BIG-IP v21.1 新機能のご紹介

F5ネットワークスジャパン合同会社

2026/5/19

Agenda

BIG-IP v21.1におけるF5システムアップデート

BIG-IP v21.1におけるソフトウェア・モダナイゼーション

BIG-IP LTM v21.1

BIG-IP DNS v21.1

BIG-IP Advanced WAF v21.1

BIG-IP Zero Trust Access (APM) v21.1

BIG-IP SSL Orchestrator v21.1

BIG-IP v21.1に関する重要な詳細情報

1

ハードウェアサポート

BIG-IP v21.xおよび今後のリリースはrSeries、VELOS、およびBIG-IP VEでのみ利用可能であり、**iSeriesまたはVIPRIONではサポートされていません。**

2

ソフトウェアライフサイクル

BIG-IP v21.1および今後のすべての**LTSリリースでは、ソフトウェアライフサイクルが3年** (従来は4年)に移行し、F5はより多くのエンジニアリングリソースを現在および将来のリリースに集中させることができるようになります。

3

BIG-IQサポート

BIG-IQとBIG-IP v21.1の相互運用性は、2026年5月リリース予定の次期バージョンv8.4.2で提供される予定です。

v21.1主な機能進化

Post-Quantum Cryptography (PQC)

- 複数の ML-KEM + SecPハイブリッド 暗号をサポート
- 耐量子TLS/SSL VPNトンネリング

AI ワークロードの配信とセキュリティ

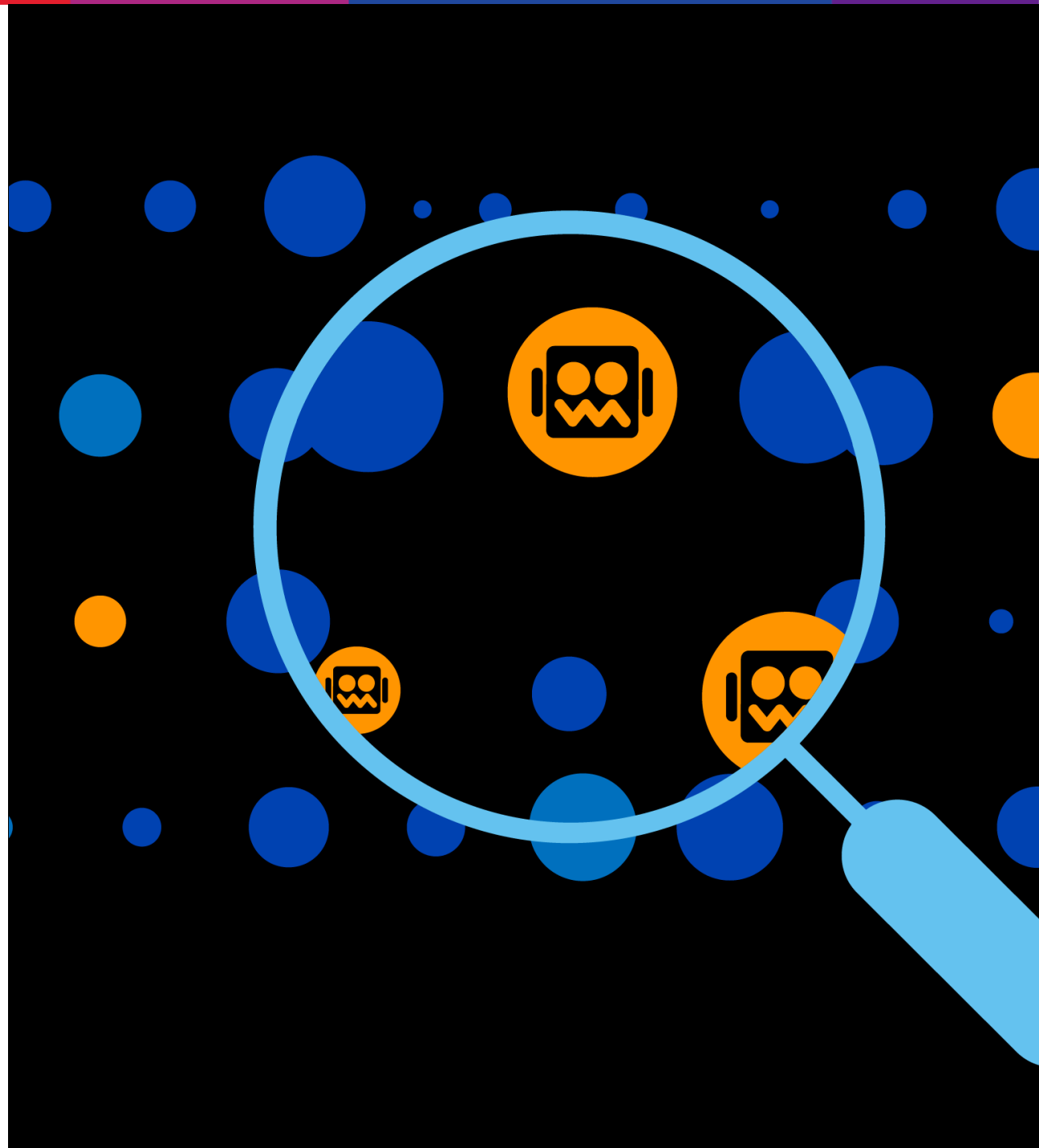
- MCPプロトコルの保護およびセッションパーシステンス
- Dynamic Client Registration (DCR)によるエージェント型AIのアクセスの高速化
- エージェント間の接続性を最適化するためのA2Aプロトコルサポート(実験的機能)

モダンAPIとプロトコルの保護

- HTTP/3トラフィックのための高度なセキュリティ
- OpenAPI Spec 3.1で定義されたAPIの保護

BIG-IP TMOS モダナイゼーション

- 新しいBIG-IPの宣言型API (アルファ版)
- 継続的なコントロールプレーンの改善
- ‘In-place’でのBIG-IPソフトウェアアップグレード



BIG-IP v21.1におけるF5システムアップデート

VELOS/rSeriesでのポスト量子TLS対応の加速

- **ポスト量子暗号 (PQC)への対応**
  - 従来型アルゴリズムと量子耐性アルゴリズムを組み合わせたハイブリッドTLS鍵交換に対応し、将来を見据えたセキュリティを実現
- **ハードウェアベースの高速化**
  - Intel QuickAssistテクノロジー (QAT)は、暗号化ハンドシェイクを高速化し、CPU使用率を削減しながらVELOSおよびrSeriesのパフォーマンスを維持
- **ポスト量子TLSの導入を簡素化**
  - アーキテクチャの再設計を必要とせずにポスト量子TLSを選択的に導入でき、プラットフォームの統合性と拡張性を維持
- **パフォーマンスとセキュリティのバランス**
  - 要求の厳しい大規模TLSセッション終端処理において、強力な暗号化と高いアプリケーションパフォーマンスのバランスを実現

VELOS/rSeriesにおけるX25519 (PQC)のQATアクセラレーション

顧客課題

組織は「harvest now, decrypt later」というリスクに備えるよう迫られており、特に顧客記録、決済データ、知的財産、重要なビジネス通信など、長期保存される機密データを含むトラフィックについてはその必要性が顕著です。X25519とMLKEM768を組み合わせたハイブリッドTLSアプローチが、現実的な解決策として浮上しています。

- ポスト量子脅威への備えとして、組織は今すぐ機密トラフィック向けにハイブリッドTLS鍵交換の導入を開始する必要があります。
- X25519MLKEM768などのハイブリッド鍵交換方式は、ハンドシェイクの複雑さを増し、大規模な環境ではCPU負荷、遅延、運用上のオーバーヘッドを増加させる可能性があります。
- セキュリティチームには、アプリケーションのパフォーマンスと可用性を維持しつつ、クライアントとの互換性を確保できる移行パスが求められています。

F5ソリューション

- QATアクセラレーションを搭載したF5 rSeries/VELOSは、TLSハンドシェイクに関連する暗号処理 (X25519)をオフロードして高速化し、CPUリソースへの負荷を軽減するとともに、大規模なセキュアなアプリケーション配信の効率を向上させます。
- Intel QATはTLSハンドシェイクの高速化を含む、セキュリティ、認証、および暗号化ワークロード向けのハードウェアアクセラレーションです。
  - QATアクセラレーションにより、rSeries/VELOSではセキュアなハンドシェイクに関連する暗号処理をオフロードし、顧客がハイブリッドPQC/TLSを導入する際にも、スループットと効率を維持するのに役立ちます。
  - 大規模かつ高性能な環境向けに構築されたモジュール式ADCプラットフォーム上で、ポスト量子対応のTLSを導入できます。
  - 新たなポイントソリューションを導入したり、システム統合を損なったりすることなく、暗号技術の俊敏性を高め、量子コンピューティングへの移行に備えることが可能になります。

レガシーハードウェア上のアップグレードワークフローを保護

- **レガシーハードウェア向けアップグレード保護機能**
  - iSeriesおよびVIPRIONハードウェア上でサポート対象外のソフトウェアが起動するのを防ぎ、アップグレードの失敗や停止を軽減
- **自動プラットフォーム互換性チェック**
  - 起動時に互換性チェックを実行し、混在環境でのアップグレード時に発生する手動操作によるエラーや認知負荷を軽減
- **戦略的な移行計画**
  - rSeriesやVELOSなどの次世代プラットフォームへの移行を計画しながら、サポート対象の旧バージョンを実行
- **運用安定性の向上**
  - アップグレードがサポート対象の予測可能なパスに沿って実行されることを保証し、コンプライアンスと安定性を向上

iSeries/VIPRIONでのBIG-IP v21.1インストールのブロック

顧客課題

- レガシーなiSeriesおよびVIPRIONプラットフォームを運用しているお客様は、サポート対象外のBIG-IP 21.xをインストール、起動することを確実に回避する手段が必要です。
  - こうした行為はアップグレード時の混乱、運用の中断、およびメンテナンス期間中の不必要なトラブルシューティングを引き起こす恐れがあります。
  - F5のサポートマトリックスには、BIG-IP 21.xはiSeriesおよびVIPRIONではサポート対象外であることが明記されています。
  - iSeries/VIPRIONではBIG-IP 21.xがサポートされていないにもかかわらず、これらのプラットフォームにBIG-IP 21.xを導入しようとするリスクが存在します。
- マルチプラットフォーム環境では、適切なアップグレード対象を徹底し、無効なソフトウェアとハードウェアの組み合わせを回避することが困難になります。
- レガシーハードウェアから次世代プラットフォームへの移行を計画する間、サポート対象のリリースを維持する必要があります。

F5ソリューション

iSeriesおよびVIPRIONシステムでのBIG-IP v21.xの起動をブロックし、サポート対象外のハードウェア構成でのソフトウェアバージョンの実行を防ぐ組み込みの保護メカニズムを提供します。

- サポート対象外のアップグレードや運用上の混乱を回避できます。
- プラットフォーム移行の準備を進める間も、レガシーハードウェア上ではサポート対象の17.xリリースを使い続けることが可能です。

Cloud-InitによるF5OSテナントのオンボーディング

- **自動化された”Day-0”オンボーディング**
  - Cloud-initのサポートにより、F5OSプラットフォーム上でBIG-IPテナントを初回起動時に自動的かつ一貫して初期化でき、手作業を削減
- **テナントプロビジョニングの簡素化**
  - 認証情報やシステム設定などの事前定義されたパラメータにより、テナントを安全かつ一貫して起動できるため、導入時の信頼性が向上
- **運用効率とセキュリティ**
  - 自動化されたオンボーディングによって導入時間を短縮し、再現性を向上
  - デフォルトの認証情報を排除することでセキュリティを強化
- **DevOpsプラクティスとの統合**
  - Infrastructure as Code (IaC)およびCI/CDパイプラインをサポートし、BIG-IPのプロビジョニングを最新の自動化ワークフローとシームレスに統合

※本機能はF5OS 2.0 (Q2CY26リリース予定)でサポート

Cloud-InitによるF5OSテナントのオンボーディング

顧客課題

- rSeries/VELOSでのBIG-IPテナントのプロビジョニングでは、テナントの作成、ネットワーク設定、サービス設定がF5OSでの管理作業となるため、テナント作成後に複数のデプロイ後手順が必要になることがあります。
- テナントはF5OSプラットフォーム層にデプロイされ、その後はWebUI、CLIまたはAPIを通じて、標準的なBIG-IPインスタンスと同様に管理されます。
  - rSeriesおよびVELOSにおけるF5OSテナントのデプロイでは、テナント作成後に複数の手動による初期設定手順が必要になる場合があります。
  - クラウドやInfrastructure-as-Code (IaC)のワークフローに整合した、より迅速で再現性のある「自動化されたテナントオンボーディング」を求めています。
  - 手動による初期設定は運用上のオーバーヘッドを増大させ、大規模なテナントデプロイの標準化を困難にします。

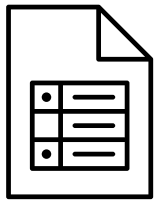
F5ソリューション

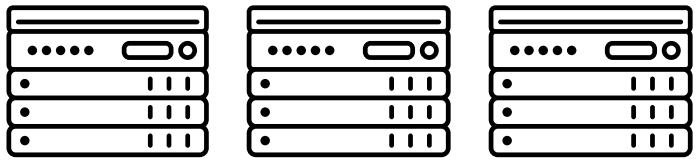
rSeries/VELOS上のF5OSテナントに対するCloud-initのサポートにより、初回起動時にユーザーデータに基づくオンボーディングでBIG-IPテナントを初期設定できるようになり、クラウドスタイルのブートストラップモデルを導入できます。

- 初回起動時のオンボーディングが効率化されます。(例: テナントを起動する際に(デフォルトではない)ユーザーが選択した安全なユーザー名とパスワードを設定)
- 手動での設定手順が削減され、セキュリティが強化されるほか、デプロイメントワークフローの一環としてテナントのブートストラップを自動化できるようになります。
- F5OSテナントがCI/CD、IaCおよびプラットフォームエンジニアリングの運用モデルに、より適したものとなります。

注: 本機能はF5OS 2.0 (Q2CY26リリース予定)でサポート

UCSベースのF5OS BIG-IPターゲットへの移行を簡素化





- **移行ワークフローの強化**
  - UCSベースの移行ワークフローを改善し、新しいF5OSテナントに移行元の構成をシームレスに読み込み可能
- **互換性レポート**
  - プラットフォームが構成オブジェクトの互換性の有無を識別し、詳細な事前レポートとdry-runレポートを提供
- **移行リスクの軽減**
  - 移行前の可視性によってより適切な計画を立てることができ、構成の違いに伴うリスクを軽減
- **運用継続性**
  - 移行レポートをBIG-IP内に統合することで移行期間を短縮
  - モダナイゼーション中の運用継続性を維持

UCSベースのF5OS BIG-IPターゲットへの移行を簡素化

iSeries/VIPRIONのUCSファイルを、新しいF5OSベースのBIG-IPにロードする際のレポート機能を提供

顧客課題

iSeries/VIPRIONからF5OSベースのBIG-IPテナントへ移行するお客様は、ハードウェアモデル、プラットフォームアーキテクチャ、インターフェース、ネットワーク構成の違いを考慮しつつ、元のUCSベースの設定を可能な限り維持する必要がある場合があります。

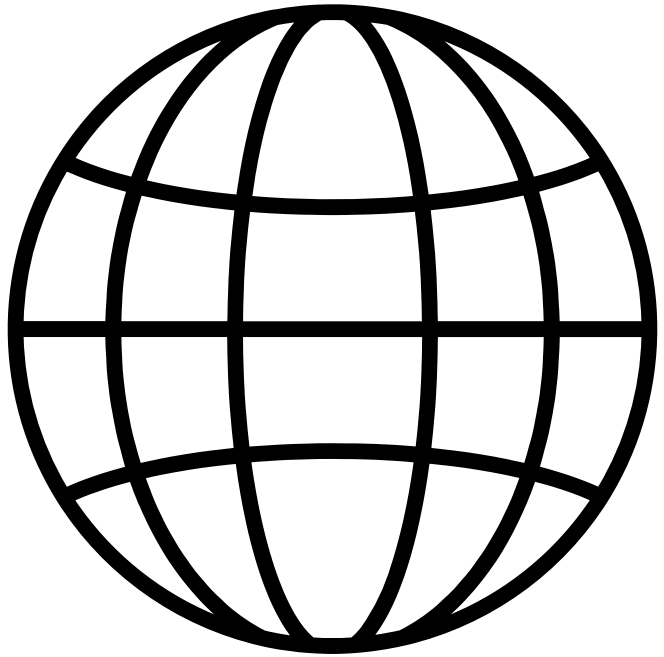
- サービスを手動で再構築するのではなく、UCSベースの設定を再利用したいと考えています。
- インターフェース、トランク、VLAN割り当て、管理設定などのハードウェア固有のオブジェクトは必ずしもF5OSテナントに直接変換できるとは限らないため、クロスプラットフォームの移行が失敗したり、手直しが必要になったりすることがあります。
- 移行に成功したもの、無視されたもの、およびカットオーバー前に修正が必要なものについては、明確なレポートを必要とする場合があります。

