Risoluzione dei problemi relativi al flusso di lavoro IPS (Secure Access Decryption and Intrusion Prevention System)

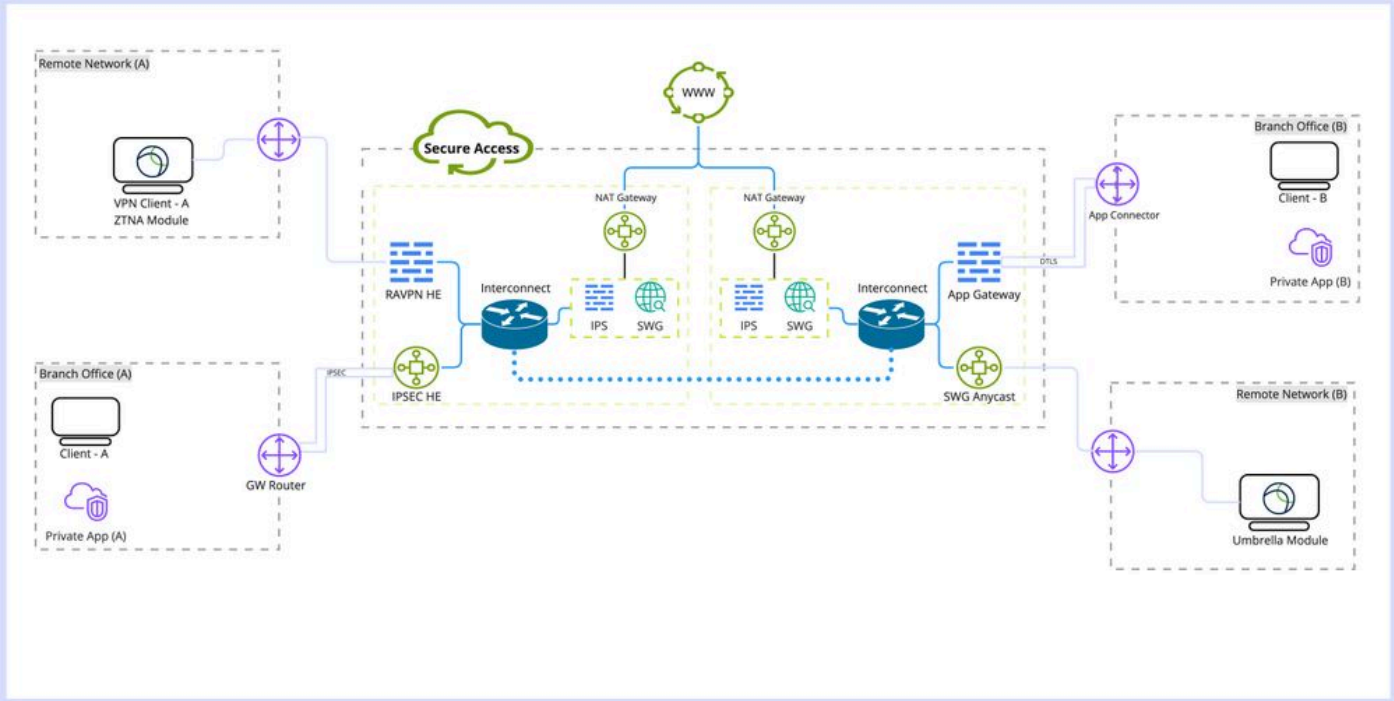
Sommario

Introduzione

In questo documento viene descritto il flusso di lavoro Decrittografia accesso sicuro e IPS e vengono evidenziate le proprietà delle impostazioni importanti.

Architettura di accesso sicuro

Questa architettura di accesso sicuro evidenzia i diversi servizi forniti da Accesso sicuro e i diversi metodi di connessione che è possibile stabilire per proteggere la rete.



Architettura di accesso sicuro

Dettagli architettura:

Termini per acquisire familiarità con:

RAVPN HE: headend di rete privata virtuale ad accesso remoto

IPSEC HE: headend IPSEC (Remote Tunnel Internet Protocol Security)

Modulo ZTNA: Zero Trust Network Access Module

SWG: Secure Web Gateway

IPS: sistema di prevenzione delle intrusioni

Gateway NAT: gateway Network Address Translation

SWG AnyCast: punto di ingresso sicuro per Anycast Gateway Web

Tipi di distribuzione:

1. VPN ad accesso remoto

2. Tunnel di accesso remoto

3. Modulo di roaming Umbrella

4. Application Connector/Application Gateway

5. Modulo Zero Trust (ZTNA)

Panoramica delle funzionalità

Secure Access consente di eseguire sia il sistema di decrittografia Web che il sistema di prevenzione delle intrusioni (IPS, Intrusion Prevention System) per migliorare il rilevamento e la categorizzazione delle applicazioni e fornire ulteriori dettagli sul traffico, inclusi percorsi URL, nomi di file e relativa categoria di applicazioni, nonché per prevenire attacchi e malware che durino zero giorni.

