

# عنم ماظن لمع ريس عاظخأ فاشكتسأ نمآلا لوصولا ريفشت كفو (IPS) لستلا اهحالصإو

## تايوت حمللا

[عمدقملا](#)

[نمآلا لوصولا ةينب](#)

[ةنيملا ىلع ةماع ةرظن](#)

[نمآلا لوصولا يف IPS وريفشتلا كفو ةلصللا تاذ تاداعلا](#)

[IPS ريفشت كفو](#)

[جهن لكلا IPS تاداعلا](#)

[مئاوقلا ريفشت كفو مدع](#)

[عمئاوقلا ريفشت كفو متي ال ريفوتملا ماظنلا](#)

[نيمأتلا في صوت تاداعلا](#)

[IPS تافيصوت](#)

[نمآلا لوصولا يف HTTPS تانايب رورم ةكرح قفدت](#)

[رورملا ةكرح ريفشت كفو نكمي ىتم](#)

[IPS ب ةلصللا تاذ ريراققتلا دادعإو ليحستلا او ريفشتلا اعغلا](#)

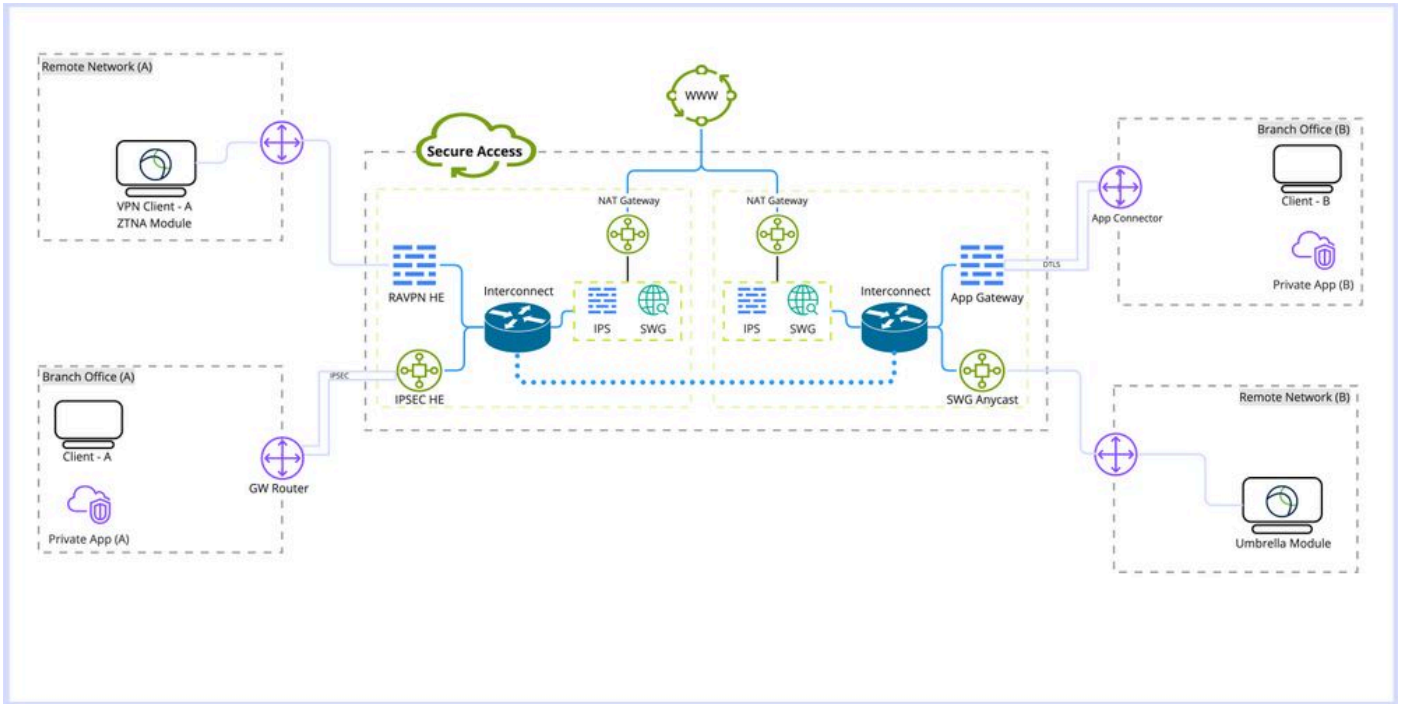
[ةلصللا تاذ تامولعم](#)

## عمدقملا

تاداعلا صئاصخ زربوي و IPS لمع ريسو نمآلا لوصولا ريفشت كفو دنتمسلا اذه فصوي  
ةمهمللا.

