

2024年2月29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/february-29th-2024-updates/>

本ドキュメントは2024年2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)

Simplified Operations

- WLANリストページでのカスタムフォーワーディングトンネル情報の表示

Marvis

- サイト、デバイス、クライアントのトラブルシューティングAPI
- サポートチケット作成ページでの要約された回答の表示

Access Assurance

- Mist EdgeプロキシIDP

Wired Assurance

- ポートリストでの認証方法とダイナミックポート設定状況の表示
- 遅い間隔でのLACPパケットの送信
- 複数サブリカントモードでのdot1x認証のサポート
- バーチャルシャーシ (VC) メンバスイッチのソフトウェアバージョン違いの警告
- ネットワーク範囲から逸脱したIPアドレス設定時の警告表示

本リリースで追加された機能一覧 (2/2)

WAN Assurance

- BGPセッションでのBFD設定
- BGPネイバの無効化
- WANエッジポートの無効化 (SSR)
- カスタムDSCP値の設定 (SSR)
- SRX1600のサポート
- SRXでのPCAP
- Zscalerサブロケーションのサポート (セキュリティ)

Mist Edge

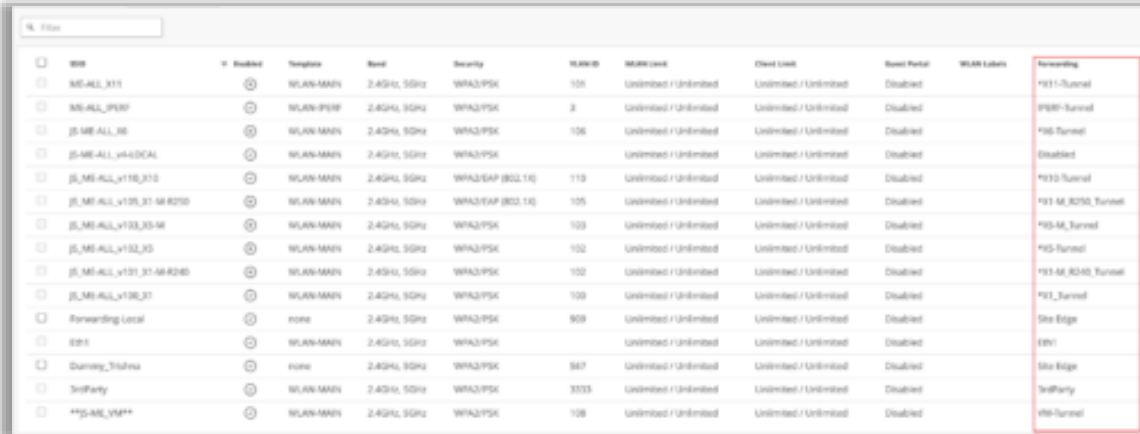
- Mist Edge名を用いてのAP検索

Network Observability and Business Intelligence

- セキュリティアシュアランスダッシュボード

Simplified Operations

WLANリストページでのカスタムフォーワーディングトンネル情報の表示

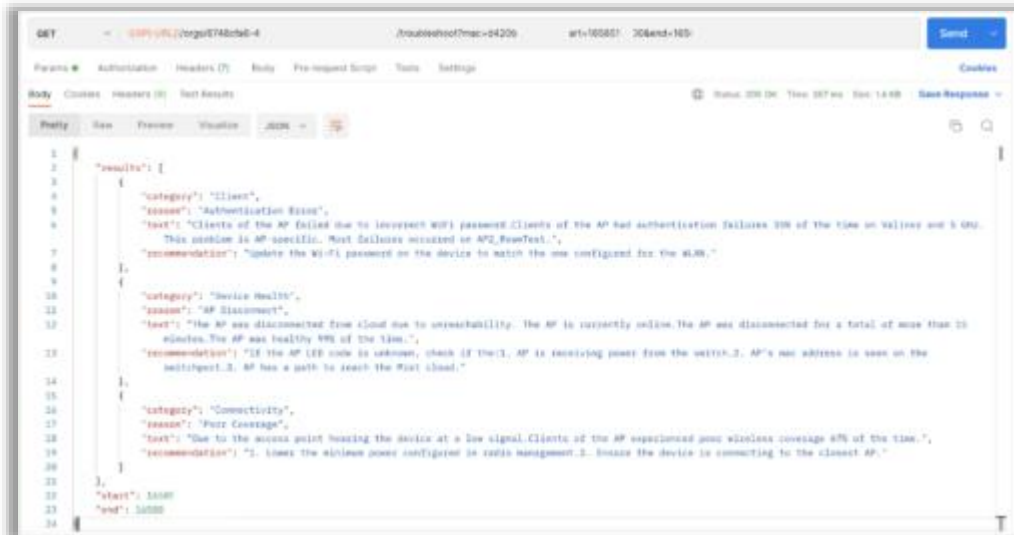
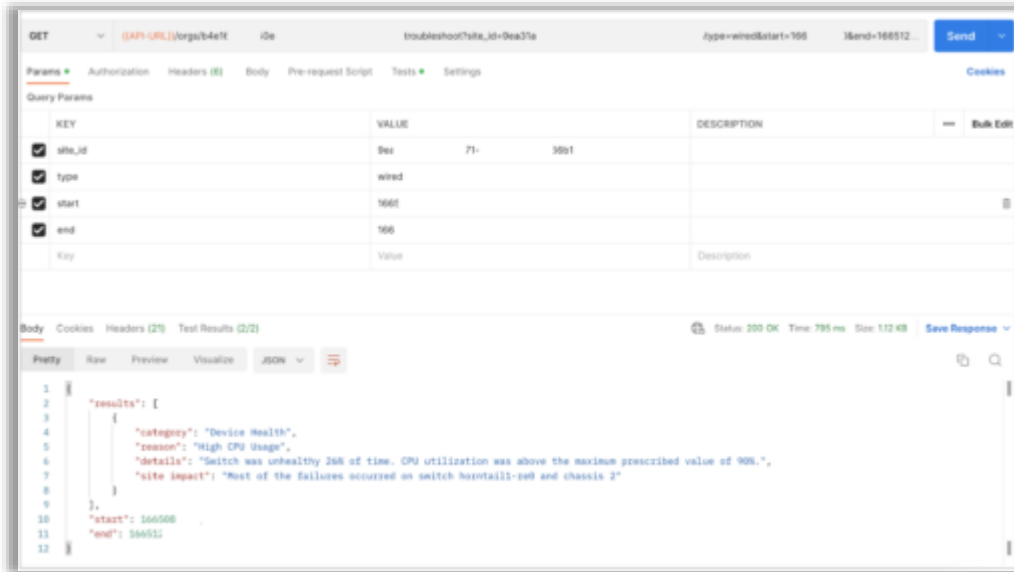


ID	Enabled	Template	Band	Security	NWID	NWID desc	Client Limit	Speed Limit	WLAN Label	Forwarding
ME-ALL_X11	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK	101	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		t11-Tunnel
ME-ALL_PSRF	⊕	WLAN-PSRF	2.4GHz, 5GHz	WPA2-PSK	3	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		PSRF-Tunnel
IS-ME-ALL_M	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK	106	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		t10-Tunnel
IS-ME-ALL_u410CAL	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK		Unlimited / Unlimited	Unlimited / Unlimited	Disabled		Disabled