F5ソリューション

- UCSベースのプラットフォーム移行ワークフローを使用して、iSeriesやVIPRIONのソースUCSオブジェクトを、rSeriesやVELOS上のF5OS BIG-IPテナントに読み込むことが可能です。
- platform-migrateオプションが機能強化され、旧プラットフォームからF5OSテナントを含む新プラットフォームへの移行において、事前チェックおよびドライランのレポート機能を提供するようになりました。
  - UCSベースの移行ワークフローを使用して、レガシープラットフォームからrSeriesやVELOSテナントへ、ソースUCSオブジェクトをロードすることをサポートしています。
  - 強化されたplatform-migrateユーティリティは、今後”Journeys”ツールを廃止するのに伴って、BIG-IP上でオンボックスレポート機能を提供します。
  - platform-migrateプロセスは、互換性のある設定を保持しつつ、サポートされていないプラットフォーム固有のオブジェクトは無視することで、手動での再構築作業を軽減します。

802.1 Q-in-Q Tagging

マルチテナント・セグメンテーションの拡張



- **Q-in-Q Double VLAN Tagging**
  - 802.1 Q-in-Q Taggingは、プロバイダVLAN内に顧客VLANをカプセル化することで、重複するIDを競合なく使用可能
- **プラットフォームレベルのVLAN処理**
  - F5OSプラットフォームはホスト層でVLANタギングを処理し、一貫性のあるスケーラブルなマルチテナントセグメンテーションを実現
- **サービスプロバイダにとってのメリット**
  - Q-in-Qにより、サービスプロバイダは番号変更なしで複数の顧客VLANを伝送でき、柔軟性と分離性が向上
- **ネットワークアーキテクチャの改善**
  - 最新のクラウドおよびデータセンターに適した、標準ベースのスケーラブルなマルチテナンシーアプローチを提供

rSeries/VELOSでの802.1 Q-in-Q taggingサポート

顧客課題

- サービスプロバイダーや大規模なマルチテナント環境では、重複するVLAN IDの再割り当てを顧客に強いることなく、共有インフラストラクチャ上で顧客のVLANを運用する必要がある場合がよくあります。
- 単一のフレームに複数のVLANタグを挿入する方法として、IEEE 802.1QinQ (Q-in-Q/double-tagged)があります。実用的なVLANスペースが”4096”から”4096×4096”に拡張され、プロバイダーが管理する外側のタグ内で独自のVLAN IDを維持できるようになります。
  - 顧客は、番号の再割り当てを強制したりセグメンテーションを放棄したりすることなく、共有インフラストラクチャ全体で重複する顧客VLANを運用する必要があります。
  - rSeries/VELOSではVLAN TaggingはF5OS層で処理されるため、高度なVLANユースケースには、テナント固有の設定ではなく、プラットフォームネイティブなサポートが必要です。
  - サービスプロバイダーおよびマルチテナント環境では、F5プラットフォーム全体でVLANベースの分離を拡張するためのスケーラブルな方法が必要です。

F5ソリューション

rSeries/VELOSでのQ-in-Q Taggingサポートにより、F5OSベースのプラットフォームでdouble-tagged VLANの処理が可能となり、共有インフラストラクチャを介した転送には外側のサービス/プロバイダータグを使用しつつ、内部の顧客VLAN識別子を保持できるようになります。

- タグ付けはテナント内部ではなく、F5OSのネットワークモデル (F5OS内で処理)に準拠しています。
- rSeriesおよびVELOSにおけるサービスプロバイダー、プライベートクラウド、およびマルチテナントのセグメンテーションといったユースケースへの適合性が向上します。

プロトコルごとのRRDAGでトラフィック分散を改善

きめ細かなトラフィック制御

処理コア間でのトラフィック分散を精密に制御し、パフォーマンスを向上

ラウンドロビン負荷分散

RRDAGはパケットをラウンドロビン方式で均等に分散し、エントロピーの低いトラフィックにおける負荷の不均衡を解消

最適化された大規模パフォーマンス

トラフィック分散の改善によってリソース利用率が向上し、高スループットワークロードにおけるパフォーマンスの予測可能性を向上

簡素化された設定

複数のプロトコルが混在する環境における設定を簡素化し、運用上の柔軟性を向上

rSeries/VELOS: プロトコルごとにRRDAGを設定

顧客課題

- rSeriesおよびVELOS上で大規模なワークロードを実行しているお客様は、着信トラフィックのエントロピーが低く、標準のDAGハッシュ処理によって一部のコアに過大な負荷が集中してしまう場合、利用可能なTMMコア全体にトラフィックを均等に分散させるためのより適切な方法を必要としています。
- DAGはTMMインスタンス間でトラフィックを分散させるメカニズムで、特にRound Robin DAG (RRDAG)は、IPアドレスやポートにエントロピーが乏しいコネクションレスパケットに対して有用です。
  - rSeriesおよびVELOS上の一部のワークロードでは、トラフィックのエントロピーが低い場合、TMMコア間でトラフィックが均等に分散されず、ホットスポットの発生やパフォーマンスの低下を招いています。
  - 既存のRRDAGに関するガイダンスは主にUDPに特化しており、UDPプロファイルの変更、UDPポートリストの設定、VLANレベルの設定など、複数の設定手順を必要とします。
  - お客様は、プロトコル種別に基づいて代替のトラフィック分散動作を適用するための、よりシンプルできめ細かな方法を求めています。

F5ソリューション

- プロトコル単位でのRRDAG設定をサポートすることで、rSeries/VELOSでトラフィック分散の適用方法をより精密に制御することが可能になります。
- DAGモードによって着信トラフィックがTMM間でどのように分散されるかを決定し、低エントロピーのトラフィックパターンに対処するためにRRDAGが使用されるという、F5の既定のモデルを拡張したものです。
  - プロトコルごとのRRDAG設定により、お客様はrSeriesおよびVELOSにおけるトラフィックの分散方法をよりきめ細かく制御できるようになり、トラフィック誘導の挙動をワークロードの特性に適合させることが可能になります。
  - UDPのみを対象とした限定的な運用制御の枠を超え、混合プロトコル環境におけるポリシーを簡素化します。
  - F5がすでにBIG-IPテナント向けにDAG関連のトラフィック分散チューニングを提供しているVELOSおよびハイエンドのrSeriesプラットフォームにおいて、特に有用です。

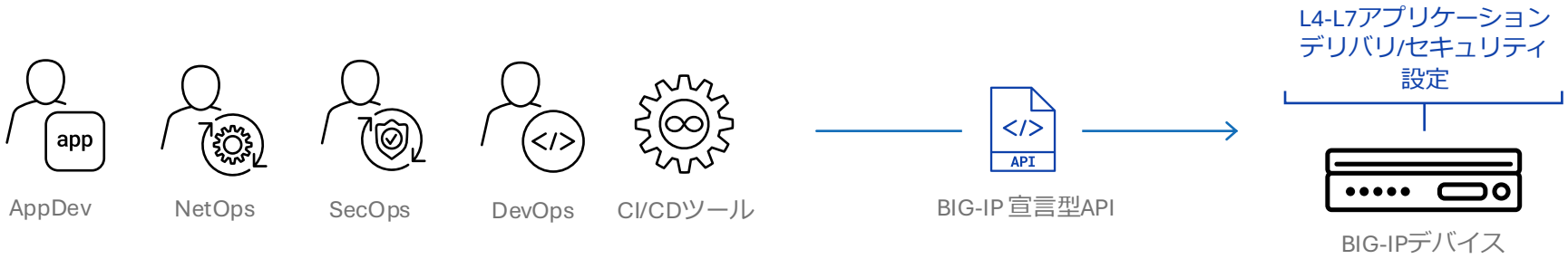
BIG-IP Virtual Edition v21.1: 主な機能強化 (Microsoft Azure)

- **WALinuxAgentパッケージをv2.2.53.1へアップグレード**
  - 以前のソフトウェアバージョンにはWALinuxAgentバージョン2.2.48.1が同梱されていましたが、これは現在サポート終了となっています。
  - 2022年7月、Microsoft Azureは今後サポートされる最小バージョンがv2.2.53.1となることを発表しました。これにより、Microsoft Azureとの継続的な互換性を確保するためには、このアップグレードが必須となります。

BIG-IP v21.1におけるソフトウェア・モダナイゼーション

新しいBIG-IP宣言型API(アルファ・リリース)

宣言型: システムに**何が**欲しいかを伝え、あとはシステム自身が**どのように**実現するかを把握



新しいBIG-IP宣言型APIとは?

- L4-L7アプリケーションサービスの構成を自動化する、アプリケーション中心のAPI
- 最も動的なアプリケーション環境をサポートするため、大規模な高性能自動化を実現するように設計
- BIG-IPにネイティブに統合され、JSONベースのAPIスクリプトを介してアクセス可能

「宣言型」の「命令型」に対する利点

- BIG-IPに関する専門知識の必要性を低減
- 人的ミスを最小化
- 設定の一貫性と再現性を最大化
- 大規模な自動化を容易に実現

注: v21.1ではBIG-IP LTMとDNSのみをサポート。その他のモジュールは将来対応予定。

AS3と新しいBIG-IP宣言型APIの比較

動的で高度にオーケストレーションされたアプリケーション環境での使いやすさを考慮して設計

AS3		BIG-IP宣言型API (New!)
iAppsLXフレームワーク内で動作 （設定の反映はtmshスクリプトに依存）	→	BIG-IP TMOS内でネイティブに動作 (MCPD/iControlを介して、BIG-IP TMOSと直接通信)
設定の実装速度は中程度	→	ほぼ瞬時に設定を実装
BIG-IPワークフローの自動化範囲は限定的 (約20%)	→	BIG-IP機能の100%を自動化可能
「テナント」中心のモデル	→	「アプリケーション」中心のモデル + 高い拡張性
設定情報の”Source of Truth”競合の可能性あり (AS3定義はBIG-IP外部のJSONドキュメントに存在)	→	単一の権威ある構成により、”Source of Truth”問題を回避
RBAC非サポート (adminのみ)	→	BIG-IPのネイティブのRBAC機能を利用可能
BIG-IPとは異なるライフサイクル管理	→	BIG-IPソフトウェア・リリースに連動したライフサイクル

新しいBIG-IPの宣言型API(アルファ)

顧客課題

AS3は宣言型の自動化の方法によりBIG-IPの自動化を革新しましたが、様々な課題に直面してきました。

- **機能カバレッジの制限:** AS3で現状BIG-IP TMOSの操作の約20%を自動化できるのに対し、iControlは約90% を自動化できます。またAS3のパフォーマンスと応答性は、大規模な導入環境では遅延が発生する可能性があります。
- **テナント中心のアーキテクチャ:** AS3はテナント重視の設計となっており、実際の導入環境で必要とされるパフォーマンス、柔軟性、スケーリングに対応したアプリケーション中心のワークフローが制限されます。複数チームでの利用においてはRBAC が必要ですが、AS3ではこれらの制限により提供できません。
- **信頼できる情報源の競合:** AS3の構成はJSONドキュメントとしてBIG-IPデバイス外に保存されるため、AS3とデバイス上の設定の間で設定のドリフトや信頼できる「唯一の情報源 (Source of Truth)」が競合する可能性があります。これらのドキュメント/宣言は、数百ものアプリにわたる場合があり、ミスが起こりやすく、検証に時間がかかり、デバッグも困難で、バージョン管理が困難という課題があります。
- **ライフサイクル管理:** AS3はBIG-IPデバイス上に個別インストールが必要な拡張機能であり、Gitを介した個別のインストールと定期的な更新が必要です。さらにTMUI/TMSH/CLIに慣れたユーザーには、学習コストが高いという課題があります。

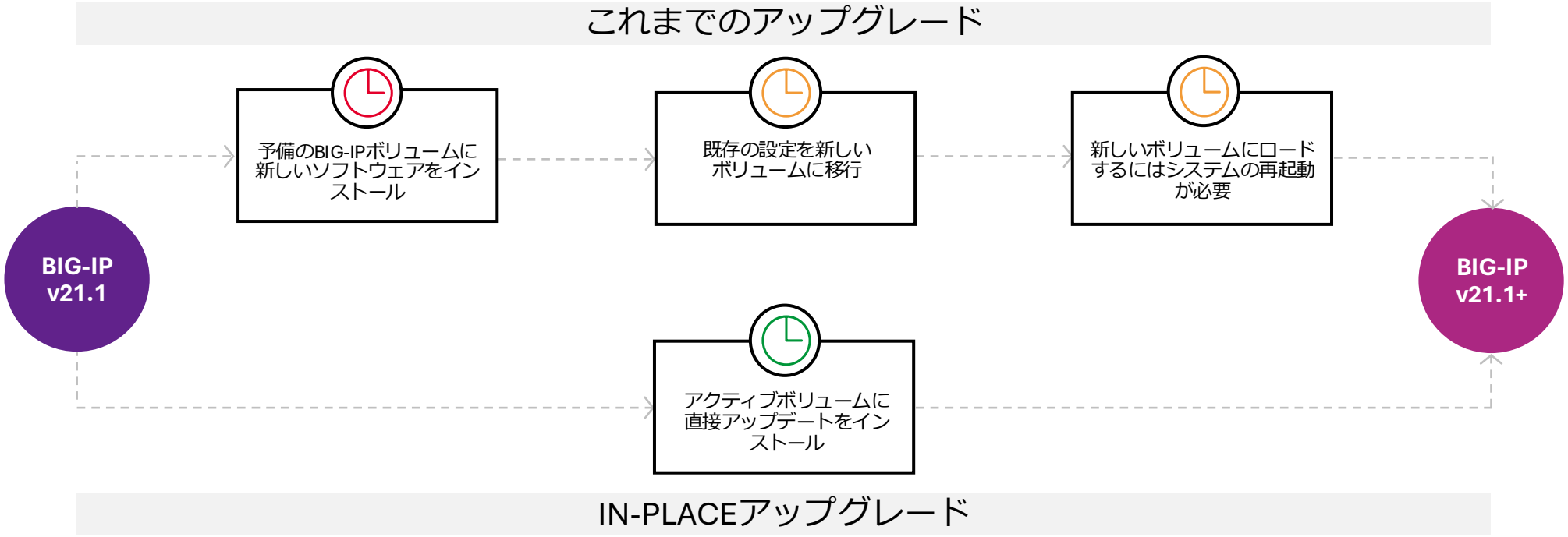
F5ソリューション

新しいBIG-IP宣言型APIを導入し、シンプルな宣言構造、簡易な検証、明確なエラーメッセージを提供することでAS3の課題を解決し、使いやすさを向上させます。

- **自動化の組み込み:** BIG-IP宣言型APIがBIG-IPソフトウェアにネイティブに統合されたため、”Source of Truth“の問題や外部拡張機能の管理が不要になりました。
- **アプリ単位でスケーラブルなモデル:** テナントモデルを廃止し、アプリケーション毎のAP I(より小さく、簡単で安全)へ移行します。大規模な構成を小さく再利用可能な構成 (プロファイル、プール、プロトコル)に分割し、ラベル付きアプリケーションのグループ化も含みます。
- **拡張されたワークフローのサポート:** すべてのソフトウェア モジュールに対して、幅広いBIG-IPのワークフローとユースケースにわたる包括的な自動化を可能にします。 (注: v21.1ではLTMとDNSのみ対応)
- **パフォーマンスの向上:** アプリ中心のアーキテクチャはより高速でスケーラブルなコントロールプレーンの操作を可能とし、デプロイメントや構成変更を300秒未満で実行できます。
- **BIG-IPとの即時互換性:** AS3のように対応が遅れるのではなく、新しいBIG-IPソフトウェアバージョンがリリースされると同時に、新しいTMOSの機能を即座にサポートします。

注: 本機能は現時点で正式サポートされておらず、GAもされておりません。初期ユーザーのフィードバックを集めるためのアルファ版として提供されます。

‘in-place’でのBIG-IPソフトウェアアップグレード/パッチ適用



影響を受けるソフトウェアコンポーネントのみをアップグレードし、**アクティブ**なBIG-IPボリュームに直接インストール

アップグレードとパッチ適用の**迅速化**
メンテナンス期間の**短縮**
アプリケーションのダウンタイムの**削減**

注:
- In-placeアップグレードはBIG-IP v21.1xの特定のEHFのみで適用可能
- 新しい”dry-run”機能により、どのアップグレードパスでもin-placeアップグレードが可能かどうかをユーザーに通知し、アップグレードを実行する前にその影響を評価可能

‘in-place’でのBIG-IPソフトウェアアップグレード/パッチ適用

顧客課題

BIG-IPのお客様は、これまで以下のようなソフトウェアアップグレード上の課題に直面していました。

- **アップグレード時間の長さ**: ソフトウェアコンポーネントの変更がごくわずかであっても、多くの不要なアップグレード用RPMパッケージをインストールする必要がありました。これにより、アップグレード時間が大幅に延長され、多くの場合、合計で数十分を要していました。
- **アプリケーションのダウンタイム**: ダウンタイムを防止するためのHA構成が導入されていない環境では、ソフトウェアアップグレードによって長時間のサービス停止が発生し、相当なメンテナンス時間が必要になる場合がありました。

