SDA導入のためのSD-WANでの最適なISE IP MTUの設定

内容

はじめに

このドキュメントでは、SD-WANを使用してSDAサイトを接続する際に、最大伝送ユニット(MTU)の問題がSDAのマイクロセグメンテーションにどのように影響するかについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- シスコソフトウェア定義型アクセス(SDA)
- シスコソフトウェア定義型ワイドエリアネットワーク(SD-WAN)
- Cisco Identity Services Engine（ISE）

使用するコンポーネント：

このドキュメントの情報は、SDA、SDWAN、およびISEに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

現代の企業ネットワークでは、SDAを活用してきめ細かなマイクロセグメンテーションと一貫したポリシーの適用が行われるようになっています。分散したSDAサイトを接続するために、Cisco SD-WANが採用されることが多く、さまざまなアンダーレイネットワーク上で俊敏で安全かつ最適化された転送を実現します。このアーキテクチャの中核をなすISEは、重要な認証、許可、アカウンティング(AAA)サービスとともに、動的なポリシーの配布(たとえば、セキュリティグループタグ(SGT)やダウンロード可能ACL)を提供します。

これらの強力なテクノロジーを統合することで、堅牢な一方で、微妙でありながら影響の大きい設定の課題が発生する可能性があります。重要なネットワークハンドオフポイントおよびSD-WANオーバーレイ間でのMTU処理は、このような問題の主な領域です。この記事では、ネットワークの動作を中断させる可能性のある2つの一般的なMTUの不一致のシナリオについて説明します。

1. SDAボーダーノードとSD-WANエッジデバイス間のMTUギャップ
2. SD-WANオーバーレイを通過するISE発信トラフィックのMTU制約

パケットのフラグメンテーションの問題やサイレントドロップを防止し、信頼性の高い認証、ポリシーの適用、およびネットワーク全体の安定性を確保するには、MTUを適切に調整することが重要です。これらの問題に対処しないと、接続やポリシーの適用に断続的な障害が発生し、トラブルシューティングに多大な労力を要する可能性があります。

MTUのアラインメントが正しくない場合の一般的な症状

MTUのアラインメントが誤っていると、さまざまな形で現れ、診断が困難な問題につながる場合があります。

- 断続的なRADIUS認証の失敗またはタイムアウト：大きなRADIUSパケットを生成するポリシー（たとえば、広範なAVペアまたは証明書を持つポリシー）では特に顕著です。
- エンドポイントがダウンロード可能ACL(dACL)またはTrustSecポリシー(SGT/SGACL)の受信または適用に失敗する：これらのポリシーは大きなRADIUSパケットで伝送されることがよくあります。
- 認証済みクライアントのセッション確立が遅い：アプリケーション層での再送信が原因です。
- 過剰なRADIUS再送信：ISEログまたはネットワークアクセスデバイス(NAD)で確認できます。
- 一貫性のないポリシーの伝搬：ISEで行われたポリシーの変更が、リモートSDAサイトのすべてのNADに一貫性のある形で伝搬されるとは限りません。

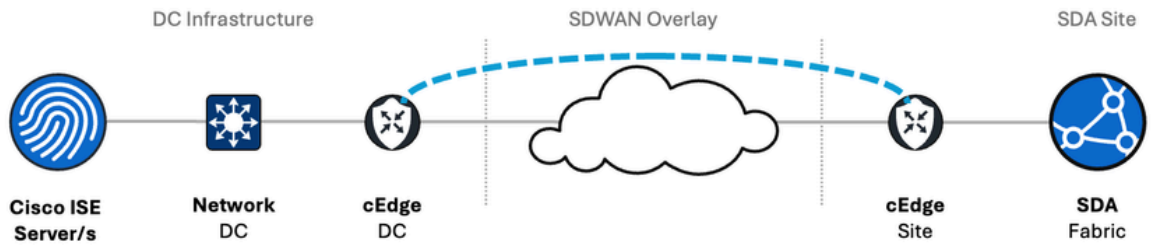
- パケットキャプチャの不一致：キャプチャで、ISEがDo Not Fragment(DF)ビットが設定された大きなパケット(たとえば>1450バイト)を送信したが、NADまたはSD-WANシスコエッジルータからの対応する応答またはICMPの「Fragmentation Needed」エラーがないことが示されます。
- パケットドロップカウンタの増加：データセンター(DC)のCiscoエッジルータの入力インターフェイスで、ISEから発信されたSDAサイト宛てのトラフィック、または逆方向のトラフィックのSDA境界に面したSD-WANのCiscoエッジルータインターフェイスで観察されます。

