JUNIPER MIST ACCESS ASSURANCE データシート

製品概要

Juniper Mist Access Assurance は、エンドツーエンドのユーザーエクスペリエンスを可視化することで、ゼロトラスト、アイデンティティベースのネットワークアクセス、フルスタックポリシーとセグメンテーションアサインメントを確保するクラウドベースのサービスです。このサービスは、ゲスト、IoT、BYOD、企業デバイスのオンボーディング向けに、柔軟性が高くシンプルな認証ポリシーフレームワークを備えた一連のアクセス制御機能を提供します。クライアント接続は、ユーザーとデバイスの識別に基づいて制御され、ネットワークに接続するデバイスのアクセスが規制されます。また Access Assurance では、802.1X 認証を活用したデバイスに対してはアクセス制御サービス、および 802.1X の許可リストに登録されていない有線 IoT デバイスに対しては MAC アドレスバイパスも提供しています。

製品説明

Juniper® Mist™ Access Assurance は、マイクロサービスベースのクラウドネットワークアクセス制御（NAC）サービスであり、企業はゼロトラストセキュリティモデルを簡単に導入できます。Access Assurance は、従来の NAC 製品に関連する多くの複雑性に関する課題を、以下で解決します。

- オンプレミスサーバーハードウェアの削除
- 本質的に可用性と耐障害性に優れたサービスを提供
- ランタイム時の自動機能更新、セキュリティ、脆弱性修正を有効にする

Access Assurance は、Juniper Mist IoT Assurance の機能を超えて、ヘッドレス IoT および BYOD デバイスのオンボーディングを簡素化します。Access Assurance により、IT チームは、802.1X 認証または MAC 認証バイパス（MAB）方式で、非 802.1X デバイスでも、有線および無線デバイスをオンボーディングできます。

Access Assurance は、X.509 認定書これらのベクトルは、デバイスが接続すべきネットワークセグメントやマイクロセグメント、およびユーザーに動的に適用すべきネットワークポリシーなど、アイデンティティベースのネットワーク 許可基準を決定するのに役立ちます。

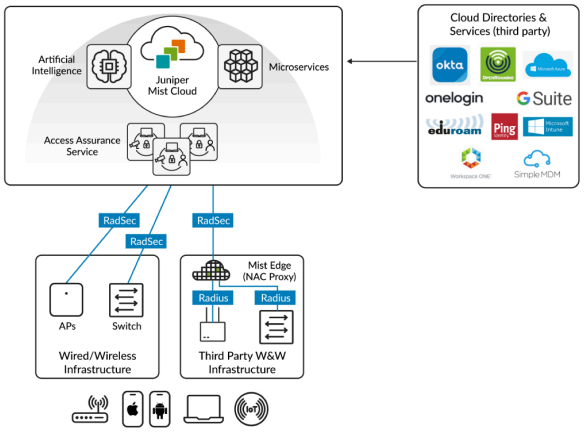

図 1：Juniper Mist Access Assurance クラウドサービスは、ネットワークアクセス制御を大幅に簡素化します。

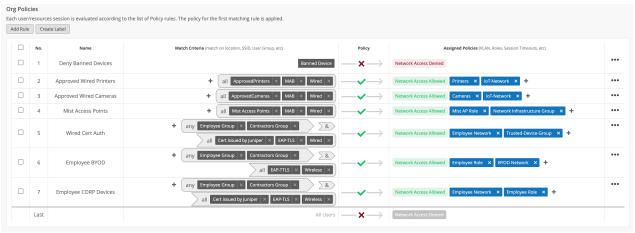

図 2：柔軟なポリシー作成インターフェイスにより、管理者はビジネス要件に基づいてポリシーを割り当てることができます。

ここで最も重要なことは、Access Assurance は、クライアント、ネットワークインフラストラクチャ、アクセス制御の観点から、エンドツーエンドの接続トラブルシューティングを提供してくれるという点であり、Day 2 のサポートが劇的に簡素化されます。IT 管理者は、エンドユーザーエクスペリエンスの一貫したビューを得ることで、エクスペリエンスの質の低下が、クライアント構成、ネットワークインフラストラクチャ、認証、サービスのいずれに起因しているのかを判断することができます。

