Trend Micro™ Cloud Edge

2023 年 7 月

管理者ガイド

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/dcx/s/solution/000207383?language=ja

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、

P/N: APEM09742/230620_JP_R1 (2024/01)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

Cloud Edge により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。Cloud Edge における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

はじめに

第 1 章：Cloud Edge について

第 2 章：Cloud Edge の配信のベストプラクティス

第 6 章：Cloud Edge Cloud Console

第 7 章：Cloud Edge On-Premises

第 8 章：テクニカルサポート

索引

はじめに

はじめに

『Trend Micro Cloud Edge 管理者ガイド』をお読みいただきありがとうございます。このガイドでは、Cloud Edge の概要を紹介し、Trend Micro Remote Manager を使用する方法、Cloud Edge Cloud Console でゲートウェイを登録してアカウントを同期する方法、Cloud Edge ゲートウェイをユーザのオフィスに配置する方法について説明します。

Trend Micro Remote Manager、Trend Micro Licensing Management Portal (LMP) は販売代理店やマネージドサービスプロバイダ (MSP) などのパートナー向けのプラットフォームです。

ドキュメント

Cloud Edge のドキュメントセットには、次のドキュメントが含まれます。

表 1. 製品ドキュメント

ドキュメント	説明
オンラインヘルプ	オンラインヘルプには、Cloud Edge のコンポーネントや機能の説明のほか、Cloud Edge を設定するために必要な手順が記載されています。 Cloud Edge Cloud Console では、各画面の右側にコンテキストに応じたヘルプが表示されます。
管理者ガイド	Cloud Edge の概要を紹介し、Trend Micro Remote Manager を使用する方法、Cloud Edge Cloud Console でゲートウェイを登録してアカウントを同期する方法、Cloud Edge ゲートウェイをユーザのオフィスに配置する方法について説明した PDF 版のドキュメントです。
新機能	新機能ファイルには、新しい機能の説明が記載されています。
サポートポータル	サポートポータルは、問題解決およびトラブルシューティング情報に関するオンラインのデータベースです。製品の既知の問題に関する最新情報も参照できます。次のサポートポータル Web サイトをご利用ください。 https://success.trendmicro.com/dcx/s/?language=ja

対象読者

Cloud Edge の各ドキュメントは IT 管理者およびセキュリティアナリストを対象としたもので、ネットワークおよび情報セキュリティに関する次のような専門的な知識があることを前提としています。

- ネットワークトポロジ
- データベース管理
- ポリシーの管理と施行

脅威イベント相関分析に精通しているかどうかは問いません。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記	説明
 注意	設定上の注意事項
 ヒント	推奨事項
 重要	必要な設定、初期設定、製品の制限事項に関する情報
 警告!	避けるべき操作や設定についての注意

要件

Cloud Edge では Amazon Elastic Compute Cloud™を利用しており、Amazon Web Services の要件を満たす必要があります。詳細については、http://aws.amazon.com/ec2/を参照してください。

表 3. サポートされている Web ブラウザ

ブラウザ	バージョン
Mozilla Firefox™	最新バージョン
Google Chrome™	最新バージョン
Microsoft Edge™	Chromium

第 1 章

Cloud Edge について

Cloud Edge の概要

Trend Micro Cloud Edge は、次世代のオンプレミスファイアウォールの利点と Security as a Service の利便性を兼ね備えた、クラウド型の Web セキュリティゲートウェイ製品です。Cloud Edge では、アプリケーション制御をユーザやポートの識別と高度に連携させることで、マルチレイヤ型の保護を提供します。URL フィルタ、帯域幅制御、侵入防止、不正プログラム検索、メールセキュリティ、Web レピュテーションなどのセキュリティ機能により、ネットワーク侵害や業務の中断に対する保護が強化されます。オンプレミスまたはクラウドのネットワークパケットを内容まで調べてフィルタリングすることで、脅威の侵入をゲートウェイで阻止します。また、仮想プライベートネットワーク (VPN) もサポートしており、モバイルデバイス、企業サイト、遠隔地の従業員による接続も保護します。

Cloud Edge ゲートウェイを顧客のオフィスに配置した後は、ユーザアクセスやセキュリティポリシーを Cloud Edge Cloud Console で一元管理できます。Cloud Edge Cloud Console には、必要に応じて、Trend Micro Remote Manager からシングルサインオンでアクセスすることもできます。Remote Manager は Cloud Edge と連携するため、Remote Manager を使用すれば、サポート対象のゲートウェイやトレンドマイクロ製品に関するグラフィック形式のレポートや要約されたダッシュボードデータに 1 か所からアクセスできます。Remote Manager は複数の顧客のライセンス管理や請求処理にも役立ちます。

次の図は、Cloud Edge の仕組みを示したものです。

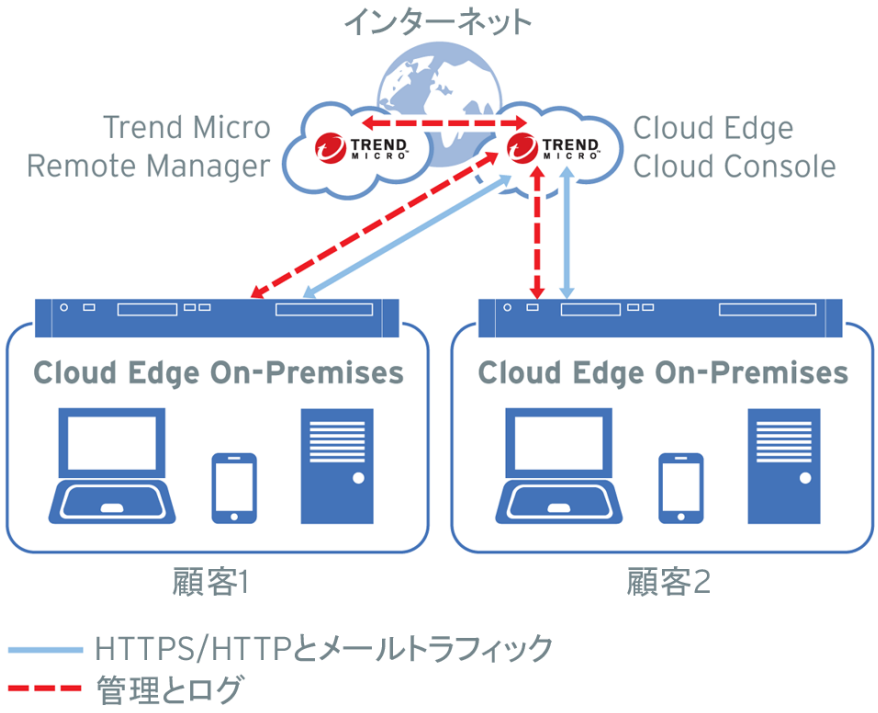


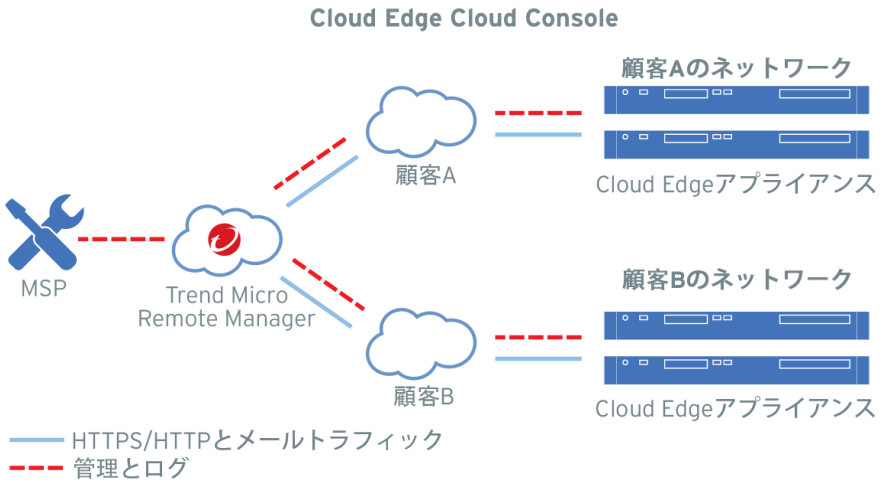
表 1-1. Cloud Edge コンポーネント

コンポーネント	説明
Cloud Edge Cloud Console	Cloud Edge Cloud Console は、クラウドでホスティングされる Security-as-a-Service 管理コンソールです。 Cloud Edge Cloud Console では、地理的に離れた複数のネットワークに分散した Cloud Edge ゲートウェイのユーザアクセスやセキュリティポリシーを管理できます。Cloud Edge Cloud Console はクラウドに配置されており、いつでも動的にアクセスできます。

コンポーネント	説明
Cloud Edge ゲートウェイ	Cloud Edge ゲートウェイは、ネットワークセキュリティを提供するために設計された、クラウドを活用する UTM (統合脅威管理) デバイスです。 Cloud Edge ゲートウェイは次世代のセキュリティを実現するコンポーネントで、顧客の環境に配置されます。オンプレミスのファイアウォールとして不正なコンテンツを検索してブロックしたり、ネットワークブリッジとしてセキュリティの脅威を透過的に監視したりできます。
Trend Micro Remote Manager	Trend Micro Remote Manager はトレンドマイクロのチャネルパートナーおよび MSP を対象とした管理コンソールです。ライセンス管理だけでなく、すべての顧客を対象としたリアルタイムのセキュリティダッシュボードおよびレポート機能を提供します。 サポート対象のゲートウェイやトレンドマイクロ製品に関するグラフィック形式のレポートや要約されたダッシュボードデータにアクセスできます。また、Remote Manager は複数の顧客のライセンス管理や請求処理にも使用できます。Cloud Edge Cloud Console には、必要に応じて、Remote Manager からシングルサインオンでアクセスすることもできます。

Cloud Edge の仕組み

次の図は、Cloud Edge の代表的な顧客環境を表しています。



1. Cloud Edge ゲートウェイを顧客のオフィスに配置します。
2. Cloud Edge Cloud Console を使用して、ユーザアクセスとセキュリティポリシーを一元的に管理します。
3. Remote Manager からシングルサインオンで Cloud Edge Cloud Console にアクセスできます。
4. Remote Manager を使用して、サポート対象のゲートウェイとトレンドマイクロ製品に関するレポートやダッシュボードデータに 1 か所からアクセスします。Remote Manager は複数の顧客のライセンス管理や請求処理にも役立ちます。
5. ログが Cloud Edge ゲートウェイから Cloud Edge Cloud Console と Remote Manager へ送信されます。

Cloud Edge ゲートウェイを配置する時に、顧客は各ゲートウェイをファイアウォール (ルーティングモード) または透過的なブリッジ (ブリッジモード) として設置できます。Cloud Edge ゲートウェイでは、ゲートウェイを通過する

データについて、内容も含めたトラフィック全体を調べて、シグネチャの検索、挙動の分析、規制やコンプライアンスの分析、および過去のセッション履歴と照らし合わせたセッションの相関関係分析を行います。

MSP は Cloud Edge Cloud Console を使用して、複数のネットワークに分散された登録済みの Cloud Edge ゲートウェイを通過するすべてのトラフィックに対するポリシーを管理します。クラウドでの安全なトラフィック転送を開始する前に、MSP が Cloud Edge ゲートウェイを Cloud Edge Cloud Console に登録します。

メールセキュリティ対策がクラウド検索 (初期設定) に設定されている場合は、すべてのメール要求が調査のためにクラウド経由で直接ルーティングされます。クラウド経由でルーティングされる要求は、マネージドサービスプロバイダが設定したポリシーに基づいて、Cloud Edge クラウドバックエンドサービスで調査、分析、およびフィルタリングされ、要求が許可されるとユーザにトラフィックがルーティングされます。要求が許可されない場合 (禁止されている URL カテゴリへの要求など)、要求がブロックされてユーザに通知されます。

MSP は、Remote Manager を使用して複数の顧客のライセンス管理や請求処理を実施できます。その際、LMP (Licensing Management Portal) というトレンドマイクロサービスを利用します。ライセンスの変更や更新はバックエンドで同期され、Cloud Edge Cloud Console および Remote Manager に表示されます。

主な機能

次の表に、Cloud Edge Cloud Console の主な機能を示します。Cloud Edge Cloud Console では、Cloud Edge アプライアンスやクラウドスキャンサービスに適用するセキュリティポリシーの設定や管理を行うことができます。

表 1-2. Cloud Edge Cloud Console の機能

機能	説明
ゲートウェイ管理	複数の Cloud Edge ゲートウェイを 1 つの Cloud Console でまとめて管理できます。 ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイに対してイントラネットセキュリティモードを管理します。 Cloud Edge ワイヤレスゲートウェイに対してワイヤレスネットワークアクセス管理とワイヤレスクライアント接続の管理を行います (本機能は日本語版では使用できません)。 Cloud Edge Cloud Console を使用して、HA グループの作成と管理を行います。2 台の登録済みゲートウェイから HA グループを作成することで、高可用性アクセスを提供できます。一方のゲートウェイが停止した場合、もう一方のゲートウェイが引き継ぎ、ネットワークトラフィックの継続を確保します。
マルチレイヤ型の保護	Cloud Edge では、ユーザやユーザグループ単位でのネットワークアクセスを、ポートとアプリケーションを識別し、ネットワークへの脅威の侵入を防止するための設定を行うことができます。このような多層構造の識別に基づくセキュリティポリシーを適用することで、従来のセキュリティソリューションをバイパスする可能性がある、巧妙化した新たな脅威に対抗できます。
ポリシーの管理と配信	任意の数の管理対象ゲートウェイにポリシーを配信できます。ポリシー管理には次のオプションがあります。 • 特定のゲートウェイ、インタフェースグループ、ユーザ/ユーザグループ、IP アドレス、FQDN、ジオロケーション、サービス、アプリケーショングループ、URL カテゴリグループ、スケジュール、およびセキュリティプロファイルのポリシーを作成する • 侵入防止システム (IPS)、不正プログラム対策、メールセキュリティ対策、Web レピュテーションサービス、HTTPS 検査、DoS 攻撃対策、エンドポイント識別など、高度なポリシー機能用のセキュリティプロファイルを作成する • 許可またはブロックする URL を設定する (ポリシールールよりも優先される) • ポリシーのイベントが発生したときに通知を送信する

機能	説明
プラグアンドプレイ方式の配信	Cloud Edge ゲートウェイは未開封の状態で顧客の元に送ることができます。顧客は、開封後に付属のドキュメントの指示に従って設定するだけです。ゲートウェイを手動で登録してオンラインにすると、カスタムのセキュリティポリシー設定を受信します。
インテリジェントなダッシュボード	ネットワーク内の 1 つまたは複数のゲートウェイで発生している活動を確認できます。ダッシュボードのコアコンポーネントであるウィジェットでは、情報がグラフの形式で視覚的に示され、脅威の追跡情報を確認したり、蓄積されたログデータと関連付けて確認したりできます。
ログ分析とレポート	トラフィックの帯域幅の消費、脅威の検出、Web 2.0 アプリケーションの使用状況、Web 閲覧活動、およびポリシー施行に関するログやイベントデータをまとめて確認および分析します。 ログクエリフィルタをお気に入りログとして保存して後で参照したり、さらに詳しく調査するためにカスタムレポートを生成したりできます。 ポリシールールの使用状況データを表示します (すべて Cloud Edge 6.0 以降のゲートウェイを実行している場合のみ使用可能)。
通信品質	帯域幅を制御し、通信の制御、不要なトラフィックのブロック、重要なトラフィックやサービスへの適切な帯域幅割り当てを行うことで、ネットワークの輻輳を緩和します。
URL フィルタ	Web ドメインアクセスを拒否または許可する URL フィルタポリシーを設定できます。 「アダルト」や「ギャンブル」などの特定の URL カテゴリに分類されるトラフィックを検索してフィルタリングするようにポリシーを設定できます。「」ユーザがある URL へのアクセスを要求すると、まずその URL のカテゴリを検索し、次にポリシー設定に基づいてアクセスを制御します。
アプリケーション制御	特定のクライアントを使用するアプリケーション (Skype、BitTorrent、P2P) や、Web サイト内で Web2.0 テクノロジを使用するアプリケーション (ソーシャルネットワーキング、Web メール、ストリーミングメディアサイト) など、3400 を超える種類のアプリケーションを管理できます。

機能	説明
セキュリティプロファイル	セキュリティプロファイルを対象とする高度なポリシーを設定します。 • 侵入防止システム (IPS) • 不正プログラム対策 • メールセキュリティ対策 • Web レピュテーション • HTTPS 復号 • Dos 対策 • エンドポイントの識別
ユーザ管理	ゲートウェイ間でユーザ情報を同期します。
ユーザ VPN	ユーザの仮想プライベートネットワーク (VPN) は、VPN のリモートユーザ向け拡張機能です。ダイヤルアップ接続 (ブロードバンド接続を含む)、LAN 接続、モバイル接続のいずれにおいても、IPv4 VPN トンネルを介してネットワークやサーバと機密情報を安全にやり取りできます。 VPN がサポートされていない Cloud Edge ゲートウェイモデルでは利用できません。
サイト間 VPN	サイト間仮想プライベートネットワーク (VPN) を使用すると、複数のオフィス間で、インターネットなどのパブリックネットワークを介した安全な IPv4 接続を確立できます。 VPN がサポートされていない Cloud Edge ゲートウェイモデルでは利用できません。
ゲートウェイのシステムステータスとイベント/ログ	ゲートウェイごとに、ゲートウェイのシステムステータスに関する情報を確認できます。また、ネットワークやシステムに関するイベント/ログ、VPN イベント (使用可能な場合)、およびポリシー施行ログを確認できます。 VPN がサポートされていない Cloud Edge ゲートウェイモデルでは、VPN イベントは表示されません。
ゲートウェイのトラブルシューティングツール	Ping、Traceroute、および ARP を使用して、ゲートウェイの IPv4 ネットワーク接続の問題に関するトラブルシューティングを行えます。

機能	説明
ウイルスバスター ビジネスセキュリティサービスとの統合	Cloud Edge の VBBSS エンドポイント保護をウイルスバスター ビジネスセキュリティサービスと統合することで、ウイルスバスター ビジネスセキュリティサービスの古いビジネスセキュリティエージェントパターンがインストールされているウイルスバスター ビジネスセキュリティサービスエンドポイントやウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントがインストールされていないエンドポイントについてのコンプライアンスチェックを実行できます。Cloud Edge では、コンプライアンスに違反しているエンドポイントのネットワークアクセスコントロールを提供できます。
不審エンドポイントのネットワークアクセスコントロール	Cloud Edge は、エンドポイントのコンプライアンスチェックを行うことでセキュリティサービスを提供します。このコンプライアンスチェックでは、設定したしきい値を超える C&C コールバックが検出されたかどうかを確認します。Cloud Edge では、しきい値を超えているエンドポイントのネットワークアクセスコントロールを提供できます。

ハイブリッドセキュリティ

Cloud Edge が提供するセキュリティ機能は、Cloud Edge アプライアンスがオンプレミスで提供するものと、クラウド上で提供するものの 2 種類があります。ポリシーに応じ、Cloud Edge がトラフィックをクラウドに転送することで、このような制御が行われます。同様に、管理機能についてもオンプレミスについては Cloud Edge On-Premises Console、クラウドについては Cloud Edge Cloud Console で提供されます。次の表に、それぞれの機能がオンプレミスとクラウドのどちらに実装されているかを示します。

表 1-3. Cloud Edge のセキュリティ実装

機能	オンプレミス	クラウド
高可用性 (HA) グループ		●
高度なファイアウォール保護	●	
アプリケーション制御	●	
エンドポイント管理	●	●

機能	オンプレミス	クラウド
ゲートウェイ管理		●
侵入防止システム (IPS)	●	
Licensing Management Platform の統合		●
Remote Manager の統合		●
スパム検索	●	●
スイッチ: ソフトウェアスイッチ	●	
スイッチ: ハードウェアスイッチチップセット	●	●
URL フィルタ	●	
仮想プライベートネットワーク	●	
ウイルス/不正プログラム検索	●	●
仮想アナライザによる高度な不正プログラム対策		●
機械学習型検索による高度な不正プログラム対策		●
Web レピュテーションサービス	●	●
ワイヤレスネットワーク	●	●

オンプレミスの機能

次の表に、オンプレミスで利用できる Cloud Edge の機能を示します。

オンプレミスの機能に関連する IPv6 のサポートの詳細については、21 ページの「IPv6 のサポート」を参照してください。

表 1-4. Cloud Edge オンプレミスの機能

機能	説明
高可用性 (HA) グループ	2 台の登録済みゲートウェイを HA グループとして設定することで、高可用性アクセスを提供できます。一方のゲートウェイが停止した場合、もう一方のゲートウェイが引き継ぐため、ネットワークトラフィックが停止することはありません。HA グループにより、ネットワークトラフィックの効率を向上することもできます。
高度なファイアウォール	攻撃のみをブロックし、適切なアプリケーショントラフィックだけを通過させる次世代のファイアウォール機能を提供します。
ウイルス対策	アプリケーションコンテンツ検索に基づいて複数のセキュリティコンポーネントやウイルス対策を利用することで、遅延を少なくし、ユーザの操作性を高めながら、保護を強化できます。
スパム検索と不正プログラム検索	メールセキュリティ対策がローカル検索に設定されている場合は、スパムメール対策と不正プログラム対策がローカルに管理および実施されます。 注意 メールセキュリティ対策の初期設定はクラウド検索ですが、一定の状況 (ネットワークに問題がある場合など) で自動的に設定をローカル検索に切り替えることができます。
E-mail レピュテーションサービス	Trend Micro Email Reputation Services (ERS) を使用して、メール送信者のレピュテーションに基づいてメールメッセージを検出し、ブロックできます。
IPS	活動中の脅威、セキュリティホール、バックドアプログラムのほか、サービス拒否 (DoS) 攻撃や分散サービス拒否 (DDoS) 攻撃など、さまざまな攻撃を識別してデバイスへの侵入を防止できます。 侵入防止システム (IPS) をファイアウォールのセキュリティポリシーと併用することで、ファイアウォールで許可されたトラフィックをさらに調べて望ましくない脅威が含まれていないかを確認できるため、セキュリティを強化することができます。
アプリケーション制御	人気の高いインターネットアプリケーションを検出し、それらのアプリケーションへのアクセスをポリシーで制御できます。

機能	説明
ネットワーク設定	検出されたネットワークインタフェースを表示および編集したり、L2 や L3 の物理ポートの設定を変更したりできます。L3 ポートに対しては次の IPv4 設定がサポートされます。 • DHCP (Dynamic Host Configuration Protocol) • IP アドレスとネットマスクによる静的ルート設定 • PPPoE (Point-to-point Protocol over Ethernet)
ブリッジ	2 つのインタフェースを透過的にブリッジしてネットワークトラフィックをフィルタリングすることで、既存のネットワーク環境への影響を最小限に抑えてエンドポイントとサーバを保護できます。STP (スパニングツリープロトコル) により、ブリッジされた Ethernet ローカルエリアネットワークでループがないトポロジが形成されます。 配信モードがブリッジモードに設定されている場合は、IPv6 機能がサポートされます。
ソフトウェアスイッチ	Cloud Edge ゲートウェイは、ソフトウェアスイッチ (ブリッジモードのバリエーション) として機能するように設定できます。これにより、小規模なビジネス環境で別途スイッチを設置する必要がなくなります。Cloud Edge はスイッチとして機能しながらも、設定されたポリシーに従ってセキュリティ検索を実行します。 配信モードがソフトウェアスイッチに設定されている場合は、IPv6 機能がサポートされます。

機能	説明
ハードウェアスイッチチップセット	ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイは、セキュリティゲートウェイとハードウェアスイッチの両方の役割を果たします。このゲートウェイはブリッジモードで、エンドポイントに直接接続できる 7 つの LAN スイッチポートを提供します。これにより、多くのビジネス環境で別途スイッチを設置する必要がなくなります。 また、必要に応じてルーティングモードで配信することもできます。ルーティングモードで配信する場合は、内部ネットワーク用に 8 つの LAN ポートを使用できます。 ルーティングモードで配信する場合も、ブリッジモードでハードウェアスイッチとして配信する場合も、ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイは設定されたポリシーに従ってセキュリティ検索を実行します。 配信モードがブリッジモードに設定されている場合は、IPv6 機能がサポートされます。
ルーティング	配信モードがルーティングモードに設定されている場合に、Cloud Edge ゲートウェイがルータとして機能するように設定します。ゲートウェイはネットワーク上で認識され、レイヤ 3 ルーティングデバイスとして機能し、セキュリティ検索機能と制御機能を提供します。IPv4 静的ルートはすべて Cloud Edge ゲートウェイによりローカルで管理されます。 配信モードがルーティングモードに設定されている場合、IPv6 機能はサポートされません。
帯域幅制御	ネットワークの輻輳を緩和するため、通信の制御、不要なトラフィックのブロック、重要なトラフィックやサービスへの適切な帯域幅割り当ての設定を行うことができます。
URL フィルタ	ポリシーごとに一意の URL フィルタを作成および設定できます。URL フィルタは、WRS とともに搭載された、複合型脅威に対するマルチレイヤ型保護ソリューションです。
NAT	NAT (Network Address Translation) ポリシーを設定して、送信元または送信先の IPv4 アドレスとポートをパブリックとプライベートの間で変換するかどうかを指定できます。
サービス	次のサービスを設定できます。 • DHCP (Dynamic Host Configuration Protocol) サーバ

機能	説明
VPN	IPv4 VPN を設定します。 • ユーザ VPN L2TP (Layer 2 Tunneling Protocol) を使用した仮想プライベートネットワーク (VPN)、または SSL VPN (Secure Socket Layer 仮想プライベートネットワーク) を設定できます。 iOS および Android モバイルデバイスのユーザが、組み込みの IPsec VPN クライアントを使用して組織環境に簡単かつ安全に接続できます。モバイルデバイス用にエージェントをインストールする必要はありません。 • サイト間 VPN IKE (Internet Key Exchange) プロトコルと IPsec (IP Security) プロトコルを使用して、暗号化された L3 トンネルを作成できます。 ピアツーピアの単一の VPN トンネル、1 台の中央のハブデバイスと最大 4 台のスポークデバイスで構成されるスター VPN トポロジ、最大 5 つのデバイスで構成されるフルメッシュ VPN トポロジを作成できます。 VPN がサポートされていない Cloud Edge ゲートウェイモデルでは、VPN を設定することはできません。
ログ	監査ログ、システムイベント、および VPN ログ (使用可能な場合) を確認および分析できます。
ゲートウェイのシステムステータスとイベント/ログ	ゲートウェイごとに、ゲートウェイのシステムステータスに関する情報を確認できます。また、ネットワークイベント、システムイベント、VPN イベント (使用可能な場合)、およびポリシー施行ログに関する情報を確認できます。 VPN がサポートされていない Cloud Edge ゲートウェイモデルでは、VPN に関する情報を確認することはできません。
ゲートウェイのトラブルシューティングツール	Ping、Traceroute、および ARP を使用して、ゲートウェイの IPv4 ネットワーク接続の問題に関するトラブルシューティングを行えます。

機能	説明
ウイルスバスター ビジネスセキュリティサービスとの統合	Cloud Edge の VBBSS エンドポイント保護をウイルスバスター ビジネスセキュリティサービスと統合することで、ウイルスバスター ビジネスセキュリティサービスの古いビジネスセキュリティエージェントパターンがインストールされているウイルスバスター ビジネスセキュリティサービスエンドポイントやウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントがインストールされていないエンドポイントについてのコンプライアンスチェックを実行できます。Cloud Edge では、コンプライアンスに違反しているエンドポイントのネットワークアクセスコントロールを提供できます。
不審エンドポイントのネットワークアクセスコントロール	Cloud Edge は、エンドポイントのコンプライアンスチェックを行うことでセキュリティサービスを提供します。このコンプライアンスチェックでは、設定したしきい値を超える C&C コールバックが検出されたかどうかを確認します。Cloud Edge では、しきい値を超えているエンドポイントのネットワークアクセスコントロールを提供できます。
ワイヤレスネットワーク	ワイヤレスネットワーク機能を備えた Cloud Edge ゲートウェイでは、MAC アドレスフィルタを使ってアクセスを制御しながら、メインネットワークとゲストネットワークへのワイヤレスネットワークアクセスを設定できます。Cloud Edge は、メインとゲスト両方のネットワークに対して包括的なセキュリティサービスを提供します。 DHCP サービス、帯域幅制御、NAT、VPN アクセス、不審エンドポイントのネットワークアクセス管理など、他のネットワークサービスもワイヤレスネットワークで設定できます。

クラウドの機能

次の表に、クラウドで利用できる Cloud Edge の機能を示します。

表 1-5. Cloud Edge のクラウドの機能

機能	説明
ゲートウェイ管理	複数の Cloud Edge On-Premises ゲートウェイを 1 つの Cloud Console で集中管理できます。 Cloud Edge Cloud Console を使用して 2 台の登録済みゲートウェイを HA グループとして設定することで、高可用性アクセスを提供できます。設定の変更、HA グループの有効化または無効化、強制テイクオーバー、および HA グループの削除を含む、既存の HA グループの管理を行います。
Web レピュテーション	トレンドマイクロの Web レピュテーションテクノロジを使用して、不正な Web サイトに対する保護レベルを制御できます。
不正プログラムおよびウイルス検索	アプリケーションコンテンツ検索に基づいて複数のセキュリティコンポーネントやウイルス対策を利用することで、遅延を少なくし、ユーザの操作性を高めながら、保護を強化できます。 クラウドベースの仮想アナライザと機械学習型検索を使用して、メールベースの不正プログラムから保護します。
スパム検索	クラウドベースのスパム検索を使用して、メールの内容に基づいてスパムメールメッセージを検出し、ブロックまたはタグ付けできます。
レポート	検出された不正プログラムや不正コード、ブロックされたファイル、アクセスされた URL に関するレポートを生成できます。この情報を使用して、プログラムの設定を最適化したり、セキュリティポリシーを微調整したりできます。
ログ分析	トラフィックの帯域幅の消費、脅威の検出、Web 2.0 アプリケーションの使用状況、Web 閲覧活動、およびポリシー施行に関するログやイベントデータをまとめて確認および分析します。 すべて Cloud Edge 6.0 以降のゲートウェイを実行している場合、ポリシールールの使用状況データが表示されます。 ログクエリフィルタをお気に入りログとして保存して後で参照したり、さらに詳しく調査するためにカスタムレポートを生成したりできます。

セキュリティプロファイルとは、各種のセキュリティ設定を 1 つにまとめ、設定適用を簡便にするための機能です。侵入防止システム (IPS)、不正プログラム対策のセキュリティ、メールセキュリティ、Web レピュテーション、DoS 攻撃、およびエンドポイント識別に対する高度なポリシー管理を設定できま

す。次の表に、セキュリティプロファイルに設定できる各プロファイルを示します。

セキュリティプロファイルに関連する IPv6 のサポートの詳細については、21 ページの「IPv6 のサポート」を参照してください。

表 1-6. Cloud Edge のセキュリティプロファイル

機能	説明
IPS プロファイル	各セキュリティプロファイルで、侵入防止プロファイルを指定して、バッファオーバーフローや不正なコード実行などのシステムの脆弱性を利用する攻撃に対する保護のレベルを指定できます。初期設定のプロファイルを使用した場合、すべての既知の脅威からクライアントとサーバが保護されます。
不正プログラム対策プロファイル	Web ベースの不正プログラム対策の処理 (初期設定の推奨処理または独自に設定した処理) を選択できます。また、許可またはブロックする URL のファイル拡張子を指定することもできます。 不正プログラム検索を強化するには、スマートスキャンを有効にします。スマートスキャンは、次世代のクラウドベース保護ソリューションです。このソリューションは、スマートスキャンサーバを活用し、クラウド上に格納された署名によって脅威を検索する高度な検索アーキテクチャを提供します。

機能	説明
メールセキュリティ対策プロファイル	メールセキュリティ対策の初期設定の推奨処理を実行するか、組織に合わせて処理設定をカスタマイズします。メールセキュリティ対策プロファイルは、IPv4 メールトラフィックを検索して処理を実行します。 不正プログラム対策 不正プログラム検索を有効にし、不正プログラムが添付されたメールの件名および本文に追加するタグを定義します。 仮想アナライザと機械学習型検索を有効にして、クラウドベースの高度な検索およびメールベースの不正プログラムからの保護を設定できます。 有効にすると、ファイルに不審な特性があり、かつシグネチャベースの検索では未知の脅威を検出できない場合に、Cloud Edge から仮想アナライザと機械学習型検索に不審な添付ファイルが送信されます。 暗号化された添付ファイルを含むメールにタグ付けし、メールの本文で使用するタグを定義します。 スパムメール対策 スパムメール対策による検索を有効にし、必要に応じて Cloud Edge を有効にして、Trend Micro ERS (Email Reputation Services) を使用し、送信元アドレスのレピュテーションに基づいてスパムメールかどうかを判定します。スパムメールの「セキュリティ」レベル (検出率) を設定します。 BEC (ビジネスメール詐欺) 対策を有効にします。BEC は、不正な送金を行う目的で、企業を標的に、ソーシャルエンジニアリングを通じて正規のビジネスメールアカウントを不正に使用します。 メールがスパムメールおよび BEC であると特定された場合の処理を定義し、タグを追加する処理の場合、スパムメールまたは BEC メールメッセージの件名および本文に追加するタグを定義します。 コンテンツフィルタと例外リスト コンテンツフィルタを設定するか、例外リストを作成し、送信元または添付ファイルの種類 (クラウド検索の場合は実際のファイルタイプ、ローカル検索の場合はファイル拡張子) に基づいてメールをブロックまたは許可できます。 詳細設定

機能	説明
	有効にするメールプロトコルを設定し、カスタム SSL ポート、および SMTP サーバの設定を実行できます。
Web レピュテーションプロファイル	各セキュリティポリシーで、サイトをブロックする Web レピュテーションのセキュリティレベルを選択できます。 Web レピュテーションテクノロジでは、レピュテーションスコアを URL に割り当てます。Cloud Edge は、URL にアクセスするたびに Web レピュテーションにレピュテーションスコアを問い合わせ、ユーザ定義のセキュリティレベルとスコアとの比較に基づき、必要な処理を実行します。
HTTPS 復号プロファイル	HTTPS 検査から除外する URL カテゴリおよび送信元 IPv4 アドレスを選択できます。 SSL (Secure Socket Layer) と TLS (Transport Layer Security) は、今日のネットワーク通信で広く採用されている暗号化プロトコルです。HTTPS 接続は、SSL/TLS の暗号化と署名によってセキュリティが確保されます。暗号化された HTTPS 接続であっても、暗号化されていない HTTP 接続と同様のリスクがあるため、Cloud Edge は、すべての IPv4 トラフィックについて潜在的なリスクや脅威を検査します。 検索する HTTPS ポートを最大 5 つ指定し、HTTPS 復号化プロファイルをカスタマイズできます。
DoS 対策プロファイル	各セキュリティポリシーで、サービス拒否 (DoS) 攻撃に対するフラッド攻撃対策および除外するアドレスを指定できます。 サービス拒否攻撃や分散サービス拒否 (DDoS) 攻撃は、インターネットに接続されたホストへのサービスを一時的または無期限に妨害または遮断することを目的とした、ユーザがコンピュータやネットワークのリソースを利用できない状態にする攻撃です。 典型的なものとしては、標的のコンピュータに外部から大量の通信要求を発行し、正規のトラフィックに応答するリソースを使い切らせる方法があります。

機能	説明
エンドポイント識別プロファイル	各セキュリティポリシーで、キャプティブポータルに対する IPv4 アドレスオブジェクトを指定して、どの IPv4 アドレスがどのユーザに割り当てられているかを識別できます。エンドポイント識別は、ポリシーマッチング用の IPv4 アドレスとユーザのマッピングキャッシュを使用したユーザの識別方法を提供します。 初期設定では、エンドポイント識別で IP アドレスを自動的に識別することはできません。どの IPv4 アドレスオブジェクトをエンドポイント識別に使用するかを定義する必要があります。選択した IPv4 アドレスオブジェクトで定義されている範囲にない送信元 IPv4 アドレスについては、エンドポイント識別は実行できません。 エンドポイント識別に IPv6 アドレスは使用できません。

IPv6 のサポート

Cloud Edge では、配信モードがブリッジモードまたはソフトウェアスイッチに設定されている場合に、IPv6 がサポートされます。

重要

IPv6 はルーティングモードではサポートされません。

次の表に、ブリッジモードおよびソフトウェアスイッチで IPv6 がサポートされる機能を示します。この表に示されている機能に加え、Cloud Edge では、Cloud Edge ゲートウェイを経由して、インターネットへの接続を提供する IPv6 ルータなどにトラフィックを IPv6 で転送することができます。

表 1-7. ブリッジモードおよびソフトウェアスイッチでの Cloud Edge による IPv6 のサポート

機能	カテゴリ	IPv6 のサポート	IPv6 サポートなし
ダッシュボード		●	
	Cloud Edge では、ダッシュボードでの IPv6 アドレスの表示がサポートされています。		
ゲートウェイ – 登録			●

機能	カテゴリ	IPv6 のサポート	IPv6 サポートなし
	Cloud Edge は IPv4 を使用して Cloud Edge Cloud Console に接続します。		
ゲートウェイ — ネットワーク	インタフェース		●
	管理アクセス		●
	DHCP		●
	動的 DNS		●
	ルーティングテーブル		●
	静的ルート		●
	NAT		●
	Cloud Edge ゲートウェイのネットワーク設定については、どのモードでも IPv6 はサポートされません。ただし、Cloud Edge では、IPv6 や DHCPv6 の DNS などの要求をエンドポイントに転送することはできます。		
ゲートウェイ — 帯域幅制御		●	
ゲートウェイ — VPN	ユーザ VPN		●
	サイト間 VPN		●
ゲートウェイ — エンドユーザ管理 — 一般設定			●
	ユーザアカウントに依存する機能では、IPv6 はサポートされません。		
ゲートウェイ — アップデート			●
	Cloud Edge は IPv4 を使用してアップデートサービスに接続します。		
ゲートウェイ — ネットワークアクセスコントロール			●

機能	カテゴリ	IPv6 のサポート	IPv6 サポートなし
	Cloud Edge では、IPv6 エンドポイントに対するネットワークアクセスコントロールはサポートされません (エンドポイントに IPv4 アドレスと IPv6 アドレスの両方が割り当てられていてもサポートされません)。		
ポリシー – ポリシー	送信元 IP	●	
	送信元 FQDN	●	
	ユーザ/ユーザグループ		●
	送信先 IP	●	
	送信先 FQDN	●	
	トラフィック – アプリケーションと URL カテゴリ	●	
	ユーザやユーザグループに基づくポリシーでは、IPv6 はサポートされません。このようなポリシーは IPv6 トラフィックには適用されません。		
ポリシー – オブジェクト	IP アドレス/FQDN	●	
	MAC アドレス	●	
	サービス	●	
	アプリケーションとアプリケーショングループ	●	
	URL カテゴリ	●	
	Cloud Edge では ICMPv6 がサポートされます。		
ポリシー – 許可/ブロックリスト	IPv6 アドレス	●	
	FQDN	●	
	URL	●	

機能	カテゴリ	IPv6 のサポート	IPv6 サポートなし
ポリシー – セキュリティプロファイル	IPS	●	
	不正プログラム対策	●	
	メールセキュリティ対策 – ローカル検索		●
	メールセキュリティ対策 – クラウド検索		●
	DoS 対策	●	
	HTTPS		●
	Web レピュテーション	●	
	エンドポイントの識別		●
	メールのローカル検索とクラウド検索では、IPv6 はサポートされません。IPv6 メールトラフィックは、検索されずに Cloud Edge ゲートウェイを通過します。 HTTPS IPv6 トラフィックは、検索されずに Cloud Edge ゲートウェイを通過します。 Cloud Edge では、IPv6 トラフィックに対するエンドポイント識別は実行されません。キャプティブポータルが有効になっている場合、キャプティブポータルウィンドウは開きますが、IPv6 トラフィックは Cloud Edge ゲートウェイを通過します。		
ポリシー – Web レピュテーションサービス		●	
ポリシー – ユーザ通知		●	
	Cloud Edge では、IPv6 クライアントへのユーザ通知の表示がサポートされています。		
分析とレポート – レポート		●	

機能	カテゴリ	IPv6 のサポート	IPv6 サポートなし
	Cloud Edge では、レポートでの IPv6 アドレスの表示がサポートされています。		
分析とレポート - ログ分析	アプリケーション帯域幅	●	
	ポリシー施行	●	
	インターネットアクセス	●	
	インターネットセキュリティ	●	
	Cloud Edge では、ログでの IPv6 アドレスの表示がサポートされています。		
管理 — ユーザとアカウント			●
	ユーザアカウントに依存する機能では、IPv6 はサポートされません。		
管理 — ユーザ認証			●
	ユーザアカウントに依存する機能では、IPv6 はサポートされません。		
管理 — 監査ログ		●	
管理 — 管理者アラート	ゲートウェイステータスの変更	●	
	メールセキュリティステータスの変更	●	
	C&C コールバック	●	
管理 — 予約アップデート			●
	Cloud Edge は IPv4 を使用してアップデートサービスに接続します。		
管理 — メンテナンス			●

機能	カテゴリ	IPv6 のサポート	IPv6 サポートなし
	Cloud Edge は IPv4 を使用して外部サーバに接続します。		
管理 — 証明書管理			●

第 2 章

Cloud Edge の配信のベストプラクティス

本章では、パートナー様向けに、Cloud Edge のセキュリティソリューションを配信および管理する際の一連のベストプラクティスの開発を支援します。

Trend Micro Cloud Edge は、クラウドを活用する UTM (統合脅威管理) ゲートウェイデバイスで、次世代のオンプレミスファイアウォールの利点とクラウドで提供される Security as a Service の利便性を兼ね備えています。Cloud Edge は、統合された機能により、ネットワークパケットを検査してフィルタリングし、巧妙化した脅威をゲートウェイで食い止めます。

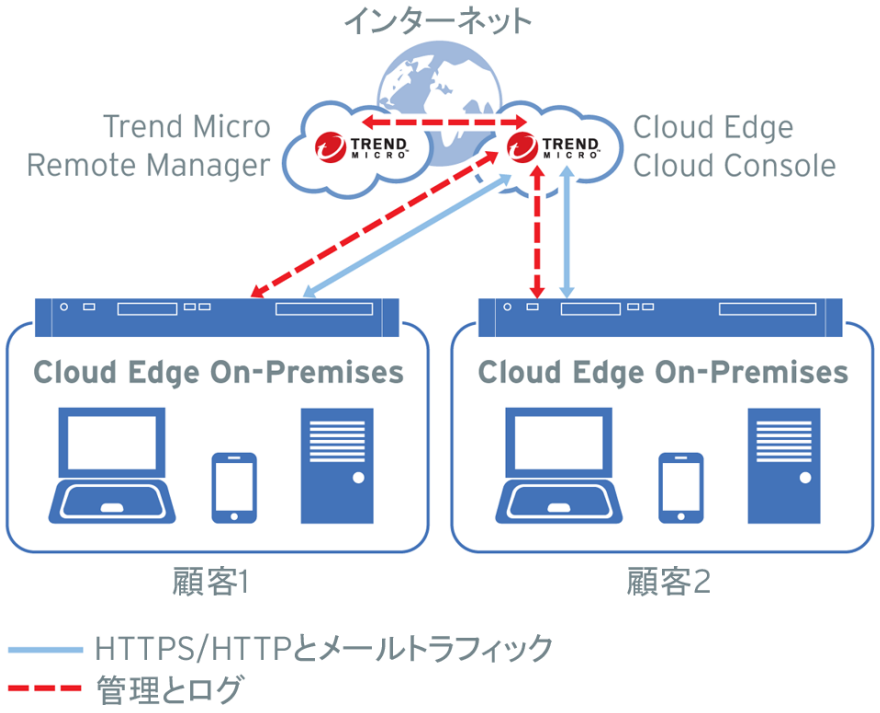
本章では、配信の簡易化、セキュリティとパフォーマンスの強化、監視とレポートのためのベストプラクティスを取り上げます。Cloud Edge のゲートウェイを配置し、定期的に操作を管理する管理者向けの内容です。本管理者ガイドおよび以下を含むその他のユーザマニュアルの情報全体に代わるものではありません。

- Cloud Edge Cloud Console オンラインヘルプ
- Readme

配信のベストプラクティス

MSP によるライセンスのプロビジョニング

MSP パートナーは、この『管理者ガイド』に従って、顧客に Cloud Edge ゲートウェイの適切なライセンス設定や配信を行うことができます。簡単にまとめると、Trend Micro Remote Manager から、すべての関連ツールを起動できます。



サービスプランを作成する

Trend Micro Licensing Management Platform (LMP) にアクセスして、Cloud Edge のサービスプランを作成します。

手順

1. 次のコンポーネントが含まれる可能性のある、Cloud Edge サービスプランを作成します。
    a. Cloud Edge — アプライアンスのファームウェアに必要なライセンス
    b. クラウドサンドボックス — サンドボックスエミュレーションのためのライセンス
    c. クラウドログサービス — サードパーティ製ログ管理システムにログを転送するためのライセンス
2. ベストプラクティスとして、次のことに注意してください。
    - Cloud Edge はアプライアンスなので、バージョンタイプには [製品版] が推奨されます。
    - [データセンター] の場所には、物理的に最も近い場所を選択します。
    - [製品/サービスを管理する] では、[Remote Manager] のチェックボックスをオンにし、リモート管理を許可します。
    - [初期ライセンス期間] は、実際のマーケティング戦略に応じて、[1 か月] または [1 年] を選択できます。
    - 実際のマーケティング設定に基づき、ライセンスの [自動更新] を有効にします。

顧客を作成する

Licensing Management Platform (LMP) を使用して顧客を作成します。

手順

1. 次のような必要な情報を入力して、顧客を作成します。
    a. 会社
    b. 住所
    c. 都市
    d. 都道府県と郵便番号

e. アカウント名

f. 担当者名とメールアドレス

2. ベストプラクティスとして、次のことに注意してください。

   - [アカウント作成メールを送信する] を、顧客を [作成した直後] に設定することをお勧めします。
   - 最後に、顧客の作成時には、サービスプランを簡単に割り当てられます。
   - 作成する顧客に配信する Cloud Edge ゲートウェイの数に基づいて、[ライセンスあたりのユニット数] を設定します。

新しいゲートウェイを追加する

サービスプランと顧客を作成したら、Cloud Edge Cloud Console に新しいゲートウェイを追加できます。

手順

1. Remote Manager で新しい顧客を選択し、Cloud Edge Cloud Console を起動します。

   ここで、シリアル番号を使用して Cloud Edge ゲートウェイを登録できます。

2. ベストプラクティスとして、次のことに注意してください。

   a. 新しいゲートウェイを顧客サイトに設置する前に、そのゲートウェイの登録をローカル環境でテストすることをお勧めします。

      こうすることで、問題が発生した場合に登録プロセスのトラブルシューティングを簡単に行えます。テストが完了したら、必要に応じてゲートウェイを登録解除できます。

   b. ネットワーク設定をローカルで設定できるように、ゲートウェイを工場出荷時の初期設定にリセットしてから、エンドユーザに出荷します。

オンプレミスでゲートウェイを配信する

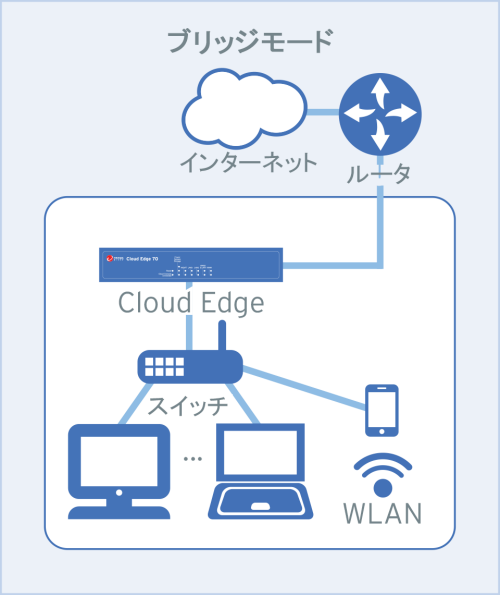
顧客サイトでゲートウェイを配置する場合は、クイックスタートガイドを参照してください。

配信モードの選択のための推奨事項

ブリッジモードとルーティングモードに関する以下の推奨事項に留意する必要があります。

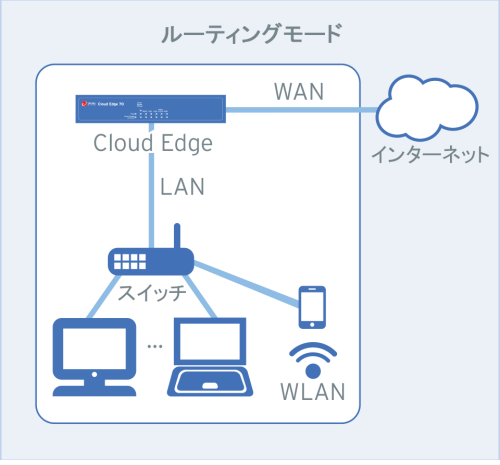
Cloud Edge ブリッジモード

可能なかぎり、ブリッジモードを選択してください。通常、ブリッジモードは、ルータの背後の、スイッチの手前にあるプライベートネットワークで使用します。これは、Cloud Edge ゲートウェイの背後にある物理スイッチを切り替えることで設定できます。ゲートウェイは、初期設定でブリッジに設定されています。ブリッジモードでは、既存のネットワークを変更することなく、Cloud Edge ゲートウェイを一時的に配信することが可能です。Cloud Edge により、強力な検索機能と脅威保護が追加されます。



Cloud Edge ルーティングモード

ルーティングモードは、Cloud Edge ゲートウェイをルータとして機能させるだけでなく、セキュリティと脅威保護を実現する場合に設定します。ゲートウェイはネットワーク上で認識され、レイヤ 3 ルーティングデバイスとして機能し、セキュリティ検索機能と制御機能を提供します。通常、ルーティングモードでは、ネットワーク上の既存のルータを Cloud Edge ゲートウェイに交換するか、このゲートウェイをルータとスイッチの間に配信します。ルータと Cloud Edge ゲートウェイの設定を変更する必要があります。



クイックセットアップを使用する

Cloud Edge ゲートウェイで基本設定を行うには、クイックセットアップを使用します。

手順

1. On-Premises Console から、[クイックセットアップ] ページに移動します。
2. ベストプラクティスとして、次のことに注意してください。
   - [アップリンク設定] — 可能な限り [DHCP] を選択します。これが不可能な場合は、ブリッジインタフェースで静的 IPv4 アドレスとサブ

ネットを割り当て、DNS を設定します。ルーティングモードで配信する場合は、PPPoE も利用できます。

- ゲートウェイが DNS にアクセスして Cloud Edge Cloud Console に接続できるかどうかを確認するには、[設定テストを開始] を使用する必要があります。
- [システム設定] ― ゲートウェイの時計を自動的に設定するには、[NTP サーバと同期する] が推奨されています。
- [シリアル番号] は、Cloud Edge On-Premise Console を使用して、[管理] > [デバイス管理] ページで確認できます。これは、Cloud Edge デバイスの底面にも記載されています。
- On-Premises Console を使用して、[ネットワーク] > [サービス] ページで、インタフェースの DHCP サービスを設定できます。

  LAN インタフェースの DHCP サービスを有効にすることをお勧めします。

  注意

  デバイスの登録後は、LAN2、LAN3、および MGMT の DHCP は、Cloud Edge Cloud Console のみで編集できます。

- ゲートウェイを登録するには、Cloud Edge Cloud Console にアクセスし、[ゲートウェイ] > [新しいゲートウェイの登録] の順に移動します。

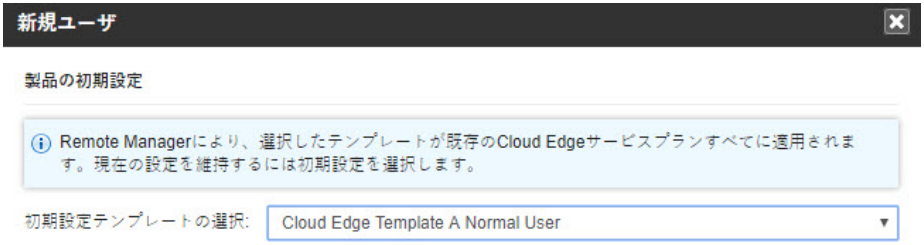
セキュリティ設定のベストプラクティス

登録が完了すると、Cloud Edge ゲートウェイを Cloud Edge Cloud Console からまとめて設定および管理できます。また、Trend Micro Remote Manager を使用して、複数のゲートウェイで共有される一般的なセキュリティ設定用のポリシールールとセキュリティプロファイルを設定して配信することもできます。その後、各ゲートウェイで独自のネットワーク設定を行うことができます。

Remote Manager のセキュリティテンプレート

Cloud Edge Cloud Console を使用して、セキュリティを設定できます。

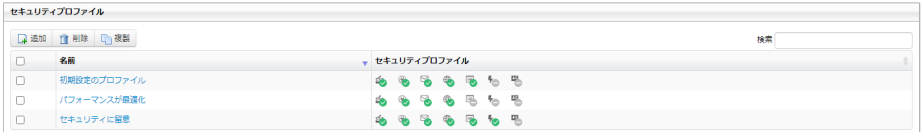
利便性のために、Remote Manager には初期設定テンプレートが用意されています。このテンプレートには、Cloud Edge Cloud Console を通じて設定できるのと同じセキュリティ設定が含まれています。Remote Manager では、これらのテンプレートをゲートウェイに割り当てて、顧客企業に関連付けられた初期設定にすることができます。そうすることで、ゲートウェイの配信時に顧客に同じ設定を使用させることが簡単になります。



セキュリティテンプレートを作成する

必要に応じて、追加のセキュリティテンプレートを作成できます。追加のセキュリティテンプレートを作成する際は、少なくとも次の 3 つのシナリオを考慮してください。

- Cloud Edge テンプレート A — 通常のユーザ (初期設定のテンプレート)
- Cloud Edge テンプレート B — セキュリティに留意するユーザ
- Cloud Edge テンプレート C — パフォーマンスが最適化されたユーザ



手順

1. 追加のセキュリティテンプレートを作成します。
2. 初期設定のテンプレートページの [ゲートウェイ] または Cloud Edge Cloud Console から、必要なセキュリティプロファイルを割り当てます。

通常のユーザ用のセキュリティテンプレートを作成する

セキュリティプロファイル A ― 通常のユーザ: 通常のユーザには、初期設定のセキュリティテンプレートを使用できます。すべての設定が初期値のままになっています。これにより、セキュリティとパフォーマンスのバランスが最善の状態になります。

手順

1. 次の手順を実行します。
   - Remote Manager から、[管理] > [初期設定テンプレートの構成] に移動します。
   - Cloud Edge Cloud Console から、[ポリシー] > [セキュリティプロファイル] > [初期設定のプロファイル] に移動します。
2. すべての値が初期値であることを確認します。

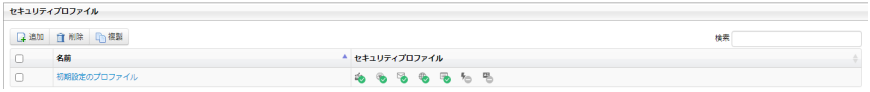
セキュリティに留意するユーザ用のテンプレートを作成する

ゲートウェイプロファイル B ― セキュリティに留意するユーザ: セキュリティが主要目的の場合に、このセキュリティテンプレートを使用できます。さらに詳しく検査を実施し、潜在的に有害なトラフィックをブロックすることで、セキュリティを強化します。

手順

1. 次の手順を実行します。
   - Remote Manager から、[管理] > [初期設定テンプレートの構成] に移動します。
   - Cloud EdgeCloud Console にログオンします。

2. [ポリシー] > [セキュリティプロファイル] > [初期設定のプロファイル] で、次の設定を有効にします。



   a. IPS:

      1. IPS の処理を [監視] から [ブロック] に変更します。
      2. [詳細設定] を有効にしてから、[ルールフィルタ] を使用して [検知対象となる最も低い重大度] を [4 – 高] に設定します。

      こうすることで、重大度が 4 – 高と 5 – 重大の IPS 検出がブロックされます。

   b. 不正プログラム対策: スマートスキャンを有効にするだけでなく、機械学習型検索を有効にすることもできます。

      こうすることで、クラウド内でスマートスキャンのリアルタイム署名サーバを活用できます。

   c. メールセキュリティ対策:

      1. [仮想アナライザの有効化]をオンにすると、クラウドサンドボックスを活用して不審ファイルを分析できます (ライセンスが必要です)。
      2. 機械学習型検索を有効にすると、未知の脅威の検出に AI を活用できます。また、[処理] を [監視] から [ブロック] または [タグの追加] に変更します。
      3. [添付ファイルが暗号化されているメールのタグ付け] をオンにして、添付ファイルを検索できなかったことをユーザに通知します。
      4. [スパムメール対策] で、メールレピュテーションを有効にし、ビジネスメール詐欺 (BEC) 対策を有効にします。

   d. Web レピュテーション: 感度レベルに [中] を選択します。

   e. HTTPS: HTTPS 検索をオンにし、除外設定リストですべての URL カテゴリすべて選択を解除します。

3. ゲートウェイプロファイルは忘れずに [保存] および [配信] してください。
4. セキュリティを強化するには、不要なアプリケーションまたは URL カテゴリをファイアウォールレベルでブロックするよう追加のポリシールールを定義できます。
   - Remote Manager のセキュリティテンプレート画面から、[ポリシー] > [ポリシールール] に移動します。
   - Cloud EdgeCloud Console から、[ポリシー] > [ポリシールール] に移動します。

   a. 「Block Internet Security URLs」という名前のポリシールールを追加します。

      [トラフィックタイプ] で、[アプリケーション/URL カテゴリを指定する] > [URL カテゴリ] > [インターネットセキュリティ] を選択し、[処理] を [ブロック] に設定します。

   b. 「Block Gaming Applications」という名前のポリシールールを追加します。

      [トラフィックタイプ] で、[アプリケーション/URL カテゴリを指定する] > [アプリケーション] > [ゲーム] を選択し、[処理] を [ブロック] に設定します。

   c. 新しく追加されたポリシールールは、「初期設定のポリシールール」の前に表示されます。
      結果は、次のようになります。

5. [ゲートウェイ] > <選択したゲートウェイ> でネットワークアクセス管理を設定します。
   - ウイルスバスター ビジネスセキュリティサービスエンドポイント保護: 顧客がウイルスバスター ビジネスセキュリティサービスも使用している場合に有効にします。

この機能により、コンプライアンスに準拠していないデバイスでのインターネットアクセスがブロックされます。

a. この機能は初期設定では無効であるため、オンにしてください。

b. 次の両方の条件で [ブロック] を選択します。

- インストールされていないクライアント
- 古いパターンファイルが使用されているクライアント

c. 保護リストに、ネットワークの IP アドレスプールを追加します。

これにより、ネットワーク上の未知のデバイスからのトラフィックがブロックされます。

d. 例外リストで、ウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントをインストールできないデバイスの IP アドレスを追加します。

e. [適用] をクリックします。

- 不審エンドポイント: 不審エンドポイントを設定することにより、設定したしきい値を超える C&C コールバックが検出されるエンドポイントに対してネットワークアクセス管理を提供できます。

a. この機能は初期設定では無効であるため、オンにしてください。

b. しきい値は初期設定を使用してください。つまり、1 時間の C&C コールバックイベントは 50 件です。

c. 処理を [ブロック] に設定します。

d. [適用] をクリックします。

パフォーマンスが最適化されたユーザ用のセキュリティテンプレートを作成する

セキュリティプロファイル C ― パフォーマンスが最適化されたユーザ: パフォーマンスが主要目的の場合に、このセキュリティテンプレートを使用できます。このプロファイルでは、さまざまな手法を使用して、指定されたユーザとグループのトラフィックを高速化します。

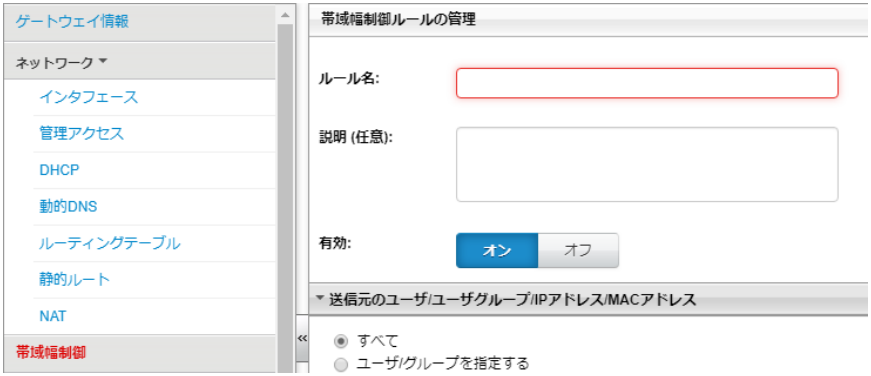
手順

1. 次の手順を実行します。
   - Remote Manager から、[管理] > [初期設定テンプレートの構成] に移動します。
   - Cloud Edge Cloud Console から、[ポリシー] > [ポリシールール] に移動します。
2. 次の設定を行います。
   - 「Bypass Trusted Sources」という名前のポリシールールを追加します。信頼できる IP アドレスまたはユーザ/グループの特定のポリシーの送信元を定義し、[処理] を [検索除外] に設定することで、これらを送信元とするトラフィックの脅威検索から除外されます。
   - または、ローカル間のネットワークトラフィックに対する検索除外ポリシールールを設定します。
   - HTTPS 復号 — [セキュリティプロファイル] で、HTTPS 復号検索を初期設定のオフのままにします。
3. ゲートウェイ特有の帯域幅制御ルールを設定することもできます。これは、重要なアプリケーションと重要でないアプリケーションの間でのトラフィックの優先度付けに使用できます。

   この機能は、Cloud Edge Cloud Console から設定する必要があります。

   選択したアプリケーショングループとネットワークサービスの両方またはいずれかに対して、特定の帯域幅制御ルールを作成します。速度重視の特定のアプリケーションに最小限の帯域幅を割り当てる場合は [保証帯域幅] を使用してルールを指定します。一方で、多くの帯域幅を必要とするアプリケーションが全帯域幅を独占して他のアプリケーションに支

障が出ることのないようにするには [最大帯域幅] を使用してルールを指定します。



その他のベストプラクティス

Cloud Edge ゲートウェイを配信する際は、以下の推奨事項に留意する必要があります。

Cloud Edge ゲートウェイを監視する

Cloud Edge のアクティビティを監視し、脅威分析を表示するには、ダッシュボードおよび分析とレポートを使用できます。

ダッシュボードを使用する

ダッシュボードを使用して Cloud Edge アクティビティを監視する際は、次の点を考慮してください。

Cloud Edge Cloud Console の [ダッシュボード] ページでは、[セキュリティステータス] と [トラフィックステータス] を一目で確認できます。

[分析とレポート] を使用する

Cloud Edge Cloud Console の [分析とレポート] ページで、事前定義されたログ統計を表示したり、独自のクエリを設定してお気に入りとして保存したりできます。

予約レポートも、実行間隔が毎日、毎週、または毎月になるように定義できます。メールによるレポート通知の送信は実際に時間を節約できる機能です。つまり、1 日の始まり、週の始まり、または管理用に月末のレポートを生成する必要があるときに、概要レポートが常に受信トレイに準備できています。

管理タスクを管理する

管理タスクを管理する際は、以下の推奨事項に留意する必要があります。

ユーザアカウントを作成する

Cloud Edge Cloud Console を使用してユーザアカウントを作成する際は、次の点を考慮してください。

手順

1. [管理] > [ユーザとアカウント] に移動します。
2. ログやレポートを表示するために Cloud Edge Cloud Console へのアクセスが必要でも、設定を変更する権限が不要なユーザには読み取り専用アカウントを作成します。

管理者アラートを管理する

管理者アラートを管理する際は、次の点を考慮してください。

手順

- 管理者アラートは、Cloud Edge Cloud Console を通じて設定します。
- [管理] > [管理者アラート] の順に移動し、[有効] を [オン] に設定します。
- 以下のアラートの種類を設定します。
  - [1 時間] に [50] 件のイベントが発生する [C&C コールバック] を選択する
  - [ゲートウェイステータスの変更] および [メールセキュリティステータスの変更] を選択する

- Remote Manager にログオンし、[管理] > [通知設定] の順に移動して、[イベント通知] 設定を調整可能な [警告しきい値] で微調整します。

予約アップデートを設定する

予約アップデートを設定する際は、次の点を考慮してください。

手順

- 通常、コンポーネント (パターンファイル/エンジン) のアップデート設定は [毎日] で十分です。ただし、不正プログラムの大規模感染が発生している間は、アップデート期間を [毎時] に変更することが望ましい場合があります。
- ファームウェアのアップデートは毎週実行することをお勧めします。初期設定を選択するか、業務時間外にアップデートが行われるように設定してください。

管理アクセスを設定する

管理アクセスを設定する際は、次の点を考慮してください。

手順

- Cloud Edge Cloud Console で、さまざまな種類の管理サービスを設定します。
- [ゲートウェイ] > <ゲートウェイの選択> > [管理アクセス] に移動し、On-Premises Console、Ping、SSH のいずれかを使用して Cloud Edge ゲートウェイへのアクセスが必要な IP 範囲または IP アドレスを指定します。

証明書管理

証明書を管理する際は、次の点を考慮してください。

手順

- Cloud Edge の証明書を管理するには、[管理] > [証明書管理] に移動します。

- 独自の証明書をインポートするか、Cloud Edge で SSL トラフィックの復号化に使用する証明書をエクスポートした後、そのエクスポート済み証明書をエンドユーザの信頼された証明書ストアにインストールします。

  これでエンドユーザは、HTTPS Web サイトにアクセスしても証明書の警告がブラウザに表示されなくなります。

第 3 章

スタートガイド

最初の作業

以下に、Remote Manager および Cloud Edge Cloud Console を使用するにあたって最初に実行する必要がある手順を示します。これらの手順が完了したら、Cloud Edge オンプレミスゲートウェイを顧客に提供します。顧客は各自のネットワーク環境に基づいてネットワーク設定を行う必要があります。

ヒント

Licensing Management Platform (LMP) を使用してサービスプランや顧客を管理できます。LMP には、直接アクセスする方法と Trend Micro Remote Manager からシングルサインオン (SSO) でアクセスする方法があります。より簡単に日常的な監視およびその他のリソースにアクセスできるため、LMP には Remote Manager からアクセスすることをお勧めします。

