# IP アドレスの重複に対するスケーラブルなソリューション

F5 Distributed Cloud Mesh は、オンプレミスでもクラウドでも、IP アドレスの重複を制御し、シームレスなサービス検出およびアドバタイズメントをサポートして、プライベートネットワーク間をきれいに分離し完全な到達可能性を保証します。

主な利点

**シンプルでスケーラブル**
ワンクリックのアウトバウンドとアプリ中心のインバウンドにより、1つずつのアドレス再マッピングにかかるオーバーヘッドが不要になります。

**効率的なフリート全体の管理**
ローカライゼーションを犠牲にすることなく、シームレスな一括設定を実現します。すべてのサイトを1つのフリートとして管理しながら、1回限りの例外を許容します。

**わかりやすさ**
フルスタックのエンドツーエンドソリューションとして、ポリシーと可観測性における手動でのリナンバリングによる混乱を解消します。

**アプリ間の自動接続向けに最適化**
統合されたサービスにより、IP アドレスの問題に関係なく、アプリがサービスアドバタイズメントおよび検出を実行できるようにします。

**包括的でシームレス**
マルチサイトのオーケストレーションにより、見過ごされる要素やカバーの穴がないことを保証します。すべてが機能します。

# IP アドレスの重複とは

企業組織は、これまでは別々であったプロジェクトを組み合わせることで得られる利点を活用しようとしています。しかし、重複や衝突するアドレス範囲でネットワークが構築されていることで、これらのシステムを接続できないことがあります。F5 Distributed Cloud Mesh は、IP アドレスの重複を修正し、シームレスなサービス検出およびアドバタイズメントをサポートして、プライベートネットワーク間をきれいに分離し完全な到達可能性を保証します。

## IP アドレスの重複の概要

これまで別々であったネットワークやセグメントを簡単に接続できるようになるにつれ、新しく接続されるセグメントのアドレスが既存のネットワークのものと競合する危険性が高まっています。直接ルーティングされるネットワークでは、ネットワークの他の部分がパケットを送信する方法を認識できるように、各セグメントで一意の IP サブネットアドレスを設定する必要があります。サブネットアドレスが別のネットワークセグメントと重複していると、ネットワークルーティングシステムは、どのセグメントが「本当の」宛先であるかを判断できなくなります。また、これまでは問題なかった、これらのセグメントを行き来するサービスが、到達不能になってしまいます。

パブリックインターネットでは、すべてのネットワークアドレス範囲が一元的に割り当てられているため、重複が広く問題になることはありません。ネットワーク内では、組織は、プライベート用に指定された特別な IP アドレスセットを再利用することで、利用可能な内部 IP アドレスの数を増やすことができます。このようなプライベート IP アドレスは、インターネット上でルーティングできないため、組織がいくつあっても組織により使用できますが、各アドレスは各組織内で一意に扱われなければなりません。つまり、IP アドレスは一度だけ使用するようにします。重複して使用すると、そのアドレスを行き来するトラフィックに問題が発生します。

従来、IP アドレスの重複は、組織の合併や買収でよく見られる、これまでは別々だった 2 つのネットワークが接続される場合のみに生じる問題でした。このような両方のネットワークで内部プライベート IP アドレスが使用されている場合、これらのプライベートアドレスの一部が両方のネットワークに割り当てられる可能性があります。

最近では、マルチクラウドネットワーキングツールが、仮想プライベートクラウド（VPC）や仮想ネットワーク（VNet）など、ネットワークセグメント間の仮想接続を俊敏に実現する方法を提供しています。IP の重複のための従来のソリューションでは、規模、制御またはマルチレイヤの問題により、このような環境への対応はより困難です。

