Firepower Threat Defense の VPN のトラブルシューティング

この章では、Firepower Threat Defense VPN のトラブルシューティング ツールとデバッグ情報について説明します。

- システム メッセージ （1 ページ）
- VPN システム ログ （1 ページ）
- debug コマンド （3 ページ）

システム メッセージ

メッセージ センターは、トラブルシューティングを開始する場所です。この機能を使用すると、システムの使用状況およびステータスについて継続的に生成されるメッセージを確認できます。メッセージ センターを開くには、メイン メニューの [展開（Deploy）] ボタンのすぐ右側にある [システム ステータス（System Status）] アイコンをクリックします。メッセージ センターの使用方法については、システム メッセージを参照してください。

VPN システム ログ

FTD デバイスのシステム ロギング（syslog）を有効にすることができます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。VPN ロギングを有効にすると、これらの syslog は FTD デバイスから Firepower Management Center に送信され、解析とアーカイブが行われます。

表示される VPN syslog には、デフォルトの重大度レベル「ERROR」以上があります（変更されない限り）。VPN ロギングは、FTD プラットフォーム設定によって管理されます。対象となるデバイスの FTD プラットフォーム設定ポリシーで [VPN ロギング設定（VPN Logging Settings）] を編集して、メッセージの重大度を調整できます（**[プラットフォーム設定（Platform Settings）]** > **[Syslog]** > **[ロギングの設定（Logging Setup）]**）。VPN ロギングの有効化、syslog サーバの設定、およびシステム ログの表示の詳細については、Syslog の設定概要 を参照してください。

（注） デバイスがサイト間 VPN またはリモート アクセス VPN で設定されると、VPN syslog はデフォルトで自動的に Firepower Management Center に送信されます。

VPN システム ログの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
エクスポート コンプライアンス	該当なし	FTD	リーフのみ	Admin

Firepower システムは、VPN の問題の原因に関する追加情報を収集するのに役立つイベント情報をキャプチャします。表示される VPN syslog には、デフォルトの重大度レベル「ERROR」以上があります（変更されない限り）。デフォルトでは、行は [時間（Time）] 列でソートされています。

始める前に

FTD プラットフォーム設定の [FMC へのロギングを有効化（Enable Logging to FMC）] チェックボックスをオンにして、VPN ロギングを有効にします（**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Syslog] > [ロギングの設定（Logging Setup）]**）。VPN ロギングの有効化、syslog サーバの設定、およびシステム ログの表示の詳細については、Syslog の設定概要 を参照してください。

手順

ステップ 1 **[デバイス（Devices）] > [VPN] > [トラブルシューティング（Troubleshooting）]** を選択します。

ステップ 2 次の選択肢があります。

- 検索：現在のメッセージ情報をフィルタリングするには、[検索の編集（Edit Search）] をクリックします。
- 表示：選択したメッセージに関連付けられた VPN の詳細をビューに表示するには、[表示（View）] をクリックします。
- すべて表示：すべてのメッセージの VPN の詳細をビューに表示するには、[すべて表示（View All）] をクリックします。
- 削除：選択したメッセージをデータベースから削除するには [削除（Delete）] をクリックするか、またはすべてのメッセージを削除するには [すべて削除（Delete All）] をクリックします。

debug コマンド

ここでは、debug コマンドを使用して、VPN 関連の問題を診断および解決する方法について説明します。すべての使用可能なデバッグ コマンドがこのセクションで説明されているわけではありません。ここに含まれているコマンドは、VPN 関連の問題の診断における有用性に基づいています。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時か、または Cisco Technical Assistance Center（TAC）とのトラブルシューティング セッション時に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

CLI セッションでのみデバッグ出力を確認できます。出力は、コンソール ポートに接続したときか、または診断 CLI（**system support diagnostic-cli** と入力）で直接使用できます。また、**show console-output** コマンドを使用して、通常の Firepower Threat Defense CLI からの出力を確認することもできます。

特定の機能のデバッグ メッセージを表示するには、**debug** コマンドを使用します。デバッグ メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。すべてのデバッグ コマンドをオフにするには、**no debug all** を使用します。

debug *feature* ［*subfeature*］［*level*］
no debug *feature* ［*subfeature*］

構文の説明

feature	デバッグをイネーブルにする機能を指定します。使用可能な機能を表示するには、**debug ?** コマンドを使用して CLI ヘルプを表示します。
subfeature	（オプション）機能によっては、1 つ以上のサブ機能のデバッグ メッセージをイネーブルにできます。使用可能なサブ機能を表示するには ? を使用します。
level	（オプション）デバッグ レベルを指定します。このレベルは、一部の機能で使用できない場合があります。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