F5ソリューション

BIG-IP v21.1以降で”インプレース”ソフトウェアアップグレードを導入します。

- 影響を受けるソフトウェアコンポーネント (RPMパッケージ)とその必要な依存関係のみを対象とし、完全な再インストールやシステム再起動を必要とせずに、アクティブボリュームに直接インストールします。
- **アップグレードの高速化、メンテナンス時間の短縮、ダウンタイムの削減**が実現します。

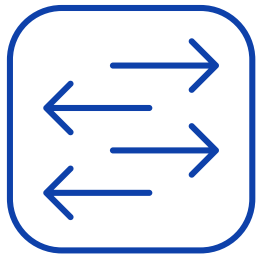
注:

- 初期リリースでは、インプレースアップグレードは特定のEngineering Hot Fix (EHF)のみに対応しており、ほとんどのお客様はv21.1ではこの機能を利用できません。今後、サポートされるアップグレードパスは順次拡大していく予定です。
- v21.1では、アップグレードを実行する前に影響を評価できる新しい”dry-run” 機能も追加されています。この機能は、選択したイメージをアクティブボリュームで現在実行されているバージョンと比較し、システムがシステム再起動を伴わないインプレースアップグレード、システム再起動を伴うインプレースアップグレード、または従来の完全なアップグレードに対応しているかどうかを判断します。

コントロールプレーンの3つのアップグレード

回復力と効率性が向上

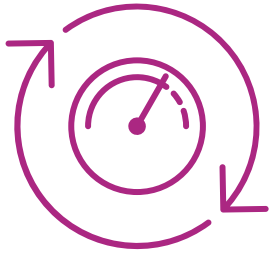
1



BigDのマルチスレッド処理

モニタリングの拡張性を向上させ、
CPU/RAMの使用率を低減

2



MCPdの耐障害性の向上

システムメモリ不足時における、
制御プレーンの可用性の向上

3

iControl REST APIのパフォーマンス向上

エンドツーエンドの設定時間を
最大10%短縮

説明:

- ***Master Control Program Daemon (MCPd)*** - 設定を管理し、*BIG-IP*コンポーネント間の通信を処理するコア制御プレーンコンポーネント
- ***BigD*** – *BIG-IP*の中核となるヘルスモニタリング・デーモンで、サーバとサービスの継続的なモニタリングを実行し、可用性と健全性の状態を判断

BigDのマルチスレッディングサポート

効果的なコントロールプレーンの監視

顧客課題	• BigDはBIG-IPのCoreなヘルスステータスモニタリングのデーモンで、サーバやサービスの可用性とヘルスステータスを判断するために継続的に監視します。 • BIG-IPデバイスでたくさんのモニターを設定されているお客様 (例えば、5000件の‘in-TMM’モニター または 25000件の通常のモニターが設定されている場合)は、BigDがCPUとメモリを多量に消費しているために、GUIやiControl RESTのアクセスに影響が発生する可能性があります。
F5ソリューション	• v21.1でBigDがマルチスレッディング対応となり、 モニタリングの拡張性が向上し、システムリソースの消費を抑えることができるようになりました。 • 大規模なモニタリングの場合には、 以下の点でコントロールプレーンの応答性と信頼性が向上することが期待されます。 • **BigDのCPUの使用量を最大10%削減** • **BigDのメモリの使用量を最大25%削減**

MCPdの改善: コントロールプレーンの信頼性と効率が向上

顧客課題

MCPdは以前のBIG-IPソフトウェアバージョンで、次のような問題に直面していました。

1. BIG-IPがメモリ不足の状態に陥ると, MCPdのような重要なプロセスが他の機能を優先するために停止してしまうことにより、コントロールプレーンが不安定になったり利用できなかったりする可能性がありました。
2. BIG-IPデバイスを工場出荷状態にリセットする際に、多量のオブジェクトを削除する間の冗長な検証ステップが行われていたために、リセットやシステム設定の再読み込みに必要な時間が延びていました。
3. 起動や設定の読み込みなどのプロセスでは、BIG-IPが設定を読み込み、検証し、有効化する際に一時的にメモリ上で作業用バージョンとして設定オブジェクトを作成する必要がありました。「work_copies」として知られるこれらは、追加のメモリを消費して、プロセスを遅延させる原因となっていました。

F5ソリューション

BIG-IP v21.1にて導入されたMCPdの改善点は以下の通りです:

1. BIG-IPがメモリ不足の状態に陥った場合、MCPdは高い優先度評価 (OOM rating)が割り当てられるようになり、MCPdが動作し続けるように改善され、停止することはなくなりました。
2. BIG-IP v21.1では、検証のステップやパターンのうち多量のオブジェクト削除のために必要ではないものが削除され、結果として設定の読み込みの時間が短縮されました。
3. BIG-IPのデータベースマネージメントシステムであるeXtreameDB はMVCC (複数バージョンを同時実行する制御)機能が備わっており、システムの起動やシステム設定の読み込みに「work_copies」を必要としなくなりました。BIG-IP v21.1でMVCCを利用することで起動や設定の読み込みをより迅速かつ効率的に実行でき、メモリの使用量も削減できます。

iControl REST APIのパフォーマンス向上

顧客課題	• 顧客は急速に変化する動的なアプリケーション環境に対応する必要があり、環境の変化に合わせてBIG-IPの設定を可能な限り迅速に更新する必要があります。 • 極端な状況では、BIG-IPのCPUやメモリの使用量が100%近くなり、コントロールプレーンのパフォーマンスの低下やその他の副作用を引き起こす可能性があります。
F5ソリューション	BIG-IP v21.1では、iControl RESTは以下のように改善しています: • **構成変更の高速化:** iControl RESTのパフォーマンスが向上し、エンドツーエンドの所要時間を最大で10%短縮できるようになり、動的に変化する環境におけるBIG-IPの応答性を向上させることが可能です。 • **リソースの消費を削減:** iControl RESTの効率改善により、CPUのリソースの使用量が最大10%削減され、メモリ使用量もわずかに減少しました。その結果、他のコントロールプレーンの機能のためのリソースを確保できます。

その他の注目すべき改善ポイント

- **iControl REST APIコールのレート制限**
  - BIG-IPのマネージメントプレーンはAPIレート制限を実施していませんが、iControl RESTのクライアントはほとんどが自動化ツールです。このことがリクエストのバーストやDoS、管理とコントロールプレーン全体のパフォーマンスの低下 を引き起こす可能性がありました。
  - v21.1では、管理者がiControl REST APIにレート制限をかけることができ、高負荷の状況であっても管理プレーンの応答性を維持し、管理ポートを狙ったアプリケーションレイヤーのDoS攻撃のリスクを低減させることができるようになりました。

BIG-IP LTM v21.1

「安全な未来」のために量子対応暗号化技術を拡張

F5でのHybrid PQC

BIG-IPがECC + ML-KEM (**SecP256r1ML-KEM-768**および**SecP384r1ML-KEM-1024**)を組み合わせた業界最先端のハイブリッド暗号と、**量子耐性VPNトンネル**をサポート

量子脅威は現実のもの

- 従来の暗号化技術は危機に瀕している。
- 攻撃者はすでに暗号化されたデータを収集し、後で復号化しようとしている。

なぜ重要なのか?

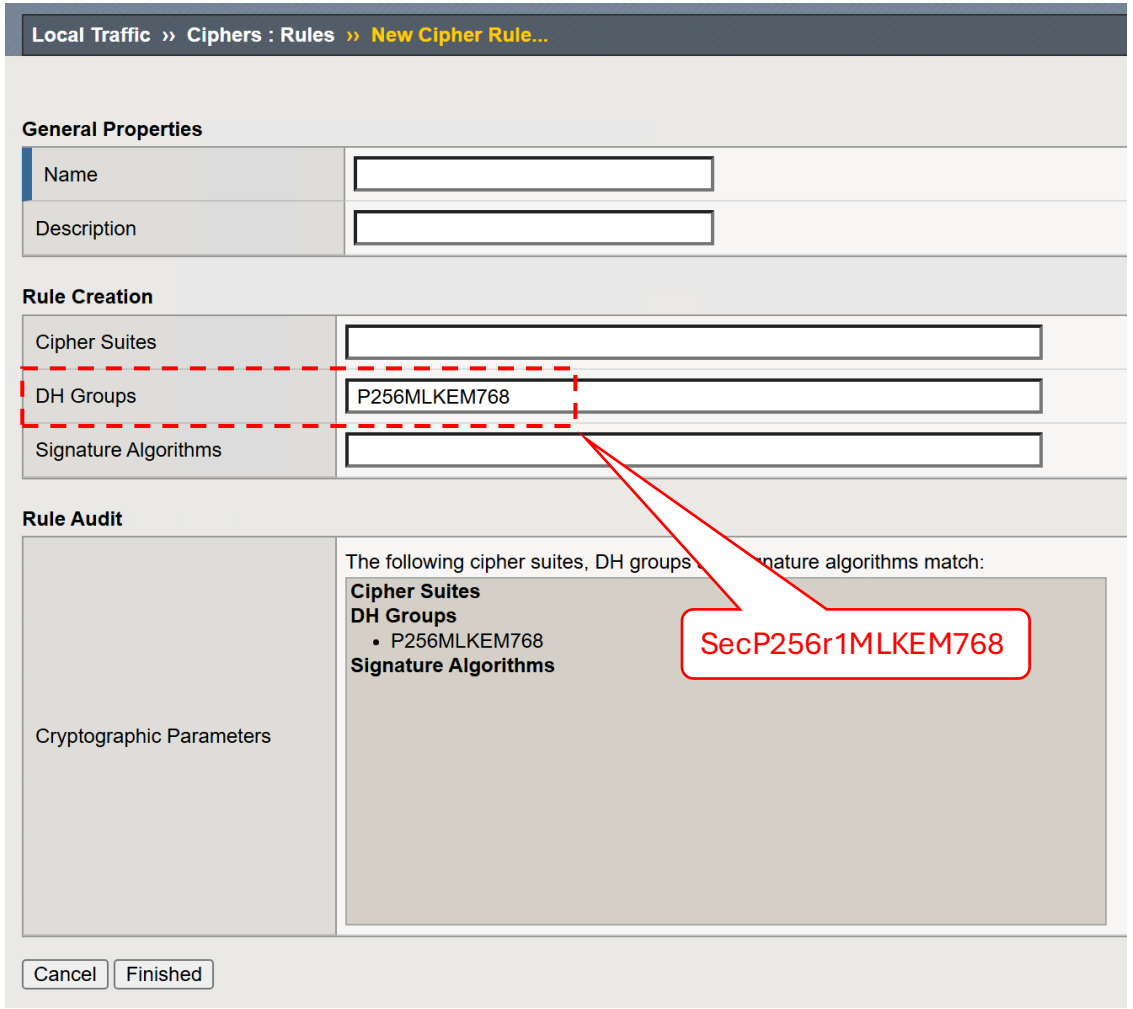
- **将来を見据えたセキュリティ:** “Harvest Now, Decrypt Later (HNDL)”攻撃から防御
- **コンプライアンスへの確信**: NIST, FIPS規格に今すぐ準拠
- **暗号技術の俊敏性**: 将来を見据えた適応性

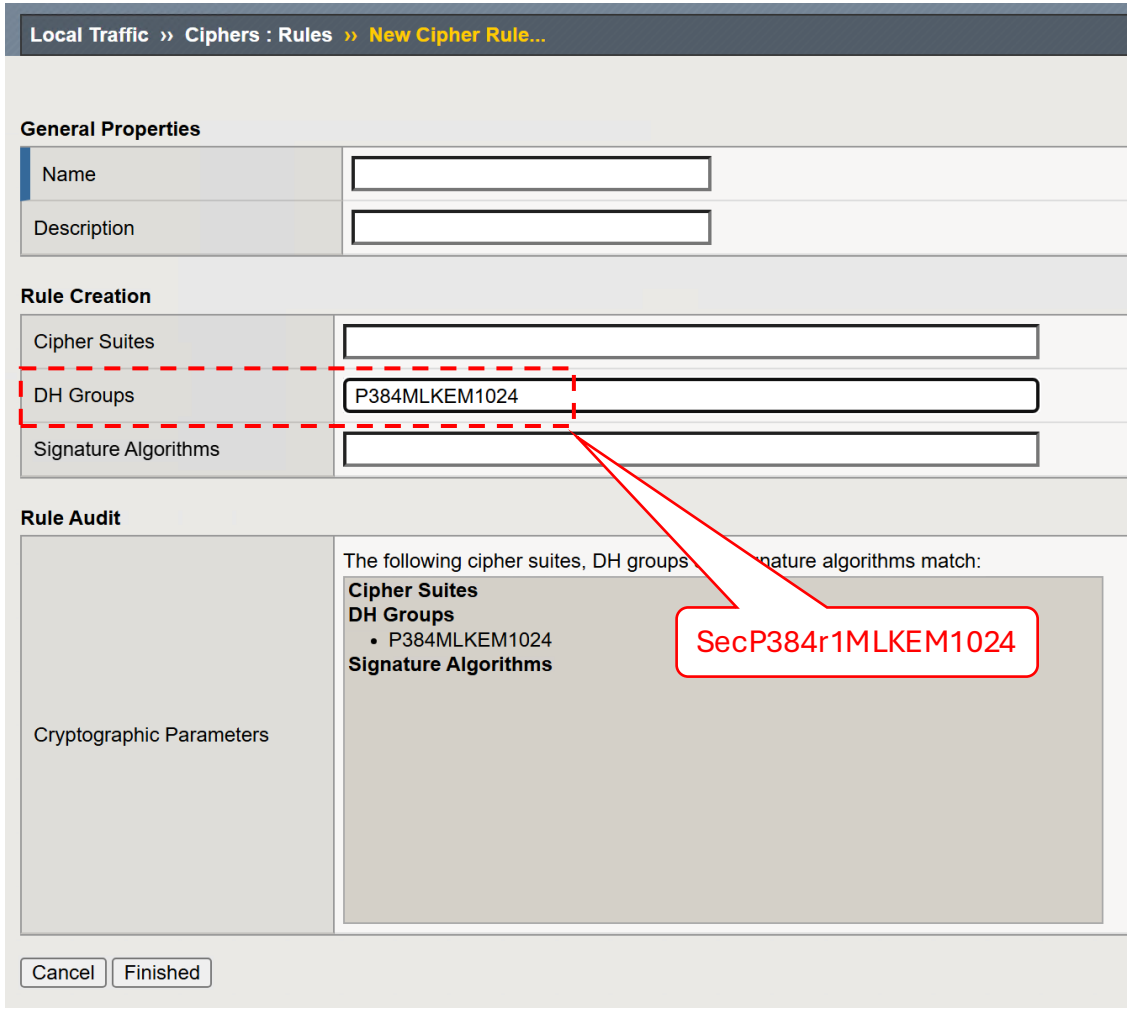
ハイブリッドPQCのサポート範囲の拡張

顧客課題	• 量子コンピューティングは急速な発展により、RSAやECCといった既存の暗号化方式は2030年までに安全性を失う可能性があります。 • 企業はポスト量子暗号技術 (PQC、別名「量子耐性暗号技術 (QRC)」)の導入によって、未来を見据えた計画を立てる必要があります。 • NISTをはじめとする規制当局は従来の暗号化と量子耐性アルゴリズムを組み合わせたハイブリッドアプローチを推奨しています。これにより、現在の安全なデータフローを維持しつつ将来に備えることができます。 • 前向きな対策を講じない場合、暗号鍵が危険にさらされ、機密データが露出し、顧客の信頼が損なわれる可能性があります。「今収集し、後で解読する」 (Harvest Now, Decrypt Later)攻撃が依然として活発であるからです。
F5 ソリューション	• F5はFIPS 203の下でML-KEM の展開に注力し、顧客が量子時代に備えられるよう取り組んでいます。 • BIG-IPは現在、NISTが承認したハイブリッドPQC暗号 (SecP256r1+ML-KEM-768およびSecP384r1+ML-KEM-1024)をサポートしています。これらは、既存のX25519+ML-KEM-768 (クライアント、サーバー共に17.5.1でサポート済)を補完します。 • これらのハイブリッド暗号は、進化する暗号化規制に準拠しながら、現在および将来の量子脅威から顧客のデータを保護するのに役立ちます。

