Konfigurieren der optimalen ISE-IP-MTU im SD-WAN für SDA-Bereitstellungen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie sich Probleme mit der Maximum Transmission Unit (MTU) auf die Mikrosegmentierung in SDA auswirken können, wenn SDA-Standorte über das SD-WAN verbunden werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Software Defined Access (SDA)
- Cisco Software-defined Wide Area Networks (SD-WAN)
- Cisco Identity Services Engine (ISE)

Komponenten benutzt:

Die Informationen in diesem Dokument basieren auf SDA, SDWAN und ISE.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Moderne Unternehmensnetzwerke nutzen zunehmend SDA für eine präzise Mikrosegmentierung und konsistente Durchsetzung von Richtlinien. Zur Verbindung verteilter SDA-Standorte wird häufig Cisco SD-WAN eingesetzt, das einen flexiblen, sicheren und optimierten Transport über verschiedene Underlay-Netzwerke ermöglicht. Zentral für diese Architektur ist die ISE mit wichtigen AAA-Services (Authentication, Authorization und Accounting) sowie einer dynamischen Richtlinienverteilung (z. B. Security Group Tags (SGTs) und herunterladbaren ACLs).

Die Integration dieser leistungsstarken Technologien ist zwar robust, kann jedoch subtile, aber dennoch wirkungsvolle Konfigurationsherausforderungen mit sich bringen. Die MTU-Verarbeitung an wichtigen Netzwerk-Übergabepunkten und über das SD-WAN-Overlay ist ein besonders wichtiger Bereich für solche Probleme. In diesem Artikel werden zwei häufige MTU-Diskrepanzen behandelt, die den Netzwerkbetrieb stören können:

1. Die MTU-Lücke zwischen SDA-Grenzknoten und SD-WAN-Edge-Geräten.
2. MTU-Beschränkungen für Datenverkehr vom ISE, der das SD-WAN-Overlay durchläuft

Eine korrekte MTU-Ausrichtung ist von entscheidender Bedeutung, um Paketfragmentierungsprobleme oder automatische Verwerfungen zu verhindern und so eine zuverlässige Authentifizierung, Richtliniendurchsetzung und allgemeine Netzwerkstabilität sicherzustellen. Werden diese Probleme nicht behoben, kann die zeitweilige Verbindungsherstellung und die Richtliniendurchsetzung verwirrend wirken und erhebliche Anstrengungen zur Fehlerbehebung nach sich ziehen.

Häufige Symptome einer falsch ausgerichteten MTU

Eine falsch ausgerichtete MTU kann sich auf verschiedene Weise manifestieren, was häufig zu schwer zu diagnostizierenden Problemen führt:

- Intermittierende Fehler oder Zeitüberschreitungen bei der RADIUS-Authentifizierung: Besonders auffällig bei Richtlinien, die größere RADIUS-Pakete generieren (z. B. solche mit umfangreichen AV-Paaren oder Zertifikaten).
- Endpunkte, die herunterladbare ACLs (dACLs) oder TrustSec-Richtlinien (SGTs/SGACLs) nicht empfangen oder anwenden: Diese Richtlinien werden häufig in großen RADIUS-Paketen übermittelt.
- Langsamer Sitzungsaufbau für authentifizierte Clients: Aufgrund von Neuübertragungen auf Anwendungsebene.
- Übermäßige RADIUS-Neuübertragungen: Beobachtbar in ISE-Protokollen oder auf den Network Access Devices (NADs).

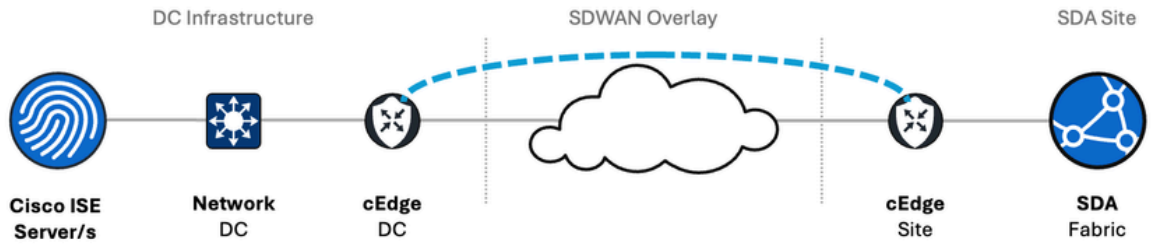
- Inkonsistente Verbreitung von Richtlinien: Richtlinienänderungen, die in der ISE vorgenommen werden, werden möglicherweise nicht konsistent auf alle NADs an Remote-SDA-Standorten propagiert.
- Unterschiede bei der Paketerfassung: Erfassungen können ISE beim Senden großer Pakete (z. B. > 1450 Byte) mit festgelegtem DF-Bit (Do Not Fragment) anzeigen, jedoch keine entsprechende Antwort oder ICMP-Fehler "Fragmentation Needed" (Fragmentierung erforderlich) vom Cisco NAD- oder SD-WAN-Edge-Router.
- Inkrementieren der Zähler für Paketverluste: Wird an der Eingangsschnittstelle des Cisco Edge-Routers des Rechenzentrums (DC) für Datenverkehr von der ISE beobachtet, der für SDA-Standorte bestimmt ist, oder an der Cisco Edge-Router-Schnittstelle für SD-WAN, die zur SDA-Grenze zeigt, für Datenverkehr in der umgekehrten Richtung.