手順

1. LMP に、直接または Remote Manager からアクセスします。

   51 ページの「LMP にアクセスする」を参照してください。

2. サービスプランを作成します。

   52 ページの「サービスプランを作成する」を参照してください。

3. 会社を作成してサービスプランを割り当てます。

   53 ページの「会社を作成してサービスプランを割り当てる」を参照してください。

4. Remote Manager から Cloud Edge Cloud Console ウィジェットを表示します。

   64 ページの「毎日の監視」を参照してください。

   ログオンすると、最初に [スタートガイド] 画面が表示されます。この画面から、Cloud Edge Cloud Console の各機能にアクセスしたり、ゲートウェイを登録したりできます。

   73 ページの「[スタートガイド] 画面」を参照してください。

5. Cloud Edge Cloud Console で管理するすべてのゲートウェイを登録します。

325 ページの「ゲートウェイを登録する」を参照してください。

6. 必要に応じて、Cloud Edge Cloud Console にアクセスするためのユーザアカウントを作成します。

   267 ページの「Cloud Console 管理者アカウントを追加する」を参照してください。

7. 登録済みゲートウェイの管理を開始します。

   オンプレミスゲートウェイの配置後、ユーザは、選択されている配信モードに基づいて一部の配置設定を調整する必要があります。

配置作業

以下は、Cloud Edge ゲートウェイを設定するための必須の手順とオプションの手順です。

手順

1. Cloud Edge ゲートウェイを配信するモードを決めます。

   を参照してください。

2. 選択した配信モードに応じて配信スイッチを切り替えます。配信スイッチは Cloud Edge ゲートウェイの背面パネルにあります。

   注意

   配信スイッチを [ブリッジ] に切り替えるのは次の場合です。

   - 配信モードをソフトウェアスイッチに設定する場合
   - ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイで配信モードをブリッジモードに設定する場合

3. 配信前チェックリストの項目を準備します。

   を参照してください。

4. インストールと初期設定を実行します。

   を参照してください。

次の手順に従ってください。

a. 303 ページの「ハードウェアをセットアップする」 (ネットワークのケーブル接続を含む)。

b. 305 ページの「管理ポートから On-Premises Console にログオンする」

c. 305 ページの「初期設定を行う」 (ブリッジモード、ブリッジモード (スイッチチップセット使用)、ソフトウェアスイッチ、およびルーティングモードを含む)

   ワイヤレス機能を備えた Cloud Edge ゲートウェイの説明は、ルーティングモードの手順に含まれます。

d. 325 ページの「ゲートウェイを登録する」 (まだ登録していない場合)

e. 327 ページの「追加の設定を実行する」 (オプション)

第 4 章

Licensing Management Platform

Trend Micro Remote Manager、Trend Micro Licensing Management Portal (LMP) は販売代理店やマネージドサービスプロバイダ (MSP) などのパートナー向けのプラットフォームです。

Trend Micro Licensing Management Platform

Trend Micro Licensing Management Platform (LMP) を使用すると、サービスプロバイダなどのパートナーがトレンドマイクロ製品のライセンスを簡単に発行および管理することができます。ブランド設定機能を使用すれば、プラットフォームをカスタマイズすることもできます。

LMP では、さまざまなライセンス設定を組み合わせたサービスプランによって顧客のニーズに対応できます。顧客の企業アカウントを設定し、企業アカウントにサービスプランを割り当てることができます。

機能と利点

Licensing Management Platform を使用して製品の機能やサービスをカスタマイズできます。主な機能は次のとおりです。

表 4-1. 主な機能

機能	詳細
サービスプラン	サービスプランを設定し、顧客向けのサブスクリプション条件を作成します。
顧客のアカウント	顧客の企業アカウントを設定し、企業アカウントにサービスプランを追加します。
ライセンス情報	顧客が購入したライセンスを確認および管理します。
通知メールのカスタマイズ	顧客向けにさまざまな通知メールを設定します。
レジストレーションキーの作成	ライセンスを生成し、サービスプランに割り当てます。
ブランド設定	ビジネスの目的に合わせてブランド設定をカスタマイズします。プラットフォームフォームに表示される連絡先情報、ログオンページ、およびバナーが含まれます。

LMP を使用して顧客、サービスプラン、ライセンスを管理する方法の詳細については、次の Web ページにあるサポートドキュメントを参照してください。

http://docs.trendmicro.com/ja-jp/smb/trend-micro-licensing-management-platform.aspx

Licensing Management Platform にアクセスする

Licensing Management Platform (LMP) を使用してサービスプランや顧客を管理できます。LMP には、直接アクセスする方法と Trend Micro Remote Manager からシングルサインオン (SSO) でアクセスする方法があります。より簡単に日常的な監視およびその他のリソースにアクセスできるため、LMP には Remote Manager からアクセスすることをお勧めします。

手順

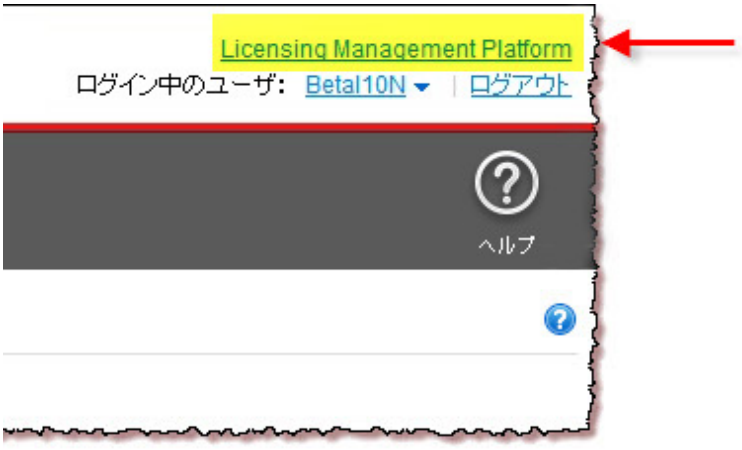
- LMP に直接アクセスします。

  LMP の URL はマネージドサービスプロバイダごとに異なり、LMP アカウントの作成後にトレンドマイクロからメールで通知されます。

- Remote Manager からシングルサインオンで LMP にアクセスします。

  a. Remote Manager にログオンします。

  b. 右上にある [Licensing Management Platform] をクリックします。



LMP ダッシュボードが表示されます。右上にある [Trend Micro Remote Manager] をクリックして Remote Manager に戻ります。

注意

LMP を使用して顧客、サービスプラン、ライセンスを管理する方法の詳細については、次の Web ページにあるサポートドキュメントを参照してください。

http://docs.trendmicro.com/ja-jp/smb/trend-micro-licensing-management-platform.aspx

サービスプランを作成する

顧客にライセンスを発行し、製品/サービスおよび顧客ごとに異なるライセンスプランを設定するには、サービスプランを使用します。サービスプランの作成には、Licensing Management Platform (LMP) を使用します。

手順

1. Remote Manager からシングルサインオンで LMP にアクセスします。
2. [ユーザとライセンス] > [サービスプラン] に移動します。
3. [サービスプランの作成] をクリックします。
4. サービスプランの設定を指定します。

オプション	説明
サービスプラン名	LMP および Remote Manager に表示されるサービスプランの名前を指定します。
製品/サービス	関連する Cloud Edge 製品またはサービスを選択します。 ライセンスの種類には、Cloud Edge ゲートウェイモデル、Cloud Edge の仮想アナライザのライセンスが含まれます。
バージョンタイプ	[体験版] または [製品版] を選択します。
体験版フォーム	必要に応じて、このサービスプランの体験版フォームを有効にします。

オプション	説明
ユニット	[ライセンス数] を選択します。
データセンター	ユーザが拠点とする国を選択します。
アクティベーションポリシー	サービスプランをいつ有効にするかを設定します。
製品/サービスを管理する	[サービスの管理を有効にする] を選択すると、Remote Manager で Cloud Edge を制御できるようになります。  重要 Remote Manager で Cloud Edge を管理するにはこの設定が必要です。

5. サブスクリプションポリシー設定を指定します。

オプション	説明
初期ライセンス期間	サブスクリプションの初期の有効期間を設定します。この期間が経過したサブスクリプションは、更新しない限り期限切れとなります。
自動更新	サブスクリプションを自動で更新する場合に選択します。
期限切れ通知	サブスクリプションの期限が切れる何日前に顧客に通知するかを選択します。 [ユーザとライセンス] > [顧客] に移動して顧客をクリックすると、ライセンスステータスが表形式で表示されます。

6. [OK] をクリックします。
7. 確認のメッセージが表示されたら、[はい] をクリックします。

会社を作成してサービスプランを割り当てる

手順

1. Remote Manager からシングルサインオンで LMP にアクセスします。

2. [ユーザとライセンス] > [顧客] に移動します。
3. [顧客の作成] をクリックします。
4. [会社のプロファイル] の情報を指定します。

オプション	説明
会社、アドレス	顧客の会社名を指定し、必要に応じて顧客の住所を指定します。
都市、都道府県、郵便番号	顧客の都市、都道府県、郵便番号を指定します。
国/地区	顧客の国を選択します。
備考	必要に応じて備考を入力します。

5. [ユーザのアカウント] の情報を指定します。

オプション	説明
アカウント名	顧客のアカウント名を指定します。
ユーザの役割	「管理者」に設定します (変更できません)。
担当者	担当者名を指定します。
メールアドレス	アカウントのメールアドレスを指定します。
タイムゾーン	顧客のタイムゾーンを選択します。
言語	Cloud Edge Cloud Console の画面表示に使用する言語を指定します。この言語は顧客へのレポートや通知にも使用されます。
アカウント作成メールを送信する	アカウント作成メールを顧客に送信するタイミングを選択します。

6. [サービスプランを割り当てる] をクリックします。
7. 「52 ページのサービスプランを作成する」で作成したサービスプランを 1 つ以上選択します。
8. 選択した各サービスプランについて、[ライセンス開始日] を選択します。

9. 選択した各サービスプランについて、[ライセンスあたりのユニット数] を製品ライセンスで許可された最大数に設定します。
10. [保存] をクリックします。
11. 次の点を確認します。
    - [ユーザとライセンス] > [顧客] で [会社名] のリストに会社が追加されていること
    - 会社の正しいサービスプランが表示されていること
12. 右上にある [Trend Micro Remote Manager] をクリックして Remote Manager に戻ります。

第 5 章

Trend Micro Remote Manager

Trend Micro Remote Manager、Trend Micro Licensing Management Portal (LMP) は販売代理店やマネージドサービスプロバイダ (MSP) などのパートナー向けのプラットフォームです。

Trend Micro Remote Manager

Trend Micro Remote Manager は、Licensing Management Platform と連携して、中小規模の企業向けのセキュリティサービスを管理するシステムです。

Remote Manager では、管理下の複数の製品およびサービスを使用して管理下の複数のネットワークの状態を監視できます。MSP の管理者は、Remote Manager を使用してコマンドを実行し、ネットワークセキュリティの重要な要素を管理できます。

Remote Manager は各地域のトレンドマイクロのデータセンターサーバでホストされ、MSP は該当するサーバのアカウントを取得します。MSP は、Remote Manager Web コンソールを使用して、ユーザアカウントの作成、ユーザネットワークの監視、セキュリティサービスの管理を行います。

Remote Manager では、ユーザネットワークが構造的に表示されます。MSP はコマンドを発行し、ネットワークセキュリティの次の状況を監視できます。

- コンポーネントのアップデートと、管理下のサーバのアップデート
- 脆弱性診断
- ダメージクリーンナップ
- 大規模感染への自動対応
- ファイアウォールとリアルタイム検索の設定
- 手動検索
- シングルサインオン

Remote Manager には包括的なレポート生成機能も備わっており、MSP は自動的に生成されたレポートを個々の担当者に送付できます。

初期設定テンプレートを設定する

注意

初期設定テンプレートは、Licensing Management Platform と統合済みである場合にのみ使用できます。

初期設定テンプレートには顧客向けの値が事前に設定されているため、複数の顧客に対して簡単に同じ設定を使用できます。

このテンプレートに設定できる内容についての詳細は、Remote Manager のドキュメントを参照してください。

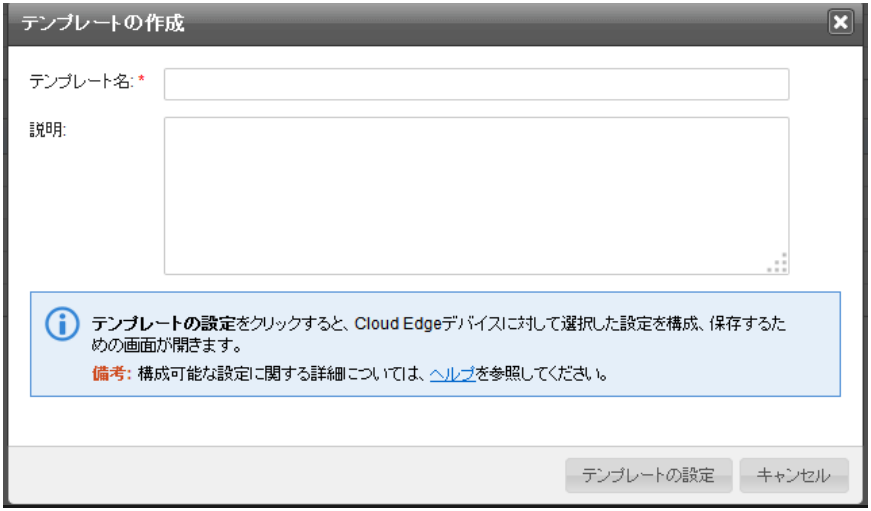
手順

1. Remote Manager にログオンします。
2. [管理] > [初期設定テンプレートの構成] に移動します。

   [初期設定テンプレートの構成] 画面が開きます。[Cloud Edge] セクションに、5 つのテンプレートのリストがあります。いずれも初期設定では空の状態です。このリストでは、5 つのテンプレートを作成できます。また、既存のテンプレートを編集することもできます。
3. 新しいテンプレートを作成するには、[Cloud Edge] セクションで、いずれかの未設定のテンプレートの横にある [作成] をクリックします。

   設定済みのテンプレートを編集するには、[編集] をクリックします。

   [テンプレートの作成] 画面が表示されます。



4. テンプレート名を指定し、必要に応じて説明を入力します。説明を指定することで、テンプレートの用途を特定しやすくなります。
5. [テンプレートの設定] をクリックします。

   Cloud Edge Cloud Console に似たコンソールが開き、ナビゲーションバーに [ポリシー]、[分析とレポート]、[管理] という 3 つのメニューが表示されます。

   注意

   このサイトでの変更はすべてテンプレートとして保存され、登録済みの製品には適用されません。

6. 関連するポリシーおよびスケジュールを設定します。

   次の設定を行うことができます。

   - ポリシー

     ポリシールール、オブジェクト、許可/ブロックリスト、ゲートウェイプロファイル、ユーザ通知

     注意

     ポリシーのセキュリティテンプレートを設定するときは、新しいインタフェースオブジェクトを設定して使用することはできません。ポリシールールのインタフェースオブジェクトを設定して使用するには、テンプレートを配信してから Cloud Edge Cloud Console を使用する必要があります。

     ポリシールールテンプレートの新しいセキュリティプロファイルセクションを設定できます。セキュリティプロファイル設定は Cloud Edge 6.0 以降を実行するゲートウェイでのみ有効です。

   - 分析とレポート

     レポート、概要レポート

   - 管理

     キャプティブポータル、監査ログ、予約アップデート、管理者アラート

ポリシーの設定については、以下の Web サイトでオンラインヘルプを参照してください。

http://docs.trendmicro.com/ja-jp/cemsp-5.3/welcome/

会社を作成してサービスプランを割り当てる

ここでは、Remote Manager を使用して会社を作成し、サービスプランを割り当てる手順を説明します。サービスプランの作成には、Licensing Management Platform (LMP) を使用します。LMP の詳細な使用方法については、53 ページの「会社を作成しサービスプランを割り当てる」を参照してください。

手順

1. Remote Manager にログオンします。
2. [ユーザ] に移動します。
3. [新規ユーザ] をクリックします。
4. [会社情報] の情報を指定します。

オプション	説明
会社名、アドレス	顧客の会社名を指定し、必要に応じて顧客の住所を指定します。
都市、都道府県、郵便番号	顧客の都市、都道府県、郵便番号を指定します。
国	顧客の国を選択します。

5. [ユーザアカウント] 情報を指定します。

オプション	説明
アカウント	顧客のアカウントを指定します。
担当者	担当者名を指定します。
電話番号	市外局番、電話番号、および内線番号 (オプション) を指定します。

オプション	説明
メール	アカウントのメールアドレスを指定します。
タイムゾーン	顧客のタイムゾーンを選択します。
言語	Cloud Edge Cloud Console の画面表示に使用する言語を指定します。この言語は顧客へのレポートや通知にも使用されます。

6. [次へ] をクリックします。
7. [サービスプラン] を選択します。

注意

サービスプランを Remote Manager で作成することはできません。サービスプランを作成するには、LMP に直接アクセスするか、シングルサイオンで Remote Manager から LMP にアクセスします。詳細については、52 ページの「サービスプランを作成する」を参照してください。

8. カレンダーをクリックして、[開始日] を選択します。
9. [ライセンス] を製品ライセンスで許可された最大数に設定します。
10. [デバイスの追加] をクリックして、デバイス名とシリアル番号を指定します。
11. [次へ] をクリックします。

    [製品の初期設定] 画面が表示されます。
12. 以前に作成したポリシーテンプレートを選択します。

    詳細については、58 ページの「初期設定テンプレートを設定する」を参照してください。
13. 必要に応じて、選択したテンプレートに関する情報を [コメント] に入力します。
14. [保存] をクリックします。
15. 次の点を確認します。
    - [ユーザ] で [ユーザ] リストに会社が追加されていること

- 会社の正しいサービスプランが表示されていること

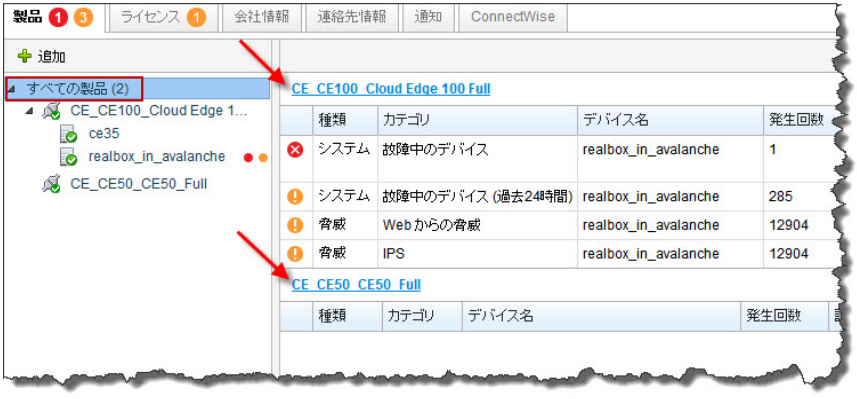
Cloud Edge Cloud Console にシングルサインオンする

ここでは、Remote Manager からシングルサインオン (SSO) で Cloud Edge Cloud Console にアクセスする手順を説明します。

手順

1. Remote Manager にログオンします。
2. [ユーザ] に移動します。
3. 会社の名前をクリックします。

   [製品] タブがデフォルトで表示されます。
4. [すべての製品] を選択します。
5. 表示された製品の名前をクリックします。
6. Cloud Edge のサービスプラン名をクリックします。



Cloud Edge Cloud Console が表示されます。

毎日の監視

手順

1. Remote Manager にログオンします。

   [ホーム] 画面に Remote Manager のダッシュボードが表示されます。

2. [ウィジェットの追加] をクリックして、Cloud Edge のウィジェットをダッシュボードに追加します。

   a. [Cloud Edge] をクリックし、下記のウィジェットを選択します。

      - 多くの脅威にさらされている Cloud Edge デバイス
      - 多くの脅威にさらされている Cloud Edge ユーザ

   b. [追加] をクリックします。

3. [ホーム] 画面で、ウィジェットが追加されているかを確認します。各ウィジェットの詳細は以下を参照してください。

   - 66 ページの「[多くの脅威にさらされている Cloud Edge デバイス] ウィジェット」
   - 67 ページの「[多くの脅威にさらされている Cloud Edge ユーザ] ウィジェット」

4. 必要に応じて、シングルサインオンで Cloud Edge Cloud Console にアクセスします。

   63 ページの「Cloud Console にシングルサインオンする」を参照してください。

レポートの概要

Cloud Edge では、レポートを生成、ダウンロード、および自動送信することができます。レポートには、ライセンスステータスや診断結果、脅威の検出情報、主な脅威、およびユーザのネットワーク内で影響を受けた上位のコンピュータ、ファイル、メールアドレスに関する概要が記載されます。

レポートには、Remote Manager で管理されるトレンドマイクロ製品から収集された統計が多数含まれます。レポートプロファイル、および単発または指

定期間中の定期レポートを設定し、複数の宛先にメールでレポートを送信できます。Remote Manager には、過去 30 件の日次レポート、10 件の週間レポート、および 5 件の月間レポートが保存されます。一般レポートは、MSP およびユーザ向けです。

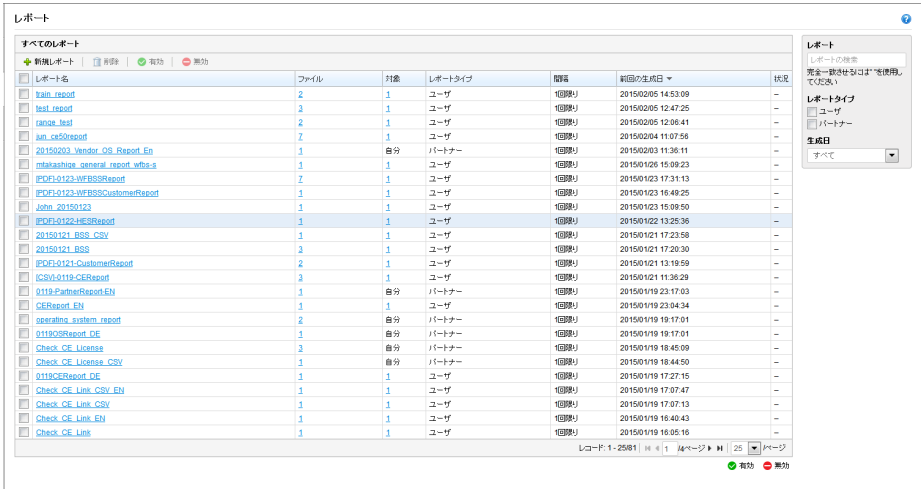


図 5-1. レポート画面

レポートプロファイルを使用すると、1 つのプロファイルから複数のレポートを作成できます。たとえば、当日の単発レポートを作成してレポートを生成し、翌日一部のオプションを変更して再度レポートを生成すれば、レポート全体を作り直す必要はありません。

Remote Manager のレポートの詳細については、Remote Manager オンラインヘルプを参照してください。

http://docs.trendmicro.com/ja-jp/smb/trend-micro-remote-manager.aspx

[多くの脅威にさらされている Cloud Edge デバイス] ウィジェット

多くの脅威イベントが発生している Cloud Edge デバイスを表示します。

- 表示されるデータの時間範囲を以下から選択して変更できます。
  - 過去 1 時間
  - 過去 24 時間
  - 過去 7 日間
  - 過去 30 日間 (初期設定)
- 表示されるデータの脅威の種類を以下から選択して変更できます。
  - すべて
  - ボットネット
  - 侵入防止システム (IPS)
  - スパムメール
  - Web レピュテーション
  - ウイルス
  - ランサムウェア
  - C&C

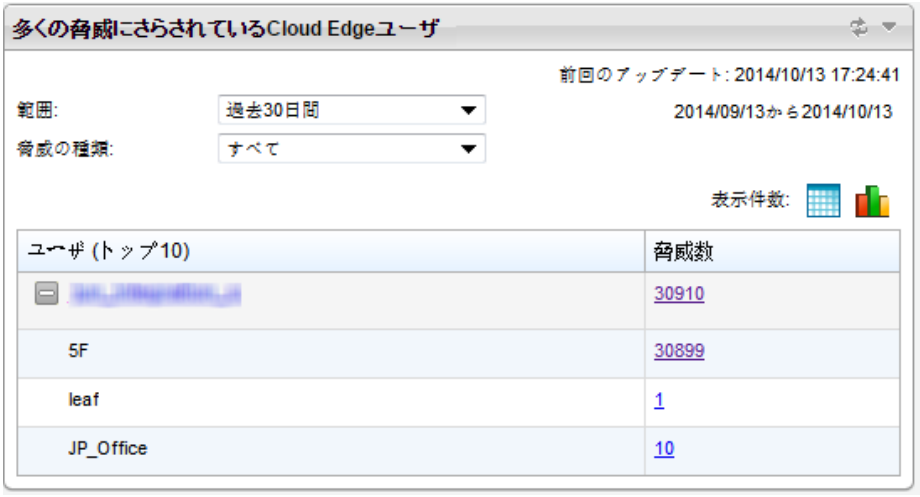
- ユーザ名をクリックすると、ユーザ情報が表示されます。
- 脅威数をクリックすると、Cloud Edge Cloud Console から脅威情報が表示されます。

注意

Cloud Edge のウィジェットは、初期設定では Remote Manager ダッシュボードに表示されません。

[多くの脅威にさらされている Cloud Edge ユーザ] ウィジェット

多くの脅威イベントが発生している Cloud Edge ユーザを表示します。データは表および円グラフに表示されます。表と円グラフは、表示アイコン ( ) をクリックして切り替えることができます。



- 表示されるデータの時間範囲を以下から選択して変更できます。
  - 過去 1 時間
  - 過去 24 時間

- 過去 7 日間
- 過去 30 日間 (初期設定)

- 表示されるデータの脅威の種類を以下から選択して変更できます。
  - すべて
  - ボットネット
  - 侵入防止システム (IPS)
  - スパムメール
  - Web レピュテーション
  - ウイルス
  - ランサムウェア
  - C&C
- ユーザ名をクリックすると、ユーザ情報が表示されます。
- 脅威数をクリックすると、Cloud Edge Cloud Console から脅威情報が表示されます。

注意

Cloud Edge のウィジェットは、初期設定では Remote Manager ダッシュボードに表示されません。

ゲートウェイデバイスを管理する

ゲートウェイデバイスの管理には Remote Manager の [ユーザ] 画面を使用します。サービスプランの選択後、次のゲートウェイデバイス管理操作を実行できます。

- 最近のゲートウェイイベントを確認する
- ゲートウェイデバイスのファームウェアを直ちに更新する
- 追加のゲートウェイデバイスをユーザに登録する

手順

1. Remote Manager にログオンします。

   [ホーム] 画面に Remote Manager のダッシュボードが表示されます。

2. [ユーザ] をクリックします。

3. [会社] 列で、ユーザ名を選択します。

4. 左側のナビゲーションで、[すべての製品] を展開し、サービスプランを選択します。

5. 次のように実行します。

オプション	説明
違反イベントとシステムイベントを表示する	[イベント] タブをクリックします。
ファームウェアをアップデートする	[ファームウェアのアップデート] タブをクリックし、期限切れまたはアップデートできなかったデバイスを選択して、[アップデート] をクリックします。 [アップデート] をクリックした後に、選択したゲートウェイデバイスのアップデートが即座に実行されます。
追加のゲートウェイを登録する	[デバイス] タブをクリックし、[登録] をクリックします。

6. ゲートウェイに関するその他の作業を行います。

   a. 登録済みゲートウェイデバイスを左側のナビゲーションから選択します。

   b. [イベント] タブをクリックして、過去 1 時間の違反イベントとシステムイベントを表示します。

   c. [コンポーネント] タブをクリックして、各製品コンポーネントの現在のバージョンと最新バージョンを表示します。

   d. [ネットワーク] タブをクリックして、過去 24 時間のユーザアクティビティを表示します。

e. [VPN] タブをクリックして、最近の VPN アクティビティを表示します。

注意

VPN がサポートされていない Cloud Edge ゲートウェイモデルでは、VPN に関する情報を確認することはできません。

Remote Manager の詳細

Remote Manager の詳細については、次のオンラインヘルプを参照してください。

http://docs.trendmicro.com/ja-jp/smb/trend-micro-remote-manager.aspx

第 6 章

Cloud Edge Cloud Console

本章では、Cloud Edge Cloud Console を使用してゲートウェイを登録および管理する方法について説明します。

Cloud Console にログオンする

Cloud Edge Cloud Console には、直接ログオンする方法と Remote Manager からシングルサインオンでログオンする方法があります。

手順

- Cloud Edge Cloud Console に直接ログオンします。
  a. トレンドマイクロから提供された Cloud Edge Cloud Console の URL にアクセスします。
  b. ユーザ名とパスワードを指定します。

  注意

  Cloud Edge Cloud Console に直接ログオンする場合は、事前に一度 Remote Manager からシングルサインオンで Cloud Edge Cloud Console にログオンし、管理者アカウントを作成しておく必要があります。

  267 ページの「Cloud Console 管理者アカウントを追加する」を参照してください。

  Cloud Edge Cloud Console にアクセスできない場合は、マネージドサービスプロバイダにお問い合わせください。

- Remote Manager からシングルサインオンで Cloud Edge Cloud Console にログオンします。

  63 ページの「Cloud Console にシングルサインオンする」を参照してください。

[スタートガイド] 画面

Cloud Edge Cloud Console に初めてログオンすると、ダッシュボードがロードされ、[スタートガイド] 画面が表示されます。

[スタートガイド] 画面には、Cloud Edge Cloud Console の利用をすぐに開始するための情報が表示されます。また、Cloud Edge ユーザに役立つ情報のリンクも用意されています。

Cloud Edge Cloud Console への次回ログオン時に [スタートガイド] 画面を表示しない場合は、[今後表示しない] を選択します。

[スタートガイド] 画面は、[ヘルプ] の横の矢印をクリックして [スタートガイド] を選択するといつでも表示できます。

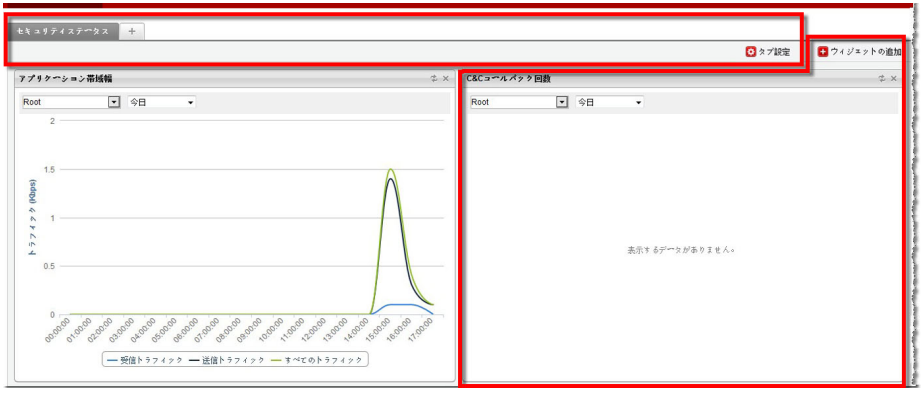
Cloud Edge Cloud Console の概要

このセクションでは、Cloud Edge Cloud Console の機能に関する基本的な概要を示します。詳細については、Cloud Edge オンラインヘルプを参照してください。

ダッシュボードについて

ダッシュボードでは、各種のウィジェットを通じてネットワークの整合性を監視できます。ユーザアカウントごとにそれぞれ独自のダッシュボードが用意されており、各ユーザアカウントで行ったダッシュボードに対する変更は他のユーザアカウントのダッシュボードには適用されません。

ダッシュボードは次のユーザインタフェース要素で構成されます。



ゲートウェイについて

Cloud Edge ゲートウェイを顧客の環境に配置したら、クラウドを介してリモートで管理できるように Cloud Edge Cloud Console にゲートウェイとして登録できます。

[ゲートウェイ] タブでは、ゲートウェイモデルと配信モードに応じて、次の処理を実行できます。

- ハードウェアやポリシーのステータス情報を確認できます。
- CPU の温度、CPU 使用率、ディスク使用率、およびメモリ使用率に関するゲートウェイステータスを確認できます。

- ゲートウェイのネットワークイベント、システムイベント、VPN イベント、およびポリシー施行ログを確認できます。
- Ping、Traceroute、および ARP ネットワークツールを使用して、ゲートウェイの IPv4 ネットワーク接続の問題に関するトラブルシューティングを行えます。
- トラフィックの負荷が高い場合の Cloud Edge ゲートウェイの動作を設定できます。
- ファームウェアや製品コンポーネントをアップデートできます。
- ネットワーク情報を設定および確認できます。
- ハードウェアスイッチチップセットを備えたゲートウェイのイントラネットセキュリティモードを設定できます。
- ワイヤレスネットワークアクセス管理の設定、およびワイヤレスネットワークがサポートされているゲートウェイのワイヤレスクライアント接続の管理を行えます。
- SSL VPN (Secure Socket Layer VPN) または L2TP (Layer 2 Tunneling Protocol) VPN を使用してユーザの仮想プライベートネットワーク (VPN) を設定できます。
- 帯域幅制御ルールを設定することで、ビジネスの目標達成を支えるネットワークトラフィックの帯域幅を節約し、通信品質を向上させることができます。
- サイト間 VPN の設定
- 静的ルートおよび NAT を設定できます。
- エンドユーザ管理を設定できます。
- 認証用の LDAP 設定を行います (日本ではサポートされていません)。
- ウイルスバスター ビジネスセキュリティサービスとの統合ソリューションである VBBSS エンドポイント保護を設定し、古いパターンファイルを使用しているビジネスセキュリティエージェントがインストールされたエンドポイント、またはビジネスセキュリティエージェントがインストールされていないエンドポイントにインターネット接続を許可するかどうかを制御できます。

- 不審エンドポイントを設定し、設定したしきい値を超える C&C コールバックが Cloud Edge で検出されるエンドポイントに対してネットワークアクセスコントロールを提供できます。
- 不審エンドポイントを有効にすることで、ネットワーク内で検出されたエンドポイントデバイスと脆弱性のリストを表示できます。
- 不審エンドポイントを設定することで、脆弱性、脆弱なパスワード、および開いているポートをエンドポイントデバイスで検索できます。

注意

VPN がサポートされていない Cloud Edge ゲートウェイモデルでは、VPN に関する情報を設定することも確認することもできません。

ログ分析について

[分析とレポート] タブでは、登録済みゲートウェイからアップロードされて Cloud Edge Cloud Console に集約されたログ統計をインタラクティブなグラフ形式で確認できます。ダッシュボードには表示されない詳細な情報を追跡したり、ドリルダウンして未加工のログを調べたりできます。

- アプリケーション帯域幅

  ネットワーク上の IP アドレス、ユーザ、アプリケーションによる帯域幅の消費を確認および分析します。ログを確認した後、ポリシーを調整して通信を制御したり、不要なトラフィックをブロックしたり、重要なトラフィックやサービスに帯域幅を割り当てたりできます。

  顧客が Cloud Edge 6.0 以降を実行する Cloud Edge 50G2 ゲートウェイのみを使用する場合は、ポリシールールの使用状況データを確認します。

- ポリシー施行

  ポリシーによるネットワークトラフィックの制御方法を確認および分析します。ログを確認した後、ポリシールールを調整して特定のトラフィックを許可またはブロックしたり、設定が適切でないポリシーのトラブルシューティングを行ったりできます。

  ポリシー施行のイベントは次のとおりです。

  - ポリシールール (アプリケーション制御、URL フィルタ、ファイアウォール)

- ブロックリスト

- インターネットアクセス

  特定のユーザがアクセスした Web サイトやドメインを確認および分析します。ログを確認した後、特定の種類のトラフィックをフィルタする URL カテゴリグループを追加したり、必要に応じてそれらのカテゴリの特定の URL を個別に許可またはブロックしたりできます。

  顧客が Cloud Edge 6.0 以降を実行する Cloud Edge 50G2 ゲートウェイのみを使用する場合は、ポリシールールの使用状況データを確認します。

- インターネットセキュリティ

  検索エンジンで不正プログラムやネットワークの脅威などからユーザを保護する方法を確認および分析します。ログを確認した後、セキュリティ機能を有効または無効にしたり、処理、スケジュール、ユーザポリシーを調整してネットワークの保護を強化したりできます。

  インターネットセキュリティのイベントは次のとおりです。

  - 侵入防止システム (IPS)
  - 不正プログラム対策
  - メールセキュリティ対策
  - Web レピュテーション
  - ボットネット検出

特定のログクエリを設定した後、[保存] をクリックして [⭐お気に入りとして保存] を選択すると、設定を保存して後で表示することができます。分析とレポート > お気に入りログに移動し、[お気に入りログ] 画面を表示します。

ポリシーについて

[ポリシー] 画面では、Cloud Edge Cloud Console のポリシールール、ポリシーオブジェクト、許可リストとブロックリスト、セキュリティプロファイル、ユーザ通知、および不審オブジェクトリストとブロック処理を管理できます。Cloud Edge Cloud Console では、登録済みのゲートウェイの一部またはすべてに対してポリシーを適用できます。

ポリシーオブジェクトを作成して、ポリシールールのオプションをカスタマイズできます。ポリシーオブジェクトには、ポリシーを適用するインタフェ

ースグループ、ユーザとユーザグループ、IP アドレス/FQDN、MAC アドレス、ジオロケーションのほか、ポリシーの対象となるサービス、アプリケーショングループ、URL グループカテゴリの種類、ポリシールールを適用するスケジュールが含まれます。

IPS、不正プログラム対策のセキュリティ、Web レピュテーション、メールセキュリティ、HTTPS 検査、DoS 攻撃、およびエンドポイントの識別に対するセキュリティプロファイルを設定することで、ポリシーの制御を微調整できます。必要に応じて、許可またはブロックする URL を追加することもできます。これらの設定は、定義済みのポリシールールよりも優先されます。

レポートについて

[分析とレポート] タブでは、予約レポートやオンデマンドレポートを確認したりダウンロードしたりできます。Cloud Edge Cloud Console には、登録済みのすべてのゲートウェイからログ情報が集約されます。それらのログから、検出されたウイルスや不正コード、ブロックされたファイル、およびアクセスされた URL に関するレポートを生成できます。ネットワークイベントに関するこれらの情報を使用して、設定を最適化したり、セキュリティポリシーを微調整したりできます。

ゲートウェイ管理

MSP は Cloud Edge Cloud Console を使用して、新しい Cloud Edge ゲートウェイを登録します。ユーザが Cloud Edge ゲートウェイの電源を投入し、ネットワークに接続すると、ポリシーが配信され、MSP は関連するダッシュボード、ログ、およびレポート統計を表示できます。

ゲートウェイを管理する

目的: Cloud Edge Cloud Console でゲートウェイを管理します。

場所: ゲートウェイ

手順

1. Cloud Edge Cloud Console でゲートウェイを管理する場合は、次の処理を実行できます。
    - 登録済みのゲートウェイに関する情報の確認。

- 新しいゲートウェイの登録。
- 複数のゲートウェイのインポート。
- 新しいゲートウェイグループの作成。
- 検索ボックスでのゲートウェイグループおよび、Cloud Edge デバイスの検索。
- リストされたゲートウェイで使用する初期設定のセキュリティプロファイルの選択。

  ゲートウェイが HA グループのメンバーである場合、プライマリゲートウェイとセカンダリゲートウェイの両方にプライマリゲートウェイのセキュリティプロファイルが使用されます。
- ゲートウェイでの選択処理の実行。

注意

一部の処理は、HA グループの一部であるゲートウェイでは実行できません。

82 ページの「ゲートウェイの処理」を参照してください。

- ゲートウェイ名をクリックしてからのゲートウェイの管理。

  ゲートウェイは標準/G3 ゲートウェイと Cloud Edge 50G2 ゲートウェイのいずれかです。

  -  : 標準/G3 ゲートウェイ
  -  : Cloud Edge 50G2 ゲートウェイ

    Cloud Edge 50G2 ゲートウェイは Cloud Edge 6.0 以降のリリースで実行される、ハードウェアとパフォーマンスが向上した第 2 世代モデルです。

  Cloud Edge Cloud Console で変更できるゲートウェイおよび実行可能な管理タスクはゲートウェイモデルと配信モードによって異なります。

2. Cloud Edge ゲートウェイの高可用性設定を管理します。

- 既存の HA グループに関する情報の確認。
- 1 つまたは複数の新規 HA グループの作成。

  HA グループを作成するには、HA グループをサポートする少なくとも 2 台のゲートウェイが必要です。
- HA グループの有効化。
- HA グループの無効化。
  - 無効にしても、2 台の Cloud Edge ゲートウェイのペアは維持されます。これらのゲートウェイのいずれかを使用して新しい HA グループを作成することはできません。
  - HA グループが無効になっている間、ユーザのネットワークトポロジによっては、エンドユーザのトラフィックが一時的に停止する場合があります。
- 既存の HA グループの編集。
- 既存の HA グループに対する手動フェイルオーバー (強制テイクオーバー) の実行。
- 既存の HA グループの削除。

注意

すべての管理処理で監査ログが生成されます。

登録

Cloud Edge Cloud Console に登録できるゲートウェイの数は、サポート契約で規定されています。

ゲートウェイの登録後、名前をクリックして次の処理を実行できます。

- ゲートウェイに関する一般的な情報の表示
- ゲートウェイのシステムステータスに関する情報の表示
- Ping、Traceroute、および ARP ネットワークツールを使用して、ゲートウェイの IPv4 ネットワーク接続の問題に関するトラブルシューティングを行えます。

- ゲートウェイのネットワークイベント、システムイベント、VPN イベント、およびポリシー施行ログを確認できます。
- トラフィックの負荷が高い場合の Cloud Edge ゲートウェイの動作を設定できます。
- ネットワークの設定
- ハードウェアスイッチチップセットを備えたゲートウェイのイントラネットセキュリティモードを設定できます。
- ワイヤレスネットワークをサポートしているゲートウェイのワイヤレスネットワーク設定の表示
- ワイヤレスネットワークアクセス管理の設定、およびワイヤレスネットワークがサポートされているゲートウェイのワイヤレスクライアント接続の管理を行えます。
- 帯域幅制御の設定
- ユーザ VPN の設定
- サイト間 VPN の設定
- エンドユーザ認証および TTL キャッシュの設定
- 認証用の LDAP 設定を行います (日本ではサポートされていません)。
- Cloud Edge ゲートウェイの更新
- VBBSS エンドポイント保護 (ウイルスバスター ビジネスセキュリティサービスとの統合ソリューション) の設定
- 不審エンドポイントを設定することにより、設定したしきい値を超える C&C コールバックが検出されるエンドポイントに対してネットワークアクセスコントロールを提供できます。

注意

VPN がサポートされていない Cloud Edge ゲートウェイモデルでは、VPN に関する情報を設定することも確認することもできません。

ゲートウェイの処理

処理	説明
	新しいゲートウェイグループを追加します。
	ゲートウェイの表示名を変更します。
	ゲートウェイを別のゲートウェイグループに移動します。 HA グループに含まれているゲートウェイは移動できません。
	新しいシリアル番号を指定してゲートウェイのハードウェアを交換します。 HA グループに含まれているゲートウェイを、元のゲートウェイと同じモデルに交換する必要があります。元のゲートウェイに適用されていたパッチを交換ゲートウェイに適用する必要があります。さらに、エンジン/パターンの更新を交換ゲートウェイにも再適用してください。
	ゲートウェイの On-Premises Console パスワードを変更します。 HA グループに含まれているゲートウェイの場合は、各ゲートウェイのパスワードを個別に変更します。
	最新のセキュリティ脅威から保護できるようにゲートウェイのコンポーネントをアップデートします。
	ゲートウェイをリモートで再起動します。
	ゲートウェイを Cloud Edge Cloud Console から削除します。このゲートウェイはオンプレミスのセキュリティ脅威を引き続き検索しますが、リモートのコマンドまたは更新を受け取ることはできません。 HA グループに含まれているゲートウェイは削除できません。

ゲートウェイを登録する

目的: Cloud Edge アプライアンスをセキュリティゲートウェイとして機能させるために、最初に Cloud Edge Cloud Console にゲートウェイとして登録します。

場所: ゲートウェイ

手順

1. [新しいゲートウェイの登録] をクリックします。
2. ゲートウェイの設定を指定します。
   - 表示名

     Cloud Console に表示される新しいゲートウェイの名前を指定します。
   - モデル

     Cloud Edge ゲートウェイのハードウェアモデルを指定します。
   - シリアル番号

     Cloud Edge ゲートウェイのシリアル番号を指定します。シリアル番号はゲートウェイの本体またはパッケージに記載されている 12 桁の英数字 (例: 4C80-9315-3A0B) です。
3. [保存] をクリックします。

   登録が完了するまで、数分かかることがあります。

   登録が完了すると、Cloud Edge Cloud Console からゲートウェイにポリシーが配信されます。ダッシュボードのウィジェット、ログ分析、およびレポートで、Cloud Edge ゲートウェイから送信されるリアルタイムのトラフィックに基づくログ統計を確認できます。

複数のゲートウェイをインポートする

目的: ユーザが CSV ファイルを指定された形式でアップロードすることで、ゲートウェイを一括登録できるようにします。

場所: [ゲートウェイ] > [ゲートウェイ管理]

手順

1. [ゲートウェイのインポート] ボタンをクリックします。
2. [ゲートウェイのインポート] ポップアップの [モデル] ドロップダウンで、ゲートウェイモデルを選択します。

3. [参照] をクリックして、ローカルドライブの CSV ファイルに移動します (.CSV ファイルをダウンロードするには、[テンプレートのダウンロード] をクリックします)。

注意

.CSV ファイルでは、各ゲートウェイのこれら 2 つの値を入力する必要があります。ゲートウェイごとに改行します。[ゲートウェイ名] フィールドは空のままでもかまいません。空のままにすると、システムにより自動的にゲートウェイ名が生成されます。自動的に生成されるゲートウェイ名は「Cloudedge_01」、「CloudEdge_02」などです。CSV ファイルの先頭の行は削除しないでください。

4. [インポート] をクリックします。

   [ゲートウェイ管理] ページで、Root グループのリストにインポート済みのゲートウェイが表示されます。[インポートの概要] バナーには、正常にインポートされたゲートウェイの数とインポートに失敗したゲートウェイの数が表示されます。[エラーの修正] をクリックすると、インポートに失敗したゲートウェイの詳細がポップアップに表示されます。これは、エラーの詳細を示します。

5. [OK] をクリックするか、ローカルドライブに.CSV ファイルをエクスポートする場合は [エラーのエクスポート] をクリックします。

登録を確認する

ゲートウェイの登録後は、登録が正常に完了したことを確認してください。確認の手順を次に示します。

手順

1. Cloud Edge Cloud Console にログオンします。
2. ゲートウェイ に移動します。
3. [ゲートウェイ管理] のリストにゲートウェイが表示されていることを確認します。
4. [ポリシー配信ステータス] 列のステータスが「成功」になっていることを確認します。

5. ゲートウェイの名前をクリックします。
6. 表示された [ゲートウェイ情報] ウィンドウでゲートウェイの情報を確認します。

すべてのゲートウェイの情報を確認する

目的: すべてのゲートウェイのゲートウェイ情報および HA グループ情報を表示します。

場所: ゲートウェイ

手順

1. すべてのゲートウェイに関する情報を表示します。
   - グループ/ゲートウェイ名: グループまたはゲートウェイの名前です。
   - ステータス: ゲートウェイの Cloud Edge Cloud Console での現在のステータスです。
   - 前回のポリシー配信: Cloud Edge Cloud Console からゲートウェイへの前回のポリシー配信のタイムスタンプです。
   - ポリシー配信ステータス: 前回のポリシー配信の結果です。
   - 前回のログアップロード: ゲートウェイから Cloud Edge Cloud Console へアップロードされた最新のログのタイムスタンプです。
   - セキュリティプロファイル: このゲートウェイに適用される Cloud Edge セキュリティプロファイルです。
   - 処理: このゲートウェイに対して行える処理です。

     HA グループに含まれているゲートウェイは移動または削除できません。これらの処理アイコンは HA ペアの一部であるゲートウェイでは使用できません。
2. HA グループに関する情報を表示します。
   - HA 名: 各 HA グループの名前です。各 HA グループ名の下に、2 つのメンバー Cloud Edge ゲートウェイの名前が表示されます。

- 有効: HA グループがオンであるかオフであるかを示します。
- HA の役割: 役割はプライマリかセカンダリのどちらかです。
- 優先度: プライマリゲートウェイとセカンダリゲートウェイの優先度が表示されます。
- ハートビートインタフェース: プライマリゲートウェイとセカンダリゲートウェイのハートビートインタフェースが表示されます。

  プライマリゲートウェイとセカンダリゲートウェイの両方でインタフェースが同じである必要があります。
- IPv4 アドレス/ネットマスク: プライマリゲートウェイとセカンダリゲートウェイの IPv4 アドレスとネットマスクが表示されます。
- バージョン: プライマリゲートウェイとセカンダリゲートウェイのバージョンが表示されます。

  一般に、どちらのゲートウェイも同じバージョンですが、アップグレード中は短時間、異なるバージョンになる場合があります。
- HA ステータス: プライマリゲートウェイとセカンダリゲートウェイのステータスです。

  ステータスには次のものがあります。
- 処理: HA グループに対して実行できる処理のリストです。これには、編集、削除、強制テイクオーバー、有効化、無効化があります。

  処理を実行するには、目的の処理をクリックします。

HA グループを作成する

目的: Cloud Edge Cloud Console から HA グループを作成できます。HA グループは 2 台の Cloud Edge ゲートウェイで構成されます。ゲートウェイは、1 つの HA グループにのみ属することができます。

場所: ゲートウェイ

手順

1. 必要に応じて、HA グループに関する情報を確認します。

   91 ページの「HA グループ」

2. HA グループのメンバーにする各ゲートウェイのハートビートインタフェース間を、Ethernet ケーブルで直接接続します。

   Cloud Edge 50G2 ゲートウェイの場合、ハートビート L3 インタフェースに LAN2 または LAN3 のみ使用できます。また、各ゲートウェイで同じインタフェースを使用する必要があります (LAN2 と LAN2、または LAN3 と LAN3)。

3. [高可用性管理] セクションの [HA グループの作成] をクリックします。

   [HA グループの作成] ウィザードが開きます。

4. [HA グループの作成と操作モードの選択] ページで、次の詳細を指定します。

オプション	説明
HA グループ名	グループ名は 1〜32 文字で指定する必要があり、英字、数字、アンダースコアを含めることができます。
操作モード	[アクティブ-パッシブ] にあらかじめ設定されています。使用できるのはこのモードだけです。
認証方法	次のいずれかを選択します。 • [なし] • [簡易] を選択し、簡易認証方法に使用するパスワードを入力します。 • [HMAC] を選択し、HMAC 認証方法に使用するパスワードを入力します。
有効にする	次のいずれかを選択します。 • オン • オフ

5. [次へ] をクリックします。

6. [プライマリゲートウェイの設定] ページで、HA グループ内でプライマリゲートウェイにする Cloud Edge ゲートウェイの設定を行います。

オプション	説明
プライマリ HA ゲートウェイ	HA プライマリゲートウェイとして指定するゲートウェイをドロップダウンリストから選択します。 HA グループ設定をサポートするゲートウェイのみがリストに表示されます。
役割	[プライマリ] に設定された読み取り専用フィールドです。この役割が、このゲートウェイに割り当てられます。
優先度	このゲートウェイの優先度の数値を入力します (1〜253)。初期設定は 253 です。 優先度が高いゲートウェイがアクティブになります。
ハートビートインタフェース	Cloud Edge でピア HA ゲートウェイとの通信に使用される L3 インタフェースをドロップダウンから選択します。 Cloud Edge 50G2 ゲートウェイの場合、ハートビートインタフェースとして LAN2 または LAN3 のみ選択できます。
ハートビートインタフェース IP/ネットマスク	まだ設定されていない場合は、ハートビートインタフェースの IPv4 アドレスとネットマスクを入力する必要があります。 プライマリゲートウェイとセカンダリゲートウェイのハートビートインタフェースの IPv4 アドレスは、同じサブネット上にある必要があります。 HA ペアにインタフェースを追加した後で、そのインタフェースのプライマリゲートウェイまたはセカンダリゲートウェイを変更することはできません。

7. [次へ] をクリックします。
8. [セカンダリゲートウェイの設定] ページで、HA グループ内でセカンダリゲートウェイにする Cloud Edge ゲートウェイの設定を行います。

オプション	説明
セカンダリ HA ゲートウェイ	HA セカンダリゲートウェイとして指定するゲートウェイをドロップダウンリストから選択します。 HA グループ設定をサポートするゲートウェイのみがリストに表示されます。
役割	[セカンダリ] に設定された読み取り専用フィールド。この役割が、このゲートウェイに割り当てられます。
優先度	このゲートウェイの優先度の数値を入力します (1〜253)。初期設定は 100 です。 優先度が高いゲートウェイがアクティブになります。
ハートビートインタフェース	ドロップダウンから L3 インタフェースがあらかじめ選択されています。これはプライマリ HA ゲートウェイに選択したのと同じインタフェースです。 Cloud Edge では、ピア HA ゲートウェイとの通信にこのインタフェースが使用されます。
ハートビートインタフェース IP/ネットマスク	まだ設定されていない場合は、ハートビートインタフェースの IPv4 アドレスとネットマスクを入力する必要があります。プライマリに設定されているハートビート IP アドレスと同じサブネット上にある必要があります。

9. [次へ] をクリックします。
10. [エラー発生時のテイクオーバーの設定] ページで、エラーが発生してテイクオーバーが行われたときの Cloud Edge HA グループの設定を行います。

オプション	説明
プリエンプション	次のいずれかを選択します。 • オン (初期設定): プライマリゲートウェイが前のエラーから回復した後にアクティブな役割に戻ります。 • オフ: プライマリゲートウェイはエラーから回復した後、アクティブな役割に自動的には戻りません。ユーザが手動でフェイルオーバーを実行する必要があります。
監視インタフェース	監視する 1 つまたは複数のインタフェースを選択します。Cloud Edge では、物理インタフェースのみ監視されます。すべての物理インタフェースでトラフィックを監視することをお勧めします。
監視 IP/FQDN	監視インタフェースごとに、監視ホストとして使用する IP アドレスまたは FQDN を最大 2 つ入力します。
テイクオーバーの実行回数	次の値を入力する必要があります。 • ハートビートエラー回数: パッシブゲートウェイが失敗したゲートウェイから引き継ぐまでのハートビートエラーの回数を示します (初期設定は 3、範囲は 3〜9)。 • Ping エラー回数: パッシブゲートウェイが失敗したゲートウェイから引き継ぐまでの Ping エラーの回数を示します (初期設定は 3、範囲は 1〜5)。

11. [VRRP (Virtual Router Redundancy Protocol) グループの設定] ページで、1 つまたは複数の VRRP グループを追加します。

    a. [追加] をクリックします。

    b. インタフェースを選択し、VRRP グループの仮想 IPv4 アドレスおよびネットマスクを入力します。

       設定に応じて、L3 物理インタフェースまたは静的 L3 VLAN インタフェースのいずれかを選択できます。

       98 ページの「HA グループ – VRRP グループ」の設定の要件を参照してください。

c. [IP アドレス/マスク] フィールドの右のチェックマークをクリックして、VRRP グループを保存します。

[次へ] をクリックする前に、少なくとも 1 つの VRRP グループを追加して保存する必要があります。

注意

VRRP グループの右の [X] をクリックすると、その VRRP グループを削除できます。

[次へ] をクリックした後、概要ページが開きます。

12. HA グループ設定の概要を確認します。

注意

HA グループを初めて作成すると、プライマリ HA ゲートウェイがアクティブになり、セカンダリ HA ゲートウェイがパッシブになります。

13. [保存] をクリックします。

HA グループ

2 台のゲートウェイを HA グループとして設定することで、高可用性アクセスを提供できます。一方のゲートウェイをプライマリ、もう一方をセカンダリとして設定します。最初に作成したときに、プライマリ HA ゲートウェイがアクティブになり、セカンダリはパッシブになります。一方のゲートウェイが停止した場合、もう一方のゲートウェイが引き継ぐ (アクティブになる) ため、ネットワークトラフィックが停止することはありません。

HA グループによって、致命的なエラーの発生に備えた冗長性を提供できることに加えて、ネットワークトラフィックの効率も向上できます。

基本情報

- HA グループの作成には、登録済みおよび未登録のゲートウェイを使用できます。
  - 未登録:

Cloud Edge Cloud Console で、HA グループ用に選択された各ゲートウェイのハードウェアモデルのみが確認されます。これらが一致しない場合、エラーが表示され、HA グループは保存されません。

- 登録済み:

  Cloud Edge Cloud Console で、以下の確認が行われます。

  - 各ゲートウェイのハードウェアモデル、ソフトウェアバージョン、配信モードの確認 — これらが一致しない場合、エラーが表示され、HA グループは保存されません。
  - ハートビートインタフェースの確認 — これらが同じサブネットにない場合、エラーが表示され、HA グループは保存されません。
  - VRRP インタフェースの確認 — これらが同じサブネットにない場合、エラーが表示され、HA グループは保存されません。
  - ゲートウェイがオンラインかどうかの確認 — HA グループを正しく保存するには、Cloud Edge ゲートウェイが両方ともオンラインである必要があります。

- ゲートウェイは、1 つの HA グループにのみ属することができます。
- アクティブ-パッシブモードのみサポートされます。
- アクティブなノードがマスターとして指定されます。
- HA グループは、プリエンプションモードと非プリエンプションモードのどちらでも機能します。
  - プリエンプション (チェックボックス、初期設定): プライマリゲートウェイが前のエラーから回復した後にアクティブな役割に戻ります。
  - 非プリエンプション: プライマリゲートウェイはエラーから回復した後、アクティブな役割に自動的には戻りません。ユーザが手動でフェイルオーバーを実行する必要があります。
- HA グループを作成する前に、次の項目が対処されていることを確認します。
  - HA グループ内のゲートウェイがルーティングモードで配信されていること。

- HA グループ内のゲートウェイが同じモデルであること。
- HA グループ内のゲートウェイでファームウェアのバージョンが同じであること。

注意

HA グループ内の一方のゲートウェイでファームウェアのバージョンがアップデートまたはロールバックされた場合は、その HA グループ内のもう一方のゲートウェイでもファームウェアを同じバージョンにアップデートまたはロールバックする必要があります。

- HA グループ内のゲートウェイに設定されているタイムゾーンが同じで、時間の差が 5 分以内であること。
- HA グループの作成前に、ゲートウェイのインタフェースで工場出荷時の初期設定が行われていること。

- Cloud Edge Cloud Console では、HA グループ内のゲートウェイの設定がゲートウェイにプッシュされます。ただし、設定のアップデートが不可能な場合は、ハートビート接続を使用して HA グループのノードを同期できます。
- ダッシュボード、ログ、レポートでは、プライマリ、セカンダリ、HA グループに対するクエリがサポートされています。
- Trend Micro Remote Manager で設定されたポリシーテンプレートは HA グループがセットアップされる前に配信されているため、HA グループには影響しません。Remote Manager は、HA グループを 2 台のスタンドアロンゲートウェイとして認識します。

その他の HA グループ情報

- 94 ページの「HA グループ - WAN トポロジ」
- 96 ページの「HA グループ – フェイルオーバーの条件」
- 97 ページの「HA グループ – ハートビートインタフェース」
- 98 ページの「HA グループ – VRRP グループ」
- 98 ページの「HA グループ - エンドポイントのネットワークアクセス」

- 99 ページの「HA グループ – 監視インタフェースとテイクオーバーの実行」
- 100 ページの「HA グループ – 設定マトリクス」
- 102 ページの「HA グループ – ポリシー設定マトリクス」
- 103 ページの「HA グループの制限事項」

HA グループでサポートされるモデル

HA グループでは次のモデルがサポートされます。

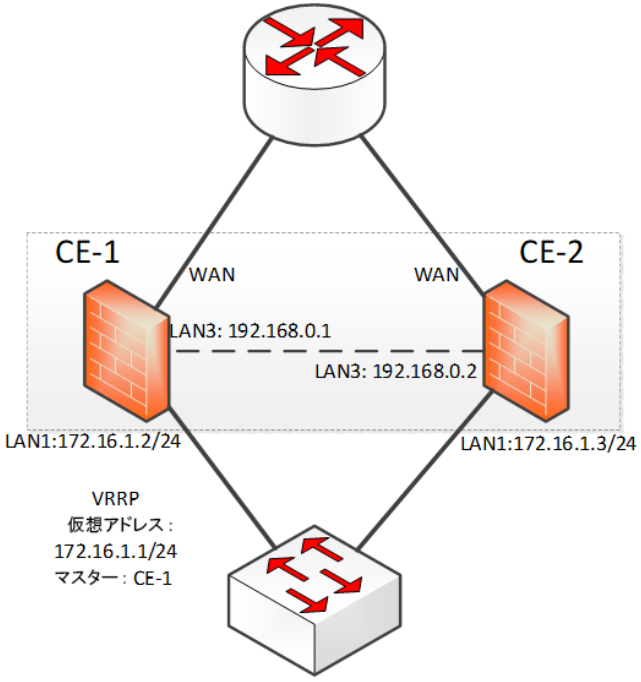
- Cloud Edge 50G2 ゲートウェイ

HA グループ - WAN トポロジ

ルートが 1 つのネクストホップ

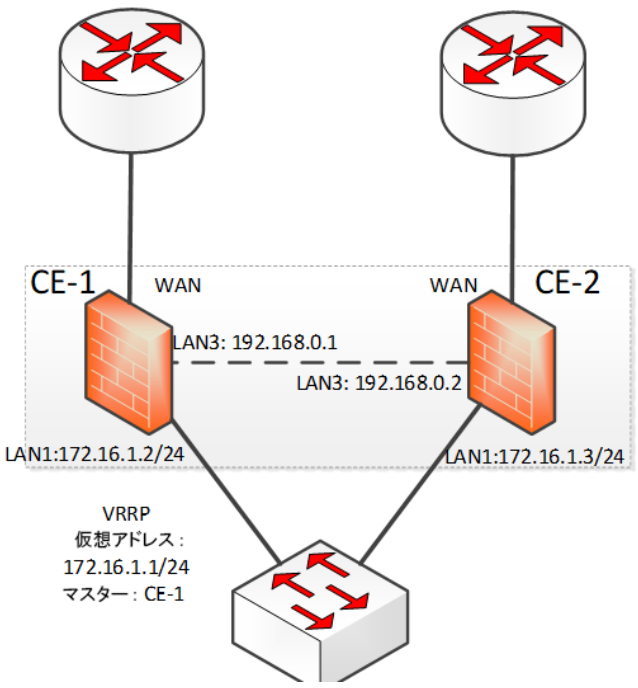
このシナリオでは、CE-1 と CE-2 が 1 つのルーターに接続されるため、CE1 の WAN インタフェース経由で受信されるパケットは、CE-2 から受信されるパケ

ットと同じサブネットに存在できません。このようなシナリオでは、NAT を有効にする必要があります。



ルーターが 2 つのホップ

このシナリオは問題ありません。



HA グループ – フェイルオーバーの条件

Cloud Edge HA グループを使用する場合、HA グループのフェイルオーバーが発生する条件を理解する必要があります。この条件には以下が含まれます。

- 1 つまたは複数の監視インタフェースが停止している
- ハートビートまたは Ping のテイクオーバーしきい値に達した
- アクティブなゲートウェイがファームウェアのアップデートを実行
- アクティブなゲートウェイの交換
- 強制テイクオーバー

HA グループが異常な状態になっている場合、強制テイクオーバーは行われません。

強制テイクオーバーが実行されると、プライマリはスタンバイになり、セカンダリがアクティブになります。

HA グループ – ハートビートインタフェース

Cloud Edge HA グループの作成時に、各 HA ピアの 1 つのインタフェースをハートビートインタフェースとして指定します。このインタフェースの選択は HA グループの作成中に行います。

- ハートビートインタフェースは L3 インタフェースである必要があります。
- ハートビートインタフェースには各ゲートウェイで同じインタフェースを使用する必要があります (例: LAN2 と LAN2、または LAN3 と LAN3)。
- 2 つのハートビートインタフェースは互いに (スイッチを介さず) 直接接続されている必要があります。
- ハートビートインタフェースは、LAN トラフィックインタフェースなどの他の目的には使用できません。
- ハートビートインタフェースに IPv4 アドレスおよびネットマスクを設定する必要があり、IPv4 アドレスは同じサブネット上になくてはなりません。
- インタフェースがハートビートインタフェースとして選択された後は、ゲートウェイ IP アドレスを含め、そのインタフェースの設定は変更できません。

スプリットブレイン状態の管理

- Cloud Edge では、HA グループのハートビートに 1 つのインタフェースのみが使用されるため、ハートビート接続の問題によってスプリットブレインと呼ばれる状態が発生する可能性があります。Cloud Edge でこの状態に対処する必要があります。
- スプリットブレイン: スプリットブレイン状態はクラスタパーティションの結果として発生します。クラスタパーティションでは、どちらの側

も相手が停止していると判断し、相手側にすでにリソースがないものとしてリソースを引き継ぎます。

HA グループ – VRRP グループ

Cloud Edge HA グループの作成時に、HA グループ設定の一部として VRRP (Virtual Router Redundancy Protocol) グループが作成されます。

- WAN 側はルーターに直接接続する可能性があるため、Cloud Edge では LAN 側の仮想 IP アドレスのみサポートされます。プライマリゲートウェイとセカンダリゲートウェイには個別の WAN 設定があります。
- 設定に応じて、L3 物理インタフェースまたは静的 L3 VLAN インタフェースのいずれかを選択できます。
  - 両方のゲートウェイが未登録: 物理インタフェースのみ選択できます
  - 両方のゲートウェイが登録済み: 物理インタフェースまたは VLAN インタフェースのいずれかを選択できます

    VLAN インタフェースは両方のゲートウェイに存在する必要があります。
  - プライマリゲートウェイが登録済み、セカンダリが未登録: 物理インタフェースのみ選択できます
  - 物理インタフェース/VLAN インタフェースは 1 つの VRRP グループでのみ使用できます。
  - WAN インタフェースは VRRP グループでは使用できません。
- VRRP グループでは、IPv4 仮想 IP アドレスのみがサポートされています。