問題の説明

一般的なエンタープライズ展開
一般的な企業トポロジについて考えてみます。

- Cisco ISEサーバ：DCネットワークインフラストラクチャに接続された集中型データセンター(DC)またはリージョナルハブに導入されます。
- DCインフラストラクチャ：ISEサーバが接続するDCコアスイッチまたはアグリゲーションスイッチで構成されます。
- SD-WANオーバーレイ：DCのCiscoエッジルータルータは、アンダーレイ転送ネットワーク(例：インターネット、MPLS)を介してリモートSDAサイトのCiscoエッジルータルータにSD-WANトンネル（一般にIPsec）を確立します。
- SDAサイト：リモートサイトのCiscoエッジルータルータは、ファブリックエッジノード、ボーダーノード、ワイヤレスLANコントローラ(WLC)、および最終的にはエンドポイントを含むローカルSDAファブリックに接続します。

トポロジの例



チャレンジ1:MTUギャップ – SDA境界からSD-WANエッジへ

Cisco SDAの設計原則は、通常はLANオートメーションを介して実装され、すべてのファブリッ

クデバイスでキャンパス全体のMTUが9100バイト（ジャンボフレーム）になることを促進します。これにはCatalyst 9000シリーズのボーダーノードが含まれ、イーサネットジャンボフレームがファブリック内で効率的に転送されます。その結果、SDAボーダーノード上のレイヤ3またはSVIハンドオフインターフェイスは、デフォルトでこの大きなMTUになります。

逆に、Catalyst 8000シリーズなどのSD-WANエッジデバイスは、通常、1500バイトのインターフェイスMTUにデフォルト設定されます。これは、ジャンボフレームのサポートが一般的でないか、または有効になっていないインターネットサービスプロバイダー(ISP)などの外部ネットワークに接続するインターフェイスの標準です。

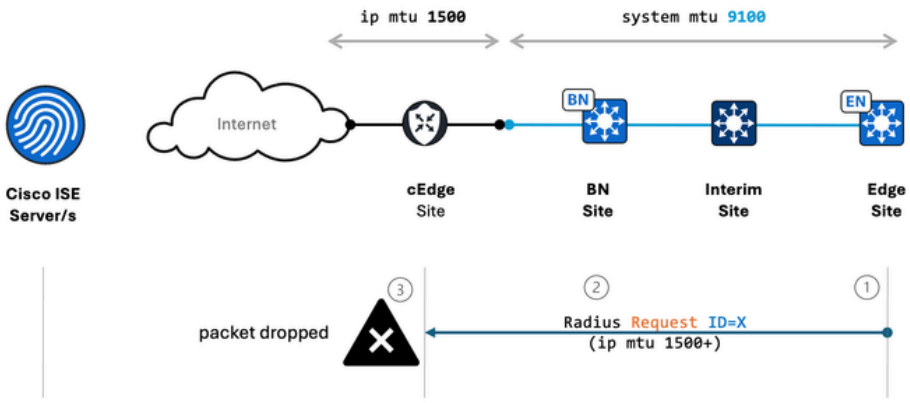
この差により、潜在的な障害の直接的なポイントが発生します。SDA境界が1500バイトよりも大きいIPパケットをSD-WANエッジに送信しようとする際に、受信インターフェイスに1500バイトのMTUが設定されています。

このタイプのMTUの不一致は、SDAの導入における一般的な落とし穴であり、設定中に見落とすことがよくあります。さらに困難な点は、Cisco IOS-XE®を実行するCatalyst 9000スイッチでRADIUS要求が生成される方法に関連する特定の動作によって、これらの問題が引き起こされる可能性が特定の重大な状況下でのみ発生する点です。

たとえば、Session Manager Daemon(SMD)プロセスで処理されるエンドユーザ認証プロセス中に生成されるRADIUS要求は、1396バイトでパケットをフラグメント化するようにハードコードされます。一方、Security Group Access Control List(SGACL)などのTrustSecポリシーの取得に関連するRADIUS要求は、Cisco Internetworking Operating System(IOSd)デーモン(IOSd)サブコンポーネントによって生成されます。これらはMTUに対応しており、サイズがシステムMTU（通常は最大9100バイト）を超えない限り、パケットのフラグメント化を回避できます。

