Configuración de MTU IP de ISE óptima en SD-WAN para implementaciones de SDA

Contenido

Introducción

Este documento describe cómo los problemas de la unidad de transmisión máxima (MTU) pueden afectar a la microsegmentación en SDA cuando se utiliza SD-WAN para conectar sitios SDA.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso definido por software (SDA) de Cisco
- Redes de área extensa definidas por software (SD-WAN) de Cisco
- Cisco Identity Services Engine (ISE)

Componentes Utilizados:

La información de este documento se basa en SDA, SDWAN e ISE.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las redes empresariales modernas aprovechan cada vez más SDA para la microsegmentación granular y la aplicación coherente de políticas. Para conectar sitios SDA distribuidos, a menudo se emplea la SD-WAN de Cisco, que ofrece un transporte ágil, seguro y optimizado a través de varias redes subyacentes. Un elemento fundamental de esta arquitectura es que ISE proporciona servicios críticos de autenticación, autorización y contabilidad (AAA), junto con la distribución dinámica de políticas (por ejemplo, etiquetas de grupos de seguridad (SGT) y ACL descargables).

Aunque robusta, la integración de estas potentes tecnologías puede introducir retos de configuración sutiles pero impactantes. La gestión de MTU en los puntos críticos de transferencia de red y a través de la superposición de SD-WAN es un área primordial para estos problemas. Este artículo aborda dos escenarios comunes de discordancia de MTU que pueden interrumpir las operaciones de red:

1. La brecha de MTU entre los nodos de borde SDA y los dispositivos de borde SD-WAN.
2. Restricciones de MTU para el tráfico originado en ISE que atraviesa la superposición SD-WAN.

La alineación adecuada de MTU es fundamental para evitar problemas de fragmentación de paquetes o caídas silenciosas, lo que garantiza una autenticación fiable, la aplicación de políticas y la estabilidad general de la red. Si no se solucionan estos problemas, puede producirse una conectividad intermitente desconcertante y fallos en la aplicación de políticas, lo que consume un esfuerzo considerable en la resolución de problemas.

Síntomas comunes de MTU desalineada

La MTU mal alineada puede manifestarse de varias maneras, lo que a menudo conduce a problemas difíciles de diagnosticar:

- Fallos o tiempos de espera intermitentes de autenticación RADIUS: Especialmente notable para las políticas que generan paquetes RADIUS más grandes (por ejemplo, aquellos con pares AV o certificados extensos).
- Terminales que no reciben o aplican ACL descargables (dACL) o políticas TrustSec (SGT/SGACL): Estas políticas se transmiten a menudo en grandes paquetes RADIUS.
- Establecimiento de sesión lento para clientes autenticados: Debido a retransmisiones en la capa de aplicación.
- Retransmisiones RADIUS excesivas: Se puede observar en los registros de ISE o en los dispositivos de acceso a la red (NAD).
- Propagación de políticas incoherente: Es posible que los cambios de políticas realizados en ISE no se propaguen de forma coherente a todos los NAD de los sitios SDA remotos.

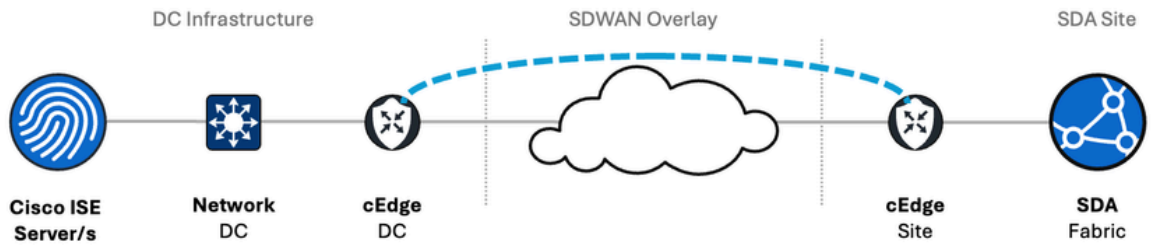
- Discrepancias en la captura de paquetes: Las capturas pueden mostrar que ISE envía paquetes grandes (por ejemplo, >1450 bytes) con el bit Do Not Fragment (DF) configurado, pero sin respuesta correspondiente o error ICMP "Fragmentation Needed" (Se necesita fragmentación) del router de extremo de Cisco NAD o SD-WAN.
- Incremento de contadores de caídas de paquetes: Se observa en la interfaz de entrada del router de extremo de Cisco para el Data Center (DC) para el tráfico procedente de ISE y destinado a sitios SDA, o en la interfaz del router de extremo de Cisco SD-WAN que se encuentra frente al borde SDA para el tráfico en dirección inversa.