HA グループ - エンドポイントのネットワークアクセス

HA グループを介したエンドポイントへのネットワークアクセスを提供するには、次のいずれかの方法を使用します。

- 動的アドレス指定

1. Cloud Console または On-Premises Console で、HA グループ内のプライマリゲートウェイとセカンダリゲートウェイの両方について VRRP グループインタフェースの DHCP サービスを設定します。

   注意

   DHCP サービスのゲートウェイアドレスには、VRRP グループの仮想 IP アドレスを指定する必要があります。

   インタフェースの DHCP 設定は、HA グループ内のプライマリゲートウェイとセカンダリゲートウェイで同じにする必要があります。

   詳細については、143 ページの「DHCP」を参照してください。

2. エンドポイントで、DHCP からアドレスを取得するようエンドポイントを設定します。

- 静的アドレス指定

  1. エンドポイントで、VRRP グループインタフェースと同じサブネット内に配置されるよう IP アドレスとサブネットマスクを設定します。
  2. エンドポイントで、VRRP グループの仮想 IP アドレスと同じになるようゲートウェイアドレスを設定します。

HA グループ – 監視インタフェースとテイクオーバーの実行

Cloud Edge HA グループの作成時に、フェイルオーバー条件に一致するかどうかを判断するための基本的なインタフェースとプロトコルの監視に使用される監視インタフェースを設定します。また、ハートビートと Ping のテイクオーバーを実行するための、テイクオーバーしきい値を設定できます。

- 監視インタフェース: Cloud Edge では、選択された物理インタフェース (WAN および一部の LAN ポート) に対し基本的なターゲット追跡が実行されます。すべての使用可能な物理インタフェースを監視するよう選択することをお勧めします。
- 監視 IP/FQDN: 選択した監視インタフェースごとに、監視する IP アドレスまたは FQDN を最大 2 つ入力できます。
- テイクオーバーのトリガ: Cloud Edge により、ハートビートと Ping のしきい値が追跡されます。

いずれかのテイクオーバーのトリガに一致したときに引き継ぎが開始されます。

2 つの監視ホストが設定されている場合、両方のホストへの Ping が失敗するとテイクオーバーが実行されます。2 つのホストのうち 1 つに対する Ping が失敗した場合、テイクオーバーは実行されません。監視ホストが 1 つしかない場合、そのホストの Ping しきい値に達するとフェイルオーバーが実行されます。

HA グループ – 設定マトリクス

以下のマトリクスに、Cloud Edge で HA グループの設定を管理する方法についての情報を示します。

以下の機能は、各ゲートウェイで個別に設定します。「はい」は Cloud Edge Cloud Console で設定を行えることを意味します。

機能	プライマリ	スタンバイ	詳細
ゲートウェイ情報 – 一般 (ステータス、ログ/イベント、ツール)	はい	はい	
ゲートウェイ情報 – 詳細 (コンサバティブモード設定)	はい	はい	
インタフェース	はい	はい	ハートビートインタフェース設定はインタフェースページではなく、HA グループを介してのみ。
管理アクセス	はい	はい	
DHCP	はい	はい	
動的 DNS	はい	はい	
ルーティングテーブル	はい	はい	
静的ルート	はい	はい	

機能	プライマリ	スタンバイ	詳細
NAT	はい	はい	
帯域幅制御	はい	はい	
L2TP VPN	はい	はい	
SSL VPN	はい	はい	
サイト間 VPN	はい	はい	
エンドユーザ管理 – 一般設定	はい	はい	
LDAP 設定	はい	はい	
アップデート	はい	はい	[インストール済みのアップデート] は短時間、同じでなくなる可能性があります。
VBBSS エンドポイント保護 (一般)	はい	はい	
VBBSS エンドポイント保護 (トラブルシューティング)	はい	はい	
不審エンドポイント (一般)	はい	はい	
不審エンドポイント (トラブルシューティング)	はい	はい	
診断ファイル	はい	はい	
パケットの取り込み	はい	はい	
非表示ページ	はい	はい	

HA グループ – ポリシー設定マトリクス

ポリシーが HA グループ内のゲートウェイとどのように連携しているかを理解する必要があります。

ポリシー設定	詳細
ポリシールール、インタフェースグループ、または許可/ブロックリストが設定されたとき、ゲートウェイは HA グループに含まれなかった。	プライマリの設定が HA ペアに適用されます。セカンダリの古いポリシーは使用されません。
ポリシールール、インタフェースグループ、または許可/ブロックリストを設定する前に、ゲートウェイがすでに HA グループに含まれている。	ポリシールールと許可/ブロックリストは、プライマリまたはセカンダリに対してではなく、HA ペアに対して設定されます。 ポリシールールでインタフェースグループを選択する場合、そのルールに対して、1 つのスタンドアロンゲートウェイまたは 1 つの HA ペアのみを選択します。
HA グループ内のゲートウェイにインタフェースグループを設定できる。	プライマリゲートウェイのインタフェースグループを設定します。これは HA ペアによって使用されます。 これには、プライマリとセカンダリの VLAN および VPN 設定が同様である必要があります。 以下の注意事項に留意してください。 プライマリが登録済みでセカンダリが未登録であり、かつプライマリのポリシールールで VLAN または VPN を含むインタフェースグループが使用されている場合、これらのプライマリルールをセカンダリに正しく適用することはできません。 この場合、セカンダリを登録してから VLAN と VPN を設定し、その後にポリシー配信を実行します。
ポリシーを HA グループの両方のゲートウェイに配信する。	以下の注意事項に留意してください。 ポリシー配信が片方のゲートウェイで成功し、もう一方で失敗することがあります。

ポリシー設定	詳細
HA グループで使用されるポリシーのジオロケーションを設定できる。	以下の注意事項に留意してください。 HA グループでのフェイルオーバーの後、ポリシールールでジオロケーションが設定された特定のポリシールールが機能しない場合があります。これは、ゲートウェイの場所データベースのバージョンが異なる可能性があるためです。
HA グループの破棄後、プライマリとセカンダリの両方で、HA グループに設定されたポリシーを使用する。	以下の注意事項に留意してください。 ポリシールールにインタフェースグループが設定されている場合、このポリシールールはプライマリゲートウェイにのみ適用されます。

HA グループの制限事項

HA グループには注意が必要な制限事項があります。

制限事項	説明
NAT 接続	NAT 接続の追跡は同期されません。
スプリットブレイン問題	Cloud Edge ゲートウェイはポートに制限があります。このため、ハートビート用のポートが 1 つしかない場合があります。

HA グループ - 処理

処理	説明
	HA グループの設定を編集します。
	HA グループ内で強制テイクオーバーを実行します。 強制テイクオーバーが実行されると、プライマリがスタンバイになり、セカンダリがアクティブになります。
	HA グループを有効にします。 [すべて配信] をクリックすると HA グループが使用可能になります。

処理	説明
	HA グループを無効にします。 [すべて配信] をクリックすると HA グループが使用不可になります。
	HA グループを Cloud Edge Cloud Console から削除します。

ゲートウェイを交換する

ゲートウェイを別の Cloud Edge ゲートウェイに交換しても、Cloud Edge Cloud Console に保存されたポリシー、設定データ、およびログはすべて維持されます。ゲートウェイを交換するのは次のような場合です。

- Cloud Edge ゲートウェイが故障した。
- より高性能な Cloud Edge ゲートウェイにアップグレードする。

新しい Cloud Edge ゲートウェイがログ統計を Cloud Edge Cloud Console と同期すると、Cloud Edge Cloud Console は新しいログ統計を交換した Cloud Edge ゲートウェイのキャッシュデータとマージします。

注意

HA グループに含まれているゲートウェイは、交換前のゲートウェイと同じモデルとファームウェアバージョンのゲートウェイにのみ交換できます。

HA グループ内のゲートウェイを交換する前に、交換前のゲートウェイのハートビートインタフェースから Ethernet ケーブルを取り外し、その Ethernet ケーブルを新しいゲートウェイのハートビートインタフェースに接続してください。

重要

各ゲートウェイには、Cloud Edge Cloud Console で特定の登録済み Cloud Edge ゲートウェイに関連付けられた一意なキー (シリアル番号) があります。ゲートウェイを交換した後、古い Cloud Edge ゲートウェイは、新たにゲートウェイとして登録しない限り Cloud Edge ゲートウェイとして使用することはできません。

注意

ゲートウェイの交換後に復元されるのは、ポリシー設定のみです。

手順

1. [ゲートウェイ] に移動します。
2. 交換するゲートウェイを右クリックし、[置換] を選択します。
3. 新しい Cloud Edge ゲートウェイのシリアル番号を指定します。
4. [置換] をクリックします。
5. 古い Cloud Edge ゲートウェイをネットワークから切断します。
6. 新しい Cloud Edge ゲートウェイをネットワークに追加します。

   新しい Cloud Edge ゲートウェイが Cloud Edge Cloud Console に登録され、古い Cloud Edge ゲートウェイが Cloud Edge Cloud Console から削除されます。

ゲートウェイ情報

目的: ゲートウェイ名をクリックして、そのゲートウェイを Cloud Edge Cloud Console から管理します。

場所: ゲートウェイ > (選択したゲートウェイ)

手順

1. 選択したゲートウェイを Cloud Edge Cloud Console から管理する場合は、次の操作を実行できます。
   - [ゲートウェイ情報] セクションでの情報の確認およびタスクの実行。
     - 一般的な情報、システムステータス情報、選択したゲートウェイのログとイベントの確認。
     - ツールを使用した、ネットワーク接続に関する問題のトラブルシューティング、または高トラフィックの状況でコンサバティブモードの有効化/無効化。

- ネットワークの設定。
  - インタフェース (VLAN を含む)
  - 管理アクセス
  - DHCP
  - 動的 DNS
  - ルーティングテーブル (表示のみ)
  - 静的ルート
  - NAT
- 帯域幅制御の設定。
- ユーザ VPN の設定。
  - L2TP VPN
  - SSL VPN
- サイト間 VPN の設定。
- エンドユーザ管理の設定。
  - 一般設定
  - LDAP 設定
- LDAP の設定。
- ゲートウェイアップデートの管理。
- ネットワークアクセスコントロールの設定。
  - ウイルスバスター ビジネスセキュリティサービス (VBBSS) エンドポイント保護
  - 不審エンドポイント

一般的なゲートウェイ情報の確認

目的: 選択したゲートウェイのハードウェア、ネットワーク、登録の情報を確認します。

場所: ゲートウェイ > (選択したゲートウェイ) > ゲートウェイ情報 > 一般

手順

1. ゲートウェイの情報を確認します。

   ゲートウェイ情報

   - 表示名: ゲートウェイの名前です。ゲートウェイの名前はゲートウェイの処理で変更できます。
   - ステータス: ゲートウェイの Cloud Edge Cloud Console での現在のステータスです。
   - 前回のポリシー配信: ゲートウェイから Cloud Edge Cloud Console へアップロードされた最新のログのタイムスタンプです。
   - ポリシー配信ステータス: 前回のポリシー配信の結果です。
   - ユーザの総数: 過去 15 分間のアクティブセッションの合計ユーザ数です。

   ネットワーク設定

   - 配信モード: Cloud Edge ゲートウェイがブリッジモードとルーティングモードのどちらで配信されているかを示します。

     配信モードがソフトウェアスイッチに設定されている Cloud Edge ゲートウェイは、ブリッジモードデバイスとしてリストされます。
   - ホスト名: Cloud Edge ゲートウェイのホスト名です。
   - DNS:Cloud Edge ゲートウェイの DNS 設定です。
   - WAN:Cloud Edge ゲートウェイとサブネットマスクの設定です。
   - インタフェースステータス (ブリッジモードラベル: 仮想インタフェースステータス): インタフェースリンクの状態です。

     インタフェース上にカーソルを置くと、次のリンク情報が表示されます: リンク速度、二重化、MTU、送受信パケット数、送受信バイト数

ワイヤレスインタフェース上にカーソルを置くと、ワイヤレスインタフェースに割り当てられているニックネームと MTU が表示されます。

ハードウェアと登録

- モデル: Cloud Edge ゲートウェイのハードウェアモデルです。
- シリアル番号: 現在登録されているシリアル番号です。
- ハードディスクのパラメータ
- 登録日: Cloud Edge ゲートウェイが Cloud Edge Cloud Console に登録された日時です。
- バージョン: Cloud Edge ゲートウェイのビルド番号です。
- 工場出荷時のバージョン: Cloud Edge ゲートウェイの工場出荷時のパッケージのバージョンです。
- 稼働時間: Cloud Edge ゲートウェイのハードウェアに電源が投入されてからの稼働時間です。
- メールセキュリティステータス: Cloud Edge のメールセキュリティ検索の現在のステータスです。
  - クラウド検索が有効になっています。
  - ローカル検索が有効になっています。
  - YYYY-MM-DD hh:mm:ss TZ 以降、クラウド検索からローカル検索にフェイルバックしています。

    TZ は会社のタイムゾーンを表します。
  - メールセキュリティ対策が無効になっています。

注意

Cloud Edge ゲートウェイがオフラインのときは、「--」が表示されます。

ゲートウェイシステムステータスを確認する

目的: 選択したゲートウェイの CPU の温度、CPU 使用率、ディスク使用率、メモリ使用率の情報を確認します。手動で画面に表示されるデータを更新できます。

場所: ゲートウェイ > (選択したゲートウェイ) > ゲートウェイ情報 > ステータス

手順

1. ゲートウェイのシステムステータス情報を確認します。

   温度

   - 選択した期間での CPU の温度を確認します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 24 時間]、または [過去 7 日間] を選択できます。

   CPU 使用率

   - 選択した期間での CPU 使用率を確認します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 24 時間]、または [過去 7 日間] を選択できます。
   - 現在の CPU 使用率を確認します。

   ディスク使用率

   注意

   Cloud Edge 5.2 より前のバージョンでは、システムディスク情報のみが表示されます。

   - 選択した期間でのシステムディスク使用率を確認します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 24 時間]、または [過去 7 日間] を選択できます。
   - 選択した期間でのデータディスク使用率を確認します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 24 時間]、または [過去 7 日間] を選択できます。
   - 現在のシステムディスク使用率を確認します。

- 現在のデータディスク使用率を確認します。

メモリ使用率

- 選択した期間でのメモリ使用率を確認します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 24 時間]、または [過去 7 日間] を選択できます。
- 現在のメモリ使用率を確認します。

ゲートウェイのログとイベントを確認する

目的: ゲートウェイのネットワークイベント、システムイベント、VPN イベント、およびポリシー施行ログを確認します。手動で画面に表示されるデータを更新できます。

場所: ゲートウェイ > (選択したゲートウェイ) > ゲートウェイ情報 > ログ/イベント

手順

1. ゲートウェイのイベントログ情報を確認します。

   ログエントリに記録される情報: 日付/時刻、クライアント IP、サブカテゴリ、イベント、メッセージ

2. (任意) 次のいずれかのカテゴリを選択して結果をフィルタします。

   - システムイベント
   - ネットワークイベント
   - VPN イベント
   - ポリシー施行ログ
   - 証明書の信頼イベント

   画面の下部に、システムイベント、ネットワークイベント、および VPN イベントが表示されます。

   [ポリシー施行ログ] を選択すると、[分析とレポート - ポリシー施行] 画面が開き、結果が表示されます。

注意

VPN イベントは、VPN がサポートされている Cloud Edge ゲートウェイモデルについてのみ表示されます。

3. 次の基準を使用して、イベントの結果をさらにフィルタすることができます。

   - 期間

     選択可能な期間: 今日、過去 15 分間 (初期設定)、過去 1 時間、過去 12 時間、過去 24 時間、過去 7 日間

   - クライアント IP
   - サブカテゴリ
   - イベント

     111 ページの「イベントのカテゴリとサブカテゴリ」を参照してください。

イベントのカテゴリとサブカテゴリ

表 6-1. イベントのカテゴリとサブカテゴリ

カテゴリ	サブカテゴリ
システムイベント	ファームウェアのアップデート
	エンジン/パターンのアップデート
	システムステータス
	サービス
	デバイスアドレス
ネットワークイベント	DHCP
	インタフェース
	PPPOE
VPN イベント	L2TP

カテゴリ	サブカテゴリ
	SSL VPN
	サイト間 VPN
ポリシー施行ログ	
証明書の信頼イベント	証明書を信頼する
	証明書を信頼しない
スマートバイパスイベント	

ツールを使用したネットワーク接続のトラブルシューティング

目的: IPv4 ネットワークツールを使用して、ゲートウェイ設定の検証やゲートウェイ接続のトラブルシューティングを行います。

場所: ゲートウェイ > (選択したゲートウェイ) > ゲートウェイ情報 > ツール

手順

1. 次の手順を実行します。
   - 112 ページの「Ping テストの実行」
   - 113 ページの「Traceroute テストの実行」
   - 114 ページの「ARP の結果の取得」

Ping テストの実行

目的: Ping テストを使用して、ゲートウェイ設定の検証やゲートウェイ接続のトラブルシューティングを行います。

場所: ゲートウェイ > (選択したゲートウェイ) > ゲートウェイ情報 > ツール

手順

1. [Ping] ツールのアイコンをクリックします。
2. Ping を送信する IPv4 アドレスまたはドメイン名を入力します。
3. 任意: Ping の追加パラメータを入力します。
   - [Ping を送信するネットワークインタフェースを選択します]: 初期設定はすべてのインタフェースです。
   - [バイト数]: 初期設定は 56 です。
   - [件数]: 初期設定は 4 です。最大値は 10 です。
4. [Ping] をクリックします。
5. 画面の下部で Ping の結果を確認します。
   - 過去の Ping の結果は 2 週間保存され、現在の Ping の結果の下に表示されます。
   - 過去の Ping の結果には、最大 10 件の結果が表示されます。
   - [ツール] 画面から移動すると、結果は画面から消去されます。

Traceroute テストの実行

目的: Traceroute テストを使用して、ゲートウェイ設定の検証やゲートウェイ接続のトラブルシューティングを行います。

場所: ゲートウェイ > (選択したゲートウェイ) > ゲートウェイ情報 > ツール

手順

1. [Traceroute] ツールのアイコンをクリックします。
2. ルートを調査する IPv4 アドレスまたはドメイン名を入力します。
3. [開始] をクリックします。
4. Traceroute が完了するまで待機するか、[停止].をクリックして Traceroute を停止します。

一度に実行できる Traceroute は 1 つだけです。Traceroute の実行中に Traceroute を新たに開始するには、実行中の Traceroute を停止する必要があります。

5. ページの下部で Traceroute の結果を確認します。
   - 過去の Traceroute の結果は 2 週間保存され、現在の Traceroute の結果の下に表示されます。
   - 過去の Traceroute の結果には、最大 10 件の結果が表示されます。
   - [ツール] 画面から移動すると、結果は画面から消去されます。

ARP の結果の取得

目的: ARP の結果を取得して、ゲートウェイ設定の検証やゲートウェイ接続のトラブルシューティングを行います。

場所: ゲートウェイ > (選択したゲートウェイ) > ゲートウェイ情報 > ツール

手順

1. [ARP] ツールのアイコンをクリックします。
2. 次の手順を実行します。
   - ARP 情報を取得するには、[ARP の取得] をクリックします。
   - ゲートウェイの ARP キャッシュをクリアするには、[ARP キャッシュのクリア] をクリックします。

   注意

   この処理を実行しても、現在のページの履歴は消去されません。
3. 画面の下部で ARP キャッシュの内容を確認します。
   - 表示される情報: IPv4 アドレス、ホスト名 (該当する場合)、MAC アドレス、インタフェース
   - 最大 100 行まで表示されます。
   - [ARP の取得] をクリックし、ARP キャッシュを再度取得します。

- [ツール] 画面から移動すると、結果の履歴は画面から消去されます。

コンサバティブモードを有効/無効にする

目的: コンサバティブモードでは、トラフィックの負荷が高い場合の Cloud Edge ゲートウェイの動作を設定できます。

場所: ゲートウェイ > (選択したゲートウェイ) > ゲートウェイ情報 > [詳細]

手順

1. 目的の処理を実行します。
   - コンサバティブモードを有効にするには、[オン] をクリックします。

     処理能力を超えた場合はトラフィックをブロックします。トラフィックの負荷が下がると、自動的に検査が再開されます。
   - コンサバティブモードを無効にするには、[オフ] をクリックします。

     処理能力を超えたトラフィックは検査しません。トラフィックは検査されずに通過します。これが初期設定の オプションであり、推奨される設定です。
2. [オン] をクリックした場合は、[コンサバティブモードを有効にする] 確認画面で [有効にする] をクリックします。

ネットワーク

クラウド内のネットワーク設定を表示および編集し、登録済みゲートウェイ上のネットワークトラフィックを処理および識別します。ゲートウェイが Cloud Edge Cloud Console に登録されると、特定のネットワーク設定はクラウドに移動し、Cloud Edge On-Premises Console からは編集できなくなります。ネットワークの停止につながる重大なネットワーク設定は、On-Premises Console から編集します。

注意

- Cloud Edge のインタフェースや VLAN を設定したり、ゲートウェイの物理インタフェースまたは仮想インタフェースに関連する機能を設定したりするときには、IPv4 のみがサポートされます。

  このほか、IPv4 のみがサポートされる機能には、管理アクセス、DHCP、ダイナミック DNS、DNS、ルーティング、NAT、VPN があります。

  21 ページの「IPv6 のサポート」を参照してください。

- ルーティングモードの Cloud Edge Cloud Console では、ブリッジの追加や編集はサポートされません。
- ソフトウェアスイッチ設定は、ブリッジモードでのみサポートされ、On-Premises Console を使用して設定する必要があります。
- ワイヤレス機能を備えた Cloud Edge ゲートウェイでは、ワイヤレスインタフェースおよび関連するネットワーク機能が設定されている場合に、IPv4 のみがサポートされます。

  ワイヤレス機能がサポートされるのはルーティングモードのみです。

- 適用できないネットワーク設定があった場合は、Cloud Edge Cloud Console に理由が表示されます。
- ゲートウェイは、ネットワーク接続ステータスを使用してネットワーク情報を収集し、Cloud Edge Cloud Console に送信します。

Cloud Console に移行されるネットワーク設定

1. インタフェース
   ルーティングモード

   - インタフェースの設定と、LAN2-LAN3 インタフェースおよび管理インタフェースに対する L3 VLAN の設定

     ハードウェアスイッチチップセットを備えたゲートウェイでは、LAN2-LAN8 インタフェースと管理インタフェースを設定します。

   - ワイヤレスネットワークアクセスの設定 (ワイヤレス機能をサポートしているゲートウェイの場合)

L3 VLAN は、ワイヤレスネットワークインタフェースではサポートされていません。

ブリッジモード

- インタフェースを設定し、管理インタフェースに対してのみ L3 VLAN を設定します。

2. 管理アクセス (ゲートウェイ登録後)
   - On-Premises Console、ping、SSH、および SNMP (すべてのインタフェース) を使用するための管理アクセスの設定
3. DHCP (ルーティングモードのみ)
   - LAN2-LAN3 および管理インタフェースを DHCP サーバとして機能するように設定します。

     ワイヤレス機能を備えたゲートウェイでは、ワイヤレスネットワークが有効な場合に、メインとゲストのワイヤレスネットワークで DHCP を追加設定できます。
   - ハードウェアスイッチチップセットを備えたゲートウェイでは、LAN2-LAN8 インタフェースと管理インタフェースの DCHP を設定します。
   - 上記の物理インタフェースのサブインタフェースである L3 VLAN で DHCP を設定できます。
4. サービス - 動的 DNS
5. ルーティング (ルーティングモードのみ)
   - ルーティングテーブルの確認 (On-Premises Console でも可能)
   - 静的ルートの設定
6. NAT
7. 帯域幅制御
8. ユーザ VPN
   - SSL VPN
   - L2TP VPN

9. サイト間 VPN
10. エンドユーザ管理
    - 一般認証設定 (認証キャッシュの TTL オプション)
11. ワイヤレスネットワーク
    - メインワイヤレスネットワークとゲストワイヤレスネットワークのネットワークアクセス管理の設定
    - ワイヤレスネットワークのクライアント接続の管理
    - ワイヤレスネットワークの設定情報とトラブルシューティングログの確認

注意

ワイヤレスネットワークの設定を変更するには、On-Premises Console を使用する必要があります。

On-Premises Console に残るネットワーク設定

1. インタフェース
    - インタフェースの編集: WAN または LAN1
    - L3 VLAN の追加/編集: WAN または LAN1
    - インタフェースの有効化/無効化: LAN2-LAN3 (ハードウェアスイッチチップセットを備えたゲートウェイの場合は、LAN2-LAN7)
    - ワイヤレスネットワークインタフェース: これらのインタフェースは、インタフェースのページからは無効にできません。

      ワイヤレスインタフェースを無効にするには、On-Premises Console を使用して各ワイヤレスネットワークを無効にする必要があります。
2. DNS - IPv4 DNS サーバの設定
3. アドレス - ポリシールーティングルールで使用されるアドレスオブジェクトの確認および編集

4. ブリッジモードの設定
    - ブリッジインタフェース (br0) またはスイッチインタフェース (sw0) の設定
    - ブリッジまたはスイッチのその他の設定
5. ソフトウェアスイッチ
    - ブリッジインタフェース (br0) の設定
    - ソフトウェアスイッチのその他の設定
6. ルーティング
    - ポリシールートルールの作成
    - ルーティングテーブルの確認 (Cloud Edge Cloud Console でも可能)
7. サービス - DHCP
   DHCP サーバとして機能するようインタフェースを設定: WAN または LAN1
8. ワイヤレスネットワーク
    - メインおよびゲストのワイヤレスネットワークの有効化と設定
    - ワイヤレスネットワークのトラブルシューティングログの確認

インタフェース

Cloud Edge では、Cloud Edge ゲートウェイの L2 および L3 インタフェースが自動検出されます。

ルーティングモード

Cloud Edge でゲートウェイを登録した後、Cloud Edge Cloud Console で WAN と LAN1 インタフェースを除くすべてのインタフェースを管理する必要があります。

- インタフェースはいずれも L3 インタフェースとして IPv4 アドレスを使用して設定されます。
- LAN2-LAN3 および管理インタフェースは静的 IPv4 アドレスを使用して設定する必要があります。

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイの場合は、静的 IP アドレスを持つ LAN2-LAN8 および MGMT インタフェースを設定する必要があります。

ワイヤレス機能を備えた Cloud Edge ゲートウェイの場合は、静的 IP アドレスを持つワイヤレスネットワークインタフェースを設定する必要があります。

注意

WAN および LAN1 は Cloud Edge On-Premises Console で設定する必要があります。

ブリッジモード

ブリッジモードのインタフェースは、Cloud Edge Cloud Console では読み取り専用になっています。ブリッジインタフェース (br0) および物理インタフェースの設定と管理は、Cloud Edge On-Premises Console で行う必要があります。

- 仮想ブリッジインタフェース (br0) は、Cloud Edge でインターネットへの接続に使用される L3 インタフェースです。このインタフェースには IPv4 アドレスが割り当てられます。
- 管理インタフェースを除くすべての物理インタフェースは、L2 インタフェースとして設定されます。

  L2 物理インタフェースの MTU を設定できます。
- Cloud Edge Cloud Console で管理ポートを L3 インタフェースとして設定できます。

ソフトウェアスイッチ

ソフトウェアスイッチのインタフェースは、Cloud Edge Cloud Console では読み取り専用になっています。ソフトウェアスイッチ設定および物理インタフェースで使用するブリッジインタフェース (br0) の設定と管理は、Cloud Edge On-Premises Console で行う必要があります。

- 仮想ブリッジインタフェース (br0) は、Cloud Edge でインターネットへの接続に使用される L3 インタフェースです。このインタフェースには IPv4 アドレスが割り当てられます。

- 3 つ以上の L2 物理インタフェースをソフトウェアスイッチ設定に追加する必要があります (WAN および LAN1 と、LAN2 または LAN3 の少なくともどちらか 1 つ)。

  L2 物理インタフェースの MTU を設定できます。

- Cloud Edge Cloud Console で管理ポートを L3 インタフェースとして設定できます。

ブリッジモード (スイッチチップセット使用)

ハードウェアスイッチチップセットを備えたゲートウェイのブリッジモードのインタフェースは、Cloud Edge Cloud Console では読み取り専用になっています。ハードウェアスイッチ設定および物理インタフェースで使用するスイッチインタフェース (sw0) の設定と管理は、Cloud Edge On-Premises Console で行う必要があります。ただし、イントラネットセキュリティのレベル (内部の LAN ポート間を通過するトラフィック) に関連するスイッチインタフェース (sw0) 設定は、Cloud Edge Cloud Console で管理する必要があります。

- 仮想スイッチインタフェース (sw0) は、Cloud Edge でインターネットへの接続に使用される L3 インタフェースです。このインタフェースには IPv4 アドレスが割り当てられます。
- 管理インタフェースを除くすべての物理インタフェースは、L2 インタフェースとして設定されます。

  ゲートウェイ用に選択したイントラネットセキュリティモードの設定に応じて、物理インタフェースの特定の設定を編集できます。

- Cloud Edge Cloud Console で管理ポートを L3 インタフェースとして設定できます。

注意

すべての配信モードおよびすべての Cloud Edge ゲートウェイモデルについて、特定のインタフェースを有効または無効にできます。

127 ページの「インタフェースの有効化または無効化」

ネットワークインタフェースを管理する

目的: 選択したゲートウェイのネットワークインタフェース設定を管理します。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > インタフェース

手順

1. 次の手順によりインタフェースを管理できます。
   - ゲートウェイのネットワーク設定とリンクステータスを表で確認します。
   - 123 ページのインタフェースを編集するには、インタフェース名をクリックします。
   - 140 ページの VLAN サブインタフェースを追加するには、⊞をクリックします。

   Cloud Edge Cloud Console で変更できるインタフェースと作成できる VLAN はゲートウェイモデルと配信モードによって異なります。
2. ブリッジモードの Cloud Edge ゲートウェイまたはブリッジモードのハードウェアスイッチチップセットを備えたゲートウェイでは、次の操作を実行できます。
   - ブリッジインタフェース (br0)またはスイッチインタフェース (sw0) 設定を表示する。
   - スイッチインタフェース (sw0) をクリックして、イントラネットセキュリティモードの設定を行う。
3. 既存の VLAN では、次の操作を実行できます。
   - VLAN テーブルで VLAN 設定とリンクステータスを確認する。
   - VLAN インタフェース名をクリックして 140 ページの VLAN サブインタフェースを編集または無効/有効にする。
   - [削除] をクリックして、VLAN インタフェースを削除する。

ネットワークインタフェースを編集する

目的: 選択したゲートウェイのネットワークインタフェース設定を管理します。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > インタフェース

手順

- ゲートウェイの配信モード設定に合わせて適切な手順に従います。
  - 123 ページの「ルーティングモード: ネットワークインタフェースを編集する」
  - 124 ページの「ルーティングモード: ワイヤレスネットワークインタフェースを編集する」
  - 126 ページの「ブリッジモード: ネットワークインタフェースを編集する」

    ブリッジモード、ブリッジモード (スイッチチップセット使用)、およびソフトウェアスイッチの配信については、こちらの手順を使用してください。

ルーティングモード: ネットワークインタフェースを編集する

目的: 選択したゲートウェイのネットワークインタフェース設定を管理します。ルーティングモードのゲートウェイを登録した後、Cloud Edge Cloud Console で WAN と LAN1 インタフェースを除くすべてのインタフェースを編集する必要があります。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > インタフェース

手順

1. インタフェースの名前をクリックします。
2. インタフェース設定を行います。

ワイヤレスネットワークインタフェースの設定方法については、124 ページの「ルーティングモード: ワイヤレスネットワークインタフェースを編集する」を参照してください。

オプション	説明
種類	[L3] を選択します。 Cloud Edge Cloud Console の設定に未適用の変更がある場合には、[すべて配信] をクリックして、変更内容を有効にした後にインタフェースの種類を変更できます。
モード	このフィールドは読み取り専用であり、モードはあらかじめ [静的] に設定されています。
IPv4 アドレス	IPv4 アドレスを指定します (例: `10.10.10.23`)。
IPv4 ネットマスク	Ipv4 サブネットマスクを指定します (例: `255.255.254.0`)。
IPv4 デフォルトゲートウェイ	IPv4 デフォルトゲートウェイを指定します (例: `10.10.10.1`)。インターネットに接続するインタフェースにのみ、この設定を適用します。
MTU	576〜1500 の値を指定します。
MSS	[上書き] を選択し、536〜1460 の値を指定します。 注意 MSS 値は、(MTU - 40) 以下の値にする必要があります。

3. [保存] をクリックします。

ルーティングモード: ワイヤレスネットワークインタフェースを編集する

目的: 選択したゲートウェイのワイヤレスネットワークインタフェース設定を管理します。ルーティングモードのゲートウェイを登録した後、Cloud Edge Cloud Console ですべてのワイヤレスネットワークインタフェースを編集する必要があります。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > インタフェース

手順

1. ワイヤレスネットワークインタフェースの名前をクリックします。

   ワイヤレスネットワークインタフェースの名前は読み取り専用で、各ワイヤレスネットワークに割り当てられた SSID にあらかじめ設定されています。

2. インタフェース設定を行います。

オプション	説明
種類	このフィールドは読み取り専用であり、[種類] はあらかじめ [L3] に設定されています。
モード	このフィールドは読み取り専用であり、モードはあらかじめ [静的] に設定されています。
IPv4 アドレス	IPv4 アドレスを指定します (例: `10.10.10.23`)。
IPv4 ネットマスク	Ipv4 サブネットマスクを指定します (例: `255.255.254.0`)。
IPv4 デフォルトゲートウェイ	IPv4 デフォルトゲートウェイを指定します (例: `10.10.10.1`)。インターネットに接続するインタフェースにのみ、この設定を適用します。
MTU	576〜1500 の値を指定します。
MSS	[上書き] を選択し、536〜1460 の値を指定します。 注意 MSS 値は、(MTU - 40) 以下の値にする必要があります。 wlan インタフェースの MTU を変更する場合、それに応じて MSS を設定する必要があります (MSS 値は MTU - 40 未満です)。

3. [保存] をクリックします。

ブリッジモード: ネットワークインタフェースを編集する

目的: 選択したゲートウェイのネットワークインタフェース設定を管理します。ブリッジモードのゲートウェイ (ブリッジモードのソフトウェアスイッチバリエーションを含む) を登録した後は、Cloud Edge Cloud Console で管理インタフェースのみを編集できます。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > インタフェース

手順

1. インタフェースの名前をクリックします。
2. [静的] モード設定で、インタフェースを設定します。

オプション	説明
種類	[L3] を選択します。 Cloud Edge Cloud Console の設定に未適用の変更がある場合には、[すべて配信] をクリックして、変更内容を有効にした後にインタフェースの種類を変更できます。
モード	このフィールドは読み取り専用であり、モードはあらかじめ [静的] に設定されています。
IPv4 アドレス	IPv4 アドレスを指定します (例: `10.10.10.23`)。
IPv4 ネットマスク	Ipv4 サブネットマスクを指定します (例: `255.255.254.0`)。
MTU	576〜1500 の値を指定します。
MSS	[上書き] を選択し、536〜1460 の値を指定します。 注意 MSS 値は、(MTU - 40) 以下の値にする必要があります。

3. [保存] をクリックします。

インタフェースの有効化または無効化

Cloud Edge ゲートウェイの特定のインタフェースは、配信モードに応じて、初期設定で有効または無効にされています。特定の設定では、一部のインタフェースを無効にすることができない場合があります。

注意

管理ポートはいずれの配信モードでも無効にできません。

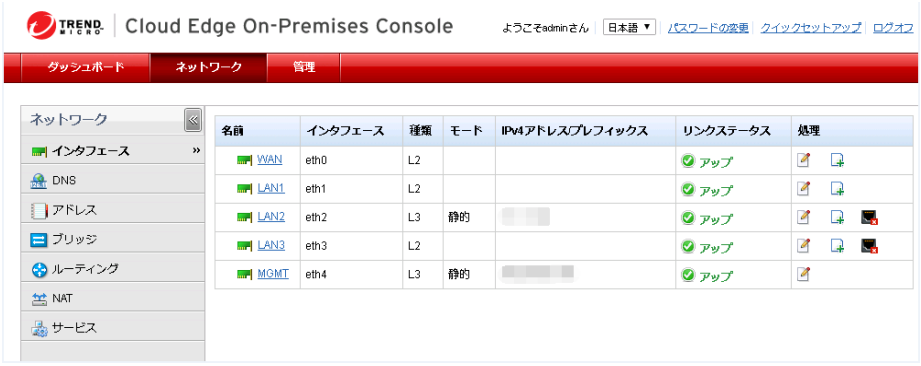


図 6-1. 例: ルーティングモードの Cloud Edge 70

Cloud Edge On-Premises Console でインタフェースを有効または無効にします。

- ルーティングモード: LAN2 および LAN3 は初期設定で有効になっています。

  これらのインタフェースは、いつでも無効にしたり再度有効にしたりできます。

- ブリッジモード: LAN2 および LAN3 は初期設定で無効になっています。

  これらのインタフェースは、いつでも有効または無効にできます。

- ソフトウェアスイッチ: LAN2 および LAN3 をソフトウェアスイッチインタフェースとして追加すると、それらのインタフェースは自動的に有効になります。

ソフトウェアスイッチ設定に含まれているインタフェースを無効にすることはできません。

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイ

図 6-2. 例: ブリッジモードの Cloud Edge 100 G2

すべてのポートは初期設定で有効になっています。WAN、LAN8、管理インタフェースは無効にすることはできません。

- ルーティングモード

  LAN1-LAN7 インタフェースを無効にすることができます。

- ブリッジモード

  WAN および LAN1-LAN8 インタフェースは、ハードウェアスイッチのポートとして自動的に選択されます。これらのポートをハードウェアスイッチの設定から削除することはできませんが、LAN1-LAN7 インタフェースを無効にすることはできます。

ワイヤレスネットワーク機能を備えた Cloud Edge ゲートウェイ

[インタフェース] ページでは、ワイヤレスネットワークインタフェースを有効にしたり、無効にしたりすることはできません。

メインワイヤレスネットワークはワイヤレスアクセスを有効にした場合に自動的に有効になり、ゲストワイヤレスネットワークはゲストワイヤレスネットワークを有効にした場合に自動的に有効になります。ワイヤレスネットワークインタフェースは、対応するワイヤレスネットワークを無効にすると自動的に無効になります。

手順

1. Cloud Edge On-Premises Console で、[ネットワーク] > [インタフェース] に移動します。
2. 次のいずれかを実行します。
   a. 有効にするインタフェースの[有効にする] アイコン ( ) をクリックします。
   b. 無効にするインタフェースの[無効にする] アイコン ( ) をクリックします。

スイッチインタフェース (sw0) を設定する

目的: ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイに対して、スイッチインタフェース (sw0) でイントラネットセキュリティを設定します。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > インタフェース > sw0

手順

1. スイッチインタフェース (sw0) 設定のリストを確認します。

   132 ページの「スイッチインタフェース (sw0) 設定のリスト」
2. [イントラネットセキュリティモード] を選択します。

オプション	説明
高セキュリティ	次のような特性があります。 • インターネット: すべてのセキュリティ検索 (ポリシールール、プロファイル、フラッド/ポート検索など) • イントラネット: すべてのセキュリティ検索 (ポリシールール、プロファイル、フラッド/ポート検索など)、ただしメール検索は除く • セキュリティ保護: パフォーマンスは最も低いが、イントラネットトラフィックのセキュリティ保護が最も高い
バランス	次のような特性があります。 • インターネット: すべてのセキュリティ検索 (ポリシールール、プロファイル、フラッド/ポート検索など) • イントラネット: 一部のセキュリティ検索 (ポリシールール、フラッド/ポート検索) • セキュリティ保護: パフォーマンスとイントラネットトラフィックのセキュリティ保護がいずれも中程度
高速	次のような特性があります。 • インターネット: すべてのセキュリティ検索 (ポリシールール、プロファイル、フラッド/ポート検索など) • イントラネット: セキュリティ検索なし • セキュリティ保護: パフォーマンスは最も高いが、イントラネットトラフィックのセキュリティ保護はない

3. (高セキュリティおよびバランスモードのみ) [異常検知] が必要な設定になっていることを確認します。

重要

これは IPS 保護が有効になっているかどうかの情報を提供する読み取り専用のフィールドです。異常検出は IPS の機能です。異常検出を使用するには、このゲートウェイに適用されているゲートウェイプロファイルの IPS ページで IPS を有効にする必要があります。Cloud Edge でフラッドおよびポート検索保護を提供するには、その前に異常検出を有効にしておく必要があります。

4. (高セキュリティおよびバランスモードのみ) 有効にする [フラッドルール] を選択し、初期設定のしきい値を変更する必要がある場合は各フラッドルールのしきい値を変更します。

   フラッド攻撃から保護するために、すべてのフラッドルールが初期設定で有効になっています。

オプション	説明
TCP SYN フラッド	初期設定しきい値: 8000
ICMP フラッド	初期設定しきい値: 8000
UDP フラッド	初期設定しきい値: 8000
IGMP フラッド	初期設定しきい値: 8000

5. (高セキュリティおよびバランスモードのみ) 有効にする [ポート検索ルール] を選択し、初期設定のしきい値を変更する必要がある場合は各ルールのしきい値を変更します。

   ポート検索攻撃から保護するために、すべてのポート検索ルールが初期設定で有効になっています。

オプション	説明
UDP ポート検索	初期設定しきい値: 1000
TCP ポート SYN 検索	初期設定しきい値: 1000
TCP ポート FIN 検索	初期設定しきい値: 1000
TCP ポート NULL 検索	初期設定しきい値: 1000

オプション	説明
TCP ポート Xmas 検索	初期設定しきい値: 1000

6. [保存] をクリックします。

スイッチインタフェース (sw0) 設定のリスト

スイッチインタフェース (sw0) を設定する前に、利用できる設定を確認しておく必要があります。設定には Cloud Edge On-Premises Console を使用して行うものと、Cloud Edge Cloud Console を使用して行うものがあります。

Cloud Edge Cloud Console は、イントラネットセキュリティモードの設定を行うのに使用します。このモードの設定では、LAN 間のイントラネットトラフィックで実現されるセキュリティのレベルを調節します。

各イントラネットセキュリティモードで実現されるセキュリティ保護の詳細については、134 ページの「各イントラネットセキュリティモードで提供されるセキュリティ保護」を参照してください。

高セキュリティモードおよびバランスモード

表 6-2. Cloud Edge Cloud Console を使用して設定

設定	説明
イントラネットセキュリティモード	内部ネットワークのネットワークセキュリティのレベルを設定します。 • 高セキュリティモード • バランスモード • 高速モード
異常検知	このゲートウェイに適用されているゲートウェイプロファイルで IPS が有効かどうかを表示する読み取り専用フィールド。 フラッドルールおよびポート検索ルールを使用するよう IPS が有効化されている必要があります。
フラッドルール	フラッドからのネットワーク IPS 保護を提供します。

設定	説明
ポート検索ルール	ポート検索からのネットワーク IPS 保護を提供します。

表 6-3. Cloud Edge On-Premises Console を使用して設定

設定	説明
モード	DHCP または静的
MTU	範囲: 576〜1500 初期設定: 1438
管理アクセス	ゲートウェイが登録されていない場合にのみ使用できます。
詳細設定: スパニングツリープロトコルを有効にする	冗長パスがあるネットワークでのループの発生を防ぎます。
詳細設定: IGMP スヌーピング	IGMP トラフィックを監視し、目的のエンドポイントにのみ IGMP トラフィックを転送します。

高速モード

表 6-4. Cloud Edge Cloud Console を使用して設定

設定	説明
イントラネットセキュリティモード	内部ネットワークのネットワークセキュリティのレベルを設定します。 • 高セキュリティモード • バランスモード • 高速モード

表 6-5. Cloud Edge On-Premises Console を使用して設定

設定	説明
モード	DHCP または静的

設定	説明
MTU	範囲: 576〜1500 初期設定: 1438
管理アクセス	ゲートウェイが登録されていない場合にのみ使用できます。
詳細設定: スパニングツリープロトコルを有効にする	冗長パスがあるネットワークでのループの発生を防ぎます。

各イントラネットセキュリティモードで提供されるセキュリティ保護

ビジネスの要件を満たすセキュリティ保護を使用してゲートウェイを設定できるよう、スイッチインタフェース (sw0) を設定する前に、それぞれのイントラネットセキュリティモードで提供されるセキュリティ保護の内容を確認することができます。

各イントラネットセキュリティモードで提供されるセキュリティ保護のマトリクス

	高セキュリティ		バランス		高速	
	インターネット	イントラネット	インターネット	イントラネット	インターネット	イントラネット
不正プログラム対策	はい	はい	はい	いいえ	はい	いいえ
IPS	はい	はい	はい	フラッド制御およびポート検索スイッチ設定に表示される IPS に限定	はい	いいえ
その他のセキュリティ機能	はい	はい	はい	いいえ	はい	いいえ

注意

- 「その他のセキュリティ機能」には、セキュリティプロファイルに属するすべての機能のほか、許可リストとブロックリストが含まれます。
- イントラネットネットワークに対するメール検索は、どのイントラネットセキュリティモードでもサポートされません。

VLAN の仕組み

VLAN (Virtual Local Area Network) とは、エンドポイント、サーバ、およびその他のネットワークデバイスをグループ化して、その物理的な場所にかかわらず、同じ LAN セグメント上に存在するかのようにデバイス間通信を行う技術のことです。物理配置が異なるエンドポイントやサーバであっても、同じ VLAN に属することができます。

VLAN は、デバイスを物理的ではなく論理的に分離します。各 VLAN はブロードキャストドメインとして扱われます。VLAN 1 に属するデバイスは、同じ VLAN 1 に属する他のデバイスと直接通信することができますが、他の VLAN に属するデバイスにはルータ経由で通信する必要があります。VLAN 上のデバイス間の通信は、物理的なネットワークとは別のものです。

VLAN では、VLAN に属するデバイスで送受信されるすべてのパケットに `802.1Q` VLAN タグを追加することでデバイスを分離します。VLAN タグは、VLAN 識別子などの情報が含まれた 4 バイトの拡張フレームです。

VLAN で Cloud Edge を配置する方法

次の情報を参照し、Cloud Edge が L3 VLAN をどのようにサポートしているかを確認してください。

- L3 VLAN のみがサポートされます。

  注意

  L2 VLAN は、どの配信モードやモデルでもサポートされません。

- Cloud Edge は 4096 VLAN タグが付いた 50 VLAN サブインタフェースをサポートしています。
- VLAN を設定する場所:

  - Cloud Edge Cloud Console: eth0 と eth1 を除くすべてのインタフェース (その配信モードとモデルでサポートされている場合)
  - On-Premises Console: eth0 と eth1 (その配信モードでサポートされている場合)
- VLAN を編集または変更するときの注意事項:
  - VLAN モードは静的または DHCP のいずれかです。
  - VLAN で DHCP が有効になっている場合、その VLAN は編集できません。
  - VLAN で DHCP が有効になっているか、NAT が使用されている場合、その VLAN は削除できません。
- ポリシールールの作成時およびインタフェースグループポリシーオブジェクトの作成時に、VLAN インタフェースを追加できます。
- 配信モードに固有の情報については、以下を参照してください。
  - 136 ページの「ブリッジモードの VLAN」
  - 139 ページの「ルーティングモードの VLAN」

ブリッジモードの VLAN

次の情報を参照し、Cloud Edge がブリッジモードで VLAN をどのようにサポートしているかを確認してください。

ブリッジモードでサポートされるインタフェース

- Cloud Edge 5.3 以降のデバイス: VLAN 設定は、管理インタフェースでのみサポートされます
- 5.3 より前の Cloud Edge: VLAN 設定は、eth0 および eth1 を除くすべてのインタフェースでサポートされます
- ブリッジインタフェース (br0 または sw0): VLAN 設定はサポートされません

ブリッジモードの注意事項

ブリッジモードで VLAN を設定する場合は、特別な注意事項があります。

- Cloud Edge は、標準スイッチなどの VLAN をネイティブにサポートしていません。そのため、以下の制限があります。

  1. Cloud Edge ポートにアクセス/トランクモードを設定することはできないため、Cloud Edge では通過トラフィックへのタグ付けまたはタグ解除ができません。

  2. Cloud Edge は、異なる VLAN からブロードキャストトラフィックまたはマルチキャストトラフィックを分離できません。

- Cloud Edge は、既存の VLAN タグを保持することでのみ通過 VLAN トラフィックをサポートできます。Cloud Edge は、通過 VLAN トラフィックにすべてのセキュリティ機能を提供します。

ブリッジモードのシナリオ

Cloud Edge がトランクリンクに配信されている場合、トレンドマイクロでは、次のように 2 つの Cloud Edge ポートのみ使用することを推奨しています。

- WAN をアップストリームのトランクポートに接続します。
- LAN1 をダウンストリームのトランクポートに接続します。

重要

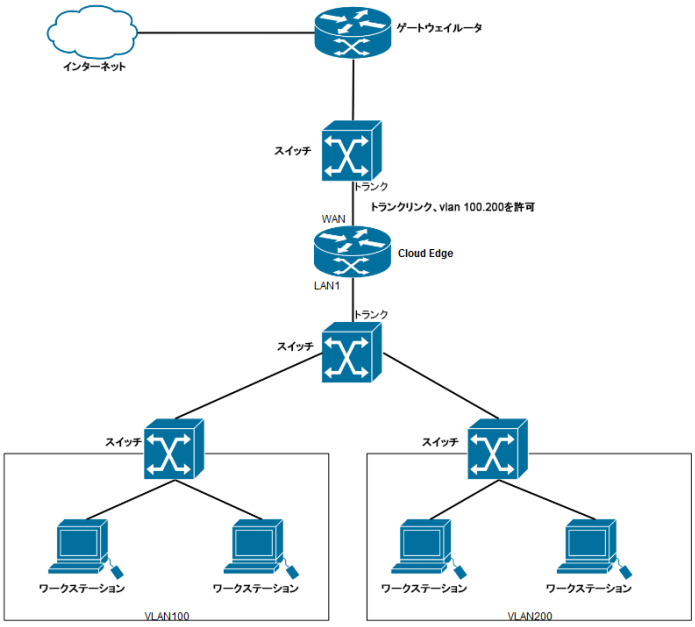
1 つのトランクリンクに 3 つ以上のポートを接続しないでください。

注意

ハードウェアスイッチチップセットを備えたゲートウェイ、またはソフトウェアスイッチモードの他のモデルを配信する場合は、WAN ポートをアップストリームのトランクポートに接続し、LAN ポートをダウンストリームのトランクポートに接続します。

次のシナリオは推奨されるブリッジモード配信を示しています。

トランクシナリオ



このシナリオで、Cloud Edge ゲートウェイを Cloud Edge Cloud Console に登録するには、ネイティブ VLAN でゲートウェイを設定する必要があります。

- トランクリンクでは、ネイティブ VLAN に属するトラフィックを除き、すべてのトラフィックに VLAN タグが付けられます。Cloud Edge ゲートウェイ自体は VLAN タグのないトラフィックのみ送信できます。
- このため、br0 が DHCP を使用して設定されている場合、ネイティブ VLAN 上に DHCP サーバとゲートウェイを設定する必要があります。br0 が静的 IP アドレスを使用して設定されている場合、ネイティブ VLAN 上にゲートウェイを設定する必要があります。

ルーティングモードの VLAN

次の情報を参照し、Cloud Edge がルーティングモードで VLAN をどのようにサポートしているかを確認してください。

ルーティングモードでサポートされるインタフェース

VLAN 設定は、eth0 と eth1 を除くすべてのインタフェースでサポートされます。

ルーティングモードの注意事項

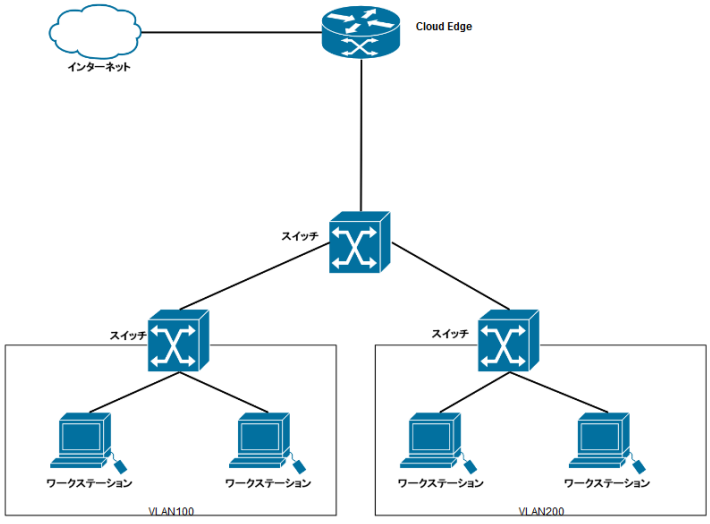
ルーティングモードで VLAN を設定する場合、特別な注意事項はありません。

ルーティングモードのシナリオ

Cloud Edge ゲートウェイがルーティングモードである場合、必要に応じて LAN インタフェース上に VLAN インタフェースを設定できます。

次のシナリオは標準的なルーティングモードの配信を示しています。

トランクシナリオ



VLAN インタフェースを追加/編集する

目的: VLAN タグ付きパケットを受信する Cloud Edge の物理インタフェースに L3 VLAN インタフェースを追加します。各 L3 VLAN インタフェースは、一意の IPv4 アドレスとネットマスクを使用して設定する必要があります。必要に応じて VLAN インタフェースを編集できます。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > インタフェース

手順

1. VLAN インタフェースを追加する前に、VLAN が Cloud Edge ゲートウェイと連携する方法について重要な情報を確認します。

   135 ページの「VLAN で Cloud Edge を配置する方法」

2. 次の手順を実行します。

   - VLAN を追加するには、[処理] 列にある VLAN 設定追加アイコン (⊞) () をクリックします。
   - VLAN を編集するには、[VLAN] セクションにある VLAN の名前をクリックします。

   [VLAN の追加/編集] ページが開きます。

   注意

   VLAN インタフェースをワイヤレスインタフェースに追加することはできません。

3. VLAN の設定を指定します。

   - 名前: VLAN インタフェースに名前を付けます。
   - 種類: L3 VLAN が自動的に表示されます。読み取り専用です。

     L2 VLAN はサポートされません。
   - モード: [DHCP] または [静的] を選択します。

     [静的] の場合は[IPv4 アドレス] および [IPv4 ネットマスク] を指定します。
   - VLAN ID: VLAN ID を指定します。VLAN ID は、この VLAN インタフェースで受信するパケットの VLAN ID と一致する必要があります。

     各 VLAN インタフェースの VLAN ID は、VLAN インタフェースに接続された IEEE 802.1Q 準拠のルータまたはスイッチによって追加される VLAN ID と一致する必要があります。VLAN ID には 1〜4094 の範囲の任意の番号を指定できます (0 と 4095 は予約されています)。

     既存の VLAN インタフェースの VLAN ID を変更することはできません。

4. [保存] をクリックします。

管理アクセス

Cloud Edge Cloud Console を使用して Cloud Edge ゲートウェイの管理インタフェースを設定することで、ゲートウェイの背後にある IPv4 デバイスから開始された特定の種類の管理サービス (トラフィック) を許可またはブロックできます。Cloud Edge ゲートウェイは、On-Premises Console、Ping、SSH、および SNMP サービスを使用した IPv4 クライアントからの管理アクセスをサポートします。

Cloud Edge ゲートウェイが Cloud Edge Cloud Console に登録されていない場合は、On-Premises Console を使用して L3 インタフェースを編集する際に管理アクセスを有効にすることができます。ゲートウェイを登録した後は、Cloud Edge Cloud Console を使用してゲートウェイへの管理アクセスを有効または無効にする必要があります。

SNMP を有効にしたら、[管理] > [デバイス管理] > [SNMP の設定] に移動し、Cloud Edge ゲートウェイの On-Premises Console を使用して SNMP を設定する必要があります。SNMP サポートを有効にして設定すると、ユーザが SNMP マネージャを使用して、サポートされるオブジェクトの情報を取得できるようになります。

ワイヤレスネットワーク機能を備えた Cloud Edge ゲートウェイでは、メインまたはゲストワイヤレスネットワークでの管理アクセスを有効にできます。ゲストワイヤレスネットワークでの管理アクセスを許可する際は、セキュリティの問題に留意する必要があります。

管理アクセスを有効にする

目的: ゲートウェイへのリモート管理アクセスを有効にします。SNMP を有効にすると、ユーザはサポートされているオブジェクトの情報を SNMP マネージャから取得できます。

場所: ゲートウェイ > (選択したゲートウェイ) > [ネットワーク] > 管理アクセス

手順

1. インタフェースで有効にするサービスを選択します。
    - On-Premises Console

- Ping
- SSH
- SNMP

2. テーブルの下のフィールドで、ゲートウェイへのリモートアクセスを許可する IPv4 アドレスを指定します。

注意

この設定により、ゲートウェイにリモートでアクセスできる IPv4 アドレス範囲が決まります。単一の IPv4 アドレスがサポートされており、範囲を表すには「-」記号を使用できます。IPv4 アドレスとネットマスクは `192.168.1.1/24` の形式で指定します。指定しない場合は、すべての IPv4 アドレスが許可されます。

管理アクセスの場合、IPv6 アドレスはサポートされません。

3. [保存] をクリックします。

DHCP

DHCP サービスは、Cloud Edge ゲートウェイの 1 つ以上の LAN インタフェースで有効にすることができます。DHCP サービスが有効になっている各インタフェースは DHCP サーバとして機能し、IPv4 アドレスや他のネットワーク設定 (デフォルトゲートウェイや DNS 設定) などを内部クライアントに割り当てます。

Cloud Edge は、DHCP サービスを使用するように設定されたインタフェースに対する DHCP 要求に自動的に応答します。

- クライアントに DNS アドレスを割り当てる際には、システムの DNS 設定やインタフェースの IPv4 アドレスを使用するように DHCP を設定することができます。または、DNS の IPv4 アドレスのリストを手動で指定することもできます。
- DHCP サーバによる DHCP クライアントへのアドレスの割り当てに使用する IPv4 アドレスプールを設定できます。
  Cloud Edge は複数のプールをサポートします。各インタフェースに対して別々の DHCP プールを作成できます。

- また、DHCP サーバごとに詳細なサーバ設定 (IPv4 アドレスの静的マッピングおよび DHCP のリース期間) を指定することもできます。

DHCP サービスを確認する

目的: DHCP 設定を確認し、管理します。

場所: ゲートウェイ > (選択したゲートウェイ) > [ネットワーク] > DHCP

手順

1. DHCP サービスに関連付けられたパラメータを確認します。

オプション	説明
有効にする	サービスの状態を示します。有効 (緑/オン) または無効 (赤/オフ) のどちらかになります。
名前	DHCP サービスの名前です (例: LAN1、LAN2)。 DHCP 設定を変更するには、インタフェース名をクリックします。
IPv4 アドレス/ネットマスク	インタフェースに割り当てられた IPv4 アドレスとサブネットマスクです。
IP プール	DHCP サービス用の IP アドレスプールの IPv4 アドレスの範囲です。
オプション	DNS サーバの IPv4 アドレス、ゲートウェイの IPv4 アドレス、およびリース期間があります。DNS の IPv4 アドレスは、DHCP サーバで指定の DNS を使用する場合にのみ表示されます。

DHCP 設定を編集する

目的: ゲートウェイの DHCP 設定を変更します。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > DHCP > 追加/編集

手順

1. 必要に応じて、以下の情報を確認します。

- 146 ページの「DHCP の配信モード情報」

  どのインタフェースを各配信モードの DHCP サーバとして設定できるのかという情報。

- 147 ページの「初期設定の DHCP IP アドレスプール」

  どのような IP アドレスが初期設定で各 IP アドレスプールに割り当てられているか。

2. DHCP 設定を行います。

オプション	説明
有効	サービスを有効にする場合に選択します。
IP アドレス/ネットマスク	インタフェースに割り当てられた IPv4 アドレスとサブネットマスクです。
優先 DNS	優先する DNS 方式を選択します。 • [ネットワーク] > [DNS] で設定されているシステムの DNS を使用する場合は、[システムの DNS 設定を使用する] を選択します。 • インタフェースの IPv4 アドレスを DNS として使用する場合は、[インタフェースの IP アドレスを使用する] を選択します。 • IPv4 アドレスを DNS 設定として手動で設定する場合は、[指定した DNS サーバを使用する] を選択します。
ゲートウェイ	インタフェースの IPv4 アドレスおよびネットマスクの設定に基づいて、DHCP サーバのゲートウェイが自動的に入力されます。必要に応じてゲートウェイの IPv4 アドレスを変更することもできます。
IP アドレスの開始値/終了値	IPv4 アドレスの範囲を指定して、DHCP 設定が適用される IP アドレスプールを作成します。

3. [詳細設定] で詳細を設定します。

   - [リース期間] で、リースされた IPv4 アドレスおよびネットマスクの有効期限の日時を調整します。

     日数、時間数、または分数を指定します。たとえば、時間のみを指定した場合、リースは設定した時間数に制限されます。

- 静的マッピングを使用して、静的 IPv4 アドレスを特定の MAC アドレスに手動でバインドできます。

  [静的マッピング] で、MAC アドレス/IPv4 アドレスマップを指定します。複数のマップをカンマで区切って入力できます。例:

  ```
  00-FF-8A-B9-5A-49 / 192.168.1.1, 00:0C: 29:A9:69:25 /
  192.168.2.1
  ```

4. [保存] をクリックします。

DHCP の配信モード情報

各配信モードの DHCP サービスをどのインタフェースで設定できるかを理解する必要があります。

- ブリッジモード: 管理インタフェースが、DHCP サーバとして設定できる唯一のインタフェースです。

  ソフトウェアスイッチ: 初期設定では、管理インタフェースを除くすべてのインタフェースが L2 インタフェースであり、ソフトウェアスイッチの一部です。WAN、LAN1、および LAN2 インタフェースがスイッチ設定に含まれていなければなりません。

  必要な場合は、スイッチ設定から LAN3 を削除できます。ソフトウェアスイッチ設定から LAN3 インタフェースを削除した後は、それを L3 インタフェースに変更し、IPv4 アドレスを割り当て、そのインタフェースで DHCP サービスを有効にすることができます。

- ルーティングモード: 有効化済みの L3 インタフェースは、すべて DHCP サーバとして設定できます。

ハードウェアスイッチチップセットを備えたゲートウェイの配信モード情報

- ブリッジモード: 管理インタフェースが、DHCP サーバとして設定できる唯一のインタフェースです。

  管理インタフェースを除くすべてのインタフェースが L2 インタフェースであり、スイッチ設定の一部です。これらはスイッチ設定から削除できず、DHCP サーバとして設定することもできません。

- ルーティングモード: 有効化済みの L3 インタフェースは、すべて DHCP サーバとして設定できます。

ワイヤレスネットワーク機能を備えたゲートウェイの配信モード情報

- ブリッジモード: 管理インタフェースが、DHCP サーバとして設定できる唯一のインタフェースです。
- ルーティングモード: L3 インタフェースは、すべて DHCP サーバとして設定できます (メインおよびゲストのワイヤレスネットワークインタフェースを含む)。

  ワイヤレスネットワークインタフェースで DHCP サービスが初期設定で有効になります。初期設定では、ワイヤレスネットワークを有効化すると、インタフェースで DHCP サービスが有効になります。

  ただし、ワイヤレスネットワークを有効にする前にワイヤレスインタフェースの DHCP サービスを無効にし、後でワイヤレスネットワークを有効にした場合、ワイヤレスネットワークを有効にしても DHCP サービスは有効になりません。この場合は、そのワイヤレスインタフェースの DHCP サービスを手動で有効にする必要があります。

初期設定の DHCP IP アドレスプール

Cloud Edge では、特定の L3 インタフェースに初期設定の DHCP IP アドレスプールが割り当てられます。

初期設定の DHCP IP アドレスプール

インタフェース	インタフェース名	IP アドレスプール
eth0	WAN	該当なし
eth1	LAN1	192.168.100.1/24
eth2	LAN2	192.168.101.1/24
eth3	LAN3	192.168.102.1/24
eth4	管理	192.168.103.1/24

ハードウェアスイッチチップセットを備えたゲートウェイの初期設定の DHCP IP アドレスプール

インタフェース	インタフェース名	IP アドレスプール
eth0	WAN	該当なし
eth1	LAN1	192.168.100.1/24
eth2	LAN2	192.168.101.1/24
eth3	LAN3	192.168.102.1/24
eth4	LAN4	192.168.103.1/24
eth5	LAN5	192.168.104.1/24
eth6	LAN6	192.168.105.1/24
eth7	LAN7	192.168.106.1/24
eth8	LAN8	192.168.107.1/24
eth9	管理	該当なし

ワイヤレスネットワーク機能を備えたゲートウェイの初期設定の DHCP IP アドレスプール

ワイヤレスインタフェース	インタフェース名	IP アドレスプール
wlan0	<WIRELESS_SSID>	192.168.201.1/24
wlan1	<GUEST_WIRELESS_SSID>	172.16.20.1/24

動的 DNS

動的ドメインネームシステム (DDNS) は、インターネットの DNS サーバをリアルタイムに自動更新し、ホスト名、アドレス、およびその他の情報のアクティブな DNS 設定を最新の状態に維持します。一般には、PPPoE や DHCP を使用してインターネットアクセスを取得するなど、業務でパブリックのホスト名と IP アドレスのマッピングを頻繁に変更する場合に使用されます。

ユーザがインターネット上の他のユーザに Web サービスなどのサービスを提供する場合に、動的 IP アドレスでは問題が生じます。IP アドレスが頻繁に変わる可能性があるため、既知の URL を使用してアクセスできる状況を維持するためには、対応するドメイン名を DNS で迅速に再マッピングする必要があります。多くのプロバイダが、このシナリオに対応するために有料または無料の DDNS サービスを提供しています。ソフトウェアを実行して DDNS サービスを更新する自動再構成機能は、通常はユーザのルータまたはコンピュータに実装されます。これまでに Web ベースの標準的な更新手段もいくつか開発されていますが (RFC 2136 その他のプロトコル)、ユーザの機器とプロバイダ間の通信は標準化されていません。

DDNS を使用すると、新しいホスト名と IP アドレスのマッピングがインターネットで自動的に伝播されます。DDNS サービスプロバイダは、この処理を管理する仲介役として機能します。Cloud Edge ゲートウェイは、外部クライアントがインターネット経由で企業サイトにアクセスする際に最初に接続するデバイスとして設計されています。すべてのインターネットユーザから企業側の各ホスト/ドメインに向けて発信されるトラフィックは、必ず Cloud Edge を通過する必要があります。Cloud Edge では、DDNS クライアントを使用して、ホスト名と IP アドレスのマッピングの変更を DDNS サービスプロバイダに伝達できます。

サポートされる DDNS サービスプロバイダ

次の 3 つの DDNS サービスプロバイダをサポートしています。

プロバイダ	サービス提供地域
Dyn DNS	グローバル
Free DNS	
DNSPod	中国

注意

IPv6 はサポートされていません。

動的 DNS の設定を行う

目的: 各サービスベンダーに応じた基本設定を行います。必要な情報は、サービスにより異なります。基本的に、各サービスにはドメイン名、アカウント、およびパスワード情報が必要となります。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > 動的 DNS