Decrittografia: in questo articolo il termine decrittografia si riferisce al traffico HTTPS (Decrypting Hyper Text Transfer Protocol) attraverso il modulo SWG (Secure Web Gateway). e anche alla decrittografia del traffico per l'ispezione IPS.

IPS: sistema di rilevamento e prevenzione delle intrusioni a livello di firewall che richiede la decrittografia del traffico per poter eseguire tutte le funzionalità.

La decrittografia è necessaria per più funzionalità di accesso sicuro, ad esempio DLP (Data Loss Prevention) e RBI (Remote Browser Isolation), ispezione dei file, analisi dei file e blocco dei tipi di file.

Impostazioni relative a decrittografia e IPS in Accesso sicuro

Di seguito viene fornita una rapida panoramica delle impostazioni relative a Decrittografia e IPS disponibili in Accesso sicuro.

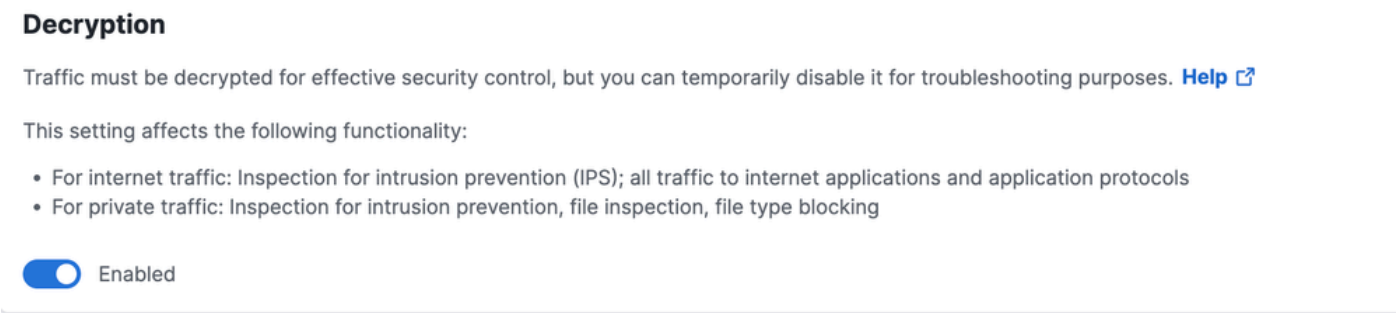
Decrittografia per IPS

Si tratta di un'impostazione globale per IPS utilizzata per disabilitare o abilitare il motore IPS per tutti i criteri.

Proprietà:

- Questa opzione non influisce sulla decrittografia del gateway Web protetta (decrittografia Web)
- La disattivazione e l'attivazione di IPS per criterio è disponibile con funzionalità limitate per ispezionare solo la fase iniziale dell'handshake senza ispezionare il corpo della richiesta.

Configurazione: Dashboard -> Protetto -> Criteri di accesso -> Impostazioni globali e predefinite regole -> Impostazioni globali -> Decrittografia per IPS



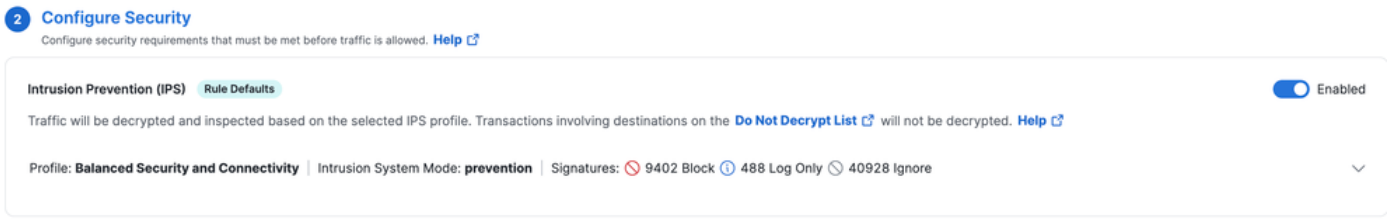
Impostazioni IPS per criterio

Questa opzione consente di disabilitare e abilitare IPS per base di criteri.