IS-ME-ALL_v110_X10	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-EAP (802.1X)	110	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		t10-Tunnel
IS-ME-ALL_v110_X1-M-RC10	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-EAP (802.1X)	105	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		t11-M-RC10-Tunnel
IS-ME-ALL_v102_X3-M	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK	103	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		t10-M-Tunnel
IS-ME-ALL_v102_X3	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK	102	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		t10-Tunnel
IS-ME-ALL_v101_X1-M-RC10	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK	100	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		t11-M-RC10-Tunnel
IS-ME-ALL_v100_X1	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK	100	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		t11-Tunnel
Forwarding Local	⊕	none	2.4GHz, 5GHz	WPA2-PSK	909	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		Site Edge
Site	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK		Unlimited / Unlimited	Unlimited / Unlimited	Disabled		Site
Dummy_Toshu	⊕	none	2.4GHz, 5GHz	WPA2-PSK	907	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		Site Edge
3rdParty	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK	3333	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		3rdParty
IS-ALL_VM	⊕	WLAN-MAN	2.4GHz, 5GHz	WPA2-PSK	108	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		t10-Tunnel

- カスタムフォーワーディングでトンネルが設定されたWLANのトンネルプロファイルがWLANリストページ (Site > WLANs) で確認できるようになりました (左図)