Problembeschreibung

Eine typische Unternehmensbereitstellung
Betrachten wir eine gängige Unternehmenstopologie:

- Cisco ISE-Server: Bereitstellung in einem zentralisierten Rechenzentrum oder regionalen Hubs, die mit der Netzwerkinfrastruktur des Rechenzentrums verbunden sind
- Rechenzentrumsinfrastruktur: Umfasst Core- oder Aggregations-Switches im Rechenzentrum, mit denen ISE-Server verbunden sind.
- SD-WAN-Overlay: Cisco Edge Router in Rechenzentren richten SD-WAN-Tunnel (i. d. R. IPsec) über ein unterlagertes Transportnetzwerk (z. B. Internet, MPLS) zu Cisco Edge Router-Routern an Remote-SDA-Standorten ein.
- SDA-Website: Cisco Edge Router am Remote-Standort sind mit der lokalen SDA-Fabric verbunden, die Fabric-Edge-Knoten, Grenzknoten, Wireless LAN-Controller (WLCs) und schließlich die Endpunkte umfasst.

Darstellende Topologie



Herausforderung 1: MTU-Lücke - SDA-Grenzen an SD-WAN-Kanten

Die oftmals über LAN-Automatisierung implementierten Cisco SDA-Designprinzipien fördern auf allen Fabric-Geräten eine campusweite MTU von 9.100 Byte (Jumbo Frames). Dies umfasst die Grenzknoten der Catalyst Serie 9000 und stellt sicher, dass Ethernet-Jumbo Frames effizient innerhalb der Fabric transportiert werden. Folglich wird für die Layer-3- oder SVI-Übergabeschnittstelle an einem SDA-Grenzknoten standardmäßig diese größere MTU verwendet.

SD-WAN-Edge-Geräte wie die Catalyst Serie 8000 hingegen verwenden standardmäßig eine Schnittstellen-MTU von 1.500 Byte. Dies ist ein Standard für Schnittstellen, die sich mit externen Netzwerken wie Internet Service Providern (ISPs) verbinden, bei denen Jumbo Frames nur gelegentlich unterstützt werden oder nicht aktiviert sind.

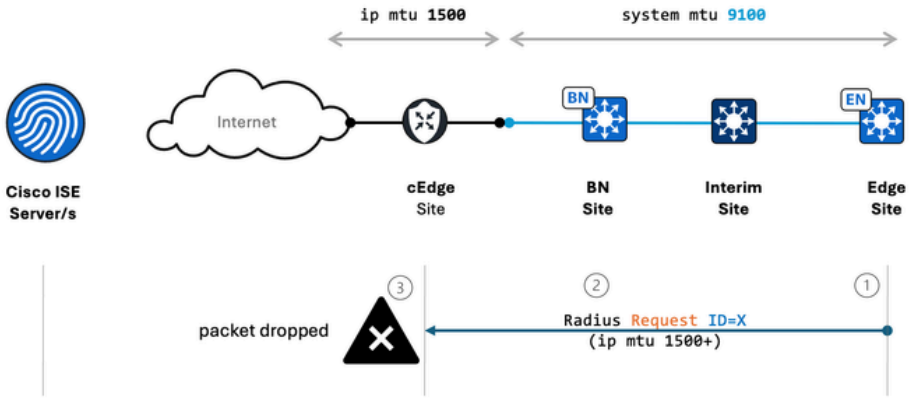
Diese Diskrepanz führt zu einem potenziellen sofortigen Scheitern: eine SDA-Grenze, die versucht, ein IP-Paket mit mehr als 1500 Byte an einen SD-WAN-Edge zu senden, dessen Empfangsschnittstelle für eine MTU von 1500 Byte konfiguriert ist.

Diese Art von MTU-Diskrepanz ist eine häufige Fallgrube in SDA-Bereitstellungen und kann während der Konfiguration oft leicht übersehen werden. Noch schwieriger wird es, wenn bestimmte Verhaltensweisen im Zusammenhang mit der Art und Weise, wie RADIUS-Anfragen auf Catalyst 9000-Switches mit Cisco IOS-XE® generiert werden, dazu führen können, dass diese Probleme nur unter bestimmten und kritischen Bedingungen auftreten.

RADIUS-Anforderungen, die während des vom Session Manager Daemon (SMD)-Prozess verarbeiteten Endbenutzer-Authentifizierungsprozesses generiert werden, sind beispielsweise fest codiert, um Pakete mit 1.396 Byte zu fragmentieren. RADIUS-Anfragen, die TrustSec-Richtlinien abrufen, z. B. Security Group Access Control List (SGACLs), werden dagegen von den Unterkomponenten des Cisco Internetworking Operating System Daemon (IOSd) generiert. Diese sind MTU-fähig und können die Fragmentierung von Paketen vermeiden, sofern ihre Größe die System-MTU nicht überschreitet (in der Regel bis zu 9100 Byte).

