2023年11月9日リリース
Mist 新機能のご紹介

ジュニパーネットワークス株式会社

JUNIPer driven by Mist AI

はじめに

❖ 本ドキュメントは以下のリリースノートを抄訳したものです

https://www.mist.com/documentation/november-9th-2023-updates/

本ドキュメントは2023年11月時点のMist cloudのGUIを使用しております

❖ 実際の画面と表示が異なる場合がございます

❖ 内容について不明な点、ご質問等がございましたら担当営業までお問い合わせください

本リリースで追加された機能一覧（1/2）

Marvis

- Microsoft Teamsの統合
- サポートチケット作成ページでのMarvisを用いたトラブルシューティング

Wireless Assurance

- WPA3パーソナルでのマルチパスフレーズ設定
- ダイナミックVLAN設定のVLAN Type Nameの変更
- 禁止クライアント機能の変更
- APリストページでのファームウェアアップグレードの推奨メッセージの表示

Wired Assurance

- Virtual Chassis機能の拡張
- スイッチ設定の一括アップロード
- ポートミラーリング
- ポート選択ページの改良
- DNS、NTP、RADIUS設定でのサイト変数のサポート
- 接続成功SLE（Successful Connect SLE）配下への新規分類の追加

本リリースで追加された機能一覧（2/2）

WAN Assurance

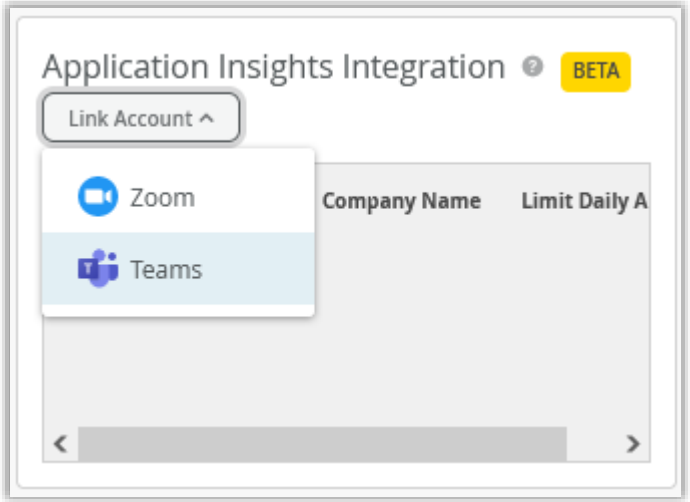
- ジュニパーセキュアエッジトンネルの自動プロビジョニング（SASE）
- IDPバイパスプロファイル
- ハブプロファイル内でのハブグループ設定
- ハブ・スポーク間トラフィックステアリング
- ネットワークページへの新規BGPオプションの追加
- BGPで学習したプレフィックスへのオーバレイトラフィックステアリング
- URLサブカテゴリによるトラフィック拒否
- フロントパネルでのLTEインタフェース表示
- DHCPクライアント情報の表示内容の追加

MIST Edge

- RADIUSプロキシ機能でのCoAのサポート

Marvis

Microsoft Teamsの統合

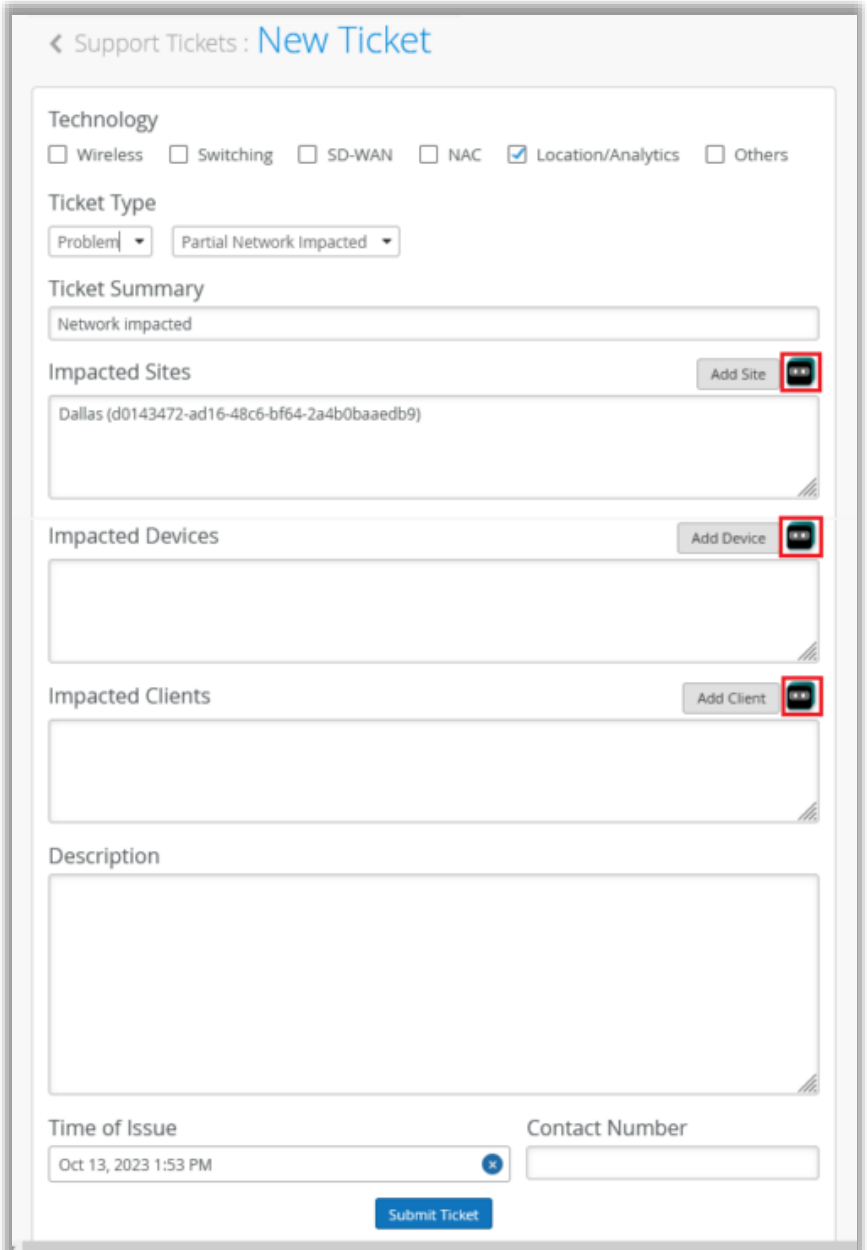


- Microsoft TeamsをMistに統合することにより、Teamsコールのインサイトを Mistで確認できるようになりました
- MistはMicrosoft Azureクラウドから Teamsコールに関する情報を収集し、 有線、無線、WANネットワークのインサイトと関連付けます
- 関連付けられたTeamsのインサイトはサイトとクライアントレベルのインサイトにて表示されます（Monitor > Service Levels）
- Mist の Organization に Teams アカウントを連携するには、Organization > Settingsページ内のLink Accountオプションで設定します（左図）

- Marvis対話型アシスタントでTeamsコールに関する調査やトラブルシューティングが可能です
- Marvis対話型アシスタントでは以下のような調査が可能です
  - Teamsコールをリストアップ
  - 問題のあったTeamsコールをリストアップ
  - クライアントMACアドレス、ホスト名、サイト情報を用いたTeamsのトラブルシューティング（過去7日間に発生したもの）

留意点：現在は当該機能はベータ版のトライアルとなります。

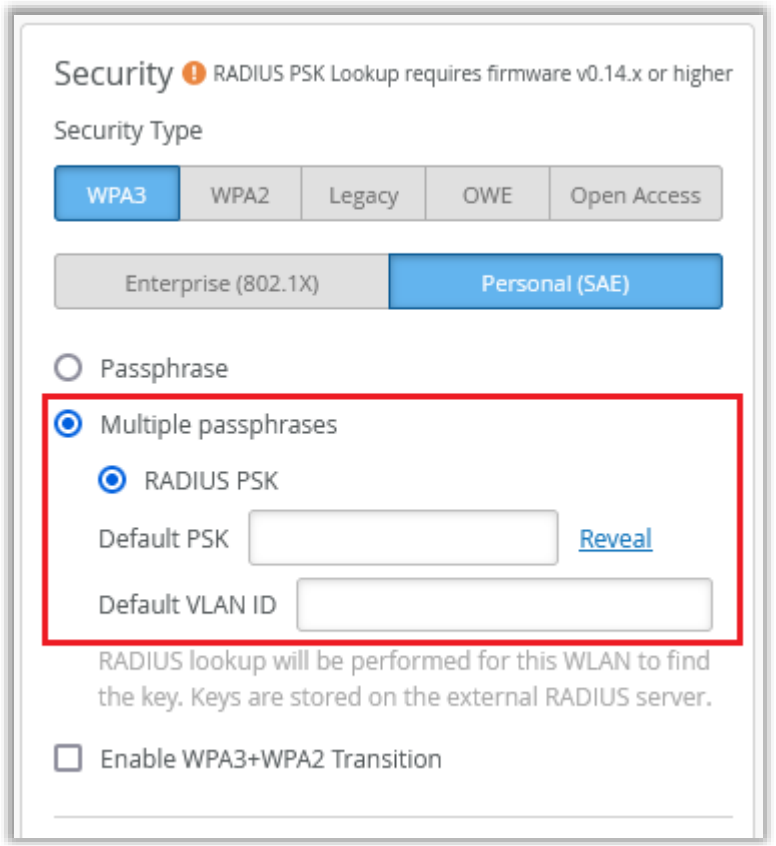
サポートチケット作成ページでのMarvisを用いたトラブルシューティング



- サポートチケット作成ページで簡単なトラブルシューティングを実行するオプションが追加されました
- ヘルプ（「？」）メニューからアクセスできるサポートチケット作成ページ内の以下の項目に対してMarvis起動ボタンが追加されました（左図）
  - Impacted Sites（影響を受けたサイト）
  - Impacted Devices（影響を受けたデバイス）
  - Impacted Clients（影響を受けたクライアント）
- トラブルシューティングを実施するには、Marvisボタンをクリックし、トラブルシューティングしたい項目を選択します（サイト、デバイス、クライアント）
- 本機能を使用するにはMarvisサブスクリプションが必要です

Wireless Assurance

WPA3パーソナルでのマルチパスフレーズ設定



- RADIUSルックアップ（RADIUS PSK）を用いたWPA3パーソナルでのマルチパスフレーズ機能が追加されました
- WPA2 RADIUS PSKと同じRADIUS AVPが使用されます
- MACアドレスベースのルックアップのみサポートしています（MACアドレス無しは未サポートです）

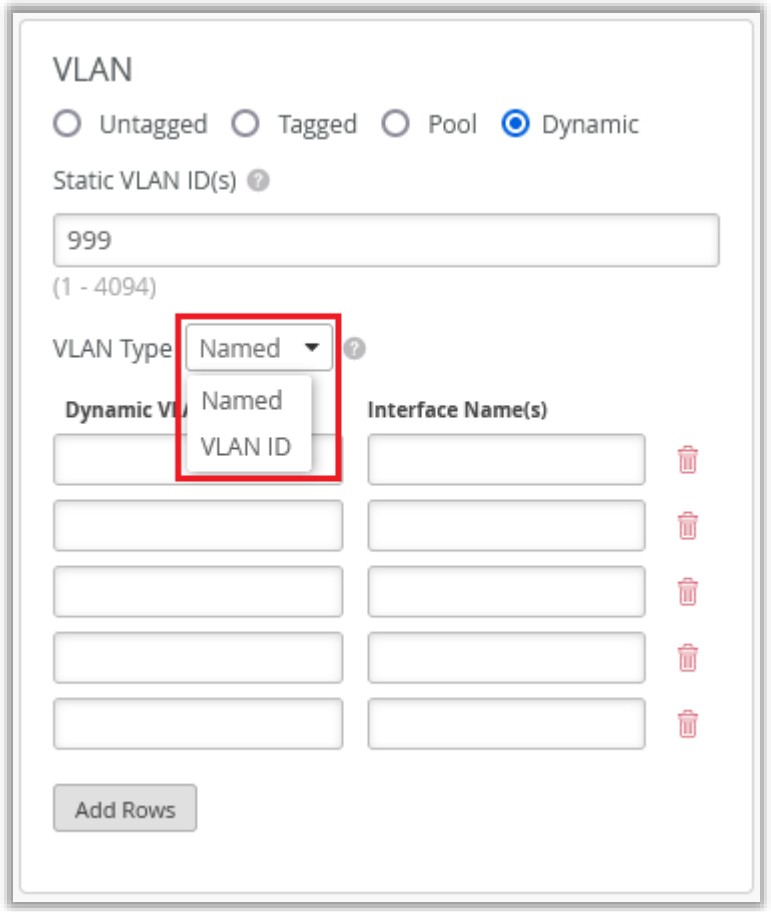
RADIUS PSKで用いるRADIUS AVP：

属性名	ベンダID	属性番号	属性フォーマット	フォーマット
Cisco-AVPair	9	1	String	psk-mode=ascii & psk=<passphrase>