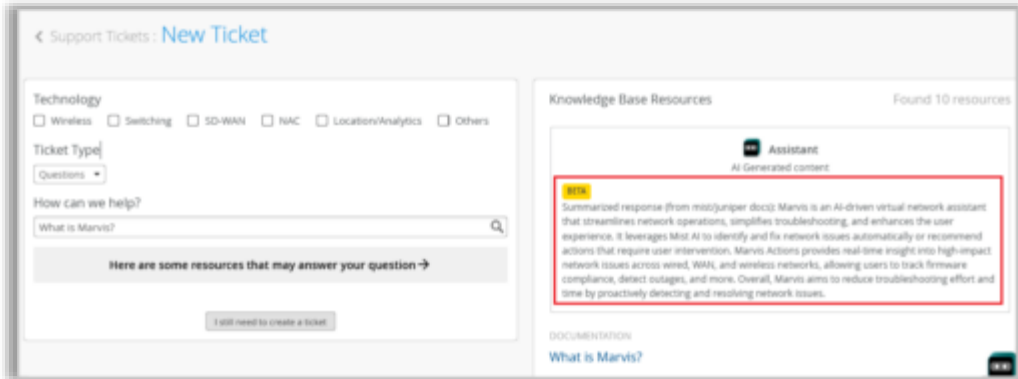
Marvis

サイト、デバイス、クライアントのトラブルシューティングAPI



- サイトとデバイスのトラブルシューティングのためにMarvisに問い合わせる手段としてMarvis APIを導入しました
- デバイスには、無線/有線クライアント、アクセスポイント（AP）、スイッチ、WANエッジが含まれます
- 問題のカテゴリ、理由、説明、および推奨アクション（該当するものがある場合）をテキストベースで応答します
- デバイスのトラブルシューティングにはMACアドレスを uses
- サイトのトラブルシューティングにはサイトIDとネットワークの種類（オプション：無線（デフォルト）、有線、WAN）を uses
- 本機能を使用するために、以下の条件が必要です
 - OrganizationレベルでのMarvisサブスクリプション
 - Marvisサブスクリプションについては以下をご参照ください
<https://www.juniper.net/documentation/us/en/software/mist/mist-aiops/topics/ref/marvis-subscriptions.html>
 - Organizationレベルのアクセス権限
- 左上図はサイトの有線ネットワークをトラブルシューティングした際の出力です
- 左下図はデバイス、またはクライアントをトラブルシューティング際の出力です
- APIドキュメントに関しては以下をご参照ください
<https://api.mist.com/api/v1/docs/Org#troubleshoot>
 - 上記URLへのアクセスにはGlobal01環境にログインしている必要があります
 - APIドキュメントはMistポータル（Organization UI）のヘルプ（？）メニューからアクセスすることができます

サポートチケット作成ページでの要約された回答の表示



- サポートチケット作成時に、問い合わせに関する関連ドキュメントのリンクに加えて、要約された回答が即座に表示されるようになりました（左図）
- ドキュメントを確認する前に、AIが生成した回答が問い合わせの答えとなっているかどうかを確認することができます
- サポートチケット作成ページはヘルプ (?) メニューからアクセスできます

Access Assurance

Mist EdgeプロキシIDP

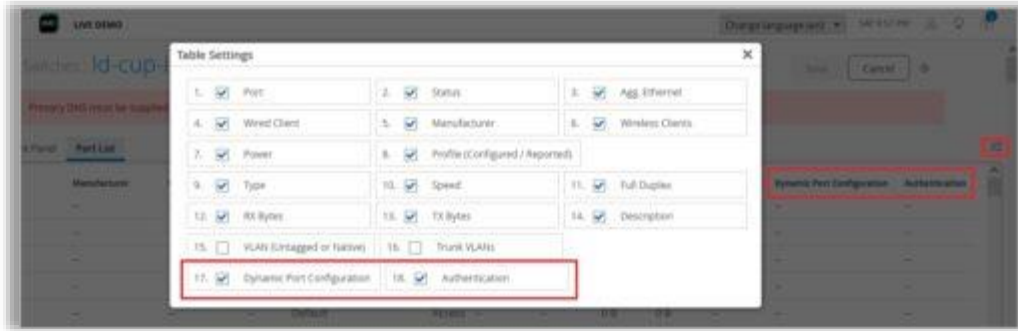
The screenshot shows the configuration page for a new Identity Provider (IDP). The 'Name' field contains 'New Identity Provider'. Under the 'Configuration' section, the 'IDP type' is set to 'Mist Edge Proxy', which is highlighted with a red box. Other fields include 'Proxy Hosts', 'SSIDs', 'Mist Edge Cluster' (set to 'Testcluster'), 'Exclude Realms', and 'Operator Name'. At the bottom, there is a section for 'RADIUS Authentication Servers' with an 'Add Server' button.

- Mist Edgeをプロキシとしたアイデンティティプロバイダ（IDP）を設定できるようになりました（左図）
- 典型的な使用例として、Mist Edgeをeduroamフェデレーションのプロキシとして使用して以下の認証を行う場合です
 - 外部からの訪問者の認証
 - ローミングユーザの認証（別の教育機関にいるが、所属する教育機関の認証情報を使用してeduroam SSIDで認証したいユーザの認証）
- 1台以上のMist Edgeが静的なパブリックIPアドレスを持つeduroamへのゲートウェイとして機能している必要があります
- Mist EdgeプロキシIDPを設定するにはアイデンティティプロバイダ設定ページ（Organization > Identity Providers > Add IDP）の「IDP Type」で「Mist Edge Proxy」を選択し、必要な情報を入力します
- 詳細な情報は以下のページをご参照ください