## نمآلا لوصولا ةينب

Secure Access اهرفوي يتلا ةفلتخملا تامدخللا ىلع عوضلا هذه Secure Access ةينب يقلت  
ةكبشلا نيمأتلا اهؤاشن نكمي يتلا ةفلتخملا لاصلتالا بيللاس أو.



نمآل لوصول ة بن

ة بن ل ل ص اف ت:

ة فول ء نو ك ت ن ء ب ح ي ي ت ل ل ا ح ل ط ص ل م ل:

ة ره ا ط ل ة ص ا خ ل ا د ع ب ن ع ل و ص و ل ا ة ك ب ش س ء ر ة ي ا ه ن : RAVPN HE

IPSec HE: (IPSec) د ي ع ب ل ل ق ف ن ل ل ت ن ر ت ن ل ل و ك و ت و ر ب ن ا م ء س ء ر ة ي ا ه ن

Zero Trust Network Access Module ة ط م ن ل ل ة د ح و ل ا : ZTNA ة ط م ن ل ل ة د ح و ل ا

ة نمآل ب ي و ل ا ة ب ا و ب : SWG

س د ح ل ا ع ن م م ا ط ن : IPS

ة ك ب ش ل ل ن ا و ن ع ة م ح ر ت ة ر ا ب ع : NAT ة ر ا ب ع

ة نمآل ب ي و ل ا ة ب ا و ب ل AnyCast ل خ د م ة ط ق ن : SWG AnyCast

ر ش ن ل ل ا ع ا و ن ء:

1. د ع ب ن ع ل و ص و ل ل VPN ة ك ب ش
2. د ع ب ن ع ل و ص و ل ا ق ف ن
3. Umbrella ل ا و ج ت ل ل ة د ح و
4. ق ي ب ط ت ل ل ا ة ب ا و ب / ق ي ب ط ت ل ل ل ص و م
5. ر ف ص ة ق ث ل ل ا ح ذ و م ن (ZTNA)

# ةزيملا ىلع ةماع ةرظن

عنم ماظن"و"ببول ريفشت ك ف ماظن" نم لك ذي فنن ةينام | "نمآل لوصولا" رفوي لىصافتلا نم ديزم ريفوت واه فينصت و تاقىببطلت فاشتك نىسحتل (IPS) "للسل اها. ةصاخلا تاقىببطلت ةئفو تافلما ءامس أو URL تاراسم كلذ ي ف امب .رورملا ةكرح لوح .ةراضلا جماربلاو دحاو موي ىوس قرغتست ال يتلا تامجهلا عنم ىلع ةدعاسملاو .

لقن لوكتورب رورم ةكرح ريفشت ك ف لىل ةراشإل متي ةلاقملا هذه ي ف : ريفشتلا ك ف ةكرح ريفشت ك ف كلذكو . (SWG) ةنمآل ببول ةرابع ةدحو لالخ نم (HTTPS) ببعشتلا صنلا IPS شيتفتل تانايبلا رورم .

ةكرح ريفشت ك ف بلطتي يذلا ةيماحل رادج ىوتسم ىلع ماحتقالا عنم و فاشتك ماظن : IPS .ةلماكل فئاظولا ذي فننل رورملا .

(DLP) تانايبلا نادق ف عنم لثم ةدعتملا نمآل لوصولا تازيمل ايرورض ريفشتلا ك ف دعوي تافلما عون رطحو تافلما لىلحتو تافلما صحفو (RBI) دي ببال ضرعتسملا لزعو .

