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（**Overview** > **Dashboards** > **Remote Access VPN**）は、Firewall Management Center が管理する脅威防御デバイスのアクティブな RA VPN セッションのスナップショットを取得します。

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）]：Secure Client 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（Secure Client Version）]：Secure Client 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、**Devices** > **Certificates** ページで証明書を表示します。

Cisco SD-WAN サマリーダッシュボード

Cisco SD-WAN サマリーダッシュボード（[概要（Overview）]>[ダッシュボード（Dashboards）] > [SD-WANサマリー（SD-WAN Summary）]）には、WAN デバイスとデバイスのインターフェイスのスナップショットが表示されます。このダッシュボードは、次の操作に役立ちます。

- アンダーレイおよびオーバーレイ（VPN）トポロジの問題を特定する。
- 既存の [ヘルスモニタリング（Health Monitoring）]、[デバイス管理（Device Management）]、および [サイト間モニタリング（Site-to-Site Monitoring）] ページを使用して、VPN の問題をトラブルシューティングする。
- WAN インターフェイスのアプリケーション パフォーマンス メトリックをモニターする。Threat Defense は、これらのメトリックに基づいてアプリケーション トラフィックを誘導します。

WAN デバイスは、次の条件のいずれかを満たしている必要があります。

- デバイスは VPN ピアである。
- デバイスに WAN インターフェイスがある。

WAN インターフェイスは、次の条件のいずれかを満たしている必要があります。

- インターフェイスで IP アドレスベースのパスモニタリングが有効になっている。
- インターフェイスには、ポリシーベースルーティング（PBR）ポリシーがあり、少なくとも 1 つのアプリケーションがポリシーをモニターするように設定されている。

PBR ポリシーとパスのモニタリングの詳細については、ポリシーベースルーティングを参照してください。

[アップリンクの決定（Uplink Decisions）] をクリックして、[VPN トラブルシューティング（VPN Troubleshooting）] ページを表示します。ID が 880001 の syslog を表示できます。これらの syslog には、設定された PBR ポリシーに基づいて、Threat Defense がトラフィックを誘導するインターフェイスが表示されます。

上記の syslog を表示し、このダッシュボードでデータを表示するには、「SD-WAN サマリーダッシュボードを使用するための前提条件 （4 ページ）」を確認してください。

クラスタの場合、このダッシュボードには、データノードではなく、制御ノードのアプリケーション評価指標のみが表示されます。

SD-WAN サマリーダッシュボードを使用するための前提条件

- このダッシュボードを表示するには、管理者、セキュリティアナリスト、またはメンテナンスユーザーである必要があります。
- Threat Defense デバイスはバージョン 7.2 以降である必要があります。
- WAN インターフェイスで IP ベースのパモニタリングと HTTP ベースのアプリケーションモニタリングを有効にします。
  1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
  2. 編集するデバイスの横にある編集アイコンをクリックします。
  3. 編集するインターフェイスの横にある編集アイコンをクリックします。
  4. [パスモニタリング（Path Monitoring）] タブをクリックします。
  5. [IP ベースのモニタリングの有効化（Enable IP based Path Monitoring）] チェックボックスをオンにします。
  6. [HTTP ベースのアプリケーション モニタリングの有効化（Enable HTTP based Application Monitoring）] チェックボックスをオンにします。
  7. [OK] をクリックします。

- 少なくとも 1 つのアプリケーションをモニタリングするように設定した PBR ポリシーを設定します。
  1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
  2. 編集するデバイスの横にある編集アイコンをクリックします。
  3. [ルーティング（Routing）] をクリックします。
  4. 左側のペインで、[ポリシーベースルーティング（Policy Based Routing）] をクリックします。
  5. [追加（Add）] をクリックします。
  6. [入力インターフェイス（Ingress Interface）] ドロップダウンリストでインターフェイスを選択します。
  7. [追加（Add）] をクリックして、転送アクションを設定します。
  8. パラメータを設定します。
  9. **[Save（保存）]** をクリックします。