- Site ＞ WLANs ＞ WLAN名ページのセキュリティ項目にて設定します（左図）
- RADIUSの設定項目でRADIUSサーバを設定する必要があります
- WPA3+WPA2 Transitionモード（移行モード）をサポートしています
- 802.11r Fast Roamingをサポートしています

- 本機能を使用するにはAPのファームウェアが0.14以上である必要があります

ダイナミックVLAN設定のVLAN Type Nameの変更



- WLANページ（Site ＞ WLANs ＞ WLAN名）内のダイナミックVLAN設定に記載されているVLAN Type名を以下のように変更しました（左図）

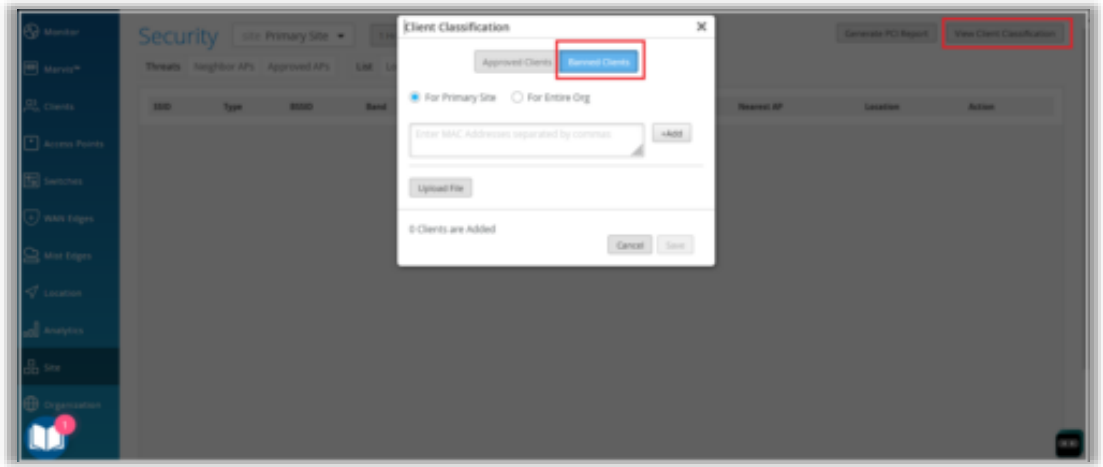
変更前	変更後
Airespace (airespace-interface-name)	Named
Standard (Tunnel-Private-Group-ID)	VLAN ID

- ダイナミックVLAN設定画面の設定項目名（ラベル）も以下のように変更しています

変更前	変更後
Static VLAN ID	Static VLAN ID(s)
Dynamic VLAN ID	Dynamic VLAN ID(s)

- Named VLAN は Airespace-Interface-Name または Tunnel-Private-Group-IDのRADIUS属性をサポートし、1つのVLAN、VLANプール、または変数で指定することが可能です
- VLAN IDはTunnel-Private-Group-IDのRADIUS属性をサポートし、1つのVLAN、VLAN範囲、または変数で指定することが可能です

禁止クライアント機能の変更

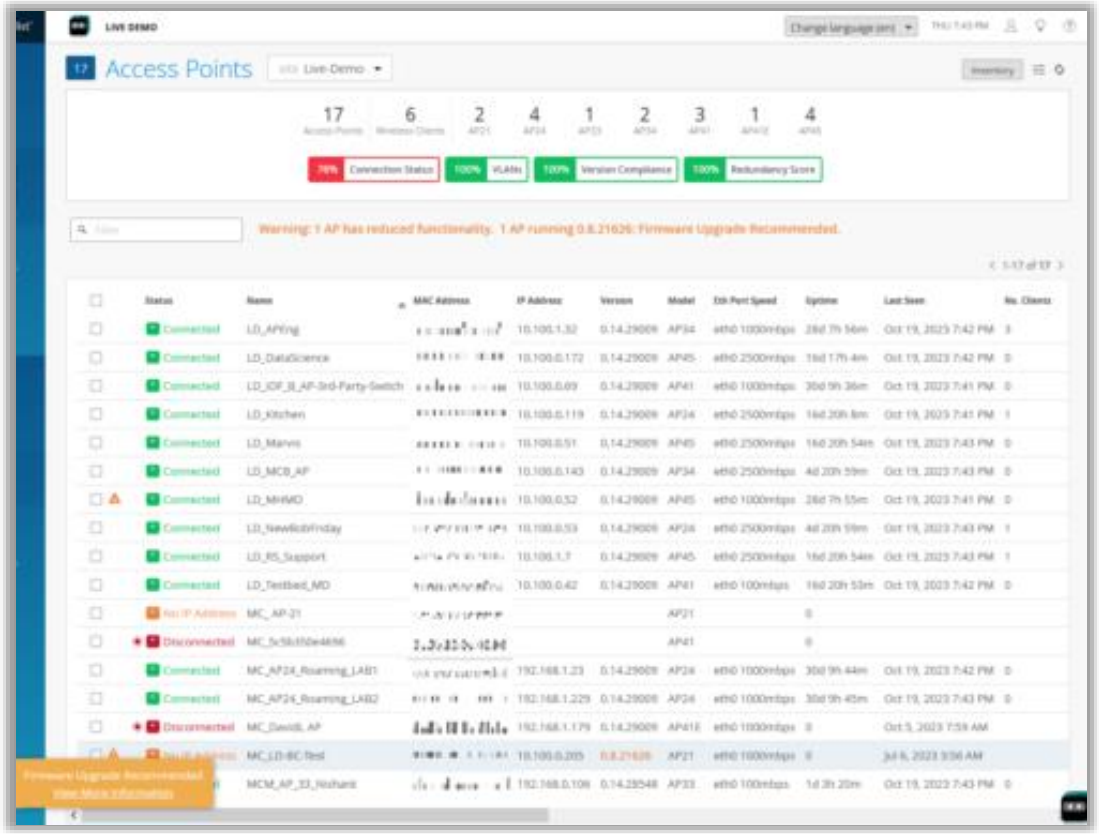


- クライアントの認証後、クラウドを用いて禁止するクライアントを判断していましたが、認証前にAPがローカルでクライアントを禁止できるようになりました（禁止クライアント数が512以下の場合）
- クライアントを認証することなく、クライアントを即時禁止にすることが可能になります
- 禁止クライアントリスト内のクライアント数が512以下の場合に、クラウドアシスト無しでAPがローカルでクライアントを認証前に禁止することができるようになります
- クライアントを禁止リストに追加するにはSite ＞ Securityページ内のView Client Classificationウィンドウを用います（左図）
- WLANの設定内で「Prevent banned clients from associating」の項目のチェックボックスもチェックください

- 本機能を使用するにはAPのファームウェアが0.14以上である必要があります
- ファームウェアのバージョンと禁止クライアント数の組み合わせによる禁止クライアント機能の挙動の違いは以下となります

APファームウェアバージョン	禁止クライアント数	挙動
0.14以上	512以下	APのローカル禁止リストが使用されます
0.14以上	513以上	クラウドでのルックアップが実行され、認証成功後に禁止となります
0.12以前	条件なし	クラウドでのルックアップが実行され、認証成功後に禁止となります

APリストページでのファームウェアアップグレードの推奨メッセージの表示



- APの一覧ページで、古いバージョンのファームウェアが動作しているAPに対して、ファーム ウェアのアップグレードを推奨するメッセージが表示されるようになりました
- メッセージはアクセス権限がSuper Userとしてログインしている際に表示されます
- メッセージはAP一覧ページの上部にバナーテキストとして表示されるか、APステータス列に表示される警告アイコンにマウスを重ねた場合に表示されます（左図）
- 警告アイコンにマウスを重ねた場合に表示されたメッセージには、ファームウェアアップグレードに関する追加のドキュメントへのハイパーリンクも表示されます
- 詳細はファームウェアリリースノートページをご覧ください。

  https://www.mist.com/documentation/firmware

Wired Assurance

Virtual Chassis機能の拡張

- Virtual Chassisに新しいメンバーを追加したり、 Virtual Chassis内の既存のメンバの番号を変更またはメンバーを置き換えたりできるようになりました
- スイッチの詳細ページにある「Modify Virtual Chassis」項目で変更が可能です（左図）
- 「Modify Virtual Chassis」項目は、 スイッチリスト（Switchesページ）の Utilitiesメニューにあ るEdit Virtual Chassisオプションに代わるものとなります
- 「Modify Virtual Chassis」項目はスイッチの設定がMistにより管理されている場合のみ使用できます
- 設定に使用するワークフローでは、Virtual Chassis内のすべてのメンバーの役割とシリアル番号を指定するJunosのプリプロビジョニング方式を利用します
- プリプロビジョニングに関しましては以下のドキュメントをご参照ください

  https://www.juniper.net/documentation/us/en/software/junos/virtual-chassis-ex-4200-4500/topics/example/virtual-chassis-ex4200-preprovisioning.html

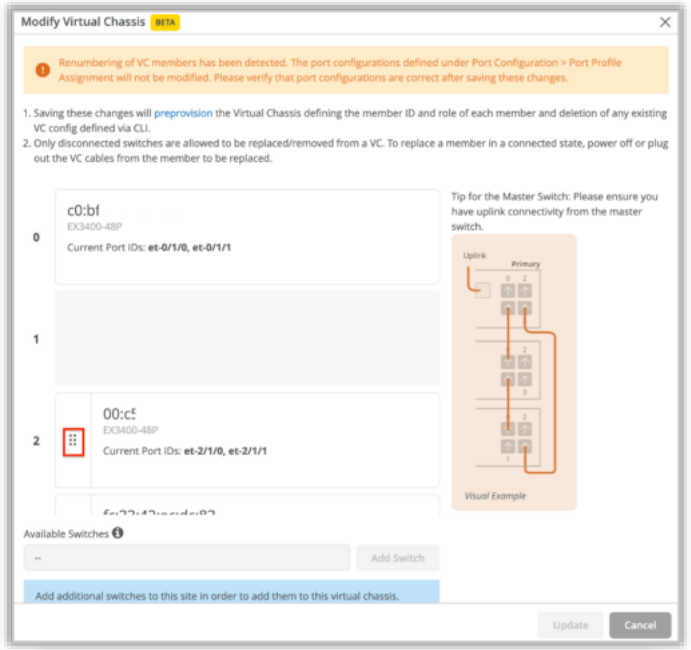
- 各ワークフローに関しましては次ページをご覧ください

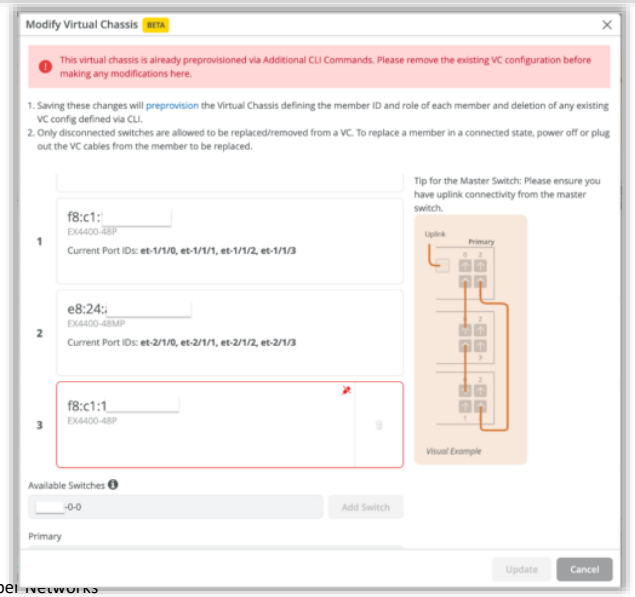
Virtual Chassis機能の拡張（続き）

- Virtual Chassis形成ワークフロー
  - このワークフローは変わりませんが、クラウドを介して形成される新規Virtual Chassisに関しては、全てプリプロビジョニングされます
  - スイッチ一覧ページの「Form Virtual Chassis」オプションを使用した Mistクラウド上でのVirtual Chassis形成は、次の3つの機種のみに適用されます
    - EX2300
    - EX4650
    - QFX5120
  - 上記以外のEXシリーズ、QFXシリーズのスイッチの場合、 専用VCポートを2台以上のメンバー間で接続すると、自動的にVirtual Chassisが形成されます