例

リモート アクセス VPN 上で複数のセッションを実行すると、ログのサイズを考慮するとトラブルシューティングが困難になることがあります。**debug webvpn condition**

コマンドを使用して、デバッグ プロセスをより正確に絞り込むためのフィルタを設定できます。

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

それぞれの説明は次のとおりです。

- **group** *name* は、グループ ポリシー（トンネル グループまたは接続プロファイルではない）でフィルタ処理を行います。
- **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] は、クライアントのパブリック IP アドレスでフィルタ処理を行います。サブネットマスク（IPv4）またはプレフィックス（IPv6）はオプションです。
- **reset** すべてのフィルタをリセットします。**no debug webvpn condition** コマンドを使用して、特定のフィルタをオフにできます。
- **user** *name* は、ユーザ名でフィルタ処理を行います。

複数の条件を設定すると、条件が結合（AND で連結）され、すべての条件が満たされた場合にのみデバッグが表示されます。

条件フィルタを設定したら、基本の **debug webvpn** コマンドを使用してデバッグをオンにします。条件を設定するだけではデバッグは有効になりません。デバッグの現在の状態を表示するには、**show debug** および **show webvpn debug-condition** コマンドを使用します。

次に、ユーザ jdoe で条件付きデバッグを有効にする例を示します。

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

関連コマンド

コマンド（Command）	説明
show debug	現在アクティブなデバッグ設定を示します。
undebug	ある機能のデバッグを無効にします。このコマンドは **no debug** の同意語です。

debug aaa

認証、認可、アカウンティング（AAA、「トリプルA」と発音）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *aaa* ［*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*］

構文の説明

aaa	AAA のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
accounting	（オプション）AAA アカウンティング デバッグを有効にします。
認証	（オプション）AAA 認証デバッグを有効にします。
authorization	（オプション）AAA 認可デバッグを有効にします。
common	（オプション）AAA 共通デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
internal	（オプション）AAA 内部デバッグを有効にします。
shim	（オプション）AAA shim デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
url-redirect	（オプション）AAA URL リダイレクト デバッグを有効にします。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド（Command）	説明
show debug aaa	AAA の現在アクティブなデバッグ設定を示します。
undebug aaa	AAA のデバッグを無効にします。このコマンドは **no debug aaa** の同意語です。

debug crypto

暗号に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto* ［*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*］

構文の説明

crypto	*crypto* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
ca	（オプション）PKIデバッグ レベルを指定します。使用可能なサブ機能を表示するには ? を使用します。

condition	（オプション）IPsec/ISAKMP デバッグ フィルタを指定します。使用可能なフィルタを表示するには ? を使用します。
engine	（オプション）暗号エンジン デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ike-common	（オプション）IKE 共通デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ikev1	（オプション）IKE バージョン 1 デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ikev2	（オプション）IKE バージョン 2 デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
ipsec	（オプション）IPsec デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
condition	(オプション）暗号化セキュア ソケット API デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
vpnclient	（オプション）EasyVPN クライアント デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド（**Command**）	説明
show debug crypto	暗号化の現在アクティブなデバッグ設定を示します。
undebug crypto	暗号化のデバッグを無効にします。このコマンドは **no debug crypto** の同意語です。

debug crypto ca

crypto ca に関連付けられたデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ca* ［*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*］［*1-255*］

構文の説明

crypto ca	*crypto ca* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
cluster	（オプション）PKI クラスタ デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

cmp	（オプション）CMP トランザクション デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
messages	（オプション）PKI の入力/出力メッセージのデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
periodic-authentication	（オプション）PKI 定期認証デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
scep-proxy	（オプション）SCEP プロキシデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
server	（オプション）ローカル CA サーバのデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
transactions	（オプション）PKI トランザクションデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
trustpool	（オプション）トラストプール デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド（**Command**）	説明
show debug crypto ca	crypto ca の現在アクティブなデバッグ設定を示します。
undebug	crypto ca のデバッグを無効にします。このコマンドは **no debug crypto ca** の同意語です。

debug crypto ikev1

インターネット キー エクスチェンジ バージョン 1（IKEv1）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ikev1* ［*timers*］［*1-255*］