Probleme im Zusammenhang mit MTU-Diskrepanzen treten daher erst bei der Verwendung von Cisco TrustSec (CTS)-Downloadrichtlinien auf. Darüber hinaus kann der Satz von rollenbasierten Zugriffskontrolllisten (RBACLs), die von einem SDA-Edge-Gerät während der Benutzerauthentifizierung heruntergeladen werden, variieren, je nachdem, welche SGACL-Richtlinien für andere Tags bereits vorhanden sind. In der Praxis lädt der Switch nur die Bereiche herunter, in denen sich die Richtlinien nicht überschneiden.

Zusammen können diese Verhaltensweisen zu unvorhersehbaren und inkonsistenten Ergebnissen führen, die von stillen Ausfällen bis hin zu unvollständigen Richtliniendownloads reichen. Dies hängt von der Größe der SGACL-Richtlinie, den aktuellen Systembedingungen und letztlich von MTU-Fehlausrichtungen entlang des Pfads ab.



SDA Border leitet ein großes RADIUS-Paket (z. B. 1600 Byte) über das SD-WAN-Edge an die ISE weiter. Dies geschieht:

1. Die SDA Border mit ihrer 9100-MTU-Schnittstelle sendet das 1600-Byte-IP-Paket.
2. Der Cisco Edge-Router im SD-WAN empfängt dieses Paket über seine Schnittstelle mit 1.500 MTU.
3. Wenn das DF-Bit (Do Not Fragment) jedoch nicht für diese RADIUS-Pakete festgelegt ist, kann der Cisco Edge-Router des SD-WAN diese Pakete beim Eingang verwerfen, nur weil sie im Verhältnis zur konfigurierten Schnittstellen-MTU "überdimensioniert" sind. Es gelangt nicht zur Stufe der IP-Weiterleitungslogik, wo eine Fragmentierung in Betracht gezogen werden kann (wenn das DF-Bit dies zulässt).

Dieser automatische Ausfall führt zu erheblichen Schwierigkeiten bei der Fehlerbehebung, insbesondere da das Problem in eine bestimmte Richtung (SDA zu SD-WAN/ISE) verläuft.

Eine ähnliche MTU-Diskrepanz kann an den Core- oder Leaf-Switches des Rechenzentrums (DC) auftreten, die in der Regel für die Unterstützung von Jumbo Frames (z. B. MTU 9000+) konfiguriert sind, um die Effizienz des internen Datenverkehrs im Rechenzentrum zu verbessern. Wenn der Datenverkehr jedoch an die LAN-Schnittstelle eines Cisco Edge-Routers mit SD-WAN-DC und einer Standard-MTU (z. B. 1500 Byte) übergeben wird, kann diese Diskrepanz zu Fragmentierung oder Paketverlusten führen, insbesondere beim Datenverkehr, der vom Rechenzentrumsnetzwerk in die SD-WAN-Fabric fließt.

Lösung für Herausforderung 1:

Richten Sie die IP-MTU an der Übergabeschnittstelle der SDA-Grenze (physisch oder SVI) mit der Cisco Edge-Router-Schnittstelle des SD-WAN-Peering aus (in der Regel 1.500 Byte).

Konfigurationsbeispiel (auf SDA Border Node):