## نمآل لوصولا ي ف IPS و ريفشتلا ك فب ةلصل تاذ تاداعإل

لوصولا" ي ف IPS و ريفشتلا ك فب ةلصل تاذ ةحاتملا تاداعإل ىلع ةعيرس ةماع ةرظن هذه "نمآل" .

### IPS ريفشت ك ف

جهنلا ةفاكل هنىكمت و IPS كرحم لىطعتل هم ادختسإ متي IPS ل يمومع دادعإ اذه .

صئاصخل:

- (ببول ريفشت ك ف) ةنمآل ببول ةبواب ريفشت ك ف ىلع رايخلا اذه رثؤي ال
- نم ةلؤلألا ةلحرملا صحفل ةدوحم فئاظو عم جهن لكك هنىكمت و IPS لىطعت رفوت ي بلطلل ىساسألا صنلا صحف نود طقف ةحفاصملا .

تاداعإل (Global Settings و Rule Default -> Access Policy -> Secure -> تامولعمل ةحول : نىوكتلا ةماع) -> Decryption ل 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

### جهن لكك IPS تاداعإل

ةسايسلل دعاوق لكك هنىكمت و IPS لىطعتب رايخلا اذه حمسي .

## صئاصخالا:

- جهن لك هلل طعت وأ IPS نل كم تل ف رائل الا اذه مكل تل
- رل فشتل ك ف رائل ل طعت م تل اذل IPS تل اءاعل رل فشتل ك ف لعل رائل الا اذه م تل عل ن طقف ةللوال ةلحرمل صلفب كولسل موقل نأل ف ببسلل هلنل، IPS ل ماعل ل بل لال نل م صلف نول ةل صلف م ل
- (ببول رل فشتل ك ف) SWG لعل رائل الا اذه رلؤل ال

-> نامأل نل وكت -> ةسلال رل رل رل -> لولل ةسلال سل -> ةنمآ -> تامول عمل ةحول: نل وكتل (IPS) لل لسلل عنم

## 2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#)

### Intrusion Prevention (IPS) Rule Defaults

Enabled

Traffic will be decrypted and inspected based on the selected IPS profile. Transactions involving destinations on the [Do Not Decrypt List](#) will not be decrypted. [Help](#)

Profile: **Balanced Security and Connectivity** | Intrusion System Mode: **prevention** | Signatures: 9402 Block 488 Log Only 40928 Ignore

## مئل اول رل فشتل ك ف مءع

نل وانع وأ زوالل الالام ل نل نامأل ف رل رل فلفم ب هل طبر نكمل لئل ةل اول مئل اول نل ةل ووم جم ال رل فشتل ك ف مئل اول نل نل IP

## صئاصخالا:

- ببول رل فشتل ك ف ل ةل صلف م الالام ل زوالل ب حامسل
- مئل اول مائلل ءانللساب IPS سلل ببول رل فشتل ك ف لعل طقف ةل مئل اول ال اذه رلؤل
- ك ف و IPS نل ال ك زوالل لئل (ةرل مائل مائلل رل فشتل ك ف مءع ةل مئل اول) لعل لئل وئل ببول رل فشتل
- ةسلال سلل ب الالام ل نل مائلل الالام ل ءل ف صول عم رائل الا اذه مء بجل
- فلف صول ف رل فشتل ك ف نل كم ةل لال ف لعل طقف ةل مئل اول ال اذه مائلل نل كم نل مائلل

مئل اول رل فشتل ك ف مءع -> ةنمآ -> تامول عمل ةحول: نل وكتل

## Do Not Decrypt Lists

+ Add Custom Web List

In order to comply with confidentiality regulations in some locations, certain traffic should not be decrypted.

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](#)

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

## عملة اقل ريفشت ك ف م تي ال رفوتم ال ماظن ال

وريفشت ال ك ف نم لك ىلع قي بطت لل ة فاضا ة زيم عم ، ريفشت ال ك ف مدع مءاوق نم عذج نم ال لوصول ال في IPS.