Proprietà:

- Questa opzione controlla se IPS è abilitato o disabilitato per criterio.
- Questa opzione dipende dalle impostazioni di Decrittografia per IPS. Se l'opzione Decrittografia globale per IPS è disabilitata, il comportamento ispeziona solo la fase iniziale dell'handshake senza esaminare il corpo della richiesta.
- Questa opzione non influisce su SWG (Web Decryption)

Configurazione: Dashboard -> Protezione -> Criteri di accesso ->Modifica criterio -> Configura protezione -> Prevenzione intrusioni (IPS)



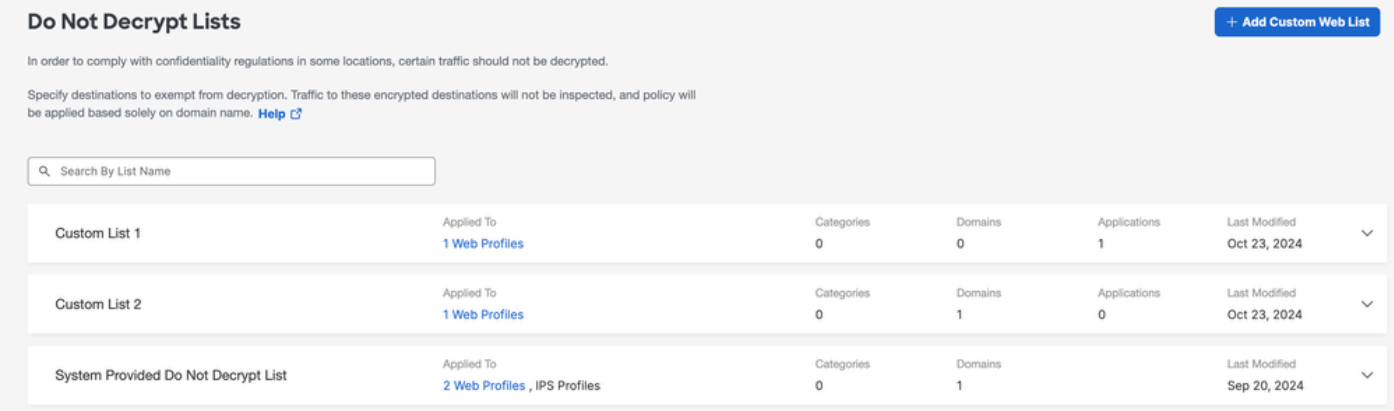
Non decrittografare elenchi

Gruppo di elenchi di destinazione che è possibile collegare al profilo di sicurezza per evitare la decrittografia di domini o indirizzi IP.

Proprietà:

- Consenti di ignorare la decrittografia Web per i domini personalizzati
- Questo elenco ha effetto solo sulla decrittografia Web e non su IPS, ad eccezione dell'elenco Do Not Decrypt fornito dal sistema
- Contiene un (elenco Do Not Decrypt fornito dal sistema) che ignora sia IPS che la decrittografia Web
- Questa opzione deve essere combinata con i profili di sicurezza da allegare al criterio
- È possibile utilizzare questo elenco solo se nel profilo di sicurezza è abilitata la decrittografia

Configurazione: Dashboard -> Protetto -> Non decrittografare elenchi



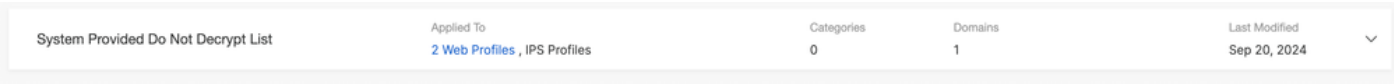
Elenco non decrittografati fornito dal sistema

Fa parte degli elenchi Non decrittografare, con la funzione aggiuntiva di applicazione sia su Decrittografia che su IPS in Accesso sicuro.

Proprietà:

- Questo è l'unico elenco personalizzato Non decrittografare che ha effetto sia su IPS che sulla decrittografia Web
- Non è possibile personalizzare l'elenco in base ai criteri.

Configurazione: Dashboard -> Protetto -> Non decrittografare elenchi -> Elenco non decrittografare fornito dal sistema



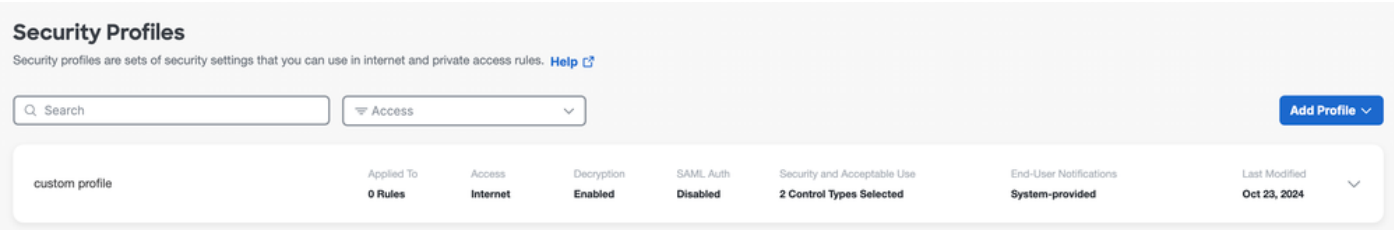
Impostazioni del profilo di sicurezza

Nelle impostazioni del profilo di sicurezza è possibile selezionare Attivazione o disattivazione della decrittografia Web che può essere successivamente associata a un criterio Internet. Se Decrittografia è abilitato, è possibile selezionare uno degli elenchi Non decrittografare configurati.