<#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
!
```

Wichtige Überlegungen: Fragmentierung an den Grenzen des Catalyst 9000

Catalyst Switches der Serie 9000 unterstützen als SDA Border Nodes die IP-Fragmentierung für native IP-Pakete auf Hardwaredatenebene. Die Reduzierung der ip mtu an der Übergabeschnittstelle auf 1500 führt nicht zu einer Leistungsverschlechterung aufgrund der softwarebasierten Fragmentierung für Datenverkehr, der von der oder über die erforderliche Grenze verläuft. Der Switch fragmentiert effizient IP-Pakete, die größer als 1500 Byte sind (wenn das DF-Bit leer ist), bevor diese spezifische Schnittstelle außer Kraft gesetzt wird, ohne die CPU zu stanzen.

Beachten Sie jedoch, dass Catalyst 9000-Switches im Allgemeinen keine Fragmentierung des VXLAN-gekapselten Datenverkehrs unterstützen. Diese Einschränkung ist für den Overlay-Datenverkehr entscheidend, hat jedoch keine Auswirkungen auf das beschriebene RADIUS-Authentifizierungsszenario, da die RADIUS-Kommunikation zwischen der SDA-Grenze und einer externen ISE in der Regel innerhalb des Underlays stattfindet (natives IP-Routing). (MTU-Überlegungen für VXLAN-Overlays sind ein separates, komplexes Thema und werden in den entsprechenden Cisco SDA-Designleitfäden ausführlich behandelt.)

Proaktive MTU-Ausrichtung bei der Übergabe von SDA Border an SD-WAN Cisco Edge Router ist wichtig.

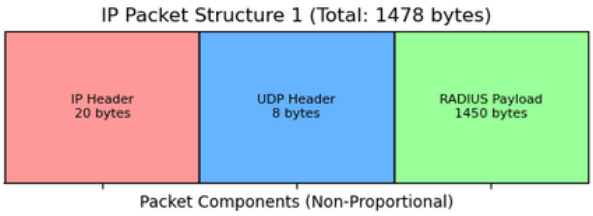
Herausforderung 2: Der MTU-Engpass - ISE-Datenverkehr über das SD-WAN-Overlay

Selbst wenn für einzelne physische Schnittstellen wie die ISE-Netzwerkschnittstellenkarte (NICs), die Switch-Ports oder die Router-Schnittstellen eine standardmäßige IP-MTU von 1500 Byte festgelegt sind, führt das SD-WAN-Overlay selbst zu einem Kapselungs-Overhead. Dieser Overhead belegt einen Teil des 1500-Byte-Grenzwerts und reduziert die effektive MTU, die für das ursprüngliche IP-Paket (die "Nutzlast" aus Sicht der ISE) zur Verfügung steht.

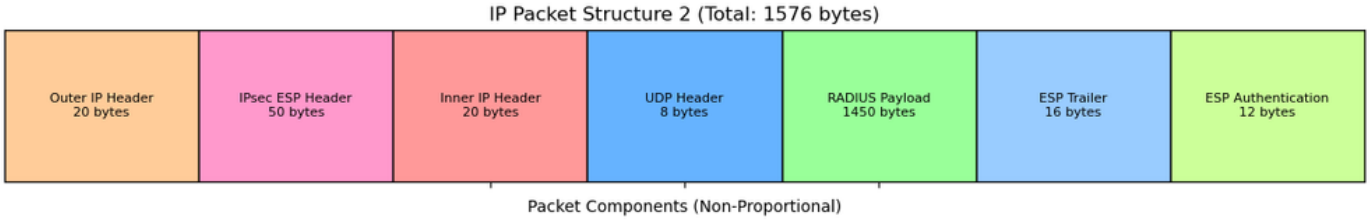
Paketstruktur und Kapselungsaufwand:

Wenn ein IP-Paket von einem ISE-Server (z. B. ein RADIUS Access-Accept-Paket) an ein Netzwerkzugriffsgerät (Network Access Device, NAD) an einem SDA-Standort gesendet wird, durchläuft es das SD-WAN-Overlay und wird gekapselt. Ein gängiger Kapselungs-Stack verwendet IPsec im Tunnelmodus, möglicherweise über UDP für NAT-Traversal (NAT-T).

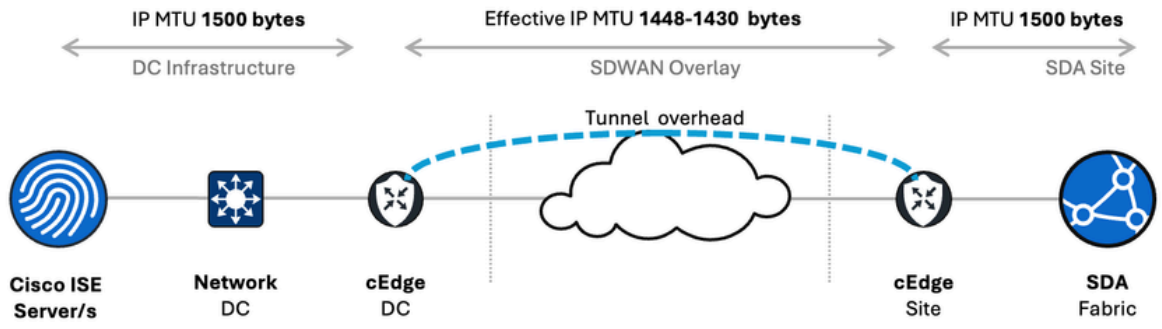
- Original-Paket von ISE (inneres Paket):
  Beispiel: Ein RADIUS-Paket mit einer Nutzlast von 1450 Byte + 8B UDP + 20B Inner IP = 1478 Byte.



- Betrachten Sie IPsec ESP im Tunnelmodus, möglicherweise mit UDP-Kapselung für NAT-T:



- Der gesamte Overhead kann je nach den spezifischen IPsec-Verschlüsselungen, Authentifizierungsmechanismen und anderen Overlay-Funktionen (wie GRE, falls verwendet) variieren. Eine typische Berechnung:
  - Äußerer IP-Header (IPv4): 20 Byte
  - UDP-Header (bei ESP über UDP für NAT-T): 8 Byte
  - ESP-Header: ~8 Byte
  - ESP IV (beispielsweise für AES-CBC): ~16 Byte (falls zutreffend)
  - ESP-Authentifizierung (z. B. HMAC-SHA256 abgeschnitten): ~12-16 Bytes
  - Allgemeiner geschätzter IPsec-Overhead: ~52-70 Byte (kann höher sein, mit allen Optionen bis zu ~80 Byte oder mehr).



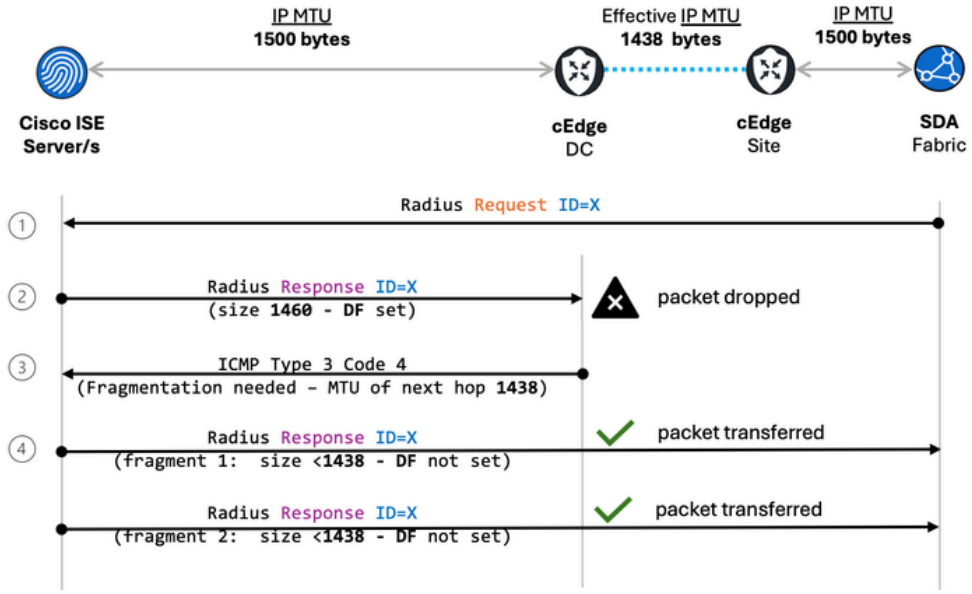
Wenn die MTU der physischen Verbindung 1.500 Byte beträgt, ergibt sich folgende Payload-MTU für das ursprüngliche IP-Paket von der ISE: 1500 Byte - SD-WAN-Overhead.
Beispiel: 1500 - 70 = 1430 Byte.

Verhalten bei Paketüberschreitung der effektiven MTU:

1. Die ISE erzeugt ein Paket (die DF-Bit-Anomalie):
    - Standardmäßig legt das zugrunde liegende Linux-Betriebssystem einer ISE-Appliance den Do Not Fragment (DF)-Befehl im IP-Header für alle Pakete fest, die von ihm ausgehen und die kleiner oder gleich der konfigurierten IP-MTU der Schnittstelle sind (z. B. 1500 Byte).
    - Zweck dieses DF-Bits:ISE setzt das DF-Bit (über sein Betriebssystem) proaktiv in erster Linie, um den später beschriebenen PMTUD-Prozess (Path MTU Discovery) zu nutzen. Auf diese Weise kann die ISE die tatsächliche PMTU zu einem Ziel dynamisch erfassen, wenn diese kleiner ist als ihre eigene Schnittstellen-MTU.
    - Verhalten für Pakete, die größer als die Schnittstellen-MTU sind:Wenn die ISE ein IP-Paket senden muss, das größer als die konfigurierte Schnittstellen-IP-MTU ist, hängt das Verhalten vom Linux-Betriebssystem ab. Normalerweise kann das Betriebssystem das Paket vor der Übertragung fragmentieren und das DF-Bit (Einstellung DF=0) für diese resultierenden Fragmente löschen. Diese Fragmentierung ist eine Funktion auf Betriebssystemebene, die nicht direkt vom ISE-Anwendungscode selbst gesteuert wird.
    - Wichtigste Unterscheidung von Netzwerkgeräten: Dieses Standardverhalten der ISE (Einstellung DF=1 auch für nicht fragmentierte Pakete, die in die MTU der Schnittstelle passen) unterscheidet sich erheblich von vielen herkömmlichen Netzwerkgeräten (Router, Switches). Netzwerkgeräte setzen das DF-Bit häufig nicht auf Pakete, die sie erzeugen oder weiterleiten, es sei denn, sie sind ausdrücklich dafür konfiguriert, oder das weitergeleitete Paket hat bereits das DF-Bit festgelegt, oder für bestimmte Protokolle, die es erfordern. Sie lassen in der Regel standardmäßig eine Fragmentierung zu, wenn ein Paket die Next-Hop-MTU (und DF=0) überschreitet.
    - Komplexität der Fehlerbehebung: Diese Asymmetrie, bei der der ISE-zu-NAD-Datenverkehr standardmäßig oft DF=1 hat, während der NAD-zu-ISE-Datenverkehr DF=0 haben kann (es sei denn, die NAD legt sie aus einem bestimmten Grund fest), kann zu einer zusätzlichen Komplexitätsschicht bei der Fehlerbehebung führen. Je nach Richtung des Datenverkehrsflusses können die Techniker unterschiedliche Fragmentierungsverhalten und PMTUD-Interaktionen beobachten.
