VPNのモニタリングとトラブルシューティング

この章では、Firepower Threat Defense VPN のモニタリングツール、パラメータ、統計情報、およびトラブルシューティングについて説明します。

[サイト間 VPN 概要（Site-to-Site VPN Summary）] ページ

[サイト間 VPN 概要（Site-to-Site VPN Summary）] ページを使用して、ユーザーの現在のステータス、デバイス タイプ、クライアント アプリケーション、ユーザーの位置情報、接続時間などの VPN ユーザーに関する統合情報を表示できます。VPN インターフェイス、トンネルステータスなど、設定された VPN トポロジの詳細情報を表示できます。

すべての VPN トポロジについて、編集ボタンと削除ボタンを使用してトポロジを編集または削除できます。SASE トポロジ VPN の場合、トポロジを展開、編集、および削除するオプションがあります。

リモートアクセス VPN ダッシュボード

リモートアクセス仮想プライベートネットワーク（RA VPN）を使用すると、リモートユーザーはネットワークに安全に接続できます。RA VPN ダッシュボードでは、デバイス上のアクティブな RA VPN セッションからのリアルタイムデータを監視でき、ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できます。

RA VPN ダッシュボード（[概要（Overview）] > [ダッシュボード（Dashboards）] > [リモートアクセスVPN（Remote Access VPN）]）には、Firewall Management Center によって管理される

Threat Defense デバイス上のアクティブな RA VPN セッションのスナップショットが表示されます。

ダッシュボードには以下のウィジェットがあります。

- [アクティブなセッション（Active Sessions）]（表形式ビュー）
- [アクティブなセッション（Active Sessions）]（マップビュー）
- セッション（Sessions）
- [デバイスアイデンティティ証明書（Device Identity Certificates）]

[アクティブなセッション（Active Sessions）]（表形式ビュー）

このウィジェットには、接続されているアクティブな RA VPN ユーザーの表形式のビューが表示されます。ユーザー名、割り当てられた IP、パブリック IP、ログイン時間、VPN ゲートウェイ（Threat Defense デバイス）、クライアント アプリケーション、クライアント オペレーティング システム、接続プロファイル、グループポリシーなど、アクティブな RA VPN セッションの詳細を確認できます。フィルタを使用して、さまざまな基準に基づいて検索を絞り込むことができ、個々のセッションで以下のアクションも実行できます。

- 特定のユーザーのセッションを終了する。
- 特定の VPN ゲートウェイに接続されている特定のユーザーのすべてのセッションを終了する。
- 特定の VPN ゲートウェイに接続されているすべてのセッションを終了する。

クライアントデバイスがデュアルアドレススタックをサポートし、Firewall Threat Defense デバイスの RA VPN 設定で IPv4 および IPv6 アドレスプールが許可されている場合、クライアントはヘッドエンドデバイスとの RA VPN セッションを確立すると、IPv4 および IPv6 アドレスをクライアントのトンネルインターフェイスに割り当てます。RA VPN セッションには、Threat Defense デバイスの IPv4 アドレスと IPv6 アドレスの 2 つの IP アドレスがあります。Firewall Management Center は、同じユーザーの 2 つのセッションを示しています。1 つは IPv4 アドレス、もう 1 つは IPv6 アドレスで、セッション数は 2 つです。

したがって、デバイスで **show vpn-sessiondb l2l filter ipaddress** コマンドが実行されユーザーからの RA VPN セッションが 1 つしかない場合でも、Firewall Management Center は 2 つの異なるセッションを示します。

[アクティブなセッション（Active Sessions）]（マップビュー）

このウィジェットには、デバイスの RA VPN セッションを介して接続されているユーザーの場所を可視化するためのインタラクティブなヒートマップが表示されます。

- ユーザーセッションがある国は、青の色合いで表示されます。
- マップの凡例には、国のセッション数とその国に使用される青の色合いとの相関関係を示すスケールが表示されます。

- マップ上にマウスポインタを合わせると、国名とアクティブなユーザーセッションの総数が表示されます。
- ズームイン、ズームアウト、およびリセットのオプションを使用できます。

セッション（Sessions）

このウィジェットでは、デバイス上のアクティブな RA VPN セッションからのリアルタイムデータを監視でき、次の項目に従って、アクティブな RA VPN セッションの分布をフィルタ処理して表示できます。

- [デバイス（Device）]：デバイスごとのセッション数が表示されます。
- [暗号化タイプ（Encryption Type）]：セキュアクライアント SSL または IPsec セッションの数が表示されます。
- [Secure Clientバージョン（セキュアクライアント Version）]：セキュアクライアント バージョンごとのセッションが表示されます。
- [オペレーティングシステム（Operating System）]：オペレーティングシステムごとのセッションが表示されます。Windows、Linux、Mac、モバイル OS など。
- [接続プロファイル（Connection Profile）]：接続プロファイルごとのセッションが表示されます。

[デバイスアイデンティティ証明書（Device Identity Certificates）]

このウィジェットには、RA VPN ゲートウェイのアイデンティティ証明書の有効期限に関する情報が表示されます。期限切れの証明書と、1 ヵ月以内に期限が切れる証明書を確認できます。[詳細の表示（View Details）] をクリックして、[デバイス（Device）] > [証明書（Certificates）] ページに証明書を表示します。