手順

1. [動的 DNS を有効にする] をオンにします。
2. [ベンダー] を選択します。

   使用可能なベンダーは、DynDNS、FreeDNS、および DNSPod です。

   ゲートウェイに Cloud Edge 5.5 よりも前のバージョンがインストールされている場合は、[ベンダー] ドロップダウンリストで [DNSPod] オプションは選択できません。
3. 次の手順を実行します。
   - DynDNS または FreeDNS の場合、[ユーザ名] と [パスワード] を入力します。
   - DNSPod の場合、[ユーザ ID] と [ユーザトークン] を入力します。
4. ドメイン情報を入力します。
   - DynDNS または FreeDNS の場合、[ドメイン] に FQDN を入力します。
   - DNSPod の場合、[ホストレコード] にホスト名を入力し、[ドメイン] にドメイン名を入力します。
5. WAN インタフェースを選択します。

自動:	(初期設定) RFC 1597 に従って、非プライベート IP アドレスとのインタフェースを自動検出します。
(インタフェース名):	WAN や LAN1 など、使用可能なインタフェースのリストから WAN インタフェースを選択します。

6. [ベンダー] に [DynDNS] を選択した場合は、HTTPS を有効にします (オプション)。

DynDNS では HTTPS 接続がオプションとして提供されます。その他のベンダー (FreeDNS など) では、HTTPS インタフェースは公開されていません。一方、DNSPod では HTTPS 接続が必須です。

7. [保存] をクリックします。

DDNS ステータスを確認する

目的: 現在の DDNS の実行ステータスを確認します。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > 動的 DNS > ステータス

手順

1. DDNS ステータスメッセージを確認します。

   151 ページの「DDNS ステータスメッセージ」を参照してください。

DDNS ステータスメッセージ

[動的 DNS] > [ステータス] タブには、現在のインタフェース (自動検出または指定)、WAN の IP アドレス、およびステータスメッセージなどの現在の DDNS の実行ステータスが表示されます。

ステータスメッセージには次のものがあります。

- 成功
- エラー: 認証に失敗しました
- エラー: アカウントがアクティベートされていません
- エラー: ドメイン情報が無効または未登録です
- エラー: インターネットにアクセスできないか、またはサービスベンダーに接続できません
- エラー: HTTPS 接続サービスなどの有料機能を使用しました。関連する設定がリセットされました
- エラー: サービスベンダーから「サービスは利用できません」というメッセージを受け取りました

- エラー: 利用可能な WAN IP が検出されませんでした
- エラー: 指定されたインタフェースには該当する IP がありません
- エラー: サービスインタフェースが変更になった可能性があります。トレンドマイクロに連絡してアップデートしてください
- エラー: 認証エラーが所定の回数を超えたため、アカウントは一時的にロックされました
- エラー: サブドメイン情報が無効または未登録です
- エラー: ラウンドロビン方式でのホストのアップデートは許可されていません
- エラー: 不明なエラー。インターネットアクセスを確認してください
- 有効ではありません

ルーティングテーブル

工場出荷時の初期設定の Cloud Edge ルーティングテーブルには、初期設定の IPv4 静的ルートが 1 つ含まれています。追加の IPv4 静的ルートを定義し、ルーティング情報をルーティングテーブルに追加します。テーブルには、同じ送信先へのルートを複数定義できます。これらのルートに指定されているネクストホップルータの IPv4 アドレス、またはこれらのルートに関連付けられている Cloud Edge インタフェースは同じとはかぎりません。

Cloud Edge は、ルーティングテーブル内の情報を評価し、送信先への最適なルートを選択します。通常は、Cloud Edge ゲートウェイと、最も近くに位置するネクストホップルータとの最短距離が選択されます。ただし、最適なルートが利用できない場合は最短でないルートが選択されることがあります。Cloud Edge は、ユニットのルーティングテーブルのサブセットであるユニットの転送テーブルに利用可能な最適ルートをインストールします。パケットは転送テーブルの情報に従って転送されます。

注意

Cloud Edge では IPv6 ルーティングはサポートされません。

ルーティングテーブルを確認する

目的: ルーティングテーブルを表示し、異なる送信元からの IPv4 ネットワークトラフィックがどのように送信先に送られるかを確認します。これらのル

ートに指定されているネクストホップルータの IPv4 アドレス、またはこれらのルートに関連付けられている Cloud Edge インタフェースは同じとはかぎりません。

場所: ゲートウェイ > (選択したゲートウェイ) > ネットワーク > ルーティングテーブル

手順

1. テーブルのインジケータを確認します。

   153 ページの「ルーティングテーブルのインジケータ」を参照してください。

ルーティングテーブルのインジケータ

次の表に、ルーティングテーブルインジケータとその説明を示します。

コード	定義
K	カーネルルート
C	接続済み
S	静的

静的ルート

静的ルートでは、パケットの宛先 IP アドレスに応じてトラフィックを転送します。IPv4 静的ルートを定義すると、特定の転送先にパケットを転送するために必要な情報が Cloud Edge に与えられます。IPv4 静的ルートを設定するには、Cloud Edge ゲートウェイが傍受するパケットの宛先 IPv4 アドレスおよびネットマスクを定義し、これらのパケットのゲートウェイ IPv4 アドレスを指定します。ゲートウェイアドレスは、トラフィックがルーティングされるネクストホップのルータを指定します。

パケットの出口となるインタフェースや、パケットのルーティング先のデバイスを指定できます。[ゲートウェイ] > (ゲートウェイ名) > [ネットワーク] > [静的ルート] の静的ルートのリストには、Cloud Edge ゲートウェイがパケットをルーティングするためにパケットヘッダと比較する情報が示されます。

静的ルートを追加する

新しい IPv4 静的ルートを追加すると、一致するルートおよび送信先が Cloud Edge のルーティングテーブル内にあるかどうかが Cloud Edge で確認されます。見つからなかった場合、そのルートがルーティングテーブルに追加されます。

注意

ルーティングモードでは IPv6 がサポートされていないため、設定できるのは IPv4 静的ルートのみです。

手順

1. [ゲートウェイ] > (ゲートウェイ名) > [ネットワーク] > [静的ルート] に移動します。
2. [追加] をクリックしてデフォルトルートを追加します。

   [静的ルートの追加/編集] 画面が表示されます。
3. [静的ルートを有効にする] を選択します。
4. [送信先ネットワーク] で、ネットワークアドレスを指定します。

   次のいずれかを指定できます。

   - IP アドレス
   - デフォルトゲートウェイ (例: `10.10.10.10/16`)

     注意

     デフォルトゲートウェイが複数設定されている場合、送信トラフィックはラウンドロビン方式でそれらのゲートウェイからルーティングされます。
   - ビットマスク

     注意

     ビットマスクはネットマスクの 10 進表記です。

- CIDR (Class InterDomain Routing) 表記 (例: `255.255.255.0/24`)

5. [ネクストホップ] で、ネクストホップの IPv4 アドレスを指定します。
6. [保存] をクリックします。

静的ルートを有効化/無効化する

手順

1. [ゲートウェイ] > (ゲートウェイ名) > [ネットワーク] > [静的ルート] に移動します。
2. 静的ルートのリストで、次のいずれかを行います。
   - 静的ルートを有効にするには、[有効] アイコンをオン () にします。
   - 静的ルートを無効にするには、[有効] アイコンをオフ () にします。

静的ルートを変更する

手順

1. [ゲートウェイ] > (ゲートウェイ名) > [ネットワーク] > [静的ルート] に移動します。
2. 次のいずれかを実行します。
   - [ルート ID] 列のルート名をクリックします。
   - [処理] 列の編集アイコン () をクリックします。

   [静的ルートの追加/編集] 画面が表示されます。
3. チェックボックスを使用して静的ルートを有効または無効にします。
4. ネットワークの IP アドレス/ビットマスクを確認します。このフィールドは読み取り専用です。

5. ネクストホップのパラメータを指定します。
6. [適用] をクリックします。

静的ルートを削除する

手順

1. [ゲートウェイ] > (ゲートウェイ名) > [ネットワーク] > [静的ルート] に移動します。
2. [処理] 列の削除アイコン ( ) をクリックします。
3. [削除] をクリックして削除を確認します。

NAT (Network Address Translation)

NAT (Network Address Translation) ポリシーを使用して、送信元または送信先の IP アドレスとポートをパブリックとプライベートの間、およびレイヤ 3 のインタフェース間で変換するかどうかを指定できます。たとえば、内部 (信頼できる) ゾーンからパブリック (信頼できない) ゾーンに送信されるトラフィックで、プライベートの送信元アドレスをパブリックアドレスに変換できます。

次の NAT ポリシールールは、ある範囲のプライベート送信元アドレス (`10.0.0.1`〜`10.0.0.100`) を単一のパブリック IP アドレス (`200.10.2.100`) および独自の送信元ポート番号に変換します (動的な送信元変換)。このルールは、内部 (信頼できる) ゾーンのレイヤ 3 インタフェース上で受信したトラフィックのうち、パブリック (信頼できない) ゾーンのインタフェースが送信先であるトラフィックのみに適用されます。プライベートアドレスは非表示であるため、ネットワークセッションはパブリックネットワークから開始されます。パブリックアドレスが Cloud Edge インタフェースアドレス (または同じサブネット上のアドレス) ではない場合、ローカルルータではリターントラフィックを Cloud Edge に送るための静的ルートが必要になります。

図 6-3. 通常の NAT ルール

NAT ルール

NAT アドレス変換ルールは、送信元および送信先の IPv4 アドレスとポートに基づいています。セキュリティポリシーと同様、NAT ポリシールールは受信したトラフィックに対して順次比較され、トラフィックと最初に一致したルールが適用されます。

NAT ルールは、管理インタフェースを除くすべての物理インタフェースに適用できます。

ワイヤレスネットワーク機能を備えた Cloud Edge ゲートウェイでは、メインまたはゲストのワイヤレスネットワークが有効な場合に、ワイヤレスネットワークインタフェースに対する NAT ルールを設定できます。

必要に応じて、静的ルートをローカルルータに追加して、パブリックアドレスへのすべての IPv4 トラフィックを Cloud Edge にルーティングすることができます。また、Cloud Edge の受信インタフェースへの静的ルートを追加すると、トラフィックをプライベート IPv4 アドレスに戻すこともできます。

クライアントとサーバの両方が同じ LAN インタフェースからゲートウェイにアクセスする場合の注意事項

クライアントとサーバが同じ LAN インタフェースから Cloud Edge ゲートウェイにアクセスする場合、クライアントはこのサーバにドメイン名でアクセスすることができません。このシナリオをサポートするには、この LAN インタフェースに送信元 NAT ルールと送信先 NAT ルールの両方を追加します。162 ページの「NAT ルールを追加してヘアピン NAT をサポートする」を参照してください。

送信先 NAT ルールを追加する

送信先 NAT (DNAT) は、パケットの IP ヘッダに含まれる送信先アドレスを変換します。この変換の主な目的は、パブリックアドレス/ポートの送信先を含む受信パケットを、ネットワーク内部のプライベート IP アドレス/ポートにリダイレクトすることです。

手順

1. [ゲートウェイ] > (選択したゲートウェイ) > [ネットワーク] > [NAT] > [追加] に移動します。
2. [NAT タイプ] に [送信先] を選択します。
3. 次の NAT 設定を行います。

オプション	説明
入口インタフェース	リストから [すべて]、すなわち任意の L3 インタフェースを選択します。このインタフェースは、ネットワークルータの外側からネットワーク内部の送信先に向けて発信されるネットワークトラフィックに対するインタフェースとして機能します。 ワイヤレスネットワーク機能を備えた Cloud Edge ゲートウェイでは、ワイヤレスネットワーク (メインまたはゲスト) が有効化されている場合に、そのワイヤレスネットワークインタフェースを入力インタフェースとして選択できます。
送信先 IP 変換	次のオプションから選択します。 • [入力インタフェースの IP アドレス] を選択し、[変換後の IP アドレス/範囲] を指定します。 入力インタフェースは外部 IP アドレスに使用され、指定した変換後の IP アドレス/範囲は入力インタフェースの IP アドレスを内部 IP アドレスに変換 (マッピング) するために使用されます。 • [仮想 IP] を選択し、[外部 IP アドレス/範囲] と [変換後の IP アドレス/範囲] を指定します。 NAT マッピングに使用するために、外部 IP アドレス/範囲を明示的に指定する必要があります。 変換後の IP アドレス範囲は、開始 IP アドレスに合わせて自動生成されます。マッピングは外部 IP アドレスと変換後の IP アドレスの 1 対 1 で行われます。
説明	用途や設定など、NAT ルールの特性がわかる説明を指定します。
ポート転送	[ポート転送]: ポート転送を伴う 1 対 1 の静的 NAT マッピングを行う場合は [オン] を選択します。

オプション	説明
	[オン] になっている場合、外部 IP アドレスは常にマッピング済みの同じ IP アドレスに変換され、外部ポート番号も常にマッピング済みの同じポート番号に変換されます。 [オン] に設定した場合は、次の情報を指定します。 • [プロトコル]: [TCP] または [UDP] を選択します。 • [外部サービスポート]: ポート範囲を指定します。 [マップ先ポート]: ポートを指定します。 [外部サービスポート] の範囲を指定すると、開始ポートに合わせて [マップ先ポート] が自動生成されます。マッピングは 1 対 1 で行われます。
一致条件の設定	次に示す、より詳細な情報や一致条件を指定できます。 • [送信元の IP アドレス範囲] • [送信元ポート範囲]

4. [保存] をクリックします。
5. 新しいルールが NAT ルールのリストに追加されていることを確認します。

NAT ルールを変更する

手順

1. [ゲートウェイ] > (選択したゲートウェイ) > [ネットワーク] > [NAT] に移動します。
2. [変換前] 列で、変更する NAT ルールをクリックします。
3. 必要に応じてパラメータを編集します。
4. [保存] をクリックします。

NAT ルールの優先度を変更する

手順

1. [ゲートウェイ] > (選択したゲートウェイ) > [ネットワーク] > [NAT] に移動します。
2. 変更する NAT ルールの優先度のチェックボックスをオンにします。
3. [移動] を選択し、NAT ルールリストの上部にある操作アイコン ([上]、[下]、[一番上]、[一番下]) を使用して順位を変更します。

送信元 NAT ルールを追加する

送信元 NAT (SNAT) は、パケットの IP ヘッダに含まれる送信元アドレスを変換します。この変換の主な目的は、ネットワークから送出されるパケットについて、プライベート (RFC 1918) アドレス/ポートをパブリックアドレス/ポートに変換することです。Cloud Edge では、初期設定の送信元 NAT ルールが自動的に作成されます。送信元 NAT ルールは追加で作成することも、初期設定のルールを変更することもできます。初期設定の送信元 NAT ルールの変更については、159 ページの「NAT ルールを変更する」を参照してください。

手順

1. [ゲートウェイ] > (選択したゲートウェイ) > [ネットワーク] > [NAT] > [追加] に移動します。
2. [NAT タイプ] に [送信元] を選択します。
3. 次の NAT 設定を行います。

オプション	説明
出力インタフェース	リストから [すべて]、または任意の L3 インタフェース (WAN など) を選択します。このインタフェースは、ネットワーク内部から発信されるトラフィックである出力トラフィック用のインタフェースとして機能します。 ワイヤレスネットワーク機能を備えた Cloud Edge ゲートウェイでは、ワイヤレスネットワーク (メインまたはゲスト) が有効化されている場合に、そのワイヤレスネットワークインタフェースを出力インタフェースとして選択できます。

オプション	説明
送信元 IP 変換 / 変換先	送信元 IP の変換方法として次のいずれかを選択します。 • [出力インタフェースの IP アドレス] この方法を選択した場合、[変換先] オプションは使用できません。出力インタフェースの IP アドレスは、変換に使用されます。 • [単一 IP アドレス] を選択し、[変換先] に IP アドレスを指定します。 指定した IP アドレスが変換に使用されます。 • [IP アドレス範囲] を選択し、[変換先] に IP アドレス範囲を指定します。 指定した IP アドレス範囲が変換に使用されます。 • [サブネット] を選択し、[変換先] にサブネットを指定します。 このサブネットが変換に使用されます。  注意 [単一 IP アドレス]、[IP アドレス範囲]、または [サブネット] を選択した場合、[出力インタフェース] オプションに特定の L3 インタフェースを指定する必要があります。
説明	用途や設定など、NAT ルールの特性がわかる説明を指定します。
一致条件の設定	[一致条件の設定] セクションを展開して、次の詳細情報または一致条件を追加で指定できます。 • プロトコル—すべて、TCP、UDP、または ICMP。[すべて] はすべてのプロトコルを意味します。 • 送信元の IP アドレス範囲 — ネットワークで指定されます。 • 送信元ポート範囲 — 管理者が指定します。 • 送信先の IP アドレス範囲 — 管理者が指定します。 • 送信先ポート範囲 — 管理者が指定します。  注意 [プロトコル] に [ICMP] を指定した場合、[送信元ポート範囲] および [送信先ポート範囲] オプションは使用できません。

4. [保存] をクリックします。
5. 新しいルールが NAT ルールのリストに追加されていることを確認します。

NAT ルールを削除する

手順

1. [ゲートウェイ] > (選択したゲートウェイ) > [ネットワーク] > [NAT] に移動します。
2. 削除する NAT ルールの行を選択します。
3. [削除] をクリックします。

   [削除] 確認メッセージが表示されます。
4. 内容を確認して [削除] をクリックします。
5. NAT ルールが NAT ルールのリストから削除されていることを確認します。

NAT ルールを追加してヘアピン NAT をサポートする

クライアントとサーバが同じ LAN インタフェースから Cloud Edge ゲートウェイにアクセスする場合、クライアントはこのサーバにドメイン名でアクセスすることができません。このシナリオをサポートするには、この LAN インタフェースに送信元 NAT ルールと送信先 NAT ルールの両方を追加します。以下に、この設定を行う手順を示します。

手順

1. [ゲートウェイ] > (選択したゲートウェイ) > [ネットワーク] > [NAT] > [追加] に移動します。
2. [NAT タイプ] に [送信元] を選択します。
3. [出力インタフェース] にクライアントおよびサーバにリンクされた LAN インタフェースを設定します。

4. [送信元 IP 変換] に [出口インターフェースの IP アドレス] を選択します。
5. [保存] をクリックします。
6. [ゲートウェイ] > (選択したゲートウェイ) > [ネットワーク] > [NAT] > [追加] に移動します。
7. [NAT タイプ] に [送信先] を選択します。
8. [入力インタフェース] にクライアントおよびサーバにリンクされた LAN インタフェースを設定します。
9. [送信先 IP 変換] に [仮想 IP] を選択します。
10. DNS サーバに登録されているサーバのインターネット IP アドレスを使用して [外部 IP アドレス/範囲] を設定します。
11. サーバのローカル IP アドレスを使用して [変換後の IP アドレス/範囲] を設定します。
12. [保存] をクリックします。
13. 新しいルールが NAT ルールのリストに追加されていることを確認します。

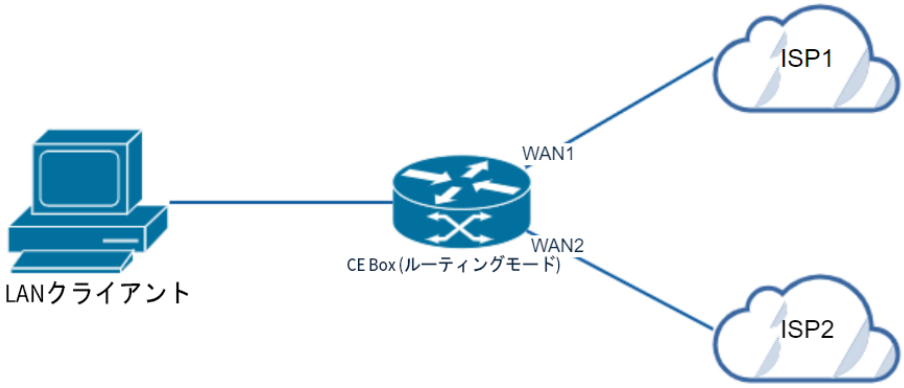
SD-WAN

ソフトウェア定義ワイドエリアネットワーク (SD-WAN) とは、ソフトウェアによってワイドエリアネットワークを管理するアプローチであり、配信の簡易化、一元管理、コスト削減のほか、インターネットやクラウドへの接続の向上を実現できます。

SD-WAN の主要なアプリケーションにより、企業は、コストの低い商用のインターネットアクセスを利用して、よりパフォーマンスの高い WAN を構築できます。これにより、企業は部分的または全面的に、MPLS などのコストの高いプライベート WAN 接続技術を交換できます。

SD-WAN の機能をフル活用するためには、ユーザがネットワークトポロジを変更し、Cloud Edge On-Premises UI で設定を行う必要があります。

Cloud Edge WAN では、PPPoE、DHCP、静的の 3 つのモードがサポートされます。SD-WAN を有効にするには、2 つの WAN リンク (WAN1 および WAN2/LAN1) を準備する必要があります。下の図を参照してください。



注意

- WAN インタフェースで静的 IP を使用する場合は、On-Premises Console で WAN1 および WAN2 のゲートウェイが正しく設定されていることを確認してください。CE Box　のゲートウェイが未設定 (空白) になっていると、SD-WAN 設定の配信時にエラーが発生します。

Cloud Edge には、以下の 3 種類のルーティング戦略があります。

- 静的ルーティング
- SD-WAN ルーティング
- ポリシールーティング

SD-WAN の配信後、ルーティング戦略の優先順位は以下のようになっている必要があります。

静的ルーティング > SD-WAN ルーティング > ポリシールーティング

SD-WAN および帯域幅設定を有効にする

目的: SD-WAN 機能を有効にし、SD-WAN の設定の概要とインタフェースの使用状況を表示します。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ホーム]

手順

1. [SD-WAN の有効化] の横にある [オン] をクリックします。
2. [SD-WAN アップリンク] の [WAN1] フィールドと [WAN2] フィールドは読み取り専用です。これらのフィールドは、Cloud Edge On-Premises Console でのみ編集できます。選択したゲートウェイのネットワークインタフェース設定を管理する方法については、123 ページの「ネットワークインタフェースを編集する」を参照してください。
3. [帯域幅設定] で、ドロップダウンから [WAN1] (初期設定) を選択しますアップストリームの帯域幅とダウンストリームの帯域幅を設定して、制限を指定します。ドロップダウンを使用して、Mbps と Kbps の制限を設定することもできます。

   注意

   手順 3 は省略可能です。
4. [保存] をクリックします。

概要ウィジェット

SD-WAN を有効にすると、ボリュームと帯域幅のデータが SD-WAN ホームページに表示されるようになります。また、設定済みの SD-WAN ルールとヘルスチェック SLA の数も表示されます。

SD-WAN ホームページの下部には、2 種類の概要ウィジェットが表示されています。[設定の概要] および [帯域幅とボリュームの使用状況] というウィジェットです。

- [設定の概要]: 追加された SD-WAN ルールの数と作成されたヘルスチェック SLA の数が表示されます。
- [帯域幅とボリュームの使用状況]: [帯域幅] タブには、WAN インタフェース (WAN1 および WAN2) のアップストリームとダウンストリームが表示されます。[ボリューム] タブには、WAN インタフェース (WAN1 および WAN2) の送受信されたボリュームが表示されます。

注意

SD-WAN ルールとヘルスチェック SLA にすばやくアクセスするには、[設定の概要] で、上記の SD-WAN ルールまたはヘルスチェック SLA の数をクリックします。この数は [ルール] ページまたは [SLA] ページにリンクされています。

SD-WAN ルール

SD-WAN ルールは、SLA を利用して目的のトラフィックをルーティングし、最適なリンクへ動的に転送するために使用します。SD-WAN ルールには以下の 3 つのモードがあります。

- 最高品質: 指定のパフォーマンスパラメータが最も優れているネットワーク内のリンクを選択します。
- 最大帯域幅: インターネット帯域幅をフル活用できるリンクを選択します。
- 優先リンク: トラフィックの転送先として優先度の高いリンクを選択します。

Cloud Edge は、DPI エンジンを使用してトラフィックを検出して ID をキャッシュすることにより、アプリケーション対応ルーティングを実現します。

SD-WAN メンバーインタフェース間の WAN トラフィックに対して動的にパスを選択するには、SD-WAN ルールを使用します。

SD-WAN ルールには以下の機能と特徴があります。

- 初期設定の SD-WAN ルールでは、送信元 IP、送信元 IP と送信先 IP、セッション、またはボリュームによって負荷分散を実行できます。初期設定のルールでは、SLA を設定できません。
- 初期設定の SD-WAN ルールでは、セッションおよびボリュームの重みが割合で示されます。重みの合計は 100%である必要があります。
- 定義できる SD-WAN ルールは最大 200 個までです (初期設定のルール 1 つを含む)。

[ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ルール] で次の操作を実行します。

- 既存のルールのリストの表示
- ルールの追加、編集、複製、削除
- ルールの優先度の変更
- ルールの有効化と無効化
- 検索

注意

[すべて配信] ボタンをクリックし、SD-WAN 設定を配信します (すべての設定が同時に配信されます。SD-WAN 設定は個別に配信されません)。

注意

初期設定の SD-WAN ルールの無効化、削除、移動、または複製は実行できません。

SD-WAN のトラフィックの再ルーティングルールがトリガーされるイベントには、以下の 3 種類があります。

- インタフェース停止: このインタフェースが物理的に停止している状態です。たとえば、ケーブルが抜けている、インタフェースのハードウェアに問題がある、接続先のインタフェースが中断しているといった状態です。
- SLA 停止: Cloud Edge ゲートウェイから監視サーバへのトラフィックで、ユーザにより設定された失敗しきい値を超えても応答を受信できない状態です。
- SLA 不履行: SLA パフォーマンス検出データが、ユーザにより設定されたしきい値を超えている状態です。

すべての最高品質戦略では、戦略自体によりパフィーマンス指標がすでに指定されているので、選択したヘルスチェック SLA の SLA パラメータは有効になりません。

最大帯域幅戦略と優先リンク戦略では、2 つの WAN リンクのうちいずれかが SLA パラメータを満たしていない場合、代替リンクにトラフィックが再ルーティングされます。

他の 2 つのイベントは、すべての種類の戦略においてトラフィックの再ルーティングに影響します。

また、上記の 3 種類のイベントについて、優先順位は以下のようになります。

1. インタフェース停止 (高)
2. SLA 停止 (中)
3. SLA 不履行 (低)

SD-WAN ルールを管理する

目的: 登録済みゲートウェイを通過するトラフィックを制御する SD-WAN ルールを管理します。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ルール]

手順

1. 次の手順を実行します。
   - 既存の SD-WAN ルールに関する情報を確認します。
   - ルールの SD-WAN 設定に関する詳細を確認するには、そのルール名の左にある展開矢印をクリックします。
   - 新しいルールを作成するには、[追加] をクリックします。

     注意

     初期設定の SD-WAN ルールは、SD-WAN を初めて有効にしたときに自動的に追加されます。

   - ルールを探すには、右上にある [検索] を使用します。
   - 設定を表示または変更するには、ルールの名前をクリックします。
   - 設定を表示または変更するには、ルールを選択して [編集] をクリックします。
   - ルールの優先順位を変更するには、ルールを選択して [移動] をクリックします。

- ステータスを変更したりルールを複製したりするには、ルールを選択して [その他] をクリックします。
- ルールを削除するには、ルールを選択して [削除] をクリックします。

SD-WAN ルールを追加/編集する

目的: ユーザまたはユーザーグループ、IP アドレスまたは FQDN を指定して、SD-WAN ルールを追加または編集します。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ルール] > [追加/編集]

手順

1. [SD-WAN ルールの追加/編集] > [ルール名] ページで、次の手順を実行します。
   a. [ルール名] を指定します。英字、数字、またはアンダースコアを使用して、1〜32 文字で指定する必要があります。
   b. [説明] を指定します (任意)。
   c. [次へ] をクリックします。

   注意
   SD-WAN ルールの名前をクリックすると、編集できます。

2. [SD-WAN ルールの追加/編集] > [送信元] ページで、[送信元] を設定します。
   a. この SD-WAN ルールをすべてのユーザグループまたは IP に適用する場合は、[すべて] を選択します。
   b. この SD-WAN ルールを特定のユーザまたはユーザグループに適用する場合は、[ユーザ/ユーザグループを指定する] を選択します。[次の中から選択] ボックスでユーザまたはユーザグループを選択して、[選択済み] ボックスに移動します。
   c. この SD-WAN ルールを特定の IP アドレスや FQDN に適用する場合は、[IP アドレス/FQDN を指定する] を選択します。[次の中から選

択] ボックスで IP アドレスまたは FQDN を選択して、[選択済み] ボックスに移動します。新しい IP アドレスまたは FQDN オブジェクトを追加するには、[新しい IP アドレス/FQDN オブジェクトの追加] をクリックします (250 ページの「IP アドレス/FQDN オブジェクトを追加/編集する」を参照)。指定したユーザ/ユーザグループ/IP アドレス/FQDN を検索するには、検索ボックスを使用します。

d. [次へ] をクリックします。

3. [SD-WAN ルールの追加/編集] > [送信先] ページで、[送信先] を設定します。

   a. この SD-WAN ルールをすべての IP アドレスまたは FQDN に適用する場合は、[アドレス] で [すべて] を選択します。この SD-WAN ルールを特定の IP アドレスや FQDN に適用する場合は、[IP アドレス/FQDN を指定する] を選択します。

   b. この SD-WAN ルールをすべてのサービスまたはアプリケーションに適用する場合は、[サービスとアプリケーション] で [すべて] を選択します。この SD-WAN ルールを特定のサービスに適用する場合は、[サービスを指定する] を選択します。新しいサービスオブジェクトを追加するには、[新しいサービスオブジェクトの追加] をクリックしますこの SD-WAN ルールを特定のアプリケーションに適用する場合は、[アプリケーションを指定する] を選択します。新しいアプリケーショングループを追加するには、[新しいアプリケーショングループの追加] をクリックします。

   c. [次へ] をクリックします。

4. [SD-WAN ルールの追加/編集] > [戦略] ページで、[戦略] を設定します。

   a. 遅延時間が短いリンクを使用する場合は、[最高品質 – 遅延時間] を選択します。

   b. 次の 3 つのオプションに基づいてトラフィックの優先順位を設定する場合は、[詳細] を選択します。

      - [最大帯域幅]: 利用可能なすべてのリンクでトラフィックを分散するために [最大帯域幅] を使用します。
      - [最高品質]: [ジッタ]、[パケットロス]、または [帯域幅] のドロップダウンで品質基準を選択するには、[最高品質] を使用します。または、ドロップダウンで [カスタムプロファイル] をクリック

すると、遅延時間、ジッタ、パケットロス、帯域幅の割合を割り当てることができます。

- [優先リンク]: [リンクの選択] ドロップダウンで選択した物理リンクが SLA を満たしている限り、このリンクにトラフィックを送信する場合は、[優先リンク] を使用します。[リンクの選択] ドロップダウンで、[WAN1] または [WAN2] を選択します。

c. [次へ] をクリックします。

5. [SD-WAN ルールの追加/編集] > [ヘルスチェック SLA] ページで、ユーザ指定のヘルスチェック SLA を選択するか、新しいヘルスチェック SLA を作成します(175 ページの「SLA」を参照)。必要に応じて、[新規ヘルスチェック SLA の追加] をクリックして、新しいヘルスチェック SLA を追加できます。

a. [ヘルスチェック SLA の追加/編集] > [一般] ページで、[SLA 名]、[説明]、[監視サーバ]、およびプロトコルの [種類] を指定します。2 番目のサーバを追加するには、[サーバの追加] をクリックします(注意: 2 番目のサーバは追加することも、不要な場合は削除することもできます)。[次へ] をクリックします。

b. [ヘルスチェック SLA の追加/編集] > [SLA パラメータ] ページで、[推奨される SLA] から SLA パラメータを選択するか、[遅延時間]、[ジッタ]、[パケットロス] にカスタムパラメータを入力します。注意: Cloud Edge Cloud Console (CECC) には、事前定義された 4 つの SLA (VoIP ビデオ、オーディオストリーミング、一般の Web、および Office 365) が用意されています (推奨される SLA の種類と説明の表を参照)。[次へ] をクリックします。

c. [ヘルスチェック SLA の追加/編集] > [リンクチェックステータス] ページで、リンクチェックステータスのしきい値と間隔を設定します。[次へ] をクリックします。

d. [ヘルスチェック SLA の追加/編集] > [非アクティブ時の処理] ページで、[静的ルートのアップデート] を選択して、SLA パラメータの条件が満たされない場合に静的ルートを無効にします(注意: リンクが非アクティブ時に有効にした場合、そのリンクのルートは削除され、トラフィックは別のリンクを介してルーティングされます。リンクが再度アクティブになると、ルートが再度有効になります)。[保存] をクリックします (注意: [保存] をクリックすると、[SD-WAN ルール

の追加/編集] > [ヘルスチェック SLA] ページに戻ります)。[次へ] をクリックします。

6. [SD-WAN ルールの追加/編集] > [確認]ページで、[保存] をクリックします。[保存] をクリックすると、[ルール] ページに戻ります。

初期設定の SD-WAN ルールを編集する

目的: 負荷分散モードの変更またはインタフェースの重みの調整。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ルール] > [初期設定の SD-WAN ルールの編集]

SD-WAN を有効にして保存すると、初期設定の SD-WAN ルールが作成されます。初期設定の SD-WAN ルールでは、送信元 IP と送信先 IP、セッション、またはボリュームによって負荷分散を実行できます。初期設定のルールでは、SLA を設定できません。初期設定の SD-WAN ルールでは、セッションおよびボリュームの重みが割合で示されます。重みの合計は 100%である必要があります。

初期設定の SD-WAN ルールは、SD-WAN を初めて有効にしたときに作成されます。[ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ルール] ページに表示されます。

手順

1. [負荷分散モード] で、WAN1 リンクと WAN2 リンク間でトラフィックの負荷を分散する際に使用するモードを選択します。
   a. 送信元 IP に基づいてトラフィックの負荷を分散する場合は、[送信元 IP] を選択します。
   b. 送信元 IP と送信先 IP の組み合わせに基づいてトラフィックの負荷を分散する場合は、[送信元 IP と送信先 IP] を選択します。
   c. セッション数の比率に従って負荷を分散する場合は、[セッション] を選択します。割合を使用して重みを設定します (重みの合計は 100% になる必要があります)。
   d. 帯域幅の比率に従って負荷を分散する場合は、[ボリューム] を選択します。ボリュームの割合を使用して重みを設定します (重みの合計は 100%になる必要があります)。

2. [保存] をクリックします。

SD-WAN ルールを複製する

目的: SD-WAN ルールを複製します。新しいルールの優先順位が最も高くなります。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ルール]

注意

初期設定の SD-WAN ルールは複製できません。

手順

1. 複製する SD-WAN ルールの横にあるチェックボックスをオンにし、[その他] プルダウンメニューをクリックします。
2. [複製] をクリックします。
3. 重複した番号の付いた新しい SD-WAN ルールが [SD-WAN] > [ルール] のリストに表示されていることを確認します。

SD-WAN ルールを移動する

目的: ユーザ指定の SD-WAN ルールを移動して、優先順位を変更します。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ルール]

注意

初期設定の SD-WAN ルールは移動できません。

手順

1. 移動し優先順位を変更する SD-WAN ルールの横にあるチェックボックスをオンにします。

2. [移動] プルダウンメニューをクリックし、[上]、[下]、[一番上]、または [一番下] を選択します。

SD-WAN ルールを有効/無効にする

目的: ユーザ指定の SD-WAN ルールを有効にしたり、有効にした SD-WAN ルールを無効にしたりします。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ルール]

注意

初期設定の SD-WAN ルールを有効または無効にすることはできません。

手順

1. 有効または無効にする SD-WAN ルールの横にあるチェックボックスをオンにします。
2. [その他] プルダウンメニューをクリックし、[有効にする] または [無効にする] を選択します。

SD-WAN ルールを削除する

目的: ユーザ指定の SD-WAN ルールを削除します。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [ルール]

手順

1. 削除する SD-WAN ルールの横にあるチェックボックスをオンにします。
2. [削除] をクリックします。
3. 削除した SD-WAN ルールが [SD-WAN] > [ルール] のリストに表示されていないことを確認します。

SLA

サービスレベルアグリーメント (SLA) とは、サービスプロバイダとその顧客との間の契約のことです。

SLA リンクの監視では、それぞれの WAN インタフェースからサーバにプロービングパケットを送信して遅延時間、ジッタ、パケットロスに基づきリンクの品質を測定することにより、SD-WAN メンバーインタフェースに接続されたリンクの状態を測定します。リンクが切断されている場合、SLA でこのイベントが検出されて Cloud Edge ゲートウェイに通知が送られ、代替リンクにトラフィックが再ルーティングされます。リンクが再び有効になると、Cloud Edge ゲートウェイはリンクを復元し、再び利用可能になったリンクにトラフィックをルーティングします。これにより、切断されたリンクにトラフィックが送信されてトラフィックが切断される事態を防止します。

Cloud Edge では、以下の 4 種類の SLA が推奨されています。

- VoIP ビデオ
- オーディオストリーミング
- 一般の Web
- Office 365

注意

[SLA の管理] ページの下部には、推奨される 4 つの SLA が表示されます。それぞれにマウスポインタを合わせると、例の説明が表示されます。

Cloud Edge でサポートされる SLA の最大数は 50 です。

SLA を管理する

目的: SD-WAN メンバーインタフェースに接続されているリンクの状態を測定する SLA を管理します。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [SLA]

手順

1. 次の手順を実行します。

   - SLA を選択し、[遅延時間]、[ジッタ]、または [パケットロス] ボタンをクリックしてその SLA に関する情報を確認します。
   - SLA を検索するには、下部ペインの右上にある [検索] を使用します。
   - 新しい SLA を作成するには、[追加] をクリックします。
   - SLA を選択した後、SLA の設定を変更するには [編集] をクリックし、SLA を編集するには SLA 名をクリックします。
   - SLA を削除するには、SLA を選択して [削除] をクリックします。

   [SLA 設定] ページでは、Cloud Edge Cloud Console に表示される UI に従って SLA を設定できます。SLA を設定する際には、以下のことに注意してください。

   - SLA 名と監視サーバを設定してください。サーバは、FQDN または IP アドレスのいずれかで指定できます。
   - 監視サーバは 2 台まで設定できます。

     注意

     監視サーバを 2 台設定する場合は、1 番目のサーバが優先されます。初期設定で Cloud Edge Cloud Console に表示される SLA データは、1 番目のサーバのデータです。1 番目のサーバが停止している場合は、2 番目のサーバに到達可能かがチェックされます。到達可能な場合、2 番目のサーバの SLA データが使用されます。両方のサーバに到達できない場合、SLA が停止しています。

   - 設定可能な検出の種類には、Ping と HTTP があります。

     注意

     一部のサーバでは Ping または HTTP が受け付けられないので、監視サーバの設定を行う際には、その監視サーバで Ping または HTTP が受け付けられることを確認してください。

ヘルスチェック SLA の追加/編集

目的: SD-WAN メンバーインタフェースに接続されているリンクの状態を測定するヘルスチェック SLA を追加または編集します。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [SLA]

手順

1. [ヘルスチェック SLA の追加/編集] > [一般] ページで、[SLA 名]、[説明]、[監視サーバ]、およびプロトコルの [種類] を指定します。2 番目のサーバを追加するには、[サーバの追加] をクリックします (注意: 2 番目のサーバは追加することも、不要な場合は削除することもできます)。[次へ] をクリックします。
2. [ヘルスチェック SLA の追加/編集] > [SLA パラメータ] ページで、[推奨される SLA] から SLA パラメータを選択するか、カスタムパラメータを入力します。また、そのパラメータを [遅延時間]、[ジッタ]、[パケットロス] にも指定します。注意: Cloud Edge Cloud Console (CECC) には、事前定義された 4 つの SLA (VoIP ビデオ、オーディオストリーミング、一般の Web、および Office 365) が用意されています (推奨される SLA の種類と説明の表を参照)。[次へ] をクリックします。
3. [ヘルスチェック SLA の追加/編集] > [リンクチェックステータス] ページで、リンクチェックステータスのしきい値と間隔を設定します。[次へ] をクリックします。
4. [ヘルスチェック SLA の追加/編集] > [非アクティブ時の処理] ページで、[静的ルートのアップデート] を選択して、SLA パラメータの条件が満たされない場合に静的ルートを無効にします(注意: リンクが非アクティブ時に有効にした場合、そのリンクの静的ルートは削除され、トラフィックは別のリンクを介してルーティングされます。リンクが再度アクティブになると、静的ルートが再度有効になります)。[保存] をクリックします [保存] をクリックすると、[SLA の管理] ページに戻ります。

SLA を削除する

目的: SLA を削除します。

場所: [ゲートウェイ] > (選択したゲートウェイ) > [SD-WAN] > [SLA]

手順

1. 削除する SLA の横にあるチェックボックスをオンにします。
2. [削除] をクリックします。
3. 削除した SLA が [SD-WAN] > [SLA] のリストに表示されていないことを確認します (注意: SLA が SD-WAN ルールで使用されている場合は削除できません)。

ワイヤレス

ワイヤレスの一般設定に関する情報を確認して、登録済みのゲートウェイに対してワイヤレスネットワークアクセス管理の設定を行います。

本機能は日本語版では使用できません。

ワイヤレスネットワークに関する情報を確認する

ワイヤレスネットワークに関する情報は、Cloud Edge Cloud Console で確認できます。

ワイヤレスネットワークの一般設定を確認する

目的: ワイヤレスネットワークの一般設定を確認します。

場所: ゲートウェイ > (選択したゲートウェイ) > ワイヤレス > ワイヤレス設定 > 一般設定

手順

1. 次の設定に関する情報を確認します。
   - ワイヤレスアクセスポイント

     ワイヤレスアクセスが有効になっているかどうかを示します。この設定を有効にすると、メインワイヤレスネットワークが有効になります。ゲストワイヤレスネットワークは有効になりません。ただし、ゲストワイヤレスネットワークを有効にするには、この設定を有効にしておく必要があります。初期設定では有効になっています。

- 国/地域
- 周波数

  Cloud Edge では、2.4GHz と 5.0GHz の周波数帯がサポートされています。
- SSID ブロードキャストを有効にする

  有効にすると、Cloud Edge ゲートウェイが SSID をブロードキャストします。これにより、付近のクライアントが、利用可能なワイヤレスネットワークの画面にあるメインワイヤレスネットワークを認識できるようになります。
- SSID

  メインワイヤレスネットワークの SSID を示します。
- チャネル
- モード

  この設定は、メインとゲスト、両方のネットワークに適用されます。
- セキュリティ

  メインワイヤレスネットワークのセキュリティ設定を示します。

2. 次の詳細設定に関する情報を示します。
   - DTIM 間隔 (初期設定)
   - ビーコン間隔
   - ショートプリアンブル
   - RTS しきい値
   - ショート GI を有効にする
   - 送信電力

注意

ネットワーク周波数が 5GHz に設定されている場合、[DTIM 間隔]、[ビーコン間隔]、および[送信電力] フィールドのみ表示されます。

ゲストワイヤレスネットワークの設定を確認する

目的: ワイヤレスネットワークの一般設定を確認します。

場所: ゲートウェイ > (選択したゲートウェイ) > ワイヤレス > ワイヤレス設定 > ゲストネットワーク

手順

1. 次の設定に関する情報を確認します。
   - ゲストネットワークを有効にする

     ゲストネットワークが有効と無効のどちらであるかを示します。初期設定では無効になっています。
   - ローカルネットワークアクセスを有効にする

     ゲストワイヤレスネットワーク上のユーザが、適切な権限を持っていることを条件として、ローカルの内部ネットワーク上のリソースにアクセスできるかどうかを示します。初期設定では無効になっています。
   - SSID ブロードキャストを有効にする

     有効にすると、Cloud Edge ゲートウェイが SSID をブロードキャストします。これにより、付近のクライアントが、利用可能なワイヤレスネットワークの画面にあるゲストワイヤレスネットワークを認識できるようになります。
   - SSID

     ゲストネットワークの SSID を示します。
   - セキュリティ

     ゲストネットワークのセキュリティ設定を示します。

ワイヤレスのトラブルシューティング情報を確認する

目的: ワイヤレスネットワークのトラブルシューティング情報を確認します。

場所: ゲートウェイ > (選択したゲートウェイ) > ワイヤレス > ワイヤレス設定 > トラブルシューティング

手順

1. トラブルシューティングを容易にするためにワイヤレスネットワークのログを確認します。
2. [表示更新] をクリックして、表示されたログエントリを更新します。

ワイヤレスネットワークアクセス管理

ワイヤレスネットワークアクセス管理の設定とクライアント接続の管理は、Cloud Edge Cloud Console で行うことができます。

ワイヤレスネットワークアクセス管理ルールの仕組み

MAC アドレスフィルタリストを使用してメインおよびゲストワイヤレスネットワークへのネットワークアクセスを管理できます。

MAC アドレスフィルタリストには、ブロックリストと許可リストの 2 種類があります。ブロックリストと許可リストのどちらでも使用できます。両方を同時に使用することはできません。

MAC アドレスフィルタオプションの仕組み

選択した MAC アドレスフィルタリストをメインおよびゲストワイヤレスネットワークに適用するかどうかは、[グローバル MAC アドレスフィルタを有効にする] および [ゲストワイヤレスネットワークに MAC フィルタを適用する] オプションの設定によって決まります。これらの設定がワイヤレスネットワークアクセス管理に及ぼす影響について以下で説明します。

[グローバル MAC アドレスフィルタを有効にする] の設定	[ゲストワイヤレスネットワークに MAC フィルタを適用する] の設定	選択した MAC アドレスフィルタリストの適用先
オン	オン	メインワイヤレスネットワークおよびゲストワイヤレスネットワークの両方
オン	オフ	メインワイヤレスネットワークおよびゲストワイヤレスネットワークの両方
オフ	オン	ゲストワイヤレスネットワークのみ。メインネットワークには適用されない。
オフ	オフ	メインワイヤレスネットワークとゲストワイヤレスネットワークのいずれにも適用されない。

[ブロックリストを使用する] と [許可リストを使用する] の仕組み

- [ブロックリストを使用する] を選択した場合:
  - Cloud Edge では、ブロックリストにクライアント MAC アドレスが存在する場合を除き、すべてのワイヤレス接続を許可します。
  - [ブロックリストを使用する] に切り替えた場合、ブロックリストにある MAC アドレスを持つクライアントが接続している場合は切断されます。
  - ブロックリストに MAC アドレスを追加すると、そのアドレスを持つクライアントが接続している場合は切断されます。
  - ワイヤレスネットワークへのアクセスを一般に許可するが、ブロックしたいクライアントの数が少ない場合は、ブロックリストの使用を検討してください。
  - ブロックリストの最大エントリ数は 256 です。
- [許可リストを使用する] を選択した場合:
  - Cloud Edge では、許可リストにクライアント MAC アドレスが存在する場合を除き、すべてのワイヤレス接続を拒否します。

- [許可リストを使用する] に切り替えると、許可リストにない MAC アドレスを持つクライアントの現在の接続は切断されます。
- 許可リストに MAC アドレスを追加すると、該当する MAC アドレスを持つクライアントがワイヤレスネットワークに接続できるようになります。
- ワイヤレスネットワークへの広範なアクセスを許可するのではなく、承認された小数のクライアントにのみアクセスを許可する場合は、許可リストの使用を検討してください。
- 許可リストの最大エントリ数は 256 です。

ワイヤレスネットワークのアクセス制御を設定する

目的: Cloud Edge ゲートウェイのワイヤレスネットワークのアクセス制御を設定します。アクセス制御は、特定のクライアントに対して、メインおよびゲストワイヤレスネットワークへのアクセスを許可または制限 (拒否) する際に使用します。

場所: ゲートウェイ > (選択したゲートウェイ) > ワイヤレス > アクセス制御

手順

1. [グローバル MAC アドレスフィルタを有効にする] で、[オン] をクリックします。

   [オン] に設定した場合、MAC アドレスはメインとゲスト両方のワイヤレスネットワークに適用されます。

2. (任意) [ゲストワイヤレスネットワークに MAC フィルタを適用する] で、[オン] をクリックします。

   グローバル MAC アドレスフィルタが [オフ] になってもゲストネットワークに対して MAC アドレスフィルタを適用する必要がある場合に、このオプションで [オン] を選択します。

3. [MAC アドレスフィルタリスト] で、適切なオプションを選択します。
   - ブロックリストを使用してアクセス制御を行うには、[ブロックリストを使用する] を選択します。
   - 許可リストを使用してアクセス制御を行うには、[許可リストを使用する] を選択します。

ワイヤレスネットワークへのアクセス制御を提供する方法として、ブロックリストまたは許可リストのどちらを使用するかを選択できます。両方を使用することはできません。

4. [保存] をクリックします。

次に進む前に

クライアントをブロックリストまたは許可リストに追加することにより、特定のクライアントからのワイヤレスネットワークアクセスを許可または制限します (どちらのリストを選択したかによる)。

- 185 ページの「ワイヤレスネットワークアクセス管理ルールを追加する」
- 185 ページの「接続済みクライアントをアクセス制御ルールに追加する」

ワイヤレスで接続されているクライアントを確認する

目的: [接続しているクライアント] セクションで、ワイヤレスで接続されているクライアントに関する情報を確認します。

場所: ゲートウェイ > (選択したゲートウェイ) > ワイヤレス > アクセス制御

手順

1. [接続しているクライアント] セクションでは、接続済みクライアントについて次の情報を確認できます。

   - クライアント ID

     接続されている各クライアントに割り当てられた一意の識別子です。

   - MAC アドレス

     接続されているクライアントの MAC アドレスです。

   - IP アドレス

     接続済みの MAC アドレスに関連付けられている IP アドレスです。

   - ホスト名

     接続済みの MAC アドレスに関連付けられているホスト名です。

- SSID

  SSID は、クライアントがメインとゲスト、どちらのネットワークに接続されているかを判別する際に使用します。

次に進む前に

接続済みクライアントのうち、特定のものを MAC アドレスフィルタリストのブロックリストまたは許可リストに追加して、ワイヤレスネットワークに対するネットワークアクセスを制御することもできます。185 ページの「接続済みクライアントをアクセス制御ルールに追加する」を参照してください。

接続済みクライアントをアクセス制御ルールに追加する

目的: [接続しているクライアント] セクションのクライアントを [MAC アドレスフィルタリスト] セクションの許可リストまたはブロックリスト内のアクセス制御ルールに追加することで、特定のクライアントによるワイヤレスネットワークへのアクセスを許可または制限 (拒否) します。

場所: ゲートウェイ > (選択したゲートウェイ) > ワイヤレス > アクセス制御

手順

1. [接続しているクライアント] セクションで、次の該当する処理を実行します。
   - ブロックリストを使用: 追加するクライアントを選択し、[ブロックリストに追加] をクリックします。
   - 許可リストを使用: 追加するクライアントを選択し、[許可リストに追加] をクリックします。
2. [保存] をクリックします。

接続済みクライアントが [MAC アドレスフィルタリスト] セクションの該当するリストに追加されます。

ワイヤレスネットワークアクセス管理ルールを追加する

目的: アクセス制御ルールを [MAC アドレスフィルタリスト] セクションの許可リストまたはブロックリストに追加します。アクセス制御ルールにより、

MAC アドレスで識別された特定のクライアントからの、メインおよびゲストワイヤレスネットワークへのアクセスが許可または制限 (拒否) されます。

場所: ゲートウェイ > (選択したゲートウェイ) > ワイヤレス > アクセス制御

手順

1. アクセス制御に使用しているリストに応じて、[MAC アドレスフィルタリスト] セクションで該当する処理を実行します。
   - ブロックリストを使用: [ブロックリストを使用する] で、[追加] をクリックします。
   - 許可リストを使用: [許可リストを使用する] で、[追加] をクリックします。

   [MAC アドレスフィルタルールの追加/編集] ダイアログボックスが表示されます。
2. [MAC アドレス] で、フィルタに使用する MAC アドレスを指定します。
3. (任意) 説明を指定します。
4. [保存] をクリックします。

ワイヤレスネットワークアクセス管理ルールを削除する

目的: ブロックリストまたは許可リストから MAC アドレスフィルタルールを削除することにより、それらの MAC アドレスをワイヤレスネットワークアクセス管理から取り除きます。

場所: ゲートウェイ > (選択したゲートウェイ) > ワイヤレス > アクセス制御

手順

1. [MAC アドレスフィルタリスト] セクションで、次の該当する処理を実行します。
   - ブロックリスト内の削除する MAC アドレスアクセス制御ルールを選択し、[削除] をクリックします。

- 許可リスト内の削除する MAC アドレスアクセス制御ルールを選択し、[削除] をクリックします。

帯域幅制御

ピアツーピアのダウンロード、ビデオストリーミング、インスタントメッセージアプリケーションなどを実行すると、生産性に影響するほどネットワーク帯域幅を消費することがあります。帯域幅制御では、通信を制御したり、不要なトラフィックを低減したり、重要なトラフィックやサービスに適切な帯域幅を割り当てたりすることで、ネットワークの輻輳を緩和できます。帯域幅制御を使用すると、すべてのユーザにリソースへの適切なアクセスを提供し、組織にとってより重要なリソースへのアクセスを確保することができます。ポリシールールと同様に、帯域幅制御では、送信元や送信先の IP アドレス、アプリケーションやサービス、および時刻に基づいてトラフィックを制限できます。

帯域幅制御ルールは、汎用的なものから限定的なものまで、必要に応じてさまざまなレベルで設定できます。帯域幅制御ルールは受信トラフィックに対して順番に照合され、トラフィックに一致する最初のルールが適用されるため、限定的なルールから汎用的なルールの順に照合する必要があります。たとえば、単一のアプリケーション向けのルールは、トラフィックに関する他の設定がすべて同じ場合に適用するすべてのアプリケーション向けのルールよりも先に照合する必要があります。トラフィックがいずれのルールにも一致しない場合は、残りの帯域幅が使用されます。

注意

帯域幅制御ポリシーは、インタフェース帯域幅設定の範囲内で設定する必要があります。

帯域幅制御を管理する

目的: 帯域幅制御では、ネットワークの輻輳を緩和するため、通信の制御、不要なトラフィックのブロック、重要なトラフィックやサービスへの適切な帯域幅割り当ての設定を行うことができます。

場所: ゲートウェイ > (ゲートウェイ名) > 帯域幅制御

手順

1. 次の手順を実行します。
   - 新しいルールを作成するには、[追加] をクリックします。
   - ルールを探すには、右上にある [検索] を使用します。
   - 設定を表示または変更するには、ルールの名前をクリックします。
   - 設定を表示または変更するには、ルールを選択して [編集] をクリックします。
   - ルールの順序を変更するには、ルールを選択して [移動] をクリックします。
   - ステータスを変更したりルールを複製したりするには、ルールを選択して [その他] をクリックします。
   - ルールを削除するには、ルールを選択して [削除] をクリックします。
2. 必要な設定を行います。
3. [保存] をクリックします。

帯域幅制御ルールを追加/編集する

目的: 送信元のユーザ、ユーザグループやアドレス、送信先、トラフィックタイプ、スケジュール、出力インタフェース、その他の帯域幅の設定を指定して、帯域幅制御ルールを追加または編集します。

場所: ゲートウェイ > (ゲートウェイ名) > 帯域幅制御 > 追加/編集

手順

1. ルール名を指定します。英字、数字、またはアンダースコアを使用して、1〜32 文字で指定する必要があります。
2. [説明] を指定します。
3. ルールを有効または無効にします。
4. [送信元のユーザ/ユーザグループ/IP アドレス/MAC アドレス] を設定します。

- ルールをすべてのユーザおよびすべての IP アドレスに適用する場合は [すべて] を選択します。
- ルールを特定のユーザまたはグループにのみ適用する場合は [ユーザ/グループを指定する] を選択します。
- ルールを特定の IP アドレスにのみ適用する場合は [IP アドレスを指定する] を選択します。
- ルールを特定の MAC アドレスにのみ適用する場合は [MAC アドレスを指定する] を選択します。

5. [送信先のアドレス] を設定します。
   - ルールにすべての IP アドレスを含める場合は [すべて] を選択します (初期設定)。
   - ルールを特定の IP アドレスにのみ適用する場合は [IP アドレスを指定する] を選択します。
6. [トラフィックタイプ] を設定します。
   - ルールにすべてのアプリケーショングループを含める場合は [すべて] (初期設定)、特定のアプリケーションのみを含める場合は [アプリケーションを指定する] を選択します。
   - ルールにすべてのサービスを含める場合は [すべて] (初期設定)、特定のサービスのみを含める場合は [サービスを指定する] を選択します。
7. [スケジュール] を設定します。

オプション	説明
常時	すべてのスケジュールを含めます(初期設定)
スケジュール名	使用可能なスケジュールオブジェクトの名前が表示されます。
新しいスケジュールオブジェクトの追加	[追加/編集] スケジュールオブジェクト作成ダイアログボックスにアクセスします。

8. [出力インタフェース] のドロップダウンメニューからインタフェースを選択します。

9. [帯域幅] でアップストリームとダウンストリームの設定を指定します。
10. [保存] をクリックします。

帯域幅制御ルールを複製する

目的: 既存のルールを複製します。

場所: ゲートウェイ > (ゲートウェイ名) > 帯域幅制御

手順

1. ルールを選択し、[その他] プルダウンメニューをクリックします。
2. [複製] をクリックします。
3. 新しいルールがリストに表示されていることを確認します。

帯域幅制御ルールを有効/無効にする

目的: 帯域幅制御ルールを無効にした状態でプロビジョニングできます。この手順は、まだ有効にしていない作成済みの帯域幅制御ルールに適用されます。変更は、[すべて配信] をクリックした後に有効になります。

場所: ゲートウェイ > (ゲートウェイ名) > 帯域幅制御

手順

1. 有効または無効にするルールの横にあるチェックボックスをオンにします。
2. [その他] プルダウンメニューをクリックし、[有効にする] または [無効にする] を選択します。
3. [すべて配信] をクリックして変更を有効にします。

帯域幅制御ルールを削除する

目的: 帯域幅制御ルールを削除します。

場所: ゲートウェイ > (ゲートウェイ名) > 帯域幅制御

手順

1. 削除するルールの横にあるチェックボックスをオンにします。
2. [削除] をクリックします。
3. [OK] をクリックして確認します。
4. 削除したルールがリストに表示されていないことを確認します。

ユーザ VPN

ユーザが遠隔地から組織のサーバにアクセスするときは、安全に接続するための通常の要件に加え、リモートクライアントが特別な要件を満たすことも不可欠です。ユーザの仮想プライベートネットワーク (VPN) は、VPN のリモートユーザ向け拡張機能です。ダイヤルアップ接続 (ブロードバンド接続を含む)、LAN 接続、モバイル接続のいずれにおいても、VPN トンネルを介してネットワークやサーバと機密情報を安全にやり取りできます。

仮想プライベートネットワーク

仮想プライベートネットワーク (VPN) テクノロジは、遠隔地で作業する従業員が企業ネットワークにアクセスする際のセキュリティ対策として広く使用されています。認証とは、大まかにいうと、ネットワークリソースにアクセスするときと VPN ネットワークにログオンするときにデジタル ID を検証するプロセスのことです。VPN では、既存のインフラストラクチャ (インターネット) を利用して既存の接続を安全に確立して強化します。VPN は、安全なインターネットプロトコルに基づいて、特殊なネットワークノードとセキュアゲートウェイ間の安全なリンクを確立できます。サイト間 VPN ではゲートウェイ間の安全なリンクが確立され、ユーザ VPN ではゲートウェイとリモートアクセスクライアントの間の安全なリンクが確立されます。

一般的な Cloud Edge の配置では、企業ネットワークのリソースにリモートから VPN を使用して接続できます。他のリモートサイトは Cloud Edge で保護され、すべてのネットワークリソースとリモートエンドポイントの間の通信が厳格なセキュリティポリシーによって規制されます。

Cloud Edge では、IPv4 間の VPN アクセスがサポートされます。

暗号化アルゴリズム

次の表に、SSL-VPN で設定可能な暗号化アルゴリズムを示します。DES (Digital Encryption Standard) は、56 ビット鍵を使用する 64 ビットのブロックアルゴリズムです。AES (Advanced Encryption Standard) は、128～256 ビットの鍵と可変長のデータブロックをサポートする秘密鍵アルゴリズムです。

アルゴリズム	説明
AES 128 CBC	128 ビット鍵を使用する 128 ビットブロックの CBC (暗号ブロック連鎖) アルゴリズムです。
AES 192 CBC	192 ビット鍵を使用する 192 ビットブロックの CBC (暗号ブロック連鎖) アルゴリズムです。
AES 256 CBC	256 ビット鍵を使用する 256 ビットブロックの CBC (暗号ブロック連鎖) アルゴリズムです。
DES EDE3 CBC	Triple-DES では、プレーンテキストが 3 つの鍵で 3 回暗号化されます。
BF-CBC	Blowfish を使用する 64 ビットブロックの対称鍵による CBC (暗号ブロック連鎖) アルゴリズムです。

認証アルゴリズム

次の表に、SSL-VPN で設定可能な認証アルゴリズムを示します。

アルゴリズム	説明
MD5	MD5 (Message Digest バージョン 5) ハッシュアルゴリズム (一方向ハッシュ関数) は、デジタル署名アプリケーション向けに RSA Data Security が開発したアルゴリズムです。大きなファイルを秘密鍵/公開鍵アルゴリズムを使用して暗号化する前に、安全な方法で圧縮する必要がある場合に使用します。

アルゴリズム	説明
SHA1	SHA1 (Secure Hash Algorithm 1) では、160 ビットのメッセージダイジェストを生成します。メッセージダイジェストが大きく、ブルートフォースアタックによる衝突や反転攻撃に対するセキュリティが高まります。
SHA-256 および SHA-512	SHA2 (Secure Hash Algorithm 2) では、256 ビットまたは 512 ビットのメッセージダイジェストを選択できます。SHA-512 はメッセージダイジェストが最も大きく、ブルートフォースアタックによる衝突や反転攻撃に対するセキュリティが最も高まります。

IKE (Internet Key Exchange) プロトコル

IKE (Internet Key Exchange) プロトコルは、IPSec (IP Security) 形式のエンコードデータを転送するためのトンネルを作成するプロトコルです。

SSL VPN

Secure Socket Layer 仮想プライベートネットワーク (SSL VPN) は、標準の Web ブラウザで使用できる VPN の 1 つです。SSL VPN を使用するにはクライアントソフトウェアをインストールする必要があります。SSL VPN は、Web ベースのメール、ビジネスや政府機関のディレクトリ、ファイル共有、リモートバックアップ、リモートシステム管理、消費者レベルの電子商取引などのアプリケーションに適しています。

エンドポイントに対する完全な管理者権限があり、さまざまなアプリケーションを使用している場合は、トンネルモードにすることで、リモートクライアントからローカルの内部ネットワークに直接接続と同じようにアクセスできます。

注意

Cloud Edge では、IPv4 間の SSL VPN アクセスがサポートされます。

Cloud Edge ゲートウェイの特定のモデルでは、VPN がサポートされません。

SSL VPN を管理する

目的: 標準の Web ブラウザで VPN を使用できるように SSL VPN (Secure Socket Layer 仮想プライベートネットワーク) を設定します。

場所: ゲートウェイ > (ゲートウェイ名) > ユーザ VPN > SSL VPN > 一般

手順

1. 必要に応じて、SSL VPN を有効にします。
2. 基本設定を行います。
   - プロトコル
   - ポート
   - 新しいアドレスオブジェクトの追加
   - ローカルネットワーク
   - クライアントネットワークプール
3. 詳細設定を行います。
   - 暗号化アルゴリズム

     192 ページの「暗号化アルゴリズム」を参照してください。
   - 認証アルゴリズム

     192 ページの「認証アルゴリズム」を参照してください。
   - 鍵のサイズ
   - 鍵の有効期限
   - ローカル DNS
   - ローカルドメイン
   - 圧縮トラフィックを有効にする
   - デバッグモードを有効にする
   - 同時ログオンを有効にする

- IP マスカレードを有効にする

SSL VPN クライアントを確認する

目的: 現在 VPN で接続しているすべてのクライアントを表示します。ユーザ名、セッションの開始時間、クライアントのパブリック IP アドレス、および仮想 IP アドレスが表の形式で表示されます。また、接続しているクライアントの総数が表の上に表示されます。

場所: ゲートウェイ > (ゲートウェイ名) > ユーザ VPN > SSL VPN > クライアント

手順

1. SSL VPN を介して接続しているすべてのクライアントを表の形式で表示します。

SSL VPN のトラブルシューティングを行う

目的: SSL VPN を設定する際の一般的なトラブルシューティングのガイドラインを確認します。

場所: ゲートウェイ > (ゲートウェイ名) > ユーザ VPN > SSL VPN > トラブルシューティング

手順

1. 次の方法で SSL VPN のトラブルシューティングを行います。
   - エラーメッセージの詳細については、196 ページの「SSL VPN のエラーメッセージについて」を参照してください。
   - クライアントから Cloud Edge ゲートウェイへの ping が成功することを確認します。
   - SSL VPN で設定されている TCP ポートまたは UDP ポートにクライアントからアクセスできることを確認します。
   - Windows クライアントの設定ファイル `openvpn.ovpn` の設定が `https://<gateway_server_IP_address>/Config/openvpn.ovpn` ファイルと同じであることを確認します。

- モバイルクライアントの設定ファイル mobile.ovpn の設定が `https://<gateway_server_IP_address>/Config/mobile.ovpn` ファイルと同じであることを確認します。

SSL VPN のエラーメッセージについて

エラーメッセージ	説明	推奨される処理
`TCP: X.X.X.X:80` への接続に失敗しました。`5` 秒後に再試行します。接続は拒否されました	SSL VPN クライアントから Cloud Edge ゲートウェイに到達できません。	1. SSL VPN クライアントと Cloud Edge ゲートウェイの間で ping を使用できる (ブロックされていない) 場合は、Cloud Edge ゲートウェイへの ping を実行します。SSL VPN クライアントと Cloud Edge ゲートウェイの間でネットワーク接続が確立されていることを確認してください。 2. SSL VPN トラフィックを許可するには、SSL VPN で設定されている TCP ポートまたは UDP ポートを Cloud Edge ゲートウェイに対して開くようにネットワークファイアウォールを設定します。
`SIGTERM[soft,auth-failure]` を受信しました。プロセスを終了します。	ユーザ名またはパスワードが無効です。	正しいユーザ名とパスワードを指定するか、管理者に依頼してパスワードをリセットします。

