

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

Contents

[Introdução](#)

[Arquitetura de acesso seguro](#)

[Visão geral do recurso](#)

[Configurações relacionadas a decodificação e IPS no Secure Access](#)

[\[Descriptografia para IPS\]\(#\)](#)

[\[Configurações de IPS por política\]\(#\)](#)

[\[Não descriptografar listas\]\(#\)](#)

[\[Lista Não Descriptografar Fornecida Pelo Sistema\]\(#\)](#)

[\[Configurações do perfil de segurança\]\(#\)](#)

[\[Perfis IPS\]\(#\)](#)

[Fluxo de tráfego HTTPS em acesso seguro](#)

[Quando esperar que o tráfego seja descriptografado](#)

[Registro e relatório relacionados a decodificação e IPS](#)

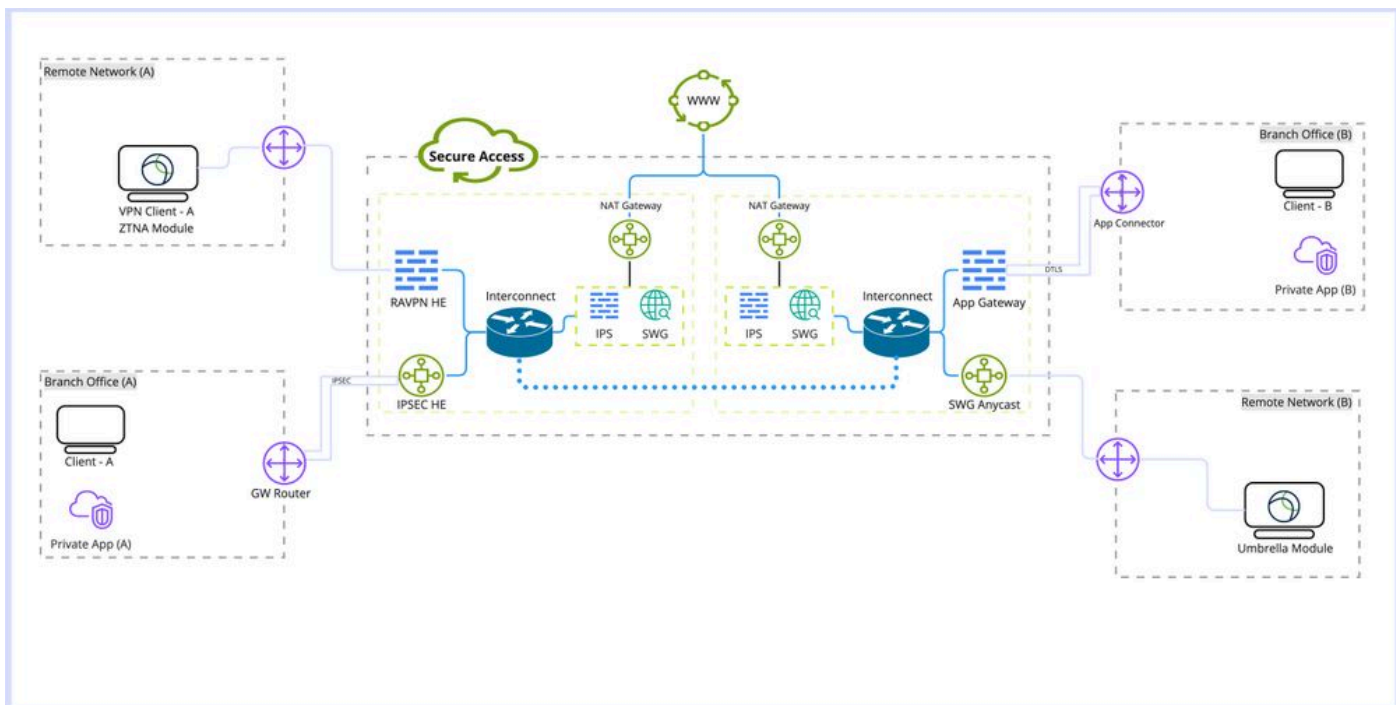
[Informações Relacionadas](#)

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

Decryption

Traffic must be decrypted for effective security control, but you can temporarily disable it for troubleshooting purposes. [Help](#) 

This setting affects the following functionality:

- For internet traffic: Inspection for intrusion prevention (IPS); all traffic to internet applications and application protocols
- For private traffic: Inspection for intrusion prevention, file inspection, file type blocking