- WAN インターフェイスのアプリケーション パフォーマンス メトリックを表示するには、以下の手順を実行する必要があります。
  - Threat Defense デバイスはバージョン 7.4.1 である必要があります。
  - SD-WANモジュールのデータ収集を正常性ポリシーで有効にします。
    1. [システム（System）] > [ポリシー（Policy）] を選択します。
    2. [正常性ポリシーの編集（Edit health policy）] アイコンをクリックします。
    3. [ヘルスモジュール（Health Modules）] タブの [SD-WAN] で、[SD-WANモニタリング（SD-WAN Monitoring）] トグルボタンをクリックします。
  - PBR ポリシーにアプリケーションを設定します。
    1. [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アクセスリスト（Access List）] > [拡張（Extended）] の順に選択します。
    2. アクセスリストの横にある編集アイコンをクリックし、PBR ポリシーにアプリケーションを追加します。
  - 4 つのアプリケーションメトリックのいずれかを使用して、ポリシーの転送アクションを設定します。
    1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
    2. 編集するデバイスの横にある編集アイコンをクリックします。
    3. [ルーティング（Routing）] をクリックします。

4. 左側のペインで、[ポリシーベースルーティング（Policy Based Routing）] をクリックします。
5. 編集するポリシーの横にある編集アイコンをクリックします。
6. [ポリシーベースルートの編集（Edit Policy Based Route）] ダイアログボックスで、対応する ACL の横にある編集アイコンをクリックします。
7. [転送アクションの編集（Edit Forwarding Actions）] ダイアログボックスで、[インターフェイスの順序（Interface Ordering）] ドロップダウンリストから以下のいずれかのオプションを選択します。
   - **最小ジッター**
   - **最大平均オピニオン評点**
   - **最小ラウンドトリップ時間**
   - **最小パケット損失**

   [インターフェイスポリシー（Interface Priority）] または [順序（Order）] を選択した場合、アプリケーション モニタリングはインターフェイスで有効になりません。

- WAN インターフェイスで ECMP を設定します。
  1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
  2. 編集するデバイスの横にある編集アイコンをクリックします。
  3. [ルーティング（Routing）] をクリックします。
  4. 左側のペインで [ECMP] をクリックします。
  5. [追加（Add）] をクリックし、ECMP ゾーンの名前を指定します。
  6. [追加 （Add）] をクリックして、[使用可能なインターフェイス（Available Interfaces）] から [選択したインターフェイス（Selected Interfaces）] にインターフェイスを移動します。
  7. [OK] をクリックします。
- トラフィックがインターフェイスを通過することを確認します。
- Threat Defense デバイスが DNS スヌーピングを実行できるように、各 WAN デバイスで DNS インスペクションを有効にし、信頼できる DNS サーバーを設定します。
  1. [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択します。
  2. 編集する Threat Defense ポリシーの横にある編集アイコンをクリックします。
  3. 左側のペインで [DNS] をクリックします。

4. [DNS設定（DNS Settings）] タブをクリックします。
5. [デバイスによるDNS名前解決を有効にする（Enable DNS name resolution by device）] チェックボックスをオンにします。
6. [信頼できるDNSサーバー（Trusted DNS Servers）] タブをクリックします。
7. 次のいずれかを実行します。
   - [すべてのDNSサーバーを信頼（Trust Any DNS server）] トグルボタンをクリックします。
   - 信頼できる DNS サーバーを追加するには、[DNSサーバーの指定（Specify DNS Servers）] で [編集（Edit）] をクリックします。

- [アップリンク判断（Uplink Decisions）] をクリックしたときに syslog を表示するには、次の手順を実行する必要があります。
  - [デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] を選択し、Threat Defense ポリシーを作成または編集します。
  - 左側のペインで、[Syslog] をクリックします。
  - [ロギングのセットアップ（Logging Setup）] タブをクリックします。
  - Threat Defense デバイスのデータ プレーン システム ロギングをオンにするには、[ロギングの有効化（Enable Logging）] チェックボックスをオンにします。
  - [すべてのログ（All Logs）] オプションボタンをクリックして、すべての障害対応 syslog メッセージのロギングを有効にします。

    または

    VPN 障害対応メッセージのみのロギングを有効にするには、[VPNログ（VPN Logs）] オプションボタンをクリックします。
  - [保存（Save）] をクリックします。

SD-WANサマリーダッシュボードを使用したWANデバイスとインターフェイスのモニタリング

SD-WAN サマリーダッシュボードの [概要（Overview）] タブには、以下のウィジェットがあります。

- 最上位アプリケーション（Top Applications） （8 ページ）
- WAN 接続 （8 ページ）
- VPN トポロジ （8 ページ）

• WAN インターフェイスのスループット （9 ページ）
• デバイスインベントリ（Device Inventory） （9 ページ）
• WAN デバイスの正常性 （9 ページ）