ハイブリッドPQCのサポート範囲の拡張

BIG-IP GUI

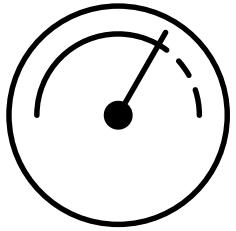




Local Traffic >> Ciphers >> Rules

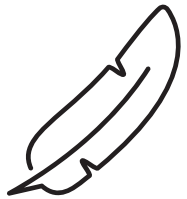
TLS 1.3とDTLS 1.2をデフォルトとして採用

業界標準への準拠を保証



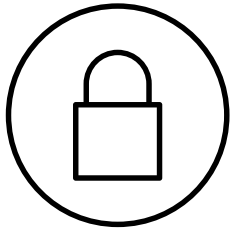
ネットワーク遅延を低減

より高速で安全なハンドシェイク処理により、パフォーマンスを向上



暗号化および転送のオーバーヘッドを削減

設定を簡素化し、静的な暗号文字列をTLS1.3対応の暗号グループに置き換え



デフォルトで安全なデプロイメントを確保

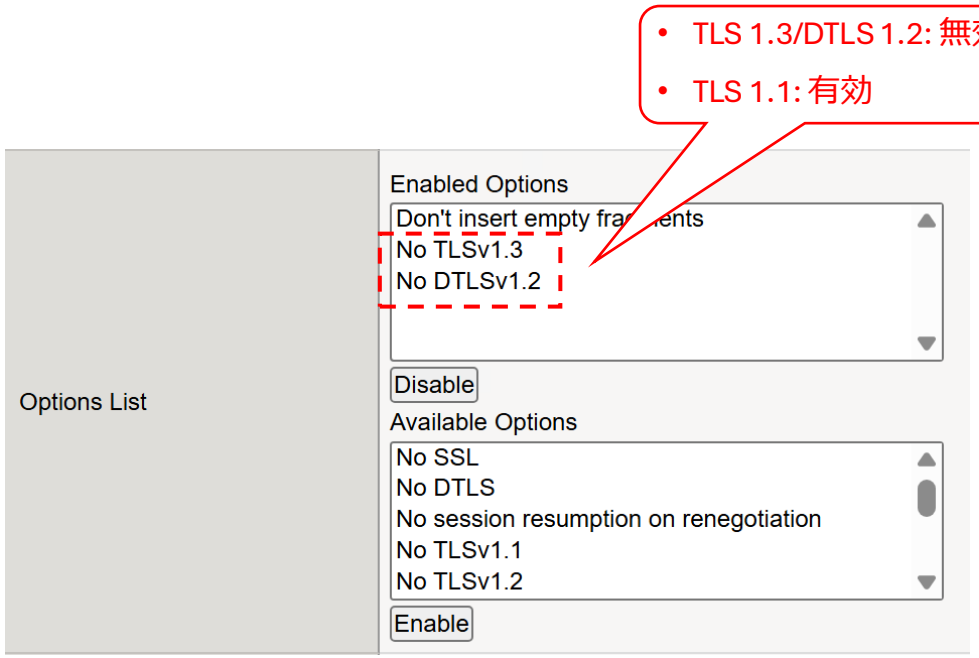
暗号化プロトコルを最新化し、コンプライアンスを維持する

デフォルトでTLS 1.3 & DTLS 1.2が有効に

顧客課題	• 顧客は、現代の業界標準に準拠し、強化された暗号化プロトコルの利点を享受するために、デフォルトで安全な最新の構成が必要です。 • TLSプロトコルの古いバージョンを使用していると、安全性が低くなり、最新の暗号化およびパフォーマンス要件を満たすことができません。
F5ソリューション	• BIG-IPは現在、TLS1.3およびDTLS1.2を有効化し、TLS1.1を無効化するデフォルト構成をサポートしています。これにより、デフォルトで安全性を確保した状態となっており、すべての新規導入において暗号化プロトコルが近代化されます。 • TLS1.3の導入により、ハンドシェイクプロセスがより高速かつ安全になり、ネットワークのレイテンシが短縮され、パフォーマンスが向上します。 • これらの変更は、静的暗号スイートをTLS1.3対応の暗号グループに置き換えることで構成を簡素化し、暗号化およびトランスポートのオーバーヘッドを削減します。

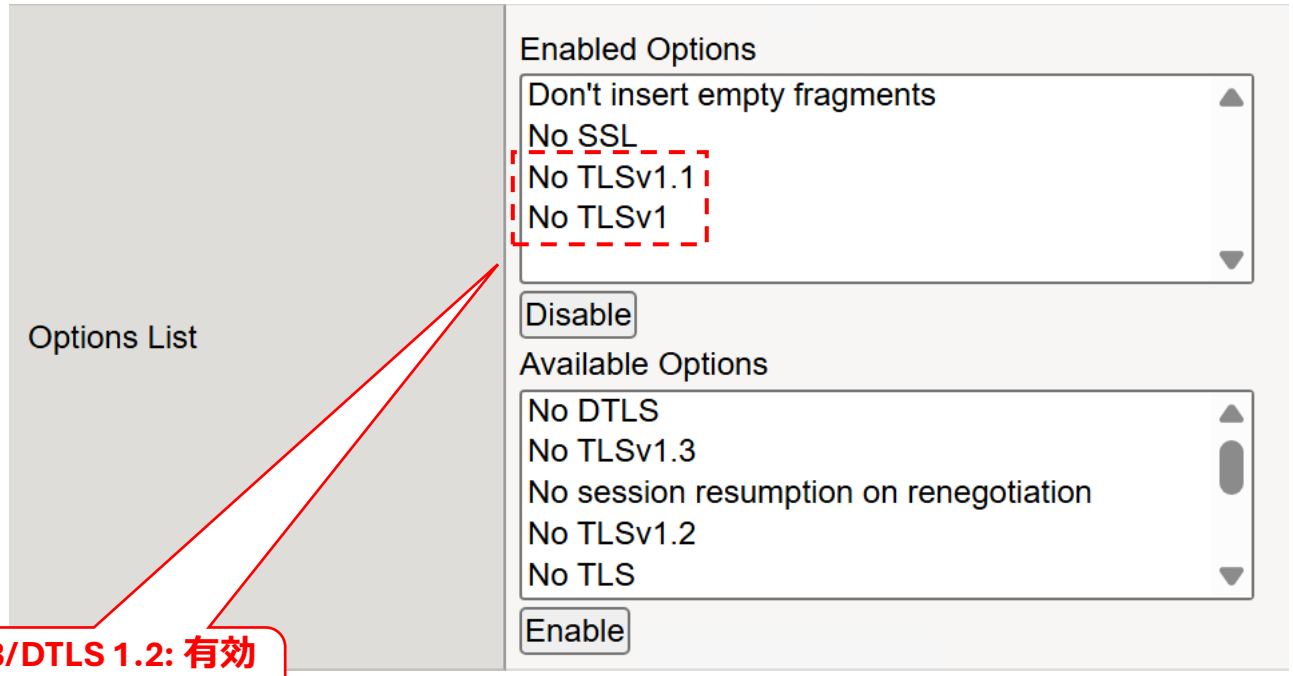
デフォルトでTLS 1.3 & DTLS 1.2が有効に

BIG-IP GUI: Client SSL Profile設定



- TLS 1.3/DTLS 1.2: 無効
- TLS 1.1: 有効

v17.5のデフォルト設定



- **TLS 1.3/DTLS 1.2: 有効**
- **TLS 1.1: 無効**

v21.1のデフォルト設定

TLS証明書の更新管理を効率化

HTTP-01を使用したACMEv2証明書自動化をサポート

ACME v2サポート以前	ACME v2サポート
非現実的なTLS証明書管理 (一部のプロバイダは、有効期限が90日間しかない証明書を発行)	TLS証明書管理のための安全でネイティブなサポート
労働集約型の手作業プロセス	ACMEv2は、最小限のユーザー操作で証明書の発行を自動化
設定ミスのリスク	BIG-IPシステムが認証局と直接通信
一貫性のないセキュリティ対策	http-01証明検証により、安全な所有権確認を保証

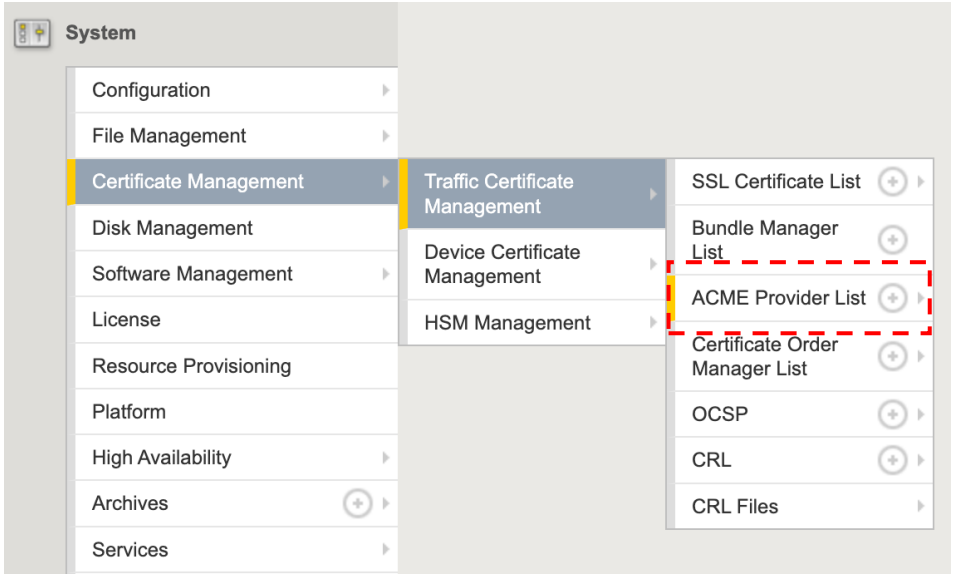
BIG-IP v21.1は、絶えず進化する技術環境において、ビジネスに不可欠なアプリケーションの最高レベルの暗号化セキュリティを維持するための労力を軽減

ACMEv2 (HTTP-01)での証明書更新自動化のサポート

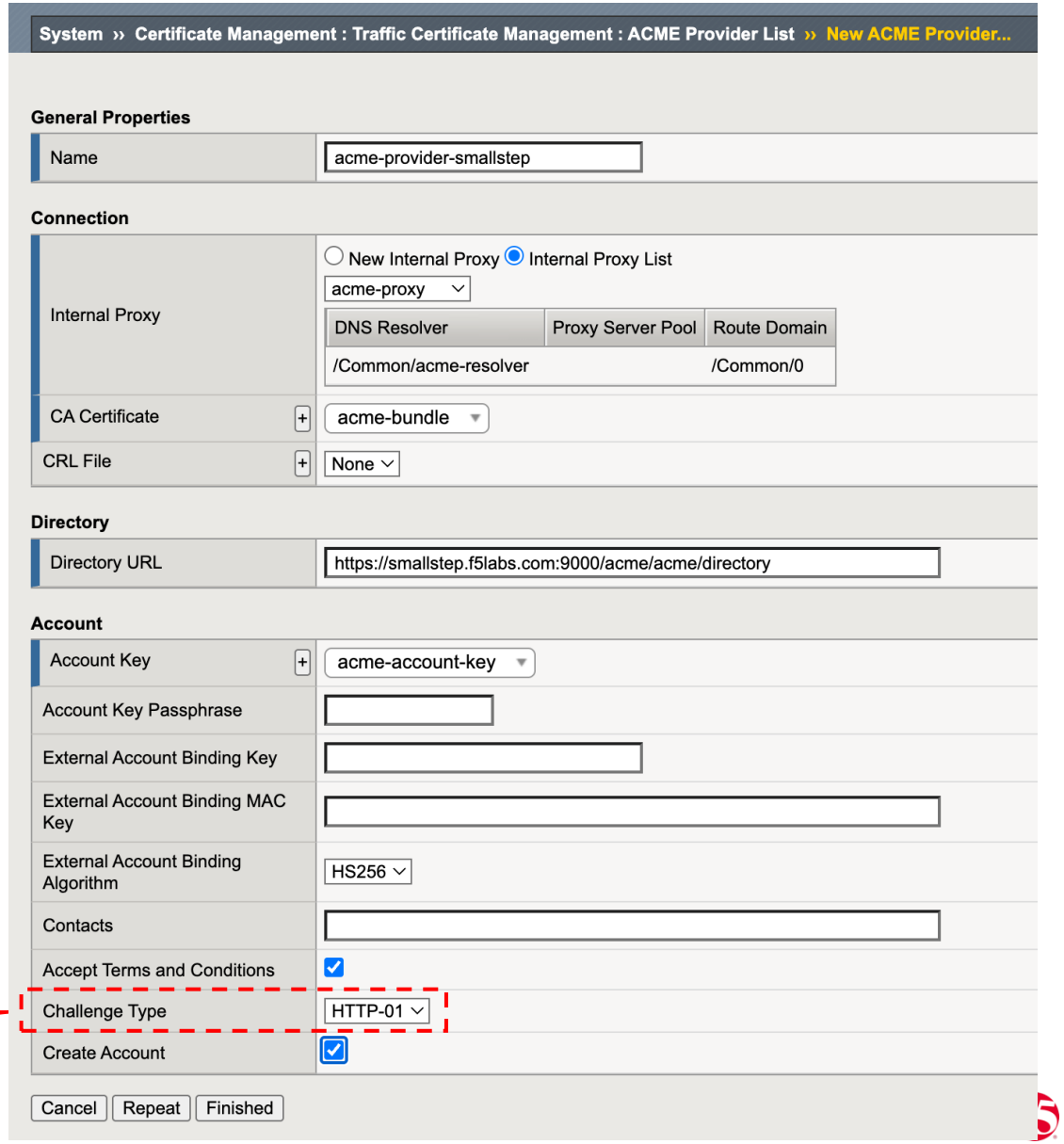
顧客課題	• TLS証明書の有効期間が短縮されていく動きが進むほどに、手動で証明書を管理することは多くの組織にとってますます非現実的になっています。 • いくつかの認証局が発行する証明書の有効期間はわずか90日間であり、頻繁な更新を効率的に処理するためには安全で自動化された仕組みが必要です。 • 自動化ができていない場合、証明書の更新作業には労力がかかり、エラーが発生しやすくなり、サービスの中断やセキュリティリスクにつながる可能性があります。
F5ソリューション	• BIG-IPはACME v2をサポートすることで、安全で自動化された証明書更新プロセスを提供します。 • ACME v2を使用することで、BIG-IPシステムは証明書認証局と直接通信し、TLS証明書のリクエストおよび更新を行うことが可能になり、NetOpsおよびDevOpsチームの運用を効率化します。 • これにはhttp-01チャレンジが含まれており、HTTPを介して安全かつ効率的な所有権検証を実現します。

ACMEv2 (HTTP-01)での証明書更新自動化のサポート

BIG-IP GUII



System >> Certificate Management >> Traffic Certificate Management >> ACME Provider List



v21.1では”HTTP-01”のみ指定可能

SNAT IPソースモニタによる効率的な運用と高可用性

予測可能な監視元IPアドレス

- SNATモニタは特定のSNAT IPアドレスまたはSNATプールに対してプローブを行うため、ヘルスチェックは常にファイアウォール/サーバーが想定するアドレスから実施

ノイズは少なく、精度は同じ

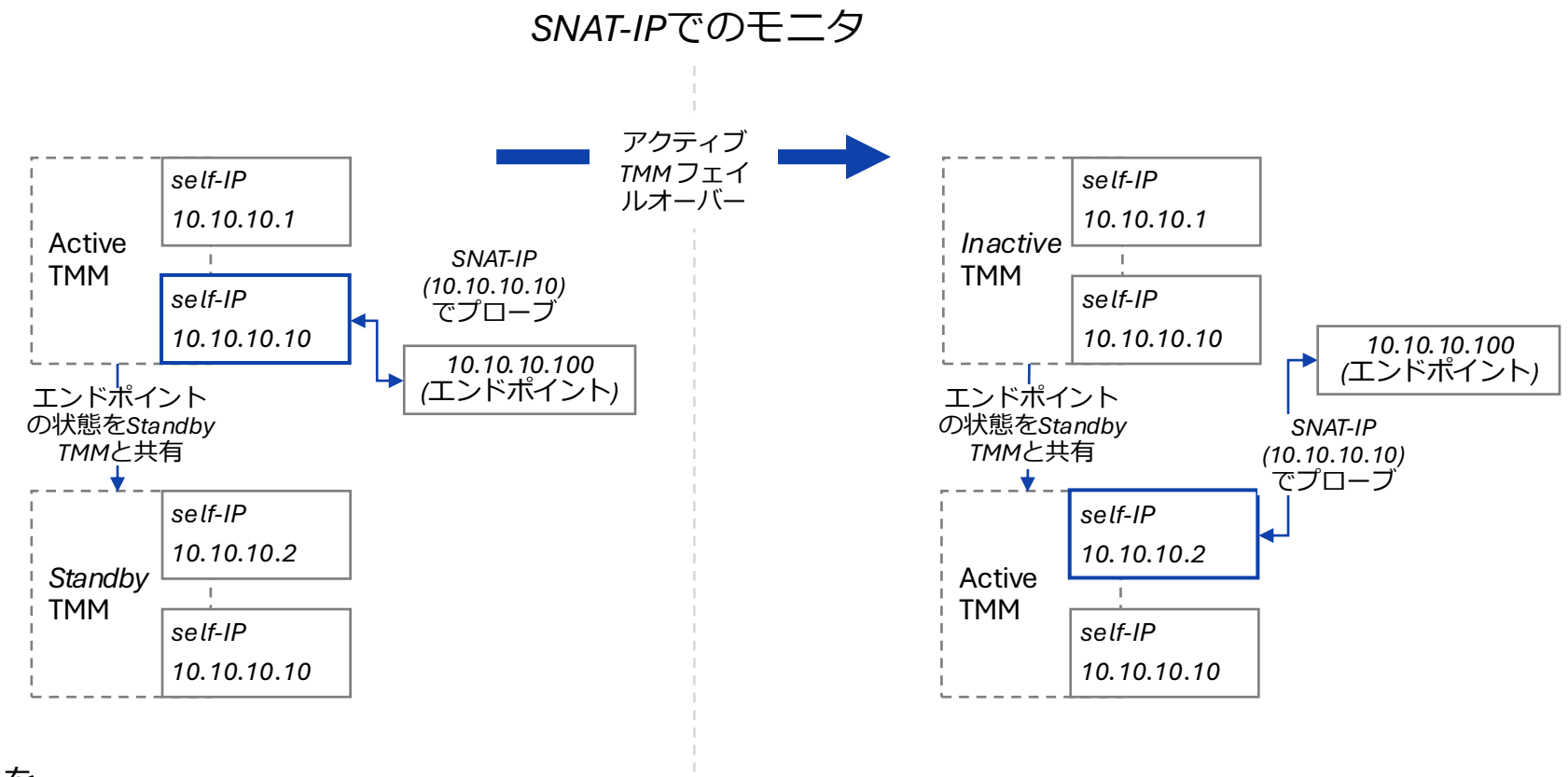
- HAペアではアクティブなTMMのみがプローブを送信するため、重複するモニタトラフィックが排除され、ヘルスステータスを正確に維持