<https://www.mist.com/documentation/mist-edge-proxy-idp-eduroam/>

Wired Assurance

ポートリストでの認証方法とダイナミックポート設定状況の表示



- スイッチの詳細ページ (Switches > スイッチ名) 内のポートリストタブに、以下の列を追加しました
 - ダイナミックポート設定
 - スイッチポートがダイナミックポートプロファイルによって有効になっているかどうか、設定状況を確認できます
 - ダイナミックポートプロファイルではインタフェースに動的にポートプロファイルを適用するためのルールを設定できます
 - 認証
 - アクセス制御としてスイッチポートに設定されている認証方法を確認できます
 - dot1x、dot1x/MAB、MABなどの値を表示します
- ダイナミックポート設定状況や認証情報はフロントパネルタブ上でポートにマウスカーソルを合わせた際に表示されるポートウィンドウでも確認できます
- ポートリストで項目が出力されない場合は、右側に表示された三重線をクリックし、出力項目として選択することができます (左図)

遅い間隔でのLACPパケットの送信

Auto

PoE
 Enabled Disabled

MTU
 Enabled Disabled

Description
Add Description

Up / Down Port Alerts ⓘ
 Enabled Disabled
Manage Alert Types in [Alerts Page](#)

Port Aggregation
 Enabled Disabled

LACP
 Enabled Disabled

LACP Force-UP ⓘ
 Enabled Disabled

LACP Periodic Slow
 Enabled Disabled

AE Index (0 - 255)

Allow switch port operator to modify port profile
 Yes No

- AEインタフェースで、遅い間隔（LACP Periodic Slow）で周期的にLACPパケットを送信することができるようになりました
- AEインタフェースで「LACP Periodic Slow」オプションを設定すると、LACPパケットが30秒毎に送信されるようになります
- デフォルトでは送信間隔はfastで設定されており、LACPパケットは毎秒送信されます
- 以下のいずれかでLACP Periodic Slowを設定できます（左図）
 - スイッチテンプレート（Organizationレベル、またはサイトレベル）内のSelect Switches Configuration項目内のPort Configタブ
 - デバイスレベルのスイッチ設定ページ（Switches > スイッチ名）内のPort Configuration項目
- LACPをポートで有効にしている場合にLACP Periodic Slowを設定できます

複数サブリカントモードでのdot1x認証のサポート

PORT PROFILES

Port configuration for a set of related ports
* System defined

New Port Profile

Name
port-1

Port Enabled
 Enabled Disabled

Description
Add Description

Mode
 Trunk Access

Port Network (Untagged/Native VLAN)
default

VoIP Network
None

Use dot1x authentication
 Allow Multiple Suplicants

Dynamic VLAN
 Mac authentication
 Use Guest Network
 Bypass authentication when server is down

Speed
Auto

Duplex
Auto

Mac Limit
0
(0 - 16383, 0 => unlimited)