その結果、MTUの不一致に関連する問題は、Cisco TrustSec(CTS)ダウンロードポリシーが使用されている場合にのみ明らかになります。また、ユーザ認証中にSDAエッジデバイスによってダウンロードされるロールベースアクセスコントロールリスト(RBACL)のセットは、他のタグ用にどのSGACLポリシーがすでに存在しているかによって異なる場合があります。実際には、スイッチはポリシーセットの重複しない部分だけをダウンロードします。

同時に、これらの動作は、SGACLポリシーのサイズ、現在のシステムの状態、および最終的にはパスに沿ったMTUの不一致に応じて、サイレント障害から不完全なポリシーダウンロードに至るまで、予測不能で一貫性のない結果を生み出す可能性があります。



SDA Borderは大きなRADIUSパケット(たとえば、1600バイト)をSD-WANエッジ経由でISEに転送します。次のことが起こります。

1. SDA Borderは、9100 MTUインターフェイスを使用して1600バイトのIPパケットを送信します。
2. SD-WAN Ciscoエッジルータは、1500 MTUインターフェイスでこのパケットを受信します。
3. ただし、これらのRADIUSパケットにDo Not Fragment(DF)ビットが設定されていない場合、SD-WAN Ciscoエッジルータでは、設定されているインターフェイスMTUに比べて「サイズが大きすぎる」というだけの理由で、入力時にDFビットのドロップが頻繁に発生します。 IP転送ロジックの段階には進まず、フラグメント化を検討できます（DFビットで許可されている場合）。

このサイレントドロップは、特に問題が指向性（SDAからSD-WAN/ISE）であるため、重大なトラブルシューティングの問題につながります。

同様のMTUの不一致が、データセンター(DC)のコアスイッチまたはリーフスイッチでも発生する可能性があります。通常、これらのスイッチは、内部DCトラフィックの効率性を高めるためにジャンボフレーム(たとえば MTU 9000+)をサポートするように設定されています。ただし、トラフィックが標準のMTU(たとえば 1500バイト)で設定されたSD-WAN DC Cisco Edge Router（ESR；シスコエッジルータ）のLAN側インターフェイスに渡された場合、この不一致が原因で特にDCネットワークからSD-WANファブリックに流れ込むトラフィックで、フラグメンテーションやパケット廃棄が発生する可能性があります。

課題1の解決策：

SDA Borderのハンドオフインターフェイス（物理またはSVI）のIP MTUを、ピアリングするSD-WAN Ciscoエッジルータインターフェイス（通常は1500バイト）に合わせます。

設定例（SDAボーダーノード）:

<#root>

```
!
interface Vlan3000  // Or your physical handoff interface, for example, TenGigabitEthernet1/0/1
 description Link to SD-WAN cEdge Router
 ip address 192.168.100.1 255.255.255.252


ip mtu 1500

  // Align with SD-WAN cEdge receiving interface MTU
!
```

重要な考慮事項：Catalyst 9000境界でのフラグメンテーション

Catalyst 9000シリーズスイッチは、SDAボーダーノードとして、ハードウェアデータプレーンのネイティブIPパケットのIPフラグメンテーションをサポートします。ハンドオフインターフェイスのip mtuを1500に減らしても、それが必要な境界を発信元または通過するトラフィックに対す

るソフトウェアベースのフラグメンテーションによるパフォーマンスの低下は発生しません。スイッチは、1500バイトを超えるIPパケット（DFビットがクリアされている場合）を、この特定のインターフェイスから出力する前に、CPUにパントすることなく効率的にフラグメント化します。

ただし、Catalyst 9000スイッチは通常、VXLANカプセル化トラフィックのフラグメンテーションをサポートしないことに注意してください。この制限は、オーバーレイトラフィックに対しては重要ですが、説明されているRADIUS認証シナリオには影響しません。SDA境界と外部ISE間のRADIUS通信は通常、アンダーレイ（ネイティブIPルーティング）内で発生するためです。（VXLANオーバーレイに関するMTUの考慮事項は、個別の複雑なトピックであり、関連するCisco SDA設計ガイドに詳細が記載されています）。

SDA境界からSD-WANへのCiscoエッジルータのハンドオフでは、事前のMTU調整が不可欠です。

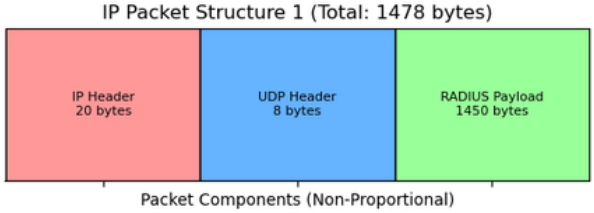
チャレンジ2:MTUのスクイーズ – SD-WANオーバーレイを通過するISEトラフィック