Descripción de problemas

Una implementación empresarial típica
Considere una topología empresarial común:

- Servidores de Cisco ISE: Implementado en un Data Center (DC) centralizado o en centros regionales, conectado a la infraestructura de red de DC.
- Infraestructura de DC: Incluye switches de agregación o núcleo de DC a los que se conectan los servidores ISE.
- Superposición de SD-WAN: Los routers Cisco Edge Router de DC establecen túneles SD-WAN (normalmente IPsec) a través de una red de transporte subyacente (por ejemplo, Internet, MPLS) a los routers Cisco Edge Router en sitios SDA remotos.
- Sitio SDA: Los routers Cisco Edge Router de sitio remoto se conectan al fabric SDA local, que incluye los nodos de borde del fabric, los nodos de borde, los controladores de LAN inalámbrica (WLC) y, en última instancia, los terminales.

Topología ilustrativa



Reto 1: La brecha de MTU: límites SDA a los extremos SD-WAN

Los principios de diseño de Cisco SDA, que a menudo se implementan mediante automatización

de LAN, promueven una MTU de 9100 bytes (tramas gigantes) en todas las instalaciones de todos los dispositivos de fabric. Esto incluye los nodos de borde de la serie Catalyst 9000 y garantiza que las tramas gigantes Ethernet se transporten de manera eficiente dentro del fabric. En consecuencia, la interfaz de transferencia de la Capa 3 o SVI en un nodo de borde SDA toma de forma predeterminada esta MTU más grande.

Por el contrario, los dispositivos periféricos SD-WAN, como Catalyst serie 8000, suelen tener de forma predeterminada una MTU de interfaz de 1500 bytes. Se trata de un estándar para las interfaces que se conectan a redes externas, como los proveedores de servicios de Internet (ISP), en las que la compatibilidad con tramas gigantes es poco común o no está habilitada.

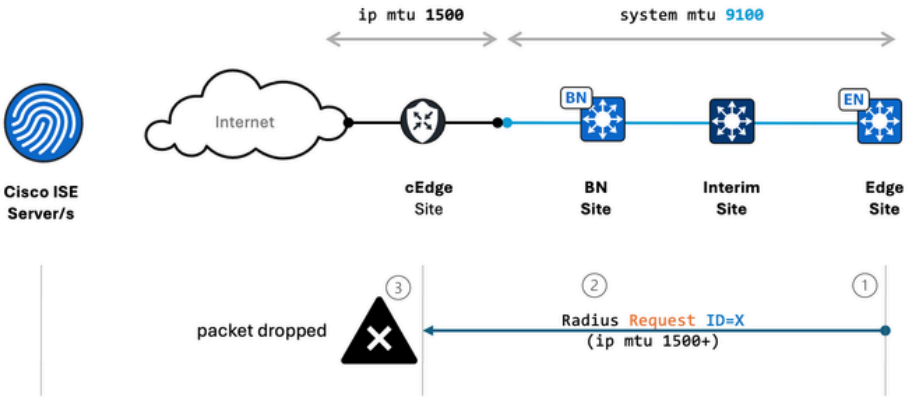
Esta disparidad crea un punto inmediato de potencial fracaso: un borde SDA que intenta enviar un paquete IP de más de 1500 bytes a un extremo SD-WAN cuya interfaz de recepción está configurada para una MTU de 1500 bytes.

Este tipo de discordancia de MTU es un obstáculo común en las implementaciones SDA y a menudo es fácil pasar por alto durante la configuración. Lo que lo hace más difícil es que ciertos comportamientos relacionados con cómo se generan las solicitudes RADIUS en los switches Catalyst 9000 que ejecutan Cisco IOS-XE® pueden hacer que estos problemas surjan solamente bajo condiciones específicas y críticas.

Por ejemplo, las solicitudes RADIUS generadas durante el proceso de autenticación de usuario final gestionado por el proceso Demonio del administrador de sesiones (SMD) están codificadas para fragmentar paquetes a 1396 bytes. Por el contrario, las solicitudes RADIUS involucradas en la recuperación de políticas TrustSec, como las listas de control de acceso de grupos de seguridad (SGACL), son generadas por los subcomponentes del daemon del sistema operativo de interconexión de redes (IOSd) de Cisco. Son compatibles con MTU y pueden evitar la fragmentación de paquetes a menos que su tamaño exceda la MTU del sistema (normalmente hasta 9100 bytes).