صئاصخ ال:

- ك ف IPS نم لك ىلع رثؤت ي ت ال ة ديحول ال ة صصخ م ال " ريفشت ال ك ف مدع " عمءاوق يه هذو ب يول ريفشت
- جهن لك ل عمءاوق ال هذو صي صخ ت ل راخ دجوي ال

موقت ال رفوتم ال ماظن ال -> مءاوق ال ريفشت ك ف مدع -> ة نم آ -> تامول عمل ة حول : نيوك ت ال عمءاوق ال ريفشت ك ف ب

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

## ني مءا ت ال في صوت تاداع

يذل بيول ريفشت ك ف لي طعت و ا ني ك م ت دي دحت ك ن ك مي ني مءا ت ال في صوت تاداع ي في دي دحت ل راخ ال ك ي دل ف ، ريفشت ال ك ف ني ك م ت اذا . ت نرت ن ا ج ه ن ب د ع ب ام ي ف ه ط ب ر ن ك مي ا ه ني و ك ت م ت ي ت ال ريفشت ال ك ف مدع مءاوق ى دح ا

صئاصخ ال:

- ريفشت ك ف مدعو بيول ريفشت ك ف لك ذ ي ف ام ب نام ال ا تازيم نم دي دحل ال ي ف م ك ح ت ال مءاوق ال
- في IPS ريفشت ك ف و بيول ريفشت ك ف نم لك ىلع رفوم ال ق فرم ال ماظن ال رثؤي نام ال في رعت فلم عمءاوق

نام ال في رعت تافل م -> ة نم آ -> تامول عمل ة حول : نيوك ت ال

Security Profiles	Applied To	Access	Decryption	SAML Auth	Security and Acceptable Use	End-User Notifications	Last Modified
custom profile	0 Rules	Internet	Enabled	Disabled	2 Control Types Selected	System-provided	Oct 23, 2024

## IPS تاف صوت

IPS في صوت ل اق بسم ة فرعم ة ي اساس ا ني مءا تاداع ا ة ب ر ا IPS تاف صوت تاداع ا نم ضتت ل ج ا نم صصخ م ال IPS في رعت فلم عاش ن ال راخ ال ك ي دل . جهن ال تاداع ا لك ل ه دي دحت ن ك مي ام ة . نورم و ا ة م ا رص رث ك ا تاداع ا

صئاصخ ال:

- IPS ل اق بسم ة ددح م نام ا تايوت سمل تاف صوت ة ب ر ا ىلع يوتحي
- صصخ م ال IPS في رعت فلم عاش ن ا ن ك مي

## IPS تافيصوت -> ةنمآ -> تامولعمل ءحول :نيوكتلا

### IPS Profiles

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](#)