2. Paket erreicht eingehenden Cisco Edge-Router (DC): Der Cisco Edge-Router des DC empfängt das IP-Paket von der ISE.
3. Kapselung und MTU-Prüfung durch Cisco Edge-Router: Der Cisco Edge-Router versucht, das Paket für den SD-WAN-Tunnel zu kapseln.
    - Wenn die ursprüngliche Paketgröße und der SD-WAN-Kapselungsoverhead die MTU der ausgehenden physischen Schnittstelle des Cisco Edge-Routers (z. B. 1500 Byte) überschreiten UND das DF-Bit für das ursprüngliche (innere) Paket der ISE festgelegt ist, darf der Cisco Edge-Router das innere Paket nicht fragmentieren.
    - Der Cisco Edge-Router sollte das Paket verwerfen.
    - Entscheidend ist, dass der Cisco Edge-Router außerdem eine ICMP-Meldung "Destination Unreachable - Fragmentation Needed and DF bit set" (Typ 3, Code 4) an die Quelle (ISE) sendet, die die MTU des nächsten Hop (die effektive MTU des Tunnels) angibt.
4. PMTUD-Prozess (Path MTU Discovery): Nach Erhalt der ICMP-Meldung "Fragmentation Needed" (Fragmentierung erforderlich) sollte die ISE (das Quellbetriebssystem) ihre PMTU-Schätzung für diesen spezifischen Zielpfad reduzieren. Diese Informationen werden

zwischengespeichert und in kleineren Paketen, die in die neu erkannte PMTU passen, erneut gesendet.

PMTUD-Prozessdiagramm:



Wo die PMTUD-Kommunikation zusammenbricht:
Die PMTUD ist in der Theorie robust, kann aber in der Praxis scheitern:

- ICMP-Filterung: Zwischengeschaltete Firewalls oder Sicherheitsrichtlinien blockieren häufig ICMP-Nachrichten und verhindern, dass die Meldung "Fragmentation Needed" (Fragmentierung erforderlich) die ISE erreicht.
- Control Plane Policing (CoPP) auf Cisco Edge-Routern: Cisco Edge Router verwenden CoPP, um ihre CPU zu schützen. Das Generieren von ICMP-Fehlermeldungen ist eine Aufgabe auf Kontrollebene. Bei hoher Auslastung oder bei vielen übergroßen Paketen kann CoPP die ICMP-Erzeugung begrenzen oder verwerfen. Die ISE erhält dieses Feedback nie.
- Stille Tropfen: Wenn die ISE die ICMP-Meldung "Fragmentation Needed" (Fragmentierung erforderlich) nicht erhält, ist sie sich der Pfadbeschränkung nicht bewusst. Es werden weiterhin große Pakete mit festgelegtem DF-Bit gesendet, sodass diese vom Eingangs-Cisco Edge-Router stillschweigend verworfen werden. Dies führt zu Timeouts und erneuten Übertragungen auf Anwendungsebene (z. B. RADIUS).
- Auswirkungen auf ISE-Services: Besonders anfällig sind große RADIUS Access-Accept-Pakete (mit dACLs, umfangreichen AVPs, SGT-Informationen). Die Manifestationen umfassen:
  - Intermittierende oder vollständige Authentifizierungsfehler.
  - Endpunkte erhalten keine richtigen Netzwerkzugriffsrichtlinien oder SGTs.
  - Unvollständige oder fehlgeschlagene Synchronisierung der Richtlinien zwischen ISE

und NADs.

Lösung für Herausforderung 2: Proaktive ISE IP MTU-Konfiguration

Angesichts der Unzuverlässigkeit der PMTUD ist ein proaktiver Ansatz am besten für kritische Services wie die ISE geeignet. Konfigurieren Sie die IP-MTU an den Netzwerkschnittstellen der ISE auf einen Wert, der den maximal erwarteten SD-WAN-Overhead sicher bewältigt. Dadurch wird sichergestellt, dass die ISE keine IP-Pakete (mit festgelegtem DF-Bit) erzeugt, die von Natur aus zu groß sind, um das SD-WAN-Overlay zu durchlaufen, ohne dass eine Fragmentierung durch ein zwischengeschaltetes Gerät erforderlich ist (was verboten ist, wenn DF=1 ist).

Berechnen und Festlegen der empfohlenen ISE-IP-MTU:

1. Festlegen einer physischen Basis-MTU: Dies sind in der Regel 1.500 Byte für Standard-Ethernet-Schnittstellen entlang des Pfads.
2. Bestimmen des maximalen Overheads der SD-WAN-Kapselung:
    - Berechnen Sie den durch Ihr spezifisches SD-WAN-Overlay (IPsec, GRE, VXLAN, MPLSoGRE usw.) verursachten Overhead genau, oder schätzen Sie ihn vorsichtig ein. Genaue Angaben zu den von Ihnen ausgewählten Protokollen und Optionen finden Sie in der Dokumentation des Herstellers.

Komponente	Beispiel-Overhead (Byte)	Hinweise
Physische Basis-MTU	1500	Standard-Ethernet auf physischen Verbindungen
Weniger: SD-WAN-Overhead		
Äußerer IP-Header (IPv4)	20	
UDP-Header (für NAT-T)	8	Wenn ESP in UDP gekapselt ist
ESP-Header	~8 bis 12	
ESP IV (z. B. AES-CBC)	~16	Variiert je nach Verschlüsselungsalgorithmus
ESP-Auth. (z. B. SHA256)	~12-16	Variiert je nach Authentifizierungsalgorithmus (z. B. 96-Bit für einige)
Andere Overlays (GRE usw.)	Variable	Hinzufügen, wenn Teil des SD-WAN-Kapselungsstapels
Geschätzter Gesamtbetrag	~68 - 80+ Byte	Summe aller relevanten Komponenten für Ihre Bereitstellung
MTU für effektiven Pfad	~1432 - 1420 Bytes	Physische MTU-Basis - geschätzter Gesamtaufwand

3. Empfohlene ISE IP MTU-Konfiguration:
    - Nehmen wir die berechnete effektive Pfad-MTU (z. B. 1420 Byte aus dem Beispiel).
    - Subtrahieren Sie eine zusätzliche Sicherheitsmarge (z. B. 20-70 Byte), um kleinere, nicht berücksichtigte L2-Header zu berücksichtigen oder einen Puffer bereitzustellen.
    - Lösungen wie Cisco SD-WAN können die PMTU-Erkennung (Path MTU) für jeden Site-to-Site-Tunnel einzeln durchführen. Dieser Mechanismus wird automatisch alle 20

Minuten ausgeführt, um die IP-MTU des Tunnels entsprechend den aktuellen Transportbedingungen an jedem Standort zu testen und dynamisch anzupassen. Dadurch können sich die MTU-Werte zwischen den Standorten unterscheiden und im Laufe der Zeit ändern.
- Eine im Allgemeinen sichere und empfohlene IP-MTU für ISE-Schnittstellen in solchen Szenarien liegt zwischen 1350 und 1400 Byte

Eine IP-MTU von 1350 Byte ist häufig ein sehr robuster Ausgangspunkt.

ISE-Konfiguration (Beispiel über CLI):

Dieser Befehl wird in der CLI der Cisco ISE-Appliance für jede relevante Netzwerkschnittstelle ausgeführt.

<#root>

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

 ip mtu 1350
!
```