Como resultado, los problemas relacionados con las discordancias de MTU solo se hacen evidentes cuando se utilizan las políticas de descarga de Cisco TrustSec (CTS). Además, el conjunto de listas de control de acceso basadas en roles (RBACL) que descarga un dispositivo de extremo SDA durante la autenticación de usuarios puede variar en función de las políticas SGACL que ya estén presentes para otras etiquetas. En la práctica, el switch descarga sólo las partes no superpuestas de los conjuntos de políticas.

Juntos, estos comportamientos pueden producir resultados impredecibles e inconsistentes, que van desde fallos silenciosos hasta descargas de políticas incompletas, dependiendo del tamaño de la política SGACL, las condiciones actuales del sistema y, en última instancia, los desajustes de MTU a lo largo del trayecto.



El borde SDA reenvía un paquete RADIUS grande (por ejemplo, 1600 bytes) hacia ISE a través del borde SD-WAN, esto es lo que ocurre:

1. El borde SDA, con su interfaz de MTU 9100, envía el paquete IP de 1600 bytes.
2. El router periférico de Cisco SD-WAN recibe este paquete en su interfaz de MTU 1500.
3. Sin embargo, si el bit Do Not Fragment (DF) no se configura en estos paquetes RADIUS, el router de borde de Cisco SD-WAN a menudo puede descartarlos al ingresar simplemente porque están "sobredimensionados" en relación con su MTU de interfaz configurada. No llega a la etapa de la lógica de reenvío IP donde puede considerar fragmentarlos (si el bit DF lo permite).

Este descenso silencioso provoca importantes quebraderos de cabeza en la resolución de problemas, especialmente porque el problema es direccional (de SDA a SD-WAN/ISE).

Puede producirse una discordancia de MTU similar en los switches de hoja o de núcleo del Data Center (DC), que suelen configurarse para admitir tramas gigantes (por ejemplo, MTU 9000+) con el fin de mejorar la eficiencia del tráfico interno de DC. Sin embargo, si el tráfico se transfiere a la interfaz de cara a la LAN de un router de extremo de Cisco DC SD-WAN configurado con una MTU estándar (por ejemplo, 1500 bytes), esta discordancia puede provocar fragmentación o caídas de paquetes, especialmente para el tráfico que fluye desde la red DC al fabric SD-WAN.

Solución al Reto 1:

Alinee la MTU IP en la interfaz de transferencia del borde SDA (física o SVI) con la interfaz de router de extremo de Cisco SD-WAN de iguales, normalmente de 1500 bytes.