Proprietà:

- Controlla diverse funzionalità di protezione, tra cui gli elenchi Decrittografia Web e Non decrittografare
- L'associazione dell'elenco Non decrittografare fornito dal sistema al profilo di sicurezza influisce sia sulla decrittografia Web che sulla decrittografia IPS

Configurazione: Dashboard -> Protezione -> Profili di protezione



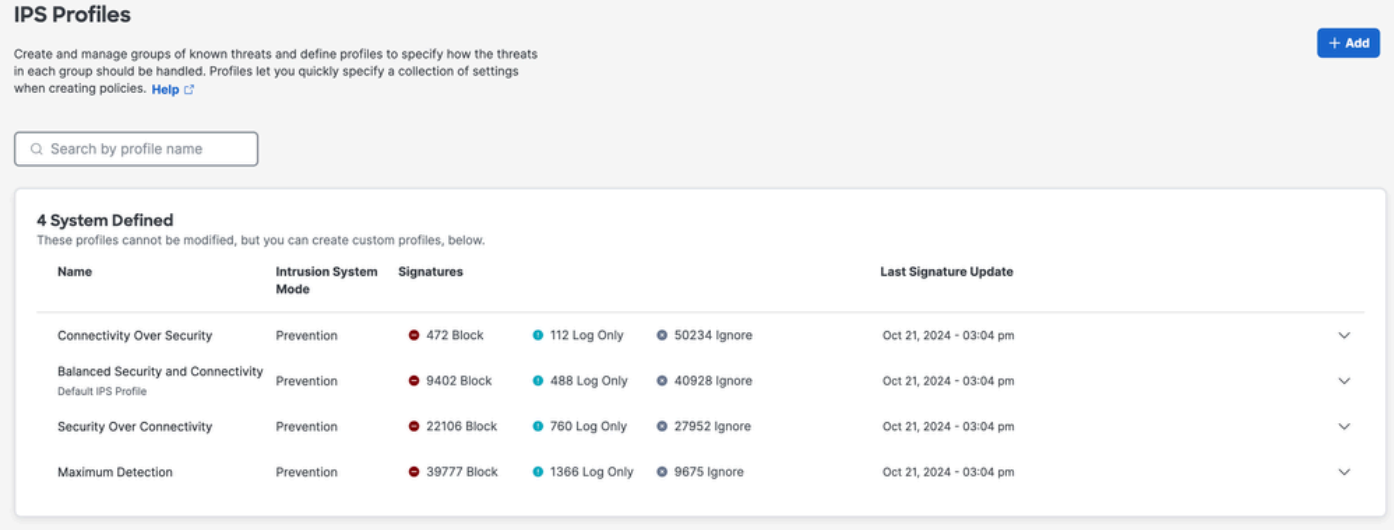
Profili IPS

Le impostazioni dei profili IPS includono quattro impostazioni di protezione predefinite principali per il profilo IPS. Selezionabile in base alle impostazioni dei criteri. È possibile creare un profilo IPS personalizzato per impostazioni più rigide o flessibili.

Proprietà:

- Contiene quattro profili dei livelli di sicurezza predefiniti per IPS
- È possibile creare un profilo IPS personalizzato