Wichtige betriebliche Aspekte bei Änderungen der ISE-IP-MTU:

- Dienstneustart erforderlich: Bei Anwendung des Befehls ip mtu auf eine ISE-Schnittstelle wird der Benutzer aufgefordert, die ISE-Anwendungsdienste neu zu starten. Diese Änderung wirkt sich auf den Service aus und muss während eines geplanten Wartungsfensters geplant werden. Einzelheiten zum Verfahren finden Sie in der offiziellen Cisco ISE-Dokumentation.
- Auf alle ISE-Knoten anwenden: Diese IP-MTU-Anpassung muss konsistent auf alle ISE-Knoten in der Bereitstellung (primäres PAN, sekundäres PAN, Policy Service Nodes (PSNs)) angewendet werden, die über das SD-WAN mit NADs kommunizieren. Inkonsistente MTU-Einstellungen führen zu unvorhersehbarem Verhalten.
- Gründliche Tests: Testen Sie diese Änderung vor der Implementierung in der Produktionsumgebung eingehend in einer Testumgebung oder einem Pilotprojekt. Verwenden Sie Tools wie Ping mit unterschiedlichen Paketgrößen und dem DF-Bit-Set, um die End-to-End-MTU-Verarbeitung zu validieren:
    - Linux-basierte Systeme:

```
ping

        -s
```

```
-M do
```

