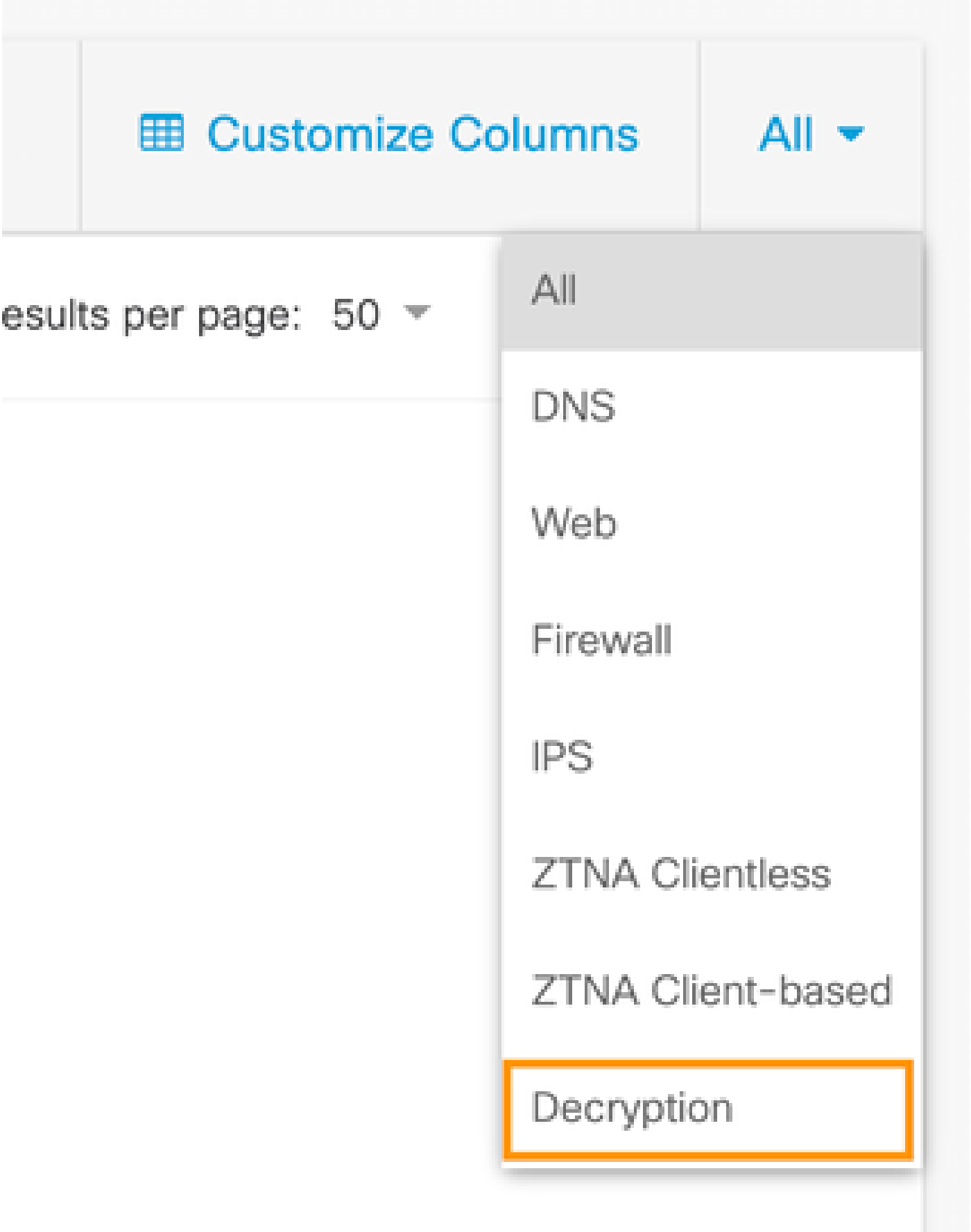
Esta seção explica em detalhes a cadeia de ações e seus principais resultados de descriptografia ou nenhuma descriptografia.