Configurazione: Dashboard -> Protetto -> Profili IPS

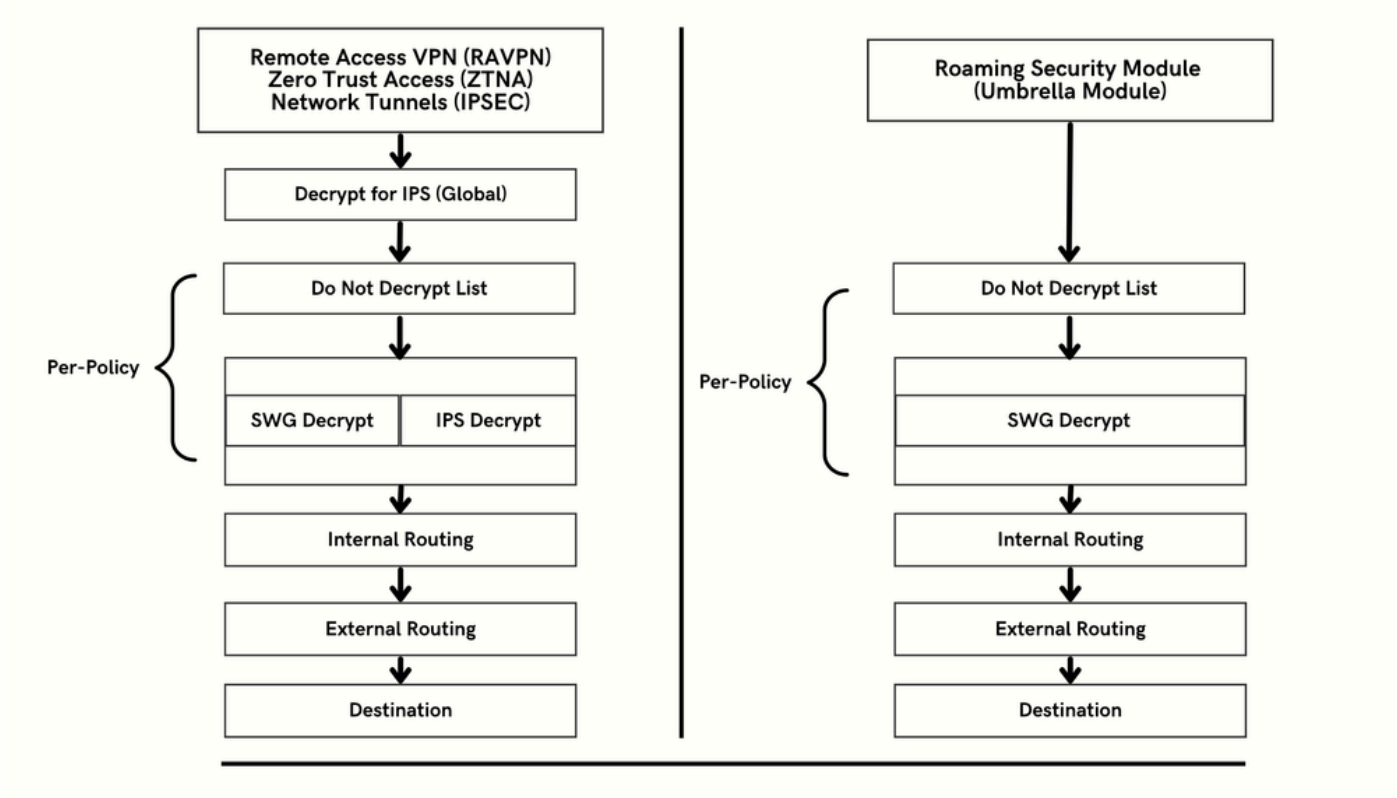


Flusso del traffico HTTPS in accesso sicuro

Accesso protetto dispone di percorsi di traffico diversi in base al metodo di connessione.

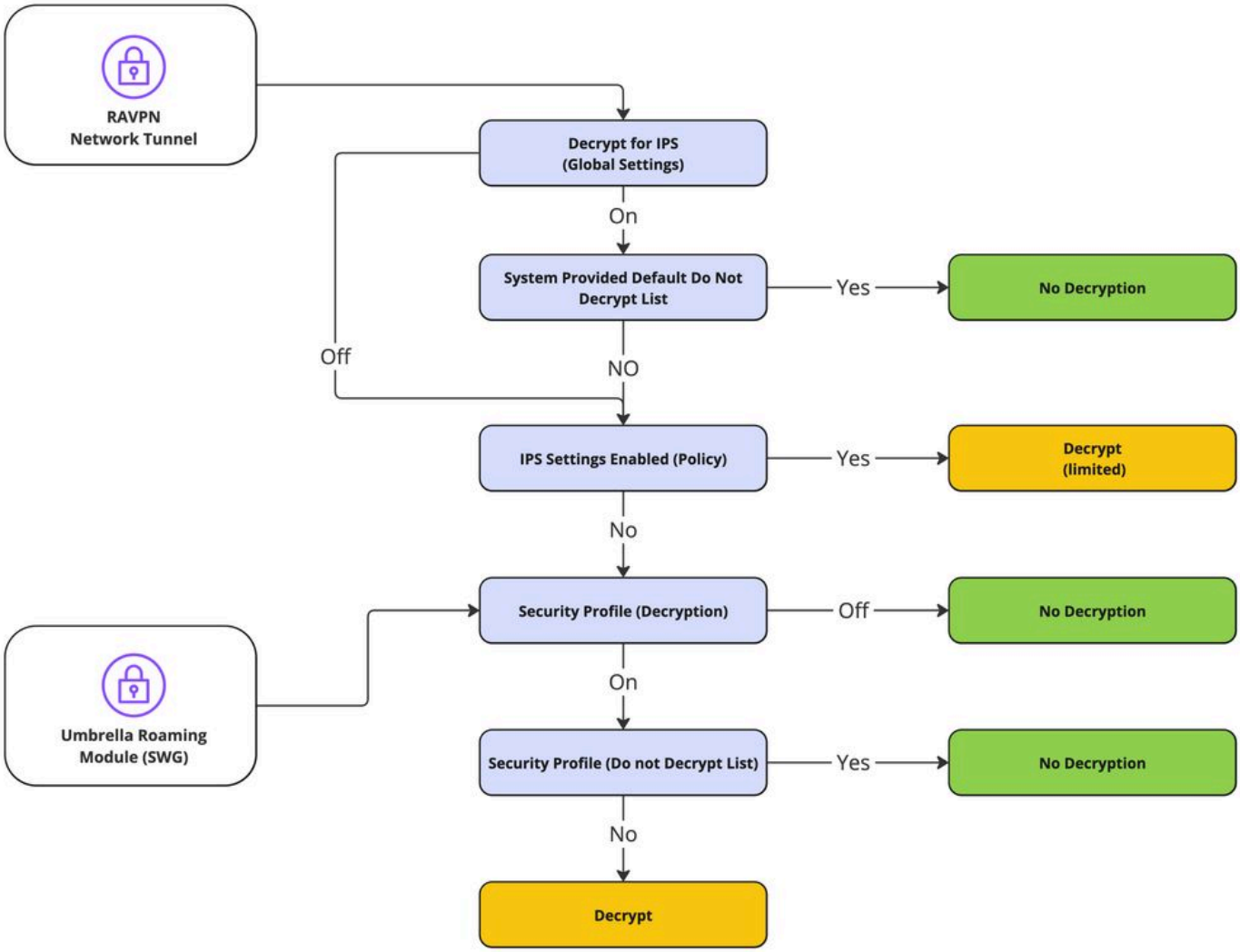
La VPN ad accesso remoto (RAVPN) e la ZTNA (Zero Trust Access) condividono gli stessi componenti.