ISEネットワークインターフェイスカード(NIC)、スイッチポート、ルータインターフェイスなどの個々の物理インターフェイスが標準の1500バイトのIP MTUに設定されている場合でも、SD-WANオーバーレイ自体によりカプセル化のオーバーヘッドが発生します。このオーバーヘッドにより、1500バイトの制限の一部が消費され、元のIPパケットで使用可能な実効 MTU(MTU)が減少します（ISEの観点からは「ペイロード」）。

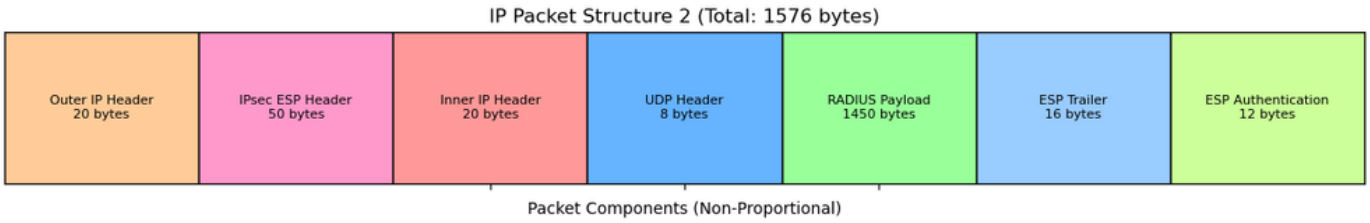
パケット構造とカプセル化のオーバーヘッド：

ISEサーバからのIPパケット(たとえば、RADIUS Access-Acceptパケット)がSDAサイトのNetwork Access Device（NAD；ネットワークアクセスデバイス）に送信されると、SD-WANオーバーレイを通過してカプセル化されます。一般的なカプセル化スタックには、トンネルモードでのIPsecが含まれており、NATトラバーサル(NAT-T)用のUDPを経由する可能性があります。

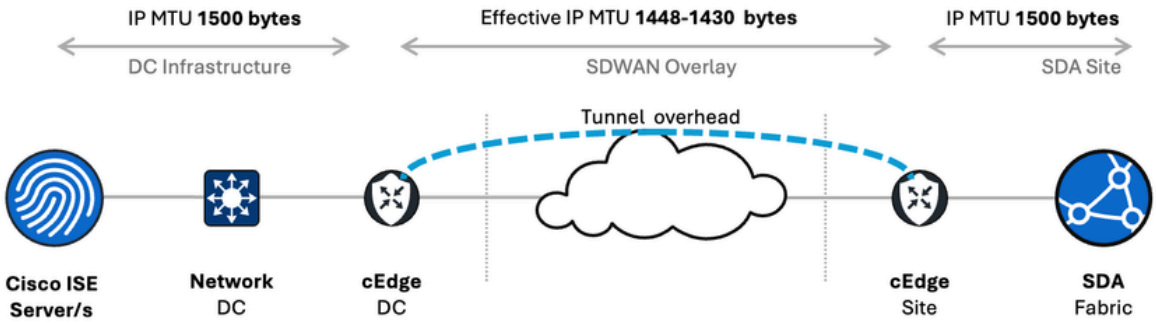
- ISEからのオリジナルパケット（内部パケット）：
  たとえば、1450バイトのペイロード+ 8B UDP + 20Bの内部IP = 1478バイトのRADIUSパケットです。



- NAT-TのUDPカプセル化を使用する可能性がある、トンネルモードのIPsec ESPを検討してください。



- オーバーヘッドの合計は、特定のIPsec暗号、認証メカニズム、およびその他のオーバーレイ機能（使用されている場合はGREなど）によって異なります。 一般的な計算は次のとおりです。
    - 外部IPヘッダー(IPv4):20バイト
    - UDPヘッダー（NAT-T用のESP over UDPの場合）:8バイト
    - ESPヘッダー：最大8バイト
    - ESP IV(AES-CBCの例)：最大16バイト（該当する場合）
    - ESP認証(例:HMAC-SHA256 truncated)：約12 ~ 16バイト
    - 一般的なIPsecオーバーヘッドの概算：最大52 ~ 70バイト（すべてのオプションでより大きく最大80バイト以上まで可能）。



物理リンクMTUが1500バイトの場合、ISEから元のIPパケットで使用可能なペイロードMTUは、1500バイト – SD-WANオーバーヘッドになります。
たとえば、1500 - 70 = 1430バイトです。