- Virtual Chassis変更ワークフローは次ページをご覧ください

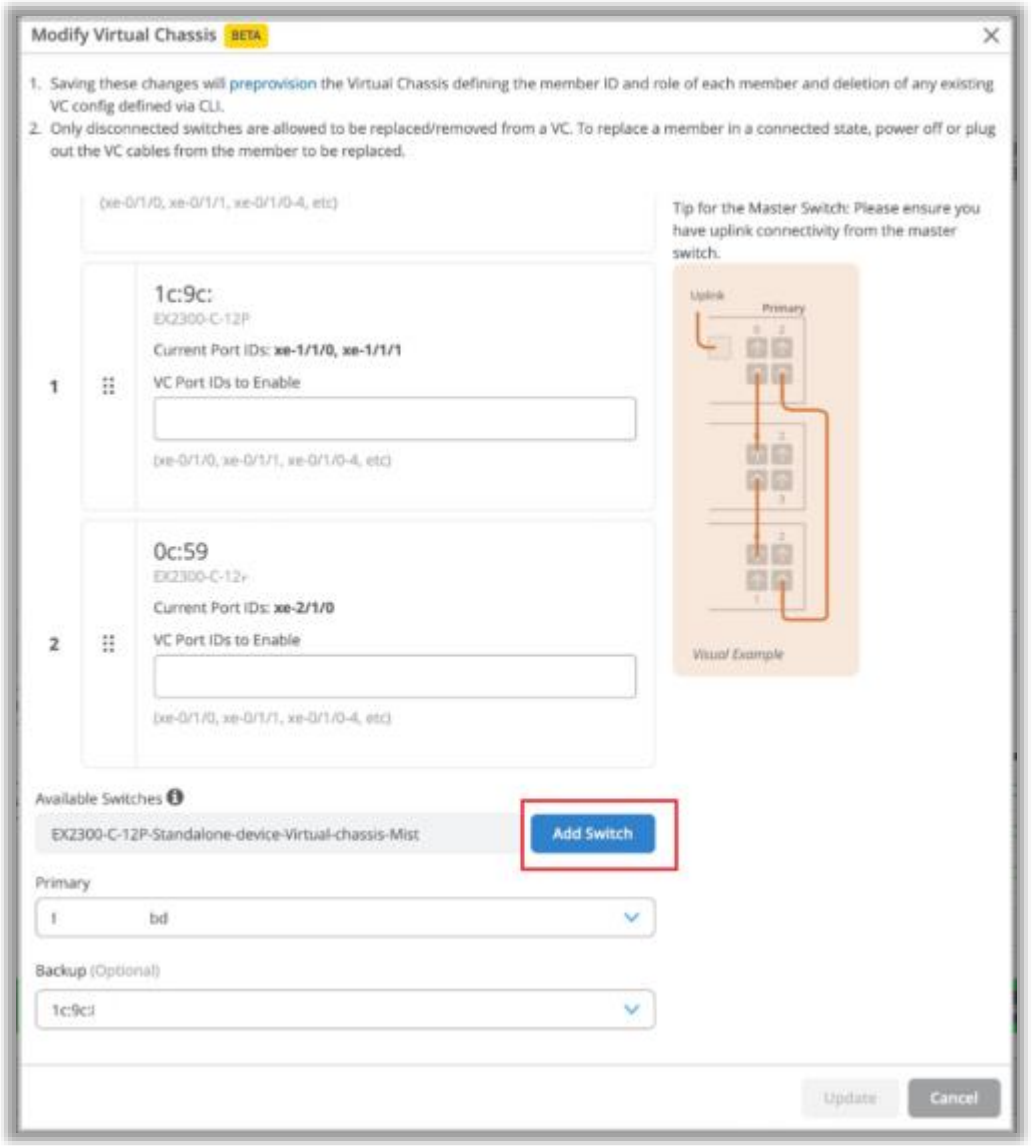
Virtual Chassis機能の拡張（続き）





- Virtual Chassis変更ワークフロー
  - このフローはVirtual Chassisをサポートするすべての EXシリーズ、QFXシリーズのスイッチで適用されます
  - 拡張された機能は以下のとおりです
    - Virtual Chassis内のメンバーの番号の変更（左上図）
      - スイッチのポートパネルを動かすことにより、メンバーの順番を変更することができます
      - 順番は昇順です（最初は0、次は1、と続きます）
      - FPC0を指定する必要があります
    - メンバーの役割の変更
      - メンバーの役割をプライマリ、またはバックアップルーティングエンジンに変更できます
      - その他のメンバーはラインカードメンバーとなります
    - プライマリ、バックアップ、ラインカードメンバーの削除（左下図）
      - Virtual Chassisから切断されたメンバーを削除できます
      - 削除するにはゴミ箱アイコンをクリックします

Virtual Chassis機能の拡張（続き）



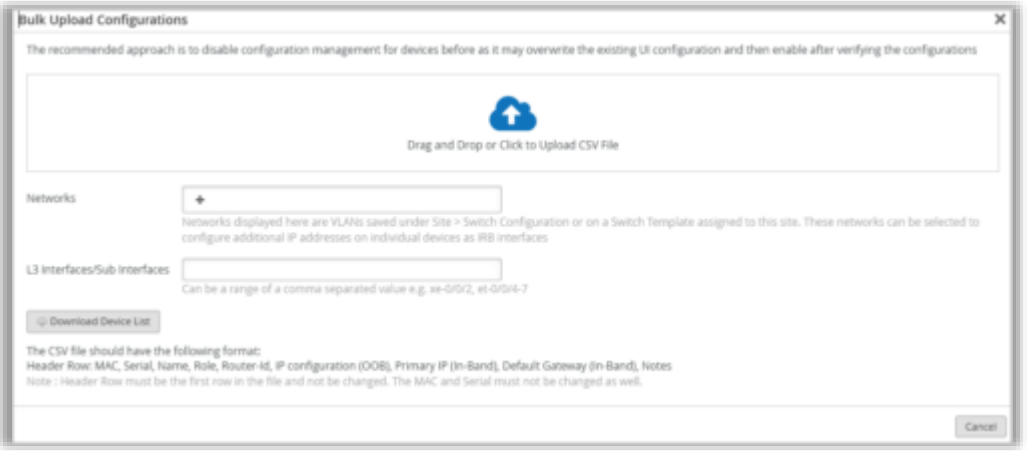
- メンバーの交換
  - 切断されたVirtual Chassisのメンバーを他の機器に交換することができます
  - メンバーを削除し、新しいスイッチを追加します
- メンバーの追加
  - 「Add Switch」をクリックすることにより、新しいメンバーをVirtual Chassisに追加することができます（左図）
  - 機器を追加するにあたり、以下を事前にご確認ください
    - 追加するスイッチがVirtual Chassisの他のメンバーと同じモデルであること
    - 追加するスイッチで起動しているJunosバージョンが他のメンバーで起動しているJunosバージョンと同じであること
    - 追加するスイッチがネットワークに接続されていること
    - 追加するスイッチが同じサイトに登録されていること

- Virtual Chassisの注意事項に関しまして次ページをご覧ください

Virtual Chassis機能の拡張（続き）

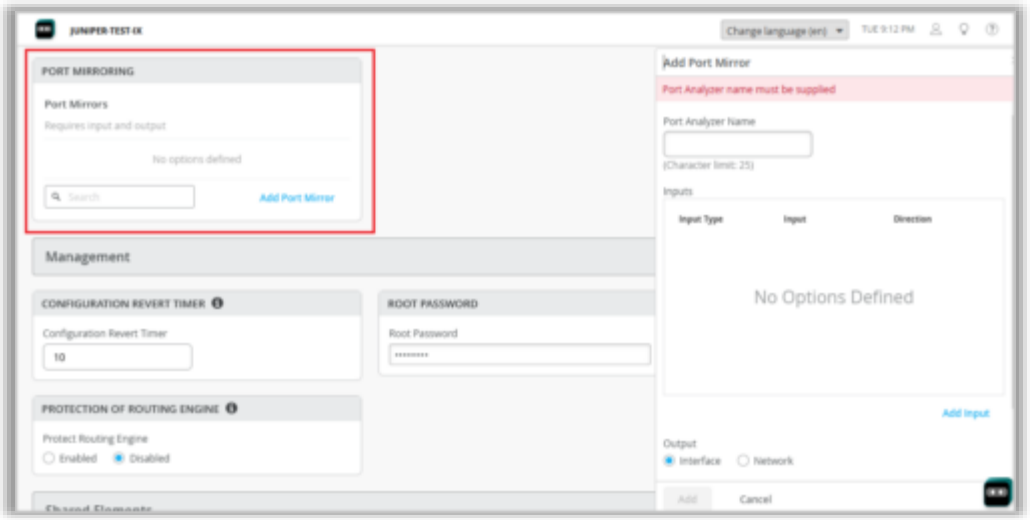
- 注意事項
  - FPC0はMistクラウドに接続するためのデバイス識別子のため、Virtual Chassis内では、FPC0が切断されていない限り、FPC0の番号の変更、移動、削除はできません
  - FPC0を削除した場合、Virtual Chassis内の他のメンバーにFPC0を置き換えます
    - FPC0削除中は新しいメンバーを追加することはできません
  - CLIによるコマンドが優先されてしまうため、Virtual Chassisを変更する前に、Virtual Chassisに関連する追加のCLIコマンドを削除する必要があります
  - 以下の条件を満たした場合に、「Add Switch」のドロップダウンリストにスイッチが表示されます
    - スイッチが同じサイトにいること
      - Virtual Chassis専用ポートを持つスイッチモデルは状態が接続、切断のいづれでも構いません
      - EX2300、EX4650、QFX5120の場合はメンバーは接続の状態である必要があります
    - スイッチが同じモデルであること
    - スイッチの設定がMistで管理されていること
    - スイッチが他のVirtual Chassisのメンバーになっていないこと
    - スイッチがVirtual Chassis内メンバーと同じJunosバージョンを使用していること
  - 設定管理（Configuration Management）が無効となっている場合は「Modify Virtual Chassis」ボタンも無効となっています
  - ユーザの権限がSuper UserかNetowrk Adminsの場合に「Modify Virtual Chassis」ボタンが有効となります

スイッチ設定の一括アップロード



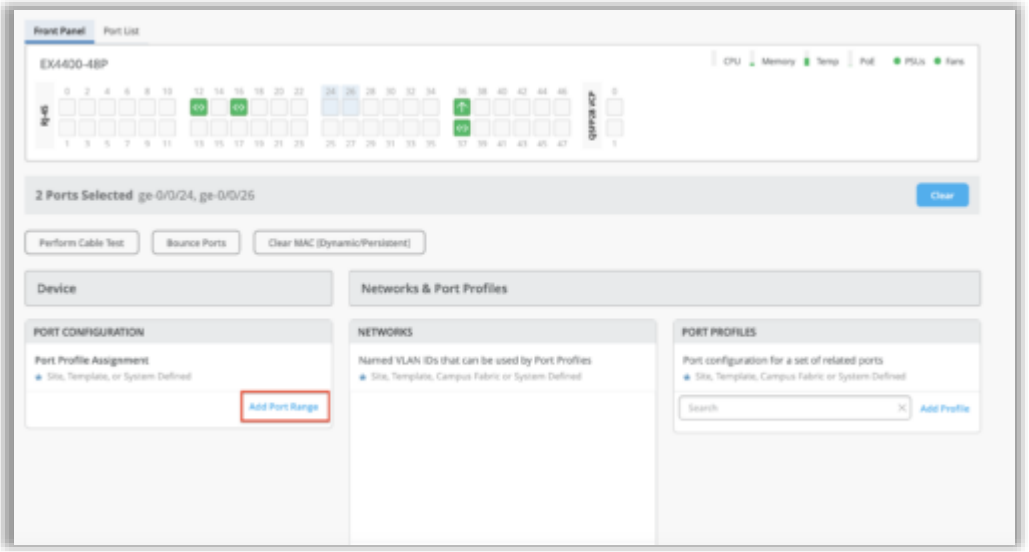
- CSVファイルを用いて以下のスイッチの設定をインポートすることができます
  - MACアドレス
  - シリアル番号
  - スイッチ名
  - スイッチの役割
  - ルータID
  - 管理IPの設定（OOB）
  - プライマリIP（In-Band）
  - デフォルトゲートウェイ（In-Band）
- スイッチの一覧ページで設定をインポートすることができます
- 設定が必要なスイッチを選択し、「Bulk Upload Configuration」ボタンをクリックします
- 「Bulk Upload Configurations」ウィンドウには、インポートを実行するために必要なガイドラインが表示されます（左図）
- 「Bulk Upload Configurations」ウィンドウからサンプルのCSVファイルをダウンロードし、ガイドラインに従って必要な情報で更新し、ファイルをアップロードして戻すことができます
- 「Bulk Upload Configurations」ウィンドウでネットワーク、またはL3インタフェースを指定すると、指定したネットワークやインタフェースが設定できます
- IRBインタフェースとして個々の機器にIPアドレスを設定したい場合はネットワークを指定します
- CSVファイル内のヘッダフィールド、MACアドレス、シリアル番号は変更しないでください