そのため、マルチクラウドやエッジ導入のアーキテクチャの拡大により、IP アドレスの重複は、同じクラウド内であっても、ますます頻発する問題になっています。

主な特徴

**自動 Egress の送信元ネットワークアドレス変換（SNAT）**
IP が重複する領域から送信される接続は、自動的にプライベートネットワーク内でグローバルにルーティング可能なアドレスを使用します。

**サービスの検出とアドバタイズメント**
IP が重複する領域内のアプリは、アプリ間接続のためにルーティング可能なアドレスで、自動的に検出および再アドバタイズできます。

**アプリケーション配信**
サービスは送信元 IP アドレスから切り離され、統合されたセキュリティとアプリパフォーマンスのインストルメンテーションによる、クライアントとユーザーに対するフルスタックの可観測性が提供されます。

**柔軟な消費**
複数のサブネットやサイトにまたがるオーケストレーション構成により、リバースプロキシ（サービス IP がクライアントからリモート）またはトランスペアレントプロキシ（サービス IP がクライアントにローカル）のいずれかとして配信できます。

**単一サイトのシンプルさ、複数サイトのスケーラビリティ**
パブリックおよびプライベートクラウドの自動化を簡単に制御するための一元型 SaaS コンソールと、さまざまなクラウドプロバイダにわたるマルチサイトのオーケストレーションに拡張可能な一貫したインターフェイスを提供します。

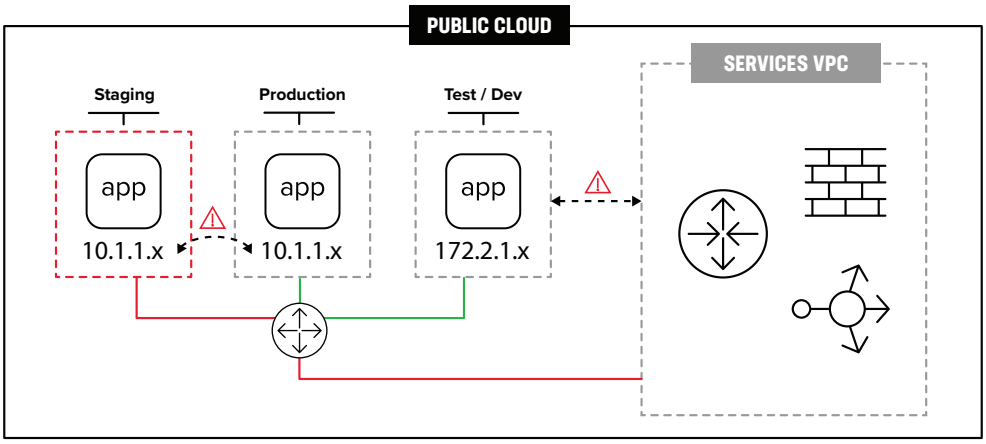


図 1：IP アドレスの重複とそれにより生じる問題

## IP アドレスの重複の例

上の図では、各リモートネットワークセグメントに、固有のパブリック IP インターネットアドレスが割り当てられていて、それぞれがプライベート内部 IP サブネットで構成されています。キャンパスと支店の拠点では、似てはいますが異なる内部サブネットアドレスで構成されていて、拡張により一元的な割り当てになる可能性があります。パブリッククラウドネットワークセグメントは、プライベート IP アドレス割り当てプールからの内部サブネットアドレスを使用しています。これらの新しく接続されるセグメントのいずれかが、同じ内部サブネットアドレスで構成されていた場合、問題が発生します。

- **従来のネットワーク：**従来のネットワーキング環境では、各セグメント内部は外部から隠れているため、問題は発生しません。パブリックまたはプライベートクラウドでホストされるサービスは、ロードバランサや NAT ピンホール、または同様の表示方法によって外部に公開されます。

- **マルチクラウドネットワーキング：**マルチクラウドネットワーキングを使用してパブリッククラウドとプライベートクラウドのネットワークセグメント間に直接 L3 ルーティング接続を作成することで、パブリッククラウドの仮想プライベートクラウド（VPC）とプライベートクラウドでサービス障害が発生する可能性があります。これらのセグメントでホストされる従来のアプリケーションは、到達不能になる可能性があります。分散型マイクロサービスアプリケーションでは、トラフィックにより内部エラーが発生し、ユーザー側 Ingress には影響がなくても、これらのサービスは到達不能になります。

この問題は、マルチクラウドネットワーキングが原因ではありません。マルチクラウドネットワーキングは、適切に実装されていれば、仮想的な直接接続を迅速に作成できるため、俊敏性を高めることができます。この問題が発生するのは、侵害されたプライベートアドレスの抽象化リー