L2TP VPN

Cloud Edge L2TP VPN を使用すると、インターネットなどのパブリックネットワークを介してリモートから社内ネットワークへの安全な接続を確立できます。

Cloud Edge では、L2TP トンネリングプロトコルを使用して、クライアントと Cloud Edge ゲートウェイの間のポイントツーポイント接続を確立します。L2TP トンネルを介してデータをエンドポイントに転送する前に、IPsec を使用して L2TP パケットが暗号化されるため、セキュリティが確保されます。L2TP が VPN トンネルを作成し、このトンネルを使用して IPsec 形式のエンコードデータが転送されます。L2TP はトンネルを作るプロセス、IPsec パケットはトンネルを通って暗号化データを運ぶトラックと考えることができます。

Cloud Edge では、Windows 7、8.1、10 クライアント、iOS、および Android モバイルクライアントで L2TP/IPsec VPN をサポートしています。

エンドユーザが VPN クライアントをインストールする必要はありません。Cloud Edge L2TP/IPsec VPN では、Windows の標準の L2TP/IPsec 設定を使用します。

Cloud Edge L2TP/IPsec VPN を使用する場合、初期設定ではクライアントからのすべてのデータが VPN 経由で送信されます。内部ネットワークへのトラフィックのみを VPN トンネルを介して送信するには、クライアントの L2TP 設定で VPN をスプリットトンネリングモードに設定します。

Cloud Edge は、エンドポイントが使用できなくなるか、または VPN が手動で切断されるまで、エンドポイントとの L2TP/IPsec 接続を維持します。

注意

Cloud Edge では、IPv4 間の L2TP VPN アクセスがサポートされます。

Cloud Edge ゲートウェイの特定のモデルでは、VPN がサポートされません。

関連情報

- 「仮想プライベートネットワーク」

L2TP VPN を管理する

目的: IPsec でリモートの Windows クライアントからの VPN として使用する L2TP VPN (Layer 2 Tunneling Protocol 仮想プライベートネットワーク) を設定します。

注意

L2TP VPN は、ルーティングモードの Cloud Edge ゲートウェイでのみ設定できます。

場所: ゲートウェイ > (ゲートウェイ名) > ユーザ VPN > L2TP VPN > 一般

手順

1. 必要に応じて、L2TP VPN を有効にします。
2. [クライアントネットワークプール] では、CIDR 形式で IPv4 アドレスプールを入力します。

   重要

   割り当てられる IP アドレスは、依存関係のないネットワークセグメントの一部である必要があります (他のインタフェースで使用しているものとは異なるネットワークセグメント)。
3. [事前共有鍵] に両方のエンドポイントで認識される鍵を入力します。

   この鍵は、接続を確立する際に L2TP エンドポイントを認証するために使用されます。

   リモートユーザは、接続を確立する前に、Cloud Edge のホスト対象ユーザを使用して認証資格情報を入力する必要があります。

   ホスト対象ユーザの設定方法については、255 ページの「ホスト対象のユーザとグループ」を参照してください。
4. 詳細設定を行います。
   - プライマリ DNS サーバ、セカンダリ DNS サーバ

     [プライマリ DNS サーバ] と [セカンダリ DNS サーバ] を両方とも空白にした場合、ゲートウェイの初期設定の DNS サーバが L2TP DNS サーバとして使用されます。
   - プライマリ WINS サーバ、セカンダリ WINS サーバ
   - MTU

サポートされる値の範囲は 500〜1400 です。これは必須フィールドです。[MTU] フィールドを空白にはできません。

- L2TP デバッグモードを有効にする
- Dead Peer 検出を有効にする

  Dead Peer 検出は、非アクティブ、つまり利用できない VPN ピアを特定する機能です。ピアが利用できないときに失われたリソースを復元するのに役立ちます。[Dead Peer 検出を有効にする] を選択すると、アイドルな接続に対して VPN トンネルが再確立され、必要に応じてデッド状態 (オフライン) の VPN ピアがクリーンアップされます。

  このオプションを使用すると、トンネル内に一切トラフィックが生成されていないときにトンネル接続を開いたままにすることができます。

- IP マスカレードを有効にする
- IKE の認証アルゴリズム
  - MD5
  - SHA1
  - SHA-256
  - SHA-512

  初期設定は SHA1 です。

  192 ページの「認証アルゴリズム」を参照してください。

- IPSec の認証アルゴリズム
  - MD5
  - SHA1
  - SHA-256
  - SHA-512

  初期設定は SHA1 です。

- IKE のデバッグ

  IKE デバッグを有効または無効にします。

5. [保存] をクリックします。

次に進む前に

すべてのトラフィックを VPN トンネル経由にしたくない場合は、Windows クライアントでスプリットトンネリングを設定します。

- 最初にクライアントで L2TP を設定し、L2TP VPN に接続する必要があります。
- L2TP 接続を切断し、L2TP の新しい接続を右クリックして [プロパティ] を選択します。
- [インターネット プロトコル バージョン 4 (TCP/IPv4)] を選択して [プロパティ] をクリックし、[詳細設定] をクリックします。
- [リモート ネットワークでデフォルト ゲートウェイを使う] をオフにして、スプリットトンネリングを有効にします。ゲートウェイの内部ネットワークへのトラフィックのみが L2TP ゲートウェイを介してルーティングされるようになります。

L2TP VPN クライアントを確認する

目的: 現在 L2TP VPN で接続しているすべてのクライアントを表示します。ユーザ名、セッションの開始時間、クライアントのパブリック IP アドレス、および仮想 IP アドレスが表の形式で表示されます。また、接続しているクライアントの総数が表の上に表示されます。

場所: ゲートウェイ > (ゲートウェイ名) > ユーザ VPN > L2TP VPN > クライアント

手順

1. L2TP VPN を介して接続しているすべてのクライアントを表の形式で表示します。

L2TP VPN のトラブルシューティングを行う

目的: L2TP VPN を設定する際の一般的なトラブルシューティングのガイドラインを確認します。

場所: ゲートウェイ > (ゲートウェイ名) > ユーザ VPN > L2TP VPN > トラブルシューティング

手順

1. 表示される L2TP および IPsec のリアルタイムログを確認します。

注意

IPsec のリアルタイムログは、L2TP およびサイト間 VPN で共通です。

サイト間 VPN

サイト間仮想プライベートネットワーク (191 ページの VPN) を使用すると、複数のオフィス間で、インターネットなどのパブリックネットワークを介した安全な接続を確立できます。サイト間 VPN は企業のネットワークを拡張し、ある場所にあるコンピュータリソースを別の場所からも利用できるようになります。サイト間 VPN を必要とする企業としては、世界中に多数の支社がある企業が挙げられます。

Cloud Edge は、IKE (Internet Key Exchange) プロトコルと IPsec (IP Security) プロトコルを使用して、暗号化されたトンネルを作成します。IKE は VPN トンネルを作成します。このトンネルは IPsec 形式のエンコードデータの転送に使用されます。IKE はトンネルを作るプロセスで、IPsec パケットはトンネルを通って暗号化データを運ぶトラックと考えることができます。

Cloud Edge ゲートウェイは、Encapsulated Security Payload (ESP) プロトコルを実装します。カプセル化されたパケットは通常のパケットと同じように認識され、任意の IP ネットワークを通じてルーティングできます。

IKE は、事前共有鍵または X.509 デジタル証明書に基づいて自動的に実行されます。必要に応じて、手動の鍵を指定することもできます。インタフェースモードは NAT/Route モードでのみサポートされ、VPN トンネルのローカル側の仮想インタフェースを作成します。

注意

Cloud Edge では、IPv4 間のサイト間 VPN アクセスがサポートされます。

Cloud Edge ゲートウェイの特定のモデルでは、VPN がサポートされません。

IPsec 接続

IPsec (VPN) トンネルは、既存の VPN 接続に関連付けられたセキュリティゲートウェイ上の仮想インタフェースです。

IP ルーティングでは、VPN ピアゲートウェイに直接接続されたポイントツーポイントインタフェースとして使用されます。

- アウトバウンドパケットは次のようにルーティングされます。
- 送信先アドレス X が指定された IP パケットが、ルーティングテーブルと照合される照合の結果、IP アドレス X は、ポイントツーポイントリンク (ピアゲートウェイ Y に関連付けられた VPN トンネルインタフェースである) 経由でルーティングされる必要があることが判明する
- パケットに仮想トンネルインタフェースが指定されているため、VPN カーネルがパケットを傍受する
- ピアゲートウェイ Y の適切な IPsec 認証タイプパラメータを使用してパケットが暗号化され、新しいパケットには送信先 IP としてピアゲートウェイ Y の IP アドレスが設定される
- 新しい送信先 IP に基づいて、Y のアドレスに対応するルーティングテーブルのエントリの物理インタフェースにパケットが再ルーティングされる

インバウンドパケットは次のようにルーティングされます。

- IPsec パケットにはゲートウェイ Y を経由するマシンが指定されている
- VPN カーネルが物理インタフェース上でパケットを傍受する
- VPN カーネルが送信元の VPN ピアゲートウェイを特定する
- VPN カーネルがパケットのカプセル化を解除し、元の IP パケットを抽出する

- ピア VPN ゲートウェイに対して VPN トンネルインタフェースが存在することを VPN カーネルが検出し、物理インタフェースから関連付けられた VPN トンネルインタフェースにパケットを再ルーティングする
- パケットに、VPN トンネルインタフェースを経由する IP スタックが指定される

サポートされる構成

- Yamaha VPN ルータは、Cloud Edge サイト間 VPN (非アグレッシブモード) の一部としてサポートされます。

注意

テスト済みのサポート対象モデルは、Yamaha FWX 120 および RTX 1200 です。

- Cloud Edge ゲートウェイには、エッジデバイス (インターネットに直接接続) または内部デバイス (ポート転送または NAT ルール用に設定された NAT デバイスの背後) を使用できます。
- Cloud Edge では、Cloud Edge 6.0 以降を実行する Cloud Edge ゲートウェイのデュアル WAN シナリオで、サイト間 VPN がサポートされます。

注意

Cloud Edge 5.x 以前を実行するゲートウェイの場合、デュアル WAN アクセスが有効な場合でも、VPN のサポート用に単一の WAN のみ構成できます。

- Cloud Edge ゲートウェイの特定のモデルでは、VPN がサポートされません。

サイト間 VPN トポロジ

VPN 設定を計画および作成する前に、サイト間 VPN の 3 種類のトポロジについて理解しておく必要があります。

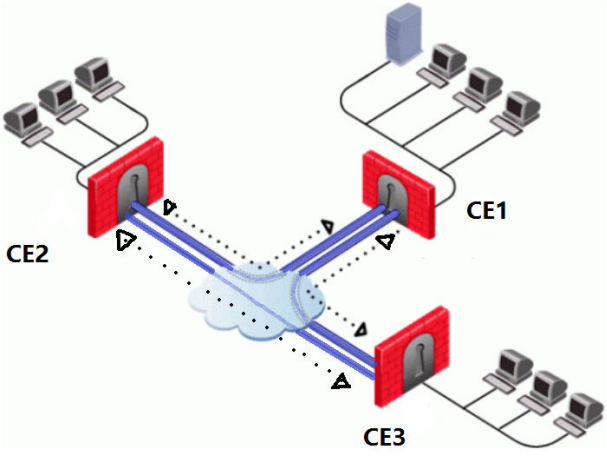
ピアツーピア VPN トポロジ

2 つのサイト間を単一の VPN ゲートウェイで暗号化します。

フルメッシュ VPN トポロジ

各リモートサイトが他のすべてのリモートサイトおよび中央のサイトに接続されます。すべてのリモートサイトが、中央のサイトに加え、他のすべてのリモートサイトとも直接通信できます。中央のサイトを介してルーティングする必要はありません。

フルメッシュ VPN は、メインのサイトが停止した場合でもすべてのリモートサイトで通信を継続できるため、信頼性に非常に優れています。また、各リモートサイトが他のリモートサイトと直接通信できるため、重要なアプリケーションの遅延時間も短くなります。



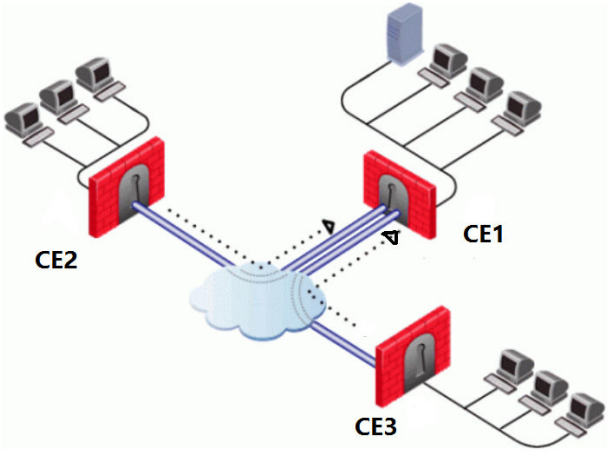
各デバイスで、最大 4 台の他のデバイス (サードパーティ製のデバイスを含む) との VPN 接続を設定できます。通信できるのは、直接接続された 2 つのピア間です。直接接続されていないピア同士は通信できません。

205 ページの「例: フルメッシュのサイト間 VPN」を参照してください。

スター VPN トポロジ

複数のリモートサイトがすべて中央のサイトに接続されます。このトポロジは、スポークとハブの構成に似ています。すべてのリモートサイトが中央のサイトとは直接通信できますが、他のリモートサイトと通信する場合は、中央のサイトを介して IPsec トラフィックを転送する必要があります。転送さ

れたトラフィックはハブデバイスによって送信先のリモートサイトにルーティングされます。



スタートポロジでは、1 台のハブデバイスと 4 台のスポークデバイス (サードパーティ製のデバイスを含む) がサポートされます (合計 5 台)。スポークデバイスはハブデバイスと直接通信できます。他のスポークデバイスと通信するときは、すべての IPsec トラフィックがハブデバイスに送信され、ハブデバイスを介して間接的に通信します。

208 ページの「例: スターのサイト間 VPN」を参照してください。

例: フルメッシュのサイト間 VPN

次の例では、3 つの Cloud Edge ゲートウェイを使用して、フルメッシュのサイト間 VPN 設定を作成しています。

設定の概要

デバイス名: CE1、CE2、CE3

- CE1 で、他の各デバイスへの接続を設定します (CE1 から CE2 への接続と CE1 から CE3 への接続の 2 つ)。
- CE2 で、他の各デバイスへの接続を設定します (CE2 から CE1 への接続と CE2 から CE3 への接続の 2 つ)。

- CE3 で、他の各デバイスへの接続を設定します (CE3 から CE1 への接続と CE3 から CE2 への接続の 2 つ)。

CE1 の設定


IPSec接続の追加/編集
IPSec接続を有効にする:
オン
オフ
名前:
CE1_CE2
インタフェース名:
eth0
対向ゲートウェイのIPアドレス:
IPアドレス
ゲートウェイ名
CE2
ローカルID:
CE1
リモートID:
CE2
新しいアドレスオブジェクトの追加
ローカルネットワークの追加:
CE1_local
リモートネットワークの追加:
CE2_local
認証の種類:
事前共有鍵
鍵:
鍵の確認:
ポリシー名:
初期設定
保存
キャンセル


IPSec接続の追加/編集
IPSec接続を有効にする:
オン
オフ
名前:
CE1_CE3
インタフェース名:
eth0
対向ゲートウェイのIPアドレス:
IPアドレス
ゲートウェイ名
CE3
ローカルID:
CE1
リモートID:
CE3
新しいアドレスオブジェクトの追加
ローカルネットワークの追加:
CE1_local
リモートネットワークの追加:
CE3_local
認証の種類:
事前共有鍵
鍵:
鍵の確認:
ポリシー名:
初期設定
保存
キャンセル

CE2 と CE3 の設定

CE2 と CE3 のゲートウェイについても、接続の設定は CE1 と同様です。

例: スターのサイト間 VPN

次の例では、3 つの Cloud Edge ゲートウェイを使用して、スターのサイト間 VPN 設定を作成しています。

設定の概要

デバイス名: CE1 (ハブ)、CE2 (スポーク)、CE3 (スポーク)

- ハブデバイス CE1 で、各スポークデバイスへの接続を設定します (CE1 から CE2 への接続と CE1 から CE3 への接続の 2 つ)。
- スポークデバイス CE2 で、ハブデバイス CE1 への接続を設定します (CE2 から CE1 への接続)。
- スポークデバイス CE3 で、ハブデバイス CE1 への接続を設定します (CE3 から CE1 への接続)。

CE1 (ハブ) の設定

CE1 から CE2 への接続:

- ローカル ID: CE1
- リモート ID: CE2

注意

CE2 は、CE2 ゲートウェイの設定ではローカル ID になります。

- ローカルネットワーク: CE1 と CE3 両方のローカルネットワークの IPv4 範囲を含むアドレスオブジェクト
- リモートネットワーク: CE2 のローカルネットワークの IPv4 範囲を含むアドレスオブジェクト

CE1 から CE3 への接続:

- ローカル ID: CE1
- リモート ID: CE3

注意

CE3 は、CE3 ゲートウェイの設定ではローカル ID になります。

- ローカルネットワーク: CE1 と CE2 両方のローカルネットワークの IPv4 範囲を含むアドレスオブジェクト
- リモートネットワーク: CE3 のローカルネットワークの IPv4 範囲を含むアドレスオブジェクト


IPSec接続の追加/編集
IPSec接続を有効にする:
オン
オフ
名前:
CE1_CE2
インタフェース名:
eth0
対向ゲートウェイのIPアドレス:
IPアドレス
ゲートウェイ名
CE2
ローカルID:
CE1
リモートID:
CE2
新しいアドレスオブジェクトの追加
ローカルネットワークの追加:
CE1_CE3
リモートネットワークの追加:
CE2_local
認証の種類:
事前共有鍵
鍵:
鍵の確認:
ポリシー名:
初期設定
保存
キャンセル


IPSec接続の追加/編集
IPSec接続を有効にする:
オン
オフ
名前:
CE1_CE3
インタフェース名:
eth0
対向ゲートウェイのIPアドレス:
IPアドレス
ゲートウェイ名
CE3
ローカルID:
CE1
リモートID:
CE3
新しいアドレスオブジェクトの追加
ローカルネットワークの追加:
CE1_CE2
リモートネットワークの追加:
CE3_local
認証の種類:
事前共有鍵
鍵:
鍵の確認:
ポリシー名:
初期設定
保存
キャンセル

CE2 (スポーク) の設定

CE2 から CE1 への接続:

- ローカル ID: CE2

> **注意**
> CE2 は、CE1 ゲートウェイの設定ではリモート ID になります。

- ローカルネットワーク: CE2 のローカルネットワークの IPv4 範囲を含むアドレスオブジェクト
- リモートネットワーク: CE1 と CE3 両方のローカルネットワークの IPv4 範囲を含むアドレスオブジェクト


IPSec接続の追加/編集
IPSec接続を有効にする:
オン
オフ
名前:
CE2_CE1
インタフェース名:
eth0
対向ゲートウェイのIPアドレス:
IPアドレス
ゲートウェイ名
CE1
ローカルID:
CE2
リモートID:
CE1
新しいアドレスオブジェクトの追加
ローカルネットワークの追加:
CE2_local
リモートネットワークの追加:
CE1_CE3
認証の種類:
事前共有鍵
鍵:
鍵の確認:
ポリシー名:
初期設定
保存
キャンセル

CE3 (スポーク) の設定


サイト間VPN
接続
ポリシー
詳細
ステータス
トラブルシューティング
追加
削除
有効にする
無効にする
検索
ステータス
名前
ローカルネットワーク
リモートネットワーク
ポリシー名
CE3_CE1
CE3_local
CE1_CE2
初期設定

CE3 から CE1 への接続:

- ローカル ID: CE3

注意

CE3 は、CE1 ゲートウェイの設定ではリモート ID になります。

- ローカルネットワーク: CE3 のローカルネットワークの IPv4 範囲を含むアドレスオブジェクト
- リモートネットワーク: CE1 と CE2 両方のローカルネットワークの IPv4 範囲を含むアドレスオブジェクト

フルメッシュのサイト間 VPN を設定する

フルメッシュのサイト間 VPN の設定は、複数の手順からなります。

各ゲートウェイに、他のすべてのゲートウェイへのトンネルを設定する必要があります。

手順

1. VPN の設定で必要になるローカルとリモートのアドレスオブジェクトを作成します。

   250 ページの「IP アドレス/FQDN オブジェクトを追加/編集する」

必要なアドレスオブジェクトについては、次の例を参考にしてください。
205 ページの「例: フルメッシュのサイト間 VPN」

2. IPsec VPN 接続を設定する際に使用する IPsec ポリシーを決めます。

   IPsec ポリシーは IPsec VPN 接続の設定時に選択します。初期設定の IPsec ポリシーを使用するか、別の既存のポリシーを使用するか、新しい IPsec ポリシーを追加できます。

   221 ページの「IPsec ポリシーを追加する」

3. 中央のハブゲートウェイで、各リモートゲートウェイへのトンネルを設定します。

   218 ページの「IPsec VPN 接続を追加する」

4. 各リモートゲートウェイで、他のすべてのリモートゲートウェイへのトンネルと中央のハブに戻るトンネルを設定します。

   218 ページの「IPsec VPN 接続を追加する」

5. 任意: Dead Peer 検出や IKE デバッグの有効化など、サイト間 VPN 設定の詳細なオプションを設定します。

   224 ページの「詳細なサイト間 VPN 設定を行う」

スターのサイト間 VPN を設定する

スターのサイト間 VPN の設定は、複数の手順からなります。

まず、中央のハブゲートウェイで、各リモートゲートウェイへのトンネル接続を設定する必要があります。次に、各リモートゲートウェイで、中央のハブに戻る接続を設定する必要があります。

手順

1. VPN の設定で必要になるローカルとリモートのアドレスオブジェクトを作成します。

   250 ページの「IP アドレス/FQDN オブジェクトを追加/編集する」

   必要なアドレスオブジェクトについては、次の例を参考にしてください。
   208 ページの「例: スターのサイト間 VPN」

2. IPsec VPN 接続を設定する際に使用する IPsec ポリシーを決めます。

   IPsec ポリシーは IPsec VPN 接続の設定時に選択します。初期設定の IPsec ポリシーを使用するか、別の既存のポリシーを使用するか、新しい IPsec ポリシーを追加できます。

   221 ページの「IPsec ポリシーを追加する」

3. 中央のハブゲートウェイで、各スポークデバイスへの接続を設定します。

   218 ページの「IPsec VPN 接続を追加する」

4. 各スポークゲートウェイで、ハブデバイスへの接続を設定します。

   218 ページの「IPsec VPN 接続を追加する」

5. 任意: Dead Peer 検出や IKE デバッグの有効化または無効化など、サイト間 VPN 設定の詳細なオプションを設定します。

   224 ページの「詳細なサイト間 VPN 設定を行う」

ピアツーピアのサイト間 VPN を設定する

ピアツーピアのサイト間 VPN の設定手順は、複数の手順からなります。

ピアツーピア構成では、ローカルゲートウェイとリモートゲートウェイが 1:1 で接続されます。

手順

1. VPN の設定で必要になるローカルとリモートのアドレスオブジェクトを作成します。

   250 ページの「IP アドレス/FQDN オブジェクトを追加/編集する」

2. IPsec VPN 接続を設定する際に使用する IPsec ポリシーを決めます。

   IPsec ポリシーは IPsec VPN 接続の設定時に選択します。

   初期設定の IPsec ポリシーを使用するか、別の既存のポリシーを使用するか、新しい IPsec ポリシーを追加できます。

   221 ページの「IPsec ポリシーを追加する」

3. 一方のピアデバイスで、もう一方のピアデバイスへの接続を設定します。

   218 ページの「IPsec VPN 接続を追加する」

4. もう一方のピアデバイスで、1 つ目のデバイスに戻る接続を設定します。

   218 ページの「IPsec VPN 接続を追加する」

5. 任意: Dead Peer 検出や IKE デバッグの有効化または無効化など、サイト間 VPN 設定の詳細なオプションを設定します。

   224 ページの「詳細なサイト間 VPN 設定を行う」

サイト間 VPN を管理する

サイト間 VPN の次の設定を管理できます。

- 217 ページの IPsec 接続を管理する
- 220 ページの IPsec ポリシーを管理する
- 224 ページの「詳細なサイト間 VPN 設定を行う」

IPsec VPN 接続を管理する

目的: Cloud Edge ゲートウェイやサードパーティ製デバイスの間に IPsec トンネルを確立するために使用するサイト間 IPsec VPN 接続を管理します。

場所: ゲートウェイ > (ゲートウェイ名) > サイト間 VPN > 接続

手順

1. サイト間 VPN の設定については、以下を参照してください。

   - 203 ページの「サポートされる構成」
   - 203 ページの「サイト間 VPN トポロジ」
   - 214 ページの「フルメッシュのサイト間 VPN を設定する」
   - 215 ページの「スターのサイト間 VPN を設定する」
   - 216 ページの「ピアツーピアのサイト間 VPN を設定する」
   - 225 ページの「複数のゲートウェイを経由する IPsec トラフィック向けの推奨設定」

2. 次の手順を実行します。
   - 新しい IPsec 接続を作成するには、[追加] をクリックします。
   - 設定を表示または変更するには、接続の名前をクリックします。

注意

既存のサイト間 VPN 接続では、ローカルネットワークまたはリモートネットワークの設定を変更できません。ローカルネットワークまたはリモートネットワークの設定を変更する場合は、既存のサイト間 VPN 接続を削除して、新たに接続を作成して設定する必要があります。

   - 接続を削除するには、接続を選択して [削除] をクリックします。
   - 接続を有効にするには、接続を選択して [有効にする] をクリックします。
   - 接続を無効にするには、接続を選択して [無効にする] をクリックします。

関連情報

- 「IPsec VPN 接続を追加する」

IPsec VPN 接続を追加する

目的: サイト間 IPsec VPN 接続を追加して、Cloud Edge ゲートウェイやサードパーティ製デバイスの間に IPsec トンネルを確立します。

場所: ゲートウェイ > (ゲートウェイ名) > サイト間 VPN > 接続

サポートされるサイト間 VPN トポロジとそれらのトポロジを実装する設定手順の詳細については、以下を参照してください。

- 203 ページの「サイト間 VPN トポロジ」
- 203 ページの「サポートされる構成」
- 214 ページの「フルメッシュのサイト間 VPN を設定する」

- 215 ページの「スターのサイト間 VPN を設定する」
- 216 ページの「ピアツーピアのサイト間 VPN を設定する」
- 225 ページの「複数のゲートウェイを経由する IPsec トラフィック向けの推奨設定」

注意

サイト間 VPN 接続の設定が完了すると、ローカルネットワークまたはリモートネットワークの設定を変更できません。設定の保存後にローカルネットワークまたはリモートネットワークの設定を変更する場合は、既存のサイト間 VPN 接続を削除して、新たに接続を作成して設定する必要があります。

手順

1. [追加] をクリックします。

   [IPSec 接続の追加/編集] 画面が表示されます。

2. IPsec の接続パラメータを指定します。

IPSec 接続を有効にする	[オン] を選択してトンネルを有効にします。
名前	IPsec VPN トンネルを識別する名前を入力します。
インタフェース名	リストからインタフェース名を選択します。
ゲートウェイ	次のいずれかの方法でゲートウェイを指定します。 IP アドレス: ゲートウェイの IP アドレスを指定します。 ゲートウェイ名: リストから使用可能なゲートウェイを選択します。 注意 VPN デバイスが Cloud Edge の場合、[IP アドレス] または [ゲートウェイ名] のどちらかを選択できます。VPN デバイスがサードパーティ製デバイスの場合は、[IP アドレス] を選択する必要があります。

ローカル ID	[ローカル ID] のテキスト文字列を入力します。Cloud Edge ではローカル ID を使用して、どのゲートウェイがトポロジ内でローカルかを特定します。
リモート ID	[リモート ID] のテキスト文字列を入力します。Cloud Edge ではリモート ID を使用して、どのゲートウェイがトポロジ内でリモートかを特定します。
ローカルネットワークの追加	ローカルネットワークを選択するか、新しいアドレスオブジェクトを追加します。
リモートネットワークの追加	リモートネットワークを選択するか、新しいアドレスオブジェクトを追加します。
認証の種類	リストから [事前共有鍵] または [RSA 鍵] を選択します。
[事前共有鍵] の場合	鍵を指定し、確認のためにもう一度入力します。 [事前共有鍵] を選択した場合、事前共有鍵を[鍵] に指定し、確認のために [鍵の確認] にもう一度入力します。この鍵が、リモートピアまたはダイヤルアップクライアントに対して Cloud Edge を認証する際に使用されます。鍵には 6 文字以上の印字可能文字を指定し、ネットワーク管理者以外には知られないようにします。現在知られている攻撃に対して最大限の防御を実現するには、ランダムな 16 文字以上の英数字で構成される鍵を使用してください。
ポリシー名	IPsec トンネルに適用する [初期設定] または特定のポリシーをリストから選択します。 注意 [ゲートウェイ] > [サイト間 VPN] > [ポリシー] に移動し、初期設定以外の IPsec ポリシーを設定します。221 ページの「IPsec ポリシーを追加する」を参照してください。

3. [保存] をクリックします。

IPsec ポリシーを管理する

目的: Cloud Edge ゲートウェイやサードパーティ製デバイスの間のサイト間 VPN トンネルを確立するために使用する IPsec ポリシーを管理します。

場所: ゲートウェイ > (ゲートウェイ名) > サイト間 VPN > ポリシー

手順

1. 次の手順を実行します。
   - 新しい IPsec ポリシーを作成するには、[追加] をクリックします。
   - 設定を表示または変更するには、ポリシーの名前をクリックします。
   - ポリシーを削除するには、ポリシーを選択して [削除] をクリックします。

IPsec ポリシーを追加する

目的: IPsec ポリシーを追加して、サイト間 VPN 接続に使用される IKE 暗号化および認証アルゴリズムを設定します。

場所: ゲートウェイ > (ゲートウェイ名) > サイト間 VPN > ポリシー

手順

1. [追加] をクリックします。

   [IPSec ポリシーの追加/編集] 画面が表示されます。
2. 新しい IPsec ポリシーの名前を指定します。
3. リストから [IKE の暗号化アルゴリズム] を選択します。

注意

DES (Digital Encryption Standard) は、56 ビット鍵を使用する 64 ビットのブロックアルゴリズムです。AES (Advanced Encryption Standard) は、128～256 ビットの鍵と可変長のデータブロックをサポートする秘密鍵アルゴリズムです。

オプション	説明
3DES	Triple-DES では、プレーンテキストが 3 つの鍵で 3 回暗号化されます。
AES 128	128 ビット鍵を使用する 128 ビットブロックの CBC (暗号ブロック連鎖) アルゴリズムです。
AES 192	128 ビット鍵を使用する 192 ビットブロックの CBC (暗号ブロック連鎖) アルゴリズムです。
AES 256	128 ビット鍵を使用する 256 ビットブロックの CBC (暗号ブロック連鎖) アルゴリズムです。

4. [IKE の認証アルゴリズム] をリストから 選択します。

   - MD5 - (Message Digest バージョン 5) ハッシュアルゴリズム (一方向ハッシュ関数) は、デジタル署名アプリケーション向けに RSA Data Security が開発したアルゴリズムです。大きなファイルを秘密鍵/公開鍵アルゴリズムを使用して暗号化する前に、安全な方法で圧縮する必要がある場合に使用します。
   - SHA1 - (Secure Hash Algorithm 1) は、160 ビットのメッセージダイジェストを生成します。メッセージダイジェストが大きく、ブルートフォースアタックによる衝突や反転攻撃に対するセキュリティが高まります。
   - SHA-256 - (Secure Hash Algorithm 2) は、256 ビットのダイジェストを生成します。ブルートフォースアタックによる衝突や反転攻撃に対するセキュリティがさらに高まります。
   - SHA-512 - (Secure Hash Algorithm 2) は、512 ビットのメッセージダイジェストを生成します。メッセージダイジェストが最も大きく、ブルートフォースアタックによる衝突や反転攻撃に対するセキュリティが最も高まります。

5. IKE SA の有効期限 (1〜24 時間) をリストから選択します。これは、ネゴシエートされたキーが有効な期間です。
6. 安全なゲートウェイでサポートされる IKE DH グループをリストから選択します。

   - グループ 2: MODP - 1024 ビット (初期設定)

- グループ 5: MODP - 1536 ビット
- グループ 14: MODP - 2048 ビット

  上記のグループは、Diffie-Hellman (DH) グループに基づく Diffie-Hellman 鍵交換 (指数鍵合意とも呼ばれる) を表しており、IKE および IPsec SA (Security Association) のセキュリティゲートウェイでサポートされます。

7. IPsec の暗号化アルゴリズムをリストから選択します。
   - 暗号化なし - 暗号化アルゴリズムを使用しません。
   - 3DES
   - AES 128
   - AES 192
   - AES 256
8. IPSec の認証アルゴリズムをリストから 選択します。
   - MD5
   - SHA1
   - SHA-256
   - SHA-512
9. IPsec の有効期限 (1〜24 時間) をリストから選択します。
10. IPsec PFS グループをリストから選択します。
    - なし
    - グループ 2: MODP
    - グループ 5: MODP
    - グループ 14: MODP
11. [保存] をクリックします。

詳細なサイト間 VPN 設定を行う

目的: Dead Peer 検出を使用するかどうかや、IKE のデバッグの有効化と無効化など、サイト間 VPN 設定の詳細なオプションを設定します。詳細な設定は、ゲートウェイのすべてのサイト間 VPN 接続に適用されます。

場所: ゲートウェイ > (ゲートウェイ名) > サイト間 VPN > 詳細

手順

1. 詳細なサイト間 VPN 設定を行います。

オプション	説明
Dead Peer 検出	Dead Peer 検出 (DPD) は、非アクティブ、つまり利用できない IKE ピアを特定する機能です。IPsec トラフィックのパターンファイルを使用して、接続が確立されているかどうかを最小限の IKE メッセージから判別します。DPD は、ピアが利用できないときに失われたリソースを復元するために使用します。[Dead Peer 検出を有効にする] を選択すると、アイドルな接続に対して VPN トンネルが再確立され、必要に応じてデッド状態 (オフライン) の VPN ピアがクリーンアップされます。
IKE のデバッグ	IKE デバッグを有効または無効にします。

2. [保存] をクリックします。

IPsec ステータス

目的: リアルタイムの IPsec 接続ステータスを表示します。

場所: ゲートウェイ > (ゲートウェイ名) > サイト間 VPN > スタータス

手順

1. IPsec ステータスを表示します。

IPsec のトラブルシューティング

IPsec のトラブルシューティングログを使用して、IPsec VPN トンネルでの処理を確認します。

IPsec 接続の特定の設定におけるパフォーマンスの問題や、それらの問題を軽減するための推奨されるベストプラクティスについて理解しておく必要があります。詳細については、225 ページの「複数のゲートウェイを経由する IPsec トラフィック向けの推奨設定」を参照してください。

複数のゲートウェイを経由する IPsec トラフィック向けの推奨設定

IPsec 接続の特定の設定におけるパフォーマンスの問題や、それらの問題を軽減するための推奨されるベストプラクティスについて理解しておく必要があります。

パフォーマンスの問題が発生する可能性があるのは、複数の Cloud Edge ゲートウェイがある環境で IPsec VPN 接続を複数設定している場合です。Cloud Edge では、複数の IPsec 接続を経由するトラフィックについて、各接続を通過するたびに検索を行います。しかし、検索の回数が増えても検出結果が向上するわけではなく、同じトラフィックを何度も検索することで結果的にパフォーマンスが低下することになります。

不要な検索が実行されないようにするには、受信トラフィックに最も近い Cloud Edge ゲートウェイで 1 回だけトラフィックを検索し、送信元から送信先までのルートにある他のゲートウェイでは検索をバイパスするように設定します。

これには、IPsec トラフィックに最も近いゲートウェイを除くすべてのゲートウェイで検索をバイパスするゲートウェイポリシールールを使用します。

推奨される設定のルール

設定におけるゲートウェイの役割	ルールのガイドライン
フルメッシュ IPsec ゲートウェイ	トラフィックの [処理] を [検索除外] に設定したポリシールールを作成し、次のようにフィールドに追加します。 • 送信先 ゲートウェイ自体のプライベートネットワークを含むネットワークオブジェクトを追加します。 • 送信元のユーザ/ユーザグループ/IP アドレス/FQDN/MAC アドレス メッシュ VPN の他のすべてのプライベートネットワークを含むネットワークオブジェクトを追加します。
スター IPsec ゲートウェイのスポーク	トラフィックの [処理] を [検索除外] に設定したポリシールールを作成し、次のようにフィールドに追加します。 • 送信先 ゲートウェイ自体のプライベートネットワークを含むネットワークオブジェクトを追加します。 • 送信元のユーザ/ユーザグループ/IP アドレス/FQDN/MAC アドレス スター VPN の他のすべてのプライベートネットワークを含むネットワークオブジェクトを追加します。
スター IPsec ゲートウェイのハブ	トラフィックの [処理] を [検索除外] に設定したポリシールールを作成し、次のようにフィールドに追加します。 • 送信先 すべてのプライベートネットワーク (それ自体のプライベートネットワークも含む) を含むネットワークオブジェクトを追加します。 • 送信元のユーザ/ユーザグループ/IP アドレス/FQDN/MAC アドレス スター VPN のすべてのスポークのプライベートネットワーク (それ自体のプライベートネットワークは除く) を含むネットワークオブジェクトを追加します。

例: 1 つのハブと 2 つのスポークで構成されるスターのサイト間 IPsec VPN

ゲートウェイ	役割	プライベートネットワーク	バイパスルール
スポーク IPsec ゲートウェイ (GS1)	スターのスポーク	NS1	• 処理: 検索除外 • 送信元: NH1、NS2 (他のすべてのプライベートネットワーク) • 送信先: NS1 (それ自体のプライベートネットワーク)
ハブ IPsec ゲートウェイ (GH1)	スターのハブ	NH1	• 処理: 検索除外 • 送信元: NS1、NS2 (他のすべてのプライベートネットワーク) • 送信先: NS1、NS2、NH1 (すべてのプライベートネットワーク)
スポーク IPsec ゲートウェイ (GS2)	スターのスポーク	NS2	• 処理: 検索除外 • 送信元: NH1、NS1 (他のすべてのプライベートネットワーク) • 送信先: NS2 (それ自体のプライベートネットワーク)

トラブルシューティングログを確認する

目的: IPsec のトラブルシューティングログを使用して、IPsec VPN トンネルでの処理を確認します。

場所: ゲートウェイ > (ゲートウェイ名) > サイト間 VPN > トラブルシューティング

手順

1. トラブルシューティングログを確認します。

アップデート

[アップデート] 画面を使用すると、トレンドマイクロから随時リリースされる Cloud Edge ゲートウェイのアップデートを簡単に実行できます。[アップデート] 画面には次の 2 つのセクションがあります。

- 利用可能なアップデート: 使用しているゲートウェイに対応する利用可能なアップデートがある場合、このセクションに表示されます。利用可能なアップデートの詳細を確認するには、[Readme] リンクをクリックして Readme ファイルを参照します。
- インストール済みのアップデート: このセクションには、すでにインストールされているアップデートが表示されます。

Cloud Edge ゲートウェイのアップデート

目的: Cloud Edge ゲートウェイのアップデートをインストールします。

場所: ゲートウェイ > (ゲートウェイ名) > アップデート

手順

1. インストールするアップデートの [処理] 列で [今すぐアップデート] をクリックします。

   選択したアップデートの詳細を確認するには、[Readme] リンクをクリックします。

   注意

   アップデートに他のファイルが必要な場合は、Cloud Edge によってそのファイルも自動的にインストールされます。

重要

HA グループの場合、アップデート (手動または予約) は特定の順序で実行されます。最初にスタンバイゲートウェイがアップデートされ、次にプライマリからセカンダリへのフェイルオーバーが行われます。フェイルオーバーが完了した後、プライマリがアップデートされます。次に、フェイルオーバーが再び実行され、プライマリがアクティブステータスに戻ります。このプロセス中、ネットワークが停止することはありません。

ゲートウェイが HA グループの一部であり、ゲートウェイの 1 つがオフラインであるか、HA グループがスプリットブレイン状態になっている場合、HA グループのゲートウェイに対する手動アップデートは許可されません。

ネットワークアクセスコントロールの管理

Cloud Edge Cloud Console を使用して、ネットワークアクセスコントロールを管理してエンドポイント保護を提供できます。

- Cloud Edge をウイルスバスター ビジネスセキュリティサービス (ウイルスバスター ビジネスセキュリティサービス) に統合することで、ウイルスバスター ビジネスセキュリティサービスエンドポイントに対してコンプライアンスチェックを実行できます。Cloud Edge は、ウイルスバスター ビジネスセキュリティサービスの古いビジネスセキュリティエージェントパターンがインストールされているウイルスバスター ビジネスセキュリティサービスエンドポイントや、ウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントがインストールされていないエンドポイントに対するネットワークアクセスコントロール機能を提供します。

  230 ページの「VBBSS エンドポイント保護」を参照してください。

- Cloud Edge は、エンドポイントのコンプライアンスチェックを行うことでセキュリティサービスを提供します。このコンプライアンスチェックでは、設定したしきい値を超える C&C コールバックが検出されたかどうかを確認します。Cloud Edge では、しきい値を超えているエンドポイントのネットワークアクセスコントロールを提供できます。

  238 ページの「不審エンドポイント」を参照してください。

VBBSS エンドポイント保護

ウイルスバスター ビジネスセキュリティサービスはエンドポイント用のセキュリティサービスです。セキュリティサービスを提供するには、ウイルスバスター ビジネスセキュリティサービスのエンドポイントにウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントをインストールする必要があります。ビジネスセキュリティエージェントはネットワークアクセスコントロールを管理する上で役立ちます。ビジネスセキュリティエージェントで使用されているパターンファイルが古い場合や、エンドポイントにエージェントがインストールされていない場合、コンプライアンスは保証されません。

Cloud Edge の VBBSS エンドポイント保護をウイルスバスター ビジネスセキュリティサービスに統合することで、コンプライアンスを適用することが可能になります。Cloud Edge では、エンドポイントのウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントで使用されているパターンファイルが古いかどうか、またはエンドポイントにウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントがインストールされているかどうかを確認することにより、エンドポイントのコンプライアンスチェックを実行できます。また、Cloud Edge では、コンプライアンスに違反しているエンドポイントのネットワークアクセスを制御することもできます。

注意

VBBSS エンドポイント保護では、IPv6 エンドポイントのチェックとコンプライアンスはサポートされません。

コンプライアンスチェックを有効にする

この機能は有効にする必要があります。初期設定では無効になっています。

この機能を有効にすると、次の 2 つの状況に対して実行する処理 (ブロックまたは検出) を指定できます。

- エンドポイントにウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントがインストールされているが、パターンファイルが古い場合。
- エンドポイントにウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントがインストールされていない場合。

Cloud Edge は 1 時間ごとにウイルスバスター ビジネスセキュリティサービスと情報を同期し、エンドポイントの最新のパターンステータスに関する新しい情報を取得します。

保護リスト

エンドポイントのコンプライアンスチェックは、自動的には実行されません。保護リストを設定し、コンプライアンス保護の対象とするエンドポイントを指定する必要があります。

- 保護リスト内のエンドポイントを対象として、エンドポイントにビジネスセキュリティエージェントがインストールされているかどうかが確認されます。また、ビジネスセキュリティエージェントがインストールされている場合は、パターンファイルが最新かどうかが確認されます。
- エンドポイントがコンプライアンスに従っていない場合は、設定された処理が実行されます。
- MAC アドレスまたは IPv4 アドレスを追加できます (単一アドレスまたはアドレス範囲)。
- 最大エントリ数は 256 です。

処理

コンプライアンスチェックの結果、保護リスト内でコンプライアンスに違反しているエンドポイントが見つかった場合は、Cloud Edge で次のいずれかの処理を実行できます。

- ブロック

  すべてのインターネットアクセスがブロックされます。

  例外: トラフィック/URL がグローバル許可リスト内にある場合、エンドポイントはブロックされません。DNS および DHCP へのトラフィックはブロックされません。

  VBBSS エンドポイント保護機能でエンドポイントがブロックされると、クライアントのブラウザは VBBSS エンドポイント保護違反の通知ページにリダイレクトされます。

注意

ビジネスセキュリティエージェントがインストールされていないエンドポイントに対する処理をブロックに設定した場合、ビジネスセキュリティエージェントがインストールされていないエンドポイントはインターネットにアクセスできなくなります。

これらのエンドポイントにビジネスセキュリティエージェントをインストールする場合は、次の URL を許可リストに追加する必要があり、これらを追加していない場合はインストールに失敗することがあります。

- `*.symcb.com/*`
- `*.digicert.com/*`
- `*.affirmtrust.com/*`
- `crl.microsoft.com/*`

また、ビジネスセキュリティエージェントがインストールされていないエンドポイントでトレンドマイクロ LMP サイトにアクセスする場合は、次の URL を許可リストに追加する必要があり、これらを追加していない場合はアクセス要求に影響することがあります。`www.google-analytics.com/*www.googletagmanager.com/*`

- 検出

  インターネットへのアクセスは許可されますが、VBBSS エンドポイント保護のトラブルシューティングページのログにアクセスが記録され、エンドポイントがコンプライアンスに違反している理由も記録されます。

例外リスト

例外リストを設定し、コンプライアンス保護の対象外とするエンドポイントを指定できます。コンプライアンス処理は例外リスト内のエンドポイントには適用されません。

- MAC アドレスまたは IPv4 アドレスを追加できます (単一アドレスまたはアドレス範囲)。
- 最大エントリ数は 256 です。

クライアントリスト

[クライアントリスト] セクションでは、過去 24 時間に Cloud Edge ゲートウェイによって検出されたすべてのエンドポイントを確認できます。

- リストは最初は空です。
- VBBSS エンドポイント保護を有効にして [適用] をクリックし、アップデートを Cloud Edge ゲートウェイに配信すると、過去 24 時間に Cloud Edge ゲートウェイを通過したトラフィックの送信元のエンドポイントに関する情報がリストにまとめられます。リストは Cloud Edge の [クライアントリスト] セクションに表示されます。

  VBBSS エンドポイント保護の配信後、利便性のため、エンドポイントは初回検出時に自動的に保護リストに追加されます。
- エンドポイントが検出された後は、リストされた各エンドポイントの [保護リスト] オプションまたは [例外リスト] オプションをクリックすると、そのエンドポイントを保護リストや例外リストに簡単に追加できます。

VBBSS エンドポイント保護を管理する

目的: ウイルスバスター ビジネスセキュリティサービスとの統合ソリューションである VBBSS エンドポイント保護を管理します。このソリューションは、ウイルスバスター ビジネスセキュリティサービスによるエンドポイントの保護の状況を確認し、コンプライアンスに従っていないエンドポイントのネットワークアクセスコントロールを管理します。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > VBBSS エンドポイント保護 > 一般

手順

1. 次の手順を実行します。
   - VBBSS エンドポイント保護を有効にします。
   - ウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントがインストールされていないエンドポイントに対する処理を選択します。初期設定は [検出] です。
   - 古いパターンファイルを使用しているウイルスバスター ビジネスセキュリティサービスのビジネスセキュリティエージェントがインス

トールされているエンドポイントに対する処理を選択します。初期設定は [検出] です。

- 保護リストにエンドポイントを追加するか、保護リストからエンドポイントを削除します。
- 例外リストにエンドポイントを追加するか、例外リストからエンドポイントを削除します。
- Cloud Edge ゲートウェイでエンドポイントのリストを確認します。
- Cloud Edge ゲートウェイのエンドポイントのリストを使用して、保護リストまたは例外リストに特定のエンドポイントを追加します。
- エンドポイントのリストを更新します。

VBBSS エンドポイント保護を設定する

目的: 新たに出現する脅威に対するゲートウェイセキュリティを強化するための設定を行います。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > VBBSS エンドポイント保護 > 一般

手順

1. 必要に応じて VBBSS エンドポイント保護を有効にします。
2. 以下のものに対する処理を選択します。
   a. ビジネスセキュリティエージェントがインストールされていないクライアント: 検出またはブロック
   b. 古いパターンファイルが使用されているビジネスセキュリティエージェントがインストールされたクライアント: 検出またはブロック
      - ブロック: すべてのインターネットアクセスがブロックされます。

        VBBSS エンドポイント保護機能でクライアントがブロックされると、クライアントのブラウザは VBBSS エンドポイント保護違反の通知ページにリダイレクトされます。
      - 検出: ネットワークリソースへのアクセスはログに記録されますが、ブロックはされません。これが初期設定です。

3. 保護リストを設定します。

   235 ページの「エンドポイントを保護リストに追加する」を参照してください。

4. 例外リストを設定します。

   236 ページの「エンドポイントを例外リストに追加する」を参照してください。

5. [適用] をクリックします。

エンドポイントを保護リストに追加する

目的: エンドポイントを VBBSS エンドポイント保護の保護リストに追加します。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > VBBSS エンドポイント保護 > 一般

手順

1. [保護リスト] にエンドポイントを追加します。

   a. [保護リスト] セクションで、[追加] をクリックします。

      [保護リストの追加] 画面が開きます。

   b. 以下を指定して、エンドポイントを保護リストに追加します。

オプション	説明
名前	どのようなエントリかを理解しやすい名前を指定します。 例: JSmith 例: Office
アドレスタイプ	[IPv4] または [MAC] を選択します。
IP/MAC アドレス	選択したタイプに応じて、適切な情報を入力します。 • IPv4: 情報をカンマで区切って入力します。

オプション	説明
	値には、単一 IP アドレス、IP アドレス範囲、または CIDR を指定できます。 例: 192.168.0.1,10.0.0.1-10.0.0.4,10.0.0.8/24 • MAC: 単一の MAC アドレスを入力します。 例: 00:FF:8A:B9:5A:49 例: 00-FF-8A-B9-5A-49

2. [保存] をクリックします。
3. 必要に応じて、その他のエンドポイントも保護リストに追加します。

   保護リストには 256 エントリまで追加できます。

エンドポイントを例外リストに追加する

目的: エンドポイントを VBBSS エンドポイント保護の例外リストに追加します。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > VBBSS エンドポイント保護 > 一般

手順

1. [例外リスト] にエンドポイントを追加します。
   a. [例外リスト] セクションで、[追加] をクリックします。

      [例外リストの追加] 画面が開きます。
   b. 以下を指定して、エンドポイントを例外リストに追加します。

オプション	説明
名前	どのようなエントリかを理解しやすい名前を指定します。 例: JSmith 例: Office
アドレスタイプ	[IPv4] または [MAC] を選択します。

オプション	説明
IP/MAC アドレス	選択したタイプに応じて、適切な情報を入力します。 • IPv4: 情報をカンマで区切って入力します。 値には、単一 IP アドレス、IP アドレス範囲、または CIDR を指定できます。 例: 192.168.0.1,10.0.0.1-10.0.0.4,10.0.0.8/24 • MAC: 単一の MAC アドレスを入力します。 例: 00:FF:8A:B9:5A:49 例: 00-FF-8A-B9-5A-49

2. [保存] をクリックします。
3. 必要に応じて、その他のエンドポイントも例外リストに追加します。

   例外リストには 256 エントリまで追加できます。

VBBSS エンドポイント保護のクライアントリストを確認する

目的: 現在 Cloud Edge ゲートウェイの管理下にあるすべてのエンドポイントを確認し、ウイルスバスター ビジネスセキュリティサービスのセキュリティエージェントのコンプライアンスをチェックします。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > VBBSS エンドポイント保護 > 一般

手順

1. 表内のすべてのエンドポイントの情報を確認します。
   - ホスト名
   - IP アドレス
   - MAC アドレス
   - ビジネスセキュリティエージェントがインストールされているかどうか

- インストールされている場合、ビジネスセキュリティエージェントで古いパターンファイルが使用されているかどうか
- OS (例: Windows 10)

2. (任意) [表示更新] をクリックし、リストの表示を更新します。
3. (任意) 選択したエンドポイントの [保護リスト] をクリックし、エンドポイントを保護リストに追加します。
4. (任意) 選択したエンドポイントの [例外リスト] をクリックし、エンドポイントを例外リストに追加します。

VBBSS エンドポイント保護のトラブルシューティングを行う

目的: VBBSS エンドポイント保護を使用する際の一般的なトラブルシューティング情報を確認します。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > VBBSS エンドポイント保護 > トラブルシューティング

手順

1. 次の方法で VBBSS エンドポイント保護のトラブルシューティングを行います。
   - 個々のログエントリを確認して、クライアントがブロックされた理由を確認します。
   - [表示更新] をクリックしてログを更新します。

不審エンドポイント

不審エンドポイントはエンドポイント用のセキュリティサービスです。不審エンドポイントを設定することにより、設定したしきい値を超える C&C コールバックが検出されるエンドポイントに対してネットワークアクセスコントロールを提供できます。

注意

- 不審エンドポイントでは、IPv6 エンドポイントについてのチェックとコンプライアンスは提供されません。
- Cloud Edge ゲートウェイとエンドポイントの間に NAT デバイスまたはプロキシがある場合、Cloud Edge ではクライアントの実際の IP アドレスを検出できず、代わりに Cloud Edge は NAT/プロキシデバイスに対する C&C コールバックイベントをカウントします。そのため、違反を引き起こす NAT/プロキシデバイスからの以降のトラフィックが設定に応じてブロックまたは監視されます。この動作は想定どおりにならないことがあります。

不審エンドポイントを有効にした後に指定できる処理

この機能は有効にする必要があります。初期設定では無効になっています。

この機能を有効にすると、設定したしきい値を超える C&C コールバックが Cloud Edge で検出された場合に実行する処理 (ブロックまたは監視) を指定できます。

指定した数のイベントが指定した期間に検出されるとしきい値に達したと見なされます。イベントの数と期間は設定することができます。

- イベント (初期設定では 50)

  範囲: 1〜1000

- 期間 (初期設定では 1 時間)

  有効な期間: 30 分、1 時間、6 時間、12 時間、1 日

Cloud Edge は定期的にエンドポイントと情報を同期し、更新された情報を取得します。

指定できる処理

コンプライアンスチェックの結果、しきい値の設定に違反しているエンドポイントが見つかった場合は、Cloud Edge で次のいずれかの処理を実行できます。

- ブロック

  すべてのインターネットアクセスがブロックされます。

  例外: トラフィック/URL がグローバル許可リスト内にある場合、エンドポイントはブロックされません。DNS および DHCP へのトラフィックはブロックされません。

  エンドポイントがブロックされると、クライアントのブラウザは不審エンドポイント違反の通知ページに送られます。

  注意

  処理を [ブロック] に設定すると、不審エンドポイントはインターネットにアクセスできません。

- 監視

  インターネットへのアクセスは許可されますが、不審エンドポイントが違反リストに追加されます。

違反リストの使用方法

[違反リスト] セクションで、不審アクティビティの検出数がしきい値を超えるすべてのエンドポイントに関する情報を確認できます。

- Cloud Edge は、不審エンドポイントの有効化後、しきい値を超えたエンドポイントを違反リストに追加します。
- 処理が [ブロック] に設定されている場合、違反リスト内の特定のエンドポイントをブロックしないようにするには、該当する行で [登録解除] をクリックします。

トラブルシューティングページのリストの使用方法

処理が [ブロック] に設定されている場合、違反しているためにブロックされたエンドポイントをトラブルシューティングページのリストで確認できます。

Cloud Edge ゲートウェイがオフラインの場合もリストは表示されますが、[登録解除] などの操作を実行することはできません。

不審エンドポイントを管理する

目的: 不審エンドポイントを管理します。これは、リスクがあるエンドポイントについてのコンプライアンスとネットワークアクセスを制御できるセキュリティサービスです。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > 不審エンドポイント > 一般

手順

1. 次の手順を実行します。
   - 不審エンドポイントを有効にします。
   - コンプライアンスに違反しているエンドポイントに対する処理を選択します。初期設定は [監視] です。
   - 処理が開始されるまでの指定した期間内において許可される C&C コールバックイベント数のしきい値を設定します。初期設定は 1 時間に 50 件のイベントです。
   - 違反リストを使用して、エンドポイントポリシーに違反しているエンドポイントに関する情報を表示します。
   - エンドポイントがブロックされないようにするには、選択したエンドポイントを違反リストから削除します。

不審エンドポイントを設定する

目的: 不審エンドポイントを設定することにより、新たな脅威に対するゲートウェイのセキュリティを強化します。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > 不審エンドポイント > 一般

手順

1. 必要に応じて不審エンドポイントを有効にします。
2. ポリシーに違反したエンドポイントに対して実行する処理を選択します。

- ブロック: すべてのインターネットアクセスがブロックされます。

  不審エンドポイント機能でエンドポイントがブロックされると、クライアントのブラウザは不審エンドポイント違反の通知ページに送られ、トラブルシューティング画面のログにイベントが記録されます。

- 監視 (初期設定): インターネットへのアクセスは許可されますが、不審エンドポイントが違反リストに追加されます。

3. C&C コールバックのしきい値を設定します。
   a. しきい値イベントの件数を入力します (初期設定: 50)。

      入力できる値の範囲は 1〜1000 です。

   b. しきい値イベントの件数がカウントされる期間を入力します (初期設定: 1 時間)。

      サポートされる値は、[30 分]、[1 時間]、[6 時間]、[12 時間]、および [1 日] です。

4. [適用] をクリックします。

不審エンドポイント違反リストを確認する

目的: すべてのエンドポイントの不審アクティビティを確認します。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > 不審エンドポイント > 一般

手順

1. 違反のあったすべてのエンドポイントの情報を確認します。
   - ホスト名
   - IP アドレス
   - 実行時間
2. (任意) [登録解除] をクリックして、選択したエンドポイントを違反リストから削除します。

不審エンドポイントのトラブルシューティングを行う

目的: 不審エンドポイントを使用する際の一般的なトラブルシューティング情報を確認します。

場所: ゲートウェイ > (ゲートウェイ名) > ネットワークアクセスコントロール > 不審エンドポイント > トラブルシューティング

手順

1. 次の方法で不審エンドポイントのトラブルシューティングを行います。
   - 個々のログエントリを確認して、不審アクティビティによってブロックされたエンドポイントを確認します。
   - [表示更新] をクリックしてログを更新します。

認識されたデバイス

Cloud Edge Cloud Console では、エンドポイントデバイスを検出、表示、管理できます。また Cloud Edge では、エンドポイントデバイスの脆弱性を検索できます。

Cloud Edge では、ネットワーク内に追加された新しいエンドポイントデバイスが自動的に検出されます。Cloud Edge でネットワーク内の新しいエンドポイントデバイスが検出されるまでには、数分かかる場合があります。Cloud Edge は、新しいエンドポイントデバイスを検出するために能動的にパケットを送信して調査を行い、Cloud Edge を経由してネットワークトラフィックを送信するエンドポイントデバイスを、受動的に検出します。

Cloud Edge ゲートウェイ 1 つにつき、最大 2,000 個のエンドポイントデバイスをサポートできます。

これらの機能を実行するには、[ゲートウェイ] > [(ゲートウェイ)] > [認識されたデバイス] から次の各画面を使用します。

- エンドポイントデバイス: この画面では、フィルタリング可能なエンドポイントデバイスのリストと、各エンドポイントデバイスの重大度および脆弱性の数が表示されます。詳細については、244 ページの「エンドポイントデバイス」を参照してください。

- 一般設定: この画面では、脆弱性検索の手動開始または予約を選択したり、認識モードを設定したりできます。詳細については、248 ページの「一般検索の設定」を参照してください。
- エンドポイントデバイスの詳細: この画面では、デバイスの詳細情報とそのデバイスの脆弱性が表示されます。詳細については、246 ページの「エンドポイントデバイスの詳細」を参照してください。

機能の大半は [認識されたデバイス] で実行できますが、次の項目はエンドポイントデバイス管理にも関連しています。

- 注意を必要とするデバイスカテゴリ: ダッシュボードの [デバイスマップとセキュリティ] タブに表示されます。このウィジェットでは、ネットワークトポロジ、脆弱性のあるエンドポイントデバイス数、インターネットのセキュリティ、およびポリシー施行について表示されます。
- ポリシールール: [ポリシー] に表示されます。この画面では、エンドポイントデバイスカテゴリに基づき、エンドポイントデバイスにポリシーを配信する際のオプションが表示されます。

エンドポイントデバイス

[エンドポイントデバイス] 画面には、Cloud Edge によりネットワーク内で検出されたエンドポイントデバイスに関する、次の情報が掲載された表が表示されます。

- 名前: デバイスの名前。
- デバイスカテゴリ: デバイスカテゴリは Cloud Edge により自動的に割り当てられます。
- IP アドレス: デバイスの IPv4 と IPv6 のアドレス。
- MAC アドレス: デバイスの MAC アドレス。
- 重大度: デバイスで検出された脆弱性および脆弱なパスワードの状況に基づく、重大度レベル。

  Cloud Edge では、重大度レベルは次のように示されます。

- - 緑: デバイスに開いているポートがある可能性があります。脆弱なパスワードや脆弱性は検出されていません。

- 黄: デバイスに脆弱なパスワードが使用されています。開いているポートがある可能性があります。脆弱性は検出されていません。
- 赤: デバイスに脆弱性があります。脆弱なパスワードと、開いているポートがある可能性があります。

- 脆弱性: デバイスで検出された脆弱性および脆弱なパスワードの数。

複数のエンドポイントデバイスを表示する

目的: Cloud Edge によってネットワーク上で検出された複数のエンドポイントデバイスを表示します。

場所: [ゲートウェイ] > (ゲートウェイ) > [認識されたデバイス] > [エンドポイントデバイス]

手順

1. (任意) デバイス名をクリックして、デバイスの情報と脆弱性に関する詳細を表示します。
2. (任意) テーブルの上部で期間を選択して、検出されたデバイスのその期間内での履歴を表示します。
3. (任意) テーブルの上部で表示更新ボタンをクリックして、Cloud Edge Cloud Console 画面を更新します。

注意

Cloud Edge ゲートウェイからの情報は更新されません。

---

4. (任意) テーブルの左側で特定のデバイスのカテゴリを選択して、テーブルに表示されているデバイスをフィルタリングします。
5. 列のヘッダーをクリックすると、その列に基づいてテーブルを並べ替えることができます。

注意

初期設定では、テーブルは [重大度]、次に [名前] で並べ替えられます。

---

6. (任意) テーブルの下部で、ページ切り替え用のコントロールを使用してテーブルの他のページに移動します。

エンドポイントデバイスの詳細

エンドポイントデバイスの詳細画面には、Cloud Edge によりネットワーク内で検出されたエンドポイントデバイスに関する、次の情報が表示されます。

- デバイス情報
  - 名前: デバイスの名前。
  - デバイスカテゴリ: デバイスカテゴリは Cloud Edge により自動的に割り当てられます。
  - IP アドレス: デバイスの IPv4 と IPv6 のアドレス。
  - MAC アドレス: デバイスの MAC アドレス。
  - ホスト名: デバイスのホスト名。
  - ブランド: デバイスのブランド。
  - モデル: デバイスのモデル。
- 脆弱性情報

注意

初期設定では、脆弱性と脆弱なパスワードの検索は無効となっています。この検索を有効にするには、248 ページの「一般検索の設定」を参照してください。

  - CVE ID: デバイスで検出された脆弱性のリスト。

注意

想定リスク、脆弱性の回避方法、詳細情報の入手先など、脆弱性に関する詳細な情報を表示するには、各脆弱性をクリックしてください。

- 脆弱なパスワード: デバイスで検出された、脆弱なパスワードが設定されているアプリケーションのリスト。

  Cloud Edge でパスワードの検索対象となるのは、SSH、FTP、および Telnet のアプリケーションのみです。

  注意

  想定リスクや脆弱なパスワードの回避方法など、脆弱なパスワードに関する詳細な情報を表示するには、各アプリケーション名をクリックしてください。

- 開いているポート: 開いている TCP/UDP ポートと、そのポートに通常関連付けられているアプリケーションのリスト。

  Cloud Edge では、次のポートのみが検索対象となります。

  - TCP: 21、22、23、53、80、135、139、443、445、515、554、631、2869、5000、5357、5432、7777、8008、8080、8192、9100、9700、12345、49152、49153、49154、49155、62078
  - UDP: 53、67、68、69、111、123、137、138、161、427、500、1022、1023、1026、1029、1812、1900、3702、4500、5353

1 つのエンドポイントデバイスを表示する

目的: Cloud Edge によってネットワーク上で検出された 1 つのエンドポイントデバイスに関する詳細と脆弱性を表示します。

場所: [ゲートウェイ] > (ゲートウェイ) > [認識されたデバイス] > [エンドポイントデバイス] > (デバイス)

手順

1. (任意) [CVE ID] または [開いているポート] で [すべて表示] をクリックし、その他の項目を表示します。
2. (任意) CVE ID または脆弱なパスワードをクリックして詳細を表示します。

3. (任意) [すべてのデバイスに戻る] をクリックして、すべてのデバイスのリストに戻ります。

一般検索の設定

Cloud Edge では、CVE リストに基づくエンドポイントデバイスの脆弱性検索と、脆弱なパスワードの検索が可能です。また、Cloud Edge では、詳細認識モードを使用して、開いているポートやエンドポイントデバイスのカテゴリを識別できます。

脆弱性検索の実行後、検索結果は次の画面に表示されます。

- エンドポイントデバイス: この画面では、フィルタリング可能なエンドポイントデバイスのリストと、各エンドポイントデバイスの重大度および脆弱性の数が表示されます。詳細については、244 ページの「エンドポイントデバイス」を参照してください。
- エンドポイントデバイスの詳細: この画面では、デバイスの詳細情報とそのエンドポイントデバイスの脆弱性が表示されます。詳細については、246 ページの「エンドポイントデバイスの詳細」を参照してください。
- 注意を必要とするデバイスカテゴリ: ダッシュボードの [デバイスマップとセキュリティ] タブに表示されます。このウィジェットでは、ネットワークトポロジ、脆弱性のあるエンドポイントデバイス数、インターネットのセキュリティ、およびポリシー施行について表示されます。

一般検索の設定を行う

目的: 脆弱性検索を実行または予約します。また、検出されたエンドポイントデバイスのための認識モードを設定します。

場所: [ゲートウェイ] > (ゲートウェイ) > [認識されたデバイス] > [一般設定]

注意!