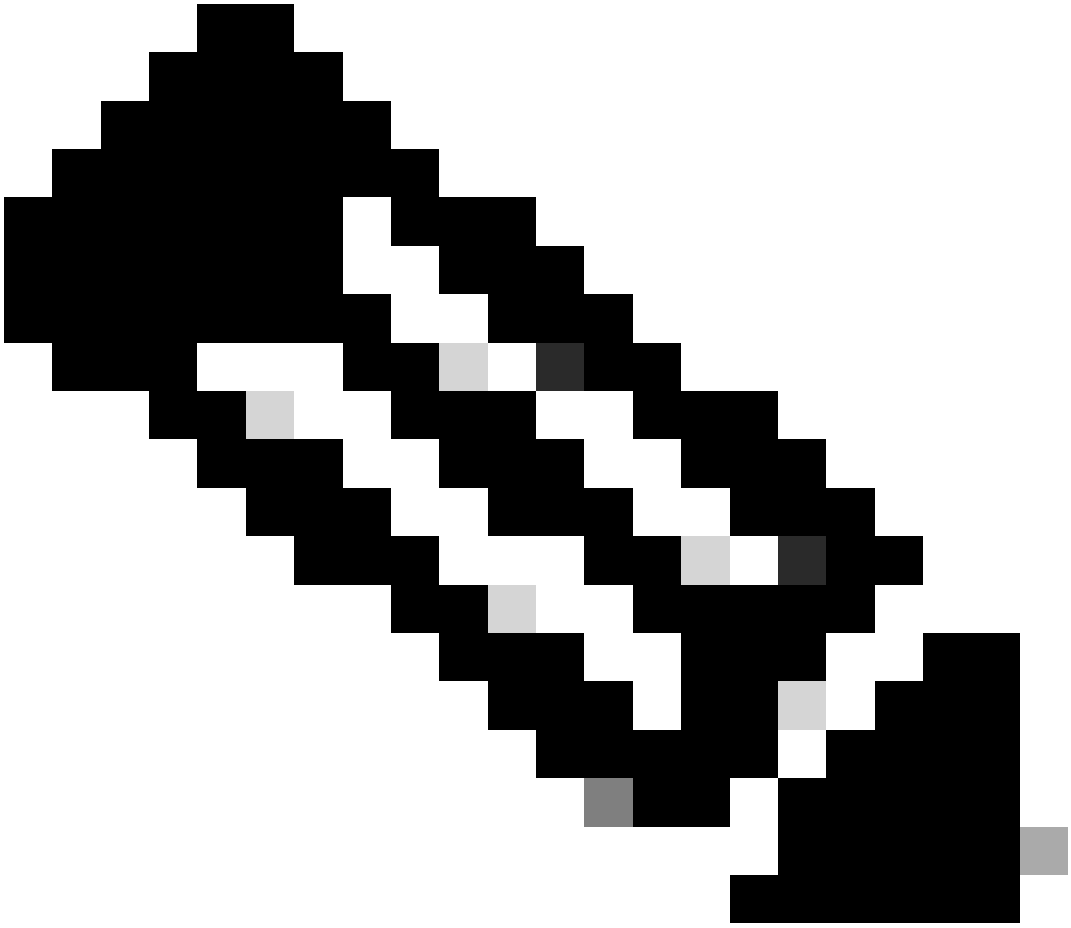


Fluxo de descriptografia

Registro e relatório relacionados a decodificação e IPS

O acesso seguro inclui uma nova seção de relatórios (Descriptografia) que pode ser acessada por meio de Painel -> Monitor -> Pesquisa de atividade -> Alternar para descriptografia.