**4 System Defined**  
These profiles cannot be modified, but you can create custom profiles, below.

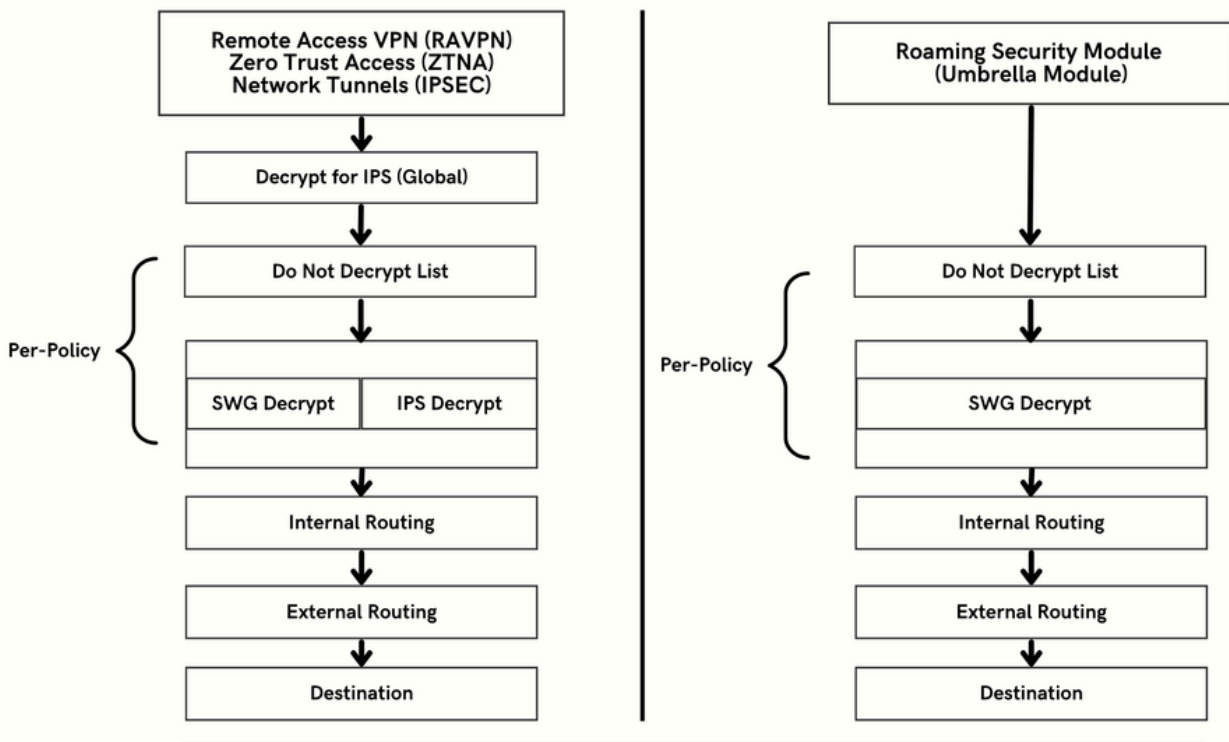
Name	Intrusion System Mode	Signatures	Last Signature Update
Connectivity Over Security	Prevention	<span style="color: red;">●</span> 472 Block <span style="color: blue;">●</span> 112 Log Only <span style="color: grey;">●</span> 50234 Ignore	Oct 21, 2024 - 03:04 pm
Balanced Security and Connectivity Default IPS Profile	Prevention	<span style="color: red;">●</span> 9402 Block <span style="color: blue;">●</span> 488 Log Only <span style="color: grey;">●</span> 40928 Ignore	Oct 21, 2024 - 03:04 pm
Security Over Connectivity	Prevention	<span style="color: red;">●</span> 22106 Block <span style="color: blue;">●</span> 760 Log Only <span style="color: grey;">●</span> 27952 Ignore	Oct 21, 2024 - 03:04 pm
Maximum Detection	Prevention	<span style="color: red;">●</span> 39777 Block <span style="color: blue;">●</span> 1366 Log Only <span style="color: grey;">●</span> 9675 Ignore	Oct 21, 2024 - 03:04 pm