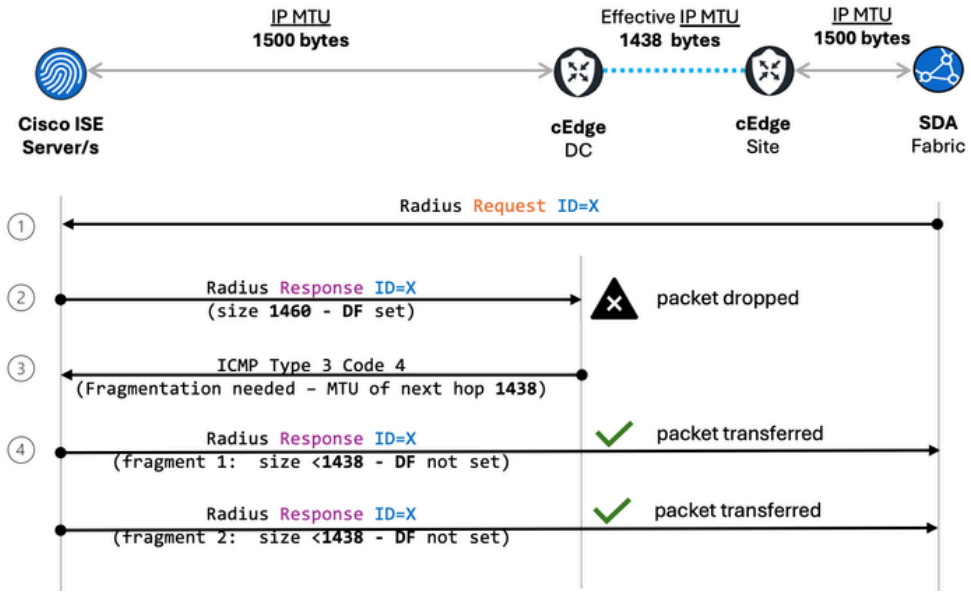
パケットが実効MTUを超えたときの動作：

1. ISEがパケットを発信する（DFビット異常）：
    - デフォルトでは、ISEアプライアンスの基盤となるLinuxオペレーティングシステム(OS)によって、設定されたインターフェイスIP MTU(たとえば、1500バイト)以下である発信パケットすべてのIPヘッダー内に、Do Not Fragment(DF)が設定されます。
    - このDFビットの目的：ISE（OSを介して）は、後で説明するパス最大伝送ユニット検出(PMTUD)プロセスを主に活用するために、DFビットを事前に設定します。これにより、ISEは自身のインターフェイスMTUよりも小さい場合に、宛先への実際のPMTUを動的に学習できます。

- インターフェイスMTUより大きいパケットの動作：ISEが、設定されているインターフェイスIP MTUより大きいIPパケットを送信する必要がある場合、動作はLinuxオペレーティングシステムによって異なります。通常、OScanfragmentはpacketbeforetransmissionをフラグメント化し、これらのフラグメントのDFビットをクリア（DF=0を設定）します。このフラグメンテーションはOSレベルの機能であり、ISEアプリケーションコード自体によって直接実行されるものではありません。
- ネットワークデバイスとの主な違い：このISEのデフォルト動作（インターフェイスMTU内に収まるフラグメント化されていないパケットに対してもDF=1を設定）は、従来の多くのネットワークデバイス（ルータ、スイッチ）とは大きく異なります。 ネットワークデバイスでは、DFビットが発信または転送されるパケットに関しては、通常、そのように明示的に設定されていない限り、あるいは、転送されるパケットにすでにDFビットが設定されている場合や、すでにDFビットを必要とする特定のプロトコルに関しては、DFビットの設定は行われません。通常、パケットがネクストホップのMTU（およびDF=0）を超えると、デフォルトでフラグメンテーションが可能になります。
- 複雑さのトラブルシューティング：この非対称の動作では、ISEからNADへのトラフィックにはデフォルトでDF=1が使用されることが多いのに対し、NADからISEへのトラフィックにはDF=0を使用できます（NADが理由で設定していない場合）。これにより、トラブルシューティング時に複雑さが増す可能性があります。エンジニアは、トラフィックフローの方向に応じて、異なるフラグメンテーション動作とPMTUDの相互作用を観察できます。