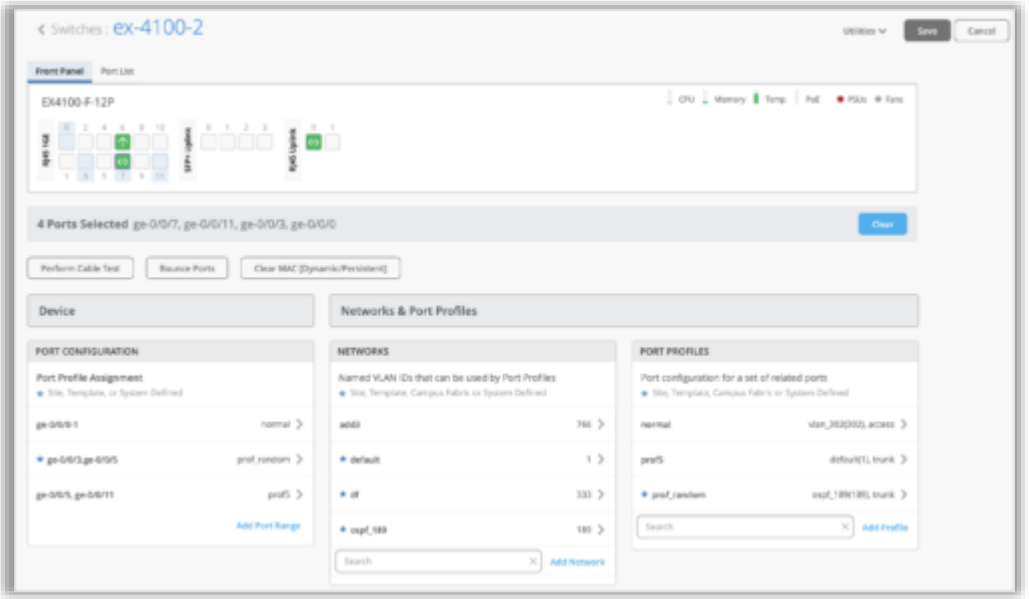
ポートミラーリング



- Organizationレベル（Organization > Switch Templates）、サイトレベル（Site > Switch Configuration）、機器レベルで、スイッチにポートミラーリングを設定できるようになりました（左図）
- ポートミラーリングの設定では、以下を指定します
  - Input
    - トラフィックをモニタリングする入力元（インタフェース、またはネットワーク）を指定します
    - 入力元と共に、モニタリングしたいトラフィックが受信トラフィックなのか、送信トラフィックなのかを指定します
    - 受信トラフィック、送受信トラフィックを共にモニタリングしたい場合は同じインタフェースに対し、2つの入力エントリーを作成し、それぞれのエントリーに受信フラグ、送信フラグを割り当てます
  - Output
    - ミラーリングしたトラフィックの出力先を指定します
    - InputとOutputを同じインタフェースやネットワークにすることはできません

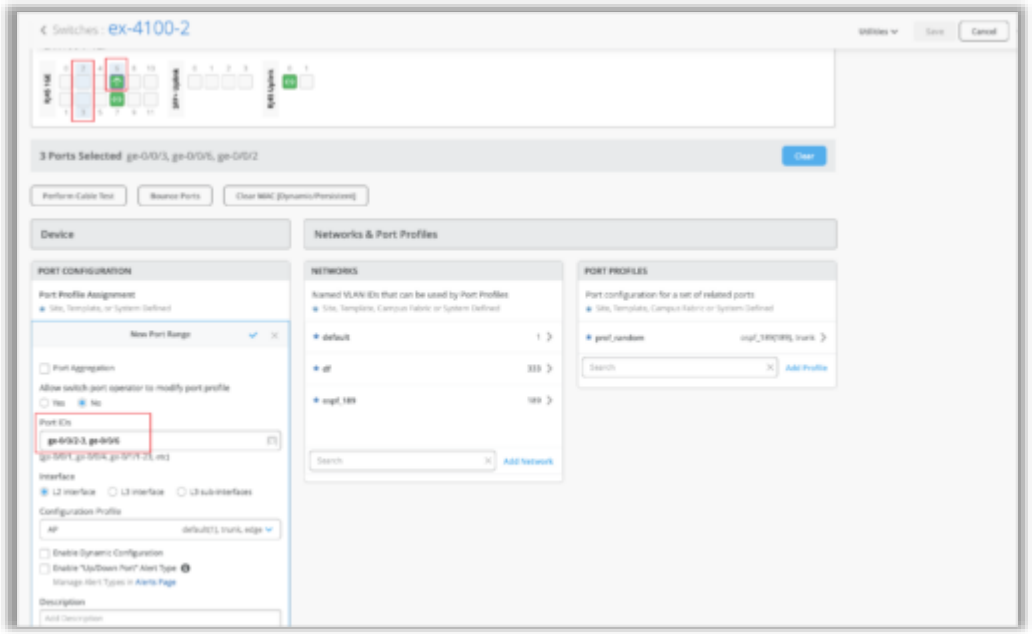
ポート選択ページの改良





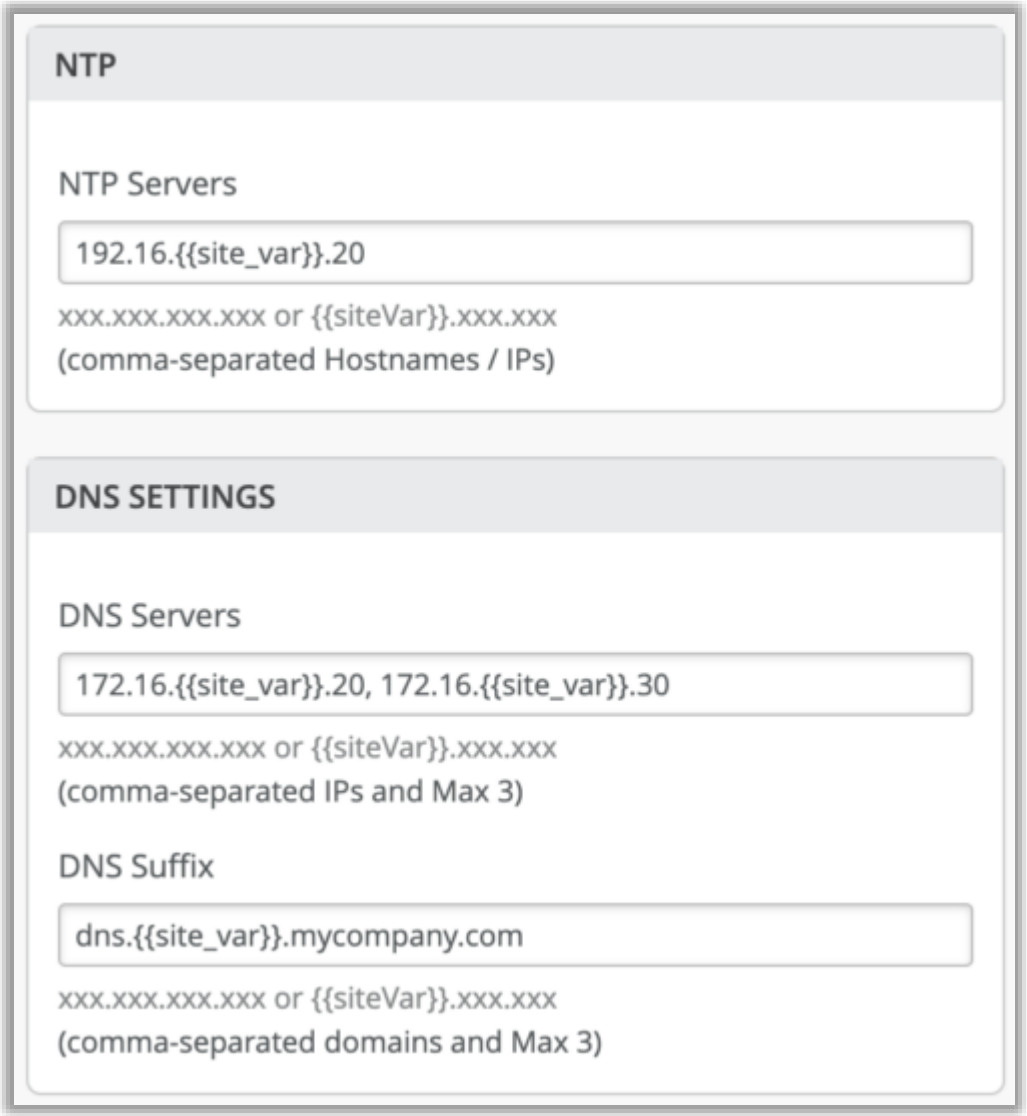
- Switchの詳細ページにおいて、ポートアクションの一括処理機能を以下のように改良しました
  - 「Edit Port Configuration」ポートアクションがPort Configuration項目の「Add Port Range」に置き換えられました（左上図）
    - この新しい実装は元のスイッチの詳細ページにある「Add Port Range」と一致しています
  - フロントパネルビューから複数のポートを選択した場合に、選択したポートに適切なPort Configuration、Networks、Port Profileの項目を表示します（左下図）
    - 選択したポートに設定が無い場合、 Port Configuration、Networks、Port Profileの項目はデータなしで表示されます
  - フロントパネルビューから1つのポートを選択すると、設定ページでは、 Port Configuration、Networks、Port Profileの項目に加えて、ポート統計と有線クライアントのインサイトが表示されます

ポート選択ページの改良（続き）



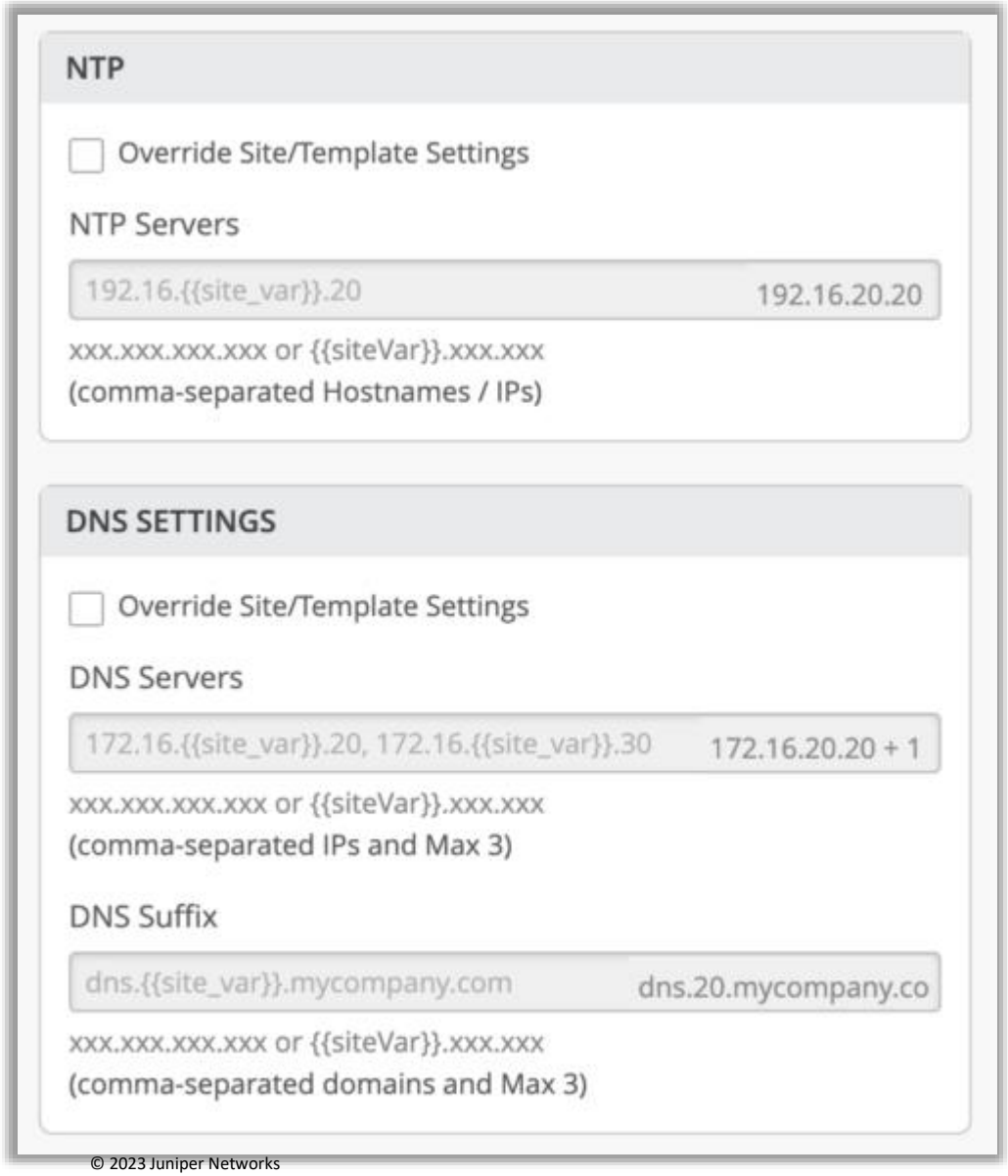
- Port Configuration項目内の「Add Port Range」オプションを用いてポート範囲を追加すると、New Port RangeウィンドウのPort IDsフィールドにフロントパネルビューで選択したポートが事前に入力されます

DNS、NTP、RADIUS設定でのサイト変数のサポート



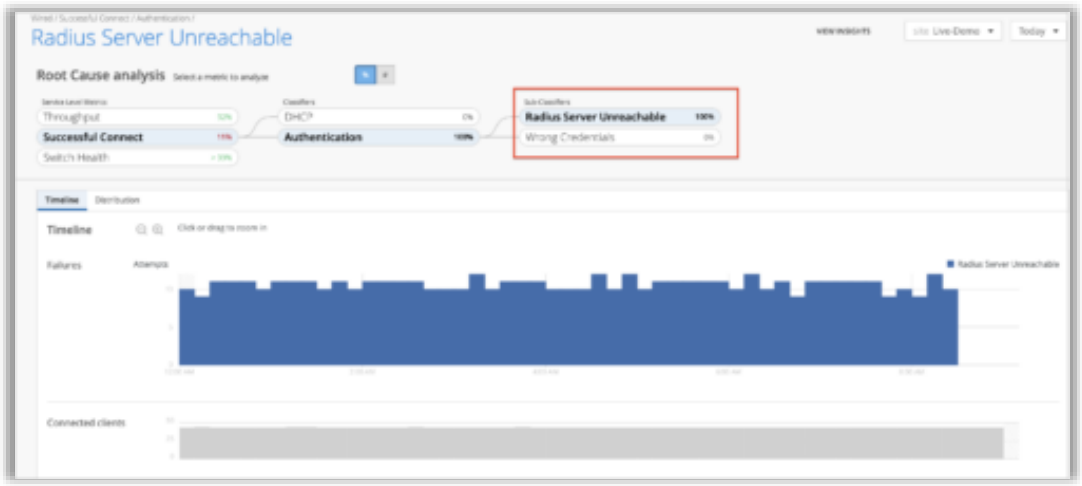
- Organizationレベルのスイッチテンプレートで DNSの設定（サーバ、DNSサフィックス）、NTP、RADIUSサーバをサイト変数として設定できるようになりました（左図）
- サイト変数を使用することにより異なるサイトで異なる値を設定できるようになります