よりシンプルなHA運用

- 両方のデバイスで共有のSNAT IP/プールを使用するため、アドレス空間を分割したり、アクティブ/スタンバイ用の個別設定が不要

スタンバイ状態を維持

- アクティブユニットがエンドポイントの状態を同期するため、スタンバイユニットは直近のメンバーの稼働状況 (アップ/ダウン)ビューを維持し、フェイルオーバー動作の一貫性を維持



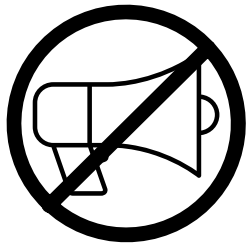
SNAT IPからのヘルスチェック

顧客課題	• モニタープローブの送信元としてSelf-IPを使用する顧客は、ルーティング接続を必要とするVIPや異なるルートドメインに属するプールのヘルスチェックをサポートするのが難しい場合があります。 • 外部関係者を含む構成では、ルーティング制限のために、プローブの送信元としてプライベートなSelf-IPアドレスを使用することがしばしば困難です。 • 顧客は、プローブがルーティングポリシー上適切なSNAT IPから送信されることを保証し、アプリケーションの接続性と状態を効果的に監視する方法を求めています。
F5ソリューション	• BIG-IPは、in-TMMモニタープローブの送信元IPをSelf-IPとSNAT IPの間で切り替え可能なモニタ機能をサポートします。 • この強化により、ヘルスチェックが適切なアドレス (SNAT)から開始され、外部VIPおよびプールメンバーに関する顧客のルーティング要件を遵守できます。 • これにより構成が簡素化され、コンプライアンスが向上し、アクティブなBIG-IPとオフラインなBIG-IP間で円滑なフェイルオーバー通信が確保されます。

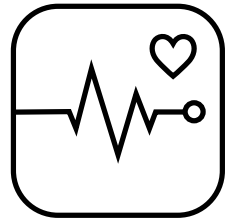
MAC in-TMM Monitor

- **従来のMonitor: 「サービスが応答している」ことを証明**
- **MAC in-TMM Monitor: 「BIG-IPがパケットをノードに配信できる」ことを証明**

L4/L7モニタとHTTP/TCPチェック**を補完**し、メンバーへのネットワークパスが切断された際にブラックホールが発生するのを防ぐ



ノイズを低減し、トラブルシューティング時間を短縮することで、運用チームの迅速なトリアージを支援



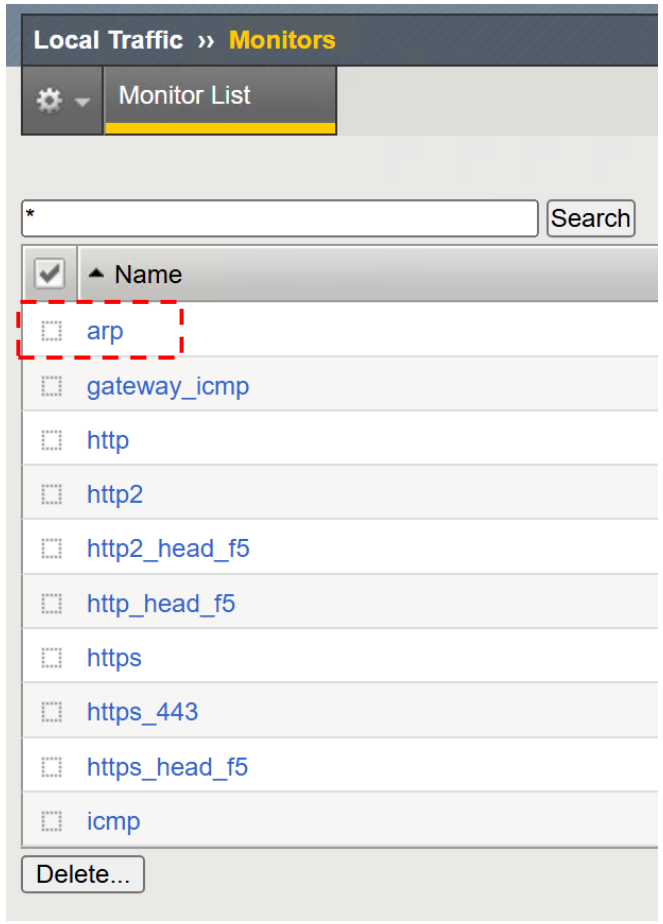
アプリレベルのプローブが実行不可能な場合に、サービスエンドポイントが不要な**到達可能性テストをデプロイ**

in-TMM MonitorでのMACサポート

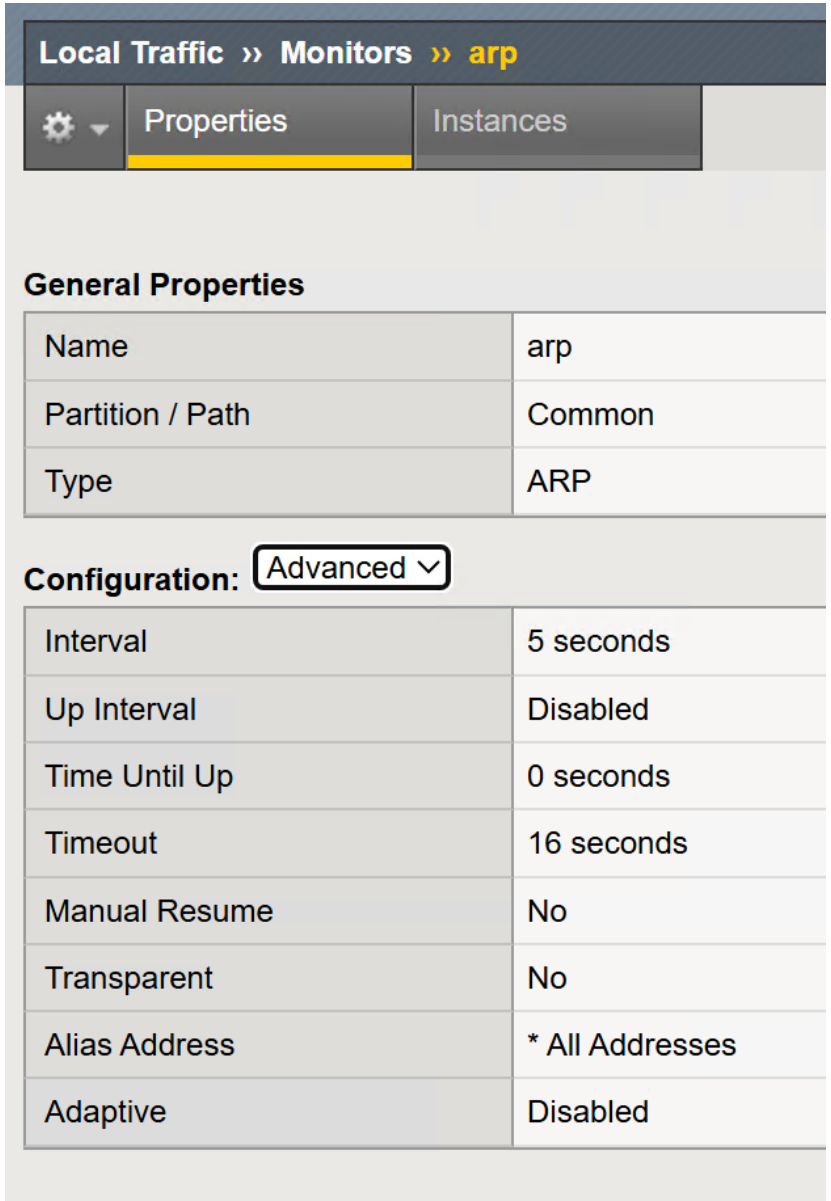
顧客課題	• TMM (Traffic Management Microkernel)内でネイティブにVLAN機能を検証し、MACレベルでのヘルスチェックを通じてノードのアクセシビリティを確認する仕組みが必要です。 • この機能がなければ、管理者はBIG-IPとプールメンバー (ノード)間の適切なレイヤ2通信を確保することができません。 • 現在のARPテーブルエントリの検証やVLANの機能を確認する方法では、通信断、ミスルーティング、または運用の非効率性が生じる可能性があります。
F5ソリューション	• in-TMMヘルスモニタで、ネイティブなMACベースのヘルスチェックをサポートします。 • このヘルスチェックは、ARPリクエストを介してプールメンバーのIPアドレスを解決し、適切なレイヤ2通信を検証します。 • ヘルスチェックでMACアドレスの応答が正常に受信された場合はモニタは正常と判断され、応答がない場合はモニタは失敗としてマークされます。 • VLANが機能していることを確認し、正確かつ最新のARPテーブルを維持することが可能になります。 • このヘルスチェックはHA Groupプールにも適用でき、可用性およびシステムパフォーマンスの最適化に貢献します。

in-TMM MonitorでのMACサポート:“ARP” Monitor

BIG-IP GUI

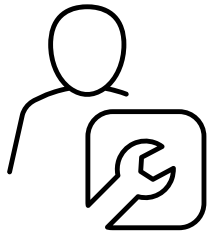


Local Traffic >> Monitors



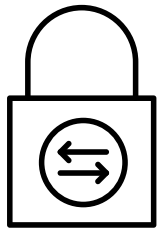
相互TLS (mTLS)セッション中のサーバーに対する精密な制御

クライアント証明書制約付き委任 (C3D)制御を使用して、受信mTLSトラフィックの復号と検査を効率化



C3D制御の追加

委任クライアント証明書におけるX.509属性および証明書拡張機能の動的制御を拡張



mTLSトラフィックの復号化と検査

制約付き委任をサポートし、証明書に対するポリシーベースの制御を適用

暗号化コンプライアンスの強制

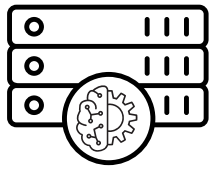
SSLO検査などの機能を、より精密なセキュリティ制御で有効化

mTLSの複合化と検査のためのC3D

顧客課題	• 組織は、着信する相互TLS (mTLS)トラフィックの復号化と検査において大きな課題に直面しています。 • 既存のソリューションは委任されたクライアント証明書に依存しており、証明書アトリビュートの制御が制限されており、高度なセキュリティおよびコンプライアンス要件を完全に満たすことができません。 • 強化されたC3D (Client Certificate Constrained Delegation)機能がなければ、動的委任のユースケースに対応し、mTLSセッション中のサーバー動作を正確に制御することが困難です。
F5ソリューション	• BIG-IPは、委任されたクライアント証明書内のX.509アトリビュートおよび拡張アトリビュートを動的に制御するためのC3D機能をサポートします。 • これにより、組織はmTLSトラフィックを復号化および検査するだけでなく、制約付き委任などのユースケースに対応しながら、サーバー証明書に対する動作制御が可能になります。 • 顧客は暗号化のコンプライアンスを確保し、SSLO (SSLオフロード)検査などの機能を有効化し、精密なセキュリティ制御を提供できます。

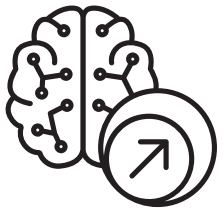
高信頼性/高拡張性のステートフルMCPセッション

LLMエージェント向けのMCPセッションプロファイル永続化による可視性と診断機能の向上



BIG-IPの背後でMCPを本番環境に対応

LLMエージェントセッションは同じMCPサーバーに戻るため、断続的な「セッション切断」障害が軽減

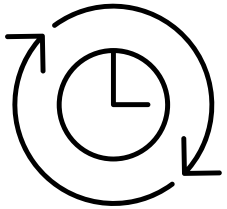


安全なスケールアウトと高スループットを実現

セッションごとのコンテキストを損なうことなく、MCPサーバのプール/オートスケーリングをサポート

セキュリティと制御を強化

暗号化され、改ざん防止機能を備えたセッショントークンにより、クライアントによる操作を防止し、バックエンドのトポロジーを隠蔽



運用を簡素化し、導入を迅速化

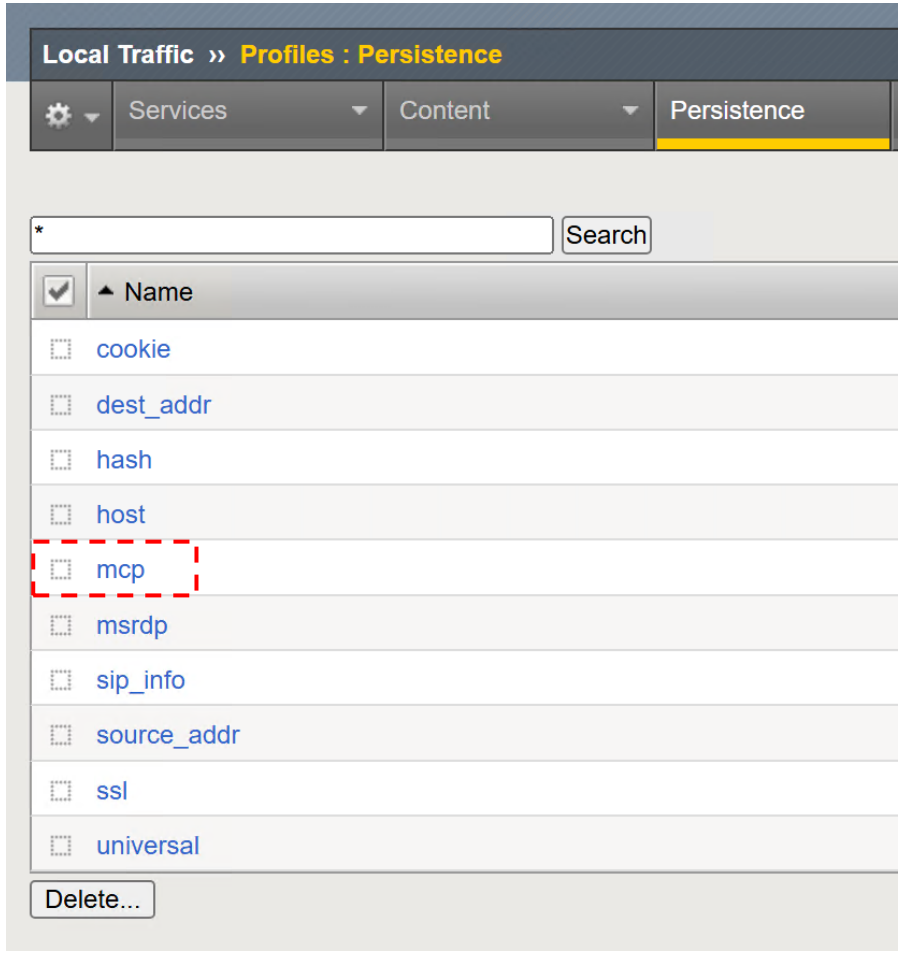
アプリケーション側でのスティッキーセッション回避策を削減し、トラブルシューティングを迅速化するための明確な永続化ログを追加