2. パケットが入力Ciscoエッジルータ(DC)に到達する:DC CiscoエッジルータがISEからIPパケットを受信します。
3. Ciscoエッジルータによるカプセル化とMTUチェック：Ciscoエッジルータは、SD-WANトンネル用にパケットのカプセル化を試みます。
    - 元のパケットのサイズ（バイト）SD-WANカプセル化オーバーヘッドがCiscoエッジルータの送信物理インターフェイスMTU(たとえば1500バイト)を超えており、ISEからの元の（内側の）パケットにDFビットが設定されている場合、Ciscoエッジルータは内側のパケットをフラグメント化する必要はありません。
    - Ciscoエッジルータはパケットをドロップします。
    - さらに重要な点として、Ciscoエッジルータは、ICMPの「Destination Unreachable - Fragmentation Needed and DF bit set」（タイプ3、コード4）メッセージを送信元(ISE)に送信し、ネクストホップのMTU（トンネルの実効MTU）を示す必要があります。
4. パスMTUディスカバリ(PMTUD)プロセス：このICMPの「Fragmentation Needed」メッセージを受信した時点で、ISE（送信元OS）はその特定の宛先パスのPMTUの予測値を減らす必要があります。この情報をキャッシュし、新しく検出されたPMTU内に収まる小さなパケットでデータを再送信します。

PMTUDプロセス図：



PMTUD通信の故障箇所：
理論上はPMTUDは堅牢ですが、実際には失敗する可能性があります。

- ICMPフィルタリング：中継ファイアウォールまたはセキュリティポリシーによってICMPメッセージがブロックされることが多く、「Fragmentation Needed」メッセージがISEに到達しません。
- Ciscoエッジルータでのコントロールプレーンポリシング(CoPP):Ciscoエッジルータルータは、CoPPを使用してCPUを保護します。ICMPエラーメッセージの生成は、コントロールプレーンのタスクです。負荷が高い場合、またはサイズが大きすぎるパケットが多い場合、CoPPはICMP生成をレート制限またはドロップできます。ISEはフィードバックを受信しません。
- サイレントドロップ：ISEがICMPの「Fragmentation Needed」メッセージを受信しない場合、パス制限を認識しません。DFビットが設定された大きなパケットを送信し続けるため、これらのパケットは入力側のCiscoエッジルータによって通知なしに廃棄されます。その結果、アプリケーション層のタイムアウトと再送信(RADIUSなど)が発生します。
- ISEサービスへの影響：大きなRADIUS Access-Acceptパケット（dACL、広範なAVP、SGT情報を含む）は特に影響を受けやすくなります。臨床像としては以下のものがある：
  - 断続的または完全な認証障害。
  - エンドポイントが正しいネットワークアクセスポリシーまたはSGTを受信していない。
  - ISEとNADの間のポリシー同期が不完全であるか、失敗しました。

課題2に対するソリューション：予防的ISE IP MTU設定

PMTUDの信頼性が低いことを考慮すると、ISEなどの重要なサービスには予防的なアプローチが

最適です。ISEのネットワークインターフェイスのIP MTUを、予想されるSD-WANオーバーレイオーバーヘッドの最大値に安全に対応できる値に設定します。これにより、ISEは、中間デバイス（DF=1の場合は禁止）によるフラグメンテーションを必要とせずに、SD-WANオーバーレイを通過するには本質的に大きすぎるIPパケット（DFビットが設定されている）を発信しなくなります。

推奨されるISE IP MTUの計算と設定：

1. 基本物理MTUの確立：これは通常、パス上の標準イーサネットインターフェイス用の1500バイトです。
2. SD-WANカプセル化のオーバーヘッドの最大値の判別：
    - 特定のSD-WANオーバーレイ（IPsec、GRE、VXLAN、MPLSoGREなど）によって生じる総オーバーヘッドを正確に計算するか、控えめに見積もります。 選択したプロトコルとオプションの正確な数値については、ベンダーのマニュアルを参照してください。

コンポーネント	オーバーヘッドの例（バイト）	注意事項
基本物理MTU	1,500	物理リンク上の標準イーサネット
少ない：SD-WANオーバーヘッド		
外部IPヘッダー(IPv4)	20	
UDPヘッダー（NAT-T用）	8	ESPがUDPでカプセル化されているかどうか
ESP ヘッダー	~8-12	
ESP IV(AES-CBCなど)	~16	暗号化アルゴリズムによって異なる
ESP認証(例:SHA256)	~12-16	認証アルゴリズムによって異なる(たとえば、一部のプロトコルでは96ビット)
その他のオーバーレイ（GREなど）	可変	SD-WANカプセル化スタックの一部である場合に追加
見積もりオーバーヘッド合計	68 ~ 80バイト以上	導入に関連するすべてのコンポーネントの合計
有効パスMTU	~ 1432 ~ 1420バイト	基本物理MTU – 合計推定オーバーヘッド