Ejemplo de configuración (en el nodo de borde 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
!
```

Consideración importante: Fragmentación en los bordes de Catalyst 9000

Los switches Catalyst de la serie 9000, como nodos fronterizos SDA, admiten la fragmentación de IP para paquetes IP nativos en el plano de datos de hardware. La reducción de la mtu ip en la interfaz de transferencia a 1500 no causa una degradación del rendimiento debido a la fragmentación basada en software para el tráfico que se origina o transita por el borde que lo necesita. El switch fragmenta de manera eficiente los paquetes IP de más de 1500 bytes (si el bit DF está despejado) antes de egresar esta interfaz específica, sin puntear a la CPU.

Sin embargo, es importante tener en cuenta que los switches Catalyst 9000 generalmente no soportan la fragmentación del tráfico encapsulado VXLAN. Esta limitación es fundamental para el tráfico superpuesto, pero no afecta al escenario de autenticación RADIUS descrito, ya que la comunicación RADIUS entre el borde SDA y un ISE externo suele producirse dentro de la capa subyacente (routing de IP nativa). (Las consideraciones de MTU para las superposiciones de VXLAN son un tema complejo e independiente, que se detalla en las guías de diseño SDA de Cisco relevantes).

La alineación proactiva de MTU en el límite SDA para la transferencia del router de extremo de Cisco SD-WAN es esencial.

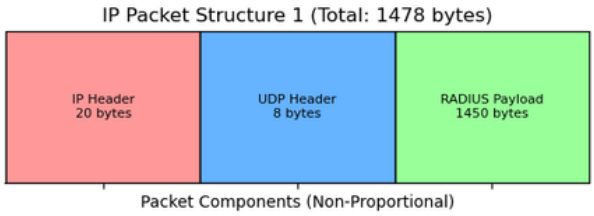
Reto 2: La compresión de MTU: tráfico de ISE a través de la superposición de SD-WAN

Incluso si las interfaces físicas individuales, como las tarjetas de interfaz de red (NIC) ISE, los puertos de switch o las interfaces de router se establecen en una MTU IP estándar de 1500 bytes, la superposición de SD-WAN introduce una sobrecarga de encapsulación. Esta sobrecarga consume una parte del límite de 1500 bytes, lo que reduce la MTU efectiva disponible para el paquete IP original (la "carga útil" desde la perspectiva de ISE).

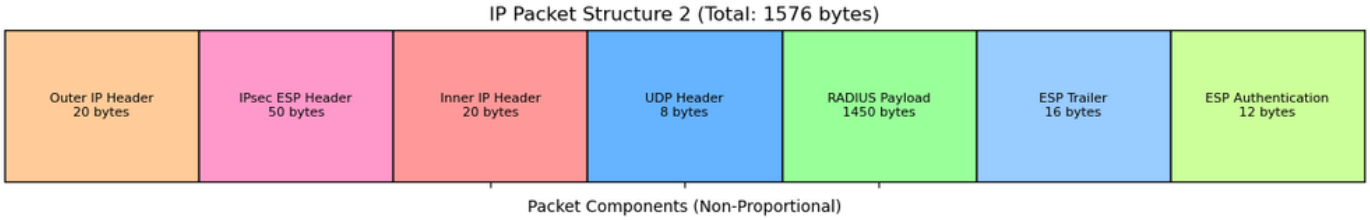
Sobrecarga de encapsulación y estructura de paquetes:

Cuando un paquete IP de un servidor ISE (por ejemplo, un paquete de aceptación de acceso RADIUS) se envía a un dispositivo de acceso a la red (NAD) en un sitio SDA, atraviesa la superposición SD-WAN y se encapsula. Una pila de encapsulación común implica IPsec en modo de túnel, potencialmente sobre UDP para NAT traversal (NAT-T).

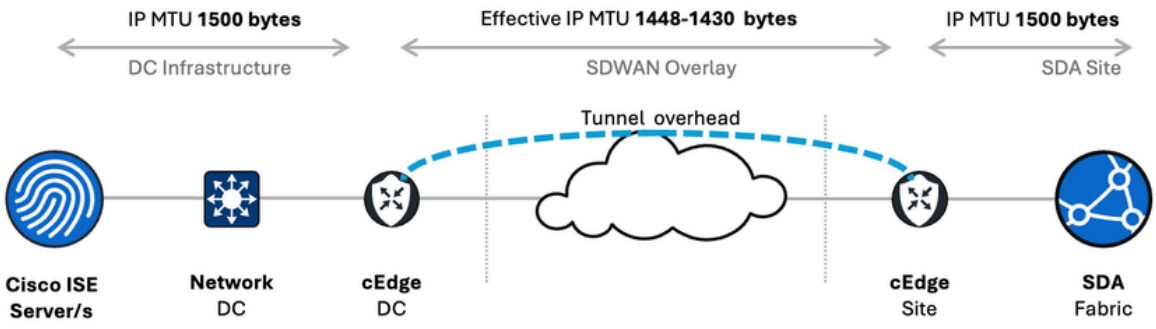
- Paquete original de ISE (paquete interno):
  Por ejemplo, un paquete RADIUS con una carga útil de 1450 bytes + 8B UDP + 20B IP interna = 1478 bytes.



- Considere IPsec ESP en modo túnel, potencialmente con encapsulación UDP para NAT-T:



- La sobrecarga total puede variar en función de los cifrados IPsec específicos, los mecanismos de autenticación y otras funciones de superposición (como GRE si se utiliza). Un cálculo típico:
    - Encabezado IP externo (IPv4): 20 bytes
    - Encabezado UDP (si ESP sobre UDP para NAT-T): 8 bytes
    - Encabezado ESP: ~8 bytes
    - ESP IV (por ejemplo, para AES-CBC): ~16 bytes (si corresponde)
    - Autenticación ESP (por ejemplo, HMAC-SHA256 truncada): ~12-16 bytes
    - Sobrecarga de IPsec estimada común: ~52-70 bytes (puede ser superior, hasta ~80 bytes o más con todas las opciones).