(Hinweis: -s gibt die ICMP-Nutzlastgröße an. IP-Gesamtpaketgröße = Nutzlast + 8 Mrd ICMP-Hdr + 20 Mrd IP-Hdr für IPv4)

- Windows:

```
ping

-f -l
```

(Hinweis: -l gibt die ICMP-Nutzlastgröße an.)

- Cisco IOS/Cisco IOS-XE®

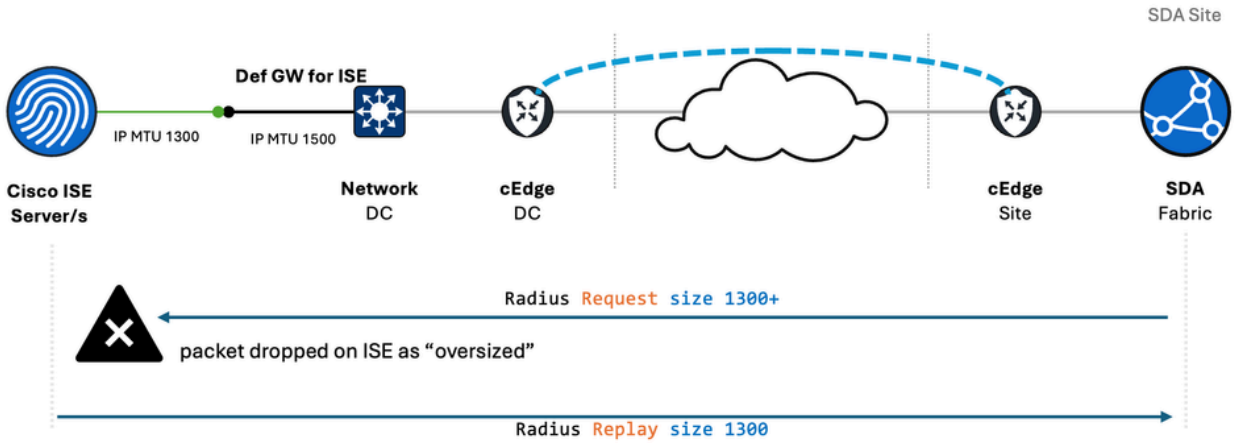
```
ping

size

df-bit
```

- ISE First Routing Point - Wenn Sie den IP-MTU-Wert an der ISE-Schnittstelle anpassen, stellen Sie sicher, dass der erste Routing-Punkt im Rechenzentrum - insbesondere die dem ISE-Subnetz zugeordnete Layer-3-Schnittstelle - ebenfalls mit demselben IP-MTU-Wert konfiguriert ist.
  Auf diese Weise können Situationen wie in Herausforderung 1 vermieden werden, in denen eine MTU-Abweichung dazu führt, dass die ISE eingehende Pakete als überdimensioniert

behandelt und verwirft.
Wenn die ISE-Schnittstelle beispielsweise eine reduzierte MTU (z. B. 1300) aufweist, der erste Routing-Punkt jedoch mit der Standard-MTU von 1500 konfiguriert bleibt, werden an die ISE gesendete Pakete, die größer als 1300 Byte, aber kleiner als 1500 Byte sind, nicht fragmentiert und werden von der ISE verworfen (siehe). Herausforderung 1:
Stellen Sie außerdem sicher, dass der erste Routing-Punkt bei Bedarf fragmentiert werden kann und dass dies nicht zu Leistungseinbußen führt.