3. 推奨されるISE IP MTU設定：
    - 計算された有効パスMTU（この例では1420バイト）を使用します。
    - 追加の安全マージン（たとえば、20 ~ 70バイト）を差し引いて、マイナーな未計上のL2ヘッダーを計上するか、バッファを提供します。
    - Cisco SD-WANなどのソリューションでは、サイト間トンネルごとに個別にパスMTU(PMTU)ディスカバリを実行できます。このメカニズムは20分ごとに自動的に実行され、各サイトの現在のトランスポート条件に従ってトンネルのIP MTUをテストし、動的に調整します。その結果、MTU値はサイト間で異なり、時間の経過とともに変更される可能性があります。
    - このようなシナリオにおけるISEインターフェイスの一般的に安全で推奨されるIP MTUは、1350 ~ 1400バイトです

1350バイトのIP MTUは、多くの場合、非常に堅牢な出発点です

ISEの設定（CLIでの例）：

このコマンドは、関連するネットワークインターフェイスごとにCisco ISEアプライアンスのCLIで実行されます。

<#root>

```
!
interface GigabitEthernet0  ! Or the specific interface used for RADIUS/SDA communication

 ip mtu 1350
!
```

ISE IP MTUの変更に関する運用上の重要な考慮事項：

- Service Restart Required:ip mtuコマンドがISEインターフェイスに適用されると、ISEアプリケーションサービスの再起動が求められます。これはサービスに影響を与える変更であり、計画されたメンテナンスの時間帯にスケジュールする必要があります。手順の詳細については、Cisco ISEの公式ドキュメントを参照してください。
- すべてのISEノードに適用：このIP MTU調整は、SD-WAN経由でNADと通信する導入のすべてのISEノード(プライマリPAN、セカンダリPAN、ポリシーサービスノード(PSN))に一貫して適用する必要があります。MTU設定に一貫性がないと、予期しない動作が発生します。
- 徹底的なテスト：実稼働環境に実装する前に、ラボまたはパイロット導入でこの変更を厳密にテストします。さまざまなパケットサイズでpingなどのツールを使用し、DFビットを設定して、エンドツーエンドのMTU処理を検証します。
    - Linuxベースのシステム

```
ping
        -s
         -M do
```

(注：-sはICMPペイロードサイズを指定します。合計IPパケットサイズ=ペイロード+ 8B ICMP

Hdr + 20B IP Hdr for IPv4)

- Windows：

```
ping

        -f -l
```

(注：-lはICMPペイロードサイズを指定します)。

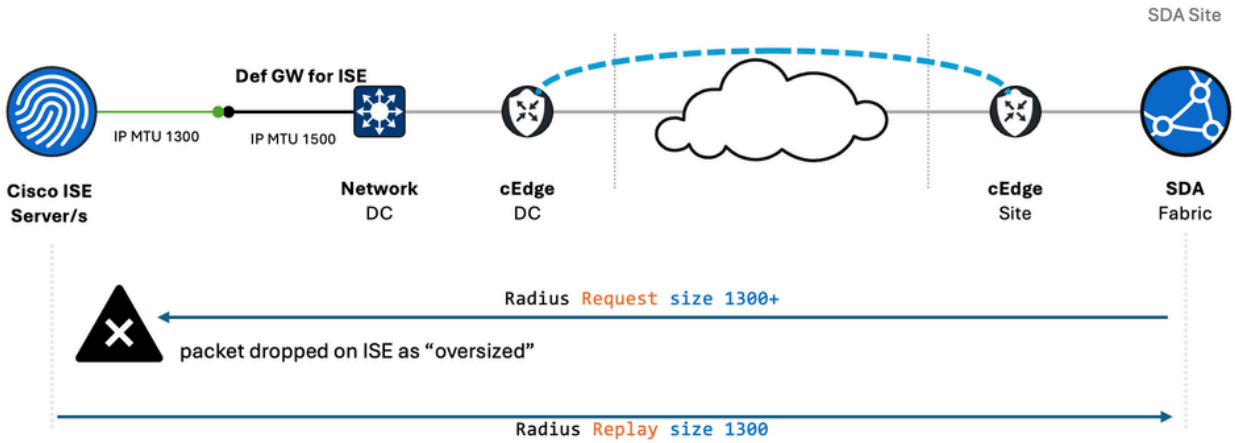
- Cisco IOS/Cisco IOS-XE®

```
ping

        size

         df-bit
```