DNS、NTP、RADIUS設定でのサイト変数のサポート（続き）



- 各サイトには対応する値が設定されているため、サイト変数は各デバイスで値に変換されます（左図）

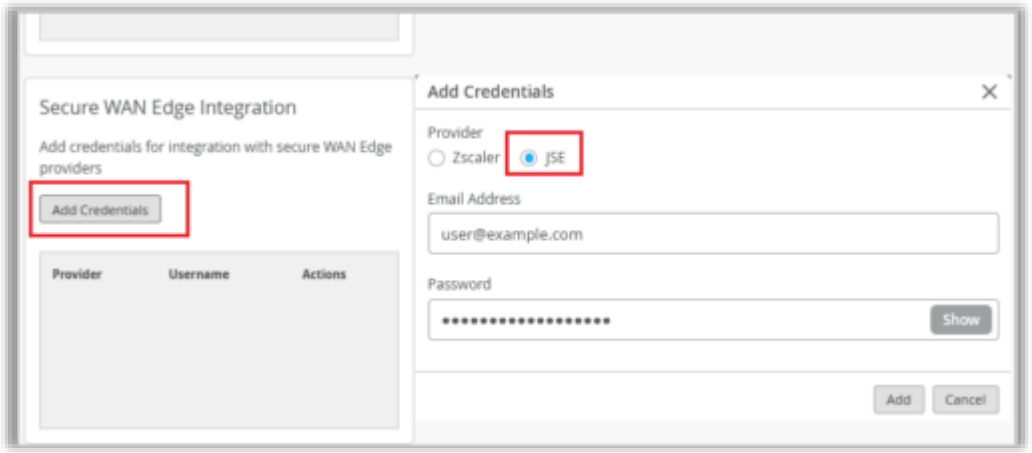
接続成功SLE（Successful Connect SLE）配下への新規分類の追加

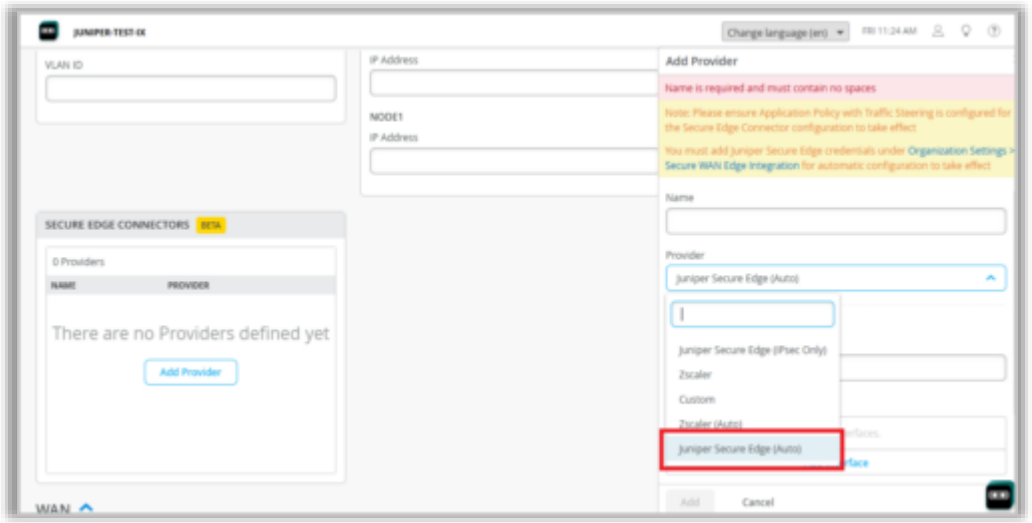


- Wired SLEのSuccessful Connectメトリックに以下の2つの新しい分類を追加しました（左図）
  - Radius Server Unreachable
    - 有線ポートの認証要求を処理するRADIUSサーバがスイッチ（NAS）に対して応答しない場合、認証リクエストの失敗によってユーザが影響を受けたものとして、失敗ユーザ分をカウントします
    - この分類ではRADIUSサーバの到達不能を報告しているスイッチも表示されます
  - Wrong Credentials
    - 認証情報（ユーザー名、またはパスワード）が正しくないために有線クライアントがネットワークへの接続に失敗した場合となります
    - スイッチがRADIUSサーバから収集したデータから問題を判断します

WAN Assurance

ジュニパーセキュアエッジトンネルの自動プロビジョニング（SASE）





- ジュニパーセキュアエッジトンネル（JSEトンネル）の自動プロビジョニング機能が追加されました
- MistとJSEを併用することにより、スポーク、またはハブのLAN側から送信されたトラフィックのどの部分を、インターネットへ転送許可を出す前に検査する必要があるかを判断することができます
- JSE自動プロビジョニングには以下の手順を実施します
  1. WANエッジプロバイダ（JSE）とMistを連携させるために必要なユーザ認証情報（メールアドレスとパスワード）をMistのOrganizationに入力します（左上図）

     Organization > SettingsページのSecure WAN Edge Integration項目内でユーザ認証情報を設定します

     留意点：

     ユーザ認証情報はジュニパーセキュアエッジポータルで作成された情報である必要があります
  2. Organization > WAN Edge Templatesページ内にあるWAN Edgeテンプレートの Secure Edge Connector項目内で、Juniper Secure Edge (Auto) オプションを有効にしたJSEプロバイダを設定します（左下図）

     留意点：

     SRXシリーズはProvider Profileで複数のプライマリおよびセカンダリWANインターフェイスをサポートしません

     SRXシリーズはProvider Profileで1つのプライマリWANインタフェースと1つのセカンダリWANインタフェースをサポートします

ジュニパーセキュアエッジトンネルの自動プロビジョニング（SASE）（続き）

3. SECURE EDGE CONNECTOR AUTO PROVISION SETTINGSのNumber of Users項目に、JSEトンネルでサポートしている最大のユーザ数を入力します
    - このオプションはステップ2のようにJSEプロバイダを設定した場合に使用できます

- Juniper Secure Edge (Auto) オプションが有効なWANテンプレートをサイトに割り当てると、関連するJSEサイト（ロケーションオブジェクト）が自動的に作成され、デバイスから最も近いネットワークPOP（Point of Presence）へのトンネルが確立されます
- Secure Edge Connectorの設定を有効にするには、Mist Secure Edge Connector・ジュニパーセキュアエッジ間のトラフィックステアリングを含むアプリケーションポリシーを作成する必要があります
- 詳細に関しましては、以下のドキュメントをご覧ください

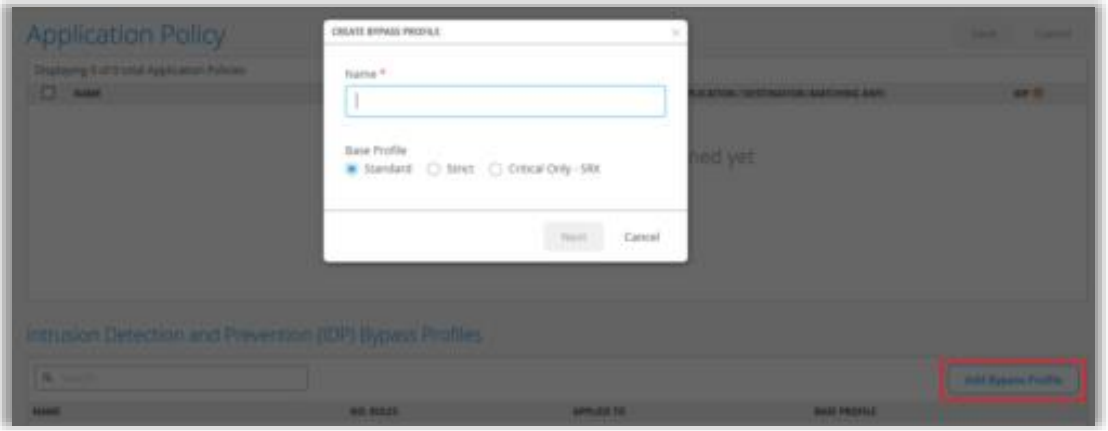
  IDP-Based Threat Detection for SRX Series Firewalls

  https://www.juniper.net/documentation/us/en/software/mist/mist-wan/topics/task/srx-idp-based-threat-detection.html

  IDP-Based Threat Detection on Session Smart Routers

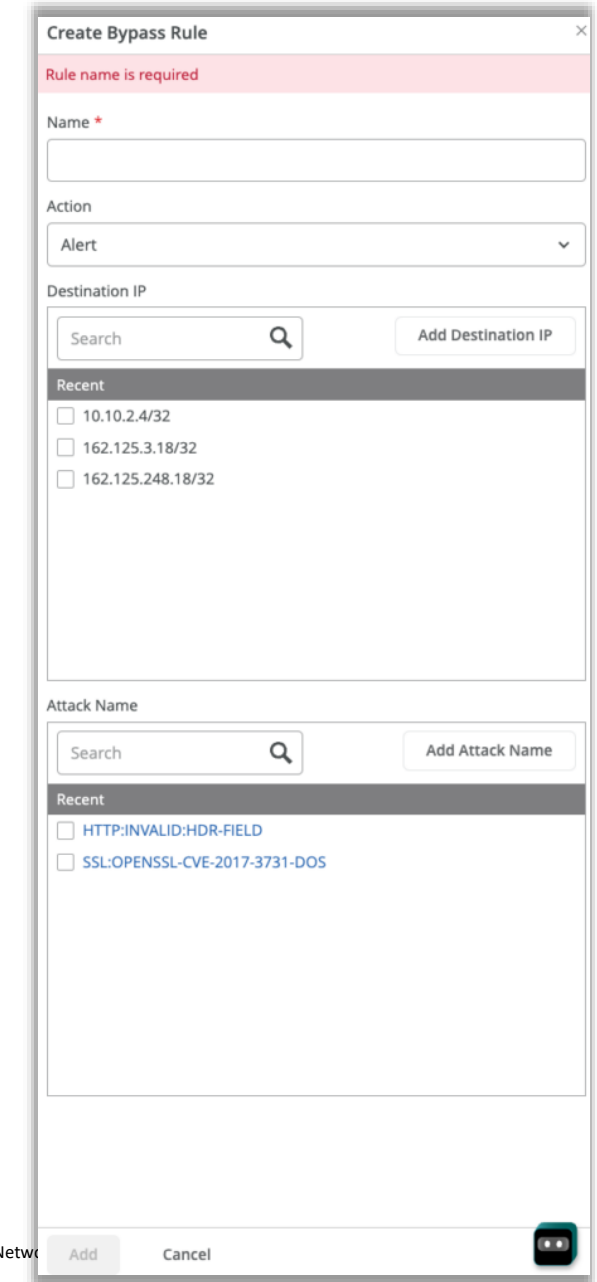
  https://www.juniper.net/documentation/us/en/software/mist/mist-wan/topics/task/ssr-idp-based-threat-detection.html

IDPバイパスプロファイル



- バイパスプロファイルを設定することにより、侵入検知防御（IDP）プロファイルに例外を追加できるようになりました（左図）
- IDPプロファイルは複数のバイパスプロファイルを持つことができ、各プロファイルで複数のバイパスルールを設定することができます
- 以下の種類のIDPプロファイルでバイパスプロファイルを追加することができます
  - Standard
    - Standardプロファイルはデフォルトのプロファイルとなり、ジュニパーが推奨するIDPシグネチャとルールのセットです
    - 各攻撃タイプと重大度には、Juniper定義の設定不可能なアクションが定義されており、IDPエンジンは攻撃を検出したときにこれを実行します
    - 可能なアクションは以下となります
      - クライアントとサーバのTCP接続を遮断
      - 検知時点とそれ以降のパケットを廃棄
      - アラートの送信（追加のアクションは無し）
  - Strict
    - Standardプロファイルと類似したIDPシグネチャとルールのセットが含まれています
    - システムが攻撃を検出すると、このプロファイルはネットワーク上で検出された悪意のあるトラフィックやその他の攻撃を積極的にブロックします
  - Critical（SRXシリーズデバイスにのみ適用可能）
    - クリティカルな攻撃シグネチャを検出し、推奨されるアクションを実行します
    - SRX3000シリーズのファイアウォールには「Critical - Only SRX」を推奨しています