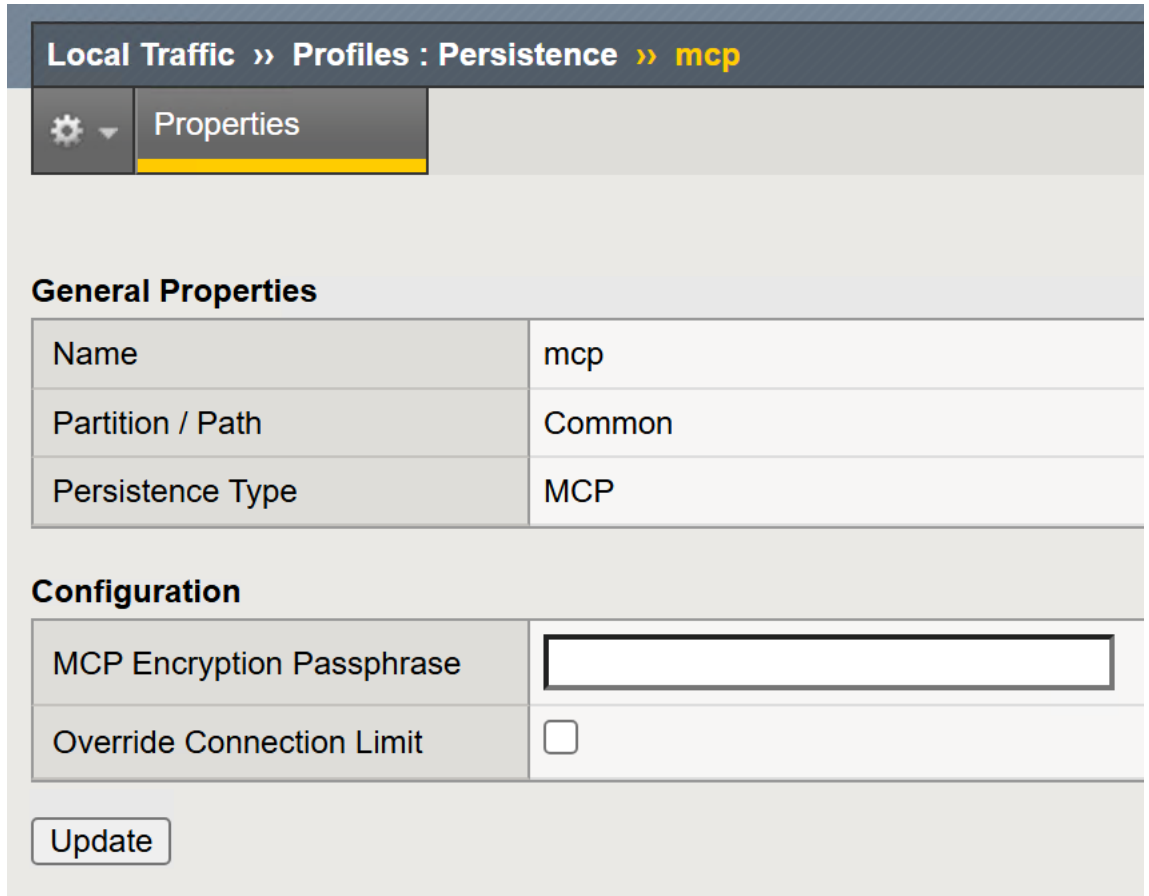
MCPセッションのためのパーシステンス・プロファイル

顧客課題	• MCPのトラフィック処理においては、セッションパーシステンスの問題に直面することが多くあります。 • MCPサーバーは初期化時にセッションを作成し、セッションIDをクライアントに返しますが、その後のリクエストでは、同じMCPサーバーインスタンスにルーティングされる必要があります。これにより、一貫した処理が可能となります。 • このタイプのセッションを維持する仕組みがない場合、こうしたトラフィックフローに依存している顧客には問題が生じます。
F5ソリューション	• BIG-IPは、Cookieの仕組みを模倣したMCPセッションパーシステンスをサポートします。 • 同じセッションIDを含むリクエストが同じプールメンバーにルーティングされ、MCPトラフィックフローにおける一貫性と信頼性が確保されます。 • 関連するログメッセージや永続性メトリクスには、この新しいMCPセッションタイプが反映されるため、顧客の管理者にとって可視性と診断能力が向上します。

MCPセッションのためのパーシステンス・プロファイル

BIG-IP GUI





Local Traffic >> Profiles >> Persistence

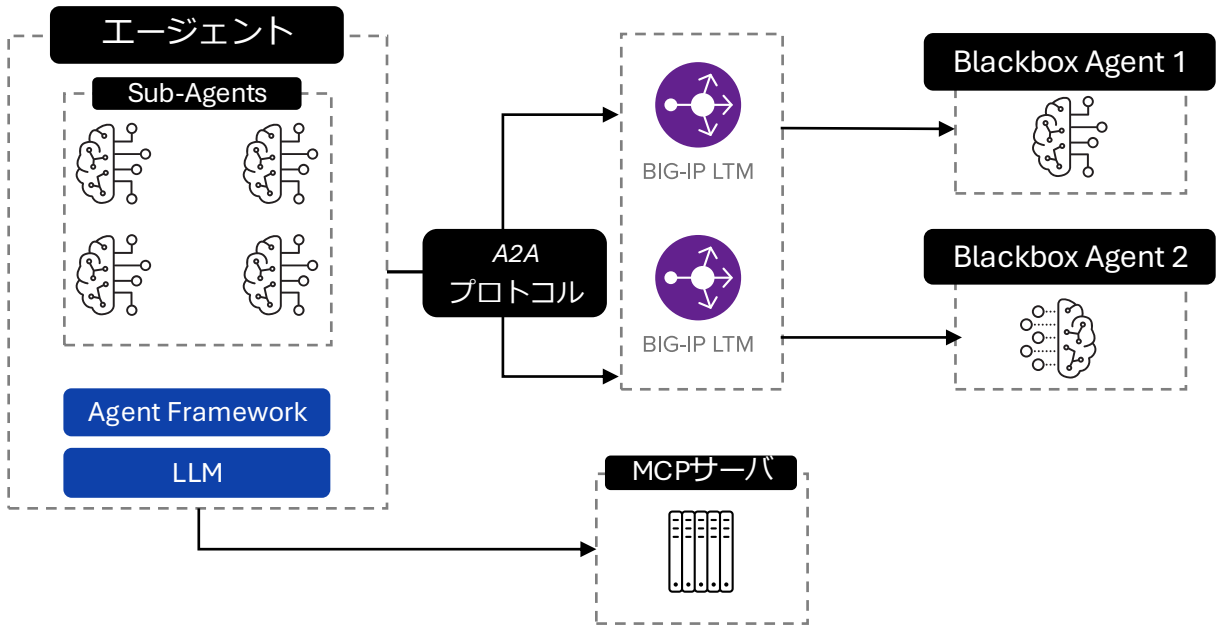
A2Aの可視性/ログ記録/デバッグ/プロトコル検証を強化

課題:

- エージェントフレームワークとベンダー間で共通のA2A標準が存在しない。
- 既存のプロトコルと限られた監視機能により、長時間実行されるマルチモーダルワークフローの統合、検証、トラブルシューティングが困難

ソリューション:

- BIG-IPでA2Aの検出、タスク交換、プッシュ通知の制御された評価を有効化
- **iRules**ですべてのA2Aトラフィックをログに記録し、プロトコル動作のデバッグと検証を行い、本番環境に展開せずにMCPなどのエンタープライズ標準と比較可能



注:
BIG-IP v21.1のA2Aプロトコルは実験的なものであり、テストおよび検証目的のみに使用してください。
本番環境でのサポート対象機能ではなく、F5は本プロトコルの使用に関する技術サポートを提供していません。

実験的なA2Aプロトコルのテスト

顧客課題

エージェントベースのアプリケーションを導入する組織は、分散環境における円滑な通信を確保するという課題に直面しています。

- 異なるフレームワークやベンダーの技術に基づいて構築されたエージェントは共通のプロトコルを持たないため、統合に多大な労力を要します。
- 従来のプロトコルは長時間実行されるタスク、マルチモーダルな情報交換、および人間が関与するワークフローへの対応に課題があり、新たな相互運用性標準の検証を困難にしています。
- エージェント間の通信の監視とログ記録が不十分なため、問題の検出とトラブルシューティングが妨げられています。

F5ソリューション

BIG-IP v21.1で、Agent-to-Agent (A2A)プロトコルの動作を検証するための実験的な機能が導入されました。iRulesとBIG-IPのインテリジェントなプロキシ・フレームワークを使用することで、エージェント間の相互運用性をテストし、エコシステム全体でプロトコルの整合性を確認できます。

- BIG-IPがエージェントの検出、タスクの交換、プッシュ通知を評価するための制御された環境を提供します。
- iRulesはすべてのA2Aプロトコルトラフィックをログに記録でき、透明性、デバッグ、プロトコル検証が向上します。
- 本番環境への本格的な導入なしに、長時間実行されるタスク (SSE経由)、非同期メッセージング、その他のインタラクションにおけるA2Aの処理を評価できます。これにより、A2Aの動作をTMOSのMCPなどの既存の企業標準と比較することが容易になります。

注: BIG-IP v21.1のA2Aプロトコルは実験的な機能であり、テストおよび検証のみを目的としています。本番環境での利用はサポートされていません。

delay timeoutによるアクティブな接続の強制切断

顧客課題	• プールメンバーのサービスをシャットダウンする際、組織は一定期間でアクティブな接続を完全に終了させることに課題を抱えています。 • 顧客は、指定された遅延タイムアウト後にアクティブなセッションを強制的に終了させる機能を必要としています。 • これがないと、サービスのタイムリーなシャットダウンが妨げられ、メンテナンスが複雑化し、リソースを消費し続ける残留アクティブセッションによる運用上の障害の可能性が高まります。
F5ソリューション	• BIG-IPは、グレースフル・シャットダウン (graceful shutdown)機能を補完するための、可変な遅延タイムアウトオプションをサポートします。 • これにより、ユーザーは定義された期間後にアクティブな接続を強制的に終了させることができ、接続が自然にタイムアウトするのを待たずにプールメンバーを完全にオフラインにすることが可能になります。 • これにより、ダウンタイムのリスクと運用の複雑さを軽減しながら、シームレスなサービス移行を実現します。

デフォルトのユーザーネームを”admin“から変更

顧客課題	• 顧客は、主要システムコンポーネントにエラーを発生させることなくデフォルトの”admin”ユーザー名を変更する機能を必要としています。 • デフォルトのadminユーザーを無効化しカスタム管理者ユーザーに置き換えると、TMUIセッションのログアウト、認証トークンの失敗、定期的なAPIエラーなどの問題が発生します。 • これらのエラーはシステムの機能を損ない、システムの信頼性と使いやすさに影響を与える持続的なエラーログを生成します。
F5ソリューション	• BIG-IPは、デフォルトのadminユーザー名をカスタムユーザー名に変更することをサポートします。 • これには、iControl RESTフレームワーク、TMSH、および基本認証メカニズムとの互換性の維持が含まれます。 • これにより、顧客はシステムの安定性を維持しながら、強固なセキュリティ対策を実践することが可能になります。

BIG-IP DNS v21.1

複数のRPZ (Response Policy Zone)フィードゾーン

DNS解決のセキュリティと制御を強化

設定と統合

複数のRPZフィードを統合することで、効率性と運用性を向上

DNSレベルのセキュリティの強化

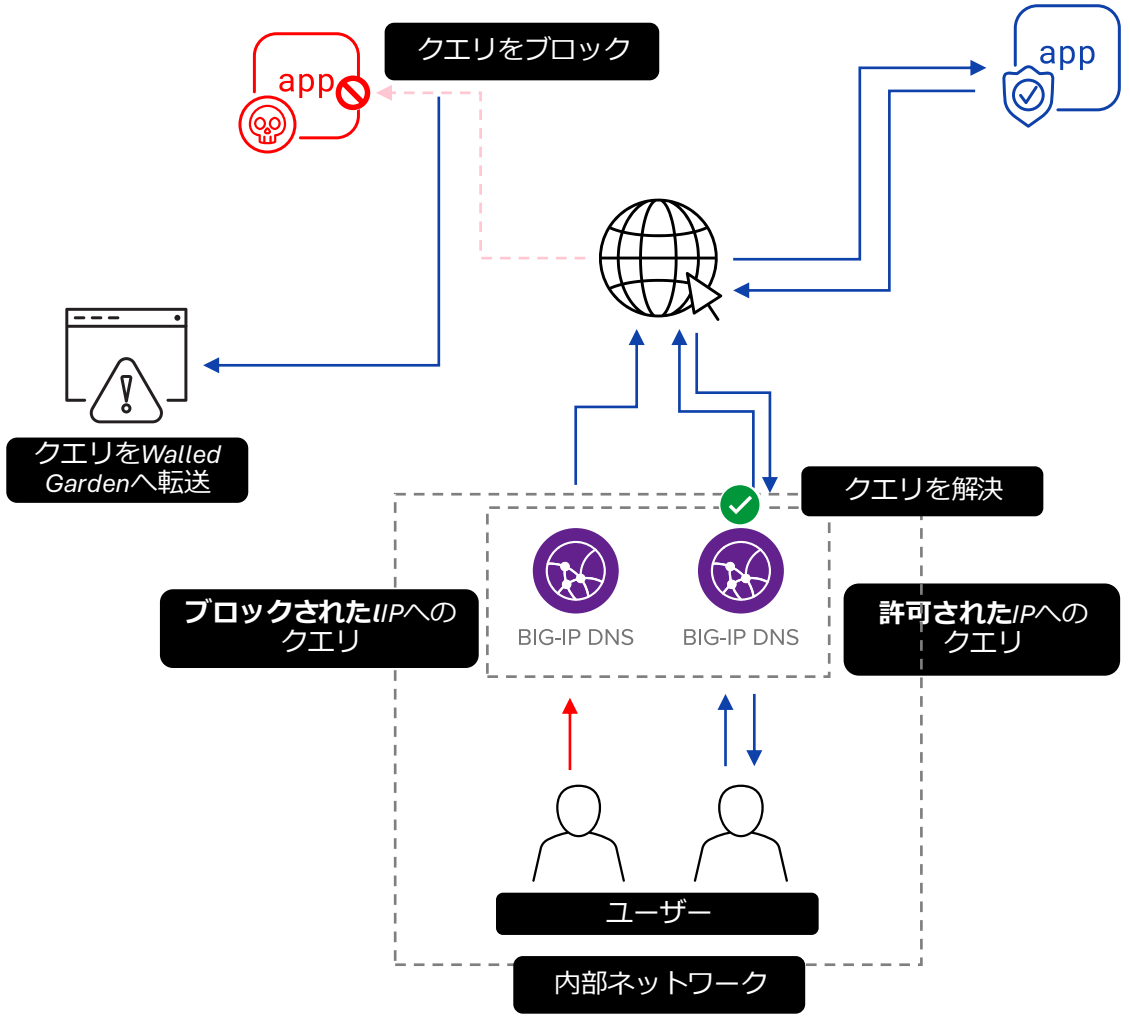
IPベースのブロック機能で、脅威対策をよりきめ細かく制御

柔軟なDNS応答アクション

悪意のあるドメインのブロック、トラフィックのリダイレクト、地域ごとのコンプライアンス要件への対応等が可能

ポリシー管理を簡素化

単一のDNSキャッシュプロファイル内で、複数の脅威インテリジェンスフィードをサポート

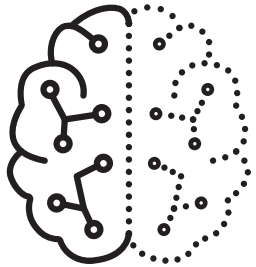


複数のRPZ (Response Policy Zone)フィードゾーン

顧客課題	• DNSポリシーの管理には、個別のキャッシュプロファイルを作成し、トラフィックを手動で分割する必要があります。 • 組織は、多様なDNSセキュリティおよびコンプライアンス要件を徹底するための統一的なアプローチが出来ずにいます。 • これらの断片化されたプロセスは複雑さ、運用のオーバーヘッド、設定ミスのリスクを増大させます。たとえば、複数のRPZ (Response Policy Zone)フィードをiRuleで反復処理すると、高いCPU負荷が発生します。 • その結果、チームはBIG-IP DNSにおける複数RPZフィードのネイティブサポートを必要としています。
F5ソリューション	• 単一のDNSキャッシュプロファイル内で複数の脅威インテリジェンスフィードをサポートすることで、DNS RPZの機能を強化し、ポリシー管理を簡素化します。 • 管理者は複数のRPZフィードを設定および統合できるため、効率が向上し、運用が合理化されます。 • 柔軟なDNSレスポンスアクション (NXDOMAIN、NODATA、CNAMEなど)を活用することで、悪意のあるドメインのブロック、トラフィックのリダイレクト、または地域のコンプライアンス要件への対応が可能になります。 • IPベースのブロッキングにより、DNSレベルのセキュリティが強化され、脅威緩和のためのよりきめ細かい制御が提供されます。

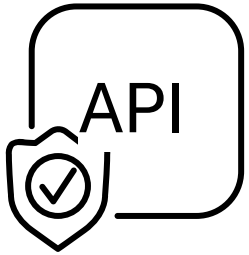
BIG-IP Advanced WAF v21.1

新しいプロトコル/API/エージェント型AI関連の保護機能



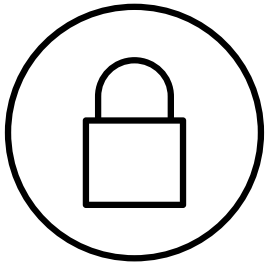
AIによる脅威からの保護

コンテキストスプーフィングからツールポイズニングまで、新たな攻撃からMCPトラフィックを保護



APIセキュリティ体制を強化

最新のAPI標準に基づいたセキュリティポリシーを適用することで、攻撃対象領域を縮小



“エッジ”で攻撃を阻止

クライアントプロトコルの種類に関わらず、悪意のあるトラフィック(DDoS攻撃、プロトコル攻撃など)をバックエンドに到達する前に阻止

OWASP Top 10の重大な脅威からMCPトラフィックを保護

MCP 01

Data Guardgが提供するマスキング機能により、機密情報を漏洩させる脆弱性から保護

MCP 02

JSONスキーマ検証により、Toolのスコープクリープ (権限昇格)や、強制失敗攻撃(Enforcement failure attack)に対するセキュリティを確保