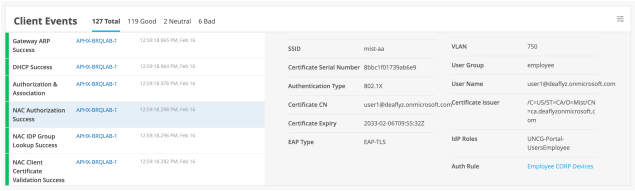

図 3：クライアント SLE は、ネットワークアクセス制御イベントを追跡

アーキテクチャと主要コンポーネント

Access Assurance は、Juniper Mist Cloud を通じて提供され、Mist AI を搭載しています。マイクロサービスアーキテクチャは、高可用性、冗長性、オートスケーリングを組み合わせることで、有線、Wi-Fi、およびワイドエリアネットワーク全体にわたって最適なネットワークアクセスを実現します。地域情報認識を使用して、Access Assurance はさまざまな地域からの認証要求を最寄りの Access Assurance インスタンスに自動的にリダイレクトすることで、遅延を最小限にして最高のエンドユーザーエクスペリエンスを提供します。

Access Assurance は、Google Workspace、Microsoft Azure AD、Okta Identity などの外部ディレクトリサービスと統合された認証サービスを提供します。また、Jamf、Microsoft Intune などの外部公開カギ基盤（PKI）とモバイルデバイス管理（MDM）プロバイダを統合することでユーザーとデバイスのきめ細かい識別を可能にし、アイデンティティベースのゼロトラストネットワークアクセス制御を強化します。

特長とメリット

クライアントエクスペリエンスの優先順位付け

Access Assurance により、クライアント接続エクスペリエンスを一元的に可視化して、容易に問題を特定し、根本的原因分析を実行できます。接続および認証の成功と失敗を含めたすべてのクライアントイベントは、Juniper Mist Cloud にキャプチャされます。このデータは、Juniper Mist Cloud がエンドユーザーに発生している接続上の問題がクライアント構成ミスなのか、ネットワークインフラストラクチャおよびサービス上の問題なのか、あるいは認証ポリシー構成の問題なのかを簡単に特定するのに役立ち、日々の運用が簡素化されます。有線および無線クライアント向け Juniper Mist サービスレベル期待値（SLE）は、認証イベント、証明書検証などのネットワークアクセスイベントも含めるように強化されています。

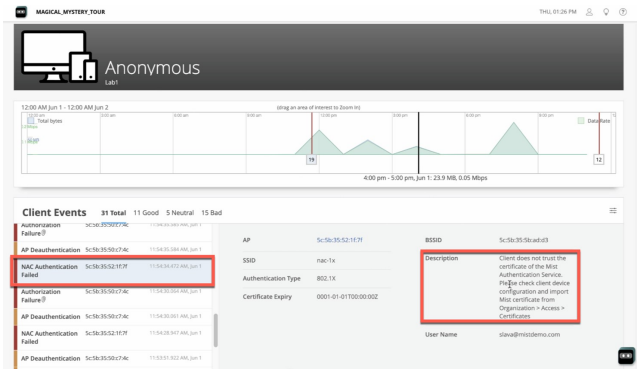

図 4：クライアント SLE 失敗イベントには、既知の問題の説明が記載されています。

管理と運用の一元管理

Access Assurance は Juniper Mist Cloud と密接に統合されており、Wi-Fi Assurance、Wired Assurance、SD-WAN Assurance、Access Assurance のフルスタック管理と日々の運用が単一のダッシュボードに表示されるため、エンドツーエンドの可視化が得られます。Marvis™AI エンジンは、複数のソースからのデータを活用して異常検知を行い、実用的なメトリックを提供します。ダッシュボードを通じて、ユーザーは以下を実行できます。

- 承認済みのデバイスとユーザーのみに対してネットワークアクセスが許可されるようにする、アクセスポリシーを作成し適用する
- ユーザーとデバイスを正しいネットワークセグメントに割り当てる
- ユーザーとデバイスが制限されたリソースにアクセスするのを防止する
- 証明書と認定機関を追加および変更する
- アイデンティティプロバイダを 構成
- 企業全体のクライアントアクティビティを監視する