VPN セッションとユーザー情報

システムは、VPN 関連アクティビティを含む、ネットワーク上のユーザーアクティビティの詳細を伝達するイベントを生成します。システムのモニタリング機能を使用すると、リモートアクセス VPN の問題が存在するかどうか、および存在する場所を迅速に特定できます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。オプションで、必要に応じてリモートアクセス VPN ユーザーをログアウトすることができます。

リモート アクセス VPN アクティブ セッションの表示

[分析（Analysis）] > [ユーザー（Users）] > [アクティブなセッション（Active Sessions）]

ユーザー名、ログイン時間、認証タイプ、割り当て済み/パブリック IP アドレス、デバイスの詳細、クライアントのバージョン、エンドポイント情報、スループット、帯域幅消費グループ

ポリシー、トンネルグループなどのサポート情報を使用して、現在ログインしているVPNユーザーを任意の時点で表示できます。また、現在のユーザー情報をフィルタ処理し、ユーザーをログアウトし、要約リストからユーザーを削除することもできます。

（注） 高可用性展開でVPNを構成する場合、アクティブなVPNセッションに対して表示されるデバイス名は、ユーザーセッションを識別したプライマリデバイスまたはセカンダリデバイスである可能性があります。

リモート アクセス VPN ユーザー アクティビティの表示

[分析（Analysis）] > [ユーザ（Users）] > [ユーザ アクティビティ（User Activity）]

ネットワーク上のユーザーアクティビティの詳細を表示できます。システムは履歴イベントを記録し、接続プロファイル情報、IPアドレス、位置情報、接続時間、スループット、デバイス情報などの VPN 関連情報が含まれています。

VPN ヘルス イベント

[ヘルスイベント（Health Events）] ページでは、Firewall Management Center のヘルスモニターで記録された VPN ヘルスイベントを確認できます。デバイス間の 1 つ以上の VPN トンネルがダウンすると、ヘルスモニターは次のイベントを追跡します。

- Secure Firewall Threat Defense のサイト間 VPN
- Secure Firewall Threat Defense のリモート アクセス VPN

VPN ヘルス イベントの表示

Secure Firewall Management Center 上の [ヘルス イベント（Health Events）] ページからヘルス イベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルスイベントが取得されます。表示したいヘルスイベントを生成したモジュールを指定することによって、イベントを絞り込むことができます。

このタスクを実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリストである必要があります。

手順

ステップ 1 **[システム（System）] > [ヘルス（Health）] > [イベント（Events）]** を選択します。

ステップ 2 [モジュール名（Module Name）] 列で [VPN ステータス（VPN Status）] を選択します。

VPN セッションが稼働していても VPN トンネルが非アクティブであるというアラートが発生する場合は、VPN正常性アラートを無効にすることができます。詳細は、次のトピックを参照してください。

- ヘルスモニタリングからのアプライアンスの除外
- 正常性ポリシーモジュールの除外

VPN のトラブルシューティング

このセクションでは、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

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）] ボタンの右隣にある [システムステータス（System Status）] をクリックします。

VPN システム ログ

Firewall Threat Defense デバイスの VPN トラブルシュート syslog のロギングを有効にできます。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、Firewall Threat Defense デバイスから Firewall Management Center に VPN syslog が送信されます。

すべての VPN syslog には、デフォルトのシビラティ（重大度）レベル [エラー（Errors）] 以上が設定されています（変更されない限り）VPN ロギングは、Firewall Threat Defense プラットフォーム設定を介して管理できます。対象となるデバイスの Firewall Threat Defense 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、メッセージのシビラティ（重大度）レベルを調整できます。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、Firewall Threat Defense デバイスの syslog ロギングの設定 を参照してください。

[トラブルシューティングログ（Troubleshooting Logs）] テーブル（[デバイス（Devices）] > [トラブルシューティングログ（Troubleshooting Logs）]）では、VPN syslog メッセージを表示および分析して、ネットワークとデバイスの設定に関する問題を特定および分離できます。

VPN ログのログレベルをレベル 3（[エラー（Errors）]）に設定することを推奨します。VPN ロギングレベルをレベル 4 以上（[警告（Warnings）]、[通知（Notification）]、[情報（Infromational）]、または [デバッグ（Debugging）]）に設定すると、Firewall Management Center が過負荷になる可能性があります。

（注） サイト間 VPN またはリモートアクセス VPN を設定してデバイスを設定すると、デフォルトで自動的に VPN syslog が Firewall Management Center に送信されます。

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。ここで説明するコマンドは、すべてを網羅しているわけではありません。ここには、VPN 関連の問題の診断に役立つコマンドが含まれています。

使用上のガイドライン

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. 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低くなります。

デバッグ出力は、CLI セッションでのみ表示できます。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）で直接入手できます。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。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、ユーザー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、ユーザー 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	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

デバッグ設定または認証、認可、およびアカウンティング（AAA）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。
authentication	（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	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	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 サーバーのデバッグ 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	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	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	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	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	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	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	（任意）WebVPN Secure Client 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	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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。