最上位アプリケーション（Top Applications）

このウィジェットには、スループットに応じてランク付けされた上位 10 個のアプリケーションが表示されます。

[最後を表示（Show Last）] ドロップダウンリストから、時間範囲を選択できます。指定できる範囲は 15 分～ 2 週間です。

WAN 接続

このウィジェットには、WANインターフェイスのステータスの概要が表示されます。[オンライン（Online）]、[オフライン（Offline）] 、または [データなし（No Data）] ステータスの WAN インターフェイスの数が表示されます。このウィジェットを使用してサブインターフェイスをモニタリングすることはできません。

[すべてのインターフェイスを表示（View All Interfaces）] をクリックして、ヘルスモニタリングページのインターフェイスに関する詳細を表示します。

WAN インターフェイスが [オフライン（Offline）] または [データなし（No Data）] ステータスの場合は、ヘルスモニタリングページからトラブルシューティングできます。

1. [モニタリング（Monitoring）] ペインで、[デバイス（Devices）] を展開します。
2. 対応する WAN デバイスをクリックして、デバイス固有の正常性情報を表示します。
3. [インターフェイス （Interface）] タブをクリックして、インターフェイスのステータスを表示し、特定の時間のトラフィック統計情報を集約します。

   または、[システムとトラブルシューティングの詳細表示（View System and Troubleshoot Details）] をクリックします。必要なすべての詳細を含むヘルスモニタリングページが表示されます。

VPN トポロジ

このウィジェットには、サイト間 VPN トンネルのステータスの概要が表示されます。[アクティブ（Active）]、 [非アクティブ（Inactive）]、および [アクティブデータなし（No Active Data）] のVPN トンネルの数が表示されます。

[すべての接続を表示（View All Connections）] をクリックして、[サイト間VPNモニタリング（Site-to-site VPN Monitoring）] ダッシュボードで VPN トンネルの詳細を確認します。

トンネルが [非アクティブ（Inactive）] または [アクティブデータなし（No Active Data）] ステータスの場合は、[サイト間VPNモニタリング（Site-to-site VPN Monitoring）] ダッシュボードを使用してトラブルシューティングできます。**[トンネルステータス（Tunnel Status）]** ウィ

ジェットで、トポロジの上にカーソルを置き、**View** ( ) をクリックして以下のいずれかを実行します。

- [CLIの詳細（CLI Details）] タブをクリックして、VPN トンネルの詳細を表示します。
- [パケットトレーサ（Packet Tracer）] タブをクリックして、トポロジにパケットトレーサツールを使用します。

WAN インターフェイスのスループット

ウィジェットは、選択した期間におけるWANインターフェイスの平均スループットをモニターします。

インターフェイスのスループットは4つの帯域に分類されます。これらの詳細は、コスト計画とリソースの調達に役立ちます。[最後を表示（Show Last）] ドロップダウンリストから、時間範囲を選択できます。指定できる範囲は 15 分～ 2 週間です。

[ヘルスモニタリングの表示（View Health Monitoring）] をクリックして、ヘルスモニタリングページのインターフェイスに関する詳細を表示します。

デバイスインベントリ（Device Inventory）

このウィジェットでは、モデルに従ってすべての管理対象 WAN デバイスがリストおよびグループ化されます。

[デバイス管理の表示（View Device Management）] をクリックして、[デバイス管理（Device Management）] ページでデバイスの詳細を確認します。

WAN デバイスの正常性

このウィジェットには、WAN デバイスの正常性に応じてデバイス数が表示されます。エラーや警告のあるデバイス、または[無効（Disabled）]ステータスのデバイスの数を表示できます。

[ヘルスモニタリングの表示（View Health Monitoring）] をクリックしてアラームを表示し、問題をすばやく特定して切り分け、解決します。

デバイスの正常性が影響を受ける場合は、[ヘルスモニタリング（Health Monitor）]ページからトラブルシューティングできます。

1. [モニタリング（Monitoring）] ペインで、[デバイス（Devices）] を展開します。
2. 対応する WAN デバイスをクリックして、デバイス固有の正常性情報を表示します。
3. [システムとトラブルシューティングの詳細を表示（View System & Troubleshoot Details）] をクリックします。必要なすべての詳細を含むヘルスモニタリングページが表示されます。