- ISEの最初のルーティングポイント:ISEインターフェイスのIP MTU値を調整する場合は、データセンターの最初のルーティングポイント（特にISEサブネットに関連付けられたレイヤ3インターフェイス）にも同じIP MTU値が設定されていることを確認します。
  これは、MTUの不一致によってISEが着信パケットをオーバーサイズとして処理し、ドロップする「チャレンジ1」で説明したような状況を防止するのに役立ちます。
  たとえば、ISEインターフェイスのMTUが小さくなっているのに(たとえば 1300)、最初のルーティングポイントがデフォルトのMTU 1500で設定されたままの場合、ISEに送信される1300バイトより大きく1500バイトより小さいパケットはフラグメント化されず、ISEによって廃棄されます(チャレンジ1を参照)。
  また、最初のルーティングポイントで、必要に応じてフラグメンテーションを実行できること、およびフラグメンテーションを実行してもパフォーマンスが低下しないことを確認します。
- 両方向の送信パス全体にわたるMTUの更新:ISEでIP MTU設定を更新する場合、送信パス全体にわたるMTUを考慮することが重要です。ISEに設定されたMTU値がファーストホップゲ

ートウェイのレイヤ3インターフェイスのMTUと一致しない場合は、同様の問題が「チャレンジ#1」で説明されているように発生する可能性があります。

たとえば、デフォルトゲートウェイでデフォルトの1500バイトのMTUが設定されたままになっている状態で、ISEのMTUを1300バイトに縮小すると、1300 ~ 1500バイトの間のパケット（通常はネットワークデバイスによって生成される）がサイズ超過としてISEによって廃棄される場合があります。



この問題を回避するには、ISEでのMTUの変更がファーストホップゲートウェイで必ずミラーリングされ、同じレイヤ3セグメント内のすべてのエンドホストで反映されていることが理想的です。これにより、エンドツーエンドのMTUの一貫性が維持され、予期しないパケットのドロップが防止されます。

結論

Cisco ISEサーバのIP MTU設定を、SD-WANカプセル化によるトランスポートレイヤMTUの効果的な制限に合わせること、およびSDA Border to SD-WAN Cisco Edge Router handoffに合わせてMTUを調整することは、推奨に限らず、最新の企業セグメント化ネットワークでAAAサービスの安定性、信頼性、およびパフォーマンスを確保するための重要な前提条件です。パスMTUディスカバリは重要なメカニズムですが、ICMPフィルタリングやSD-WAN環境でのコントロールプレーンポリシング(COPP)などの要因によって、その実用的な効果が妨げられる場合があります。

ISEで削減されたIP MTU(たとえば1350 ~ 1400バイト)を予防的に設定することで、ネットワークアーキテクトおよびエンジニアはMTU関連のパケット廃棄のリスクを大幅に軽減し、予測可能で復元力のあるネットワーク運用を実現できます。これは、ISEが高度なマイクロセグメンテーションと動的なポリシー適用を調整するCisco SDAの導入で特に重要です。これらの調整は、サイズが大きくなる可能性のあるコントロールプレーンメッセージを正常に配信できることに依存することが多くなります。すべてのISEノードにわたる入念な計画、包括的なテスト、および一貫した設定は、問題なく導入を成功させるための鍵です。

標準と参考資料

詳細については、公式標準およびシスコのドキュメントを参照してください。

RFC:

- RFC 1191:パスMTUディスカバリ
- RFC 791:インターネットプロトコル(IP):Do Not Fragment(DF)ビットを含むIPヘッダーを定義します。
- RFC 8200:IPv6仕様（IPv6が使用される場合に関連、同様のPMTUD概念を含む）
- RFC 4459:In-the-Network Tunneling(VPNs)に関するMTUおよびフラグメンテーションの問題 – VPN環境における一般的なMTUの問題に直接対処します。

シスコのドキュメント：

- Cisco SDAの設計および導入ガイド：ファブリックMTUの推奨事項とボーダーノードの設定に関する情報
- Cisco SD-WAN設計および設定ガイド：SD-WANファブリック内のカプセル化オーバーヘッド、トンネルインターフェイスMTU、およびPMTUDに関する考慮事項の詳細。
- 『Cisco Catalyst 9000シリーズスイッチ設定ガイド』:MTU設定およびフラグメンテーション機能に関するプラットフォーム固有の詳細について
- Cisco Identity Services Engine(ISE)管理者ガイドおよびCLIガイド：インターフェイス設定の詳細(ip mtuコマンドなど)およびサービス再起動の影響

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。