初期設定では、脆弱性と脆弱なパスワードの予約検索は無効となっています。この予約検索は、セキュリティソフトウェアやセキュリティデバイスにより、セキュリティイベントとして検出されることがあります。

手順

1. (任意) 認識モードを、次のオプションのどちらかに切り替えます。
   - 詳細
   - 標準

   注意

   詳細認識モードでは、アクティブ検索を使用して、エンドポイントデバイスのカテゴリと開いているポートを識別できます。標準認識モードを選択すると、デバイスカテゴリの識別の精度が低くなる可能性があります。
2. (任意) 脆弱性検索を手動で実行するには、[検索開始] をクリックします。
3. (任意) 脆弱性の予約検索を有効にするには、[有効] で [オン] を、無効にするには [オフ] を選択します。
   a. [オン] を選択した場合は、検索の頻度を選択します。

IP アドレス/FQDN オブジェクトを管理する

目的: アドレスオブジェクトの管理作業として、IPv4、IPv6、および FQDN アドレスオブジェクトの追加、変更、複製、削除を実行します。

場所: ポリシー > アイデンティティオブジェクト > IP アドレス/FQDN

手順

1. 次の手順を実行します。
   - 新しいオブジェクトを作成するには、[追加] をクリックします。
   - 設定を表示または変更するには、オブジェクトの名前をクリックします。
   - オブジェクトをコピーするには、オブジェクトを選択して [複製] をクリックします。
   - オブジェクトを削除するには、オブジェクトを選択して [削除] をクリックします。

2. 必要な設定を行います。
3. [保存] をクリックします。

IP アドレス/FQDN オブジェクトを追加/編集する

目的: アドレスオブジェクトを追加または編集します。このオブジェクトは、IPv4 アドレス、IPv6 アドレス、または FQDN オブジェクトを設定するときに使用します。

場所: ポリシー > アイデンティティオブジェクト > IP アドレス/FQDN > [追加/編集]

手順

1. IP アドレス/FQDN オブジェクトの名前を指定します。
2. オブジェクトの種類を選択します。

   選択できる種類: IPv4、IPv6、または FQDN

   ブリッジモードまたはソフトウェアスイッチ

   Cloud Edge ゲートウェイをブリッジモードで実行している場合や、ソフトウェアスイッチとして実行している場合は、Cloud Edge で IPv6 がサポートされます。

   - IPv4 アドレスオブジェクトと IPv6 アドレスオブジェクトの両方を設定できます。
   - FQDN は IPv4 アドレスまたは IPv6 アドレスに解決できます。

   ルーティングモード

   Cloud Edge ゲートウェイがルーティングモードで実行されている場合は、Cloud Edge で IPv6 はサポートされません。

   - 設定できるのは、IPv4 アドレスオブジェクトのみです。
   - FQDN は IPv4 アドレスに解決する必要があります。
3. IP アドレスまたは FQDN を指定します。複数指定する場合はカンマで区切ります。

IP アドレスオブジェクトには、単一アドレス、アドレス範囲、または Class InterDomain Routing (CIDR) ネットワークを指定できます。

例:

- `192.168.0.1`
- `10.0.0.1-10.0.0.4`
- `10.0.0.8/23`
- `fd00:1:1111:200::1fff`
- `fd00:1:1111:200::1000-fd00:1:1111:200::1fff`
- `fd00:1:1111:200::1000/116`
- `host.example.com`
- `example.com`
- `*.com`
- `*example.com`
- `*.example.com`

注意

上記の例で示したとおり、FQDN オブジェクトは、あいまい一致にワイルドカード文字 (*) を使用できます。ワイルドカードは FQDN の途中や末尾ではなく先頭のみで使用するように注意してください。

4. [保存] をクリックします。

IP アドレス/FQDN オブジェクトのパラメータ

次の表に、設定可能な IPv4 アドレスオブジェクト、IPv6 アドレスオブジェクト、および FQDN (完全修飾ドメイン名) オブジェクトのパラメータを示します。

表 6-6. アドレスオブジェクトのパラメータ

パラメータ	説明
オブジェクト名	オブジェクトの内容がわかるように名前を指定します。この名前は、セキュリティポリシーを定義するときにアドレスのリストに表示されます。大文字と小文字が区別され、一意の名前を指定する必要があります。使用できる文字は、英字、数字、スペース、ハイフン、およびアンダースコアのみです。
種類	次のいずれかで、アドレスの種類を指定します。 • IPv4 • IPv6 • FQDN ブリッジモードおよびソフトウェアスイッチで使用するオブジェクトには、IPv4 アドレスと IPv6 アドレスの両方を設定できます。また、FQDN は IPv4 アドレスか IPv6 アドレスのどちらかに解決できます。 ルーティングモードで使用するオブジェクトには、IPv4 アドレスを設定できます。FQDN は IPv4 アドレスに解決する必要があります。

パラメータ	説明
アドレス	IPv4 アドレス: 次のいずれかの形式で IP アドレスまたはネットワークを指定します。 • ip_address • ip_address_range • ip_address/bitmask 例: 192.168.1.1、192.168.1.1-192.168.1.10、または 192.168.80.0/24 IPv6 アドレス 次のいずれかの形式で IPv6 アドレスまたはネットワークを指定します。 • ipv6_address • ipv6_address_range • ipv6_address/bitmask (IPv6 CIDR) 例: 2001:db8:123:1::1、2001:db8:123:1::1-2001:db8:123:1::10、または 2001:db8:123:1::/64 FQDN 次のいずれかの形式で FQDN を指定します。 • [domain].[tld] • [hostname].[domain].[tld]  注意 FQDN オブジェクトは、あいまい一致にワイルドカード文字 (*) を使用できます。ワイルドカードは FQDN の途中や末尾ではなく先頭のみで使用するように注意してください。 例: • 完全な FQDN: example.com または host.example.com

パラメータ	説明
	• ワイルドカードを含む FQDN: `*.com`、`*example.com`、または`*.example.com` 注意 FQDN オブジェクトタイプは、送信元/送信先の接続に一致するポリシールールを設定する場合にのみ使用できます。

ユーザ認証

認証設定

エンドユーザの認証で使用する認証ソースと認証キャッシュ設定を定義します。

- ホスト対象のユーザアカウント、LDAP アカウント、または RADIUS アカウントによるユーザ認証。
- Cloud Edge では、2 種類の認証キャッシュ有効期間 (TTL) オプションがサポートされます。
  - 固定 TTL (最初の検出) - ユーザが最後に認証された時間がキャッシュされます。初期設定: 2 時間
  - 前回アクティブになった時点からの TTL (最後の検出) - ユーザが Cloud Edge と最後に通信した時間がキャッシュされます。初期設定: 2 時間

認証の設定を行う

目的: 認証設定を認証ソースと認証キャッシュ TTL に使用します。

場所: [管理] > [ユーザ認証] > [認証設定]

手順

1. [認証ソース] で、次のいずれかのオプションを選択します。

- ホスト対象のユーザ

  Cloud Edge で設定した資格情報を使用してログオンします。詳細については、255 ページの「ホスト対象のユーザとグループ」を参照してください。

- LDAP

  LDAP 認証を使用してログオンします。詳細については、261 ページの「LDAP 設定」を参照してください。

- RADIUS

  RADIUS 認証を使用してログオンします。詳細については、264 ページの「RADIUS 設定」を参照してください。

2. [認証キャッシュ] で、次のいずれかを選択し、TTL の時間数を選択します。
   - 固定 TTL (時間)
   - 前回アクティブになった時点からの TTL (時間)
3. [保存] をクリックします。

注意

- Cloud Edge 6.0 以降のゲートウェイは、LDAP による認証をサポートしています。
- Cloud Edge 6.0 SP3 以降のゲートウェイは、RADIUS による認証をサポートしています。

ホスト対象のユーザとグループ

VPN またはキャプティブポータル経由のログオンをユーザに許可するには、Cloud Edge Cloud Console でホスト対象のユーザアカウントを作成します。ホスト対象のユーザをホスト対象のグループに割り当てることで、それらのすべてのホスト対象のユーザを対象とするポリシーを配信することもできます。VPN とキャプティブポータルは Cloud Edge Cloud Console で管理します。

ホスト対象のユーザとグループは同じ企業のすべてのゲートウェイで同期されます。必要に応じて、この同期された情報に基づいてポリシーを設定したりレポートを実行したりできます。

認証にホスト対象のユーザとグループを使用している場合、ホスト対象のユーザアカウントを無効にすると、そのユーザは VPN およびキャプティブポータルにログオンできなくなります。

注意

VPN をサポートしていない Cloud Edge ゲートウェイモデルの場合は、ホスト対象のユーザとグループを使用すると、キャプティブポータル経由でログオンできるようになります。

IPv6 トラフィックの場合、ユーザ認証はサポートされません。管理アクセスや、セキュリティ制御にユーザを使用するポリシーや、キャプティブポータルなど、ユーザ認証に依存する機能もサポートされません。

ホスト対象のユーザを管理する

目的: ホスト対象のユーザを管理して、ゲートウェイで管理されているリソースへのアクセスをエンドユーザに許可します。

場所: 管理 > ユーザ認証 > ホスト対象のユーザとグループ > ホスト対象のユーザ

手順

1. 次の手順を実行します。
   - 新しいホスト対象のユーザアカウントを作成するには、[追加] をクリックします。
   - ユーザアカウントを探すには、右上にある [検索] を使用します。
   - 設定を表示または変更するには、ホスト対象のユーザのアカウント名をクリックします。
   - ホスト対象のユーザによる VPN およびキャプティブポータルへのログオンを許可するには、そのアカウントを選択して [有効にする] をクリックします。

- ホスト対象のユーザによる VPN およびキャプティブポータルへのログオンをブロックするには、そのアカウントを選択して [無効にする] をクリックします。
- ホスト対象のユーザを削除するには、ユーザを選択して [削除] をクリックします。

ホスト対象のユーザを追加/編集する

目的: ホスト対象のユーザを追加して、VPN またはキャプティブポータルを介したログオンを許可します。

場所: 管理 > ユーザ認証 > ホスト対象のユーザとグループ > ホスト対象のユーザ > ユーザの追加/編集

手順

1. ホスト対象のユーザを有効にします。
2. ユーザの詳細を指定します。
3. ホスト対象のユーザを既存のホスト対象のグループに割り当てます。必要に応じて、新規のホスト対象のグループに割り当てることもできます。

   258 ページの「ホスト対象のグループを追加/編集する」を参照してください。
4. キャプティブポータルまたは VPN ポータルのパスワードの変更をユーザに許可する場合は、対応するチェックボックスをオンにします。

   警告!

   このチェックボックスは、同じアカウントを複数のユーザで共有する場合はオンにしないでください。ユーザによってパスワードが変更され、他のユーザがアクセスできなくなることがあります。
5. [保存] をクリックします。

ホスト対象のグループを管理する

目的: ホスト対象のグループを管理してホスト対象のユーザを整理し、類似するホスト対象のユーザをより効率的に管理できるようにします。

場所: 管理 > ユーザ認証 > ホスト対象のユーザとグループ > ホスト対象のグループ

手順

1. 次の手順を実行します。
   - 新しいホスト対象のグループを作成するには、[追加] をクリックします。
   - ホスト対象のグループを探すには、右上にある [検索] を使用します。
   - 設定を表示または変更するには、ホスト対象のグループのアカウント名をクリックします。
   - 関連付けられたホスト対象のユーザによる VPN およびキャプティブポータルへのログオンを許可するには、ホスト対象のグループを選択して [有効にする] をクリックします。
   - 関連付けられたホスト対象のユーザによる VPN およびキャプティブポータルへのログオンをブロックするには、ホスト対象のグループを選択して [無効にする] をクリックします。
   - ホスト対象のグループを削除するには、グループを選択して [削除] をクリックします。

ホスト対象のグループを追加/編集する

目的: ホスト対象のグループを作成します。ホスト対象のグループにホスト対象のユーザを割り当てることで、それらのすべてのホスト対象のユーザに対するポリシーを配信できます。

場所: 管理 > ユーザ認証 > ホスト対象のユーザとグループ > ホスト対象のグループ > グループの追加/編集

手順

1. ホスト対象のグループの詳細を指定します。
2. [保存] をクリックします。

ホスト対象のユーザとグループをインポート/エクスポートする

目的: ユーザとグループをインポートまたはエクスポートします。ホスト対象のユーザ/ホスト対象のグループの作成や更新を簡単に実行できるほか、設定のバックアップとして使用することもできます。

場所: 管理 > ユーザ認証 > ホスト対象のユーザとグループ > インポート/エクスポート

手順

1. 次のように実行します。
   - ホスト対象のユーザとグループをインポートするには、CSV ファイルを選択し、[インポート] をクリックします。

     必要に応じて、該当するチェックボックスをオンにすることで、インポートで競合が発生したときに既存のユーザやグループを上書きすることができます。重複があった場合に既存のホスト対象のユーザ/グループの情報を保持する場合は、このチェックボックスをオフ (初期設定) のままにしてください。

     注意

     インポートファイルの設定の詳細については、260 ページの「インポートファイルを準備する」を参照してください。
   - ホスト対象のユーザとグループを CSV ファイルにエクスポートするには、[エクスポート] をクリックします。

注意

ホスト対象のユーザが割り当てられていないホスト対象のグループは、CSV ファイルにエクスポートされません。CSV ファイルには、ホスト対象のユーザが割り当てられているホスト対象のグループだけがエクスポートされます。

インポートファイルを準備する

Cloud Edge Cloud Console は、より多くの言語をサポートするために CSV ファイルで UTF-8 エンコードを使用します。一部の表計算プログラム (Microsoft Excel) では、UTF-8 でエンコードされた CSV ファイルを正しく表示するために追加の設定が必要です。

注意

ホスト対象のユーザおよびグループの CSV ファイルの作成には Google スプレッドシートを使用することをお勧めします。

手順

1. CSV ファイルを次の形式で作成します。

```
user name, full name, email address, group, description, enable, password
juser, joe user, joeuser@example.com, group1, user's group, yes, asdg#2345
```

2. CSV ファイルを Microsoft Excel などのスプレッドシートプログラムで開きます。
3. [ファイル] > [名前を付けて保存] に移動します。
4. [ファイルの種類] ドロップダウンメニューから、[CSV (カンマ区切り) (*.csv)] を選択します。
5. [保存] をクリックします。
6. Microsoft Excel を使用している場合は、[はい] をクリックして確定します。
7. この CSV ファイルをメモ帳などのテキストエディタで開きます。

8. [ファイル] > [名前を付けて保存] に移動します。
9. [文字コード] ドロップダウンメニューを [UTF-8] に設定します。
10. [保存] をクリックします。

LDAP 設定

Cloud Edge 6.0 以降のゲートウェイは、LDAP (Lightweight Directory Access Protocol) による認証をサポートしています。LDAP サーバを使用すると、ユーザ固有またはグループ固有のポリシーの作成が便利になります。ユーザはキャプティブポータルまたは VPN ポータルを介して LDAP を使用して認証できます。イベントログ、レポート、および通知は、ユーザの認識に LDAP の階層を使用します。

重要

Cloud Edge G3 デバイスでは、LDAP または Radius がサポートされません。

Cloud Edge は以下で LDAP をサポートしています。

- Microsoft Windows 2012R2、Windows 2016、Windows 2019
- OpenLDAP

LDAP 認証

LDAP 設定を使用して、Cloud Edge と統合する LDAP サーバを指定します。Cloud Edge では、指定された LDAP サーバを使用して以下を実行します。

- キャプティブポータルで識別されるユーザの認証
- VPN ポータルで識別されるユーザの認証
- ポリシールール設定で送信元として LDAP ユーザまたはグループを使用する
- レポートの追加または編集時に [レポートの基準] フィールドで LDAP ユーザまたはグループを使用する

LDAP に対するユーザの設定を簡素化するため、Cloud Edge では LDAP のセットアップに基本認証と詳細認証の両方を使用できます。

LDAP 設定を行う

目的: ユーザ認証用の LDAP 設定を行います。

場所: [管理] > [ユーザ認証] > [LDAP 設定]

手順

1. 次のオプションのいずれかを選択します。

基本	[ドメイン名]、[ユーザ名]、および [パスワード] を指定します。詳細については、263 ページの「LDAP の基本認証」を参照してください。
詳細	LDAP サーバとのバインド、LDAP サーバの追加、認証方法の選択に使用する認証サーバ、ベース DN、ユーザ名、パスワードを指定します。詳細については、263 ページの「LDAP の詳細認証」を参照してください。

重要

Cloud Edge G3 デバイスでは、LDAP または Radius がサポートされません。

2. [LDAP サーバ接続のテスト] をクリックします。

注意

[LDAP サーバ接続のテスト] ボタンをクリックした後、選択したゲートウェイを使用して自動的に接続がテストされます。特定のゲートウェイを選択する場合は、[同期またはテストするゲートウェイの選択] の横にあるリストから選択します。

3. [保存] をクリックします。

LDAP の基本認証

Cloud Edge では、最も普及している LDAP サービスである Microsoft Active Directory (AD) に対して LDAP の簡易設定を実行できます。Active Directory を使用する場合は、ドメイン名、ユーザ名、およびパスワードの基本情報を Cloud Edge Cloud Console に入力してユーザの識別方法を設定します。

この情報をもとに、Cloud Edge は Active Directory の自動検出ツールを使用して次の必要な情報を取得します。

- LDAP サーバのアドレス
- 基本ドメイン名
- 認証情報 (Kerberos のレルム/ドメイン/KDC)

この情報は、LDAP の詳細認証の各フィールドに入力されます。管理者は、自動検出の結果が正しくない、または自動検出が機能していないと判断した場合、詳細モードに切り替えて設定を変更できます。

LDAP サーバのアドレスについては、自動検出ツールがドメインのすべてのドメインコントローラを判別し、Cloud Edge はその中から最も高速なサーバを 2 台選択して使用します。

LDAP の詳細認証

LDAP に精通しているユーザは、Cloud Edge で詳細認証モードを設定できます。

詳細モードの設定では、ユーザが LDAP サーバを追加、削除、移動、表示更新できます。

Cloud Edge では、次の種類の LDAP サーバがサポートされます。

- Microsoft Active Directory
- OpenLDAP

Cloud Edge では、これらのサーバ間の「フェイルオーバー」関係のみがサポートされます。プライマリサーバの認証に失敗すると、Cloud Edge はセカンダリサーバの認証を試みます。

注意

Cloud Edge では、同一ドメイン内の複数の LDAP サーバ間のフェイルオーバーのみがサポートされます。異なるドメインの LDAP サーバ間でのフェイルオーバーはサポートされません。

Cloud Edge では、Microsoft Active Directory と OpenLDAP の両方で、次の LDAP 認証方法がサポートされます。

- 簡易
- 詳細 (Kerberos)

設定済みの LDAP サーバの認証機能を確認したり結果のレポートを作成したりするには、基本モードと詳細モードの両方で、[LDAP サーバ接続のテスト] ボタンをクリックします。

RADIUS 設定

Cloud Edge 6.0 SP3 以降のゲートウェイは、RADIUS による認証をサポートしています。ユーザはキャプティブポータルまたは VPN ポータルを介して RADIUS を使用して認証を実行できます。また、設定でユーザとグループを追加した後、Cloud Edge でユーザ固有またはグループ固有のポリシーを作成することもできます。Cloud Edge では以下で RADIUS をサポートしています。

- Microsoft Windows 2012R2、Windows 2016、Windows 2019 のネットワークポリシーサーバー。
- FreeRADIUS 3.0.13 以降。

RADIUS 認証

RADIUS 設定を使用して、Cloud Edge と統合する RADIUS サーバを指定します。Cloud Edge では、指定された RADIUS サーバを使用して以下を実行します。

- キャプティブポータルで識別されるユーザの認証
- VPN ポータルで識別されるユーザの認証
- ポリシールール設定で送信元として RADIUS ユーザまたはグループを使用する

- レポートの追加または編集時に [レポートの基準] フィールドで RADIUS ユーザを使用する

RADIUS 認証を実行するために、RADIUS サーバおよび RADIUS ユーザまたはグループを設定できます。

RADIUS 設定を行う

目的: ユーザ認証用の RADIUS 設定を行います。

場所: [管理] > [ユーザ認証] > [RADIUS 設定] > [一般設定]

手順

1. [プライマリ RADIUS サーバ]、[ポート]、および [シークレット] を指定して RADIUS 設定を行います。
2. [接続のテスト] をクリックして、RADIUS サーバへの接続を確認します。
3. [テストユーザの資格情報] をクリックして、RADIUS サーバの認証機能をテストします。RADIUS サーバのユーザ名およびパスワードを指定し、[テスト] をクリックします。

   注意

   [接続のテスト] ボタンをクリックした後、選択したゲートウェイを使用して自動的に接続がテストされます。特定のゲートウェイを選択する場合は、[テストするゲートウェイの選択] の横にあるリストから選択します。

   ---

4. [セカンダリ RAIUDS サーバ] を設定します (任意)。
5. [RADIUS マッピング属性] ([ベンダー固有/フィルタ ID]) を指定します。

   注意

   ベンダー固有オプションを選択した場合は、RADIUS サーバのベンダーコードとしてトレンドマイクロのコード (6101) を設定する必要があります。

   ---

6. [保存] をクリックします。

RADIUS ユーザ/グループを管理する

目的: ポリシーおよびレポートにユーザ/グループを設定するために RADIUS ユーザ/グループを管理します。

場所: [管理] > [ユーザ認証] > [RADIUS 設定] > [RADIUS ユーザ/グループ]

手順

1. 次の手順を実行します。
   - 新しい RADIUS ユーザ/グループを作成するには、[追加] をクリックします。
   - RADIUS ユーザ/グループ名を探すには、右上にある [検索] を使用します。
   - 説明を表示または変更するには、RADIUS ユーザ/グループ名をクリックします。
   - ユーザ/グループを削除するには、RADIUS ユーザ/グループ名を選択して [削除] をクリックします。

RADIUS ユーザとグループ

RADIUS サーバでユーザを認証できますが、ポリシーとレポートに対して RADIUS ユーザまたはグループを設定する場合は、同じユーザまたはグループを Cloud Edge Cloud Console に追加する必要があります。

ポリシーとレポートに対して RADIUS ユーザとグループを設定しない場合、RADIUS サーバの設定のみ必要です。

Cloud Edge では、RADIUS ユーザおよびグループはゲートウェイと同期されず、関連ポリシーが配信されるだけです。

ユーザアカウントおよびグループを同期する

ユーザアカウントおよびグループを手動で同期する手順を次に示します。同期されたユーザおよびグループの情報に基づいて、ポリシーを設定したりレポートを生成したりできます。Cloud Edge Cloud Console では、登録されているすべてのゲートウェイのユーザおよびグループが 8 時間ごとに自動的に同期されます。

同期される情報には、Cloud Edge Cloud Console で設定されているホスト対象のユーザとグループの情報が含まれます。

手順

1. [管理] > [ユーザ認証] > [ユーザ ID の同期] に移動します。
2. [すべてのゲートウェイを同期] をクリックします。

   Cloud Edge Cloud Console により、登録されているすべてのゲートウェイでユーザおよびグループの情報が同期されます。

Cloud Console 管理者アカウントを追加する

Cloud Edge Cloud Console のユーザアカウントでは、同じ企業に属する登録済みのすべてのゲートウェイにアクセスできます。初期設定では、管理者権限を持つ「Admin」アカウントが作成されます。

Cloud Edge Cloud Console には、2 種類のユーザアカウントがあります。

- 管理者
- 読み取り専用ユーザ

手順

1. 管理 > ユーザとアカウント > アカウント管理 に移動します。
2. [追加] をクリックするか、変更するアカウントの名前をクリックします。

   [アカウントの追加/編集] 画面が表示されます。
3. 必要な設定を行います。

オプション	説明
名前	ユーザの名前を入力します。この名前は、ユーザが Cloud Edge Cloud Console にログインしているときに画面右上に表示されます。
ユーザ名	ユーザのメールアドレスを入力します。ユーザがログオンするときに入力するメールアドレスです。

オプション	説明
	 注意 ユーザアカウントの作成後にユーザ名を変更することはできません。
パスワード	ユーザのパスワードを入力します。 パスワードは、大文字アルファベット、小文字アルファベット、および数字をそれぞれ 1 文字以上使用し、8 文字以上で指定する必要があります。任意で特殊文字を使用することもできます。  ヒント 次のヒントは強力なパスワードの作成に役立ちます。 • パスワードに特殊文字を含めます。 • 辞書やその他の言語に存在する言葉の使用は避けます。 • 意図的に誤った綴りを使用します。 • 成句や語の組み合わせを使用します。
パスワードの確認	ユーザのパスワードをもう一度入力します。
読み取り専用	このチェックボックスは、ユーザの権限を制限する場合にオンにします。このチェックボックスをオフにすると管理者ユーザになります。 読み取り専用ユーザが実行できる操作は、以下に限定されます。 • [ゲートウェイ]、[ポリシー]、[分析とレポート]、および [管理] の各タブでオブジェクトを表示する • ダッシュボードでタブやウィジェットを表示および変更する • [ユーザプロファイルの変更] 画面を使用する • [レポート] 画面の [今すぐ実行] ボタンをクリックする

4. [保存] をクリックします。

メールクライアントに Cloud Edge の CA 証明書をインポートする

セキュリティプロファイルを設定する際に、メールセキュリティ対策としてセキュアプロトコル (SMTPS、POP3S、および IMAPS) を有効にできます。セキュアなメールを使用する場合、Cloud Edge がプライベート認証局 (CA) として機能し、デジタル証明書を動的に生成します。制止された証明書は、安全な接続経路を確保するためにメールクライアントに送信されます。ただし、初期設定の CA にはインターネット上の既知の (信頼できる) CA による署名がありません。そのため、メールクライアントでは、接続先のサーバで使用されているセキュリティ証明書を確認できないことを示す警告メッセージが常に表示されます。

この警告メッセージが表示されないようにして、SSL または startTLS でメールが送受信されるようにするには、Cloud Edge の CA 証明書をメールクライアントにインストールします。

このセクションでは、次の手順について説明します。

- 270 ページの「CA 証明書をエクスポートする」
- 270 ページの「Microsoft Outlook 用に Cloud Edge の CA 証明書をインポートする」
- 271 ページの「Mozilla Thunderbird 用に Cloud Edge の CA 証明書をインポートする」
- 272 ページの「Mac OS 用に Cloud Edge の CA 証明書をインポートする」
- 273 ページの「Android デバイスに Cloud Edge の CA 証明書をインポートする」
- 274 ページの「iOS デバイスに Cloud Edge の CA 証明書をインポートする」

注意

Foxmail については説明していません。このバージョンの Cloud Edge では、Foxmail に対するセキュアなメール検索はサポートされていません。

CA 証明書をエクスポートする

Cloud Edge の CA 証明書をメールクライアントにインストールするには、まず証明書をエクスポートする必要があります。

手順

1. [管理] > [証明書管理] に移動します。
2. 証明書をエクスポートするには、[エクスポート] をクリックします。
3. 証明書ファイル (`CloudEdge.crt`) をコンピュータに保存します。

Microsoft Outlook 用に Cloud Edge の CA 証明書をインポートする

Microsoft Outlook でセキュアなメールがスムーズに復号化されるようにするには、Microsoft Windows の信頼された認証局の証明書ストアに Cloud Edge の CA 証明書をインポートする必要があります。

手順

1. Cloud Edge からエクスポートしておいた証明書ファイル (`CloudEdge.crt`) を対象のメールクライアントマシンにコピーします。
2. 対象のマシンで、証明書ファイルをダブルクリックして開きます。
3. [証明書のインストール] をクリックします。

   証明書のインポートウィザード画面が表示されます。
4. [証明書をすべて次のストアに配置する] を選択し、[参照] をクリックします。

   [証明書ストアの選択] 画面が表示されます。
5. [信頼されたルート証明機関] ストアを選択し、[OK] をクリックします。
6. [次へ] をクリックし、[セキュリティ警告 画面で [はい] を選択します。

   「正しくインポートされました」と表示されれば、証明書のインポートは完了です。

7. Microsoft Outlook を再起動します。

   メールを送受信する際に、証明書の警告が生成されなくなります。

Mozilla Thunderbird 用に Cloud Edge の CA 証明書をインポートする

Mozilla Thunderbird でセキュアなメールがスムーズに復号化されるようにするには、Thunderbird の信頼された認証局の証明書ストアに Cloud Edge の CA 証明書をインポートする必要があります。

注意

ここに記載する手順は Thunderbird 45.7.1 用で、順は Thunderbird のバージョンによっては手順が異なることがあります。必要に応じて、Thunderbird の該当するバージョンのドキュメントを参照してください。

手順

1. Cloud Edge からエクスポートしておいた証明書ファイル (`CloudEdge.crt`) を対象のメールクライアントマシンにコピーします。
2. 対象のマシンで、Thunderbird メールアプリケーションを開き、アプリケーションメニューボタン (☰) をクリックします。
3. リストから [オプション] を選択します。

   [オプション] 画面が表示されます。
4. [詳細] を選択し、[証明書] タブを選択します。
5. [証明書を表示] をクリックします。

   [証明書マネージャ] 画面が表示されます。
6. [認証局証明書] タブをクリックします。
7. [インポート] をクリックします。

   [証明書のインポート] 画面が表示されます。この画面で、信頼した Cloud Edge の証明書を使用する用途を選択します。

8. [この認証局による Web サイトの識別を信頼する] と [この認証局によるメールユーザの識別を信頼する] を選択します。
9. [OK] をクリックします。
10. Thunderbird アプリケーションを再起動し、[証明書マネージャ] 画面を開いて、Cloud Edge の証明書が信頼された CA のストアにインポートされたことを確認します。

Mac OS 用に Cloud Edge の CA 証明書をインポートする

Mac OS でセキュアなメールがスムーズに復号化されるようにするには、Mac OS の信頼された認証局の証明書ストアに Cloud Edge の CA 証明書をインポートする必要があります。

注意

ここに記載する手順は Mac OS El Capitan 10.11.6 用で、Mac OS のバージョンによっては手順が異なることがあります。必要に応じて、Mac OS の該当するバージョンのドキュメントを参照してください。

手順の途中で、認証のために管理者の資格情報を求められることがあります。

手順

1. Cloud Edge からエクスポートしておいた証明書ファイル (`CloudEdge.crt`) を対象の Mac OS マシンにコピーします。
2. `CloudEdge.crt` ファイルを右クリックします。
3. [このアプリケーションで開く] > [キーチェーンアクセス] に移動します。

   [キーチェーン] 画面が表示されます。
4. 左側のペインで、[システム] キーチェーンを選択します。

   Cloud Edge の証明書が右側のペインに表示されますが、システムから信頼されていません。
5. 右側のペインで、Cloud Edge の証明書を右クリックし、[情報を見る] を選択します。

   Cloud Edge の証明書の情報画面が表示されます。

6. [信頼] 情報セクションを展開します。
7. [この証明書を使用するとき] リストから [常に信頼] を選択します。

   このセクションに表示されたすべてのアプリケーションの値が自動的に [常に信頼] に変更されます。
8. 画面を閉じます。

   [システム] キーチェーンの右側のペインに、Cloud Edge の証明書が信頼された証明書として表示されます。
9. メールクライアントを再起動します。

   メールを送受信する際に、証明書の警告が生成されなくなります。

Android デバイスに Cloud Edge の CA 証明書をインポートする

Android デバイスでセキュアなメールがスムーズに復号化されるようにするには、信頼できる認証情報ストアに Cloud Edge の CA 証明書をインポートする必要があります。

注意

証明書をインストールする手順は、Android のデバイスやバージョンによって異なることがあります。必要に応じて、Android のドキュメントで詳細を確認してください。

Cloud Edge の CA 証明書をインストールしない場合は、メールアカウントの詳細設定に移動し、[証明書をすべて承認] がオンになっていることを確認してください。

手順

1. Cloud Edge からエクスポートしておいた証明書ファイル (`CloudEdge.crt`) を対象の Android デバイスにダウンロードします。

   証明書にアクセスしてダウンロードする方法としては、ブラウザやメール添付があります。

2. 対象の Android デバイスで、[設定] > [セキュリティ] に移動します。
3. [ストレージからインストール] に移動してタップします。

   [次から開く] 画面が表示されます。
4. [内部ストレージ] を選択し、[ダウンロード] フォルダを選択します。
5. Cloud Edge の証明書を選択してインストールします。
   - 初期設定の資格情報を使用します。
   - [VPN とアプリ] が選択されていることを確認します。
6. [設定] > [セキュリティ] > [信頼できる認証情報] に移動して [ユーザー タブを選択し、Cloud Edge の証明書がインポートされたことを確認します。
7. Android デバイスでモバイルメールクライアントを再起動します。

iOS デバイスに Cloud Edge の CA 証明書をインポートする

セキュアなメールが iOS デバイスでシームレスに復号化されるようにするには、信頼された資格情報のストアに Cloud Edge の CA 証明書をインポートする必要があります。

注意

証明書をインストールする手順は、iOS のバージョンによって異なることがあります。必要に応じて、iOS のドキュメントで詳細を確認してください。

手順

1. メールアカウントを使用して、Cloud Edge からエクスポートしておいた証明書ファイル (`CloudEdge.crt`) を送信してダウンロードします。
2. メールに添付された証明書ファイルをクリックします。

   [プロファイルをインストール] 画面が開き、証明書をインストールするように求められます。
3. [インストール] をタップします。

   この証明書は信頼されていないため、警告が表示されます。

4. プロファイルをインストールするための確認画面で、[インストール] をタップします。

   [インストール完了] 確認画面が開き、[信頼されています] という緑のチェックマークが表示されます。

5. [完了] をタップして [インストール完了] 画面を閉じます。

6. [設定] > [一般] > [プロファイル] に移動して、Cloud Edge の証明書がインストールされたことを確認します。

   次に、Cloud Edge の CA 証明書に対する完全な信頼を有効にする必要があります。

7. [設定] > [一般] > [情報] > [証明書信頼設定] に移動し、[Cloud Edge] の設定を [ON] にスライドして、Cloud Edge の CA 証明書に対する完全な信頼を有効にします。

8. iOS デバイスでモバイルメールクライアントを再起動します。

アップデート

最新のリスクに対する対策を最新に保つために、アップデート可能なパターンファイルコンポーネントがいくつかあります。これらのファイルは、既知のセキュリティ上の脅威のバイナリ「シグネチャ」やパターンを格納しています。Cloud Edge ではそれらを使用して、インターネットゲートウェイを通過する既知の脅威を検出します。一方、プロトコルや IPS のパターンファイルはそれほど頻繁にはアップデートされません。

Cloud Edge ではアップデート機能を使用しています。これは、ウイルスパターンファイルや検索エンジンのほか、スパイウェアやゲートウェイのパターンファイルに対する、手動またはバックグラウンドでのアップデートが可能なトレンドマイクロのユーティリティです。アップデートは、多くのトレンドマイクロ製品に共通するサービスです。アップデート機能により、トレンドマイクロのアップデートサーバに接続し、最新のパターンファイルおよびエンジンをダウンロードします。アップデートの実行後、エンドポイントを再起動する必要はありません。アップデートは、予約しておいた間隔で自動で行うことも、必要に応じて手動で行うことも可能です。

関連情報

- 「アップデート可能なコンポーネント」

アップデート可能なコンポーネント

最新のリスクに対する対策を最新に保つために、アップデート可能なエンジンおよびパターンファイルのコンポーネントがいくつかあります。

パターンファイルは、既知のセキュリティ上の脅威のバイナリの「「シグネチャ」」やパターンを格納しています。Cloud Edge ではそれらを使用して、インターネットゲートウェイを通過する既知の脅威を検出します。ウイルスやスマートスキャンのパターンファイルなど、一部のパターンファイルは通常、週に数回提供されています。一方、プロトコルや IPS のパターンファイルなど、一部のパターンファイルはそれほど頻繁にはアップデートされません。

スパムメール対策のパターンファイルおよびエンジン

Cloud Edge では、スパムメール判定ルールを使用することで、最新のスパムメールを検出することができます。スパムメール対策エンジンは、メッセージおよび添付ファイルに含まれる情報を元にスパムを検出します。

C&C 情報パターンファイル

Cloud Edge では、コマンド&コントロール (C&C) 情報パターンファイルを使用することで、ボットネットから C&C サーバへの接続を検出することができます。これにより、APT (標的型攻撃) による被害を軽減します。

IntelliTrap パターンファイルおよび除外パターンファイル

IntelliTrap 検出では、トレンドマイクロのウイルス検索エンジンの検索オプションに、IntelliTrap パターンファイル (不正な可能性のあるファイル) と IntelliTrap 除外パターンファイル (許可リスト) を組み合わせて使用します。Cloud Edge は、IntelliTrap オプションとパターンファイルを使用して、不正な圧縮ファイル (圧縮ファイル内のボットなど) を検出します。ウイルス作成者は、複数のファイル圧縮スキームを使用して、ウイルスフィルタを回避しようとします。IntelliTrap は圧縮ファイルをヒューリスティックに評価することで、ボットやその他の不正な圧縮ファイルによってネットワークにもたらされる潜在リスクを削減します。

IPS パターンファイル

Cloud Edge では、IPS のパターンファイルを使用して IPS 脆弱性をブロックします。ネットワークトラフィックが IPS パターンにマッチすると、Cloud Edge は設定に応じた処理 (ブロックまたは監視) を行います。

スパイウェアパターンファイル

機密情報を不正に収集する新しいプログラム (スパイウェア) が発見されるたびに、トレンドマイクロはその明らかな特徴 (シグネチャ) を収集してスパイウェアパターンファイルに追加します。

ウイルス検索エンジンおよびパターンファイル

ウイルス検索エンジンは、各ファイルのバイナリパターンを分析し、パターンファイル内のバイナリ情報と照合します。パターンが一致した場合、そのファイルは不正なファイルと判定されます。

スマートスキャンエージェントパターンファイル

スマートスキャンエージェントパターンファイルは、スマートスキャンの高度な不正プログラム検索ソリューションのローカルファイルです。スマートスキャンを有効にすると、Cloud Edge がスマートスキャンサーバにコンテンツを送信し、検索が行われます。スマートスキャンエージェントパターンファイルは、スマートスキャンソリューションのハンドラとなる部分です。ローカルのスマートスキャンエージェントパターンファイルは 1 日に 1 回しかアップデートされませんが、スマートスキャンサーバに格納されているスマートスキャンパターンファイルは頻繁にアップデートされます。

アップデートスケジュールを設定する

予約アップデート以外に、手動でコンポーネントおよびファームウェアのアップデートを行うことができます。トレンドマイクロでは、新たに確認された脅威に対応して、新しいバージョンのウイルスパターンファイルとスパイウェアパターンファイルを頻繁にリリースします。

手順

1. [管理] > [予約アップデート] の順に選択します。

2. [オン] をクリックして予約アップデートを有効にします。
   - コンポーネントのアップデート
   - ファームウェアのアップデートおよび工場出荷時のイメージのアップデート

   注意
   工場出荷時のイメージの自動アップデート期間のスケジュール設定では、自動ファームウェアアップデート期間と同じスケジュールパターンを共有します。

3. アップデートを実行する頻度を選択します。

   注意
   アップデート間隔を選択するときに指定する予約アップデートの実行時刻は、Cloud Edge ゲートウェイを使用している現地の時刻です。

4. [保存] をクリックします。
5. アップデートが有効になるまで数分待ちます。
6. [すべて配信] をクリックして変更を有効にします。

手動アップデート

予約アップデート以外に、手動でコンポーネントおよびファームウェアのアップデートを行うことができます。トレンドマイクロでは、新たに確認された脅威に対応して、新しいバージョンのウイルスパターンファイルとスパイウェアパターンファイルを頻繁にリリースします。

手順

1. [ゲートウェイ] に移動します。
2. ゲートウェイを右クリックし、[アップデート] を選択します。

   [手動アップデート] 画面が表示されます。

3. アップデートするコンポーネントを選択します。
4. [アップデート] をクリックします。

第 7 章

Cloud Edge On-Premises

本章では、ユーザネットワークに Cloud Edge ゲートウェイを配置する方法と基本的な管理操作について説明します。

配信

安全のためのガイドライン

安全にご利用いただくために、次のガイドラインに従ってください。

- 設置時および設置後に、ケースの表面を塞いだりほこりが入ったりしないようにしてください。
- 衣類やアクセサリーがケースに引っかからないように注意してください。ネクタイやスカーフは結び、袖はまくってください。
- 状況に応じて、異物が目に入らないように保護眼鏡を着用してください。
- 人や機器に危害を加えることがないように注意してください。
- ケースの取り付け/取り外しや電源付近の作業を行うときは、必ずすべての電源を切り、電源コードを抜いてから作業してください。
- 危険な作業を行うときは、1 人で作業しないでください。
- 電源回路の遮断については、作業のたびに必ず確認してください。

パッケージ内容

Cloud Edge ゲートウェイのパッケージを開封したら、パッケージに同封されているクイックスタートガイドを参照して中身を確認してください。

配信モード

配信モードの概要

Cloud Edge ゲートウェイには、ルーティングモード、ブリッジモード、ソフトウェアスイッチ (ブリッジモードのバリエーション) の 3 つの配信設定があります。これらの設定によって、Cloud Edge ゲートウェイでのネットワークパケットのルーティング方法と、インタフェースによる転送方法が決まります。

表 7-1. 配信モード

配信モード	目的
ブリッジモード	配信モードがブリッジモードに設定されている場合は、ブリッジモード設定またはソフトウェアスイッチ設定のいずれかを配信できます。 ブリッジモード設定 Cloud Edge ユニットは、ネットワーク上で認識されません。ネットワークデバイス (スイッチ、ルータ、ファイアウォール、またはエンドポイント) 間のレイヤ 2 ブリッジとして機能し、両方向のネットワークトラフィックを透過的に検索します。 そのインタフェースはすべて同じサブネット上にあります。ブリッジインタフェース (br0) だけを、インターネットへの接続を提供可能な IP アドレスを使用して設定する必要があります。ブリッジインタフェース (br0) は、Cloud Edge Cloud Console への接続、クラウドメッセージ検索サービスの提供、および他のクラウドサービス (トレンドマイクロのアップデートなど) へのアクセスに使用されます。 通常、ブリッジモードは、既存のファイアウォールまたはルータの背後にあるプライベートネットワークで使用します。 ブリッジモードは Cloud Edge を既存のネットワークトポロジーに配信する最も簡単な方法で、クライアント、ルータ、またはスイッチの設定を変更する必要もありません。 ソフトウェアスイッチ設定 ソフトウェアスイッチはブリッジモードのバリエーションです。モードスイッチはブリッジにセットします。 Cloud Edge は、アップストリームのネットワークデバイス (スイッチ、ルータ、またはファイアウォール) とエンドポイントの間のソフトウェアスイッチとして機能します。Cloud Edge ゲートウェイは、通過するすべてのトラフィックについて不正プログラムの有無を検索します。 ブリッジモードと同様、インタフェースはすべて同じサブネット上にあり、IP アドレスを使用してブリッジインタフェース (br0) のみを設定することができます。ブリッジインタフェース (br0) は、インターネットへの接続を提供します。ただし、配信モードをソフトウェアスイッチに設定する場合は、アップリンクポートを含むすべてのポートを、クライアント、サーバ、Wi-Fi アクセスルータなどのエンドポイントに直接接続する必要があります。 通常、ソフトウェアスイッチは、既存のファイアウォールまたはルータの背後にあるプライベートネットワーク上で Cloud Edge を使用し、

配信モード	目的
	エンドポイントを Cloud Edge ゲートウェイに直接接続する場合に使用します。 ブリッジモード (スイッチチップセット使用) ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイには追加の利点があります。このゲートウェイはブリッジモードで、クライアント、サーバ、Wi-Fi アクセスルータなどのエンドポイントに直接接続できる 7 つの LAN ポートを持つハードウェアスイッチとして機能します。 ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイは、インターネットトラフィックに対して、包括的なセキュリティ機能を提供します。さらに、イントラネットトラフィックに対して提供するセキュリティのレベルを、高セキュリティ、バランスセキュリティ、または高速セキュリティから設定できます。 通常、既存のファイアウォールまたはルータの背後にあるプライベートネットワーク上で Cloud Edge を使用し、複数のエンドポイントを Cloud Edge ゲートウェイに直接接続する場合に、ハードウェアスイッチとして Cloud Edge ゲートウェイを配信します。
ルーティングモード	Cloud Edge ユニットは、ネットワーク上で認識され、レイヤ 3 ルーティングデバイス (プライベートネットワークとインターネットの間のゲートウェイ) として機能します。プライベートネットワークの IP アドレスは、トラフィックストリーム検索機能を備えた NAT によって隠されます。 ルーティングモードでの配信では、少なくとも 2 つのネットワークインタフェースを設定する必要があります。1 つは内部用、もう 1 つは外部用です。インタフェースはすべて別々のサブネット上にあるため、インターネットに対して単一の IP アドレスを使用できます。 ネットワークに接続されているインタフェースはそれぞれ、そのネットワークで有効な IP アドレスを使用して設定する必要があります。Cloud Edge は、相手側のネットワークとの間でパケットを送受信する前にネットワークアドレスを変換し、ルータとして機能します。 ルーティングモードの Cloud Edge には PPPoE (Point-to-point Protocol over Ethernet) 機能も備わっており、ADSL (非対称型デジタル加入者回線) を使用した ISP へのダイヤルがサポートされます。 Cloud Edge ユニットをプライベートネットワークと公衆ネットワークの間のゲートウェイとして配信する場合は、通常はルーティングモードを使用します。

配信モード	目的
	ルーティングモードでのワイヤレスネットワーク ワイヤレスアクセスをサポートする Cloud Edge ゲートウェイモデルでは、メインワイヤレスアクセスポイントとゲストワイヤレスアクセスポイントを設定できます。ワイヤレスネットワークに対して包括的なセキュリティ検索が提供されます。 Cloud Edge 6.0 SP1 以降をルーティングモードで実行している Cloud Edge ゲートウェイモデルの場合、高可用性グループ (HA グループ) を設定することで、単一点障害を回避し、ネットワークの可用性を向上することができます。

注意

ブリッジモードまたはソフトウェアスイッチでは、レイヤ 3 ネットワークを使用する特定のゲートウェイ機能 (VPN や NAT など) を使用できません。

どの配信設定もポリシーによって配信されるすべてのセキュリティ機能をサポートし、ネットワークを保護します。

ルーティングモードのネットワークトポロジー

ルーティングモードの Cloud Edge はネットワーク上で認識され、トラフィックストリームの検索機能を持つレイヤ 3 ルーティングデバイスとして機能します。

次の図は、ルーティングモードの Cloud Edge の標準的なネットワークトポロジを示しています。

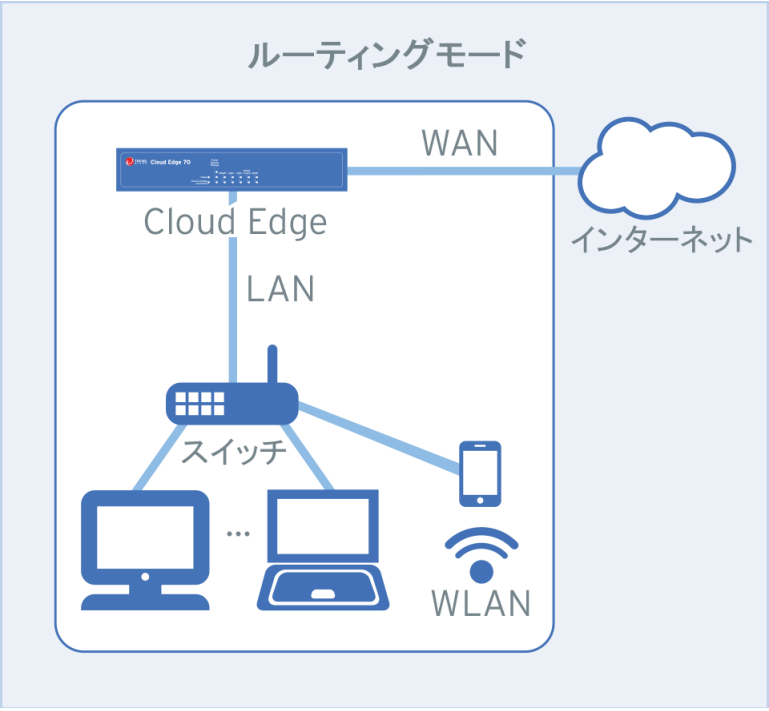


図 7-1. ルーティングモードの Cloud Edge

ルーティングモードの Cloud Edge ゲートウェイは、プライベートネットワークとパブリックネットワークの間のゲートウェイであり、ルータとして機能する、レイヤ 3 デバイスとして動作します。接続された各インタフェースには、IP アドレスが割り当てられます。インタフェースはすべて別々のサブネット上にあるため、インターネットに対して単一の IP アドレスを使用できます。Cloud Edge は、相手側のネットワークとの間でパケットを送受信する前にネットワークアドレスを変換します。

WAN インタフェースをインターネットに接続して、Cloud Edge ゲートウェイを Cloud Edge Cloud Console に登録できるようにする必要があります。WAN 接続は、クラウドメッセージ検索 (CMS) に使用されるほか、Cloud Edge でパ

ターンファイルの定期アップデートを管理したり、クラウドで提供される Trend Micro Smart Protection Network™のリアルタイムセキュリティ情報を利用したりする場合に使用されます。

Cloud Edge には、PPPoE (Point–to–point Protocol over Ethernet) 機能も備わっており、ADSL (非対称型デジタル加入者回線) を使用した ISP へのダイヤルをサポートしています。

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイ

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイは、他のすべての Cloud Edge モデルの設定に使用されるのと同じ設定を使用して、ルーティングモードで設定できます。

ルーティングモードでのワイヤレスネットワーク

次の図は、ルーティングモードのワイヤレスネットワークアクセス機能を備えた Cloud Edge ゲートウェイの標準的なネットワークトポロジを示しています。

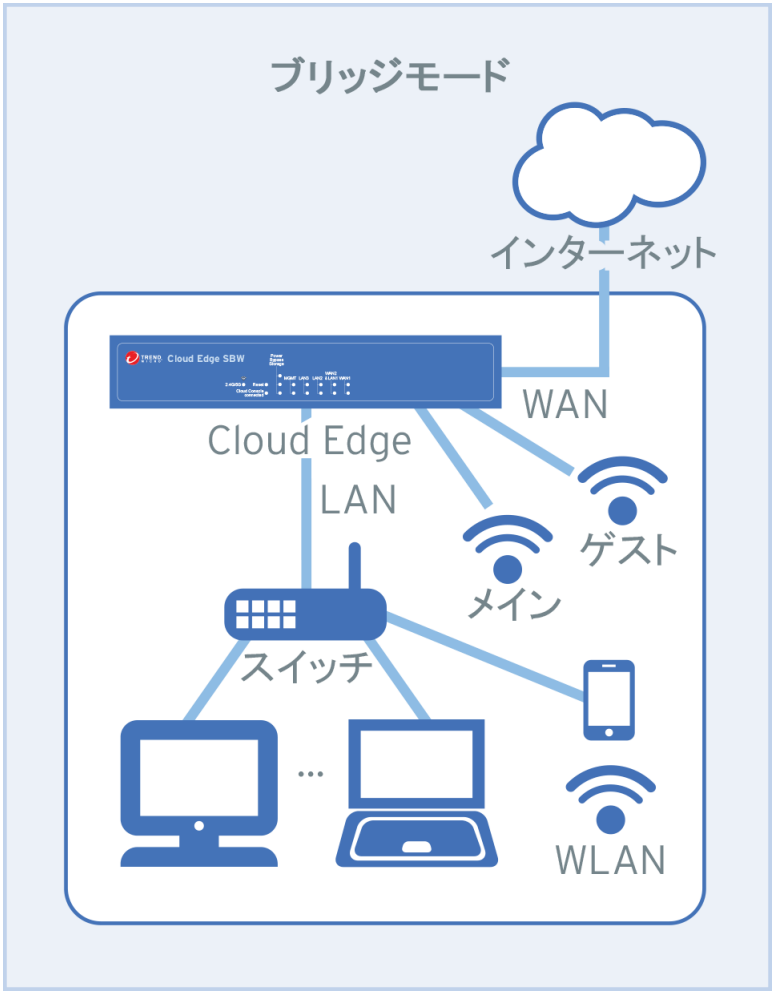


図 7-2. ルーティングモードのワイヤレスアクセス機能を備えた Cloud Edge

ワイヤレスネットワークアクセス機能を備えた Cloud Edge ゲートウェイでは、メインとゲストのワイヤレスアクセスポイントを設定できます。ワイヤレスネットワークに対しては、包括的なセキュリティ機能が提供されています。MAC アドレスフィルタを使用して、ワイヤレスネットワークアクセスを制御できます。DHCP サービス、帯域幅制御、NAT、VPN など、その他のサービスもワイヤレスネットワークに設定できます。

ルーティングモードでの HA グループ

Cloud Edge 6.0 SP1 以降をルーティングモードで実行している Cloud Edge ゲートウェイモデルの場合、高可用性グループ (HA グループ) を設定することで、単一点障害を回避し、ネットワークの可用性を向上することができます。

Cloud Edge Cloud Console を使用して HA グループを設定する必要があります。このトポロジおよびこの配信の設定方法については、86 ページの「HA グループを作成する」を参照してください。

ブリッジモードのネットワークトポロジー

ブリッジモードでは、Cloud Edge がネットワークデバイス (スイッチ、ルータ、またはファイアウォール) 間のレイヤ 2 ブリッジとして機能します。Cloud Edge ゲートウェイは、通過するすべてのトラフィックについて不正プログラムの有無を検索します。

次の図は、ブリッジモードの Cloud Edge の標準的なネットワークトポロジを示しています。

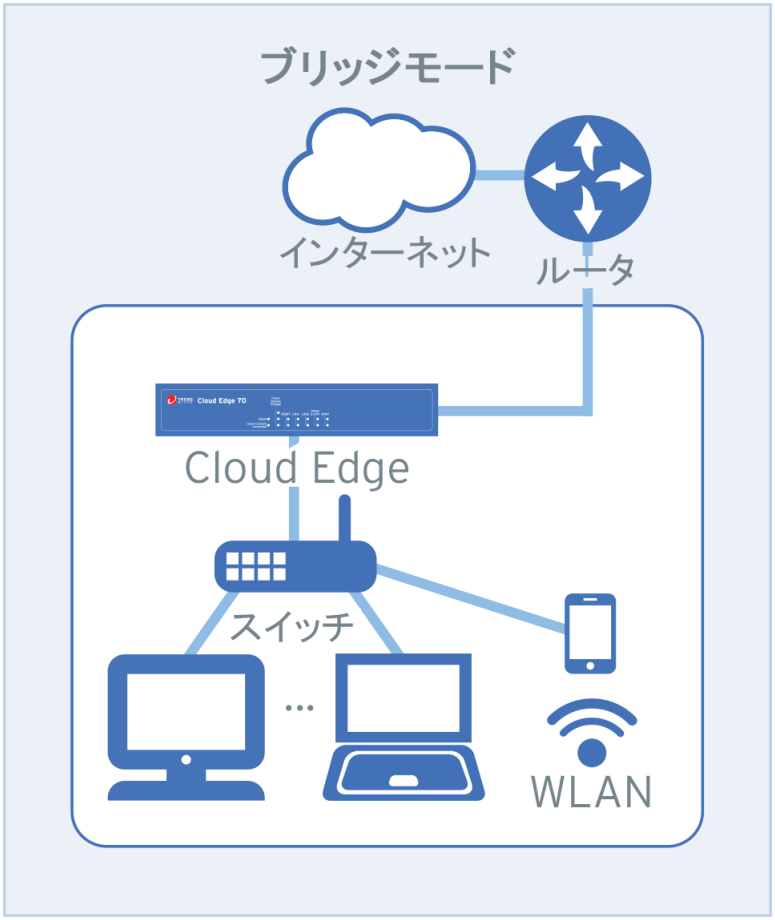


図 7-3. ブリッジモードの Cloud Edge

ブリッジモードを設定するには、WAN インタフェースと LAN1 インタフェースにケーブル接続する必要があります。ネットワークブリッジの場合と同様に、WAN インタフェースと LAN インタフェースは同じサブネット上に存在する必要があります。

ブリッジモードの Cloud Edge ゲートウェイはレイヤ 2 ネットワークを使用するため、接続されたインタフェースには IP アドレスが割り当てられません。ただし、Cloud Edge ゲートウェイを Cloud Edge Cloud Console に登録するために、ブリッジインタフェース (br0) で IP アドレスを設定する必要があります。ブリッジインタフェース (br0) に割り当てられた IP アドレスは、クラウドベースのクラウドメッセージ検索 (CMS) に使用されるほか、Cloud Edge でパターンファイルの定期アップデートを管理したり、クラウドで提供される Trend Micro™ Smart Protection Network™のリアルタイムセキュリティ情報を利用したりする場合に使用されます。

ブリッジモードは、Cloud Edge ですべての検索機能を透過的に実行できるよう、既存のファイアウォールまたはルータの背後にあるプライベートネットワークで Cloud Edge が動作している場合に設定します。

ソフトウェアスイッチのネットワークトポロジ

ソフトウェアスイッチ設定では、Cloud Edge は、ネットワークデバイス (スイッチ、ルータ、またはファイアウォール) とエンドポイントの間のソフトウェアスイッチとして機能します。ソフトウェアスイッチは、既存のファイアウォールまたはルータの背後にあるプライベートネットワーク上で Cloud Edge を運用し、エンドポイントを Cloud Edge ゲートウェイに直接接続する場合に使用します。

ソフトウェアスイッチとして設定した場合、Cloud Edge ゲートウェイは、通過するすべてのトラフィックについて不正プログラムの有無を検索します。

次の図は、ソフトウェアスイッチ設定の Cloud Edge の標準的なネットワークトポロジーを示しています。

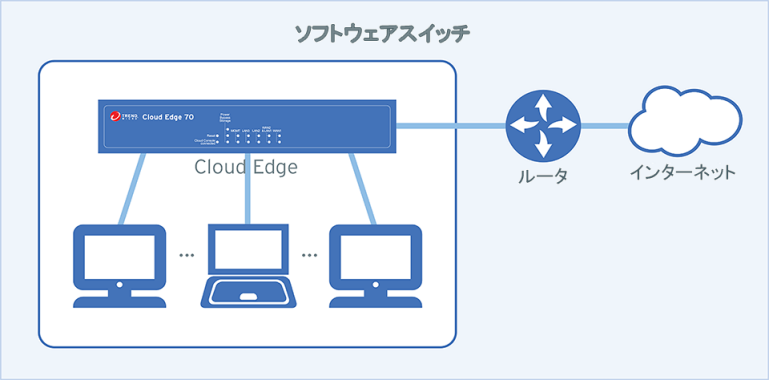


図 7-4. ソフトウェアスイッチ設定の Cloud Edge

- Cloud Edge の配信スイッチはブリッジに設定されていますが、配信モードを設定する際に、透過型ブリッジではなく、ソフトウェアスイッチとしてゲートウェイを設定します。
- Cloud Edge ゲートウェイをソフトウェアスイッチとして設定するには、3 つ以上のポートにケーブルを接続する必要があります。
  - WAN インタフェースと LAN1 インタフェースは必須です。
  - 少なくとも LAN2 ポートと LAN3 ポートのどちらかを接続する必要があります。
  - 必要な場合は、LAN2 と LAN3 を両方接続することもできます。
- ケーブルを接続する際には、ネットワークトポロジに留意する必要があります。
  - これらのインタフェースは同じサブネット上に存在している必要があります。
  - WAN インタフェースは、ルータへのアップリンクとして接続します (直接またはアップストリームスイッチ経由で接続)。

  - LAN1 ポート、LAN2 ポート、LAN3 ポートは、内部ネットワーク上のエンドポイントに接続します。

- ソフトウェアスイッチ設定はレイヤ 2 ネットワークに依存するため、接続されたインタフェースには IP アドレスが割り当てられません。
- Cloud Edge ゲートウェイを Cloud Edge Cloud Console に登録するためには、ブリッジインタフェース (br0) で IP アドレスを設定する必要があります。

  ブリッジインタフェース (br0) に割り当てられた IP アドレスは、クラウドベースのクラウドメッセージ検索 (CMS) に使用されるほか、Cloud Edge でパターンファイルの定期アップデートを管理したり、クラウドで提供される Trend Micro™ Smart Protection Network™のリアルタイムセキュリティ情報を利用したりする場合に使用されます。

ブリッジモードのネットワークトポロジー (スイッチチップセット使用)

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイは包括的なセキュリティ機能を備えたデバイスですが、ブリッジモード時はハードウェアスイッチとしても機能します。ブリッジモードのゲートウェイは、ネットワークデバイス (スイッチ、ルータ、またはファイアウォール) とエンドポイントの間のハードウェアスイッチとして機能します。このゲートウェイは、LAN ポートの数が 8 個 (LAN1-LAN8) まで増設されています。LAN1-LAN7 は、エンドポイントに直接接続できます。LAN8 はバイパス機能のために使用し、エンドポイントへの接続には使用しません。

次の図は、ブリッジモードのハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイの標準的なネットワークトポロジを示しています。

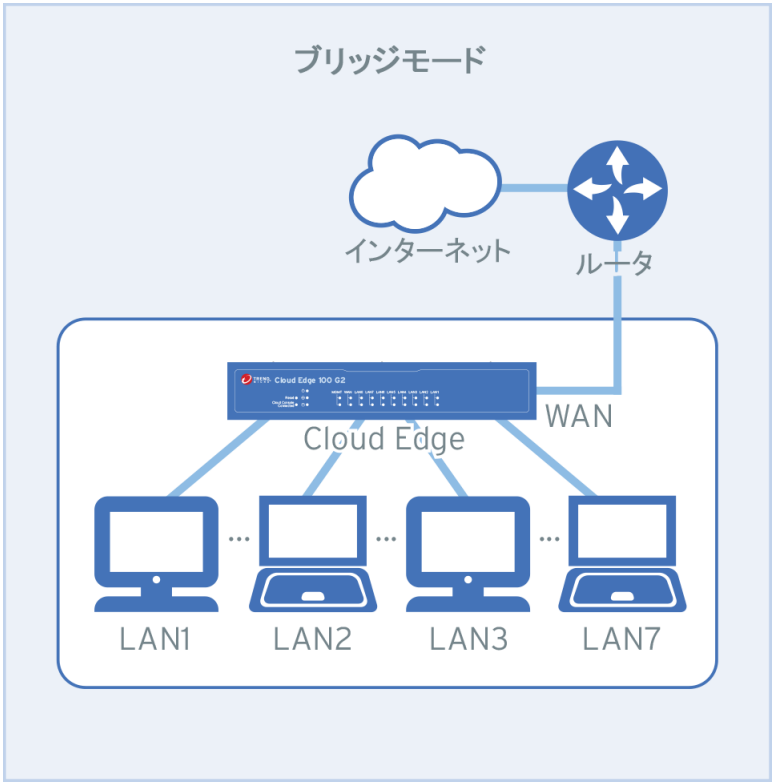


図 7-5. ブリッジモードのハードウェアスイッチチップセットを備えた Cloud Edge

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイをブリッジモードで配信するのは、Cloud Edge が既存のファイアウォールまたはルータの背後にあるプライベートネットワークで動作し、最大 7 個のエンドポイントを Cloud Edge ゲートウェイに直接接続する必要がある場合です。

ゲートウェイによって WAN インタフェースを通過するすべてのトラフィックが検索されると共に、包括的なセキュリティ機能が提供されます。

内部トラフィック (LAN 間トラフィック) 向けに提供されるセキュリティは、ゲートウェイの設定時に選択するセキュリティモードによって異なります。

ブリッジモードを設定するには、WAN および LAN1 インタフェースにケーブル接続する必要があります。また、LAN2-LAN7 から内部エンドポイントへのケーブル接続を追加することもできます。WAN および LAN インタフェースは、すべてが同じサブネット上に存在していなければなりません。

ブリッジモードのゲートウェイはレイヤ 2 ネットワークを使用するため、接続されたインタフェースには IP アドレスが割り当てられません。ただし、Cloud Edge ゲートウェイを Cloud Edge Cloud Console に登録するために、仮想スイッチインタフェース (sw0) で IP アドレスを設定する必要があります。また、その他のスイッチ関連の設定もスイッチインタフェース (sw0) で行います。

スイッチインタフェース (sw0) に割り当てられた IP アドレスは、クラウドベースのクラウドメッセージ検索 (CMS) に使用されるほか、Cloud Edge でパターンファイルの定期アップデートを管理したり、クラウドで提供される Trend Micro™ Smart Protection Network™のリアルタイムセキュリティ情報を利用したりする場合に使用されます。

WAN および LAN1-LAN8 インタフェースは L2 インタフェースであり、IP アドレスはありませんが、ハードウェアスイッチ設定に関連する、設定可能な多数のインタフェース設定があります。

ハードウェアスイッチチップセットを備えたゲートウェイでのバイパスポート

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイでは、特定のポートで高度なバイパス機能を使用できます。これによりトラフィックは、再起動、システムの問題、電源オフなど、検索の妨げとなるイベント中でもゲートウェイを通過できます。ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイを設定する前に、特定のビジネスニーズに応じて使用するポートを選択できるよう、バイパスポートの仕組みを理解しておく必要があります。

バイパスモードには以下の 2 つがあります。

- バイパスモード 1:

  ゲートウェイは WAN と LAN1-LAN7 の間のトラフィックをすべてバイパスします。バイパス中は LAN8 を使用できません。ゲートウェイの電

源が投入されると、システムエラー、システム起動、アップグレードなどの最中に必要に応じてバイパスモード 1 が機能します。バイパスモード 1 を有効にするには、ゲートウェイの電源が投入されている必要があります。

ゲートウェイの電源が投入されていない場合、バイパスモード 1 は機能しません。

このモードはハードウェアスイッチチップセットを備えたゲートウェイで実装されており、その他の Cloud Edge モデルにはありません。

- バイパスモード 2:

  ゲートウェイは、WAN と LAN1 の間のトラフィックをバイパスします。ゲートウェイの電源を切ってもバイパスモード 2 は機能します。

  このバイパス処理は他の Cloud Edge モデルと共通です。ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイの電源を投入すると、バイパスモード 1 が有効になるため、バイパスモード 2 の機能は停止します。

各種シナリオでバイパス機能がどのように相互作用するかについて、次の表を参照してください。

電源投入

転換点	→ DC 入力	→ 起動	→ バイパスモジュールのインストール	→ 初期化完了	
システムのフェーズ	DC 出力	BIOS	OS 起動	初期化	標準
ブリッジモード	WAN および LAN1 のバイパス	WAN および LAN1-LAN7 のバイパス	WAN および LAN1-LAN7 のバイパス	WAN および LAN1-LAN7 のバイパス	バイパスオフ/検索オン
ルーティングモード	バイパスなし	バイパスなし	バイパスなし	バイパスなし	バイパスなし/検索オン