マルチクラウドやエッジ導入のアーキテクチャの拡大により、IPアドレスの重複は、同じクラウド内であっても、ますます頻発する問題になっています。

クが俊敏性により明らかになるときです。これを解決するには、修正して将来的な発生を防止するスケーラブルなパターンを採用します。

## IP の重複に対する従来の手法

- **防止：**IP アドレスの重複に対処する最も確実な方法は、ネットワークアドレスを一元的に割り当て、これを防止することです。これを行うのは、インターネット上では Internet Assigned Numbers Authority（IANA）であり、ほとんどの組織では、IT 部門にあたります。ほとんどの大規模な組織では、IP アドレス管理（IPAM）のための特別なツールを使用していますが、一部の地域では、スプレッドシートのようなツールを使用して手動でアドレスを追跡しています。この手法は、合併によって別のネットワークとの結合が必要になる、または「シャドー IT」プロジェクトで統合が必要になる、あるいはパブリッククラウドのような以前の外部ネットワークへの直接接続が必要になるなど、IT 部門が制御できない事態が起こるまではうまく機能します。

- **リナンバリング：**重複に対する従来の対策は、「リナンバリング」、または他と重複するセグメントの IP アドレスを変更することです。これは、そのセグメントのルーター、セグメント上のすべてのデバイス、およびそれらのデバイスへのすべての外部参照を再構成することを意味します。これは面倒で間違いが起こりやすい作業ですが、少なくとも次の合併までは一度だけで済む作業です。また、マルチクラウドやエッジ環境では常に可能というわけではありませんが、IT 部門に変更できる権限がある場合、これは有効です。

- **ネットワークアドレス変換：**IP の重複に対するより最新の一般的な解決策は、ネットワークアドレス変換（NAT）を使用することです。これは、セグメントにネットワークの他の部分とは異なるサブネットが割り当てられているように見せるだけです。NAT は、組織のネットワークがパブリックインターネット内におけるプライベートネットワークであるのと同様に、セグメントを組織全体のネットワーク内における独自のプライベートネットワークに効果的に変えます。

## マルチクラウドネットワーキングと最新アプリケーション

NAT は、歴史的に見てもリナンバリングよりはるかに簡単ですが、その代償として、内側と外側の 2 つの別々の領域が形成されます。すべてのトラフィックが従来のトラフィックである場合、この分離を維持することによる影響はごくわずかです。しかし、トラフィックでは、アプリの内部を相互通信させるために、サービスのアドバタイズメントと検出が追加されます。NAT では、サービス調整レイヤーは、何が「内部」リソースで何が「外部」リソースなのかを認識する必要があ

DISTRIBUTED CLOUD MESH は、ネットワーキング、セキュリティ、アプリケーションおよびサービスの可観測性を提供するため、大規模な管理と個別の可視化のどちらも妥協しません。

ります。

クラウドのような大規模な環境では、特に、スケーラブルなパターンが必要です。これがないと、各 VPC または VNet は、サービスの到達可能性を維持するために、その独自の「内部」となり、他のすべてを「外部」として扱わなければなりません。

# F5 Distributed Cloud Mesh：IP アドレスの重複に対するスケーラブルなソリューション

F5® Distributed Cloud Mesh は、SaaS ベースでアプリを中心としたネットワークおよびセキュリティサービスを提供し、1 つまたは複数のパブリックおよびプライベートクラウド内のネットワークにおける管理を統合し、相互接続を簡素化します。

## マルチクラウドネットワーキングにおける IP アドレスの重複を解決する方法

F5 Distributed Cloud Mesh は、導入してすぐに問題を解決および防止するシンプルでスケーラブルなソリューションにより、IP の重複を解決します。各仮想ネットワークセグメントは、ルーターではなく、トランスペアレントプロキシによって他のセグメントと接続されます。仮想ネットワークセグメント（VNS）内から始まる接続は、その途中で、送信元ネットワークアドレス変換（SNAT）により、ネットワーク内全体でルーティング可能なアドレスに変更されます。