- MTU über den gesamten Übertragungspfad und in beide Richtungen aktualisieren - Bei der Aktualisierung der IP-MTU-Einstellungen auf der ISE ist es wichtig, die MTU über den gesamten Übertragungspfad und in beide Richtungen zu berücksichtigen. Wenn der auf der ISE konfigurierte MTU-Wert nicht mit der MTU auf der Layer-3-Schnittstelle des First-Hop-Gateways abgestimmt ist, können ähnliche Probleme auftreten, wie in Challenge #1 beschrieben.

  Wenn die ISE-MTU beispielsweise auf 1.300 Byte reduziert wird, während die standardmäßige 1.500-Byte-MTU auf dem Standard-Gateway konfiguriert bleibt, können Pakete mit einer Größe zwischen 1.300 und 1.500 Byte, die in der Regel von Netzwerkgeräten generiert werden, von der ISE als überdimensioniert verworfen werden.



  Um dieses Problem zu vermeiden, müssen Sie immer sicherstellen, dass MTU-Änderungen auf der ISE auf dem First-Hop-Gateway gespiegelt werden und sich im Idealfall auf allen End-Hosts im gleichen Layer-3-Segment widerspiegeln. Dies trägt zur Erhaltung der End-to-End-MTU-Konsistenz bei und verhindert unerwartete Paketverluste.

Schlussfolgerung

Die Anpassung der IP-MTU-Einstellungen auf Cisco ISE-Servern an die effektiven MTU-Grenzwerte auf Transportebene, die durch SD-WAN-Kapselung und MTU-Ausrichtung bei der Übergabe von SDA Border an SD-WAN Cisco Edge Router auferlegt werden, ist nicht nur eine Empfehlung, sondern eine entscheidende Voraussetzung für die Gewährleistung der Stabilität, Zuverlässigkeit und Leistung von AAA-Services in modernen, segmentierten Unternehmensnetzwerken. Die MTU-Pfaderkennung ist zwar ein wichtiger Mechanismus, seine praktische Wirksamkeit kann jedoch durch Faktoren wie ICMP-Filterung oder Control Plane

Policing in SD-WAN-Umgebungen beeinträchtigt werden.

Durch die proaktive Konfiguration einer reduzierten IP-MTU auf der ISE (z. B. 1350-1400 Byte) können Netzwerkarchitekten und -techniker das Risiko von Paketverlusten aufgrund der MTU erheblich reduzieren und einen besser vorhersehbaren und ausfallsichereren Netzwerkbetrieb sicherstellen. Dies ist besonders wichtig in Cisco SDA-Bereitstellungen, in denen die ISE eine differenzierte Mikrosegmentierung und dynamische Richtliniendurchsetzung orchestriert, die häufig auf der erfolgreichen Bereitstellung potenziell großer Kontrollebenen-Nachrichten beruht. Sorgfältige Planung, umfassende Tests und eine konsistente Konfiguration über alle ISE-Knoten hinweg sind der Schlüssel zu einer erfolgreichen und problemlosen Bereitstellung.

Standards und Referenzen

Weitere Informationen finden Sie in den offiziellen Standards und in der Cisco Dokumentation:

RFCs

- RFC 1191 MTU-Pfaderkennung
- RFC 791: Internet Protocol (IP) - Definiert den IP-Header, einschließlich des DF-Bits (Do Not Fragment).
- RFC 8200: IPv6-Spezifikation (relevant bei Verwendung von IPv6, beinhaltet ähnliche PMTUD-Konzepte).
- RFC 4459: Probleme mit MTU und Fragmentierung bei In-the-Network Tunneling (VPNs): Behebt Probleme mit MTU in VPN-Umgebungen direkt.

Cisco-Dokumentation:

- Cisco SDA Design- und Bereitstellungsleitfäden: Weitere Informationen zu den Fabric-MTU-Empfehlungen und den Grenzknotenkonfigurationen finden Sie hier.
- Cisco SD-WAN Design- und Konfigurationsleitfäden: Nähere Informationen zu Kapselungs-Overhead, MTU der Tunnelschnittstellen und PMTUD innerhalb der SD-WAN-Fabric
- Konfigurationsanleitungen für Cisco Catalyst Switches der Serie 9000: Plattformspezifische Details zu MTU-Einstellungen und Fragmentierungsfunktionen
- Cisco Identity Services Engine (ISE) Administrator- und CLI-Leitfäden: Informationen zur Schnittstellenkonfiguration, einschließlich des Befehls ip mtu und Auswirkungen auf den Neustart des Diensts.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.