MCP 03

JSONスキーマ検証により、ツールポイズニングに対するセキュリティを確保

MCP 05

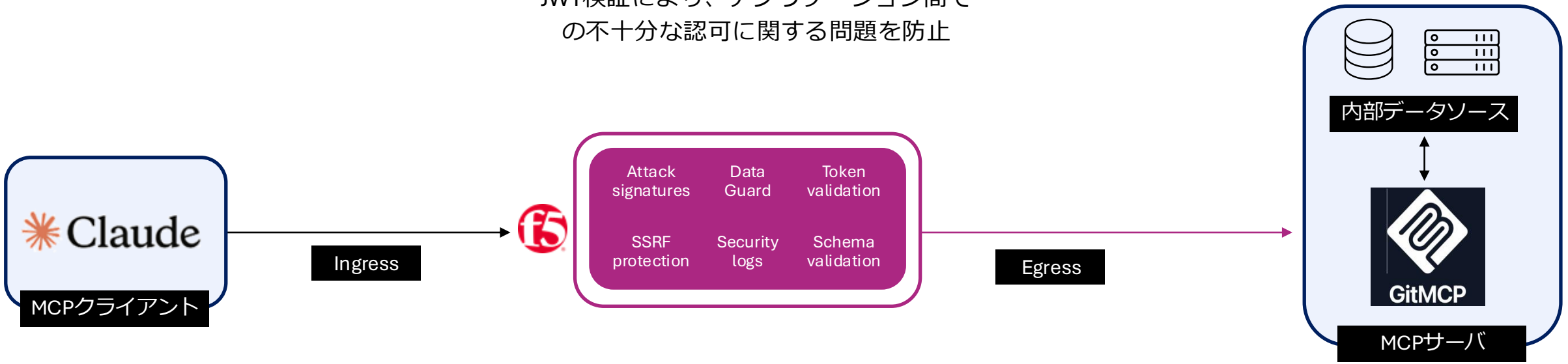
攻撃シグネチャの検査により、コマンドインジェクション関連の脅威から保護

MCP 07

攻撃シグネチャの検査により、コマンドインジェクション関連の脅威から保護
JWT検証により、アプリケーション間での不十分な認可に関する問題を防止

MCP 08

監査とテレメトリの課題に対処する包括的なログ



主要な攻撃からMCPトラフィックを保護

顧客課題

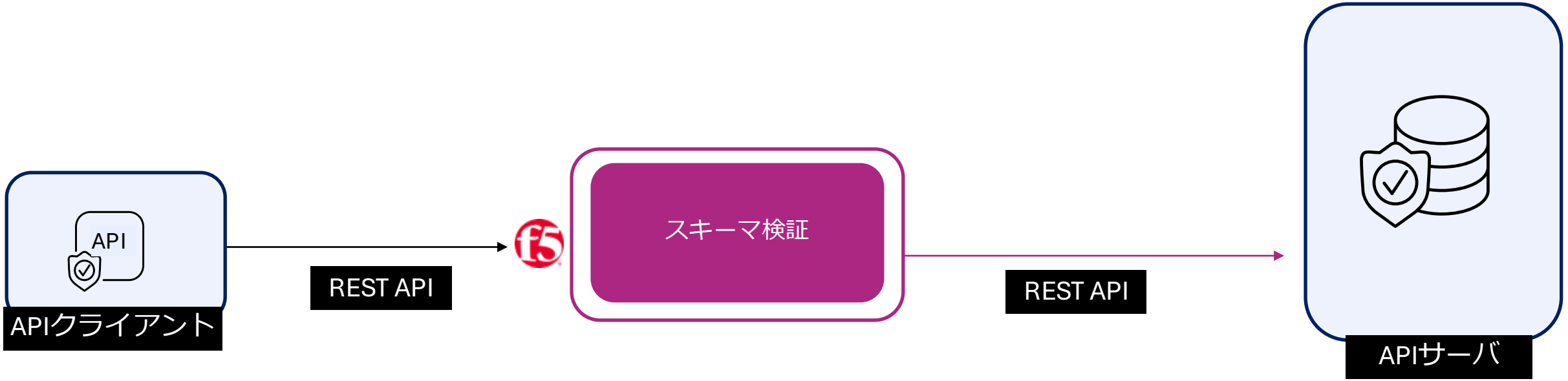
- Model Context Protocol (MCP)とMCPサーバの登場により、現在のアプリケーションの脅威対象領域が拡大し、アプリ、API、ワークロードと同様のセキュリティ対策が必要になっています。
- Model Context ProtocolとMCPトラフィックは、アプリとデータソースがAIモデルとどの様に連携するか、標準化します。より多くの顧客がAIアプリを作成したり利用したりするにつれ、MCPは環境の一部になります。
- MCPトラフィックはトークン窃取、プロンプトインジェクション、ツールポイズニングといった攻撃に対して脆弱であり、侵害を防ぐために新たなセキュリティ対策を実装する必要があります。

F5ソリューション

- BIG-IP Advanced WAFは現在、リクエスト側のMCP検査/保護をサポートしており、主要な脅威をプロアクティブに検知、緩和できるように支援し、パフォーマンスやレイテンシへ影響を与えることなく、AIトラフィックの安全性を確保します。
- 脅威からの保護は主要なOWASP Top 10 MCPの脆弱性にわたります:
  - MCP01: 機密情報を露出させる脆弱性から保護するためのData Guardによるマスキング
  - MCP02: ツールのスコープクリープ(スコープ拡大)や強制適用の失敗を狙った攻撃に対するセキュリティを確保するためのJSONスキーマ検証
  - MCP03: ツールポイズニングを防止するためのJSONスキーマ検証
  - MCP05: コマンドインジェクションに関連する脅威を緩和するためのAttack Signatureによる検査
  - MCP07: アプリケーション間での不十分な認可の問題を防ぐためのJWT検証
  - MCP08: 監査やテレメトリ不足に伴う課題を支援するための包括的なログ

最新のOpenAPI標準に基づいてAPIトラフィックを保護

- ✓ 最新のOpenAPI標準を適用することで、攻撃対象領域を縮小
- ✓ OpenAPIドキュメントを、WAFポリシーエンティティ (URL, コンテンツプロファイル etc.)に変換する機能をサポート



OpenAPI Spec 3.1のサポート

より強固なAPIセキュリティを実現

顧客課題	• OpenAPI spec 3.1は、最新のJSONスキーマ標準に準拠したREST API向けの業界標準です。 • 現行のBIG-IP Advanced WAFはOpenAPI Spec 2.0および3.0 のみサポートしており、最新のOpenAPI Spec 3.1 が提供する「セキュア・バイ・デザイン」のアプローチを利用することができません。
F5ソリューション	• v21.1でBIG-IP Advanced WAFがOpen API Spec 3.1をサポートし、より精密でコンピュータが解釈可能なAPI定義が可能になることにより、アタックサーフェス (攻撃対象範囲)を縮小します。 • OpenAPI Spec 3.1のサポートにより、より強力な入力検証とセキュリティスキームの明確なドキュメント化が可能になり、API全体のリスクを低減します。

その他の注目すべき改善ポイント

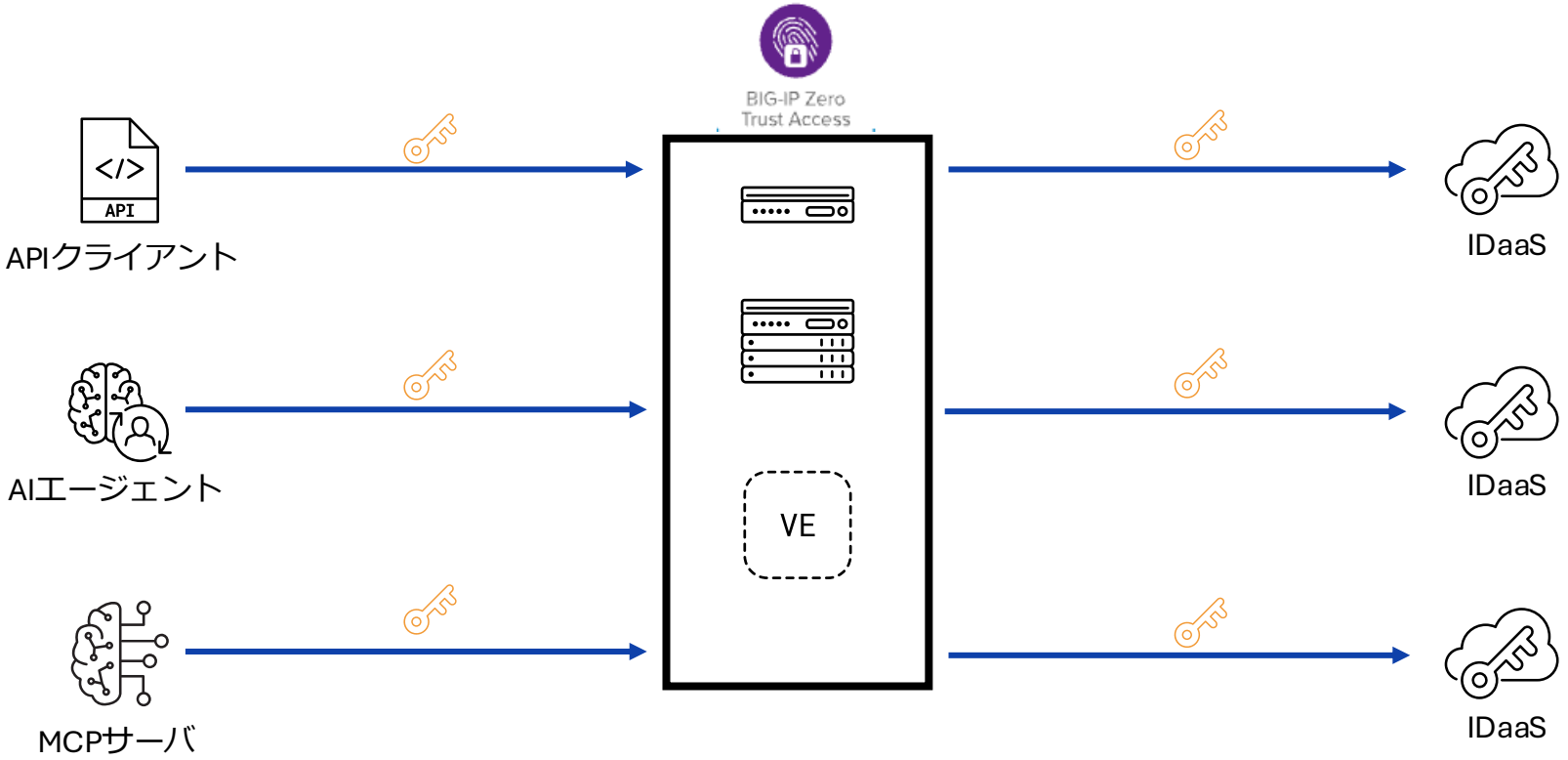
- **外部SIEM/SOARとの連携**
  - BIG-IP Advanced WAFは、Splunk向けに拡張されたキー・バリュー方式のリモートログの詳細 (例 : Violationの詳細)を提供するようになりました。

- **HTTP/3保護のサポート (クライアント側)**
  - クライアントのプロトコルバージョン (HTTP/1.1、HTTP/2、HTTP/3)にかかわらず、攻撃がサーバーに到達する前に阻止できるようになりました。

BIG-IP Zero Trust Access (APM) v21.1

Dynamic Client Registration (DCR)サポート

クライアントアプリケーションを登録するための、自動化されたAPI駆動型メソッド



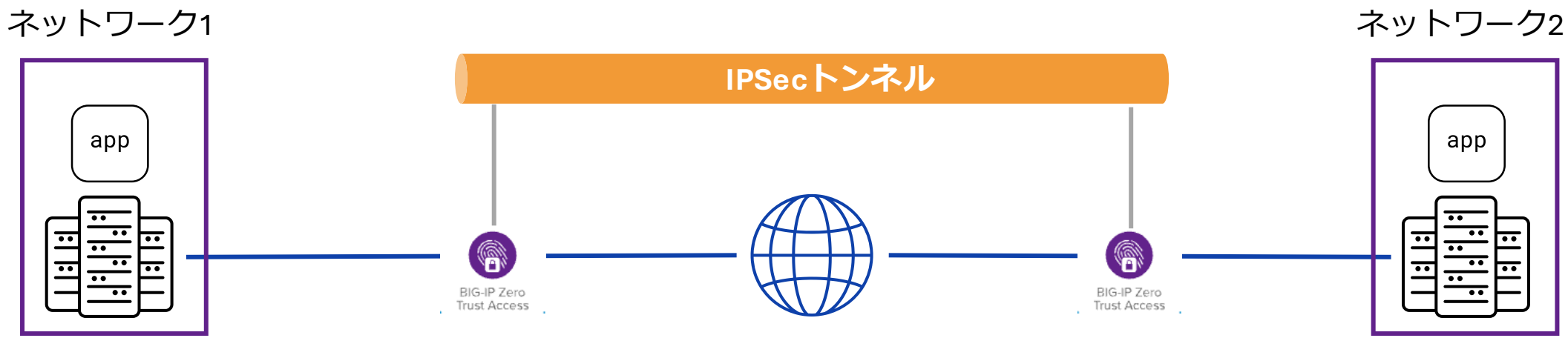
- 管理者による手動設定が不要
- クライアントメタデータの処理、クライアント認証情報の発行、ゼロトラストアクセスへのシームレスな統合を実現する、安全な登録エンドポイントを作成
- 認証と認可の自己登録と自己管理
- MCPサーバー、エージェントAIなどのクライアント登録を容易に

Dynamic Client Registration (DCR)

顧客課題	• 現在、BIG-IP Zero Trust Access (APM)が集中型認証サーバー (AS)として機能する場合、アプリケーションの所有者や開発者は、開発中の新しいアプリケーションの認証および認可設定を、BIG-IP 管理者に事前に登録する必要があります。 • BIG-IP管理者は、各アプリケーションの認証および認可設定を行うために、Zero Trust Access (APM)内で新しいクライアントを手動で設定する必要があります。 • これは複雑で手作業を要するタスクであり、管理者の作業負荷を増大させるだけでなく、エラーの原因となり、手動設定のミスやオンボーディングの遅延に関連するサポートリクエストの増加を招く可能性があります。
F5ソリューション	• Dynamic Client Registration (DCR)は、Zero Trust Accessが認証サーバー (AS)として構成されている場合に、クライアントアプリケーションがZero Trust Accessに登録するための自動化されたAPI駆動型の方法です。これにより、管理者の手動設定が不要になります。 • DCRはクライアントのメタデータを処理し、クライアントの認証情報を発行し、新しいクライアントをZero Trust Accessにシームレスに統合する、安全な登録エンドポイントを作成します。 • アプリケーション所有者は、アプリケーションを即座かつ直接自己登録できるため、管理者の手動設定を待つことなく、CI/CDパイプライン内でアプリケーションの認証および認可要件を直接管理できるようになり、開発速度とサイクルを大幅に向上させます。 • 管理者の貴重な時間を解放し、設定ミスを削減します。 • Model Context Protocol (MCP)サーバーやエージェント型AIなどにおける、クライアント登録を容易にします。