Enabled

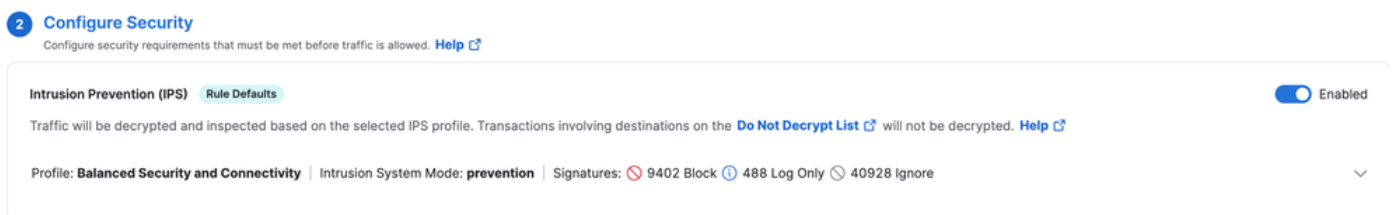
Configurações de IPS por política

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

Do Not Decrypt Lists						+ Add Custom Web List
<p>In order to comply with confidentiality regulations in some locations, certain traffic should not be decrypted.</p> <p>Specify destinations to exempt from decryption. Traffic to these encrypted destinations will not be inspected, and policy will be applied based solely on domain name. Help</p>						
<input type="text" value="Search By List Name"/>						
Custom List 1	Applied To 1 Web Profiles	Categories 0	Domains 0	Applications 1	Last Modified Oct 23, 2024	▼
Custom List 2	Applied To 1 Web Profiles	Categories 0	Domains 1	Applications 0	Last Modified Oct 23, 2024	▼
System Provided Do Not Decrypt List	Applied To 2 Web Profiles , IPS Profiles	Categories 0	Domains 1		Last Modified Sep 20, 2024	▼

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

System Provided Do Not Decrypt List	Applied To 2 Web Profiles , IPS Profiles	Categories 0	Domains 1	Last Modified Sep 20, 2024	▼
-------------------------------------	---	-----------------	--------------	-------------------------------	---

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

Security Profiles								
<p>Security profiles are sets of security settings that you can use in internet and private access rules. Help</p>								
<input type="text" value="Search"/>		<input type="text" value="Access"/>		+ Add Profile				
custom profile	Applied To 0 Rules	Access Internet	Decryption Enabled	SAML Auth Disabled	Security and Acceptable Use 2 Control Types Selected	End-User Notifications System-provided	Last Modified Oct 23, 2024	▼

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

The screenshot shows the 'IPS Profiles' management page. At the top, there is a title 'IPS Profiles' and a '+ Add' button. Below the title, there is a brief description: 'Create and manage groups of known threats and define profiles to specify how the threats in each group should be handled. Profiles let you quickly specify a collection of settings when creating policies. [Help](#)'. A search bar labeled 'Search by profile name' is located below the description. The main content area is titled '4 System Defined' and includes a note: 'These profiles cannot be modified, but you can create custom profiles, below.' Below this note is a table with the following columns: 'Name', 'Intrusion System Mode', 'Signatures', and 'Last Signature Update'. The table lists four profiles: 'Connectivity Over Security', 'Balanced Security and Connectivity (Default IPS Profile)', 'Security Over Connectivity', and 'Maximum Detection'. Each profile row shows its mode (all are 'Prevention'), a breakdown of signature counts for 'Block', 'Log Only', and 'Ignore' actions, and the last update timestamp (all are 'Oct 21, 2024 - 03:04 pm').