構文の説明

ikev1	*ikev1* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
timers	（オプション）IKEv1 タイマーのデバッグを有効にします。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド（Command）	説明
show debug crypto ikev1	IKEv1 の現在アクティブなデバッグ設定を示します。
undebug crypto ikev1	IKEv1 のデバッグを無効にします。このコマンドは **no debug crypto ikev1** の同意語です。

debug crypto ikev2

インターネット キー エクスチェンジ バージョン 2（IKEv2）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ikev2* ［*ha* | *platform* | *protocol* | *timers*］

構文の説明

ikev2	デバッグ *ikev2* を有効にします。使用可能なサブ機能を表示するには ? を使用します。
ha	（オプション）IKEv2 HA デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
platform	（オプション）IKEv2 プラットフォーム デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
protocol	（オプション）IKEv2 プロトコル デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
timers	（オプション）IKEv2 タイマーのデバッグを有効にします。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド（Command）	説明
show debug crypto ikev2	IKEv2 の現在アクティブなデバッグ設定を示します。
undebugcrypto ikev2	IKEv2 のデバッグを無効にします。このコマンドは **no debug crypto ikev2** の同意語です。

debug crypto ipsec

IPsec に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *crypto ipsec* ［*1-255*］

構文の説明

ipsec	*ipsec* のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。

1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド（Command）	説明
show debug crypto ipsec	IPsec の現在アクティブなデバッグ設定を示します。
undebugcrypto ipsec	IPsec のデバッグを無効にします。このコマンドは **no debug crypto ipsec** の同意語です。

debug ldap

LDAP（Lightweight Directory Access Protocol）に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *ldap* ［*1-255*］

構文の説明

ldap	LDAP のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド（Command）	説明
show debug ldap	LDAP の現在アクティブなデバッグ設定を示します。
undebugldap	LDAP のデバッグを無効にします。このコマンドは **no debug ldap** の同意語です。

debug ssl

SSL セッションに関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *ssl* ［*cipher* | *device*］［*1-255*］

構文の説明

ssl	SSL のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
cipher	（オプション）SSL 暗号デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

device	（オプション）SSL デバイス デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
1-255	（オプション）デバッグ レベルを指定します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド（**Command**）	説明
show debug ssl	SSL の現在アクティブなデバッグ設定を示します。
undebug ssl	SSL のデバッグを無効にします。このコマンドは **no debug ssl** の同意語です。

debug webvpn

WebVPN に関連するデバッグの構成または設定については、次のコマンドを参照してください。

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

構文の説明

webvpn	WebVPN のデバッグをイネーブルにします。使用可能なサブ機能を表示するには ? を使用します。
anyconnect	（オプション）WebVPN AnyConnect デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
chunk	（オプション）WebVPN チャンク デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
cifs	（オプション）WebVPN CIFS デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
citrix	（オプション）WebVPN Citrix デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
compression	（オプション）WebVPN 圧縮デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
condition	（オプション）WebVPN フィルタ条件デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
cstp-auth	（オプション）WebVPN CSTP 認証デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

customization	（オプション）WebVPNカスタマイズデバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
failover	（オプション）WebVPN フェールオーバー デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
html	（オプション）WebVPN HTML デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
javascript	（オプション）WebVPN Javascript デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
kcd	（オプション）WebVPN KCD デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
listener	（オプション）WebVPN リスナー デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
mus	（オプション）WebVPN MUS デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
nfs	（オプション）WebVPN NFS デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
request	（オプション）WebVPN 要求デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
response	（オプション）WebVPN 応答デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
saml	（オプション）WebVPN SAML デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
session	（オプション）WebVPN セッション デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
task	（オプション）WebVPN タスク デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
transformation	（オプション）WebVPN 変換デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
url	（オプション）WebVPN URL デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
util	（オプション）WebVPN ユーティリティ デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。
xml	（オプション）WebVPN XML デバッグ レベルを指定します。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

関連コマンド

コマンド（Command）	説明
show debug webvpn	WebVPN の現在アクティブなデバッグ設定を示します。
undebug webvpn	WebVPN のデバッグを無効にします。このコマンドは **no debug webvpn** の同意語です。