デバイスは、以下のような複数の理由で[無効（Disabled）]ステータスになることがあります。

- 管理インターフェイスが無効になっています。
- デバイスの電源がオフになっています。

• デバイスをアップグレード中です。

SD-WAN サマリーダッシュボードを使用した WAN インターフェイスのアプリケーション評価指標のモニタリング

[アプリケーション モニタリング（Application Monitoring）] タブでは、WAN デバイスを選択し、対応する WAN インターフェイスのアプリケーション パフォーマンス メトリックを表示できます。これらのメトリックには、ジッター、ラウンドトリップ時間（RTT）、平均オピニオン評点（MOS）、パケット損失が含まれます。

デフォルトでは、メトリックデータは5分ごとに更新されます。更新時間は変更できます。範囲は 5 ～ 30 分です。メトリックは、表形式またはグラフィック形式で表示できます。WAN インターフェイスごとに、最新のメトリック値が表に表示されます。グラフィカルデータの場合、最大 24 時間の時間間隔を選択して、対応する WAN インターフェイスのメトリックデータを表示できます。

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。

サイト間 VPN 接続イベントのモニタリング

サイト間 VPN 接続イベントでは、VPN が接続を暗号化するかどうかを知ることができ、特にマルチホップ VPN 展開における接続の問題のトラブルシューティングに役立ちます。Firewall Management Center のイベントダッシュボードには、トラフィックを暗号化または復号する VPN ピアの IP アドレス（ピアの IKE アドレス）が表示され、VPN アクションが次のように表示されます。

- 接続が VPN によって復号されている場合、**[復号ピア（Decrypt Peer）]** 列には、フローが受信されたピアの IP アドレスが表示され、VPN アクションは **[復号（Decrypt）]** と表示されます。
- 接続が VPN によって暗号化されている場合、**[暗号化ピア（Encrypt Peer）]** 列には、フローの送信先である VPN ピアの IP アドレスが表示され、VPN アクションは **[暗号化（Encrypt）]** と表示されます。
- VPN サーバーが接続をカスケードする場合、1 つのトンネルで復号され、別のトンネルで再暗号化されます。この場合、[暗号化ピア（Encrypt Peer）] と [復号ピア（Decrypt Peer）] の IP アドレスの両方がイベントに表示されます。[VPNアクション（VPN Action）] 列には、アクションとして [VPNルーティング（VPN Routing）] が表示され、接続が VPN サーバーを通過することを示します。

復号されたトラフィックのアクセス コントロール ポリシーのバイパス（sysopt permit-vpn）オプションを有効にすると、システムはアクセス コントロール ポリシーをバイパスし、復号されたトラフィックのイベントをログに記録しません。このオプションはデフォルトで無効になっており、VPN トンネル内のすべての復号されたトラフィックは ACL インスペクションの対象となります。

サイト間 VPN 接続イベントの表示

Firewall Management Center の接続イベントビューアにアクセスして、VPN で接続トラフィックが暗号化されるかどうかを確認し、VPN ピアの詳細を取得します。

始める前に

アクセス制御ルールで、接続の開始時と終了時に接続イベントのロギングを有効にするようにしてください。

手順

ステップ 1 **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]**を選択します。

ステップ 2 [接続イベントのテーブルビュー（Table View of Connection Events）] タブに移動します。

ステップ 3 イベントのテーブルビューでは、デフォルトで複数のフィールドが非表示になっています。表示されるフィールドを変更するには、任意の列名の [x] アイコンをクリックして、フィールド選択ツールを表示します。

ステップ 4 次の列を選択します。

- ピアの復号（Decrypt Peer）
- ピアの暗号化（Encrypt Peer）
- VPN Action

ステップ 5 [Apply] をクリックします。

接続イベントの詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイド [英語] の「Connection and Security-Related Connection Events」を参照してください。

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

Debug commands consume high-priority CPU resources, which can make the system unusable. Only use debug commands for specific troubleshooting or when instructed by Cisco TAC. To minimize impact, run these commands during periods of low network traffic.

You can view debug output in a CLI session only. Output is directly available when connected to the Console port, or when in the diagnostic CLI (enter **system support diagnostic-cli**). You can also view output from the device CLI with **show console-output** command.

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。