PoE
 Enabled Disabled

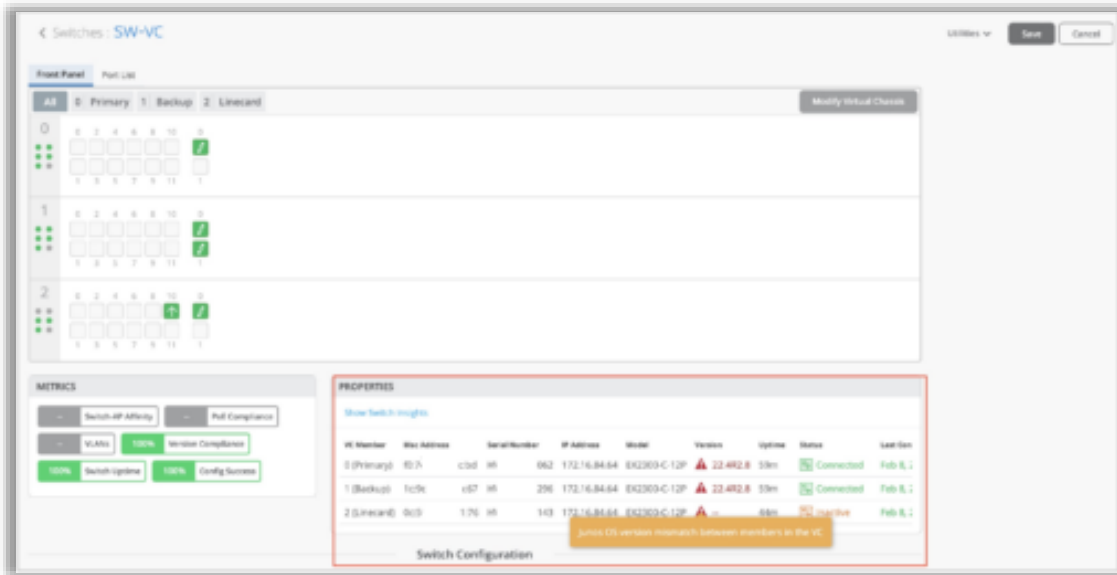
STP Edge
 Yes No

QoS
 Enabled Disabled
 Enable MTU

Storm Control
 Enabled Disabled

- スイッチポートに複数サブリカントモードのdot1x認証を設定できるようになりました
 - このモードでは、複数のデバイスをポートに接続し、各デバイスを認証することができるようになります
- 以下のいずれかの場所にあるポートプロファイル項目の「Allow Multiple Suppliant」チェックボックスを選択することにより、設定が可能です（左図）
 - スイッチテンプレート（Organizationレベル、サイトレベル）
 - デバイスレベルのスイッチ設定ページ（Switches > スイッチ名）
- 「Use dot1x authentication」オプションを選択したときに、「Allow Multiple Suppliant」チェックボックスが表示されます
- この設定を有効にするために、スイッチポートにポートプロファイルを適用する必要があります

バーチャルシャーシ（VC）メンバスイッチのソフトウェアバージョン違いの警告



- VC内の他のメンバスイッチと異なるソフトウェアバージョンで起動しているメンバスイッチに対し、VCスイッチ詳細ページ（Switches > スイッチ名）内で警告メッセージが表示されるようになりました（左図）
- ソフトウェアバージョンが違う場合、スイッチ詳細ページの Properties項目内のバージョンで警告アイコンが表示されます
- 警告メッセージを確認したい場合、警告アイコンにマウスカーソルを合わせます
- ソフトウェアバージョンが違うメンバスイッチの状態は「inactive」として表示されます

ネットワーク範囲から逸脱したIPアドレス設定時の警告表示

The screenshot shows the 'IP CONFIGURATION' page in a Juniper network management interface. At the top, it says 'Configure IRB/SVI interfaces using DHCP or Static IP assignment'. A red-bordered box highlights a warning message: 'IP address 100.100.100.10 out of scope defined under subnet field for Network vlan_test'. Below this, there are several configuration fields: 'Override Site/Template Settings' (checked), 'IP Address' (DHCP selected), 'Network (VLAN)' (dummy, 50), 'Primary DNS', 'Secondary DNS', and 'DNS Suffix'. At the bottom, there is an 'Additional IP Configuration' section for 'vlan_test' with 'Static' IP selected, IP address '100.100.100.10', Subnet Mask '/24', and Network (VLAN) 'vlan_test'.

- スイッチ詳細ページ（Switches > スイッチ名）のIP Configuration項目内にあるAdditional IP Configuration設定で、関連するネットワーク（VLAN）範囲外のIPアドレスを設定しようとするすると警告メッセージが出力されるようになりました（左図）