IDPバイパスプロファイル（続き）



- プロファイルの詳細については以下のドキュメントをご覧ください

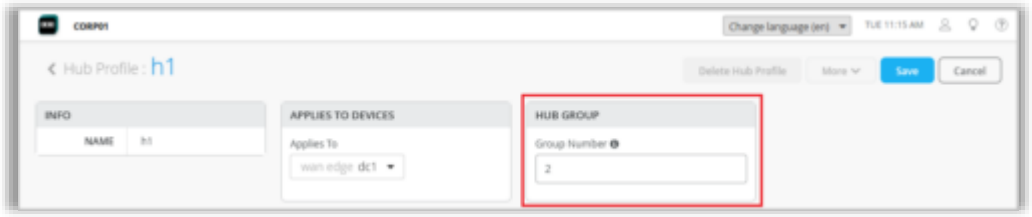
  IDP-based threat detection (SRX)

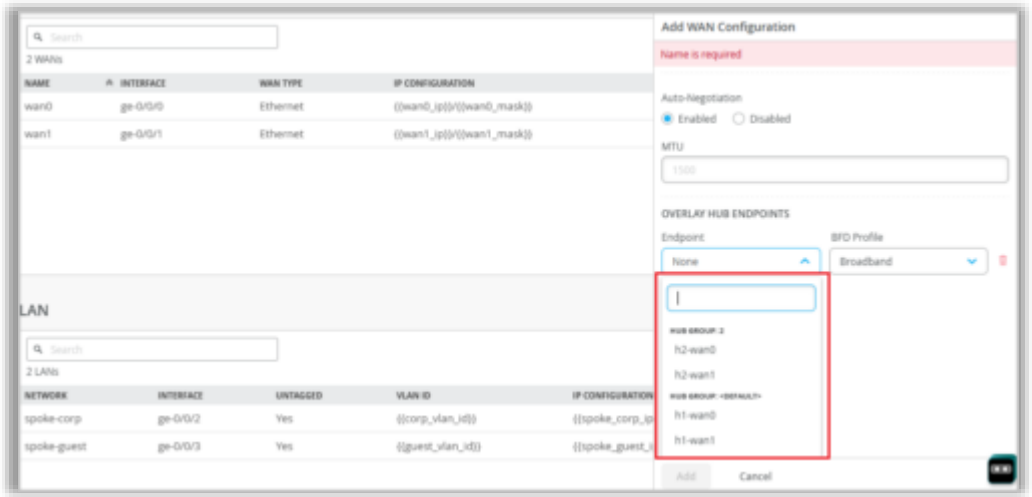
  https://www.mist.com/documentation/idp-based-threat-detection/

  IDP-based threat detection (SSR)

  https://www.mist.com/documentation/idp-based-threat-detection-2/
- IDPバイパスプロファイルはOrganization ＞ Application Policyページで作成できます
- 特定の宛先IPアドレス、攻撃名、重大度に対してバイパスルールを作成できます（左図）

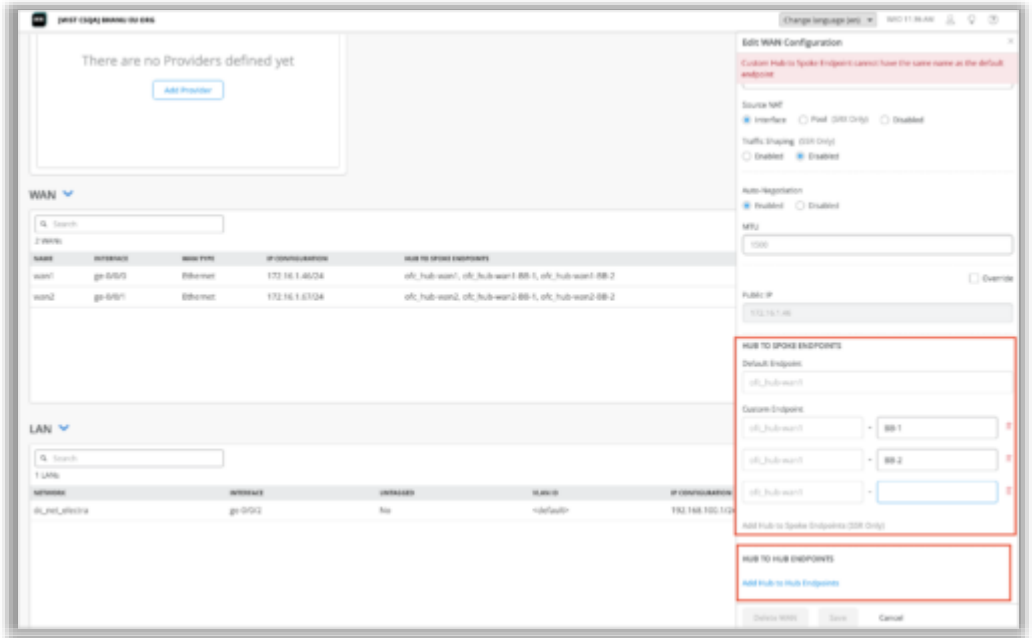
ハブプロファイル内でのハブグループ設定

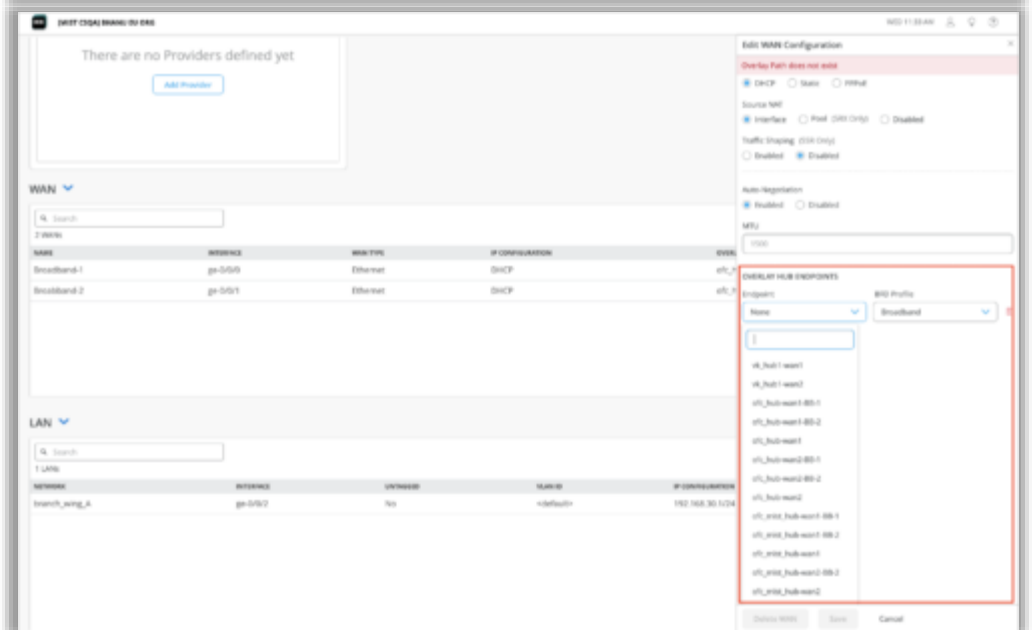




- ハブグループを使用することにより、オーバレイパスの数を増やすことができるようになりました
- 各ハブグループは最大31のハブエンドポイントをサポートします
- ハブグループの機能により、オーバレイ毎に31のハブエンドポイントという、これまでの制限を乗り越えることができます
- 設定の流れは以下となります
  1. ハブプロファイルでハブグループを設定します（左上図）
     - ハブグループ番号に使用できる範囲は2～128です
     - 複数のハブを同じハブグループに追加したい場合は、関係するハブプロファイルに同じハブグループ値を設定します
     - 値1はデフォルトのハブグループを表します
  2. スポークデバイスでハブへのオーバレイパス（OVERLAY HUB ENDPOINTS）を選択します（左下図）
     - 以下のいづれかのWAN設定セクションで設定できます
       - WAN Edges > WAN Edges > WANエッジ名
       - Organization > WAN Edge Template > WANエッジテンプレート名

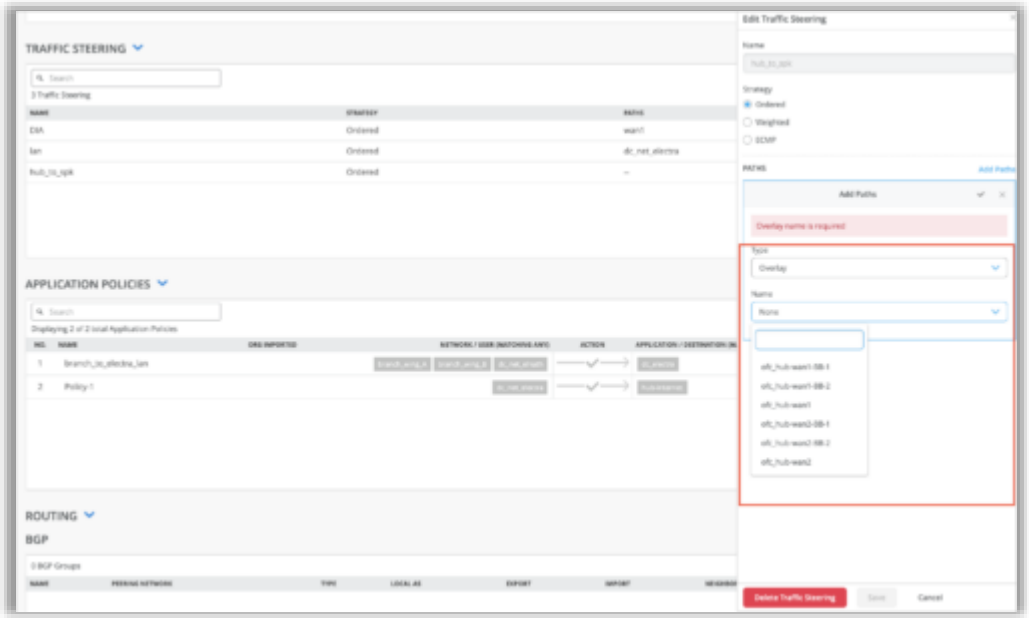
ハブ・スポーク間トラフィックステアリング





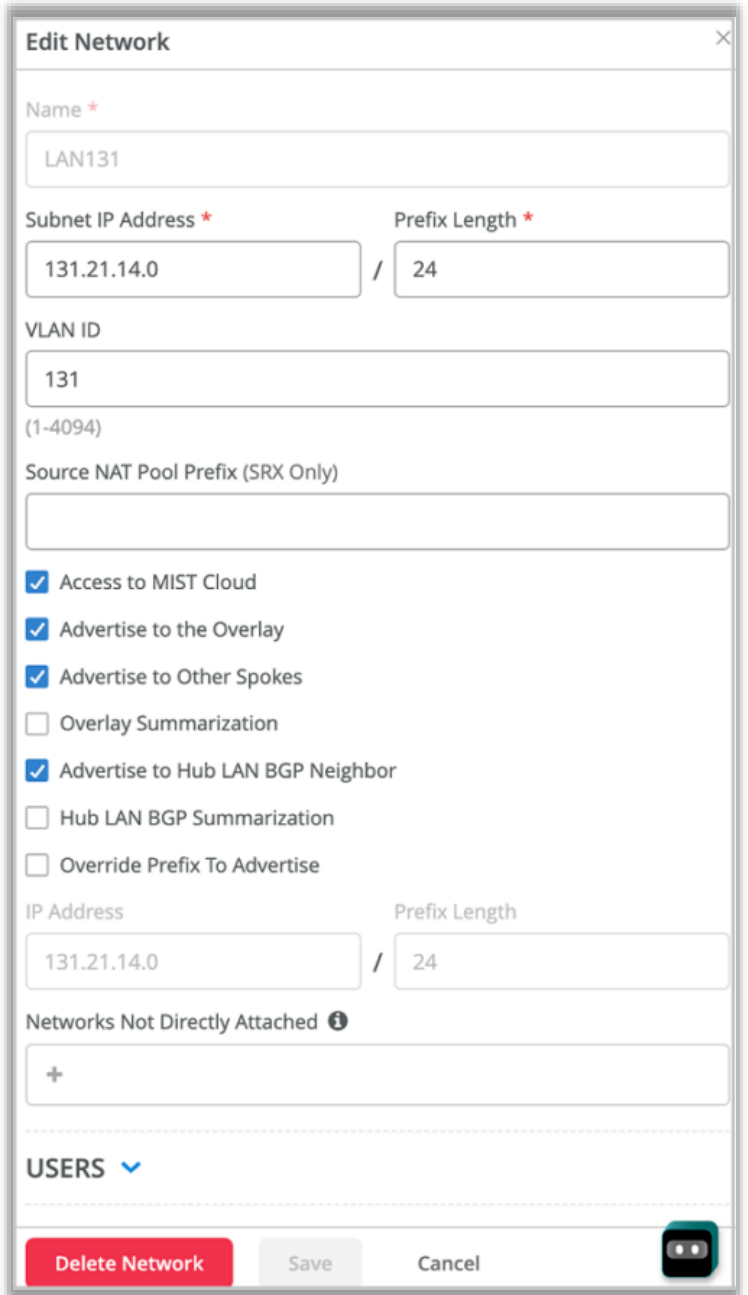
- ハブプロファイルでハブからスポークに向かうトラフィックの経路の選択を制御できるようになりました
- 設定手順は以下となります
  1. ハブプロファイルのHUB TO SPOKE ENDPOINTSセクションでハブからスポークへのオーバーレイエンドポイントを設定します
     - 本機能の追加により、ハブ・ハブ間とハブ・スポーク間エンドポイントを別々に指定できるようになりました
     - ハブ・スポーク間の設定は、ハブプロファイル名を表示する読み取り専用部分と、エンドポイント名を設定する編集可能部分の2つで構成されています（左上図）
     - 設定項目フィールド名「Hub Endpoint」を「Default Endpoint」に変更し、設定項目をHUB TO SPOKE ENDPOINTSセクション内に移動したことにご注意ください
  2. スポークデバイスの詳細ページ（WAN Edges > WAN Edges > WANエッジ名）、またはスポークテンプレート（Organization > WAN Edge Template > WANエッジテンプレート名）で、手順1で設定したハブエンドポイントを指定します（左下図）
     - WAN設定セクション内のOVERLAY HUB ENDPOINTSフィールドから、ハブエンドポイントを選択します
     - エンドポイントはハブグループ単位でリスト表示されます