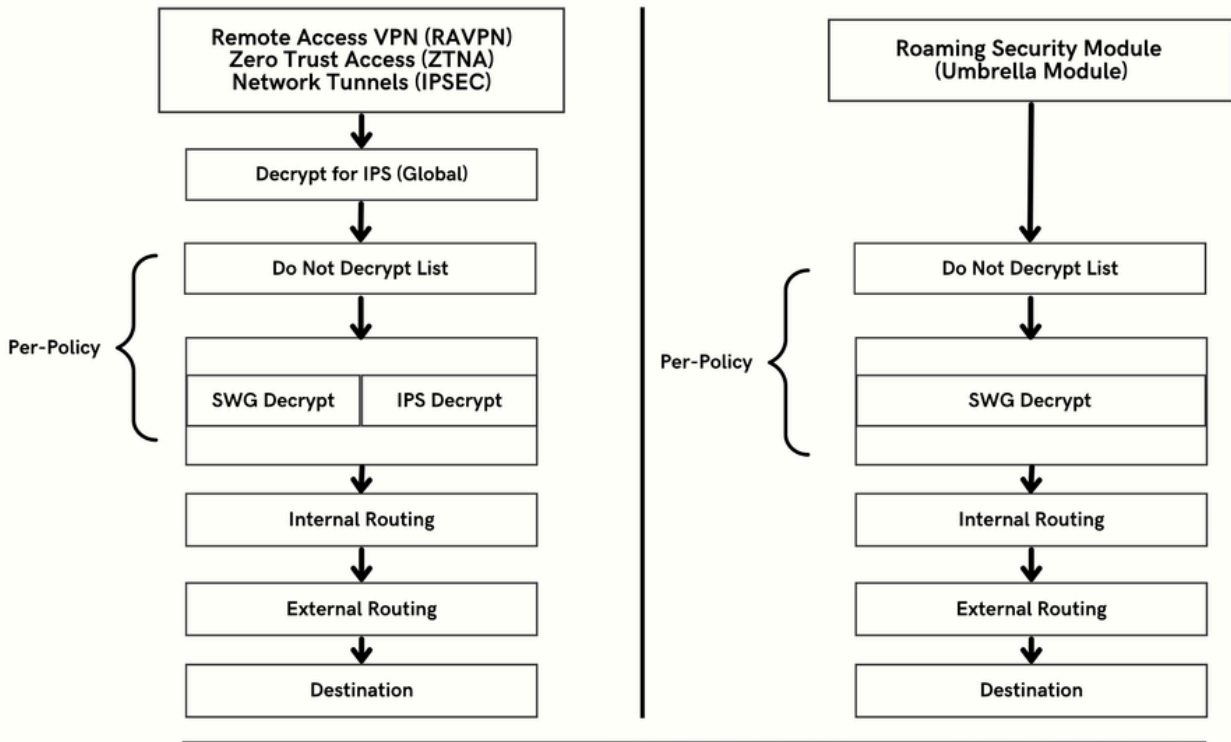
Name	Intrusion System Mode	Signatures	Last Signature Update
Connectivity Over Security	Prevention	472 Block, 112 Log Only, 50234 Ignore	Oct 21, 2024 - 03:04 pm
Balanced Security and Connectivity Default IPS Profile	Prevention	9402 Block, 488 Log Only, 40928 Ignore	Oct 21, 2024 - 03:04 pm
Security Over Connectivity	Prevention	22106 Block, 760 Log Only, 27952 Ignore	Oct 21, 2024 - 03:04 pm
Maximum Detection	Prevention	39777 Block, 1366 Log Only, 9675 Ignore	Oct 21, 2024 - 03:04 pm