WAN Assurance

BGPセッションでのBFD設定

Add BGP Group

Name is required

Name *

Peering Network

WAN LAN Overlay BETA

Advertise to the Overlay

BFD

Enabled Disabled

Type *

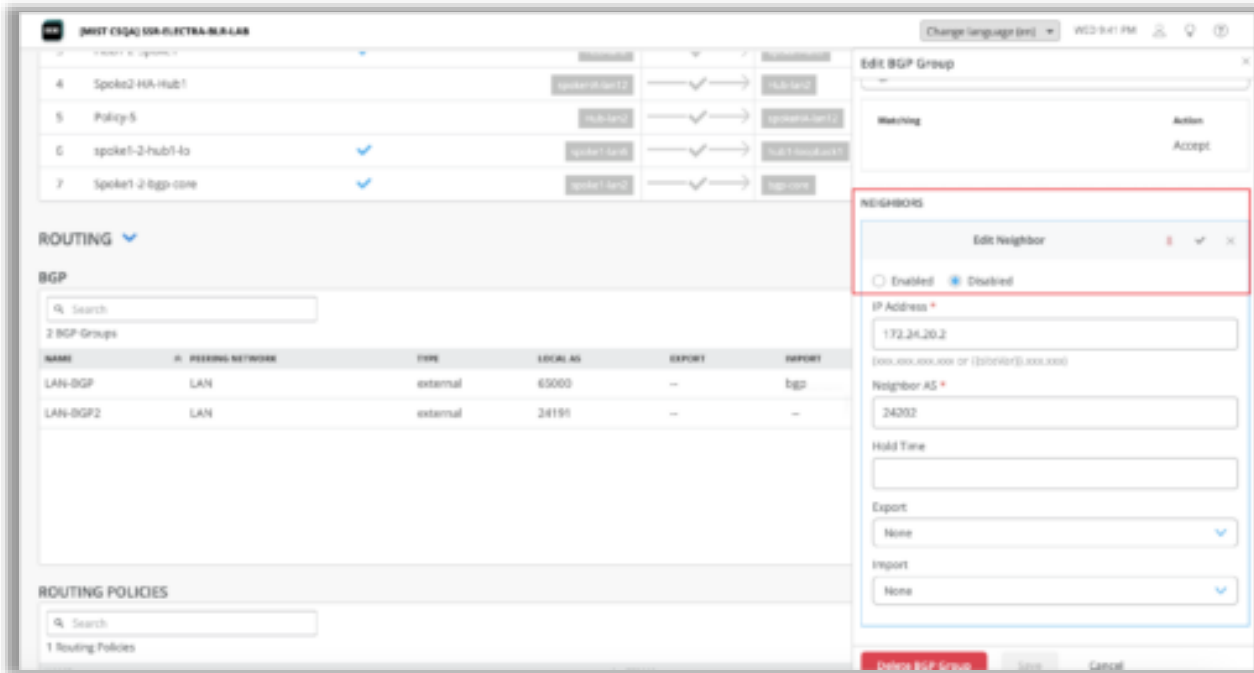
Local AS *

Hold Time *

Add Cancel

- WANエッジでBGPセッションのBFD（Bidirectional Forwarding Detection）を有効・無効に設定できるようになりました（左図）
 - BFD :
 - Helloパケットの仕組みを用いた、ネットワーク障害を検知するプロトコル
- 以下のいずれかの設定内にあるAdd BGP Group項目でBFDの有効、無効を設定できます
 - WANエッジテンプレート（Organization > WANエッジテンプレート）
 - WANエッジ設定ページ（WAN Edges > WAN Edges > WANエッジ名）

BGPネイバの無効化



- WANエッジでBGPネイバを無効化できるようになりました
- 以下のいずれかの設定箇所にあるAdd BGP Groupページ、またはEdit BGP Groupページ内のEdit Neighborセクションで「Disabled」を選択することにより、無効化が可能です(左図)
 - WANエッジテンプレート (Organization > WANエッジテンプレート)
 - WANエッジ設定ページ (WAN Edges > WAN Edges > WANエッジ名)

WANエッジポートの無効化 (SSR)

Edit WAN Configuration

Name * VAR
spokeWan

Description VAR

WAN Type
 Ethernet DSL ⓘ LTE

Interface * VAR
ge-0/1/1
(ge-0/0/1, ge-0/0/3, ge-0/1/1-3, etc)

Disabled (SSR Only)

Port Aggregation

Redundant BETA

Enable "Up/Down Port" Alert Type ⓘ
(Manage Alert Types in [Alerts Page](#))

VLAN ID VAR
100

Delete WAN Save Cancel

- SSRのLANポート、WANポートを無効化できるようになりました
- 以下のいずれかの設定箇所にあるLAN、またはWAN設定ページで「Disabled」を選択することにより、無効化が可能です（左図）
 - WANエッジテンプレート（Organization > WANエッジテンプレート）
 - WANエッジ設定ページ（WAN Edges > WAN Edges > WANエッジ名）

カスタムDSCP値の設定 (SSR)

Add Application ×

ADVANCED SETTINGS

Traffic Type *
Custom

Failover Policy
 Revertible Non-Revertible

Traffic Class *
High

DSCP Class (SSR Only) VAR
46

Maximum Latency VAR
(milliseconds)

Maximum Jitter VAR
(milliseconds)

Maximum Loss VAR

Add Cancel

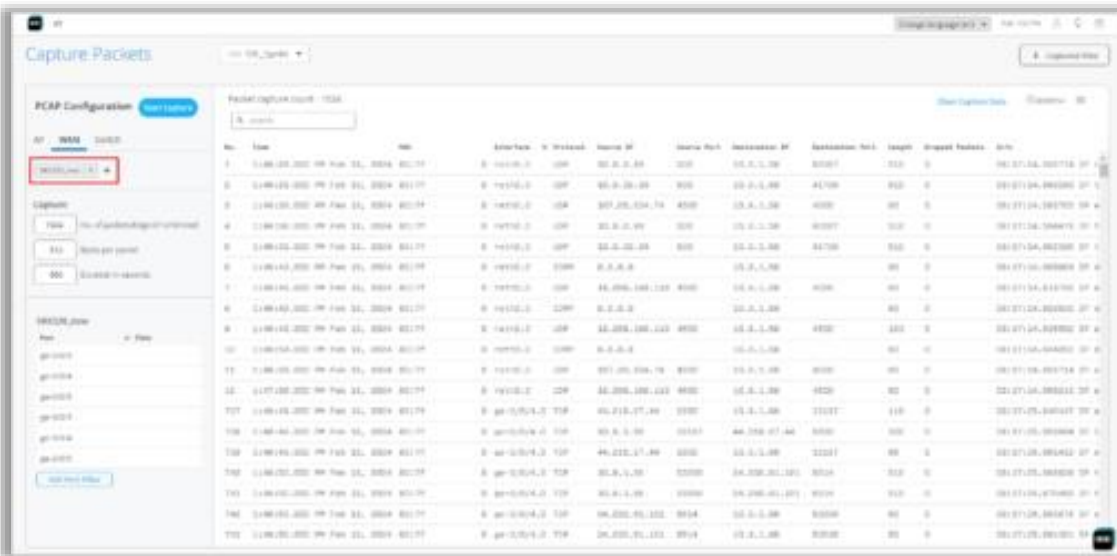
- アプリケーションのトラフィックの種類毎にDSCP値 (0~63) をカスタマイズして設定できるようになりました
 - これまでは各トラフィックの種類に事前設定された値をDCSP Classのドロップダウンリストから選択するのみでした
 - DSCP :
 - トラフィックを分類する仕組みとなり、IPヘッダにある6ビットのDSフィールドを用い、L3 IPネットワークにおいてQoSサービスを提供します
- Add Applicationページ (Organization > Applications) でDSCP値を設定できます
- トラフィッククラス (Best Effort、High、Medium、Low) を選択すると、デフォルトのDSCP値が入力されます (左図)
- デフォルトの値を上書きすることが可能です