仮想ネットワークセグメントへの受け入れを許可すべき接続に対して、このプロキシは、他のネットワークも利用できるようにする必要がある各アプリやサービスを検出し、そのサービスをネットワークの残りの部分にアドバタイズできます。従来、この機能は、発信元および宛先アドレスに対するファイアウォールポリシーで表現されていました。ここでの違いは、各仮想ネットワークセグメントのプロキシが、分散したファイアウォールのように動作し、互いに隔離することで、仮想ネットワークセグメントの IP アドレスを各セグメント内のすべてのアプリケーションに対して透過的にするという点です。便利なツールは、作業を難しくするのではなく、簡単にするものなので、すべての設定はオーケストレーションおよび自動化されます。

必要であれば、トラフィックのニーズに応じて、各セグメントの方法およびポリシーを個別に制御できます。さらに細かい制御が必要な場合、Ingress と Egress を API ゲートウェイで処理し、可視化とポリシー適用を強化することもできます。抽象化をなくして直接ルーティングされたアクセスを作成することもできますが、この場合は IP の重複の保護が無効になるという注意点があります。

## 最新アプリケーションにおける IP アドレスの重複を解決する方法

スケーラビリティの観点からも、Distributed Cloud Mesh には大きな利点があります。すべてのサイトを 1 つのフリートとして管理できるため、管理者はサイトを 1 つの論理オブジェクトのように扱って設定し、サイト固有の詳細は自動化によって処理できます。これにより、多数のサイトを管理する複雑さが軽減され、単一のファイアウォールポリシー、単一のネットワークポリシー、

単一のサービスポリシーなどが、数百または数千のサイト全体に反映されるシンプルな構成が可能になります。 自動化により、アプリは、重複の有無に関係なく IP アドレスから切り離され、相互に検出および接続できようになります。

さらに、Distributed Cloud Mesh は、ネットワーク、セキュリティ、アプリケーションおよびサービスに対して、アプリケーションベースの可観測性を提供するため、IP アドレスによる曖昧さがなくなり、大規模な管理と個別の可視化のどちらも妥協しません。

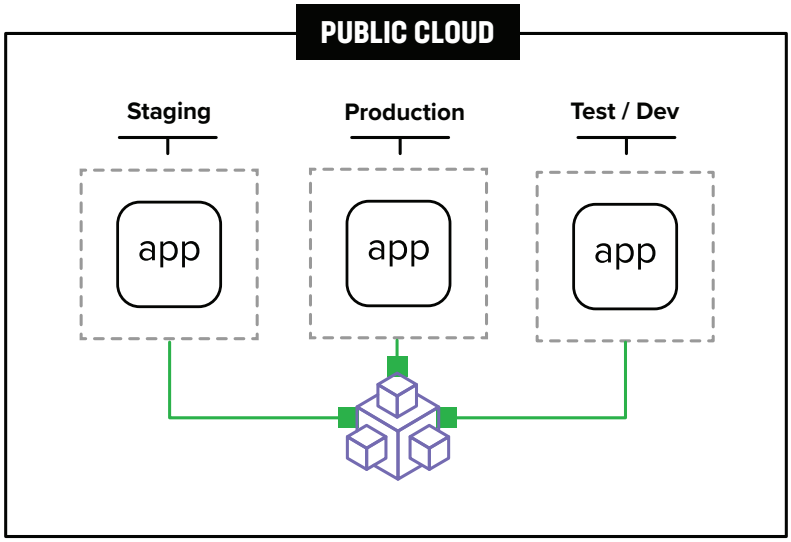


図 2：アプリレイヤーネットワーキングを介して IP アドレスの重複の解決方法

## まとめ

ネットワークが成長するにつれ、IT 部門は必然的に、これまではベストプラクティスと考えられていた古い次善策により引き起こされる問題に直面します。F5 は、IT および運用チームが最新のインターネットのライフサイクル全体でアプリケーションを配信できるよう支援してきました。また、Distributed Cloud Mesh により、将来にわたって新たな問題を引き起こすことなく、デジタル変革の継続的なプロセスを支援する準備が整っています。F5 は、大規模なアプリケーション配信を支援できます。

**IP アドレスの重複の解決は F5 Distributed Cloud Mesh の一部として提供されています。詳細については、無料トライアルに登録して、実際にお試しください。**

**F5 Distributed Cloud 販売担当部の専門家にご質問がある方は、sales@f5.com までお問い合わせください。**