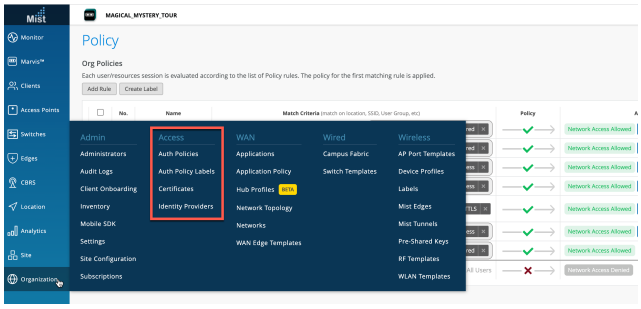

図 5：アクセス制御がハイライトされた、使いやすいユーザーインターフェイス

詳細なユーザーとデバイスのアイデンティティ

Access Assurance では、X.509 認証属性に基づいて、詳細な識別フィンガープリントを実行できます。また、グループメンバーシップ、ユーザーアカウントの状態、MDM コンプライアンス状態、クライアントリスト、ユーザーロケーションなどのアイデンティティプロバイダ（IDP）情報もフィンガープリントに使用し

ます。その結果、ユーザーとデバイスのフィンガープリントが、ゼロトラスト原則の中で正確なポリシー割り当てを行うためのアイデンティティベクトルとなります。

図 6：アイデンティティフィンガープリントは 、複数の方法で実行できます。

ネットワークポリシー強化とマイクロセグメンテーション

ユーザーとデバイスの識別に基づいて、Access Assurance は、特定のネットワークセグメント（VLAN またはグループベースのポリシータグ）にユーザーを割り当てるようにネットワークに指示し、ユーザー役割を割り当てることでネットワークポリシーを適用できます。このような役割は、Juniper Mist の WxLAN ポリシーフレームワークまたはスイッチポリシーで活用できます。

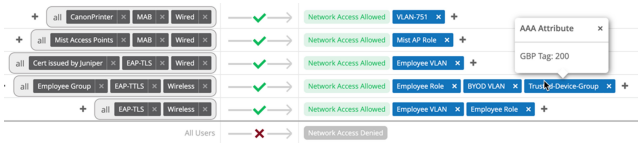

図 7：VLAN、グループベースのポリシー、ユーザーロールに対して適用されているポリシーを簡単に目で確認できます。

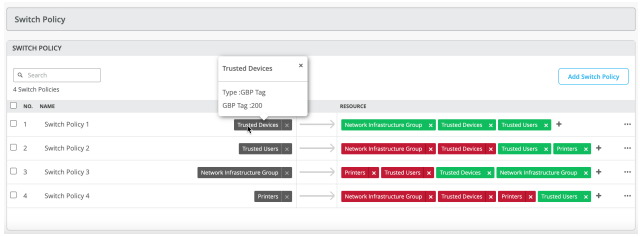

図 8：グループベースのタグでポリシーを認識すると、素早く理解できます。

組み込みの高可用性とジオアフィニティ

Access Assurance を使用することで、企業はシングルサイトおよびマルチサイトの展開において、信頼性が高く低遅延のネットワークアクセス制御を得ることができます。ジュニパーは、ネットワークアクセス制御クラウドサービスのクラウドインスタンスを複数の地域に配置しています。マルチサイト展開では、ネットワークインフラストラクチャから送信される認証トラフィックは、自動的に最寄りの Access Assurance インスタンスへと送信されます。遅延が最小限に抑えられるため、ユーザーは優れた無線エクスペリエンスを楽しめます。この自動化プロセスは、ユーザーに対して完全に可視化されているので、IT 運用チームが操作や監視などする必要はありません。企業は、最寄りの地域インスタンスの状態に関係なく、クライアントデバイスに対して、信頼性の高い冗長ネットワークアクセスを確保できます。