## نمآلا لوصولا يف HTTPS تانايب رورم ءكرح قفدت

لاصتالا ءقيرط ىلا اءانتسا ءفلتخم رورم ءكرح تاراسم ىلع Secure Access يوتحي

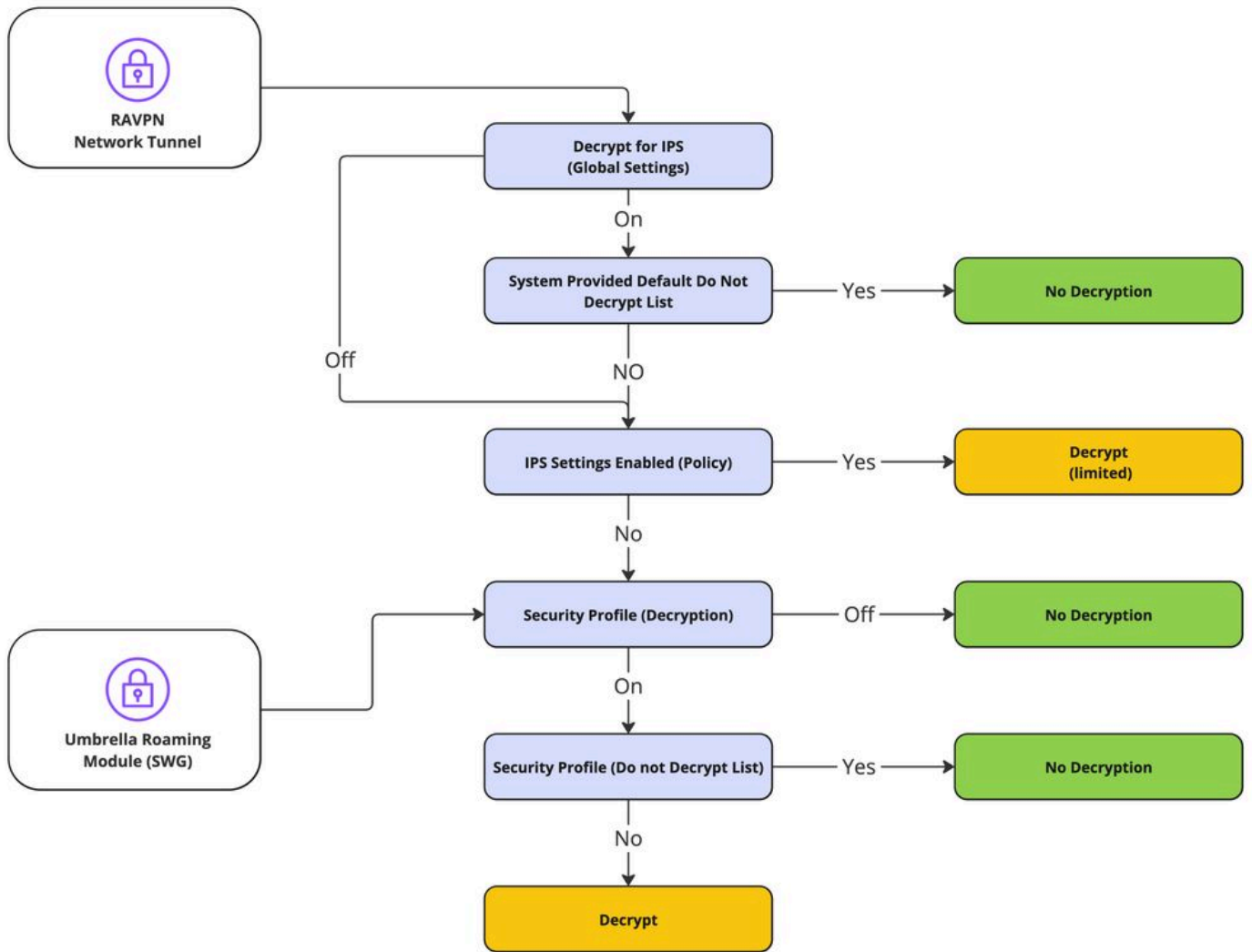
تانونوملا يف Zero Trust Access (ZTNA) و Remote Access VPN (RAVPN) نم لك كراشتي اهسفن.

فلتخم رورم ءكرح راسم ىلع (Umbrella Module ءيظمنلا ءءحولا) لاوچتلا نامأ ءءو يوتحت



## رورملا ءكرح ريفشت لك ف نكمي ىتم

كفل اهب ةصاخلا ةيسيئرلا جئاتنلاو اءارءإلا ةلسلس ليصفتلاب مسقلا اذء حرشي ريفشتلا كف مدع وأ ريفشتلا



زيمرتلا كف قفدت

## IPS ب ةلصللا اذ ريراقنلا دادعإو ليچستلاو ريفشتلا اءاغلإ

نم هيلإ لوصولان كم يذلا ريفشتلا كف ديءال ريراقنلا مسق Secure Access نمضتي ريفشتلا كف لىل لوءملا -> طاشنلا نع ثءبلا -> ةشاشلا -> تامولعملل ةءول لالء

 Customize Columns

All ▼

results per page: 50 ▼

All

DNS

Web

Firewall

IPS

ZTNA Clientless

ZTNA Client-based

Decryption





## Activity Search

Schedule Export CSV LAST 30 DAYS

FILTERS 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** X

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

## قلم تاذ تامول عم

- [Secure Access مدختسم ليلد](#)
- [تاليزن تالاولي نفالام عدلا - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت م م م دقت ل ة يرش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت م م مچرت م ا م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا م ل ا ح ل ا و ه  
ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا