Configuration de la MTU IP ISE optimale dans SD-WAN pour les déploiements SDA

Table des matières

Introduction

Ce document décrit comment les problèmes de Maximum Transmission Unit (MTU) peuvent avoir un impact sur la microsegmentation dans SDA lorsque SD-WAN est utilisé pour connecter des sites SDA.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès défini par logiciel (SDA) Cisco
- Réseaux étendus définis par logiciel Cisco (SD-WAN)
- Cisco Identity Services Engine (ISE)

Composants utilisés:

Les informations contenues dans ce document sont basées sur SDA, SDWAN et ISE.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les réseaux d'entreprise modernes exploitent de plus en plus le SDA pour une microsegmentation granulaire et une application cohérente des politiques. Pour connecter des sites SDA distribués, Cisco SD-WAN est souvent utilisé, offrant un transport agile, sécurisé et optimisé sur divers réseaux sous-jacents. Au coeur de cette architecture, l'ISE fournit des services AAA (Authentication, Authorization, and Accounting) critiques, ainsi qu'une distribution dynamique des stratégies (par exemple, des balises de groupe de sécurité et des listes de contrôle d'accès téléchargeables).

Bien que robuste, l'intégration de ces puissantes technologies peut présenter des défis de configuration subtils mais percutants. La gestion de la MTU au niveau des points de transfert réseau critiques et à travers la superposition SD-WAN est une zone privilégiée pour de tels problèmes. Cet article traite de deux scénarios courants de non-concordance des MTU qui peuvent perturber le fonctionnement du réseau :

1. Écart MTU entre les noeuds périphériques SDA et les périphériques périphériques SD-WAN.
2. Contraintes MTU pour le trafic provenant d'ISE traversant la superposition SD-WAN.

Un alignement correct de la MTU est primordial pour éviter les problèmes de fragmentation de paquets ou les abandons silencieux, afin de garantir une authentification fiable, l'application des politiques et la stabilité globale du réseau. Si ces problèmes ne sont pas résolus, la connectivité intermittente et l'application des politiques risquent d'être perturbantes et de nécessiter d'importants efforts de dépannage.

Symptômes courants de MTU mal aligné

Un MTU mal aligné peut se manifester de différentes manières, ce qui entraîne souvent des problèmes difficiles à diagnostiquer :

- Échecs ou dépassements de délai d'authentification RADIUS intermittents : Particulièrement remarquable pour les politiques générant des paquets RADIUS plus importants (par exemple, ceux avec des paires AV ou des certificats étendus).
- Terminaux ne recevant pas ou n'appliquant pas de listes de contrôle d'accès téléchargeables (dACL) ou de stratégies TrustSec (SGT/SGACL) : Ces politiques sont souvent véhiculées dans de grands paquets RADIUS.
- Établissement lent de la session pour les clients authentifiés : En raison des retransmissions au niveau de la couche application.
- Retransmissions RADIUS excessives : Observable dans les journaux ISE ou sur les périphériques d'accès au réseau (NAD).
- Propagation incohérente des politiques : Les modifications apportées à la stratégie ISE

peuvent ne pas être propagées de manière cohérente à tous les NAD des sites SDA distants.

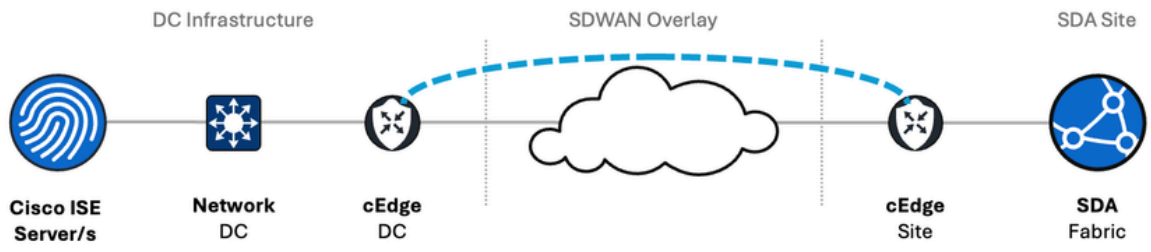
- Différences de capture de paquets : Les captures peuvent montrer que l'ISE envoie des paquets volumineux (par exemple, >1450 octets) avec le bit DF (Do Not Fragment) défini, mais aucune réponse correspondante ou erreur ICMP « Fragmentation Needed » (Fragmentation requise) du routeur de périphérie Cisco NAD ou SD-WAN.
- Incrémentation des compteurs de suppression de paquets : Observé sur l'interface d'entrée du routeur de périphérie Cisco Data Center (DC) pour le trafic provenant d'ISE destiné aux sites SDA, ou sur l'interface du routeur de périphérie Cisco SD-WAN faisant face à la frontière SDA pour le trafic dans le sens inverse.

Description du problème

Un déploiement d'entreprise typique
Considérez une topologie d'entreprise commune :

- Serveurs Cisco ISE : Déployé dans un data center centralisé ou dans des concentrateurs régionaux, connecté à l'infrastructure réseau du data center.
- Infrastructure DC : Comprend les commutateurs de coeur ou d'agrégation DC auxquels les serveurs ISE se connectent.
- Superposition SD-WAN : Les routeurs de périphérie Cisco DC établissent des tunnels SD-WAN (généralement IPsec) sur un réseau de transport sous-jacent (par exemple, Internet, MPLS) vers les routeurs de périphérie Cisco sur des sites SDA distants.
- Site SDA : Les routeurs Cisco Edge Router du site distant se connectent au fabric SDA local, qui inclut les noeuds de périphérie du fabric, les noeuds de périphérie, les contrôleurs LAN sans fil (WLC) et, finalement, les points d'extrémité.

Topologie illustrative



Défi 1 : Écart MTU - Frontières SDA aux périphéries SD-WAN

Les principes de conception de Cisco SDA, souvent mis en oeuvre via l'automatisation LAN, promeuvent une MTU de 9 100 octets (trames jumbo) sur tous les périphériques de fabric. Cela inclut les noeuds de périphérie de la gamme Catalyst 9000 et garantit que les trames jumbo Ethernet sont transportées efficacement au sein du fabric. Par conséquent, l'interface de transfert de couche 3 ou SVI sur un noeud de frontière SDA utilise par défaut cette MTU plus grande.

À l'inverse, les périphériques de périphérie SD-WAN, tels que la gamme Catalyst 8000, utilisent généralement par défaut une MTU d'interface de 1 500 octets. Il s'agit d'une norme pour les interfaces se connectant à des réseaux externes tels que les fournisseurs d'accès Internet (FAI), où la prise en charge des trames jumbo est rare ou non activée.

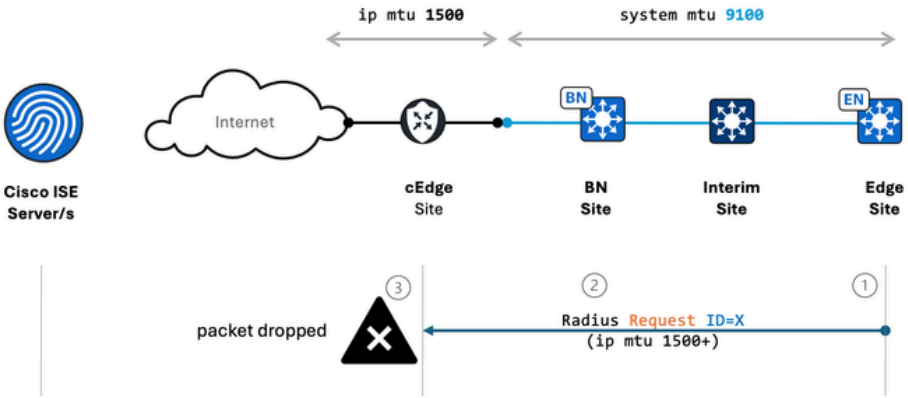
Cette disparité crée un point de défaillance potentiel immédiat : une frontière SDA qui tente d'envoyer un paquet IP de plus de 1500 octets à une périphérie SD-WAN dont l'interface de réception est configurée pour un MTU de 1500 octets.

Ce type de non-concordance de MTU est un piège courant dans les déploiements SDA et est souvent facile à ignorer lors de la configuration. Ce qui complique les choses, c'est que certains comportements liés à la manière dont les requêtes RADIUS sont générées sur les commutateurs Catalyst 9000 exécutant Cisco IOS-XE® peuvent faire apparaître ces problèmes uniquement dans des conditions spécifiques et critiques.

Par exemple, les requêtes RADIUS générées pendant le processus d'authentification de l'utilisateur final géré par le processus de démon du gestionnaire de session (SMD) sont codées en dur pour fragmenter les paquets à 1396 octets. En revanche, les requêtes RADIUS impliquées dans la récupération des stratégies TrustSec, telles que les listes de contrôle d'accès du groupe de sécurité (SGACL), sont générées par les sous-composants du démon IOSd (Internetworking Operating System daemon) de Cisco. Ils sont sensibles à la MTU et peuvent éviter de fragmenter les paquets à moins que leur taille ne dépasse la MTU système (généralement jusqu'à 9 100 octets).

Par conséquent, les problèmes liés aux incohérences de MTU ne deviennent apparents que lorsque les politiques de téléchargement de Cisco TrustSec (CTS) sont utilisées. En outre, l'ensemble de listes de contrôle d'accès basées sur les rôles (RBACL) téléchargées par un périphérique de périphérie SDA pendant l'authentification de l'utilisateur peut varier en fonction des stratégies SGACL déjà présentes pour d'autres balises. En pratique, le commutateur télécharge uniquement les parties non chevauchantes des ensembles de politiques.

Ensemble, ces comportements peuvent produire des résultats imprévisibles et incohérents, allant de défaillances silencieuses à des téléchargements incomplets de politiques, en fonction de la taille de la politique SGACL, des conditions système actuelles et, en fin de compte, des désalignements de MTU le long du chemin.



La frontière SDA transfère un paquet RADIUS volumineux (par exemple, 1600 octets) vers l'ISE via la périphérie SD-WAN, c'est ce qui se produit :

1. La frontière SDA, avec son interface MTU 9100, envoie le paquet IP de 1 600 octets.
2. Le routeur de périphérie Cisco SD-WAN reçoit ce paquet sur son interface MTU 1500.
3. Cependant, si le bit Do Not Fragment (DF) n'est pas défini sur ces paquets RADIUS, le routeur de périphérie Cisco SD-WAN peut souvent les abandonner en entrée simplement parce qu'ils sont « surdimensionnés » par rapport à sa MTU d'interface configurée. Il n'arrive pas au stade de la logique de transfert IP où il peut envisager de les fragmenter (si le bit DF le permet).

Cette baisse silencieuse entraîne d'importants problèmes de dépannage, d'autant plus que le problème est directionnel (SDA vers SD-WAN/ISE).

Une disparité de MTU similaire peut se produire au niveau des commutateurs principaux ou terminaux du data center (DC), généralement configurés pour prendre en charge les trames jumbo (par exemple, MTU 9000+) afin d'améliorer l'efficacité du trafic DC interne. Cependant, si le trafic est transféré vers l'interface orientée LAN d'un routeur de périphérie Cisco SD-WAN DC configuré avec une MTU standard (par exemple, 1500 octets), cette non-correspondance peut entraîner une fragmentation ou des pertes de paquets, en particulier pour le trafic circulant du réseau DC dans le fabric SD-WAN.

Solution au défi 1 :

Alignez le MTU IP sur l'interface de transfert de la frontière SDA (physique ou SVI) avec l'interface de routeur périphérique Cisco SD-WAN d'appairage, généralement 1 500 octets.

Exemple de configuration (sur le noeud périphérique SDA) :

<#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
!
```

Considération importante : Fragmentation sur les limites du Catalyst 9000

Les commutateurs de la gamme Catalyst 9000, en tant que noeuds périphériques SDA, prennent en charge la fragmentation IP pour les paquets IP natifs dans le plan de données matériel. La réduction de la mtu ip sur l'interface de transfert à 1500 ne provoque pas de dégradation des performances due à la fragmentation logicielle pour le trafic provenant de ou transitant par la frontière qui en a besoin. Le commutateur fragmente efficacement les paquets IP de plus de 1500 octets (si le bit DF est libre) avant de quitter cette interface spécifique, sans envoyer de paquet au processeur.

Cependant, il est important de noter que les commutateurs Catalyst 9000 ne prennent généralement pas en charge la fragmentation du trafic encapsulé VXLAN. Cette limitation est cruciale pour le trafic de superposition, mais n'a pas d'impact sur le scénario d'authentification RADIUS décrit, car la communication RADIUS entre la frontière SDA et un ISE externe se produit généralement au sein du sous-réseau (routage IP natif). (Les considérations relatives à la MTU pour les superpositions VXLAN sont un sujet distinct et complexe, détaillé dans les guides de conception Cisco SDA pertinents).

L'alignement proactif de la MTU à la frontière SDA vers le transfert du routeur de périphérie Cisco SD-WAN est essentiel.

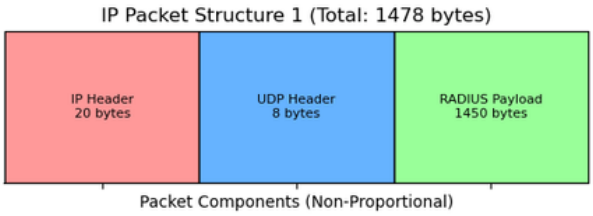
Défi 2 : La compression MTU - Trafic ISE sur la superposition SD-WAN

Même si des interfaces physiques individuelles, telles que des cartes réseau ISE, des ports de commutateur ou des interfaces de routeur sont configurés sur une MTU IP standard de 1 500 octets, la superposition SD-WAN elle-même introduit une surcharge d’encapsulation. Cette surcharge consomme une partie de la limite de 1 500 octets, réduisant ainsi le MTU effectif disponible pour le paquet IP d'origine (la « charge utile » du point de vue d'ISE).

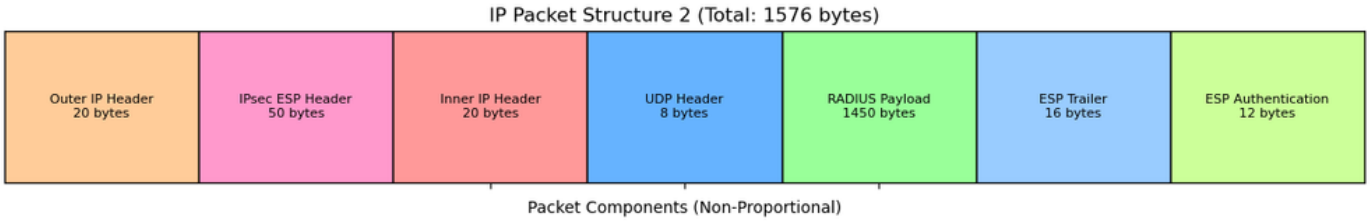
Structure des paquets et surcharge d’encapsulation :

Lorsqu'un paquet IP provenant d'un serveur ISE (par exemple, un paquet d'acceptation d'accès RADIUS) est envoyé à un périphérique d'accès réseau (NAD) dans un site SDA, il traverse la superposition SD-WAN et est encapsulé. Une pile d'encapsulation commune implique IPsec en mode tunnel, potentiellement sur UDP pour NAT traversal (NAT-T).

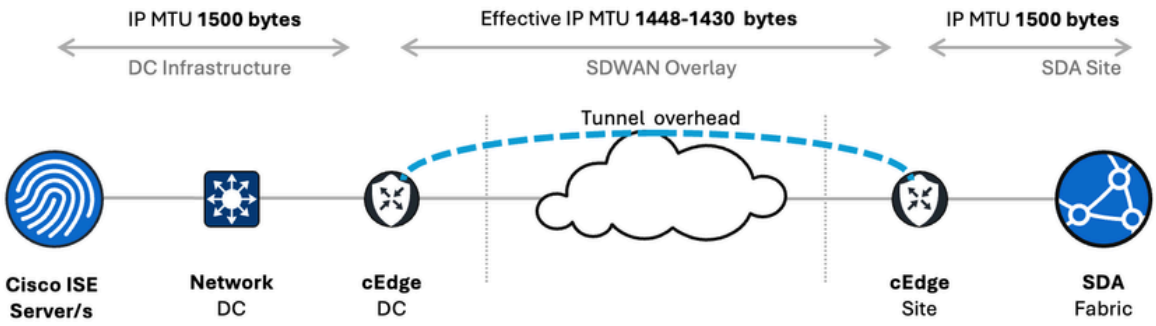
- Paquet d'origine d'ISE (paquet interne) :
  Par exemple, un paquet RADIUS avec une charge utile de 1 450 octets + 8 milliards d'UDP + 20 milliards d'IP interne = 1 478 octets.



- Considérez IPsec ESP en mode tunnel, potentiellement avec l'encapsulation UDP pour NAT-T :



- La surcharge totale peut varier en fonction des chiffrements IPsec spécifiques, des mécanismes d'authentification et d'autres fonctionnalités de superposition (comme GRE si utilisé). Un calcul typique :
  - En-tête IP externe (IPv4) : 20 octets
  - En-tête UDP (si ESP sur UDP pour NAT-T) : 8 octets
  - En-tête ESP : ~8 octets
  - ESP IV (par exemple, pour AES-CBC) : ~16 octets (le cas échéant)
  - Authentification ESP (par exemple, HMAC-SHA256 tronqué) : ~12-16 octets
  - Surcharge IPsec estimée commune : ~52-70 octets (peut être supérieur, jusqu'à ~80 octets ou plus avec toutes les options).



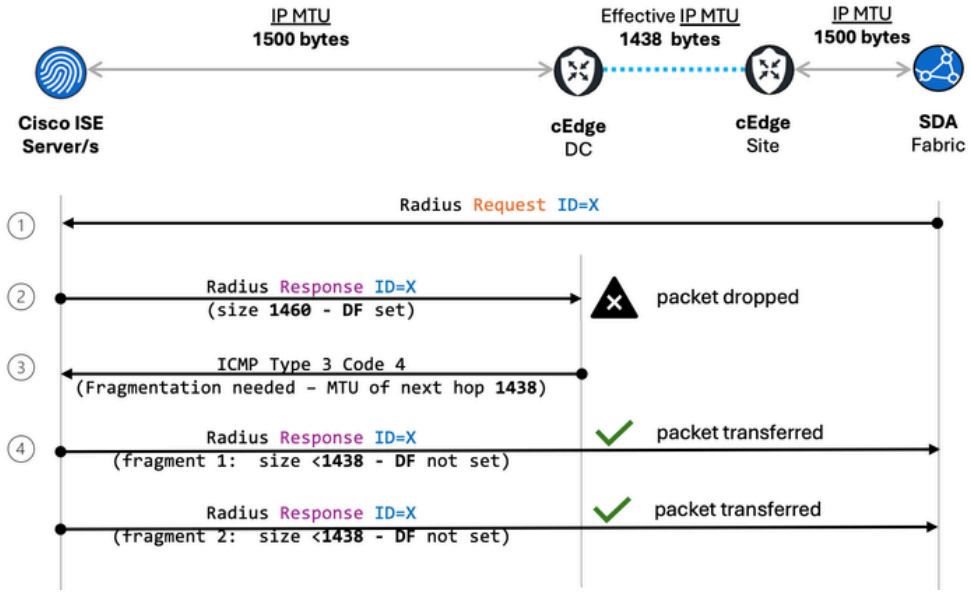
Si la MTU de la liaison physique est de 1 500 octets, la MTU de charge utile disponible pour le paquet IP d'origine provenant d'ISE devient : 1 500 octets - Surcharge SD-WAN.
Par exemple, 1 500 - 70 = 1 430 octets.

Comportement lorsque les paquets dépassent la MTU effective :

1. ISE génère un paquet (anomalie du bit DF) :
    - Par défaut, le système d'exploitation Linux sous-jacent d'une appliance ISE définit le bit DF (Do Not Fragment) dans l'en-tête IP pour tous les paquets qu'il émet qui sont inférieurs ou égaux à sa MTU IP d'interface configurée (par exemple, 1500 octets).
    - Objectif de ce bit DF : ISE (via son système d'exploitation) définit de manière proactive le bit DF principalement pour tirer parti du processus de détection de MTU de chemin (PMTUD), qui est décrit plus loin. Cela permet à ISE d'apprendre dynamiquement la PMTU réelle vers une destination si elle est plus petite que sa propre MTU d'interface.
    - Comportement pour les paquets supérieurs à la MTU de l'interface : Si ISE doit envoyer un paquet IP qui est supérieur à sa MTU IP de l'interface configurée, le comportement dépend de son système d'exploitation Linux. En général, le système d'exploitation peut fragmenter le paquet avant la transmission et effacer le bit DF (paramétrage DF=0) sur ces fragments résultants. Cette fragmentation est une fonction au niveau du système d'exploitation, qui n'est pas directement pilotée par le code d'application ISE lui-même.
    - Principale distinction par rapport aux périphériques réseau : ce comportement par défaut d'ISE (paramétrage de DF=1 même pour les paquets non fragmentés s'adaptant à sa MTU d'interface) est sensiblement différent de celui de nombreux périphériques réseau traditionnels (routeurs, commutateurs). Les périphériques réseau ne définissent souvent pas le bit DF sur les paquets qu'ils émettent ou transfèrent, sauf s'ils sont explicitement configurés pour le faire, ou si le bit DF est déjà défini sur le paquet en cours de transmission, ou pour des protocoles spécifiques qui le commandent. Ils autorisent généralement la fragmentation par défaut si un paquet dépasse la MTU du tronçon suivant (et DF=0).
    - Complexité du dépannage : cette asymétrie, où le trafic ISE-à-NAD a souvent DF=1 par défaut, tandis que le trafic NAD-à-ISE peut avoir DF=0 (sauf si le NAD le définit pour une raison), peut introduire une couche supplémentaire de complexité lors du dépannage. Les ingénieurs peuvent observer différents comportements de fragmentation et interactions PMTUD en fonction de la direction du flux de trafic.
2. Le paquet atteint le routeur de périphérie Cisco (DC) entrant : le routeur de périphérie Cisco DC reçoit le paquet IP d'ISE.
3. Encapsulation and MTU Check by Cisco Edge Router : le routeur Cisco Edge tente d'encapsuler le paquet pour le tunnel SD-WAN.
    - Si la taille du paquet d'origine plus la surcharge d'encapsulation SD-WAN dépassent la MTU de l'interface physique sortante du routeur de périphérie Cisco (par exemple, 1 500 octets), ET que le bit DF est défini sur le paquet d'origine (interne) provenant d'ISE, le routeur de périphérie Cisco ne doit pas fragmenter le paquet interne.
    - Le routeur de périphérie Cisco doit abandonner le paquet.
    - Le routeur de périphérie Cisco doit également envoyer un message ICMP « Destination Unreachable - Fragmentation Needed and DF bit set » (Destination inaccessible - Fragmentation requise et bit DF défini) (Type 3, Code 4) à la source (ISE), indiquant le MTU du tronçon suivant (le MTU effectif du tunnel).
4. Processus de détection de MTU de chemin (PMTUD) : À la réception de ce message ICMP « Fragmentation Needed » (Fragmentation requise), ISE (le système d'exploitation source)

doit réduire son estimation de PMTU pour ce chemin de destination spécifique. Il mettrait ces informations en cache et renverrait les données dans des paquets plus petits qui s'intègrent dans la PMTU nouvellement découverte.

Schéma du processus PMTUD :



Où la communication PMTUD se décompose :
La PMTUD est robuste en théorie, mais peut échouer en pratique :

- Filtrage ICMP : Les pare-feu intermédiaires ou les stratégies de sécurité bloquent souvent les messages ICMP, empêchant ainsi le message « Fragmentation requise » d'atteindre ISE.

- Contrôle du plan de contrôle (CoPP) sur le routeur de périphérie Cisco : Les routeurs Cisco Edge Router utilisent CoPP pour protéger leur processeur. La génération de messages d'erreur ICMP est une tâche du plan de contrôle. Sous une charge importante ou avec de nombreux paquets surdimensionnés, CoPP peut limiter le débit ou abandonner la génération ICMP. ISE ne reçoit jamais les commentaires.

- Abandons silencieux : Si ISE ne reçoit pas le message ICMP « Fragmentation Needed » (Fragmentation requise), il ne connaît pas la restriction de chemin. Il continue d'envoyer de gros paquets avec le bit DF défini, ce qui entraîne leur suppression silencieuse par le routeur de périphérie Cisco d'entrée. Il en résulte des délais d'attente et des retransmissions de la couche application (par exemple RADIUS).

- Impact sur les services ISE : Les grands paquets d'acceptation d'accès RADIUS (transportant des dACL, des AVP étendus, des informations SGT) sont particulièrement sensibles. Les manifestations comprennent :

    - Échecs d'authentification intermittents ou complets.

    - Les terminaux ne reçoivent pas les politiques d'accès réseau ou les SGT correctes.

- Synchronisation de stratégie incomplète ou ayant échoué entre ISE et NAD.

Solution au défi 2 : Configuration proactive de MTU IP ISE

Étant donné le manque de fiabilité de PMTUD, une approche proactive est préférable pour les services critiques comme ISE. Configurez la MTU IP sur les interfaces réseau d'ISE à une valeur qui s'adapte en toute sécurité à la surcharge de superposition SD-WAN maximale attendue. Cela garantit qu'ISE n'émet pas de paquets IP (avec le bit DF défini) qui sont intrinsèquement trop volumineux pour traverser la superposition SD-WAN sans avoir besoin d'une fragmentation par un périphérique intermédiaire (ce qui est interdit si DF=1).

Calcul et configuration de la MTU IP ISE recommandée :

1. Établissement de la MTU physique de base : il s'agit généralement de 1 500 octets pour les interfaces Ethernet standard le long du chemin.
2. Déterminer la surcharge maximale d'encapsulation SD-WAN :
   - Calculez avec précision ou estimez avec prudence la surcharge totale introduite par votre superposition SD-WAN spécifique (IPsec, GRE, VXLAN, MPLSoGRE, etc.). Consultez la documentation du fournisseur pour obtenir des chiffres précis sur les protocoles et les options que vous avez choisis.

Composante	Exemple de surcharge (octets)	Remarques
MTU physique de base	1500	Ethernet standard sur les liaisons physiques
Moins : Surcharge SD-WAN		
En-tête IP externe (IPv4)	20	
En-tête UDP (pour NAT-T)	8	Si ESP est encapsulé dans UDP
En-tête ESP	~8-12	
ESP IV (par exemple, AES-CBC)	~16	Varie selon l'algorithme de chiffrement
Authentification ESP (par exemple, SHA256)	~12-16	Varie selon l'algorithme d'authentification (par exemple, 96 bits pour certains)
Autres superpositions (GRE, etc.)	Variable	Ajoutez si cela fait partie de votre pile d'encapsulation SD-WAN
Frais généraux totaux estimés	~68 à plus de 80 octets	Somme de tous les composants pertinents pour votre déploiement
MTU du chemin effectif	~1 432 - 1 420 octets	MTU physique de base - Total des frais généraux estimés

3. Configuration MTU IP ISE recommandée :
   - Prenez le MTU du chemin effectif calculé (par exemple, 1420 octets de l'exemple).
   - Soustrayez une marge de sécurité supplémentaire (par exemple, 20 à 70 octets) pour tenir compte des en-têtes L2 mineurs non pris en compte ou pour fournir une mémoire tampon.
   - Les solutions telles que Cisco SD-WAN peuvent effectuer une détection de MTU de chemin (PMTU) individuellement pour chaque tunnel de site à site. Ce mécanisme

s'exécute automatiquement toutes les 20 minutes pour tester et ajuster dynamiquement la MTU IP du tunnel en fonction des conditions de transport actuelles sur chaque site. Par conséquent, les valeurs MTU peuvent différer d'un site à l'autre et changer au fil du temps.
- Un MTU IP généralement sûr et recommandé pour les interfaces ISE dans de tels scénarios est compris entre 1 350 et 1 400 octets

Un MTU IP de 1 350 octets est souvent un point de départ très robuste

Configuration ISE (exemple via CLI) :

Cette commande est exécutée sur l'interface de ligne de commande de l'appliance Cisco ISE pour chaque interface réseau concernée.

<#root>

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


 ip mtu 1350

!
```

Considérations opérationnelles importantes concernant les modifications de la MTU IP ISE :

- Redémarrage du service requis : une fois la commande ip mtu appliquée à une interface ISE, l'utilisateur est invité à redémarrer les services d'application ISE. Il s'agit d'une modification ayant un impact sur le service et qui doit être planifiée pendant une fenêtre de maintenance planifiée. Consultez la documentation officielle de Cisco ISE pour plus de détails sur la procédure.
- Appliquer à tous les noeuds ISE : Cet ajustement de la MTU IP doit être appliqué de manière cohérente à tous les noeuds ISE du déploiement (PAN principal, PAN secondaire, noeuds de service de stratégie (PSN)) qui communiquent avec les NAD sur le SD-WAN. Des paramètres MTU incohérents entraînent un comportement imprévisible.
- Test approfondi : Avant de procéder à l'implémentation en production, testez rigoureusement cette modification dans un laboratoire ou lors d'un déploiement pilote. Utilisez des outils tels que ping avec des tailles de paquets variables et le bit DF défini pour valider la gestion de MTU de bout en bout :
    - Systèmes Linux :

```
ping
```

```
-s

 -M do
```

(Remarque: -s spécifie la taille de la charge utile ICMP. Taille totale des paquets IP = charge utile + 8 Go d'Hdr ICMP + 20 Go d'Hdr IP pour IPv4)

- Fenêtres:

```
ping

-f -l
```

(Remarque: -l indique la taille de la charge utile ICMP.)

- Cisco IOS/Cisco IOS-XE®

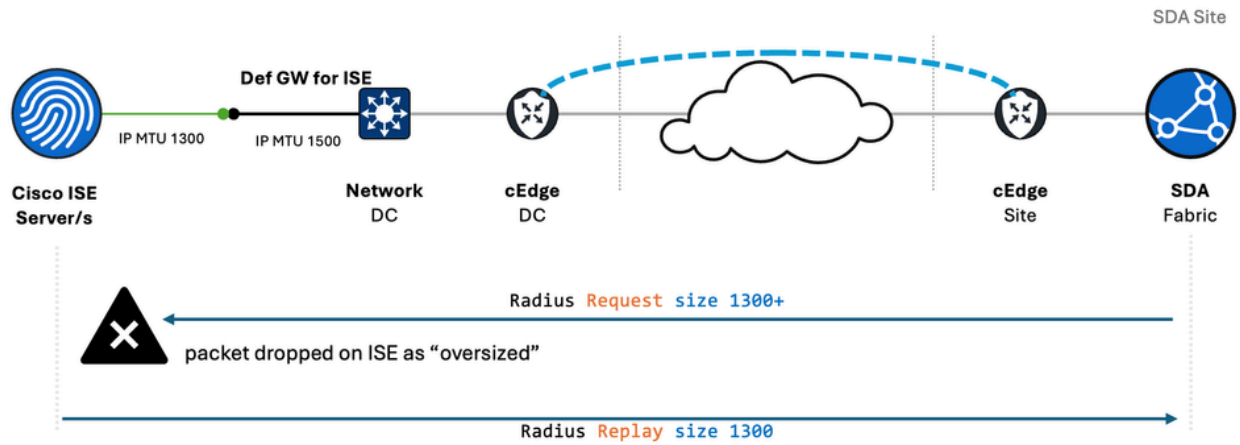
```
ping

size

 df-bit
```

- Premier point de routage ISE : lors de l'ajustement de la valeur de MTU IP sur l'interface ISE, assurez-vous que le premier point de routage du centre de données, en particulier l'interface de couche 3 associée au sous-réseau ISE, est également configuré avec la même valeur de MTU IP.
  Cela permet d'éviter des situations comme celle décrite dans le défi 1, où une non-