自動機能とセキュリティ更新

Juniper Mist のマイクロサービスベースのクラウドアーキテクチャにより、Access Assurance は最先端テクノロジーで継続的に最適化されます。新機能、セキュリティパッチ、更新が隔週で自動的に Access Assurance に追加されます。サービスの中断やダウンタイムが発生することはありません。この機能により、長時間にわたるソフトウェアアップグレードやサービスのダウンタイムが解消され、ネットワーク IT 管理者のサービス運用が大幅に簡略化および改善されます。ジュニパーは、クラウドベースのサービスに新しい機能を簡単に展開できるため、市場投入が迅速化され、お客様のクライアントからクラウドへのエクスペリエンスを継続的に向上させることができます。

Access Assurance が Juniper Mist の IoT Assurance を拡張

Access Assurance に、Juniper Mist IoT Assurance を組み合わせることで、802.1X 認証による企業デバイスのオンボーディングと、802.1X 非対応 IoT および BYOD デバイスの MAC レスオンボーディングの管理を構築できます。IoT Assurance 機能は IT 運用を簡素化し、複数の事前共有キー（MPSK）メカニズムを介して、ヘッドレス IoT および BYOD デバイスの接続を保護します。MPSK またはプライベート事前共有キー（PPSK）を新しいタイプの識別情報およびポリシーベクトルとして活用するフルセットのアクセス制御機能を搭載しています。

IoT Assurance ではまた、ユーザーのアイデンティティに 基づいて PSK 生成を自動化することで、BYOD オンボーディングのワークフローを実現する PSK ポータル作成も提供しており、Security Assertion Markup Language（SAML）を活用した SSO エクスペリエンスが得られます。クライアントソフトウェアをインストールすることなく、モバイル QR コードを介して、またはパーソナライズされたパスフレーズを入力することで、シームレスなクライアントデバイスのオンボーディングを実現します。

Access Assurance サブスクリプションには、接続方法に関係なく、ネットワーク上のすべてのクライアントとデバイスに対して、簡単なアクセス制御を行う IOT Assurance 機能が含まれています。

仮想ネットワークアシスタント「Marvis」

仮想ネットワークアシスタント「Marvis」は Mist AI を使用しています。IT 運用チームのネットワークの操作などをサポートします。Marvis AI エンジンが、Access Assurance を Wired Assurance、Wi-Fi Assurance、WAN Assurance などの Juniper

Mist クラウドベースのサービスと結びつけてくれるため、運用チームはトラブルシューティングとパフォーマンス 分析を簡略化して、Self-Driving Network™の実現に一歩近づくことができます。

Mist AI を搭載した機能を使用して、ヘルプデスクの人員やネットワーク管理者は、ネットワークの問題の特定と解決に役立つ Marvis の会話インターフェイスを使用して、自然な言葉で質問するだけで、実用的なインサイトを得ることができます。Marvis はプロアクティブな異常検知を SLE ダッシュボードにもたらします。Marvis Actions を使用することで、スタッフはプロアクティブで実用的なインサイトを得て、フルスタックにわたるネットワーク アクセスの問題を特定し、ユーザーの接続性の問題に対する推奨事項を提供します。これにより、フルネットワークスタックと認証サービス全体をカバーする簡単な根本的原因分析がお客様に提供されます。

ドリブンアーキテクチャ

Access Assurance サービスは、公開されている Representational State Transfer（REST）API に完全に基づいており、構成とポリシー割り当ての両方において、外部のセキュリティ情報およびイベント管理（SIEM）または IT サービス管理システムまたは他のプラットフォームと簡単に統合できます。この API は、ユーザーイベントや外部イベントに基づいてアクションを呼び出す機能だけでなく、クラウドネイティブの Webhook フレームワークを使用する機能も提供します。Juniper Mist プラットフォームでは総合的に、オープン API を使用して 100%プログラム可能であり、補完的なジュニパーアクセス、有線、無線、WAN、セキュリティ、ユーザーエンゲージメント、アセットの可視化で、完全な自動化とシームレスな統合を実現します。