IPSec VPNのサポート

より強力なセキュリティ機能を提供



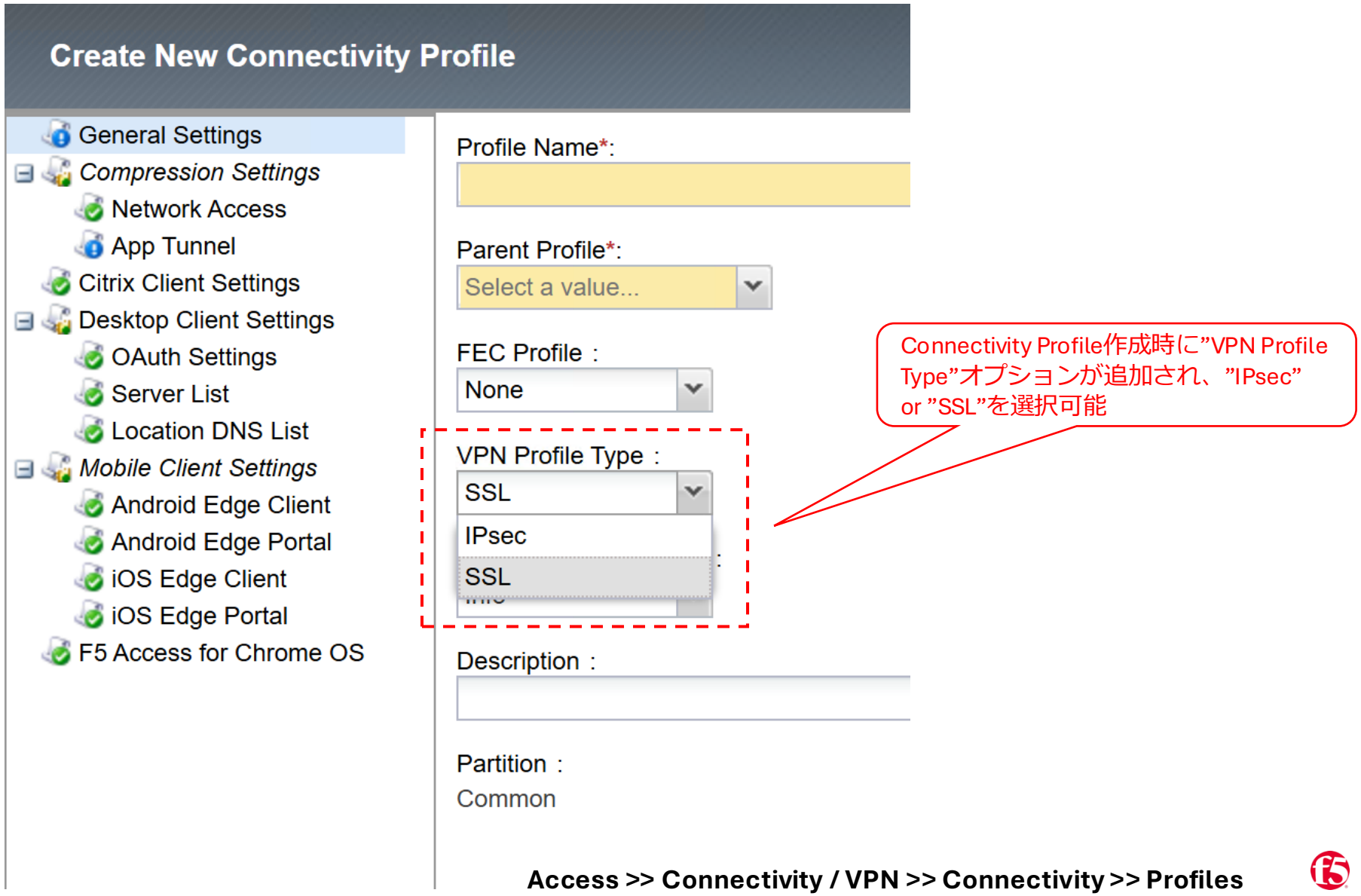
- **F5は連邦政府機関、治安機関、そして世界中の金融機関から信頼されている、包括的で高信頼性のVPNを提供するリーディングカンパニー**
- **グローバルなサイバーセキュリティ基準に準拠した優れたセキュリティを提供し、従来のSSL VPNに代わる堅牢なソリューションを提供することによって、現在の業界の期待に対処**

IPSec VPNのサポート

顧客課題	• IPsec VPNはネットワーク層で動作し、セキュアなネットワークプロトコルを使用してIPパケットを暗号化および認証することで、パブリックネットワーク上にプライベートで安全なトンネルを構築し、サイト間接続またはクライアント間接続においてエンドツーエンドのセキュリティを提供します。 • 世界のセキュリティ機関 (NSA、NCSCなど)は、組織に対してSSL/TLS VPNからIPsec VPNへの移行を推奨しています。IPsec VPNはPPP-SSL VPNと比較して、より高いセキュリティとパフォーマンスを提供します。 • 世界の一部の金融機関は、SSL VPNからの移行計画を開始しています。
F5ソリューション	• BIG-IP Zero Trust Access (APM)はIPsec VPNをサポートし、より強力なセキュリティ機能を提供します。 • グローバルなサイバーセキュリティ基準に準拠した優れたセキュリティを実現し、従来のSSL VPNに代わる堅牢なソリューションを提供することで、業界の最新ニーズに応えます。

IPSec VPNのサポート

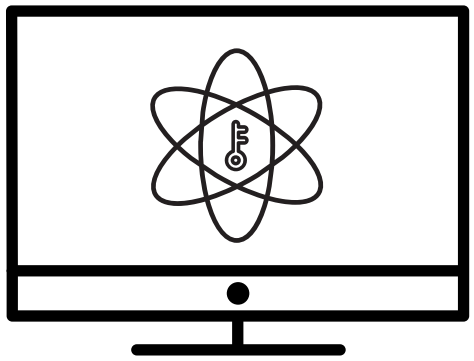
BIG-IP GUI



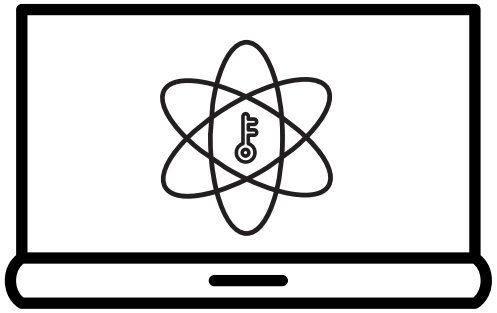
Access >> Connectivity / VPN >> Connectivity >> Profiles

Windows/macOSクライアントでのPQCサポート

PQCで保護されたSSL VPNアクセスを有効化



Windows



macOS

- クライアント側とサーバ側の両方で、主流のPQC暗号(ML-KEM)をサポート
- 実績のある従来の暗号技術と、新しい量子耐性アルゴリズムを組み合わせ、ハイブリッド暗号を構築
- “Harvest Now, Decrypt Later (HNDL)“攻撃などの現在の脅威と、将来の量子技術を用いた攻撃の両方に対するセキュリティを提供

Windows/macOSクライアントでのPQCサポート

顧客課題	• 金融サービス業界や政府機関を含む多くの企業が、現在PQCへの移行を検討しています。 • 同盟国や敵対国の政府、企業、そしてサイバー犯罪者たちは皆、量子コンピュータの開発に取り組んでおり、量子コンピュータが実現した日には、PII (個人識別情報)、PHI (医療情報)、政府機密、企業秘密など、現在の暗号化アルゴリズムによって保護されているあらゆる情報を解読できてしまう可能性があります。 • NISTのような政府機関は、量子耐性暗号 (QRC)を急速に構築しており、一部は最近標準化に至っています。
F5ソリューション	• TLSはVPNトンネルのセキュリティ確保に不可欠です。F5は、ポスト量子暗号 (PQC)を含む最先端の暗号技術の分野においてリーダーとしての役割を果たし、その開発を引き続き支援しています。 • Zero Trust Access (APM)およびそのクライアントにおいて、主流のPQC暗号 (ML-KEM)に対するクライアント側およびサーバー側のサポートを提供し、現在実績のある従来の暗号技術 (RSA、ECC)と新しい量子耐性アルゴリズムを組み合わせることで、今日の脅威と将来の量子技術による脅威の両方に対してセキュリティを提供するハイブリッド暗号を形成しています。

その他の注目すべき改善ポイント

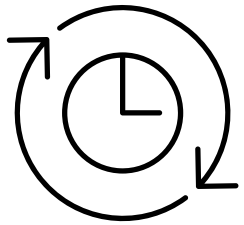
- **F5 Access (AndroidおよびiOS)におけるOIDCおよびFIDO2のサポート**
  - OIDCはフェデレーション機能のサポートにおいて広く受け入れられている事実上の標準です。
  - FIDO2は広く利用されている多要素認証メカニズムです。
  - BIG-IP Edge Clientでは、OAuth2およびSAMLプロトコルを通じて、すでにOIDCとFIDO2をサポートしています。
  - F5 VPNクライアント製品 (BIG-IP Edge ClientおよびF5 Access)全体でOIDCとFIDO2を統一的にサポートすることで、お客様は認証スキームを統一し、ネットワーク全体のセキュリティを強化できます。これにより、お客様がAPM (Zero Trust Access) クライアント向けに異なる認証スキームを設定する必要がなくなります。
- **クライアントサイドのHTTP/3 Web保護**
  - 従来のトランスポートプロトコル (HTTP/1.1、HTTP/2など)は、HTTP/3のような、より新しく、より安全で効率的なトランスポートプロトコルに取って代わられつつあります。
  - HTTP/3プロトコルをサポートすることで、基盤となるプロトコルに関係なく顧客エージェントのトラフィックをWeb攻撃から保護し、保護されていないプロトコル経路による攻撃対象領域とリスクを低減し、セキュリティ上の妥協を伴わずに最新のネットワークスタックへシームレスに移行することが可能になります。
  - HTTP/3として正式に定義されたHTTP over QUIC/UDPは、パケット損失によるパフォーマンスの低下を解消し、セットアップ遅延を短縮するという点で価値があります。

その他の注目すべき改善ポイント

- **OpenAPI Spec 3.1サポート**
  - OpenAPI Spec 3.1ファイルに基づいてAPIトラフィックを保護します。
- **Per-Session PolicyでのHTTP Connectorのサポート**
  - 外部サービスへの接続を必要とするPer-Session Policyが必要な場合、現在はこれを実現するにはiRuleの作成が必要となる場合があり、時間がかかり、遅延が生じる可能性があります。
    - 例: 特定のユーザーを認証・認可するために、REST API呼び出しを介してカスタムログインおよび認可サービスへの接続を必要とするセッションポリシーを保有している場合
  - APM (Zero Trust Access)のHTTP Connectorは、外部HTTPサーバーにHTTPリクエストを送信することができます。
    - これによりiRule等を使用することなく、Per-Session PolicyからAPM (Zero Trust Access)がHTTPコール呼び出しを行うことが可能です。
  - HTTP Connectorは通常、外部APIやサービスへのアクセスを提供するために使用されます。
    - 例: HTTP Connectorを使用して、サーバーを外部ブロックリストや外部レピュテーションエンジンと照合し、その結果をAPM (Zero Trust Access)のPer-Request Policyで利用
- **Linux ARM64 UbuntuでのEndpoint Inspectionサポート**
  - デバイスのポスチャーチェックをより包括的に実行し、安全なVPNアクセスを確保できます。

BIG-IP SSL Orchestrator v21.1

検査サービスの永続性: より強力なセキュリティ/完全なビュー



これまで: “ワークアラウンド”での対応

- 単一ユーザーのすべてのアクティビティを同一サービスで検査することを保証する簡単な方法がなく、コンテキストが断片化され、セキュリティ分析の一貫性確保が困難

今後: “ビルトイン”の機能

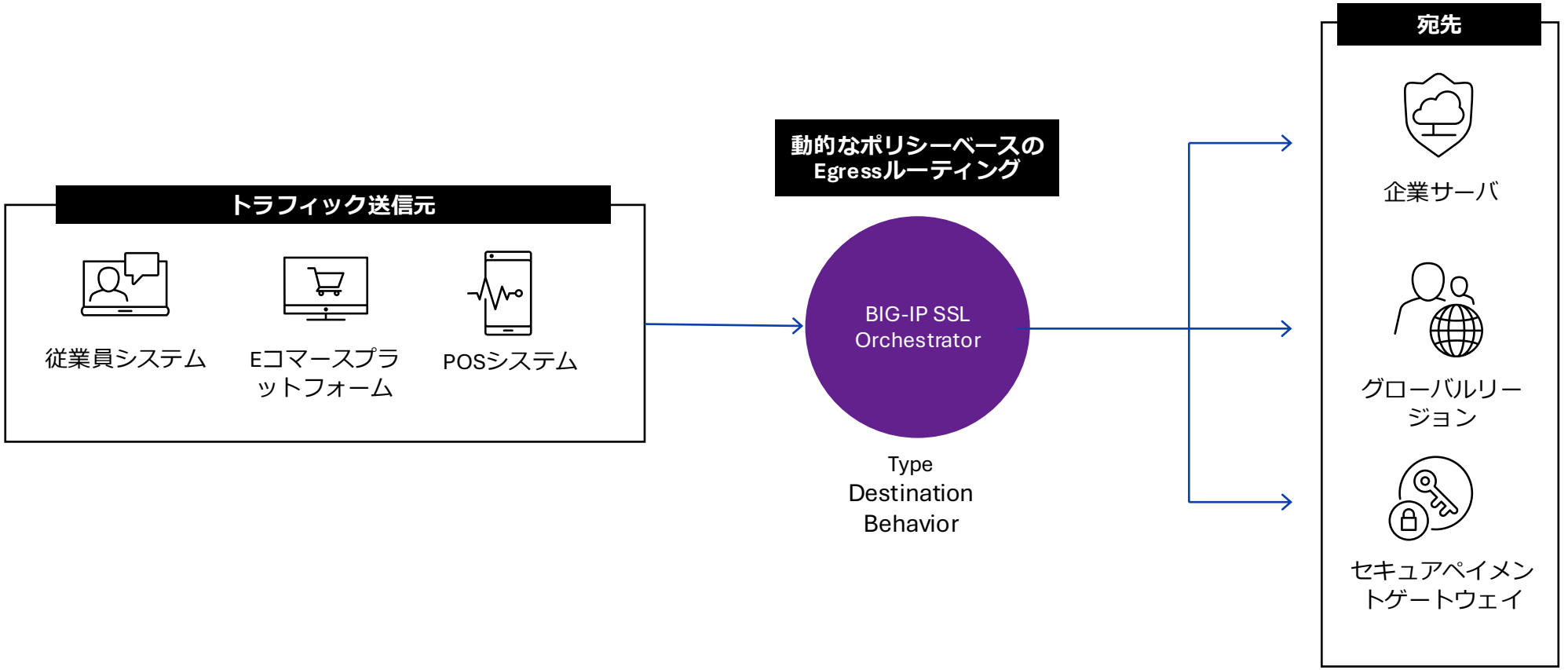
- **組み込み (ビルトイン)で提供される検査サービス永続性**により、すべてのユーザーアクティビティが一貫して検査され、シームレスなセキュリティが実現し、死角が減り、脅威検出が強化

検査サービス(Inspection Service)の永続性の提供

顧客課題	• 単一ユーザーのアプリ操作に関するすべての処理が同じサービスによって検査されることを確実にする必要がある場合があります。 • v21.0以前では、これを簡単に実現できる組み込みの方法はありませんでした。 • 一貫性 (パーシステンス)がない場合、ユーザーの操作が複数の検査サービスに分散され、どのサービスも全体像を把握できなくなります。 • この不完全な視点により、セキュリティ脅威の検知が難しくなり、組織のリスクが高まるだけではなく顧客の信頼を損なう可能性があります。 • いくつかの顧客では、カスタムiRuleのようなソリューションで対応しようとしましたが、これらのソリューションはrSeriesやVELOSのSSL Orchestratorでは動作しませんでした。
F5ソリューション	• SSL Orchestratorは、同じサービスでの検査の永続性が組み込み機能として追加され、これにより一時的な修正や回避策が不要になりました。 • パーシステンスにより、ユーザーの全てのアクティビティが同じ検査サービスで処理されるため、完全で一貫した可視化が可能になります。 • 脅威の検知が容易になり、正確で信頼性の高いセキュリティ分析を提供できます。

スムーズなEgressルーティング

- トラフィックに応じて、動的に変化するEgressルーティングポリシーを簡単に設定可能
- カスタムiRuleや複雑な設定は不要
- 運用を簡素化し、容易に拡張でき、手作業による負担を排除



ポリシーベースのEgress Routing

顧客課題	• トラフィックの種類や宛先などの条件に基づいて送信 (Egress)トラフィックをルーティンングする簡単な方法を必要としています。 • v21.0以前では、複雑なレイヤードアーキテクチャのパターンやカスタムiRuleに頼らざるを得ませんでした。 • このアプローチは非効率で管理が難しく、遅延やコスト増、技術的な制約につながっていました。
F5ソリューション	• 動的なポリシーベースのEgress Routingを、SSL Orchestratorの組み込み機能として提供できるようになりました。 • ポリシー内で直接トラフィックのルーティングルールを設定できるため、カスタムiRulesや複雑な構成が不要になります。 • ルーティングは自動化され、トラフィックの種類、宛先、挙動などの特性に応じて動的に適応する様になりました。 • この機能により、運用を簡素化され、ビジネスの要件に応じてスケールでき、手動のプロセスによる煩わしさを解消します。

その他の注目すべき改善ポイント

- **URLデータベースのミラーリング**
  - Forcepoint (Secure Web Gateway (SWG)のURL Filtering DBの提供元)はデータベースを更新し、新たに”Cryptocurrency (暗号通貨)”と”Crypto Mining (暗号通貨マイニング)”の2つのカテゴリを追加し、既存のカテゴリ名の標準化を行いました。
  - 変更内容には、特殊文字の単語への置き換え (例: “&”を”and”に変更)が含まれます。
  - これらの更新は、SSL OrchestratorおよびSWGのカテゴリー一覧にも反映されています。
- **L2サポートの拡張**
  - レイヤ2のInspection Service Poolで最大40デバイスをサポートし、以前の上限の7デバイスから大幅に拡張されています。
  - この改善により、段階的防御 (Defense-in-Depth)のセキュリティ戦略をより容易かつ信頼性を持って管理できるようになりました。
- **柔軟なプロトコル準拠を可能に**
  - SSL OrchestratorはL7/HTTPプロトコル準拠の確認を緩和する設定をサポートする様になり、セキュリティをバイパスすることなく、プロトコル非準拠の外部Webサイトもアクセス可能となりました。
  - この機能強化により柔軟性と強力なセキュリティ基準を両立し、固有の課題に対応しながら顧客ニーズを満たします。