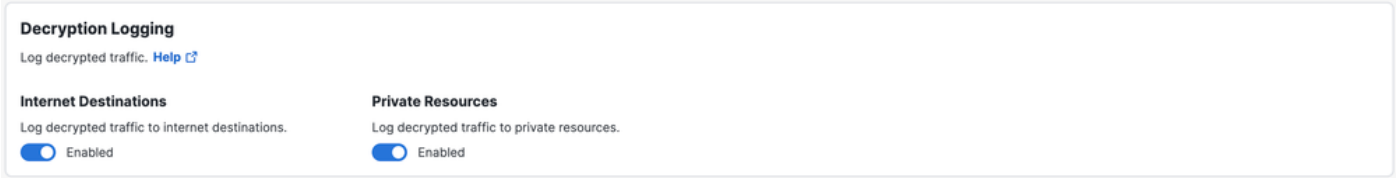

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



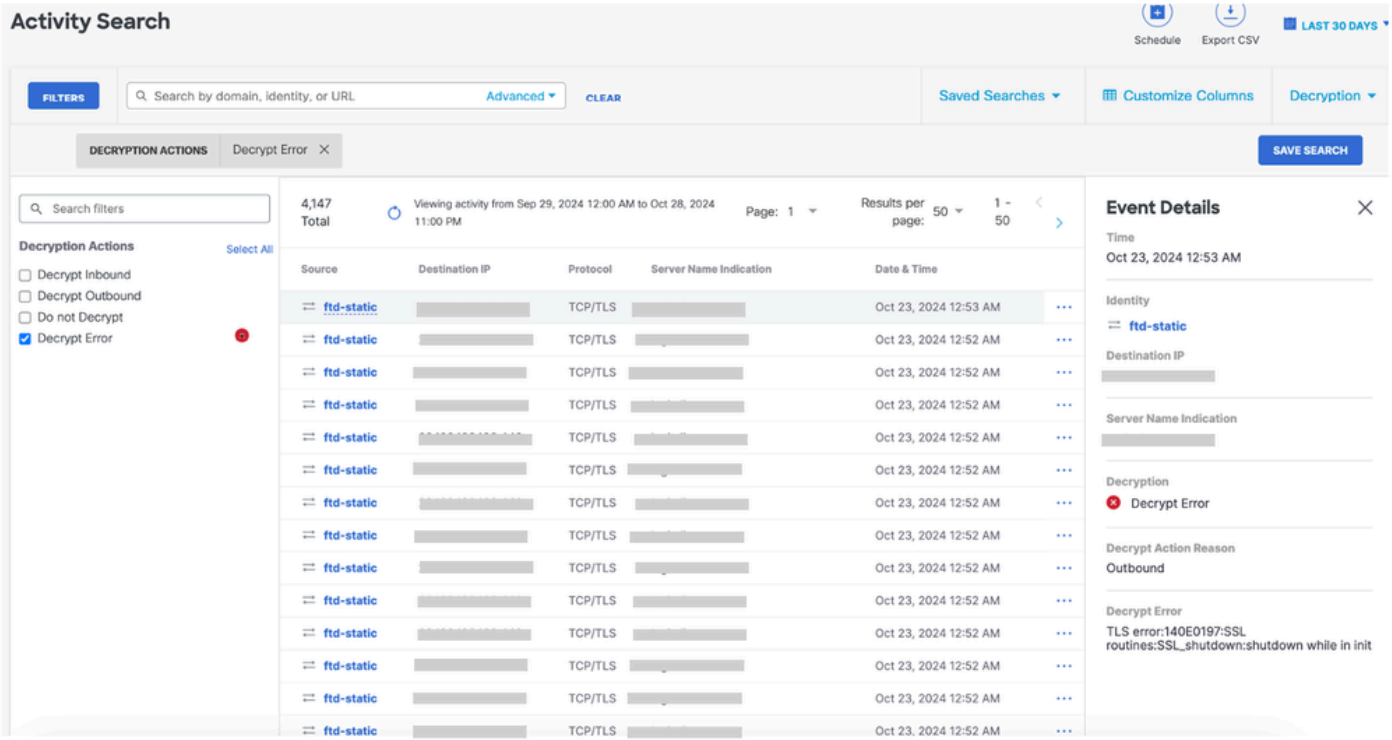
Observação: para habilitar logs de descriptografia, esta configuração pode ser habilitada nas configurações globais:

Painel de Controle -> Seguro -> Política de Acesso -> Padrões de Regra e Configurações Globais -> Configurações Globais -> Log de Descriptografia.

Configurações de log de descriptografia:



Exemplo de erro de descriptografia:



Informações Relacionadas

- Guia do usuário do Secure Access
- Suporte técnico e downloads – Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.