Il modulo di sicurezza per il roaming (modulo Umbrella) ha un percorso del traffico diverso.



Quando è prevista la decrittografia del traffico

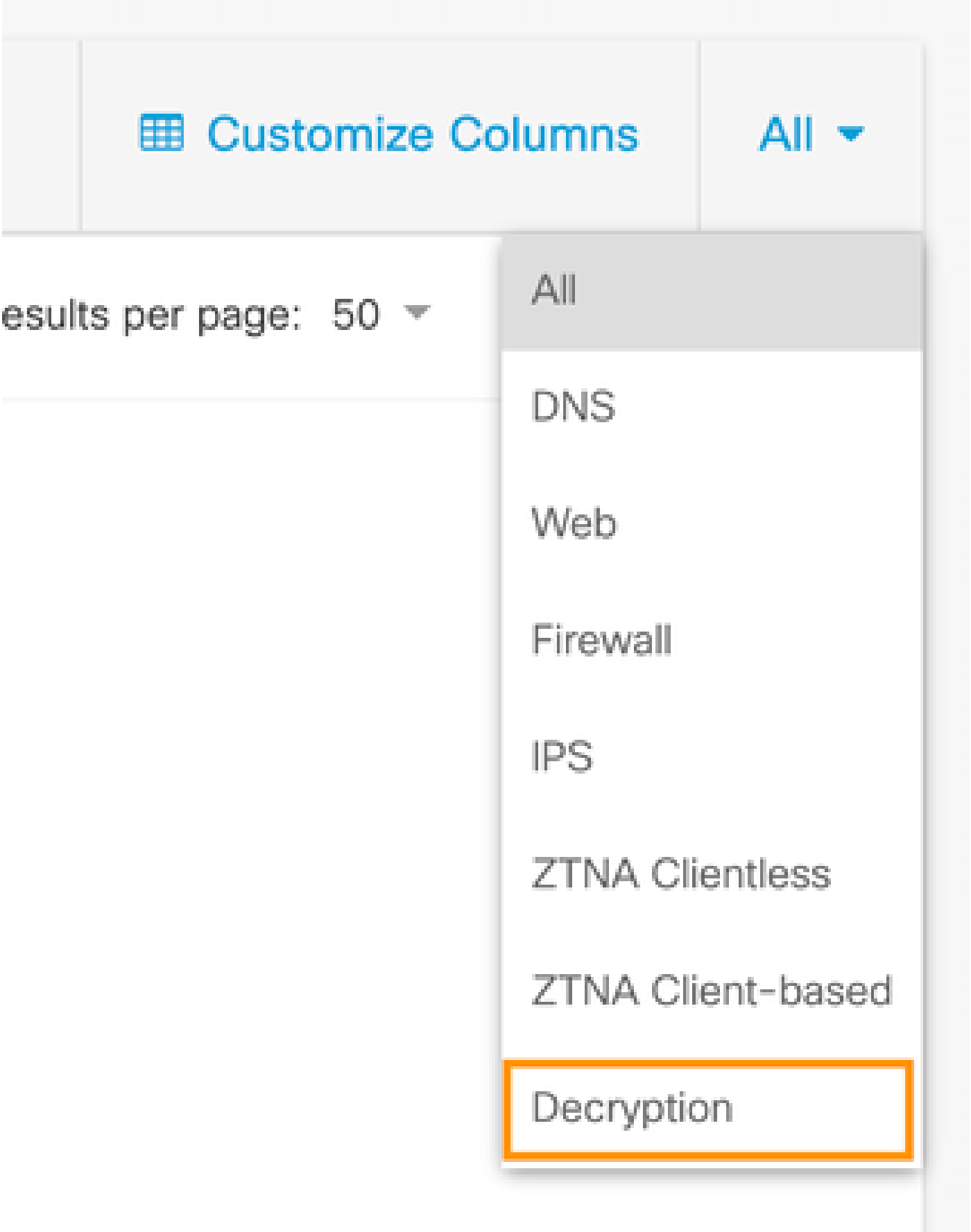
In questa sezione viene illustrata in dettaglio la catena di azioni e i risultati principali della decrittografia o della mancata decrittografia.