SRX1600のサポート

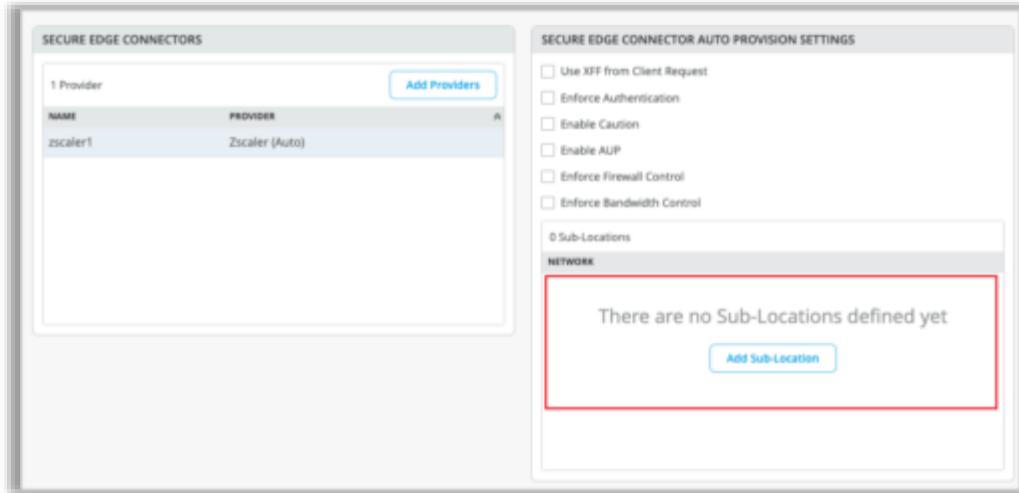
- SRX1600がサポートされました
- SRX1600の登録には、インベントリページ（Organization > Inventory > WAN Edges）にあるAdopt WAN Edgesワークフローを使用してください（Claim WAN Edgesワークフローには対応していません）

SRXでのPCAP

- SRXでパケットキャプチャ（PCAP）がサポートされました
- パケットキャプチャページ（Site > WAN Edge Packet Captures）のWANのタブ内でSRXを選択できるようになりました（左図）
 - SSRでは既にパケットキャプチャが可能です
- パケットキャプチャ機能により、監視、ログ目的でリアルタイムで送受信されるパケットをキャプチャできます