再起動

転換点	再起動コマンドの入力	→ 再起動	→ 起動	→ バイパスモジュールのインストール	→ 初期化完了	
システムのフェーズ	標準	準備	BIOS	OS 起動	初期化	標準
ブリッジモード	バイパスオフ/検索オン	WAN および LAN1-LAN7 のバイパス	WAN および LAN1-LAN7 のバイパス	WAN および LAN1-LAN7 のバイパス	WAN および LAN1-LAN7 のバイパス	バイパスオフ/検索オン
ルーティングモード	バイパスなし/検索オン	バイパスなし	バイパスなし	バイパスなし	バイパスなし	バイパスなし/検索オン

カーネルパニック

転換点	パニック	→ WDT タイムアウト (80 秒)	→ 再起動	→ 起動	→ バイパスモジュールのインストール	→ 初期化完了	
システムのフェーズ	標準	カーネルパニック	電源オフ (0.2 秒)	BIOS	OS 起動	初期化	標準
ブリッジモード	バイパスオフ/検索オン	WAN および LAN1-LAN7 のバイパス	WAN および LAN1 のバイパス	WAN および LAN1-LAN7 のバイパス	WAN および LAN1-LAN7 のバイパス	WAN および LAN1-LAN7 のバイパス	バイパスオフ/検索オン
ルーティングモード	バイパスなし/検索オン	バイパスなし	バイパスなし	バイパスなし	バイパスなし	バイパスなし	バイパスなし/検索オン

配信モードスイッチ

Cloud Edge ゲートウェイには、ルーティングモード、ブリッジモード、ソフトウェアスイッチ (特殊なブリッジモード設定) の 3 つの配信タイプがあります。これらの設定によって、Cloud Edge ゲートウェイでのネットワークパケットのルーティング方法と、インタフェースによる転送方法が決まります。

Cloud Edge ゲートウェイのモデルに関係なく、初期設定の配信モードはすべてブリッジモードです。

配信モードの切り替えは、Cloud Edge ゲートウェイの背面パネルにあるスイッチで行います。配信モードを切り替えるには、スイッチを目的のモードに動かします。切り替えたら、ゲートウェイを手動で再起動する必要があります。

注意

ソフトウェアスイッチ設定を選択する場合は、配信スイッチを [ブリッジ] にセットします。これは、ソフトウェアスイッチ設定がブリッジモードのバリエーションであるためです。

図 7-6. 配信モードスイッチ

注意

このマニュアルで示す図は、実際の Cloud Edge ゲートウェイとはポート構成などが異なる場合があります。

配信前チェックリスト

コンピュータの要件

表 7-2. コンピュータの要件

要件	詳細

Ethernet ポートを備えたコンピュータ	次のソフトウェアがインストールされたコンピュータ:
	• Adobe™ Flash™ 10 以降
	• サポートされている Web ブラウザ
	  • Firefox™ 70 以降
	  • Google™ Chrome 78 以降
	  • Microsoft Edge™ (Chromium) 85 以降

配信の要件

表 7-3. ブリッジモードの要件

要件	詳細
Ethernet ケーブル (3 本)	管理ポート (MGMT)、WAN データポート、および LAN1 データポートに接続します。
IP アドレス (1 個)	• ISP (インターネットサービスプロバイダ) から WAN への接続に関する情報 (DHCP、静的) を入手します。入手した情報を使用して、ハードウェアスイッチチップセットを備えたゲートウェイのブリッジインタフェース (br0) またはスイッチインタフェース (sw0) を設定します。
DNS 設定	• ネットワーク DNS サーバの IP アドレス。

表 7-4. ルーティングモードの要件

要件	詳細
Ethernet ケーブル (3 本)	管理ポート (MGMT)、WAN データポート、および LAN1 データポートに接続します。 注意 この設定では、LAN1 ポートは内部ローカルエリアネットワークへの接続に使用されます。 ハードウェアスイッチチップセットを備えたゲートウェイの場合は、LAN1 を内部エンドポイントに接続します。
IP アドレス (2 個)	• ISP (インターネットサービスプロバイダ) から WAN への接続に関する情報(DHCP、静的、または PPPoE) を入手します 。 • 内部 LAN1 接続の IP アドレス情報を取得します (静的)。 • ワイヤレス機能を備えたゲートウェイでは、最初の配信時にメインワイヤレスネットワークを有効にする場合に、ワイヤレスネットワークインタフェース用に 3 つ目の IP アドレスが必要になります。
DNS 設定	• ISP の DHCP から割り当てられた自動 DNS 設定を使用するか、ネットワーク DNS サーバの IP アドレスを取得します。

表 7-5. ソフトウェアスイッチの要件

要件	詳細
Ethernet ケーブル (4〜5 本)	管理ポート (MGMT)、WAN、LAN1、LAN2、および LAN3 (任意) に接続します。 • WAN は外部ネットワークに接続するアップリンクです (直接またはアップストリームスイッチ経由で接続)。 • LAN1、LAN2、および LAN3 (任意) は、内部ローカルエリアネットワーク上のエンドポイントに接続します。  注意 ソフトウェアスイッチ設定には、接続されたインタフェースが 3 つ必要です。WAN と LAN1 に加えて、他の LAN インタフェースを少なくとも 1 つ接続する必要があります。
IP アドレス (1 個)	• ISP (インターネットサービスプロバイダ) から WAN への接続に関する情報 (DHCP、静的) を入手します。入手した情報を使用して、ブリッジインタフェース (br0)を L3 インタフェースとして設定します。  注意 ソフトウェアスイッチで使用するその他のインタフェースは、L2 インタフェースとして設定されます。L2 インタフェースに IP アドレスを割り当てることはできません。
DNS 設定	• ネットワーク DNS サーバの IP アドレス。

注意

ブリッジモードおよびルーティングモード: 他の内部ネットワークかエンドポイントに追加の LAN ポートを接続する場合は、ケーブルと IP アドレスがさらに必要となることがあります。

ルーティングモード: LAN1 ポートを冗長化されたセカンダリ WAN 接続として設定することもできます。この場合は、残りの LAN ポートを内部ネットワークとして設定できます。詳細については、373 ページの「ルーティングを管理する」を参照してください。

インストールと初期設定

Trend Micro™ Cloud Edge は、オンプレミスとクラウドベースのセキュリティ機能を兼ね備えた、MSP (マネージドサービスプロバイダ) 向けの次世代のセキュリティソリューションです。Cloud Edge ゲートウェイのインストールと初期設定をオンプレミスで実行すると、MSP はクラウド経由でネットワークをリモート管理できます。

手順

1. ハードウェアをセットアップします。

   303 ページの「ハードウェアをセットアップする」

2. 管理ポートから On-Premises Console にログオンします。

   305 ページの「管理ポートから On-Premises Console にログオンする」

3. 初期設定を行います。

   305 ページの「初期設定を行う」

4. ゲートウェイを登録します (まだ登録していない場合)。

   325 ページの「ゲートウェイを登録する」

5. ビジネス要件に合わせてその他の設定を行います。

   327 ページの「追加の設定を実行する」

ハードウェアをセットアップする

Cloud Edge ゲートウェイを接続して Cloud Edge Cloud Console に登録するには、ハードウェアをセットアップする必要があります。

注意

Cloud Edge ゲートウェイの電源は指示があるまで投入しないでください。

手順

1. 背面パネルにあるスイッチで配信モードを選択します。

   初期設定では、Cloud Edge ゲートウェイはブリッジモードに設定されています。

   注意

   このマニュアルで示す図は、実際のゲートウェイとはわずかに異なる場合があります。

   ---

2. ゲートウェイを電源に接続します。
3. ゲートウェイをネットワークに接続します。
   a. ゲートウェイの WAN ポートを広域ネットワーク (インターネット) に接続します。
   b. ゲートウェイの LAN1 ポートを内部ローカルエリアネットワークに接続します。

      ソフトウェアスイッチ設定を配信する場合、またはハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイをブリッジモードで配信する場合は、LAN1 を適切なエンドポイントに接続します。

4. 配信設定に応じて次の手順を実行します。

   - ブリッジモード: 必要に応じて、ゲートウェイの残りの LAN ポートを他の内部ネットワークに接続します。
   - ブリッジモード (スイッチチップセット使用): 必要に応じて、ゲートウェイの LAN2-LAN7 ポートを内部ネットワーク上のエンドポイントに接続します。

     ブリッジモードのハードウェアスイッチチップセットを備えたゲートウェイは、アップグレード、再起動、電源オフ、システムパニックなどのイベント中に使用できる独自のバイパス機能を備えています。バイパス機能はポートによって決まります。各ポートにエンドポイントを割り当てる方法を決定するには、295 ページの「ハードウェアスイッチチップセットを備えたゲートウェイでのバイパスポート」を参照してください。
   - ソフトウェアスイッチ: ゲートウェイの LAN2 ポートと、必要に応じて LAN3 ポートを他のエンドポイントに接続します。

     ソフトウェアスイッチ設定には、接続されたポートが 3 つ以上必要です。WAN と LAN1 は必須です。残りの LAN2 ポートと LAN3 ポートのどちらかまたは両方を接続します。
   - ルーティングモード: 必要に応じて、ゲートウェイの残りの LAN ポートを他の内部ネットワークに接続します。

5. ゲートウェイの電源を投入します。

   WAN インタフェースで DHCP が使用されていて、ゲートウェイが事前に登録されている場合、ゲートウェイは自動的に Cloud Edge Cloud Console に接続されます。

次に進む前に

WAN インタフェースで PPPoE または静的 IP アドレスが使用されている場合は、Cloud Edge ゲートウェイを Cloud Edge Cloud Console に接続する前に、ゲートウェイの On-Premises Console にログオンして WAN インタフェースを設定する必要があります。

管理ポートから On-Premises Console にログオンする

手順

1. Ethernet ケーブルを使用してコンピュータを Cloud Edge ゲートウェイの管理ポートに接続します。
2. 管理ポートとの接続に使用されている Ethernet インタフェースの IP アドレスを自動的に取得するよう、コンピュータを設定します。
3. サポートされている Web ブラウザを開きます。
4. 次の URL にアクセスします。

   `https://192.168.252.1:8443`
5. ログオン資格情報を指定します。

   管理者アカウントの初期設定の資格情報は次のとおりです。

   ユーザ名: `admin`

   パスワード: `adminCloudEdge`
6. <ENTER> キーを押すか、[ログオン] をクリックします。

   Cloud Edge On-Premises Console の [クイックセットアップ] ページが表示されます。

初期設定を行う

Cloud Edge On-Premises Console に初めてログインすると、[クイックセットアップ] 画面が自動的に表示されます。

トレンドマイクロでは、[クイックセットアップ] 画面を使用して WAN アップリンクの設定とシステム設定を行うことを推奨します。

注意

[クイックセットアップ] 画面が自動的に表示されるのは、Cloud Edge ゲートウェイが未登録またはオフラインのときだけです。デバイスがオンラインのときに [クイックセットアップ] 画面を表示するには、画面右上の [クイックセットアップ] リンクをクリックします。

選択した配信モードに応じて、次のいずれかの初期設定を行います。

- 306 ページの「ブリッジモードの初期設定」
- 309 ページの「ブリッジモード (スイッチチップセット使用) の初期設定」
- 312 ページの「ソフトウェアスイッチの初期設定」
- 316 ページの「ルーティングモードの初期設定」
- 319 ページの「ルーティングモードの初期設定 (ワイヤレス)」

[クイックセットアップ] 画面からテストを実行して、配信設定を確認できます。

- 323 ページの「配信設定の確認テスト」

関連情報

- 「配信モードの概要」
- 「配信モードスイッチ」

ブリッジモードの初期設定

[クイックセットアップ] 画面を使用すると、Cloud Edge ゲートウェイのブリッジモードの基本的な配信設定を行えます。基本的な配信設定後に、On-Premises Console を使用してその他の設定を指定できます。

手順

1. Cloud Edge On-Premises Console にログオンします。
2. [アップリンク設定] セクションで、次の情報を指定してブリッジインタフェース (br0) のネットワーク情報を設定します。

オプション	説明
配信モード	ブリッジモードに設定された読み取り専用フィールド 配信モードを設定するには、ゲートウェイの背面パネルにある配信モードスイッチをブリッジに設定します。298 ページの「配信モードスイッチ」を参照してください。

オプション	説明
種類	[ブリッジ] を選択します。
インタフェース 1/インタフェース 2	これらのフィールドはブリッジモードでのみ表示されますが、すべてのインタフェースがレイヤ 2 インタフェースであるため設定はできません。レイヤ 2 インタフェースには IP アドレスを割り当てることができません。
モード	次のいずれかのオプションを使用してブリッジインタフェース (br0) に IP アドレスを割り当てます。 • DHCP • 静的: [IPv4 アドレス]、[IPv4 ネットマスク]、および [IPv4 デフォルトゲートウェイ] を指定します。 **注意** 割り当てた IP アドレスを使用して Cloud Edge ゲートウェイがインターネットリソースにアクセスできる必要があります。
プライマリ DNS	DNS サーバの IP アドレスを指定します。[モード] フィールドで [静的] を選択している場合、これは必須の設定です。
セカンダリ DNS ターシャリ DNS	必要に応じて、セカンダリ DNS サーバとターシャリ DNS サーバの IP アドレスを指定します。

3. [システム設定] セクションで、Cloud Edge ゲートウェイのホスト名、時間、場所を設定します。

オプション	説明
ホスト名	ホスト名を指定します。
NTP サーバと同期する	NTP サーバと同期する場合は、このオプションを選択して、[NTP サーバ] フィールドで NTP サーバの IP アドレスを追加します。

オプション	説明
時間を手動で設定	時間を手動で設定する場合は、このオプションを選択して、[現地時間] フィールドに現在の時刻を `yyyy-mm-dd hh:mm:ss` の形式で指定します。たとえば、「`2015-01-16 13:03:28`」のように指定します。
[場所] と [都市]	Cloud Edge ゲートウェイに最も近い場所および都市を選択して、適切なタイムゾーンを設定します。 [場所]/[都市] がアジア/東京でない場合、タイムゾーンの情報が Cloud Edge Cloud Console から同期され、ゲートウェイが登録されている国のタイムゾーンになります。

4. [設定テストを開始] をクリックしてネットワークアップリンクの設定を確認します。

   詳細については、323 ページの「配信設定の確認テスト」を参照してください。

   > **注意**
   > 初期設定の前にデバイスが登録されていない場合は、登録テストと依存サービスの確認が正常に行われません。これは通常の動作です。登録後、[クイックセットアップ] 画面に戻り、設定テストを再実行して登録ステータスを確認し、依存サービステストが正常に行われることを確認します。

5. (任意) テストに時間がかかりすぎる場合は、[設定テストを中止] をクリックして完了前にテストを停止できます。

   設定とサービスがすべて正常に動作するように、テストを完了させることをお勧めします。

6. [保存して登録] をクリックします。

   > **注意**
   > Cloud Edge ゲートウェイが Cloud Edge Cloud Console に正常に登録されると、ボタンの名前が [設定を保存] に変わります。

ブリッジモード (スイッチチップセット使用) の初期設定

[クイックセットアップ] 画面を使用すると、ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイのブリッジモードの基本的な配信設定を行えます。基本的な配信設定後に、On-Premises Console を使用して、ハードウェアスイッチ設定など、その他の設定を指定できます。

注意

特定のスイッチインタフェース (sw0) の設定を行うには、Cloud Edge Cloud Console を使用する必要があります。

手順

1. Cloud Edge On-Premises Console にログオンします。
2. [アップリンク設定] セクションで、次の情報を指定してスイッチインタフェース (sw0) のネットワーク情報を設定します。

オプション	説明
配信モード	ブリッジモードに設定された読み取り専用フィールド 配信モードを設定するには、ゲートウェイの背面パネルにある配信モードスイッチをブリッジに設定します。298 ページの「配信モードスイッチ」を参照してください。
イントラネットセキュリティモード	[高セキュリティ] に設定された読み取り専用フィールド。 これは最初の初期設定です。初期設定が完了したら、Cloud Edge Cloud Console を使用してイントラネットセキュリティモードを変更できます。134 ページの「各イントラネットセキュリティモードで提供されるセキュリティ保護」を参照してください。

オプション	説明
インタフェース	WAN、LAN1–LAN8 に設定された読み取り専用フィールド WAN および LAN1-LAN8 L2 インタフェースはハードウェアスイッチ設定に自動的に含まれ、削除したり無効化したりすることはできません。L3 インタフェースに変更することはできません。
モード	次のいずれかのオプションを使用してスイッチインタフェース (sw0) に IP アドレスを割り当てます。 • DHCP • 静的: [IPv4 アドレス]、[IPv4 ネットマスク]、および [IPv4 デフォルトゲートウェイ] を指定します。 **注意** 割り当てた IP アドレスを使用して Cloud Edge ゲートウェイがインターネットリソースにアクセスできる必要があります。
プライマリ DNS	DNS サーバの IP アドレスを指定します。[モード] フィールドで [静的] を選択している場合、これは必須の設定です。
セカンダリ DNS ターシャリ DNS	必要に応じて、セカンダリ DNS サーバとターシャリ DNS サーバの IP アドレスを指定します。

3. [システム設定] セクションで、Cloud Edge ゲートウェイのホスト名、時間、場所を設定します。

オプション	説明
ホスト名	ホスト名を指定します。
NTP サーバと同期する	NTP サーバと同期する場合は、このオプションを選択して、[NTP サーバ] フィールドで NTP サーバの IP アドレスを追加します。

オプション	説明
時間を手動で設定	時間を手動で設定する場合は、このオプションを選択して、[現地時間] フィールドに現在の時刻を `yyyy-mm-dd hh:mm:ss` の形式で指定します。たとえば、「`2015-01-16 13:03:28`」のように指定します。
[場所] と [都市]	Cloud Edge ゲートウェイに最も近い場所および都市を選択して、適切なタイムゾーンを設定します。 [場所]/[都市] がアジア/東京でない場合、タイムゾーンの情報が Cloud Edge Cloud Console から同期され、ゲートウェイが登録されている国のタイムゾーンになります。

4. [設定テストを開始] をクリックしてネットワークアップリンクの設定を確認します。

   詳細については、323 ページの「配信設定の確認テスト」を参照してください。

   注意

   初期設定の前にデバイスが登録されていない場合は、登録テストと依存サービスの確認が正常に行われません。これは通常の動作です。登録後、[クイックセットアップ] 画面に戻り、設定テストを再実行して登録ステータスを確認し、依存サービステストが正常に行われることを確認します。

5. (任意) テストに時間がかかりすぎる場合は、[設定テストを中止] をクリックして完了前にテストを停止できます。

   設定とサービスがすべて正常に動作するように、テストを完了させることをお勧めします。

6. [保存して登録] をクリックします。

   注意

   Cloud Edge ゲートウェイが Cloud Edge Cloud Console に正常に登録されると、ボタンの名前が [設定を保存] に変わります。

ソフトウェアスイッチの初期設定

ソフトウェアスイッチ設定を備えた Cloud Edge ゲートウェイの基本的な初期設定を行うには、最初に On-Premises Console を使用して一定の設定を行ったうえで、[クイックセットアップ] 画面を使用して初期設定を完了する必要があります。基本設定の完了後に、On-Premises Console を使用してその他の設定を指定できます。

重要

配信モードをソフトウェアスイッチに設定するには、配信モードスイッチをブリッジにセットする必要があります。298 ページの「配信モードスイッチ」を参照してください。

手順

1. Cloud Edge On-Premises Console にログオンします。

   [クイックセットアップ] 画面が開きます。On-Premises Console を使用してソフトウェアスイッチの初期設定を行う必要があるため、ここで On-Premises Console を開きます。

2. 画面の右上にある [Cloud Edge On-Premises Console] リンクをクリックします。

   [Cloud Edge On-Premises Console] 画面が開きます。

3. ネットワーク > ブリッジ に移動します。

4. 名前の列で、[br0] をクリックします。

   [ブリッジの追加/編集] 画面が開きます。

5. 次の設定を行います。

オプション	説明
種類	種類を [ブリッジ] から [ソフトウェアスイッチ] に変更します。 [ソフトウェアスイッチ] を選択すると、使用できるオプションが変わります。[インタフェース 1] フィールドと [インタフェース 2] フィールドが [スイッチインタフェース] フィールドに置き換わります。
スイッチインタフェース	ソフトウェアスイッチ設定に含めるインタフェースを選択します。 • [スイッチインタフェース] フィールドは、[WAN] と [LAN1] があらかじめ選択された状態で表示されます。それらの選択を解除することはできません。 設定には少なくとも 3 つのインタフェースを含める必要があるため、少なくともあと 1 つはインタフェースを選択する必要があります。[LAN2] または [LAN3] のどちらかを選択するか、それらの両方のインタフェースを選択します。 • これらは L2 インタフェースです。L2 インタフェースに IP アドレスを割り当てることはできません。
モード	次のいずれかのオプションを使用してブリッジインタフェース (br0) に IP アドレスを割り当てます。 • DHCP • 静的: [IPv4 アドレス]、[IPv4 ネットマスク]、および [IPv4 デフォルトゲートウェイ] を指定します。 注意 割り当てた IP アドレスを使用して Cloud Edge ゲートウェイがインターネットリソースにアクセスできる必要があります。

6. [適用] をクリックします。
7. 右上にある [クイックセットアップ] をクリックします。

[クイックセットアップ] 画面が開きます。

8. [アップリンク設定] セクションで、次の情報を指定してブリッジインタフェース (br0) の DNS を設定します。

オプション	説明
プライマリ DNS	DNS サーバの IPv4 アドレスを指定します。[モード] フィールドで [静的] を選択している場合、これは必須の設定です。
セカンダリ DNS ターシャリ DNS	必要に応じて、セカンダリ DNS サーバとターシャリ DNS サーバの IPv4 アドレスを指定します。

注意

[クイックセットアップ] 画面では、[配信モード]、[種類]、および [インタフェース] の各フィールドは読み取り専用になります。

9. [システム設定] セクションで、Cloud Edge ゲートウェイのホスト名、時間、場所を設定します。

オプション	説明
ホスト名	ホスト名を指定します。
NTP サーバと同期する	NTP サーバと同期する場合は、このオプションを選択して、[NTP サーバ] フィールドで NTP サーバの IP アドレスを追加します。
時間を手動で設定	時間を手動で設定する場合は、このオプションを選択して、[現地時間] フィールドに現在の時刻を `yyyy-mm-dd hh:mm:ss` の形式で指定します。たとえば、「`2015-01-16 13:03:28`」のように指定します。

オプション	説明
[場所] と [都市]	必要に応じて、Cloud Edge ゲートウェイに最も近い場所および都市を選択して、適切なタイムゾーンを設定します。 [場所]/[都市] がアジア/東京でない場合、タイムゾーンの情報が Cloud Edge Cloud Console から同期され、ゲートウェイが登録されている国のタイムゾーンになります。

10. [設定テストを開始] をクリックしてネットワークアップリンクの設定を確認します。

    詳細については、323 ページの「配信設定の確認テスト」を参照してください。

    注意

    初期設定の前にデバイスが登録されていない場合は、登録テストと依存サービスの確認が正常に行われません。これは通常の動作です。登録後、[クイックセットアップ] 画面に戻り、設定テストを再実行して登録ステータスを確認し、依存サービステストが正常に行われることを確認します。

11. (任意) テストに時間がかかりすぎる場合は、[設定テストを中止] をクリックして完了前にテストを停止できます。

    設定とサービスがすべて正常に動作するように、テストを完了させることをお勧めします。

12. [保存して登録] をクリックします。

    注意

    Cloud Edge ゲートウェイが Cloud Edge Cloud Console に正常に登録されると、ボタンの名前が [設定を保存] に変わります。

ルーティングモードの初期設定

[クイックセットアップ] 画面を使用すると、Cloud Edge ゲートウェイのルーティングモードの基本的な配信設定を行えます。基本的な配信設定後に、On-Premises Console を使用してその他の設定を指定できます。

手順

1. Cloud Edge On-Premises Console にログオンします。
2. [アップリンク設定] セクションで、次の情報を指定してインターネットに接続する WAN インタフェースのネットワーク情報を設定します。

オプション	説明
配信モード	ルーティングモードに設定された読み取り専用フィールド 配信モードを設定するには、ゲートウェイの背面パネルにある配信モードスイッチをルーティングに設定します。298 ページの「配信モードスイッチ」を参照してください。
WAN インタフェース	このフィールドは読み取り専用で、WAN に設定されています。Cloud Edge ゲートウェイの配信モードがルーティングモードに設定されている場合にのみ表示されます。[クイックセットアップ] 画面で変更することはできません。

オプション	説明
モード	次のいずれかのオプションを使用して WAN インタフェースに IP アドレスを割り当てます。 • DHCP • PPPoE:[ユーザ名] と [パスワード] を指定します。このオプションは、ルーティングモードでのみ使用できます。 • 静的: [IPv4 アドレス]、[IPv4 ネットマスク]、および [IPv4 デフォルトゲートウェイ] を指定します。 **注意** 割り当てた IP アドレスを使用して Cloud Edge ゲートウェイがインターネットリソースにアクセスできる必要があります。
プライマリ DNS	DNS サーバの IP アドレスを指定します。[モード] フィールドで [静的] を選択している場合、これは必須の設定です。
セカンダリ DNS ターシャリ DNS	必要に応じて、セカンダリ DNS サーバとターシャリ DNS サーバの IP アドレスを指定します。

3. [システム設定] セクションで、Cloud Edge ゲートウェイのホスト名、時間、場所を設定します。

オプション	説明
ホスト名	ホスト名を指定します。
NTP サーバと同期する	NTP サーバと同期する場合は、このオプションを選択して、[NTP サーバ] フィールドで NTP サーバの IP アドレスを追加します。
時間を手動で設定	時間を手動で設定する場合は、このオプションを選択して、[現地時間] フィールドに現在の時刻を `yyyy-mm-dd hh:mm:ss` の形式で指定します。たとえば、「`2015-01-16 13:03:28`」のように指定します。

オプション	説明
[場所] と [都市]	Cloud Edge ゲートウェイに最も近い場所および都市を選択して、適切なタイムゾーンを設定します。 [場所]/[都市] がアジア/東京でない場合、タイムゾーンの情報が Cloud Edge Cloud Console から同期され、ゲートウェイが登録されている国のタイムゾーンになります。

4. [設定テストを開始] をクリックしてネットワークアップリンクの設定を確認します。

   詳細については、323 ページの「配信設定の確認テスト」を参照してください。

注意

初期設定の前にデバイスが登録されていない場合は、登録テストと依存サービスの確認が正常に行われません。これは通常の動作です。登録後、[クイックセットアップ] 画面に戻り、設定テストを再実行して登録ステータスを確認し、依存サービステストが正常に行われることを確認します。

---

5. (任意) テストに時間がかかりすぎる場合は、[設定テストを中止] をクリックして完了前にテストを停止できます。

   設定とサービスがすべて正常に動作するように、テストを完了させることをお勧めします。

6. [保存して登録] をクリックします。

注意

Cloud Edge ゲートウェイが Cloud Edge Cloud Console に正常に登録されると、ボタンの名前が [設定を保存] に変わります。

---

7. On-Premises Console を使用して LAN1 インタフェースを設定します。

   a. [クイックセットアップ] 画面の右上にある [Cloud Edge On-Premises Console] リンクをクリックします。

   b. [ネットワーク] > [インタフェース] に移動します。

c. 設定を編集する LAN1 インタフェースをクリックします。

d. [種類] リストから [L3] を選択し、IP アドレスを設定します。

- DHCP: 必要に応じて、[MTU]/[MSS] を指定します。
- 静的: IPv4 のアドレス情報 ([IPv4 アドレス]、[IPv4 ネットマスク]) と、必要に応じてゲートウェイアドレスを手動で入力します。必要に応じて、[MTU]/[MSS] を指定します。

e. [適用] をクリックします。

8. 必要に応じて、Cloud Edge Cloud Console を使用して追加のインタフェースを設定します。

123 ページの「ルーティングモード: ネットワークインタフェースを編集する」

ルーティングモードの初期設定 (ワイヤレス)

[クイックセットアップ] 画面を使用すると、ワイヤレスネットワークアクセス機能を備えた Cloud Edge ゲートウェイのルーティングモードの基本的な配信設定を行えます。基本的な配信設定後に、On-Premises Console を使用して、ワイヤレスネットワーク設定など、その他の設定を指定できます。

注意

ワイヤレスネットワークアクセス管理の設定を行うには、Cloud Edge Cloud Console を使用する必要があります。

手順

1. Cloud Edge On-Premises Console にログオンします。
2. [アップリンク設定] セクションで、次の情報を指定してインターネットに接続する WAN インタフェースのネットワーク情報を設定します。

オプション	説明
配信モード	ルーティングモードに設定された読み取り専用フィールド 配信モードを設定するには、ゲートウェイの背面パネルにある配信モードスイッチをルーティングに設定します。298 ページの「配信モードスイッチ」を参照してください。
WAN インタフェース	このフィールドは読み取り専用で、WAN に設定されています。Cloud Edge ゲートウェイの配信モードがルーティングモードに設定されている場合にのみ表示されます。[クイックセットアップ] で変更することはできません。
モード	次のいずれかのオプションを使用して WAN インタフェースに IP アドレスを割り当てます。 • DHCP • PPPoE:[ユーザ名] と [パスワード] を指定します。このオプションは、ルーティングモードでのみ使用できます。 • 静的: [IPv4 アドレス]、[IPv4 ネットマスク]、および [IPv4 デフォルトゲートウェイ] を指定します。 注意 割り当てた IP アドレスを使用して Cloud Edge ゲートウェイがインターネットリソースにアクセスできる必要があります。
プライマリ DNS	DNS サーバの IP アドレスを指定します。[モード] フィールドで [静的] を選択している場合、これは必須の設定です。
セカンダリ DNS ターシャリ DNS	必要に応じて、セカンダリ DNS サーバとターシャリ DNS サーバの IP アドレスを指定します。

3. [ワイヤレス設定] セクションで、次の情報を指定して Cloud Edge ゲートウェイのワイヤレスネットワークアクセスを設定します。

オプション	説明
ワイヤレス AP を有効にする	ワイヤレスネットワークアクセスを有効にする場合に選択します。 このオプションを選択すると、メインワイヤレスネットワークが有効になります。ゲストワイヤレスネットワークは有効になりません。
周波数	[2.4GHz] または [5GHz] のいずれかのオプションを選択します。
SSID	ワイヤレスネットワークに割り当てる SSID を入力します。 初期設定の SSID は、`CloudEdge-XXYY` (2.4GHz) または `CloudEdge-GUEST-XXYY` (5GHz) です。 XXYY は、ゲートウェイのシリアル番号の最初の 4 桁の数字です。
セキュリティ設定	[開く] または [WPA-PSK[TKIP]+WPA2-PSK[AES]] のいずれかのオプションを選択します。 セキュリティ設定のその他のオプションを利用できます。初期設定後、On-Premises Console を使用して、セキュリティ設定を含むワイヤレスネットワーク設定を変更できます。 ワイヤレスネットワークに対しては [開く] オプションを使用せず、セキュリティを使用することをお勧めします。

4. [システム設定] セクションで、Cloud Edge ゲートウェイのホスト名、時間、場所を設定します。

オプション	説明
ホスト名	ホスト名を指定します。
NTP サーバと同期する	NTP サーバと同期する場合は、このオプションを選択して、[NTP サーバ] フィールドで NTP サーバの IP アドレスを追加します。

オプション	説明
時間を手動で設定	時間を手動で設定する場合は、このオプションを選択して、[現地時間] フィールドに現在の時刻を `yyyy-mm-dd hh:mm:ss` の形式で指定します。たとえば、「`2015-01-16 13:03:28`」のように指定します。
[場所] と [都市]	Cloud Edge ゲートウェイに最も近い場所および都市を選択して、適切なタイムゾーンを設定します。 [場所]/[都市] がアジア/東京でない場合、タイムゾーンの情報が Cloud Edge Cloud Console から同期され、ゲートウェイが登録されている国のタイムゾーンになります。

5. [設定テストを開始] をクリックしてネットワークアップリンクの設定を確認します。

   詳細については、323 ページの「配信設定の確認テスト」を参照してください。

> **注意**
> 初期設定の前にデバイスが登録されていない場合は、登録テストと依存サービスの確認が正常に行われません。これは通常の動作です。登録後、[クイックセットアップ] 画面に戻り、設定テストを再実行して登録ステータスを確認し、依存サービステストが正常に行われることを確認します。

6. (任意) テストに時間がかかりすぎる場合は、[設定テストを中止] をクリックして完了前にテストを停止できます。

   設定とサービスがすべて正常に動作するように、テストを完了させることをお勧めします。

7. [保存して登録] をクリックします。

> **注意**
> Cloud Edge ゲートウェイが Cloud Edge Cloud Console に正常に登録されると、ボタンの名前が [設定を保存] に変わります。

8. On-Premises Console を使用して LAN1 インタフェースを設定します。
   a. [クイックセットアップ] 画面の右上にある [Cloud Edge On-Premises Console] リンクをクリックします。
   b. ネットワーク > インタフェース に移動します。
   c. 設定を編集する LAN1 インタフェースをクリックします。
   d. [種類] リストから [L3] を選択し、IP アドレスを設定します。
      - [DHCP]: 必要に応じて [MTU]/[MSS] を指定します。
      - [静的]: IPv4 のアドレス情報 ([IPv4 アドレス]、[IPv4 ネットマスク]) と、必要に応じてゲートウェイアドレスを手動で入力します。必要な場合は、[MTU]/[MSS] を指定します。
   e. [適用] をクリックします。
9. 必要に応じて、Cloud Edge Cloud Console を使用して追加のインタフェースを設定します。
   a. Cloud Edge Cloud Console にログオンします。

      72 ページの「Cloud Console にログオンする」
   b. 必要に応じてインタフェースを設定します。

      123 ページの「ルーティングモード: ネットワークインタフェースを編集する」

      124 ページの「ルーティングモード: ワイヤレスネットワークインタフェースを編集する」

配信設定の確認テスト

最初の配信設定が完了したら、Cloud Edge は一連のテストを実施して、ゲートウェイがインターネットに接続できること、ゲートウェイのステータスが登録済みであること、必要なさまざまなサービスが利用可能であることを確認できます。いずれか 1 つのテストが失敗すると、以降のテストは実施されません。テストが失敗した原因である問題を修正し、テストを再実行する必要があります。

次のテストが順番に実施されます。

順番	テスト	説明	テストが失敗する条件
1	インタフェースチェック	WAN および LAN1 インタフェースのステータスを確認します (アップまたはダウン)。	両方のインタフェースが停止中の場合。
2	DNS チェック	DNS 設定を確認します。 DNS 要求が成功するかどうかを確認します。	DNS が設定されていない場合。 DNS チェックのいずれか 1 つが失敗した場合。
3	デフォルトゲートウェイチェック	デフォルトゲートウェイの設定を確認します。 外部の Web サイトに正常に接続できるかどうかを確認します。	WAN へのルートが存在しない場合。 Cloud Edge が外部の Web サイトに接続できない場合。
4	登録ステータスチェック	登録ステータスを確認します。	ゲートウェイが登録されていない場合。
5	以下の内容を含むクラウドサービスチェック • アップデート • クラウド検索 • クラウドメール検索 • メールレピュテーション • ログ • Web レピュテーション • スマートスキャン • 機械学習型検索	すべてのサービスを確認します。	各サービスを個別に確認して、各サービスが個別に成功または失敗と判定された場合。 すべてのサービスチェックが失敗すると、全体の依存チェックは失敗します。

ゲートウェイを登録する

Cloud Edge Cloud Console を使用して Cloud Edge ゲートウェイをまだ登録していない場合は、登録してセキュリティポリシーを配信する必要があります。

手順

1. Cloud Edge Cloud Console にログオンします。
2. Cloud Edge Cloud Console で、[ゲートウェイ] に移動します。
3. [新しいゲートウェイの登録] をクリックします。
4. ゲートウェイの設定を指定します。

オプション	説明
表示名	Cloud Edge Cloud Console に表示される新しいゲートウェイの名前を指定します。
モデル	Cloud Edge ゲートウェイのハードウェアモデルを指定します。
シリアル番号	Cloud Edge ゲートウェイのシリアル番号を指定します。シリアル番号はゲートウェイの本体またはパッケージに記載されている 12 桁の英数字 (例: 4C80-9315-3A0B) です。

5. [保存] をクリックします。

   登録が完了するまで、数分かかることがあります。

   登録が完了すると、Cloud Edge Cloud Console からゲートウェイにポリシーが配信されます。登録完了後は、Cloud Edge Cloud Console のダッシュボードウィジェット、ログ分析、およびレポートで、Cloud Edge ゲートウェイから送信されるリアルタイムのトラフィックに基づくログ統計を確認できます。

6. 登録が正しく完了したことを確認します。

   84 ページの「登録を確認する」を参照してください。

登録を確認する

ゲートウェイの登録後は、登録が正常に完了したことを確認してください。Cloud Edge Cloud Console へのゲートウェイの登録が正しく完了したことを Cloud Edge On-Premises Console で確認する手順を次に示します。

手順

1. Cloud Edge On-Premises Console にログオンします。
2. 次のいずれかを実行します。
   - [ダッシュボード] > [システム情報] (ウィジェット) に移動し、[クラウド管理ステータス] に表示された情報を確認します。
   - [管理] > [デバイス管理] > [クラウド管理] (タブ) に移動し、表示された情報を確認します。
3. 326 ページの「接続を確認する」の手順に従って接続を確認します。

接続を確認する

Cloud Edge ゲートウェイが Cloud Edge Cloud Console に登録され、ポリシーに基づいてトラフィックが正しくルーティングされることを確認するために、接続を確認して配信をテストします。

手順

1. 次の表を参照して LED のステータスを確認します。

LED	ステータス
消灯	Cloud Edge ゲートウェイでインターネット接続が確立されていません。
緑色の点灯	Cloud Edge ゲートウェイが登録されており、Cloud Edge Cloud Console と通信している状態です。
緑色の点滅	Cloud Edge ゲートウェイはインターネットに接続されていますが、Cloud Edge Cloud Console に登録されていないか、Cloud Console と通信できない状態です。

2. Cloud Edge の登録に問題がなければ、内部エンドポイントからインターネットへのアクセスを試行します。

   インターネットにアクセスできれば、Cloud Edge は正常に機能しています。

注意

接続を確認できなかった場合は、マネージドサービスプロバイダにお問い合わせください。

追加の設定を実行する

ビジネス要件を満たすために、追加の設定手順を実行できます。次の各手順の指示に従って、Cloud Edge On-Premises Console または Cloud Edge Cloud Console を使用します。

手順

1. ワイヤレスネットワーク機能を備えた Cloud Edge ゲートウェイでは、ワイヤレス設定を行います。
   - ゲストワイヤレスネットワークの設定を含む、ワイヤレスネットワークの設定 (On-Premises Console):

     351 ページの「ワイヤレスネットワークの管理」
   - ワイヤレスアクセス制御 (Cloud Edge Cloud Console):

     183 ページの「ワイヤレスネットワークのアクセス制御を設定する」
   - ワイヤレスインタフェースの設定 (Cloud Edge Cloud Console):

     123 ページの「ルーティングモード: ネットワークインタフェースを編集する」
2. 接続されたネットワーク上のクライアントの DHCP サーバとして機能するよう、インタフェースを設定します。
   - WAN または LAN1 インタフェース (On-Premises Console):

     382 ページの「DHCP サービス設定を変更する」

- 追加の LAN インタフェース、または管理インタフェース (Cloud Edge Cloud Console):

  144 ページの「DHCP 設定を編集する」

  ワイヤレスネットワークアクセス機能を備えた Cloud Edge ゲートウェイでは、メインとゲストのワイヤレスネットワークで DHCP を設定できます。

3. ポリシーベースのルートを追加します (On-Premises Console)。
   - 377 ページの「ポリシーベースのルートを追加する」
4. 静的ルートを追加します (Cloud Edge Cloud Console)。
   - 154 ページの「静的ルートを追加する」
5. Cloud Edge ゲートウェイのインタフェースに NAT を設定します (Cloud Edge Cloud Console)。
   - 157 ページの「送信先 NAT ルールを追加する」
   - 160 ページの「送信元 NAT ルールを追加する」
   - 159 ページの「NAT ルールの優先度を変更する」
6. On-Premises Console タイムアウトを設定します (On-Premises Console)。
   - 386 ページの「On-Premises Console タイムアウトを設定する」
7. Cloud Edge ゲートウェイへの管理アクセスを管理します (Cloud Edge Cloud Console)。
   - 388 ページの「管理アクセスを有効にする」
8. WAN および LAN1 インタフェースで、ホストの監視を設定します (On-Premises Console)。
   - 348 ページの「インタフェースでのホストの監視を設定する」

管理

ネットワーク設定を管理する

ネットワーク設定を管理して、ネットワークトラフィックを処理および確認できます。

ネットワークインタフェースを管理する

Cloud Edge ゲートウェイを Cloud Edge Cloud Console に登録する前は、自動検出されたすべてのネットワークインタフェースを Cloud Edge On-Premises Console で表示し、変更できます。

ゲートウェイの登録後は、Cloud Edge On-Premises Console を使用して、次のインタフェースの設定を表示または変更できます。

注意

登録後、Cloud Edge Cloud Console を使用して管理インタフェースを設定する必要があります。

- ブリッジモード: ブリッジインタフェース (br0)
  - ブリッジモードの使用時に使用できる L3 インタフェースは、仮想ブリッジインタフェース (br0) だけです。
  - このインタフェースの設定時には、静的 IPv4 アドレスまたは DHCP IPv4 アドレスを使用できます。

    PPPoE はブリッジインタフェース (br0) ではサポートされていません。
  - VLAN は、ブリッジインタフェース (br0)ではサポートされていません。

  注意

  MTU など、物理インタフェース上の特定の L2 設定を編集できます。On-Premises Console を使用して WAN およびすべての LAN L2 インタフェースを編集します。

- ブリッジモード (スイッチチップセット使用): スイッチインタフェース (sw0)

- ブリッジモードの使用時に使用できる L3 インタフェースは、仮想スイッチインタフェース (sw0) だけです。
- このインタフェースの設定時には、静的 IPv4 アドレスまたは DHCP IPv4 アドレスを使用できます。

  PPPoE はスイッチインタフェース (sw0) ではサポートされていません。
- VLAN は、スイッチインタフェース (sw0)ではサポートされていません。
- WAN および LAN1-LAN8 インタフェースは自動的にスイッチ設定に追加されます。
  - これらのインタフェースは、どれもスイッチ設定から削除したり、L3 インタフェースに変更したりすることができません。
  - LAN2-LAN7 インタフェースを無効にすることができます。
  - WAN、LAN1、LAN8 インタフェースは無効にすることができません。
  - LAN1-LAN7 インタフェースにエンドポイントを接続することができます。
    LAN8 インタフェースはバイパス機能として使用されるため、エンドポイントを接続しないでください。

注意

MTU、フロー制御など、物理インタフェース上の特定の L2 設定を編集できます。On-Premises Console を使用して WAN および LAN1-LAN8 インタフェースを編集します。

- ソフトウェアスイッチ: ブリッジインタフェース (br0)
  - ソフトウェアスイッチ設定の配信時に使用できる L3 インタフェースは、仮想ブリッジインタフェース (br0) だけです。
  - このインタフェースの設定時には、静的 IPv4 アドレスまたは DHCP IPv4 アドレスを使用できます。

    PPPoE はブリッジインタフェース (br0) ではサポートされていません。

- ソフトウェアスイッチとして使用する L2 インタフェースを 3 つ以上追加する必要があります。

  WAN と LAN1 を追加する必要があります。LAN2 と LAN3 のどちらかまたは両方をソフトウェアスイッチ設定に追加できます。

  ソフトウェアスイッチの設定には L3 インタフェースを追加できます。Cloud Edge では、L3 インタフェースをソフトウェアスイッチに追加すると、L2 インタフェースに自動的に変更されます。

  この変更は、ゲートウェイが最初にルーティングモードで配信され、その後ブリッジモードに変更されてソフトウェアスイッチとして配信されると行われる可能性があります。その場合、既存の L3 インタフェースは、スイッチ設定に追加されていなければ L2 インタフェースに変換されません。

注意

MTU など、物理インタフェース上の特定の L2 設定を編集できます。On-Premises Console を使用して WAN およびすべての LAN L2 インタフェースを編集します。

- ルーティングモード: WAN および LAN1
  - WAN または LAN1 インタフェースでは、静的、DHCP、および PPPoE IPv4 アドレスを設定できます。

注意

LAN1 インタフェースが、冗長化された WAN 接続として使用されている場合は、PPPoE を LAN1 で使用できることもあります。

  - WAN インタフェースは、インターネットへの接続を提供します。
  - LAN1 インタフェースは、インターネットへの接続を冗長化する 2 番目の WAN インタフェースとして、または内部ネットワークに接続する LAN インタフェースとして設定できます。

    デュアル WAN 設定の詳細については、376 ページの「複数の ISP/WAN 環境の自動フェイルオーバー」を参照してください。

注意

On-Premises Console を使用して、WAN および LAN1 を編集できます。その他のインタフェースを編集するには、Cloud Edge Cloud Console を使用する必要があります。

On-Premises Console を使用して、L3 VLAN を WAN および LAN1 インタフェースに追加できます。ただし、L2 VLAN は Cloud Edge 6.0 以降を実行するゲートウェイではサポートされていません。

サポートされるネットワークインタフェース設定

Cloud Edge ゲートウェイは、次のネットワーク L3 インタフェース設定をサポートします。

- 静的 IP アドレス (静的)
  - ルーティングモード: すべての L3 インタフェースでサポート
  - ルーティングモード: ワイヤレスネットワークインタフェースでサポート
  - ブリッジモードおよびソフトウェアスイッチ: ブリッジインタフェース (br0)でサポート
  - ブリッジモード (スイッチチップセット使用): スイッチインタフェース (sw0)でサポート
  - 全モード: 管理ポートでサポート
- DHCP (Dynamic Host Configuration Protocol)
  - ルーティングモード: WAN または LAN1 L3 インタフェースでサポート
  - ブリッジモードおよびソフトウェアスイッチ: ブリッジインタフェース (br0)でサポート
  - ブリッジモード (スイッチチップセット使用): スイッチインタフェース (sw0)でサポート
  - 全モード: 管理ポートではサポート対象外
- PPPoE (Point-to-point Protocol over Ethernet)

- ルーティングモード: WAN および LAN1 L3 インタフェースでサポート
- ブリッジモードおよびソフトウェアスイッチ: ブリッジインタフェース (br0)ではサポート対象外
- ブリッジモード (スイッチチップセット使用): スイッチインタフェース (sw0)ではサポート対象外
- 全モード: 管理ポートではサポート対象外

ソフトウェアスイッチへの配信モードの切り替えに関する情報

Cloud Edge ゲートウェイの配信モードをソフトウェアスイッチに切り替える場合、留意すべき点がいくつかあります。

- ソフトウェアスイッチには、管理インタフェース (MGMT) を除くすべてのインタフェースを追加できます。
  3 つのインタフェースが必要です。WAN と LAN1 は必須です。LAN2 または LAN3 を 3 番目のインタフェースとして追加できます。必要に応じて LAN2 と LAN3 の両方をソフトウェアスイッチに追加できます。
- WAN および LAN1 インタフェースのフェールセーフアクセス:
  - 配信モードをソフトウェアスイッチに設定したゲートウェイをマルチポートブリッジのように機能させる場合でも、Cloud Edge は WAN および LAN1 インタフェースを使用してフェールセーフアクセスを提供します。
  - WAN および LAN1 インタフェースは、ゲートウェイがオフラインになっていても、バイパスポートとして機能し、LAN1 ポート経由のアクセスをサポートします。インターネットを必要とするデバイスは、LAN1 インタフェース経由で接続する必要があります。
- インタフェースをソフトウェアスイッチ設定に追加すると、次の処理が実行されます。
  - インタフェースは自動的に有効になります。
  - L3 インタフェースは自動的に L2 に変更されます。
  - インタフェースの DHCP サービスは無効になります。
  - 関連する SNAT ルールは削除されます。

- ソフトウェアスイッチに含まれている L2 インタフェースを L3 インタフェースに変更することはできません。
- ソフトウェアスイッチに含まれている L2 インタフェースを無効にすることはできません。

- ソフトウェアスイッチ設定を設定するときは次のルールが適用されます。
  - ソフトウェアスイッチに追加された L2 インタフェースでは、MTU 設定と帯域幅設定のみ変更できます。

    ソフトウェアスイッチの MTU (初期設定は 1438) とポートの MTU (初期設定は 1504) は、どちらも変更できます。ソフトウェアスイッチの MTU を、ポートの MTU よりも大きくすることはできません。
  - ソフトウェアスイッチの設定は、On-Premises Console で行う必要があります。
- ソフトウェアスイッチ配信のメール検索には以下が適用されます。
  - ブリッジモードでは、Cloud Edge は WAN インタフェースと LAN1 インタフェースの間のトラフィックに対してのみメール検索を実行します。

    メール検索は LAN インタフェース間のトラフィックに対しては実行されません。
  - ソフトウェアスイッチ配信では、Cloud Edge は WAN インタフェースとすべての LAN インタフェースの間のトラフィックに対してメール検索を実行します。

    メール検索は LAN インタフェース間のトラフィックに対して実行されます。
- ソフトウェアスイッチとルーティングモードで配信を切り替えるときは、次の点に留意してください。
  - ソフトウェアスイッチからルーティングモードに設定を変更した場合、ソフトウェアスイッチの設定は失われます。
  - ルーティングモードからソフトウェアスイッチに設定を変更した場合、LAN2 および LAN3 の設定と関連する NAT ルールが失われます。

インタフェースの有効化または無効化

Cloud Edge ゲートウェイの特定のインタフェースは、配信モードに応じて、初期設定で有効または無効にされています。特定の設定では、一部のインタフェースを無効にすることができない場合があります。

注意

管理ポートはいずれの配信モードでも無効にできません。

図 7-7. 例: ルーティングモードの Cloud Edge 70

Cloud Edge On-Premises Console でインタフェースを有効または無効にします。

- ルーティングモード: LAN2 および LAN3 は初期設定で有効になっています。

  これらのインタフェースは、いつでも無効にしたり再度有効にしたりできます。

- ブリッジモード: LAN2 および LAN3 は初期設定で無効になっています。

  これらのインタフェースは、いつでも有効または無効にできます。

- ソフトウェアスイッチ: LAN2 および LAN3 をソフトウェアスイッチインタフェースとして追加すると、それらのインタフェースは自動的に有効になります。

ソフトウェアスイッチ設定に含まれているインタフェースを無効にすることはできません。

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイ

図 7-8. 例: ブリッジモードの Cloud Edge 100 G2

すべてのポートは初期設定で有効になっています。WAN、LAN8、管理インタフェースは無効にすることはできません。

- ルーティングモード

  LAN1-LAN7 インタフェースを無効にすることができます。

- ブリッジモード

  WAN および LAN1-LAN8 インタフェースは、ハードウェアスイッチのポートとして自動的に選択されます。これらのポートをハードウェアスイッチの設定から削除することはできませんが、LAN1-LAN7 インタフェースを無効にすることはできます。

ワイヤレスネットワーク機能を備えた Cloud Edge ゲートウェイ

[インタフェース] ページでは、ワイヤレスネットワークインタフェースを有効にしたり、無効にしたりすることはできません。

メインワイヤレスネットワークはワイヤレスアクセスを有効にした場合に自動的に有効になり、ゲストワイヤレスネットワークはゲストワイヤレスネットワークを有効にした場合に自動的に有効になります。ワイヤレスネットワークインタフェースは、対応するワイヤレスネットワークを無効にすると自動的に無効になります。

手順

1. Cloud Edge On-Premises Console で、[ネットワーク] > [インタフェース] に移動します。
2. 次のいずれかを実行します。
   a. 有効にするインタフェースの[有効にする] アイコン ( ) をクリックします。
   b. 無効にするインタフェースの[無効にする] アイコン ( ) をクリックします。

ブリッジモード/ソフトウェアスイッチのネットワークインタフェースを編集する

ブリッジモードまたはソフトウェアスイッチ設定の Cloud Edge ゲートウェイで、L2 物理インタフェースの MTU を設定できます。この手順には、On-Premises Console を使用する必要があります。

注意

ブリッジモード (スイッチチップセット使用) の物理インタフェースを設定する場合の手順については、338 ページの「ブリッジモード (スイッチチップセット使用) のネットワークインタフェースを編集する」を参照してください。

ルーティングモードの物理インタフェースを設定する場合の手順については、343 ページの「ルーティングモードのネットワークインタフェースを編集する」を参照してください。

手順

1. [ネットワーク] > [インタフェース] に移動します。

2. 編集する L2 インタフェースの名前をクリックします。

   [インタフェースの編集] 画面が開きます。

3. [MTU] に、必要な MTU を入力します。

   入力できる値の範囲は 576〜1504 です。物理インタフェースで設定する MTU は、ブリッジインタフェース (br0)で設定する MTU と区別されます。ブリッジインタフェース (br0) で設定する MTU を、物理インタフェースで設定されている MTU より小さくすることはできません。

4. [適用] をクリックします。

ブリッジモード (スイッチチップセット使用) のネットワークインタフェースを編集する

ブリッジモードでは、ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイで L2 物理インタフェース (WAN、LAN1-LAN8) を設定できます。この手順には、On-Premises Console を使用する必要があります。インタフェースやイントラネットセキュリティモードに応じて、MTU、ストーム制御、フロー制御などの設定を行えます。

ブリッジモードのハードウェアスイッチチップセットを備えたゲートウェイは、アップグレード、再起動、電源オフ、システムパニックなどのイベント中に使用できる独自のバイパス機能を備えています。バイパス機能はインタフェースによって決まります。各インタフェースにエンドポイントを割り当てる方法を決定するには、295 ページの「ハードウェアスイッチチップセットを備えたゲートウェイでのバイパスポート」を参照してください。

注意

ブリッジモードまたはソフトウェアスイッチで L2 物理インタフェースを設定する場合の手順については、337 ページの「ブリッジモード/ソフトウェアスイッチのネットワークインタフェースを編集する」を参照してください。

ルーティングモードの L3 物理インタフェースを設定する場合の手順については、343 ページの「ルーティングモードのネットワークインタフェースを編集する」を参照してください。

手順

1. [ネットワーク] > [インタフェース] に移動します。
2. [名前] で WAN インタフェースをクリックし、MTU を設定します。

オプション	説明
種類	読み取り専用フィールド。[種類] は変更できず、WAN インタフェースをスイッチ設定から削除することもできません。
MTU	576〜1504 の値を指定します。WAN インタフェース用にジャンボフレームを設定することはできません。 WAN インタフェースで編集可能なフィールドは MTU だけです。

3. [名前] で編集する L2 インタフェースの名前 (LAN1-LAN8) をクリックし、編集可能なインタフェース設定を設定します。

   高セキュリティモードおよびバランスモード

オプション	説明
種類	読み取り専用フィールド。[種類] は変更できず、WAN インタフェースをスイッチ設定から削除することもできません。
MTU	範囲: 576〜9216、初期設定値: 1504 物理インタフェースで設定する MTU は、スイッチインタフェース (sw0)で設定する MTU と区別されます。スイッチインタフェース (sw0) で設定する MTU を、物理インタフェースで設定されている MTU より小さくすることはできません。
ストーム制御しきい値	しきい値 (Mbps) を整数で指定します。
ストーム制御モード	ストーム制御を適用するパケットの種類を選択します。 • マルチキャスト • ブロードキャスト

   高速モード

注意

高速モードの MTU は変更できません。MTU は、ジャンボフレームを受け入れるようにあらかじめ設定されています。

オプション	説明
種類	読み取り専用フィールド。[種類] は変更できず、WAN インタフェースをスイッチ設定から削除することもできません。
フロー制御	フロー制御を有効にするには、[有効にする] を選択します。
ストーム制御しきい値	しきい値 (Mbps) を整数で指定します。
ストーム制御モード	ストーム制御を適用するパケットの種類を選択します。 • 宛先不明ユニキャスト • マルチキャスト • ブロードキャスト

4. [適用] をクリックします。

インタフェース設定のリスト: ブリッジモード (スイッチチップセット使用)

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイに物理インタフェース (WAN、LAN1-LAN8) を設定する前に、高セキュリティ、バランス、および高速の各イントラネットセキュリティモードで利用できる設定を確認できます。On-Premises Console を使用して WAN、LAN1-LAN8 インタフェースを設定する必要があります。

各モードで提供されているネットワークセキュリティの詳細については、134 ページの「各イントラネットセキュリティモードで提供されるセキュリティ保護」を参照してください。

高セキュリティモード

設定	説明
種類	[L2] に設定します。 ブリッジモードの読み取り専用フィールド。種類は変更できません。また、WAN/LAN1-LAN8 インタフェースはスイッチ設定から削除できません。
MTU	高セキュリティモードおよびバランスモードの設定が可能です。 LAN1-LAN8 のジャンボフレームサポート。 範囲: 576～9216、初期設定値: 1504。 注意 WAN MTU の範囲は 576～1504 です。
ストーム制御しきい値	すべてのセキュリティモードの設定が可能です。 このしきい値は各種のストーム制御に対して個別に適用されます。たとえば、20 に設定すると、マルチキャストしきい値とブロードキャストしきい値はそれぞれ 20 に設定されます。
ストーム制御モード: マルチキャスト	すべてのセキュリティモードの設定が可能です。
ストーム制御モード: ブロードキャスト	すべてのセキュリティモードの設定が可能です。

バランスモード

設定	説明
種類	[L2] に設定します。 ブリッジモードの読み取り専用フィールド。種類は変更できません。また、WAN/LAN1-LAN8 インタフェースはスイッチ設定から削除できません。

設定	説明
MTU	高セキュリティモードおよびバランスモードの設定が可能です。 LAN1-LAN8 のジャンボフレームサポート。 範囲: 576〜9216、初期設定値: 1504。 注意 WAN MTU の範囲は 576〜1504 です。
ストーム制御しきい値	すべてのセキュリティモードの設定が可能です。 このしきい値は各種のストーム制御に対して個別に適用されます。たとえば、20 に設定すると、マルチキャストしきい値とブロードキャストしきい値はそれぞれ 20 に設定されます。
ストーム制御モード: マルチキャスト	すべてのセキュリティモードの設定が可能です。
ストーム制御モード: ブロードキャスト	すべてのセキュリティモードの設定が可能です。

高速モード

設定	説明
種類	[L2] に設定します。 ブリッジモードの読み取り専用フィールド種類は変更できません。また、WAN/LAN1-LAN8 インタフェースはスイッチ設定から削除できません。
MTU	高速モードに設定されている場合は表示されないフィールド。 高速モードでは LAN インタフェースの MTU を変更できませんが、LAN1-LAN8 の MTU はジャンボフレームを受け入れるよう事前に設定されています。WAN MTU の範囲は 576〜1504 です。
フロー制御	高速モードの設定のみ。

設定	説明
ストーム制御しきい値	すべてのセキュリティモードの設定が可能です。 このしきい値は各種のストーム制御に対して個別に適用されます。たとえば、20 に設定すると、宛先不明ユニキャストしきい値、マルチキャストしきい値、ブロードキャストしきい値はそれぞれ 20 に設定されます。
ストーム制御モード: 宛先不明ユニキャスト	高速モードの設定のみ。
ストーム制御モード: マルチキャスト	すべてのセキュリティモードの設定が可能です。
ストーム制御モード: ブロードキャスト	すべてのセキュリティモードの設定が可能です。

注意

管理インタフェースは Cloud Edge Cloud Console で設定します。

ハードウェアスイッチチップセットを備えたゲートウェイをルーティングモードで配信する場合は、ルーティングモードに設定されたその他のすべての Cloud Edge モデルを設定するのと同じ方法でゲートウェイを設定します。

ルーティングモードのネットワークインタフェースを編集する

ルーティングモードの Cloud Edge ゲートウェイを登録する前に、On-Premises Console を使用してすべての L3 物理インタフェースを設定できます。Cloud Edge Cloud Console に Cloud Edge ゲートウェイを登録した後、On-Premises Console では WAN および LAN1 物理インタフェースのみ編集できます。

注意

ブリッジモードまたはソフトウェアスイッチで物理インタフェースを設定する場合の手順については、337 ページの「ブリッジモード/ソフトウェアスイッチのネットワークインタフェースを編集する」を参照してください。

ブリッジモード (スイッチチップセット使用) の物理インタフェースを設定する場合の手順については、338 ページの「ブリッジモード (スイッチチップセット使用) のネットワークインタフェースを編集する」を参照してください。

手順

1. [ネットワーク] > [インタフェース] に移動します。
2. インタフェースの名前をクリックします。
3. インタフェースモードに基づいてインタフェース設定を行います。

   WAN および LAN1 インタフェースでは、静的アドレス、DHCP アドレス、または PPPoE アドレスを使用できます。

   - 静的アドレスの場合は、次の該当するパラメータを設定します。

オプション	説明
種類	[L3] を選択します。
モード	[静的] を選択します。
MTU	576〜1500 の値を指定します。
MSS	[上書き] を選択し、536〜1460 の値を指定します。 **注意** MSS 値は、(MTU - 40) 以下の値にする必要があります。
IPv4 アドレス	IPv4 アドレスを指定します (例: `10.10.10.23`)。
IPv4 ネットマスク	Ipv4 サブネットマスクを指定します (例: `255.255.254.0`)。

オプション	説明
IPv4 デフォルトゲートウェイ	IPv4 デフォルトゲートウェイを指定します (例: `10.10.10.1`)。インターネットに接続するインタフェースにのみ、この設定を適用します。

- DHCP の場合は、次の該当するパラメータを設定します。

オプション	説明
種類	[L3] を選択します。
モード	[DHCP] を選択します。
MTU	576〜1500 の値を指定します。
MSS	[上書き] を選択し、536〜1460 の値を指定します。 注意 MSS 値は、(MTU - 40) 以下の値にする必要があります。

- PPPoE の場合は、次のパラメータを設定します。

注意
PPPoE の使用時には、MTU または MSS は設定できません。

オプション	説明
種類	[L3] を選択します。
モード	[PPPoE] を選択します。
ユーザ名	インターネットサービスプロバイダから提供されたユーザ名を指定します。

オプション	説明
	注意 最大 3 つの ISP アカウントを指定できます。プライマリ ISP アカウントが使用できない場合、Cloud Edge は自動的にセカンダリ ISP アカウントまたはターシャリ ISP アカウントを使用してネットワークに接続します。プライマリ ISP アカウントが使用できるようになるとすぐに、Cloud Edge はプライマリ ISP アカウントに切り替わります。
パスワード	インターネットサービスプロバイダから提供されたパスワードを指定します。
PPPoE の詳細設定	次の設定を行います。 • オンデマンドアイドルタイム (秒): 非アクティブな時間が指定した時間以上続くと、Cloud Edge ゲートウェイはインターネット接続を切断します。非アクティブな時間がこの設定を超えたために Cloud Edge ゲートウェイのインターネット接続が切断された場合は、インターネットへのアクセスを試みた時点ですぐに接続が復元されます。 このオプションは、初期設定では無効になっています。 • 接続タイムアウト (秒): このオプションを設定すると、インターネット接続が指定した間隔で定期的にチェックされます。インターネット接続が使用できない場合は、接続が自動的に再確立されます。 このオプションでは、接続がアイドル状態のままであっても、ゲートウェイからインターネットへの接続は維持されます。このオプションを使用すると、常時接続されるため、インターネット接続の応答時間が最小限になります。 この設定の初期設定値は 30 (秒) です。

4. ゲートウェイが登録されていない場合は、インタフェースの管理アクセスを設定します。

   許可する管理サービスおよびトラフィックを選択します (On-Premises Console、Ping、SSH、SNMP)。選択したサービスを使用して Cloud Edge ゲートウェイを内部ネットワークから管理できるようになります。On-Premises Console 管理サービスを有効にすると、承認されたユーザは On-Premises Console へのログオンが可能になります。

注意

Cloud Edge ゲートウェイが登録されていない場合にのみ、On-Premises Console で管理アクセスを設定できます。ゲートウェイの登録後、このフィールドは読み取り専用となり、管理アクセスは Cloud Edge Cloud Console で設定する必要があります。

管理サービスは Cloud Edge ゲートウェイの WAN インタフェースでも有効にできますが、この方法はお勧めしません。管理サービスおよびトラフィックを有効にするのは、内部インタフェースのみにしてください。

5. [監視設定] セクションで、Cloud Edge で監視するホスト (IP アドレスまたはドメイン名) を指定します。

   あるホストにアクセスできない場合、Cloud Edge ゲートウェイは現在の接続を切断し、次に設定されている ISP アカウントを使用して接続を確立します。使用できないホストがある場合は、静的ルート、またはインタフェースに関連付けられたポリシーベースのルートが無効になります。ただし、プライマリ接続が使用できるようになると、Cloud Edge はアクティブな接続を切断し、プライマリ接続を再確立します。

   詳細については、348 ページの「監視ホストを使用してルートが使用可能かどうかを確認する」を参照してください。

6. [帯域幅設定] セクションで、次の指定を行います。

   - ダウンストリーム: ポート経由の最大ダウンロード速度。初期設定値は空白です。
   - アップストリーム: ポート経由の最大アップロード速度。初期設定値は空白です。

   詳細については、349 ページの「インタフェース帯域幅設定を使用してトラフィックを制限する」を参照してください。

7. [適用] をクリックします。

8. [ネットワーク] > [インタフェース] のリストでインタフェースが更新されていることを確認します。

監視ホストを使用してルートが使用可能かどうかを確認する

監視ホスト

Cloud Edge は、各出力インタフェースから対応する監視 IP アドレスまたはホスト名への ping を実行することで、ネットワークの健全性を確認します。監視ホストに到達できない場合、インタフェースに関連付けられた静的ルートとポリシーベースのルートはすべて無効になります。トラフィックが別のルートに一致する場合は、他の静的ルートまたはポリシーベースのルートにルーティングされます。別のルートに一致しないトラフィックは、デフォルトゲートウェイ経由でルーティングされるか破棄されます。

- 監視ホストの設定方法については、348 ページの「インタフェースでのホストの監視を設定する」を参照してください。
- デフォルトゲートウェイの設定方法については、154 ページの「静的ルートを追加する」を参照してください。
- ポリシーベースのルートの設定方法については、377 ページの「ポリシーベースのルートを追加する」を参照してください。

自動フェイルオーバーについては、376 ページの「複数の ISP/WAN 環境の自動フェイルオーバー」を参照してください。

インタフェースでのホストの監視を設定する

手順

1. [ネットワーク] > [インタフェース] に移動します。

   注意

   Cloud Edge Cloud Console に Cloud Edge ゲートウェイを登録する前は、すべてのインタフェースでホストの監視を設定できます。登録後は、WAN および LAN1 インタフェースでのみホストの監視を設定できます。