correspondance de MTU amène ISE à traiter les paquets entrants comme étant surdimensionnés et à les abandonner.
Par exemple, si l'interface ISE a une MTU réduite (par exemple, 1300), mais que le premier point de routage reste configuré avec la MTU par défaut de 1500, les paquets envoyés à ISE qui sont supérieurs à 1300 octets mais inférieurs à 1500 octets ne sont pas fragmentés et sont rejetés par ISE, comme observé dans le défi 1.
En outre, assurez-vous que le premier point de routage est capable d'effectuer la fragmentation si nécessaire, et que cela n'entraîne pas de dégradation des performances.

- Mise à jour du MTU sur l'ensemble du chemin de transmission et dans les deux sens - Lors de la mise à jour des paramètres IP MTU sur ISE, il est important de prendre en compte le MTU sur l'ensemble du chemin de transmission et dans les deux sens. Si la valeur de MTU configurée sur ISE n'est pas alignée sur la MTU sur l'interface de couche 3 de la passerelle de premier saut, des problèmes similaires peuvent survenir, comme décrit dans le défi #1.

  Par exemple, si la MTU d'ISE est réduite à 1 300 octets alors que la MTU de 1 500 octets par défaut reste configurée sur la passerelle par défaut, les paquets dont la taille est comprise entre 1 300 et 1 500 octets, généralement générés par les périphériques réseau, peuvent être abandonnés par ISE comme étant surdimensionnés.



  Pour éviter ce problème, assurez-vous toujours que les modifications de MTU sur ISE sont mises en miroir sur la passerelle de premier saut et, idéalement, reflétées sur tous les hôtes finaux au sein du même segment de couche 3. Cela permet de maintenir la cohérence MTU de bout en bout et d’éviter les pertes de paquets inattendues.

Conclusion

L'alignement des paramètres MTU IP sur les serveurs Cisco ISE avec les limites MTU de couche transport effectives imposées par l'encapsulation SD-WAN et l'alignement MTU à la frontière SDA sur le transfert du routeur de périphérie Cisco SD-WAN n'est pas seulement une recommandation, mais une condition préalable essentielle pour assurer la stabilité, la fiabilité et les performances des services AAA dans les réseaux d'entreprise segmentés modernes. Bien que la découverte de MTU de chemin soit un mécanisme important, son efficacité pratique peut être entravée par des facteurs tels que le filtrage ICMP ou la réglementation du plan de contrôle dans les

environnements SD-WAN.

En configurant de manière proactive une MTU IP réduite sur ISE (par exemple, 1 350-1 400 octets), les architectes et ingénieurs réseau peuvent réduire considérablement le risque de pertes de paquets liées à la MTU, ce qui permet des opérations réseau plus prévisibles et plus résilientes. Cela est particulièrement important dans les déploiements Cisco SDA où ISE orchestre une micro-segmentation sophistiquée et l'application dynamique des politiques, qui reposent souvent sur la livraison réussie de messages de plan de contrôle potentiellement volumineux. Une planification diligente, des tests complets et une configuration cohérente sur tous les noeuds ISE sont essentiels à un déploiement réussi et sans problème.

Normes et références

Pour en savoir plus, consultez les normes officielles et la documentation Cisco :

RFC :

- RFC 1191 : Découverte MTU du chemin
- RFC 791 : IP (Internet Protocol) : définit l'en-tête IP, y compris le bit DF (Do Not Fragment).
- RFC 8200 : Spécification IPv6 (pertinente si IPv6 est utilisé, inclut des concepts PMTUD similaires).
- RFC 4459 : Problèmes de MTU et de fragmentation avec les VPN (In-the-Network Tunneling) : résout directement les problèmes de MTU courants dans les environnements VPN.

Documentation Cisco :

- Guides de conception et de déploiement Cisco SDA : Pour plus d'informations sur les recommandations MTU du fabric et les configurations des noeuds périphériques.
- Guides de conception et de configuration de Cisco SD-WAN : Pour plus d'informations sur la surcharge d'encapsulation, le MTU d'interface de tunnel et les considérations PMTUD dans le fabric SD-WAN.
- Guides de configuration des commutateurs Cisco Catalyst 9000 : Pour obtenir des détails spécifiques à la plate-forme sur les paramètres MTU et les fonctionnalités de fragmentation.
- Guides d'administration et de CLI de Cisco Identity Services Engine (ISE) : Pour plus d'informations sur la configuration de l'interface, y compris la commande ip mtu et les implications du redémarrage du service.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.