Zscalerサブロケーションのサポート（セキュリティ）

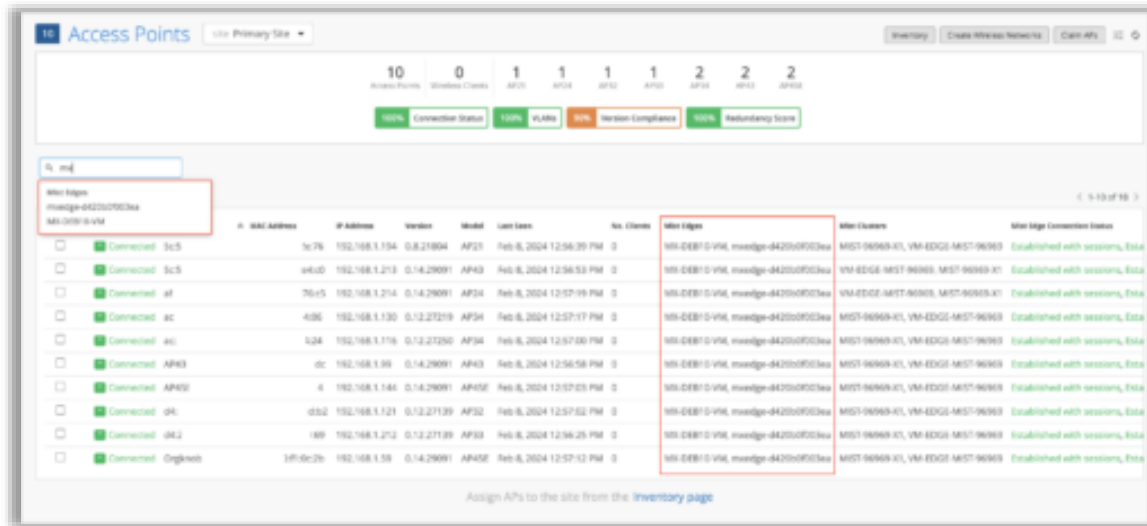


- Zscalerのサブロケーションを設定できるようになりました
 - サブロケーション：
 - ロケーションオブジェクトの子エンティティ
- ロケーションは組織がどこからインターネットへトラフィックを送信するかを識別します
- 同じGREトンネルやIPSecトンネルを通過するトラフィックでも異なるネットワークとしてサブロケーションを設定できます
- サブロケーションは以下のような使用方法が可能です
 - IPアドレスに基づいて異なるポリシーを適用
 - 社内ネットワークに対しては認証を強制し、ゲストネットワークでは認証を無効にする
 - 親ロケーションでは未使用帯域幅を利用できるようにしながら、サブロケーションでは帯域幅制御を強制
- 各サブロケーションではゲートウェイオプションと内部ネットワークを指定できます
- 以下のいずれかの設定箇所Zscalerサブロケーションを設定できます
 - WANエッジテンプレート（Organization > WAN Edge Templates）
 - WANエッジ設定ページ（WAN Edges > WAN Edges > WANエッジ名）
- Zscalerがセキュアエッジコネクタとして設定されている場合にAdd Sub-Locationオプションが表示されます

Mist Edge

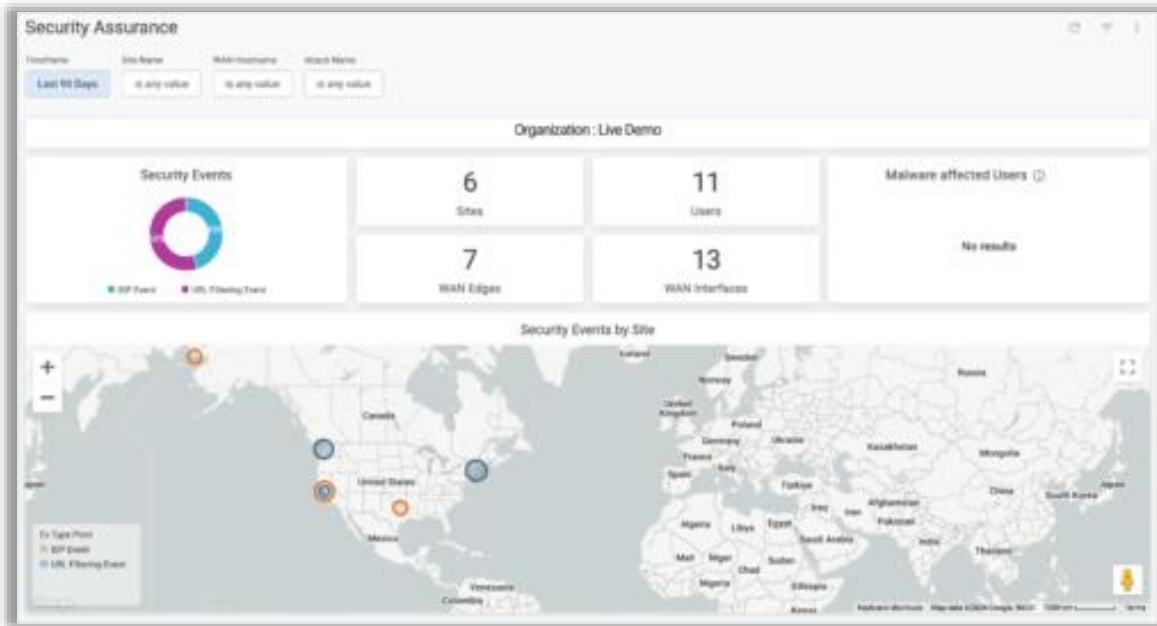
Mist Edge名を用いてのAP検索

- Mist Edge名を用いてアクセスポイント（AP）を検索できるようになりました（左図）
- APが複数のMist Edgeとトンネルを確立していても検索が可能です
 - 以前は複数のトンネルを確立している場合は検索不可でした
- APをMist Edge名毎に並べ替えることもできます



Network Observability and Business Intelligence

セキュリティアシュアランスダッシュボード



- Premium AnalyticsのダッシュボードにWANセキュリティダッシュボードとなるセキュリティアシュアランスダッシュボードを追加しました
- このダッシュボードでは、SSRやSRX（アドバンスセキュリティパック搭載）が生成するURLフィルタリングやIDS/IPS（Intrusion Detection and Prevention System）イベントから得られるセキュリティインサイトを提供します
- このダッシュボードはPremium Analyticsページ（Analytics > Premium Analytics）のWANセクションから閲覧できます

Thank you