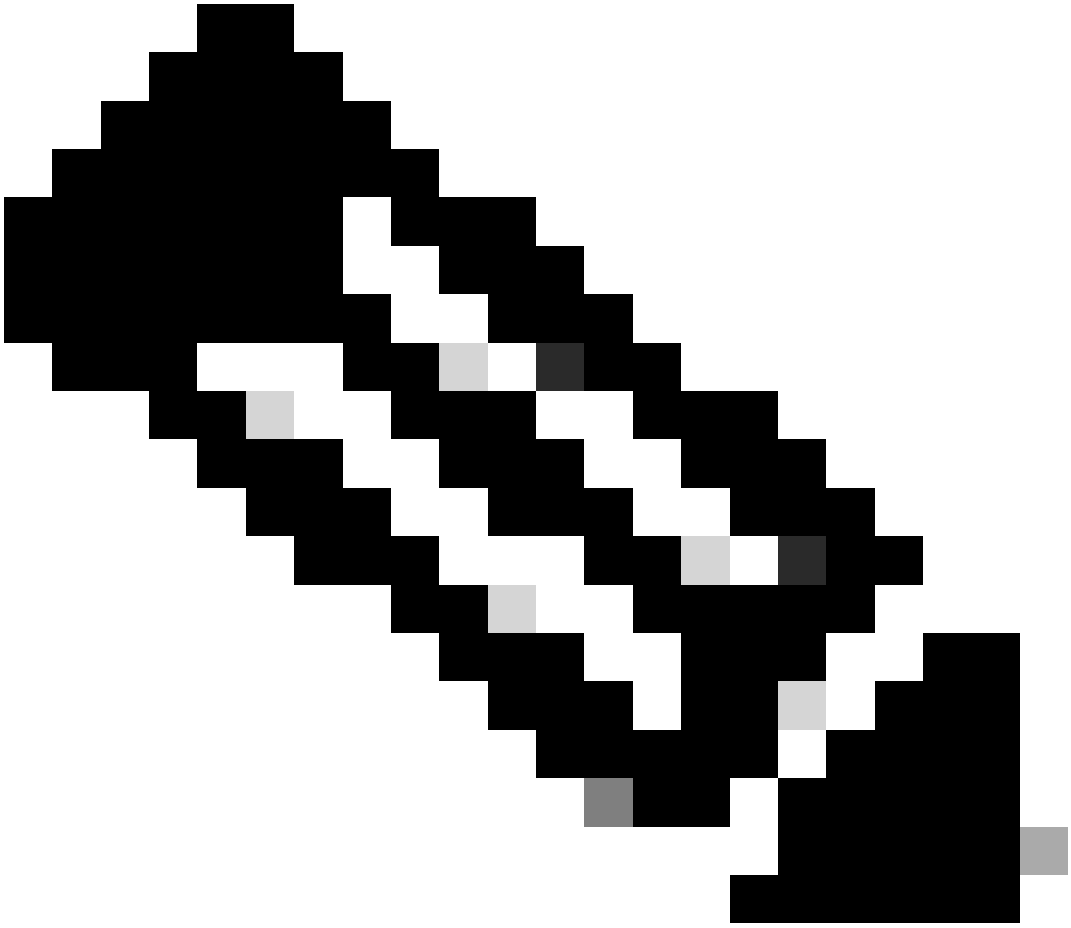


Flusso di decrittografia

Registrazione e report relativi a decrittografia e IPS

Secure Access include una nuova sezione di report (Decrittografia) a cui è possibile accedere tramite Dashboard -> Monitor -> Ricerca attività -> Switch to Decryption.