Fluxo de tráfego HTTPS em acesso seguro

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

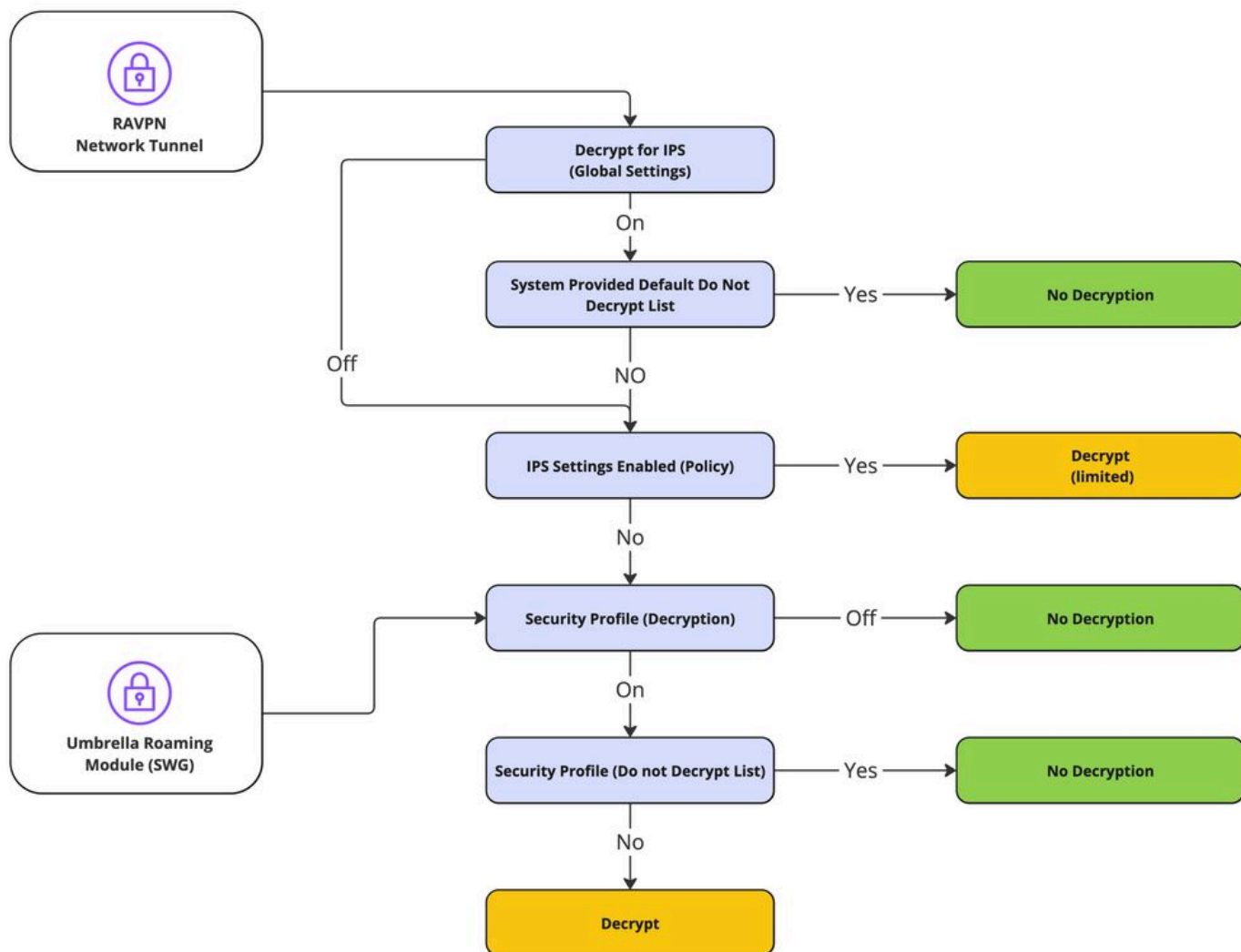
A VPN de acesso remoto (RAVPN) e o acesso zero confiável (ZTNA) compartilham os mesmos componentes.

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 decriptografia

Registro e relatório relacionados a decodificação e IPS

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

 Customize Columns

All ▼

results per page: 50 ▼

All

DNS

Web

Firewall

IPS

ZTNA Clientless

ZTNA Client-based

Decryption



Observação: para habilitar logs de decriptografia, 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 Decriptografia.

Configurações de log de decriptografia:

Decryption Logging
Log decrypted traffic. [Help](#)

Internet Destinations Log decrypted traffic to internet destinations. <input checked="" type="checkbox"/> Enabled	Private Resources Log decrypted traffic to private resources. <input checked="" type="checkbox"/> Enabled
--	--

Exemplo de erro de decriptografia:

Activity Search

Schedule Export CSV LAST 30 DAYS

Search by domain, identity, or URL Advanced CLEAR Saved Searches Customize Columns Decryption

DECRYPTION ACTIONS Decrypt Error X SAVE SEARCH

4,147 Total Viewing activity from Sep 29, 2024 12:00 AM to Oct 28, 2024 11:00 PM Page: 1 Results per page: 50 1 - 50

Search filters

Decryption Actions Select All

- Decrypt Inbound
- Decrypt Outbound
- Do not Decrypt
- Decrypt Error

Source	Destination IP	Protocol	Server Name Indication	Date & Time
ftd-static		TCP/TLS		Oct 23, 2024 12:53 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM
ftd-static		TCP/TLS		Oct 23, 2024 12:52 AM

Event Details

Time
Oct 23, 2024 12:53 AM

Identity
ftd-static

Destination IP

Server Name Indication

Decryption
Decrypt Error

Decryption Action Reason
Outbound

Decryption Error
TLS error:140E0197:SSL routines:SSL_shutdown:shutdown while in init

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.