仕様

特長	説明
X.509 証明書の管理	外部 PKI サポート 自動 CRL/OSCP 証明書失効チェック
外部アイデンティティプロバイダとの統合	ユーザー検索とデバイスの状態情報を取得するために、任意のアイデンティティプロバイダと統合できるように以下のプロトコルがサポートされています。 • セキュア Lightweight Directory Access Protocol (LDAP) • OAuth2 • eduroam セキュアネットワークアクセス • 主要な統合エンドポイント管理（UEM）、エンタープライズモビリティ管理（EMM）、モバイルデバイス管理（MDM）ツールのために、統合が継続的に追加されました。
802.1X 認証方式	セキュアな 802.1X アクセスでは、以下の EAP 方式がサポートされています。 • Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) • Protected Extensible Authentication Protocol PEAP TLS Tunnel • Extensible Authentication Protocol (TEAP) (TLS/TLS) Extensible Authentication Protocol-Tunneled TLS (EAP-TTLS (PAP)
非 802.1X 認証方式	MAC Authentication Bypass (MAB) Multi Pre-Shared Key (MPSK)
ネットワークポリシーとマイクロセグメンテーション	ユーザー識別情報に基づいた VLAN、ロール、グループベースポリシータグの動的な割り当て
サードパーティネットワークインフラストラクチャのサポート	Mist Edge Auth Proxy アプリケーションを介してサポートされており、サードパーティベンダーのデバイスは、標準の RADIUS を介して Mist Edge Auth Proxy と通信可能
Juniper Mist IoT Assurance（Access Assurance サブスクリプションに含まれます）	IoT および BYOD クライアントデバイスのオンボーディング • PSK および MPSK の作成、ローテーション、自動失効 • ダイナミックトラフィック制御 • キーベースの WxLAN ポリシー • パーソナル WLAN の作成と管理 • PSK ごとのアクティブ デバイス使用追跡 • カギの自動プロビジョニングとローテーション

注文情報

Access Assurance サービスは、7 日間にわたって確認された、同時にアクティブになったクライアントデバイスの平均数に基づいて、サブスクリプションとして提供されます。

スタンダードサブスクリプションには、Juniper Mist Cloud 内のすべてのネットワークアクセス制御機能が含まれています。

アドバンストサブスクリプションでは、クライアントポスチャチェック（UEM/EMM/MDM）とファイアウォール統合が、標準の Access Assurance 機能に追加されます。

SKU	説明
S-CLIENT-S-1	スタンダードアクセスと IOT Assurance サブスクリプション（1 クライアント 1 年間）
S-CLIENT-S-3	Standard Access Assurance と IOT Assurance サブスクリプション（1 クライアント、3 年間）
S-CLIENT-S-5	Standard Access Assurance と IOT Assurance サブスクリプション（1 クライアント、5 年間）
S-CLIENT-A-1	Advanced Access と IOT Assurance サブスクリプション（1 クライアント、1 年間）
S-CLIENT-A-3	Advanced Access と IOT Assurance サブスクリプション（1 クライアント、3 年間）
S-CLIENT-A-5	Advanced Access と IOT Assurance サブスクリプション（1 クライアント、5 年間）

ジュニパーネットワークスについて

ジュニパーネットワークスは、接続性は、優れた接続を経験するのと同じではないと考えています。ジュニパーの AI ネイティブネットワーキングプラットフォームは、AI の機能を AIOps レイヤーとジュニパーのシステム全体で活用できるように、最初から構築されています。リアルタイムの障害分離、事前対応型の異常検知、自動是正措置などにより、キャンパス、支社/拠点、データセンター、WAN の運用に対して、予測性、信頼性、セキュリティをレベルアップします。詳細については、ジュニパーネットワークス （www.juniper.net/jp/ja）をご覧ください。また、X（Twitter）、LinkedIn、Facebook でもジュニパーをフォローしてください。

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号： 888.JUNIPER (888.586.4737)
または +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
日本, 東京本社
ジュニパーネットワークス株式会社
〒 163-1445 東京都新宿区西新宿 3-20-2
東京オペラシティタワー 45 階
電話番号： 03-5333-7400
FAX：03-5333-7401
www.juniper.net/jp/ja/