2. インタフェースの名前をクリックします。
3. [監視設定] をクリックします。

   [監視設定] セクションが開きます。

4. [インタフェースの監視を有効にする] を選択します。
5. インタフェースを監視するホストの IP アドレスを追加します。
6. [適用] をクリックします。

インタフェース帯域幅設定を使用してトラフィックを制限する

インタフェース帯域幅設定では、ダウンストリームおよびアップストリームのトラフィックに対する最大しきい値を設定できます。帯域幅制御ポリシーは、インタフェース帯域幅のしきい値の範囲内で設定する必要があります。初期設定では、帯域幅に制限はありません。しきい値はインタフェースごとに個別に設定できます。

インタフェース帯域幅設定が正しく割り当てられていないと、ネットワークに輻輳が生じることがあります。インタフェース帯域幅をそのインタフェースに対して許容される最大しきい値に設定したうえで、どのトラフィックを優先するかを制御する帯域幅制御ポリシーを設定することをお勧めします。

インタフェース帯域幅を設定するには、[ネットワーク] > [インタフェース] の順に選択します。詳細については、Cloud Edge On-Premises Console に関するトピック 343 ページの「ルーティングモードのネットワークインタフェースを編集する」を参照してください。

注意

Cloud Edge ゲートウェイを Cloud Edge Cloud Console に登録する前は、すべてのルーティングモードインタフェースで帯域幅を設定できます。登録後、帯域幅は WAN インタフェースまたは LAN1 インタフェースでのみ設定できます。

VLAN を管理する

VLAN の仕組み

VLAN (Virtual Local Area Network) とは、エンドポイント、サーバ、およびその他のネットワークデバイスをグループ化して、その物理的な場所にかかわらず、同じ LAN セグメント上に存在するかのようにデバイス間通信を行う技術のことです。物理配置が異なるエンドポイントやサーバであっても、同じ VLAN に属することができます。

VLAN は、デバイスを物理的ではなく論理的に分離します。各 VLAN はブロードキャストドメインとして扱われます。VLAN 1 に属するデバイスは、同じ VLAN 1 に属する他のデバイスと直接通信することができますが、他の VLAN に属するデバイスにはルータ経由で通信する必要があります。VLAN 上のデバイス間の通信は、物理的なネットワークとは別のものです。

VLAN では、VLAN に属するデバイスで送受信されるすべてのパケットに 802.1Q VLAN タグを追加することでデバイスを分離します。VLAN タグは、VLAN 識別子などの情報が含まれた 4 バイトの拡張フレームです。

VLAN サブインタフェースを追加/編集する

VLAN タグ付きパケットを受信する Cloud Edge eth0 および eth1 インタフェースに L3 VLAN サブインタフェースを追加できます。各 L3 VLAN サブインタフェースは、一意の IPv4 アドレスとネットマスクを使用して設定する必要があります。必要に応じて VLAN インタフェースを編集できます。

注意

VLAN サブインタフェースをワイヤレスインタフェースに追加することはできません。

手順

1. VLAN サブインタフェースを追加する前に、VLAN が Cloud Edge ゲートウェイと連携する方法について重要な情報を確認します。

   135 ページの「VLAN で Cloud Edge を配置する方法」

2. ネットワーク > インタフェース に移動します。
3. 次の手順を実行します。
   - VLAN を追加するには、[処理] 列にある VLAN 設定追加アイコン () をクリックします。
   - VLAN を編集するには、[VLAN] セクションにある VLAN の名前をクリックします。
4. VLAN の設定を指定します。
   - 名前: VLAN インタフェースに名前を付けます。

- 種類: L3 VLAN が自動的に表示されます。読み取り専用です。

  L2 VLAN はサポートされません。

- モード: [DHCP] または [静的] を選択します。

  [静的] の場合は[IPv4 アドレス] および [IPv4 ネットマスク] を指定します。

- VLAN ID: VLAN ID を指定します。VLAN ID は、この VLAN インタフェースで受信するパケットの VLAN ID と一致する必要があります。

  各 VLAN インタフェースの VLAN ID は、VLAN インタフェースに接続された IEEE 802.1Q 準拠のルータまたはスイッチによって追加される VLAN ID と一致する必要があります。VLAN ID には 1〜4094 の範囲の任意の番号を指定できます (0 と 4095 は予約されています)。

  既存の VLAN インタフェースの VLAN ID を変更することはできません。

ワイヤレスネットワークの管理

Cloud Edge On-Premises Console を使用してワイヤレスネットワークを管理します。

ワイヤレスネットワークの概要

サポート対象の Cloud Edge ゲートウェイでは、メインワイヤレスネットワークとゲストワイヤレスネットワークを設定できます。ワイヤレスネットワークを配置して設定する方法と、ワイヤレスネットワークで使用できるゲートウェイの機能について理解しておく必要があります。

一般的な情報

ワイヤレスネットワークの設定に関する一般的な情報は、次のとおりです。

- ワイヤレスネットワークは、ルーティングモードでのみサポートされています。

  ブリッジモードからルーティングモードに変更すると、ワイヤレスネットワーク設定は初期設定になります。

- メインとゲスト、いずれのワイヤレスネットワークも、初期設定では無効になっています。
- 初期設定では、ゲストワイヤレスネットワークを有効にした場合に、ゲストワイヤレスネットワーク上のクライアントが、メインのワイヤレスネットワークまたは内部ローカルネットワークにあるリソースにアクセスできません。

  ローカルアクセスは必要に応じて有効にできます。内部リソースへのゲストアクセスを許可する前に、セキュリティに関して十分に考慮するようにしてください。
- ネットワークの周波数帯は、2.4GHz と 5GHz がサポートされています。ただし、両方を同時に使用することはできません。

  初期設定は 2.4GHz です。
- サポートされるワイヤレスクライアント接続の数は 20 です。

ワイヤレスネットワークの設定と構成

Cloud Edge ゲートウェイでワイヤレスネットワークを設定および構成する際は、次の方法に従ってください。

- メインワイヤレスネットワークの基本設定は、[クイックセットアップ] 画面から実行できます。
- 初期設定を行った後、次の場所でワイヤレスネットワークの設定を管理できます。
  - Cloud Edge On-Premises Console: 一般設定、およびメインワイヤレスネットワークとゲストワイヤレスネットワークの設定。
  - Cloud Edge Cloud Console: ワイヤレスネットワークアクセス管理の設定、およびワイヤレスクライアント接続の管理。

注意

ゲストおよびメインのワイヤレスネットワークの設定は Cloud Edge Cloud Console で確認できますが、その設定を変更するには、On-Premises Console を使用する必要があります。

ワイヤレスネットワークインタフェースの設定

ワイヤレスネットワークインタフェースを編集できます。

- ワイヤレスインタフェースの設定と情報確認は、Cloud Edge Cloud Console から行います。
- 静的 IP アドレスを持つメインおよびゲストのワイヤレスインタフェースは、[インタフェース] 画面から設定できます。

  VLAN は、ワイヤレスインタフェースではサポートされていません。

注意

ワイヤレスインタフェースが有効になっていない場合、各ワイヤレスインタフェースは [インタフェース] 画面に表示されますが、ステータスは「ダウン」になります。

- ワイヤレスインタフェースのステータスおよび統計に関する情報を確認するには、[ゲートウェイ情報] 画面を使用します。

  メインまたはゲストのワイヤレスネットワークでワイヤレスネットワーク作成が有効になっていない場合、各インタフェースのステータスは「ダウン」になります。

ワイヤレスネットワークおよび関連するネットワーク機能

管理アクセス、静的ルート、DHCP アクセス、NAT、帯域幅制御、VPN、エンドポイント保護など、ワイヤレスネットワークに関する機能を設定および構成できます。

- 管理アクセスを有効にするには、Cloud Edge Cloud Console を使用します。

  管理アクセスはメインとゲストのワイヤレスネットワークで有効にできます。ただし、ゲストワイヤレスネットワークでのアクセスの有効化は慎重に行ってください。
- 静的ルートの設定は、Cloud Edge Cloud Console から行います。
- DHCP サービスの設定は、Cloud Edge Cloud Console から行います。
  - DHCP サービスは、メインとゲストのワイヤレスネットワークで設定できます。

- ワイヤレスインタフェースは、ゲストまたはメインの各ワイヤレスネットワークが有効であるか無効であるかにかかわらず [DHCP] 画面に表示されます。

  初期設定では、DHCP サービスは既定の IP アドレスプールを使用して有効になります。

- NAT の設定は、Cloud Edge Cloud Console から行います。
  - NAT は、メインとゲストのワイヤレスネットワークで設定できます。
  - ワイヤレスインタフェースは、ゲストまたはメインの各ワイヤレスネットワークが有効であるか無効であるかにかかわらず [NAT] 画面に表示されます。

    送信先 NAT ルール: ワイヤレスインタフェースを入力インタフェースとして選択します。

    送信元 NAT ルール: ワイヤレスインタフェースを出力インタフェースとして選択します。

- 帯域幅制御を設定します。
  - 帯域幅制御は、メインおよびゲストのワイヤレスネットワークで設定できます。
  - 帯域幅制御をワイヤレスネットワークからのトラフィックに適用するには、送信元または送信先の帯域幅制御パラメータとして [すべて] を選択します。または、帯域幅制御の適用先となるワイヤレスネットワークの IP アドレスが含まれている指定のアドレスオブジェクトを設定します。

- VPN アクセスの設定は、Cloud Edge Cloud Console から行います。
  - メインとゲストのワイヤレスネットワークでユーザ VPN またはサイト間 VPN を設定できます。
  - ワイヤレスネットワークで VPN を作成するには、目的のワイヤレスネットワークの IP アドレスが含まれるネットワークオブジェクトを作成および使用します。

    メインまたはゲストのワイヤレスネットワークで VPN を作成するには、そのワイヤレスネットワークを有効にしておく必要があります。

- ネットワークアクセス管理 (エンドポイント保護) を設定できます。

  選択したゲートウェイで VBBSS エンドポイント保護および不審なクライアントからのエンドポイント保護を設定すると、ワイヤレスネットワーク上のクライアントが保護されます。

ワイヤレスネットワークと Cloud Edge のセキュリティ

ワイヤレスネットワークは Cloud Edge のセキュリティで保護されます。この保護は、Cloud Edge Cloud Console を使用して設定できます。

- ポリシーオブジェクト

  ポリシーオブジェクトを設定すると、ワイヤレスネットワークの IP アドレスまたは MAC アドレスを使用できます。

- ポリシー

  メインとゲストのワイヤレスネットワークを含むアドレスオブジェクト、またはワイヤレスネットワーク経由でログインしたユーザとグループをポリシーの対象にするには、送信元または送信先のパラメータを使用します。

- HTTPS 検査ルール

  メインとゲストのワイヤレスネットワークを含むアドレスオブジェクト、またはワイヤレスネットワーク経由でログインしたユーザとグループを HTTPS 検査ルールの対象にするには、復号の送信元または送信先のパラメータを使用します。

- 許可/ブロックリスト

  設定済みの許可リストとブロックリストは、ワイヤレスネットワークトラフィックに適用されます。

- セキュリティプロファイル

  Cloud Edge ゲートウェイ用に選択したセキュリティプロファイルは、ワイヤレスネットワークトラフィックに適用されます。

- 通知

  ワイヤレスネットワークトラフィックで違反が発生した場合、通知が送信されます。

監査と診断のサポート

ワイヤレスネットワークの設定は監査されており、ワイヤレスネットワークでは一定の診断機能を使用することができます。

- Cloud Edge Cloud Console の監査ログ: ワイヤレスネットワークを有効にすると、ワイヤレス設定の変更に関するエントリが監査ログに追加されます。
- Cloud Edge On-Premises Console の診断:
  - ワイヤレスインタフェース (wlan0 と wlan1) またはワイヤレスプロトコル (wifi0) に対してパケットの取り込みが実行されます。

    メインまたはゲストのワイヤレスネットワークが有効になっていない場合、各ワイヤレスインタフェースはパケットの取り込みの画面に表示されません。
  - 診断ファイルコレクションの [基本設定とイベントログ] カテゴリには、ワイヤレスネットワークに関する情報が含まれています。
  - ヘルスチェックでは、メインとゲストのワイヤレスインタフェースステータスに関する情報が得られます。

一般ワイヤレスネットワーク設定を行う

ワイヤレスネットワーク要件に応じた一般ワイヤレスネットワーク設定を行います。一般ワイヤレス設定には、メインワイヤレスネットワークに適用される設定もあれば、次の手順に示すように、メインとゲスト両方のワイヤレスネットワークに適用される設定もあります。

手順

1. ネットワーク > ワイヤレス > ワイヤレス設定 > 一般設定 に移動します。
2. [メインワイヤレスネットワークを有効にする] を選択します。

   設定はメインワイヤレスネットワークにのみ適用されます。初期設定では無効になっています。

   このオプションを選択しても、ゲストワイヤレスネットワークは有効になりません。ゲストワイヤレスネットワークは、[ゲストネットワーク] タブから有効にする必要があります。

3. 次の設定を行います。

   - [周波数]: ワイヤレスネットワークの周波数を選択します。

     設定はメインとゲスト両方のワイヤレスネットワークに適用されます。

     Cloud Edge のワイヤレスネットワーキングは、2.4GHz または 5.0GHz の周波数で動作できます。ゲートウェイを両方の周波数で同時に動作させることはできません。初期設定は 2.4GHz です。

   - [SSID ブロードキャストを有効にする]: メインワイヤレスネットワークの SSID をブロードキャストする場合は、このオプションを選択します。

     設定はメインワイヤレスネットワークにのみ適用されます。

     有効にすると、Cloud Edge ゲートウェイによってメインワイヤレスネットワークの SSID がブロードキャストされるので、近くにあるクライアントの利用可能なワイヤレスネットワークの画面でそのネットワークを確認できます。初期設定では有効になっています。

   - [SSID]: メインワイヤレスネットワークのアクセスポイントの名前を指定します。

     設定はメインワイヤレスネットワークにのみ適用されます。

     初期設定の SSID は次のとおりです。

     - 2.4GHz: CloudEdge-XXYY
     - 5GHz: CloudEdge-5G-XXYY

     注意

     XXYY は、Cloud Edge ゲートウェイのシリアル番号の最初の 4 文字を表しています。セキュリティを最適にするには、初期設定以外の値を SSID として入力する必要があります。

   - [チャネル]: チャネル番号を指定します。

     設定はメインとゲスト両方のワイヤレスネットワークに適用されます。

チャネルは選択する周波数と国/地域によって異なります。初期設定値は [自動] です。

- [モード]: モードを指定します。

  設定はメインとゲスト両方のワイヤレスネットワークに適用されます。

  2.4GHz: オプションには [11bgn 混在] と [11bg 混在] があります。

  5GHz: オプションには [11a のみ]、[11a/n 混在]、および [11a/n/ac 混在] があります。

- [セキュリティ]: 使用するセキュリティの種類を指定します。

  設定はメインワイヤレスネットワークにのみ適用されます。

  - [開く] を選択した場合、追加のセキュリティ設定は必要ありません。
  - [WPA-PSK[TKIP]]、[WPA2-PSK[AES]]、または [WPA-PSK[TKIP]+WPA2-PSK[AES]] のセキュリティの種類を選択した場合は、[事前共有鍵] も指定する必要があります。

    注意

    [WPA-PSK[TKIP]] セキュリティ設定は、[11bg 混在] (2.4GHz) または [11a のみ] (5GHz) のいずれかのモードが選択されている場合にのみ選択できます。

  - [WPA/WPA2 エンタープライズ] のセキュリティの種類を選択した場合は、[RADIUS サーバ IP アドレス]、[RADIUS サーバポート]、および [RADIUS サーバシークレット] も指定する必要があります。

4. (任意) [WPA/WPA2 エンタープライズ] を選択した場合は、[テスト] をクリックし、Cloud Edge が正常に接続できるかどうかの確認のために RADIUS サーバに接続する際に使用するユーザ名とパスワードを入力します。
5. [詳細設定] セクションで、次の詳細ワイヤレス設定を行います。

   詳細設定はメインとゲスト両方のワイヤレスネットワークに適用されます。

- [DTIM 間隔]: DTIM 間隔を指定します。入力できる値の範囲は 1〜255 です。初期設定値は `3` です。
- [ビーコン間隔]: ビーコン間隔をミリ秒単位で指定します。入力できる値の範囲は 100〜1000 です。初期設定値は `100` です。
- [ショートプリアンブル]: このオプションは、[有効にする] または [無効にする] をクリックして有効または無効にします。
- [RTS しきい値]: RTS しきい値を 0〜2347 バイトの範囲で指定します。初期設定値は `2347` バイトです。
- [ショート GI を有効にする]: このオプションは、[有効にする] または [無効にする] をクリックして有効または無効にします。
- [送信電力]: アクセスポイントの送信電力の割合を指定します。入力できる値の範囲は 1〜100 です。初期設定値は `100` です。

注意

[ショートプリアンブル]、[RTS しきい値]、および [ショート GI を有効にする] フィールドは、2.4GHz のネットワーク周波数を選択した場合にのみ指定できます。

6. [保存] をクリックします。

ゲストワイヤレスネットワークを設定する

ワイヤレスネットワークの要件に応じてゲストワイヤレスネットワークを設定します。

手順

1. ネットワーク > ワイヤレス > ワイヤレス設定 > ゲストネットワーク に移動します。
2. [ゲストネットワークを有効にする] を選択します。

   初期設定では、ゲストワイヤレスネットワークは有効になっていません。

注意

ゲストワイヤレスネットワークを有効にするには、その前にメインワイヤレスネットワークを有効にする必要があります。

3. ゲストネットワークに使用するオプションを有効にします。
   - SSID ブロードキャストを有効にする

     有効にすると、Cloud Edge ゲートウェイによってゲストネットワークの SSID がブロードキャストされるので、近くにあるクライアントの利用可能なワイヤレスネットワークの画面でそのゲストワイヤレスネットワークを確認できます。初期設定では有効になっています。
   - ローカルネットワークアクセスを有効にする

     有効にすると、ゲストワイヤレスネットワーク上のユーザが、適切な権限を持っていることを条件として、ローカルの内部ネットワーク上のリソースにアクセスできます。初期設定では無効になっています。
4. ゲストワイヤレスネットワークの [SSID] を指定します。

   初期設定の SSID は次のとおりです。
   - 2.4GHz: CloudEdge-GUEST-XXYY
   - 5GHz: CloudEdge-5G-GUEST-XXYY

注意

XXYY は、Cloud Edge ゲートウェイのシリアル番号の最初の 4 文字を表しています。セキュリティを最適にするには、初期設定以外の値を SSID として入力する必要があります。

5. [セキュリティ設定] で、ゲストワイヤレスネットワークに使用するセキュリティの種類を指定します。
   - [開く] を選択した場合、追加のセキュリティ設定は必要ありません。
   - [WPA-PSK[TKIP]]、[WPA2-PSK[AES]]、または [WPA-PSK[TKIP] +WPA2-PSK[AES]] のセキュリティの種類を選択した場合は、[事前共有鍵] も指定する必要があります。

注意

[WPA-PSK[TKIP]] セキュリティ設定は、[一般設定] タブで [11bg 混在] (2.4GHz) または [11a のみ] (5GHz) のいずれかのモードが選択されている場合にのみ選択できます。

- [WPA/WPA2 エンタープライズ] のセキュリティの種類を選択した場合は、[RADIUS サーバ IP アドレス]、[RADIUS サーバポート]、および [RADIUS サーバシークレット] も指定する必要があります。

6. (任意) [WPA/WPA2 エンタープライズ] を選択した場合は、[テスト] をクリックし、Cloud Edge が正常に接続できるかどうかの確認のために RADIUS サーバに接続する際に使用するユーザ名とパスワードを入力します。
7. [保存] をクリックします。

ワイヤレスネットワークのトラブルシューティング

ワイヤレスネットワークのトラブルシューティング情報を確認します。

手順

1. ネットワーク > ワイヤレス > ワイヤレス設定 > トラブルシューティングに移動します。
2. ログを利用して、ワイヤレスネットワークのトラブルシューティングを実行します。
3. ページの右上にある更新アイコンをクリックして、表示されたログエントリを更新します。

   表示できるレコードの最大数は 100 です。

DNS を管理する

Cloud Edge ゲートウェイの DNS (ドメインネームサーバ) 設定を表示し、編集することができます。

DHCP または PPPoE を使用してインターネットにアクセスする環境では、DNS 設定が ISP から動的に取得されるため、DNS の設定が不要である場合があります。

DNS ベストプラクティスの提案

Cloud Edge アプライアンスは、トレンドマイクロの提供するクラウドベースのサービス Smart Protection Network を使用します。Smart Protection Network への接続には名前解決が必要なため、Cloud Edge デバイスには DNS サーバを設定する必要があります。最大 3 つの DNS サーバを設定できます。

DNS サーバには、Cloud Edge からのまとまった DNS 要求に対応することが求められます。通常は、アクセスされる URL ごとに 2 つの DNS 要求が作成され、Cloud Edge 用のローカルな DNS キャッシュが作成されます。DNS サーバが、必要以上の DNS を処理できるだけのリソースとパフォーマンスを備えたサーバに設置されていることを確認します。

遅延時間を少なくするには、それぞれの DNS サーバが高速なネットワークカードを保有し、高速なネットワークスイッチに取り付けられている必要があります。

トレンドマイクロは、現地 DNS サーバと、企業ネットワーク外に設置された ISP 提供の DNS サーバを使用することをお勧めします。通常、IPS DNS サーバは遅延時間が長く、単一の IP アドレスからの多量の DNS クエリはサポートしません。多くの IPS DNS サーバは、1 秒あたりの DNS 要求数を制限する調整メカニズムを備えているため、Cloud Edge の Web レピュテーションサービス (WRS) のパフォーマンスに影響を与える可能性があります。

ネットワーク応答時間とパフォーマンスを向上させるには、DNS サーバを Cloud Edge ユニットのできるだけ近くに設置し、デバイス間の不要なネットワークホップを削減するようにしてください。

WRS と URL フィルタ要求は、HTTP ポート 80 を介して作成されます。ファイアウォール上のこれらのポートでは、Cloud Edge の管理 IP アドレスをブロックしないでください。

DNS の設定を行う

手順

1. [ネットワーク] > [DNS] に移動します。
2. 該当する DNS サーバの IPv4 アドレスを設定します。

注意

Cloud Edge により、DNS サーバの IP アドレスがインターネットサービスプロバイダから動的に取得される場合、[DNS 情報を継承] には DNS 情報が読み取り専用で表示されます。

3. [適用] をクリックします。

アドレスオブジェクトを管理する

アドレスオブジェクトは、内部ネットワークで許可される IP アドレス範囲を指定するオブジェクトです。初期設定では「初期設定の内部アドレス」アドレスオブジェクトが使用されます。このオブジェクトには、すべての内部 IP アドレス範囲 (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16) が含まれます。アドレスオブジェクトは、ポリシーベースのルーティングを設定するときにも使用します。

- 設定されている IPv4 アドレスオブジェクトを表示および編集するには、Cloud Edge On-Premises Console で [ネットワーク] > [アドレス] に移動します。
- ゲートウェイ登録後は、Cloud Edge On-Premises Console の [ネットワーク] > [アドレス] ページで、アドレスオブジェクトを新たに追加したり削除したりすることはできません。
- ネットワーク設定やポリシーベースのルーティングで使用する IPv4 アドレスオブジェクトを追加、編集、削除するには、Cloud Edge Cloud Console を使用します。

注意

[ルーティング] でポリシーベースのルールを作成するときに、新しい IPv4 アドレスオブジェクトを追加できます。ポリシーベースのルーティングの設定時に追加したアドレスオブジェクトは、[ネットワーク] > [アドレス] ページで後から編集できます。

IP アドレスオブジェクトのパラメータ

次の表に、Cloud Edge On-Premises Console で IPv4 オブジェクトを追加または編集するときに設定可能なパラメータを示します。これらの IPv4 アドレスオブジェクトは、On-Premises Console でポリシールーティングのルールを設定するときに使用できます。

表 7-6. アドレスオブジェクトのパラメータ

パラメータ	説明
オブジェクト名	アドレスの内容がわかるように名前を指定します。この名前は、ポリシーベースのルーティングのためのルールを定義するときにアドレスリストに表示されます。大文字と小文字が区別され、一意の名前を指定する必要があります。使用できる文字は、英字、数字、スペース、ハイフン、およびアンダースコアのみです。
種類	IPv4
アドレス	次のいずれかの形式で IP アドレスまたはネットワークを指定します。 • `ip_address` • `ip_address_range` • `ip_address/bitmask` 例: 192.168.1.1、192.168.1.1-192.168.1.10、または 192.168.80.0/24

アドレスオブジェクトを表示する

手順

- [ネットワーク] > [アドレス] に移動します。

アドレスオブジェクトを編集する

Cloud Edge On-Premises Console を使用して、既存の IPv4 アドレスオブジェクトの IP アドレスを編集できます。

「初期設定の内部アドレス」という、初期設定の IPv4 アドレスオブジェクトには、10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 という IP アドレスが設定されています。

手順

1. [ネットワーク] > [アドレス] に移動します。
2. 編集するアドレスオブジェクトの名前をクリックします。
3. IP アドレスを編集します。

   Cloud Edge で IPv4 アドレスオブジェクトの設定を編集する場合は、単一の IP アドレス、範囲を表す「-」記号、および IP アドレス/ネットマスク (192.168.1.1/24) がサポートされます。

   例: `192.168.0.1,10.0.0.1-10.0.0.4,192.168.1.1/24`
4. [OK] をクリックします。
5. [ネットワーク] > [アドレス] のリストで、編集したアドレスオブジェクトの IP アドレスが変更されていることを確認します。

注意

[ネットワーク][アドレス] ページでは、IPv4 アドレスオブジェクトを編集できますが、新たに追加することはできません。ただし、[ルーティング] でポリシーベースのルールを作成するときに、新しい IPv4 アドレスオブジェクトを追加できます。ポリシーベースのルーティングの設定時に追加したアドレスオブジェクトは、後からこの手順で編集できます。

ブリッジ/スイッチ設定を管理する

Cloud Edge On-Premises Console でブリッジモード/ソフトウェアスイッチ配信のブリッジインタフェース (br0) またはブリッジモード (スイッチチップセット使用) のスイッチインタフェース (sw0) を表示し、管理できます。

手順

1. Cloud Edge ゲートウェイのモデルに応じて次の手順を実行します。
   a. ネットワーク > ブリッジ に移動します。
   b. ネットワーク > スイッチ に移動します。
2. [名前] で適切な処理を実行します。
   a. [br0] をクリックします。
   b. ハードウェアスイッチチップセットを備えたゲートウェイの [sw0] をクリックします。
3. 次のように実行します。
   - ブリッジインタフェース (br0) またはスイッチインタフェース (sw0) の設定の概要を表示します。
   - ブリッジインタフェース (br0) またはスイッチインタフェース (sw0) の名前をクリックし、詳細を表示するか設定を編集します。

次に進む前に

Cloud Edge Cloud Console を使用してスイッチインタフェース (sw0)のイントラネットセキュリティモードの設定を行います。

セキュリティモードの変更またはセキュリティモード設定の編集を行うには、Cloud Edge Cloud Console にログオンし、ゲートウェイ > (選択したゲートウェイ) > ネットワーク > インタフェース 画面の順に進みます。

129 ページの「スイッチインタフェース (sw0) を設定する」を参照してください。

ブリッジインタフェース (br0) を設定する

選択したブリッジモードのゲートウェイに対してブリッジインタフェース (br0) を設定できます。ブリッジインタフェース (br0) は仮想インタフェースであり、Cloud Edge On-Premises Console で設定する必要があります。

注意

ソフトウェアスイッチ用にブリッジインタフェース (br0) を設定する場合の手順については、369 ページの「ソフトウェアスイッチ用のブリッジインタフェース (br0) を設定する」を参照してください。

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイでブリッジモード用のスイッチインタフェース (sw0)を設定する場合の手順については、次を参照してください。

- 371 ページの「スイッチインタフェース (sw0) を設定する」 (Cloud Edge On-Premises Console で設定)
- 129 ページの「スイッチインタフェース (sw0) を設定する」 (Cloud Edge Cloud Console で設定)

手順

1. ネットワーク > ブリッジ に移動します。
2. [名前] で [br0] をクリックします。

   [ブリッジの追加/編集] 画面が開きます。
3. [種類] で [ブリッジ] を選択します。

   [インタフェース 1] と [インタフェース 2] フィールドは読み取り専用フィールドです。それぞれ [WAN [L2]] と [LAN1 [L2]] があらかじめ選択され、L2 インタフェースとして設定されています。
4. 編集可能なインタフェース設定を設定します。

   ブリッジインタフェース (br0) では、静的アドレスまたは DHCP アドレスを使用できます。

   - 静的アドレスの場合は、次の該当するパラメータを設定します。

オプション	説明
モード	[静的] を選択します。
MTU	576〜1500 の値を指定します。
IPv4 アドレス	IPv4 アドレスを指定します (例: `10.10.10.23`)。
IPv4 ネットマスク	Ipv4 サブネットマスクを指定します (例: `255.255.254.0`)。
IPv4 デフォルトゲートウェイ	IPv4 デフォルトゲートウェイを指定します (例: `10.10.10.1`)。インターネットに接続するインタフェースにのみ、この設定を適用します。

- DHCP の場合は、次の該当するパラメータを設定します。

オプション	説明
モード	[DHCP] を選択します。
MTU	576〜1500 の値を指定します。

5. ゲートウェイが登録されていない場合は、ブリッジインタフェース (br0) の管理アクセスを設定します。

   許可する管理サービスおよびトラフィックを選択します (On-Premises Console、Ping、SSH、SNMP)。選択したサービスを使用して Cloud Edge ゲートウェイを内部ネットワークから管理できるようになります。On-Premises Console 管理サービスを有効にすると、承認されたユーザは On-Premises Console へのログオンが可能になります。

   注意

   Cloud Edge ゲートウェイが登録されていない場合にのみ、On-Premises Console で管理アクセスを設定できます。ゲートウェイの登録後、このフィールドは読み取り専用となり、管理アクセスは Cloud Edge Cloud Console で設定する必要があります。

6. [詳細設定] で、必要に応じて [スパニングツリープロトコルを有効にする] を選択します。

   Cloud Edge はスパニングツリープロトコルを使用して、ゲートウェイが設置されているネットワーク上のループを検出して防止します。Cloud

Edge はダウンストリームのネットワークやダウンストリームのデバイス上で発生したループを検出できません。

7. [詳細設定] で、必要に応じて [リンクロス転送を有効にする] を選択します。
8. [適用] をクリックします。

ソフトウェアスイッチ用のブリッジインタフェース (br0) を設定する

ソフトウェアスイッチ (ブリッジモードのバリエーション) として配信される選択したゲートウェイに対して、ブリッジインタフェース (br0) でソフトウェアスイッチを設定できます。ブリッジインタフェース (br0) は仮想インタフェースであり、Cloud Edge On-Premises Console で設定する必要があります。

- 配信モードをソフトウェアスイッチに設定する場合は、Cloud Edge ゲートウェイ配信のモードスイッチを [ブリッジ] にセットし、基本的なブリッジモード配信と同じ IP アドレス設定を使用してブリッジインタフェース (br0) を設定します。
- また、ソフトウェアスイッチの L2 インタフェースとして機能させる物理インタフェースを 3 つ以上追加する必要があります。WAN と LAN1 は必須ポートです。LAN2 または LAN3 を 3 番目のソフトウェアスイッチインタフェースとして追加できます。必要な場合は LAN2 ポートと LAN3 ポートを両方追加することもできます。

注意

ブリッジモードでブリッジインタフェース (br0) を設定する場合の手順については、367 ページの「ブリッジインタフェース (br0) を設定する」を参照してください。

ハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイでブリッジモード用のスイッチインタフェース (sw0)を設定する場合の手順については、次を参照してください。

- 371 ページの「スイッチインタフェース (sw0) を設定する」 (Cloud Edge On-Premises Console で設定)
- 129 ページの「スイッチインタフェース (sw0) を設定する」 (Cloud Edge Cloud Console で設定)

手順

1. ネットワーク > ブリッジ に移動します。
2. [名前] で [br0] をクリックします。

   [ブリッジの追加/編集] 画面が開きます。
3. [種類] で [ソフトウェアスイッチ] を選択します。

   ソフトウェアスイッチ設定用の追加パラメータが使用可能になります。
4. [スイッチインタフェース] で、ソフトウェアスイッチに含める物理インタフェースを選択します。

   - [WAN[L2]] と [LAN1[L2]] は必須であり、あらかじめ選択されています。選択解除はできません。
   - 少なくとも [LAN2[L2]] または [LAN3[L2]] のどちらかを選択する必要があります。[LAN2[L2]] と [LAN3[L2]] を両方選択することもできます。
5. ブリッジインタフェース (br0) の設定に使用する [モード] を選択します。

   [静的] または [DHCP] を選択します。
6. (任意) ソフトウェアスイッチの [MTU] を変更します。

   初期設定は 1438 です。選択できる値の範囲は 576～1500 です。

   Cloud Edge ゲートウェイの物理インタフェースの MTU を変更することもできます。ソフトウェアスイッチの MTU 設定は、物理インタフェースで設定されている MTU より大きくすることはできません。
7. [モード] が [静的] の場合は、該当する IPv4 インタフェースを設定します。

オプション	説明
IPv4 アドレス	IPv4 アドレスを指定します (例: `10.10.10.23`)。
IPv4 ネットマスク	Ipv4 サブネットマスクを指定します (例: `255.255.254.0`)。

オプション	説明
IPv4 デフォルトゲートウェイ	IPv4 デフォルトゲートウェイを指定します (例: `10.10.10.1`)。インターネットに接続するインタフェースにのみ、この設定を適用します。

8. ゲートウェイが登録されていない場合は、ブリッジインタフェース (br0) の管理アクセスを設定します。

   許可する管理サービスおよびトラフィックを選択します (On-Premises Console、Ping、SSH、SNMP)。選択したサービスを使用して Cloud Edge ゲートウェイを内部ネットワークから管理できるようになります。On-Premises Console 管理サービスを有効にすると、承認されたユーザは On-Premises Console へのログオンが可能になります。

   注意

   Cloud Edge ゲートウェイが登録されていない場合にのみ、On-Premises Console で管理アクセスを設定できます。ゲートウェイの登録後、このフィールドは読み取り専用となり、管理アクセスは Cloud Edge Cloud Console で設定する必要があります。

9. [詳細設定] で、必要に応じて [スパニングツリープロトコルを有効にする] を選択します。

   Cloud Edge はスパニングツリープロトコルを使用して、ゲートウェイが設置されているネットワーク上のループを検出して防止します。Cloud Edge はダウンストリームのネットワークやダウンストリームのデバイス上で発生したループを検出できません。

10. [適用] をクリックします。

スイッチインタフェース (sw0) を設定する

選択したブリッジモードのハードウェアスイッチチップセットを備えた Cloud Edge ゲートウェイに対してスイッチインタフェース (sw0)を設定できます。スイッチインタフェース (sw0)は仮想インタフェースであり、Cloud Edge On-Premises Console で設定します。

注意

ブリッジモードでブリッジインタフェース (br0) を設定する場合の手順については、367 ページの「ブリッジインタフェース (br0) を設定する」を参照してください。

ソフトウェアスイッチ用にブリッジインタフェース (br0) を設定する場合の手順については、369 ページの「ソフトウェアスイッチ用のブリッジインタフェース (br0) を設定する」を参照してください。

手順

1. ネットワーク > スイッチ に移動します。
2. [名前] で [sw0] をクリックします。

   [スイッチの追加/編集] 画面が開きます。

   - [名前] フィールドは読み取り専用で、[sw0] に設定されています。
   - [イントラネットセキュリティモード] フィールドは読み取り専用で、[高セキュリティ] に設定されています。

     イントラネットセキュリティモードは Cloud Edge Cloud Console を使用して変更できます。
3. [モード] では、[DHCP] または [静的] を選択します。
4. モードを [静的] にした場合は、IPv4 アドレス、IPv4 ネットマスク、および IPv4 デフォルトゲートウェイを入力します。
5. 必要に応じて、[MTU] を設定します。

   576～1500 の値を指定します。初期設定は 1438 です。
6. ゲートウェイが登録されていない場合は、スイッチインタフェース (sw0) の管理アクセスを設定します。

   許可する管理サービスおよびトラフィックを選択します (On-Premises Console、Ping、SSH、SNMP)。選択したサービスを使用して Cloud Edge ゲートウェイを内部ネットワークから管理できるようになります。On-Premises Console 管理サービスを有効にすると、承認されたユーザは On-Premises Console へのログオンが可能になります。

注意

Cloud Edge ゲートウェイが登録されていない場合にのみ、On-Premises Console で管理アクセスを設定できます。ゲートウェイの登録後、このフィールドは読み取り専用となり、管理アクセスは Cloud Edge Cloud Console で設定する必要があります。

7. ([高セキュリティ] モードと [バランス] モードのみ): 必要に応じて、[詳細設定] で次の手順を実行します。

   a. [スパニングツリープロトコルを有効にする] を選択します。

      Cloud Edge はスパニングツリープロトコルを使用して、ゲートウェイが設置されているネットワーク上のループを検出して防止します。Cloud Edge はダウンストリームのネットワークやダウンストリームのデバイス上で発生したループを検出できません。

   b. [IGMP スヌーピング] を選択します。

8. [適用] をクリックします。

次に進む前に

イントラネットセキュリティモードなどの追加のスイッチインタフェース (sw0)設定を、Cloud Edge Cloud Console で設定します。

129 ページの「スイッチインタフェース (sw0) を設定する」を参照してください。

ルーティングを管理する

Cloud Edge ゲートウェイはネットワーク上のセキュリティデバイスとして機能し、すべてのパケットがゲートウェイを通過します。Cloud Edge ゲートウェイを適切に設定するためには、ルーティングの基本概念を理解しておく必要があります。

Cloud Edge ゲートウェイには、初期設定の静的ルートが事前に定義されています。ネットワークトラフィックがポリシーベースのルーティングルールまたは設定された静的ルートのいずれにも一致しない場合は、定義済みの静的ルートが IPv4 デフォルトゲートウェイ (0.0.0.0/0 への静的ルート) として使用され、その後、すべてのトラフィックに適用されます。

事前定義された初期設定の静的ルートの代わりに、またはこれに追加して、トラフィックのルーティングを制御する次の項目を設定できます。

- IPv4 ポリシーベースのルート (環境でのトラフィックのルーティングを手動で制御する場合)
- IPv4 静的ルート
- 各インタフェースの IPv4 デフォルトゲートウェイ

重要

Cloud Edge Cloud Console に接続するためのデフォルトゲートウェイを少なくとも 1 つ設定する必要があります。

Cloud Edge はルートを選択し、指定されたルールに基づいてルーティングテーブルを動的に更新します。Cloud Edge は、一連のルールから、宛先にパケットを送信するための最適なルート (パス) を決定できます。

注意

Cloud Edge では IPv6 ルーティングはサポートされません。

ルートの設定手段

ルートを設定して、Cloud Edge ゲートウェイでのトラフィックのルーティングを制御する場合は、以下の情報を参照してください。

- IPv4 ポリシーベースのルート

  ポリシーベースのルーティングを設定するには、Cloud Edge On-Premises Console を使用する必要があります。詳細については、377 ページの「ポリシーベースのルートを追加する」を参照してください。

- IPv4 静的ルート

  静的ルートを設定するには、Cloud Edge Cloud Console を使用する必要があります。静的ルート (ゲートウェイのデフォルトルートを含む) を設定する場合は、154 ページの「静的ルートを追加する」を参照してください。

- 各インタフェースの IPv4 デフォルトゲートウェイ

  Cloud Edge On-Premises Console を使用して WAN インタフェースまたは LAN1 インタフェースにデフォルトゲートウェイを設定するには、343 ページの「ルーティングモードのネットワークインタフェースを編集する」を参照してください。

  Cloud Edge Cloud Console を使用して他のインタフェースおよび管理インタフェースにデフォルトゲートウェイを設定するには、123 ページの「ルーティングモード: ネットワークインタフェースを編集する」を参照してください。

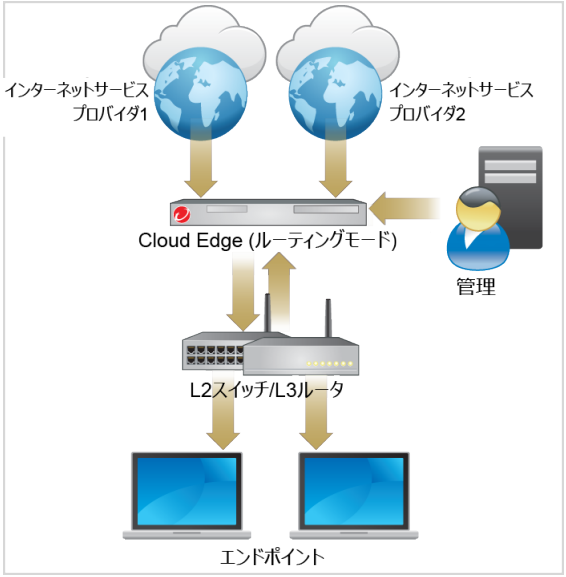
ポリシーベースのルート管理について

今日の高速ネットワーク環境においては、従来のルーティングプロトコルにとどまらない、各組織が独自に定義したポリシーに従って自由にパケットの転送およびルーティングを実装できることが求められます。静的ルーティングと動的ルーティングは、主にトラフィックの送信先に基づいてルーティングを決定する手法であるのに対し、ポリシーベースのルーティングは、パケットごとにトラフィックの特性に応じてルーティングを決定するメカニズムです。特定のトラフィックのルーティング動作を変更することは、送信先に基づくルーティング手法では簡単ではありませんが、「インテリジェントルーティング」とも呼ばれるポリシーベースのルーティングであれば、送信先のネットワークのほかに、送信元のインタフェース、送信元や送信先のアドレス、サービスの種類など、さまざまな条件に基づいてルーティング動作を指定できます。

たとえば、会社の拠点間に、高帯域幅で低遅延の高コストなリンクと、それよりも低帯域幅で高遅延の低コストなリンクの 2 つがあるとします。この場合、従来のルーティングプロトコルでは、リンクの帯域幅や遅延 (EIGRP または OSPF を使用) 特性によって得られる削減効果に基づいて、トラフィックのほとんどもしくはすべてが高帯域幅のリンク経由で送信されます。一方、ポリシーベースのルーティングであれば、優先度が高いトラフィックを高帯域幅/低遅延のリンクでルーティングし、それ以外のすべてのトラフィックを低帯域幅/高遅延のリンクで送信することができます。

ポリシーベースのルーティングでは、複数の ISP および WAN からのトラフィックをルーティングできます。次の図は、2 つの ISP 用に L2 スイッチを使用して Cloud Edge を設定した例を示したものです。

図 7-9. ポリシーベースのルーティングの例



いずれかのインタフェースの監視 IP アドレスを利用できない場合、そのインタフェースに関連付けられたポリシーベースのルートはすべて無効になります。ポリシーベースのルーティングルールに一致するトラフィックは、すべてデフォルトゲートウェイ経由でルーティングされます。監視 IP アドレスの設定方法については、348 ページの「監視ホスト」を参照してください。デフォルトゲートウェイが複数設定されている場合、送信トラフィックはラウンドロビン方式でそれらのゲートウェイからルーティングされます。

複数の ISP/WAN 環境の自動フェイルオーバー

Cloud Edge では、複数の WAN/ISP リンクがある環境において、いずれかの ISP または WAN の接続で障害が発生した場合の自動フェイルオーバーがサポートされています。10 秒おきに接続が確認され、接続を検出できなかった

場合はさらに 2 秒おきに確認が繰り返されます。連続して 4 回接続に失敗すると、自動フェイルオーバーが開始されます。後で接続が確立された時点でリンクは自動的に復旧します。

フェイルオーバーが発生したときは次の処理を実行してください。

- システムイベントログを確認する
- ルーティングテーブルでトラフィックの実際のルーティングを確認する

注意

監視ホストの詳細については、348 ページの「監視ホスト」を参照してください。

ポリシーベースのルートを追加する

環境でのトラフィックのルーティング方法を手動で制御する場合は、IPv4 ポリシーベースのルートを設定できます。

手順

1. [ネットワーク] > [ルーティング] > [ポリシールーティング] に移動します。
2. [新規追加] をクリックします。
3. 必要に応じて、ルールを有効にします。
4. ポリシー名を指定します。英字、数字、またはアンダースコアを使用して、1〜32 文字で指定する必要があります。
5. 必要に応じて、[説明] を入力します。
6. [送信元のアドレス] で、次のいずれかのパラメータを選択します。
   - すべて: すべての送信元アドレスを含みます。(初期設定)
   - アドレスを指定する: 以前に設定した送信元アドレスのリストが表示されるほか、必要に応じて新しい IPv4 アドレスオブジェクトを追加するための [新規追加] アイコン () が表示されます。

新しい IP アドレスオブジェクトを設定する場合は、378 ページの「ポリシールーティング用の新しい IPv4 アドレスオブジェクトを追加する」を参照してください。

7. [送信元のインタフェース] ドロップダウンリストから適切な送信元インタフェースを選択します。
8. [送信先のアドレス] で、次のいずれかのパラメータを選択します。
   - すべて: すべての送信先アドレスを追加します。(初期設定)
   - アドレスを指定する: 以前に設定した送信先アドレスのリストが表示されるほか、必要に応じて新しい IPv4 アドレスオブジェクトを追加するための [新規追加] アイコン () が表示されます。

     新しい IP アドレスオブジェクトを設定する場合は、378 ページの「ポリシールーティング用の新しい IPv4 アドレスオブジェクトを追加する」を参照してください。
9. [サービスの種類] で、次のいずれかのパラメータを選択します。
   - すべて: すべてのサービスを含みます。
   - 指定する: 選択したサービスのみを含みます。
10. 出力インタフェースを選択します。
11. 静的 IP アドレスが設定されたインタフェースの場合は、ネクストホップを指定します。
12. 必要に応じて、IP マスカレードを有効にします。

注意

内部 IP アドレスを出力インタフェースの IP アドレスに変換する必要がある場合は、[IP マスカレードを有効にする] を選択します。

13. [OK] をクリックします。

ポリシールーティング用の新しい IPv4 アドレスオブジェクトを追加する

ポリシーベースのルーティングのためのルールを設定する際に、新しい IPv4 アドレスオブジェクトを追加できます。

注意

ポリシールーティングルールにアドレスオブジェクトを追加する際に、IPv6 アドレスオブジェクトを設定することはできません。

手順

1. [ネットワーク] > [ルーティング] > [ポリシールーティング] の順に選択し、[新規追加] をクリックして、追加するポリシールーティングルールの設定画面を開きます。
2. 追加するポリシールーティングルールの設定画面の[送信元のアドレス] または [送信先のアドレス] で、[アドレスを指定する] を選択します。
3. [新規追加] をクリックします。

   [アドレスオブジェクトの追加/編集] 画面が開きます。
4. アドレスオブジェクトの名前を指定します。
5. Ipv4 は唯一のオプションであり、[プロトコル] リストであらかじめ選択されています。
6. IP アドレスまたは CIDR ネットワークを指定します。複数指定する場合はカンマで区切ります。

   Cloud Edge で IPv4 アドレスオブジェクトを設定する場合は、単一の IP アドレス、範囲を表す「-」記号、および IP アドレス/ネットマスク (192.168.1.1/24) がサポートされます。

   例: 192.168.0.1,10.0.0.1-10.0.0.4,192.168.1.1/24
7. [OK] をクリックします。

ルーティングテーブル

工場出荷時の初期設定の Cloud Edge ルーティングテーブルには、初期設定の IPv4 静的ルートが 1 つ含まれています。追加の IPv4 静的ルートを定義し、ルーティング情報をルーティングテーブルに追加します。テーブルには、同じ送信先へのルートを複数定義できます。これらのルートに指定されているネクストホップルータの IPv4 アドレス、またはこれらのルートに関連付けられている Cloud Edge インタフェースは同じとはかぎりません。

Cloud Edge は、ルーティングテーブル内の情報を評価し、送信先への最適なルートを選択します。通常は、Cloud Edge ゲートウェイと、最も近くに位置するネクストホップルータとの最短距離が選択されます。ただし、最適なルートが利用できない場合は最短でないルートが選択されることがあります。Cloud Edge は、ユニットのルーティングテーブルのサブセットであるユニットの転送テーブルに利用可能な最適ルートをインストールします。パケットは転送テーブルの情報に従って転送されます。

注意

Cloud Edge では IPv6 ルーティングはサポートされません。

ルーティングテーブルを確認する

手順

1. [ネットワーク] > [ルーティング] > [ルーティングテーブル] に移動します。
2. IPv4 ルートを確認します。

ルーティングテーブルのインジケータ

次の表に、ルーティングテーブルインジケータとその説明を示します。

コード	定義
K	カーネルルート
C	接続済み
S	静的

DHCP サービスと DDNS サービスを管理する

Cloud Edge ゲートウェイは、DHCP (Dynamic Host Configuration Protocol) サービスと DDNS (動的 DNS) サービスをサポートします。

DHCP (Dynamic Host Configuration Protocol)

DHCP サービスは、Cloud Edge ゲートウェイの 1 つ以上の LAN インタフェースで有効にすることができます。DHCP サービスが有効になっている各イン

タフェースは DHCP サーバとして機能し、IPv4 アドレスや他のネットワーク設定 (デフォルトゲートウェイや DNS (IPv4) 設定) などを内部クライアントに割り当てます。

また、DHCP サーバごとに詳細なサーバ設定 (IPv4 アドレスの静的マッピングおよび DHCP のリース期間) を指定することもできます。

Cloud Edge は、DHCP サービスを使用するように設定されたインタフェースに対する DHCP 要求に自動的に応答します。

- Cloud Edge On-Premises Console を使用した DHCP サービスの設定については、382 ページの「DHCP サービス設定を変更する」を参照してください。
- Cloud Edge Cloud Console を使用した DHCP サービスの設定については、144 ページの「DHCP 設定を編集する」を参照してください。

DDNS (動的ドメインネームシステム)

DDNS は、インターネットの DNS サーバをリアルタイムに自動更新し、ホスト名、IPv4 アドレス、およびその他の情報のアクティブな DNS 設定を最新の状態に維持します。

DDNS サービスは Cloud Edge ゲートウェイの WAN インタフェースに設定できます。DDNS を設定するには、Cloud Edge Cloud Console を使用する必要があります。詳細については、148 ページの動的 DNS を参照してください。

DHCP サービスおよび設定を表示する

手順

1. [ネットワーク] > [サービス] > [DHCP] に移動します。
2. DHCP サービスに関連付けられたパラメータを確認します。

オプション	説明
名前	DHCP サービスの名前です (例: LAN1)。

オプション	説明
IP アドレス/プレフィックス	インタフェースに割り当てられた IPv4 アドレスとサブネットマスクです。
有効	サービスの状態を示します。有効 (緑/オン) または無効 (赤/オフ) のどちらかになります。
IP プール	DHCP サービスがクライアントにリース可能な IPv4 アドレスの範囲です。
オプション	DNS サーバの IPv4 アドレス、ゲートウェイの IPv4 アドレス、およびリース期間があります。DNS の IPv4 アドレスは、DHCP サーバで指定の DNS を使用する場合にのみ表示されます。
処理	DHCP サービスの設定を編集する場合はアイコンをクリックします。

DHCP サービス設定を変更する

手順

1. 必要に応じて、以下の情報を確認します。
   - 146 ページの「DHCP の配信モード情報」
   - 147 ページの「初期設定の DHCP IP アドレスプール」
2. [ネットワーク] > [サービス] > [DHCP] に移動します。
3. 次のいずれかを実行します。
   - [名前] 列で、変更する DHCP サーバの名前をクリックします。
   - [処理] 列で、変更する DHCP サービスの行にある編集アイコン ( ) をクリックします。
4. DHCP 設定を行います。

   以下の詳細については、147 ページの「初期設定の DHCP IP アドレスプール」を参照してください。
   - DHCP サーバとして設定可能なインタフェースに関する配信モード固有の情報

- どのような IP アドレスが初期設定で各 IP アドレスプールに割り当てられているか。

オプション	説明
有効	サービスを有効にする場合に選択します。
IP アドレス/ネットマスク	インタフェースに割り当てられた IPv4 アドレスとサブネットマスクです。
優先 DNS	優先する DNS 方式を選択します。 • [ネットワーク] > [DNS] で設定されているシステムの DNS を使用する場合は、[システムの DNS 設定を使用する] を選択します。 • インタフェースの IPv4 アドレスを DNS として使用する場合は、[インタフェースの IP アドレスを使用する] を選択します。 • IPv4 アドレスを DNS 設定として手動で設定する場合は、[指定した DNS サーバを使用する] を選択します。
ゲートウェイ	インタフェースの IPv4 アドレスおよびネットマスクの設定に基づいて、DHCP サーバのゲートウェイが自動的に入力されます。必要に応じてゲートウェイの IPv4 アドレスを変更することもできます。
IP アドレスの開始値/終了値	IPv4 アドレスの範囲を指定して、DHCP 設定が適用される IP アドレスプールを作成します。 注意 Cloud Edge では IPv6 アドレスプールはサポートされません。

5. [詳細設定] で詳細を設定します。

オプション	説明
リース期間	[リース期間] で、リースされた IPv4 アドレスおよびネットマスクの有効期限の日時を調整します。 日数、時間数、または分数を指定します。たとえば、時間のみを指定した場合、リースは設定した時間数に制限されます。
静的マッピング	静的マッピングを使用して、静的 IPv4 アドレスを特定の MAC アドレスに手動でバインドできます。

オプション	説明

	[静的マッピング] で、MAC アドレス/IPv4 アドレスマップを指定します。複数のマップを入力できます。例:
	`00:0C:29:A9:69:25 maps to 192.168.2.1`
	`00-FF-8A-B9-5A-49 maps to 192.168.1.1`

6. [適用] をクリックします。
7. [ネットワーク] > [サービス] > [DHCP] で設定が変更されたことを確認します。

管理タスクを実行する

Cloud Edge ゲートウェイの On-Premises Console から次の管理タスクを実行できます。

- 言語設定として日本語、英語、または簡体字中国語のいずれかを選択する
- グローバルシステム設定を行う
  - ホスト名と日時を設定する
  - Cloud Edge On-Premises Console へのユーザのアクセス方法を管理する
  - プロキシを設定する
- Cloud Edge のデバイス設定を管理する
- アップデートを実行する
- デバイスログを表示する
- メンテナンスタスクを実行する
- 診断テストを実行し、ヘルスチェック情報を表示する
- サポートへの問い合わせ方法を確認する

言語設定を切り替える

Cloud Edge On-Premises Console では、日本語および英語をサポートしています。

手順

1. Cloud Edge On-Premises Console の右上にあるドロップダウンリストを展開します。
2. 適切な言語を選択します。

グローバルシステム設定を管理する

Cloud Edge ゲートウェイのグローバルシステム設定 (ホスト名や日時の設定など) を管理することができます。その他の詳細設定には、Cloud Edge On-premises Console のセッションタイムアウトやプロキシ設定があります。

ホスト名と日時を設定する

Cloud Edge On-Premises Console または Cloud Edge ゲートウェイの [クイックセットアップ] 画面を使用して、Cloud Edge ゲートウェイのホスト名と日時を設定することができます。

手順

1. Cloud Edge On-Premises Console にログオンします。
2. 次の処理のいずれかを実行します。

オプション	説明
Cloud Edge On-Premises Console を使用する場合	[管理] > [システム設定] > [一般] タブに移動します。
[クイックセットアップ] 画面を使用する場合	Cloud Edge On-Premises 画面右上の [クイックセットアップ] リンクをクリックし、[システム設定] セクションに移動します。

3. 次の設定を行います。

オプション	説明
ホスト名	ホスト名を指定します。
NTP サーバと同期する	NTP サーバと同期する場合は、このオプションを選択して、[NTP サーバ] フィールドでサーバの IP アドレスを追加します。
時間を手動で設定	時間を手動で設定する場合は、このオプションを選択して、[現地時間] フィールドに現在の時刻を `yyyy-mm-dd hh:mm:ss` の形式で指定します。例: `2015-01-16 13:03:28`
[場所] と [都市]	Cloud Edge ゲートウェイに最も近い場所および都市を選択して、適切なタイムゾーンを設定します。

4. 次の手順を実行します。
   - [一般] タブを使用した場合は、[適用] をクリックします。
   - [クイックセットアップ] 画面を使用した場合は、[設定を保存] をクリックします。

注意

Cloud Edge ゲートウェイが Cloud Edge Cloud Console に登録されていない場合は、ボタンには [保存して登録] と表示されます。

On-Premises Console を設定する

Cloud Edge On-Premises Console の設定には、次のオプションがあります。

- アイドルタイムアウト: 初期設定では、何も操作しない状態が 5 分間続いた場合に、Cloud Edge ゲートウェイによって管理セッションが切断されます。Cloud Edge にログインしている PC が無人の状態になっているときに、Cloud Edge On-Premises Console を他の人が使用するのを防ぐためにも、このアイドルタイムアウトを設定することをお勧めします。アイドルタイムアウトは必要に応じて調整できます。
- 証明書: Cloud Edge On-Premises Console の SSL 証明書を参照して選択できます。

On-Premises Console タイムアウトを設定する

手順

1. [管理] > [システム設定] > [コンソール設定] タブに移動します。
2. [アイドルタイムアウト] で、必要に応じてセッションタイムアウトを設定します。
3. [適用] をクリックします。

On-Premises Console 証明書を設定する

手順

1. [管理] > [システム設定] > [コンソール設定] タブに移動します。
2. [証明書の設定] で、証明書の設定を追加します。
   - SSL 証明書
   - SSL パスワード
3. [適用] をクリックします。

プロキシを設定する

製品アップデート、ライセンスアップデート、Web レピュテーションクエリ、およびクラウドメッセージ検索 (CMS) に HTTP プロキシサーバを使用するように Cloud Edge ゲートウェイを設定できます。

手順

1. [管理] > [システム設定] > [プロキシ設定] タブに移動します。
2. [HTTP プロキシサーバを使用する] チェックボックスをオンにします。
3. HTTP プロキシサーバの IPv4 アドレスとポート番号を指定します。
4. 必要に応じて、サーバで必要なユーザ名とパスワードを指定します。
5. [適用] をクリックします。

デバイス管理

デバイス管理を設定して、Cloud Edge ゲートウェイをリモートで管理および監視することができます。Cloud Edge CLI へのアクセスポイントを設定することもできます。

管理アクセスを管理する

Cloud Edge ゲートウェイの On-Premises Console を使用して、Cloud Edge ゲートウェイのリモートでの管理および監視に使用する特定の種類の管理サービス (On-Premises Console、Ping、SSH、および SNMP) を許可またはブロックするように、このゲートウェイを設定できます。On-Premises Console 管理サービスを有効にすると、承認されたユーザは On-Premises Console へのログオンが可能になります。

必要に応じて、各 L3 インタフェースで各サービスを有効または無効にすることができます。

注意

WAN インタフェースで管理サービスを有効にすることもできますが、セキュリティ的には、Cloud Edge ゲートウェイの背後にあるデバイスからのみ Cloud Edge を管理できるように、内部インタフェースで管理サービスとトラフィックを有効にする必要があります。

SNMP を有効にしたら、[管理] > [デバイス管理] > [SNMP の設定] に移動して SNMP を設定する必要があります。選択したインタフェースで SNMP サポートを有効にして設定すると、ユーザが SNMP マネージャを使用して、サポートされるオブジェクトの情報を取得できるようになります。

ワイヤレスネットワーク機能を備えた Cloud Edge ゲートウェイのメインワイヤレスネットワークまたはゲストワイヤレスネットワークで管理アクセスを有効にすることができます。ゲストワイヤレスネットワークでの管理アクセスを許可する際は、セキュリティの問題に留意する必要があります。

管理アクセスを有効にする

Cloud Edge ゲートウェイは、On-Premises Console、Ping、SSH、および SNMP サービスを使用した管理アクセスをサポートします。管理アクセスを有効にすると、選択したプロトコルを使用したリモートアクセスが可能になります。

Cloud Edge ゲートウェイを登録した後、Cloud Edge Cloud Console を使用して、On-Premises Console、Ping、SSH、または SNMP サービスを使用した管理アクセスを有効または無効にする必要があります。

手順

1. Cloud Edge Cloud Console にログオンします。
2. [ゲートウェイ] > (ゲートウェイ名) > [管理アクセス] に移動します。
3. テーブルの下のフィールドで、ゲートウェイへのリモートアクセスを許可する IPv4 アドレスを指定します。

   IPv6 を使用した管理アクセスはサポートされていません。

   注意

   この設定により、ゲートウェイにリモートでアクセスできる IPv4 アドレス範囲が決まります。単一の IPv4 アドレスがサポートされており、範囲を表すには「-」記号を使用できます。IPv4 アドレスとネットマスクは `192.168.1.1/24` の形式で指定します。指定しない場合は、すべての IPv4 アドレスが許可されます。

4. インタフェースで有効にするサービスを選択します。
   - On-Premises Console

     On-Premises Console サービスでは、Cloud Edge ゲートウェイの On-Premises Console にアクセスできます。
   - Ping
   - SSH
   - SNMP
5. [保存] をクリックします。

次に進む前に

SNMP アクセスを有効にした場合、Cloud Edge の On-Premises Console を使用して SNMP を設定する必要があります。

390 ページの「SNMP の設定を行う」を参照してください。

SNMP の設定を行う

Cloud Edge On-Premises Console を使用して SNMP の設定を行う必要があります。

手順

1. Cloud Edge On-Premises Console にログオンします。
2. [管理] > [デバイス管理] > [SNMP の設定] に移動します。
3. [SNMP を有効にする] チェックボックスをオンにします。
4. SNMP の設定を指定します。

オプション	説明
メールアドレス	連絡先のメールアドレスを指定します。
場所	「China office, IT room」など、連絡先の場所です。
コミュニティ名	Cloud Edge からの情報の取得に必要なコミュニティ文字列を指定します (初期設定: public).

注意

Cloud Edge ゲートウェイの連絡先のメールアドレスと場所の情報は、SNMP マネージャで確認することができます。

SNMP 管理が有効である場合、ユーザは SNMP マネージャを使用してデバイスを管理できます。SNMP マネージャは、指定されたコミュニティ文字列が有効な v2 コミュニティ文字列である場合にのみ、ゲートウェイを管理することができます。

Web シェル

[Web シェル] タブから Cloud Edge コマンドラインインタフェース (CLI) にアクセスして、高度な設定を実行できます。CLI を使用する場合は、設定エラー

が発生しないように、トレンドマイクロのサポート担当者と一緒に作業することをお勧めします。

診断

診断テストを実行し、ヘルスチェックの結果を確認することによって、問題をトラブルシューティングしたり、問題のない、または問題のある Cloud Edge デバイスコンポーネントを特定したりできます。また、診断ファイルを収集およびダウンロードすることもできます。

- パケットの取り込みの実行
- トラフィックの追跡の実行
- ファイルの収集およびダウンロード
- ヘルスチェック情報の確認

ヘルスチェック情報を確認する

On-Premises Console から、ゲートウェイのヘルスチェック情報を確認できます。

手順

1. Cloud Edge On-Premises Console にログオンします。
2. [管理] > [診断] > [ヘルスチェック] に移動します。
3. ゲートウェイのヘルスチェック情報を確認します。含まれる情報は次のとおりです。

セクション	エントリ	説明
ハードウェア情報	シリアル番号	読み取り専用エントリ
	Cloud Edge デバイスの種類	読み取り専用エントリ デバイスの種類は Cloud Edge モデルです。
	Cloud Edge ファームウェアのバージョン	読み取り専用エントリ

セクション	エントリ	説明
システムリソース	CPU の温度	現在のステータスの表示
	システムディスク使用率	
	データディスク使用率	
ネットワークインタフェースステータス	すべてのネットワークインタフェースのリスト	ステータス: アップまたはダウン メインネットワークのステータスが確認できます。 また、ワイヤレスネットワーク機能をサポートする Cloud Edge ゲートウェイのゲストワイヤレスネットワークのステータスも確認できます。
サービス稼働ステータス	自動登録モジュール	ステータス: 実行中またはエラー
	DHCP サービス	ステータス: 実行中、エラー、または無効
	ハートビートモジュール	ステータス: 実行中、エラー、または該当なし
	L2TP VPN サービス	ステータス: 実行中、エラー、無効、または該当なし
	ログアップロードモジュール	ステータス: 実行中またはエラー
	メール検索サービス	ステータス: 実行中またはエラー
	NTP サービス	ステータス: 実行中、エラー、または無効
	検索サービス	ステータス: 実行中またはエラー
	システム監視モジュール	ステータス: 実行中またはエラー

セクション	エントリ	説明
	サイト間 VPN サービス	ステータス: 実行中、エラー、無効、または該当なし
	SSL VPN サービス	ステータス: 実行中、エラー、無効、または該当なし
	ユーザ認証モジュール	ステータス: 実行中またはエラー

ソフトウェアのパッチをロールバックする

手順

1. On-Premises Console で、[管理] > [アップデート] > [ソフトウェアのパッチ] に移動します。
2. ロールバックする適用済みのパッチを選択し、[ロールバック] をクリックします。

出荷時の設定

出荷時の設定に戻すと、Cloud Edge ゲートウェイのネットワーク設定が初期設定にリセットされ、ログおよびデータベース情報がすべて消去されます。

出荷時の設定に戻すのは、次のような場合です。

- Cloud Edge ゲートウェイのハードディスクがいっぱいになった。
- Cloud Edge ゲートウェイを別の場所で使用する。
- Cloud Edge ゲートウェイの使用を中止するため、コンプライアンスに従ってデータを削除する。

出荷時の設定に戻す

警告!

出荷時の設定に戻すと、Cloud Edge ゲートウェイに保存されているログおよびデータベース情報がすべて削除されます。この情報は復元できません。

手順

1. Cloud Edge ゲートウェイの電源を切ります。
2. 背面パネルにあるリセットボタンを押したままにします。

   リセットボタンは、Cloud Edge ゲートウェイ背面の電源スロットと USB ポートの間にあります。
3. Cloud Edge ゲートウェイの電源を再投入します。
4. ゲートウェイの背面パネルにある黄色の LED が点滅を開始したら、リセットボタンを放します。

   黄色の LED が約 2 分間点滅します。Cloud Edge ゲートウェイが出荷時の設定で再起動します。

第 8 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/dcx/s/?language=ja

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/dcx/s/threat?language=ja

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

索引

アルファベット

あ

か

さ

た

な

は

ま

や

ら

わ