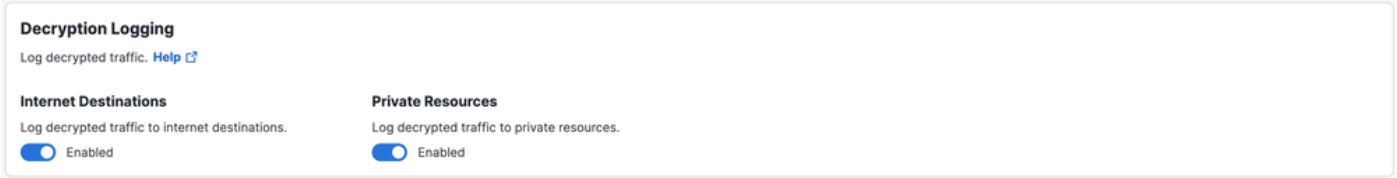

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



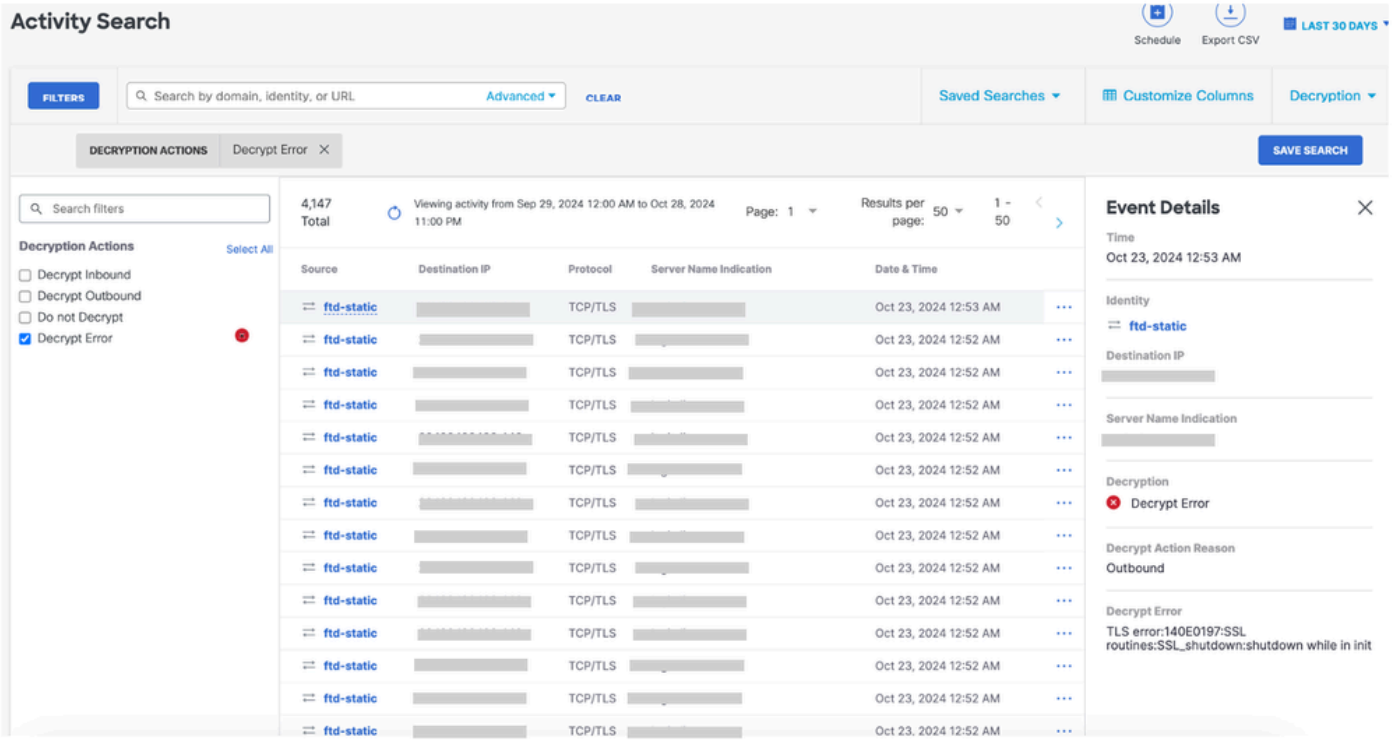
Nota: per abilitare i log di decrittografia, è possibile abilitare questa impostazione nelle impostazioni globali:

Dashboard -> Protetto -> Criteri di accesso -> Impostazioni predefinite regole e impostazioni globali -> Impostazioni globali -> Registrazione decrittografia.

Impostazioni registrazione decrittografia:



Esempio di errore di decrittografia:



Informazioni correlate

- Guida per l'utente di Secure Access
- Supporto tecnico e download - Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).