ハブ・スポーク間トラフィックステアリング（続き）



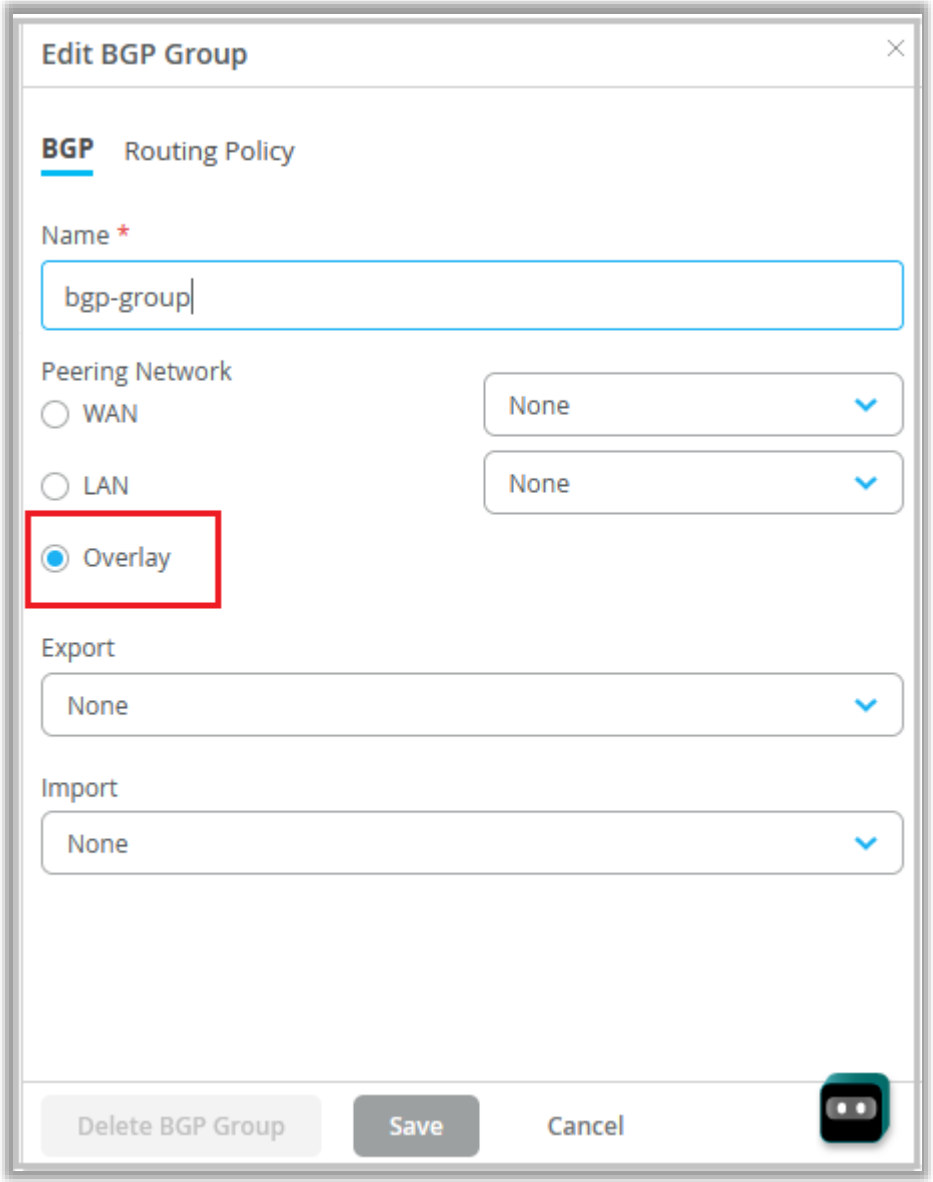
3. エンドポイントを設定後、ハブのトラフィックステアリング設定内（Organization > Hub Profiles > ハブプロファイル名）で設定したエンドポイントを使用して、ハブからスポークに向かうトラフィックをステアリングします（左図）
   - ステアリングには以下の3つの方法があります
     - Ordered：順序付け
     - Weighted：重み付け
     - ECMP：等コストマルチパス
   - 選択した方法に基づいて、トラフィックはハブからスポークへの対応するパスを通じてステアリングされます

ネットワークページへの新規BGPオプションの追加



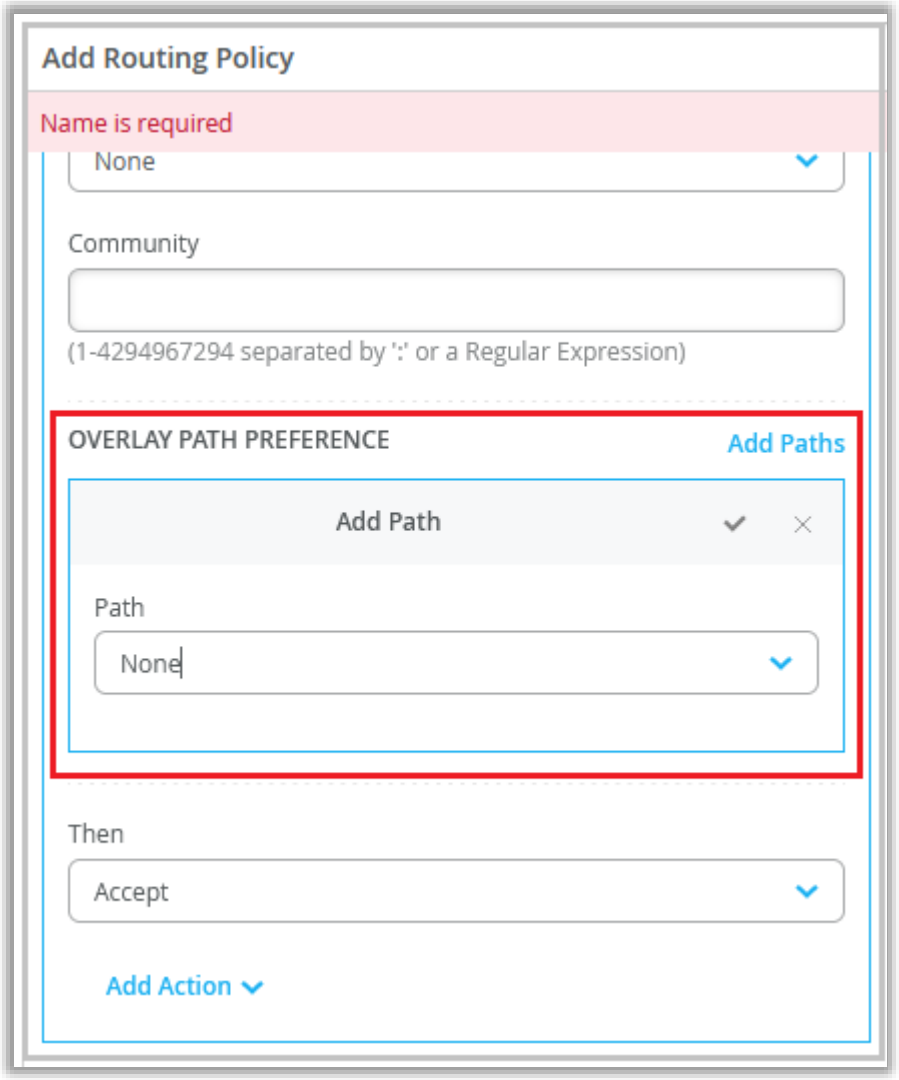
- Networksページ（Organization > Networks）に以下のオプションを追加しました（左図）
  - Advertise to Other Spokes
    - 他のスポークにネットワークをアドバタイズしたい場合に有効にします
    - このオプションはデフォルトで有効です
    - ネットワークをスポークにはアドバタイズせず、ハブのみにアドバタイズしたい場合はこのオプションを無効にします
  - Advertise to Hub LAN BGP Neighbor
    - デフォルトでは、ネットワークプレフィックスはハブのLAN BGPネイバにアドバタイズされます
    - ハブのLAN BGPネイバにネットワークプレフィックスをアドバタイズされたくない場合に、このオプションを無効にします
  - Overlay Summarization
    - オーバレイにアドバタイズするネットワークプレフィックスを集約したい場合は、このオプションを有効にします
      - 例：192.168.1.0/24 → 192.168.0.0/16
    - ハブが各スポークから受信し、ハブが他のすべてのスポークに送り返すBGPアップデートの数を制限します
  - LAN BGP Summarization
    - LAN BGPネイバにアドバタイズするネットワークプレフィックスを集約したい場合は、このオプションを有効にします
      - 例：192.168.1.0/24 → 192.168.0.0/16

BGPで学習したプレフィックスへのオーバレイトラフィックステアリング



- ハブからオーバレイ経由で得るBGP学習経路を制御できるようになりました
- スポークのルーティングポリシーでオーバレイ経路のプリファレンスを設定することにより、可能となります
- スポーク詳細ページ（WAN Edges > WAN Edges > WANエッジ名）、またはスポークテンプレート（Organization WAN Edge Templates）内にあるBGPセクションで以下の手順を実施します
  1. ピアリングネットワークとしてOverlayを選択したBGPグループを設定します（左図）

BGPで学習したプレフィックスへのオーバレイトラフィックステアリング（続き）

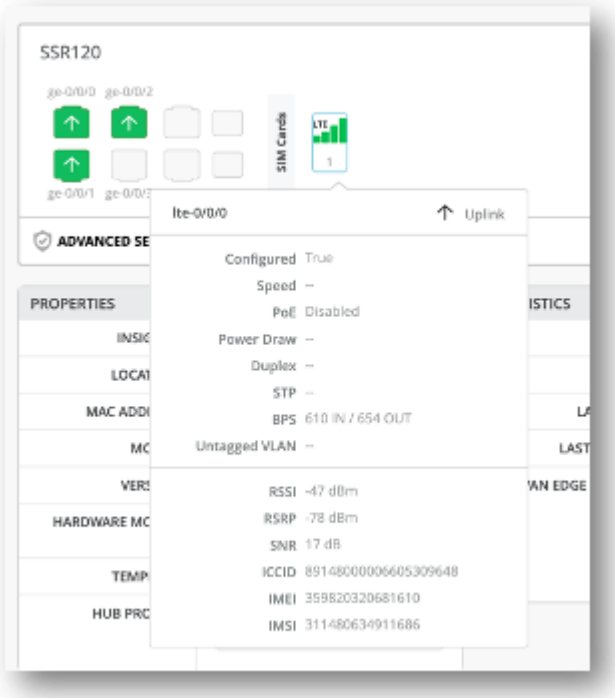


2. Routing Policyウィンドウ内でCreate Policyをクリック後、Add Termsをクリックします
   - ポリシーターム内でオーバーレイパスのプリファレンスを指定して経路ポリシーを設定します
   - OVERLAY PATH PREFERENCEフィールドには、スポークのWAN設定セクションで定義されたオーバーレイエンドポイントがリスト表示されます（左図）
3. Edit BGP Groupウィンドウ内で、作成したポリシーをエクスポートするポリシーとして選択します

URLサブカテゴリによるトラフィック拒否

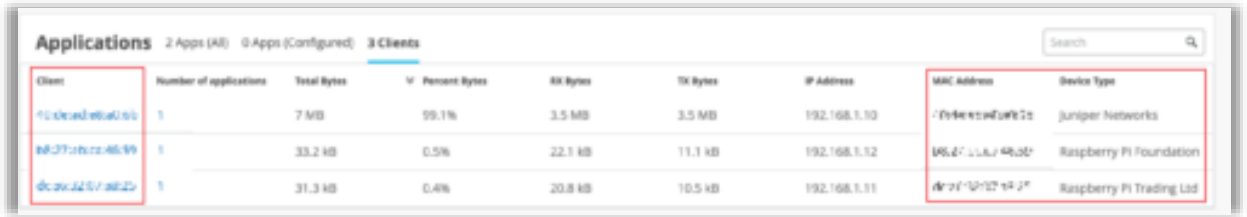
- URLサブカテゴリレベルでトラフィックをブロックできるようになりました
- 本機能により、URLのサブセットに対してアプリケーションポリシーを定義できるようになるため、トラフィックをブロックする際の制御がよりきめ細かくなります
- URLサブカテゴリは、アプリケーション作成画面（Organization > Applications > Add Applications）で選択できます
- これまでの設定方法となる、カテゴリレベルでのURLのアプリケーションポリシーを設定した場合、複数のURLサブカテゴリに同じポリシーを適用することになります

フロントパネルでのLTEインタフェース表示



- SSR及びSRXのLTEインタフェース固有の情報が、WANエッジのフロントパネルに表示されるようになりました（LTEインタフェース搭載の機器に限ります）
- フロントパネルには、LTEインタフェースを表すポートアイコンが表示されます
- ポートアイコンにマウスのカーソルを合わせると、インターフェースのステータスの詳細とともに、以下の LTE 固有の情報が表示されます（左図）
  - RSSI（受信信号強度）
  - RSRP（基準信号受信電力）
  - SNR（信号対雑音比）
  - ICCID（集積回路カードID）
  - IMEI（国際移動体装置識別番号）
  - IMSI（国際移動体加入者識別番号）

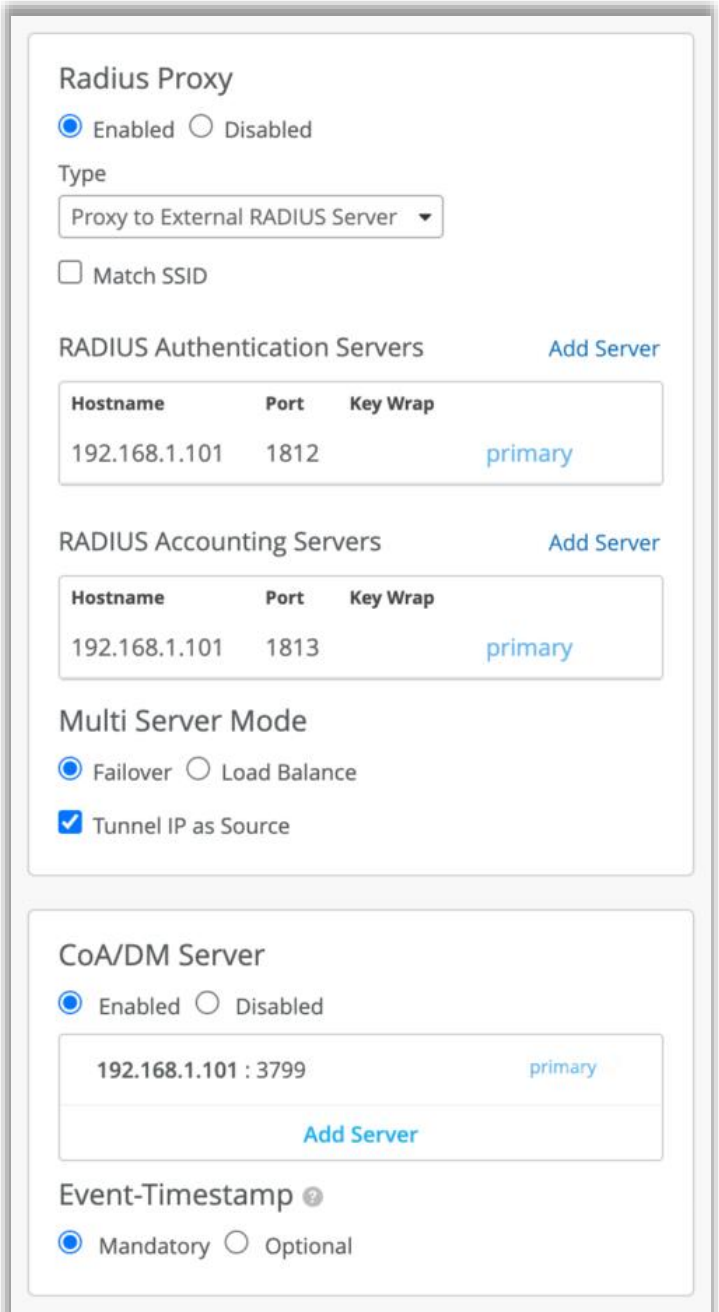
DHCPクライアント情報の表示内容の追加



- DHCPサーバが設定されているSRXがMistクラウドへ送信しているDHCPクライアント情報を表示できるようになりました
- 以下の情報が表示されます（左図）
  - クライアント
  - MACアドレス
  - デバイスの種類
- これらの情報はアプリケーション数、TXバイト数、RXバイト数、合計バイト数とともに、WANインサイトページのアプリケーションセクションで確認できます

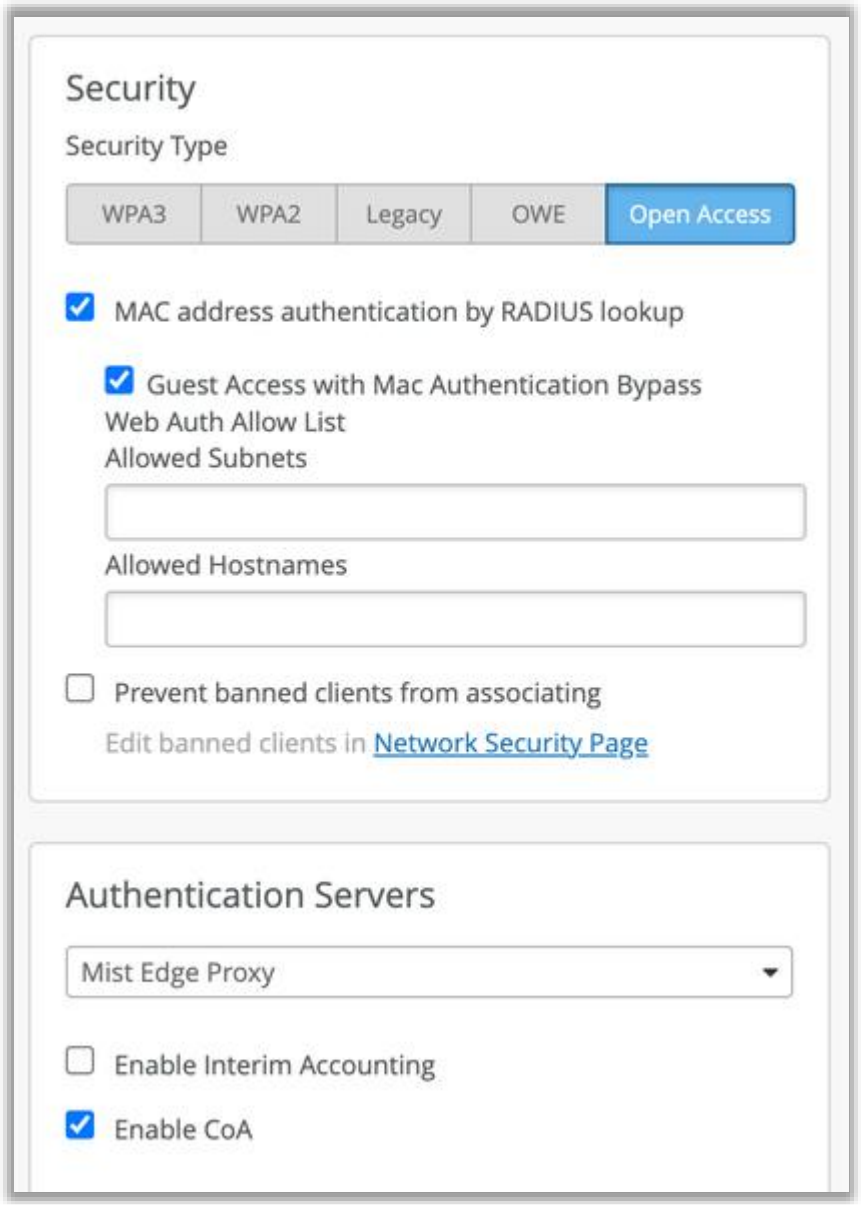
MIST Edge

RADIUSプロキシ機能でのCoAのサポート



- Mist EdgeのRADIUSプロキシがCoA（Change of Authorization）をサポートしました
  - CoA：ユーザーやデバイスが認証された後に、その認証を動的に変更する仕組み
- 本機能を使用するにはAPのファームウェアが0.14.29091以上である必要があります
- 設定は以下の手順となります
  1. Mist Edgeでの設定（左図）：
     a. RADIUSプロキシを有効にします
        - RADIUSプロキシタイプとして、「Proxy to External RADIUS Server」を選択する必要があります
        - RADIUSリクエストをTunterm IPから送信したい場合は、「Tunnel IP as Source」オプションを有効にします
        - 「Tunnel IP as Source」オプションが有効になっていない場合は、リクエストはOut of Boundインタフェースから送信されます
     b. 動的認証クライアント（DAC）からCoAリクエストパケットまたは切断リクエストパケットを受信するために、Mist EdgeでCoA/DMサーバを設定します
        - CoA/DMサーバの設定には、サーバのIPアドレスと共有シークレットが含まれます
        - イベントのタイムスタンプを含めることを必須、またはオプションに設定できます
        - この設定により、Mist EdgeはRADIUSサーバからのCoAリクエスト、または切断リクエストパケットをCoAポート（UDP 3799）で受信できるようになります
  - 上記設定は以下のいづれかで設定可能です
    - OrganizationレベルのMist Edge：Mist Edges > Mist Edge名 > Mist Edge Cluster
    - サイトレベルのMist Edge：Organization > Site Configuration > サイト名

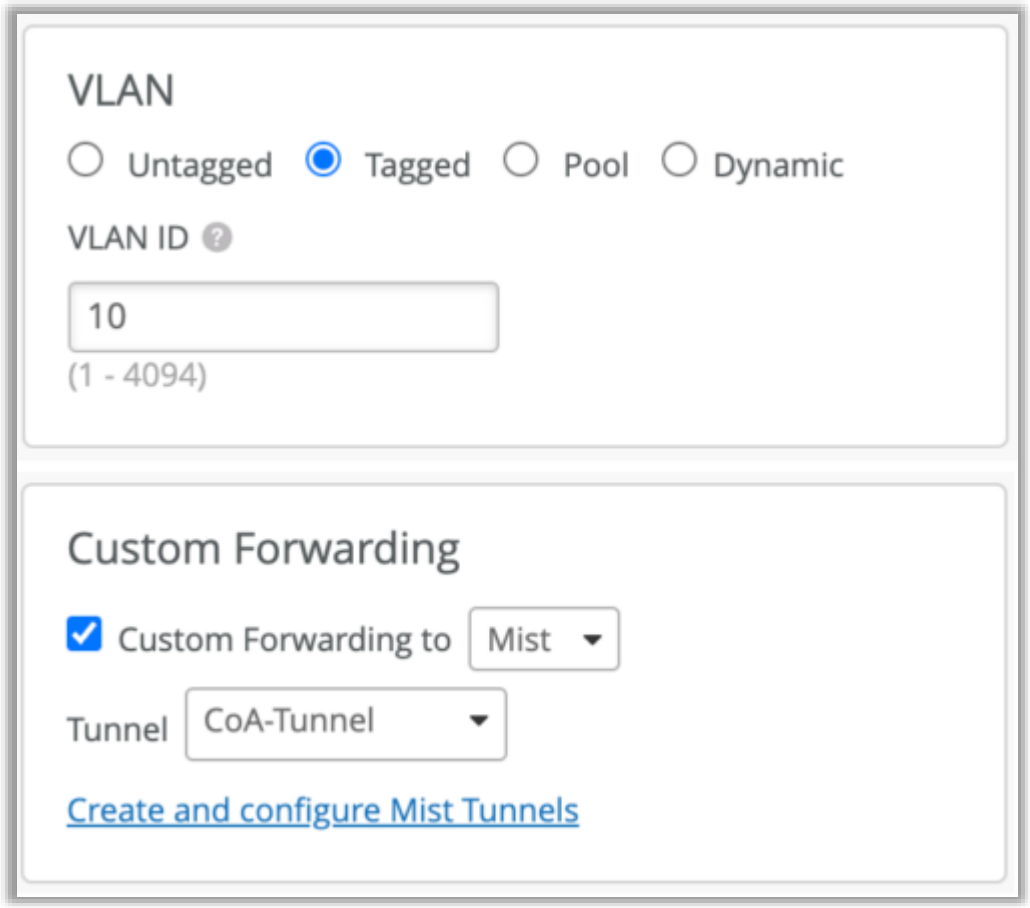
RADIUSプロキシ機能でのCoAのサポート（続き）



2. WLANページでの設定：
   b. 対応するセキュリティの種類を選択します
      - 以下のセキュリティの種類をサポートしています
        - Enterprise (802.1x)
        - Personal (SAE/PSK) + MAC Address Authentication by RADIUS lookup
        - OWE + MAC Address Authentication by RADIUS lookup
        - Open Access + MAC Address Authentication by RADIUS lookup
   c. Authentication Servers項目で「Mist Edge Proxy」を選択し、CoAを有効にします（左図）

次のページに続きます

RADIUSプロキシ機能でのCoAのサポート（続き）



d. VLANタギングを有効にし、Custom Forwarding項目にてMist Tunnel（OrganizationレベルのMist Edgeの場合）、またはSite Edge（サイトレベルの Mist Edgeの場合）を選択します（左図）


Thank you
JUNIPER
driven by Mist AI