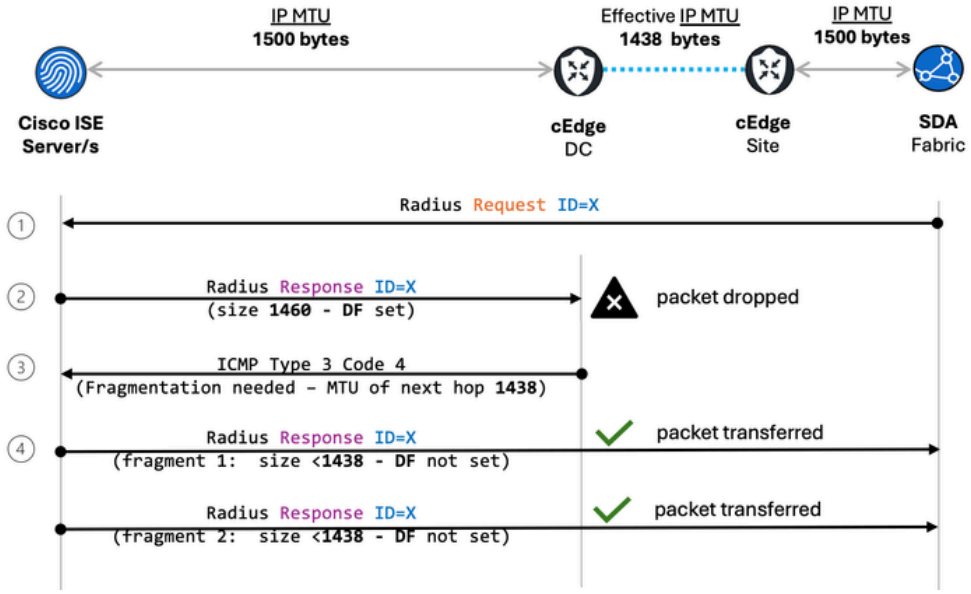
Si la MTU del link físico es de 1500 bytes, la MTU de carga útil disponible para el paquete de IP original de ISE se convierte en: 1500 bytes - Sobrecarga SD-WAN.
Por ejemplo, 1500 - 70 = 1430 bytes.

Comportamiento Cuando los Paquetes Exceden la MTU Efectiva:

1. ISE origina un paquete (la anomalía del bit DF):
    - De forma predeterminada, el sistema operativo Linux subyacente de un dispositivo ISE establece el bit Do Not Fragment (DF) en el encabezado IP para todos los paquetes que origina que sean menores o iguales a su MTU IP de interfaz configurada (por ejemplo, 1500 bytes).
    - Objetivo de este bit DF: ISE (a través de su sistema operativo) configura proactivamente el bit DF principalmente para aprovechar el proceso Path MTU Discovery (PMTUD), que se describe más adelante. Esto permite a ISE aprender dinámicamente la PMTU real a un destino si es más pequeña que su propia MTU de interfaz.
    - Comportamiento para paquetes mayores que la MTU de la interfaz:Si ISE necesita enviar un paquete IP mayor que la MTU de IP de la interfaz configurada, el comportamiento depende de su sistema operativo Linux. Normalmente, el comando OScanfragment fragmenta el paquete antes de la transmisión y borra el bit DF (configurando DF=0) en estos fragmentos resultantes. Esta fragmentación es una función de nivel de SO, no controlada directamente por el propio código de la aplicación ISE.
    - Distinción clave de los dispositivos de red:Este comportamiento predeterminado de ISE (configuración DF=1 incluso para paquetes no fragmentados que encajan dentro de su interfaz MTU) es significativamente diferente de muchos dispositivos de red tradicionales (routers, switches). Los dispositivos de red a menudo no configuran el bit DF en los paquetes que originan o reenvían a menos que se configure explícitamente para hacerlo, o si el paquete que se reenvía ya tiene el bit DF configurado, o para protocolos específicos que lo requieran. Normalmente permiten la fragmentación de forma predeterminada si un paquete excede la MTU del salto siguiente (y DF=0).
    - Resolución de problemas de complejidad:esta asimetría, en la que el tráfico de ISE a NAD suele tener DF=1 de forma predeterminada, mientras que el tráfico de NAD a ISE puede tener DF=0 (a menos que NAD lo establezca por un motivo), puede introducir un nivel adicional de complejidad durante la resolución de problemas. Los ingenieros pueden observar diferentes comportamientos de fragmentación e interacciones de PMTUD en función de la dirección del flujo de tráfico.
2. El paquete llega al router periférico Cisco (DC) de entrada: el router periférico Cisco DC recibe el paquete IP de ISE.
3. Encapsulación y comprobación de MTU mediante el router de extremo de Cisco:El router de extremo de Cisco intenta encapsular el paquete para el túnel SD-WAN.
    - Si el tamaño original del paquete más la sobrecarga de encapsulación SD-WAN excede la MTU de la interfaz física saliente del router de borde de Cisco (por ejemplo, 1500 bytes), Y el bit DF está configurado en el paquete original (interno) de ISE, el router de borde de Cisco no debe fragmentar el paquete interno.
    - El router de borde de Cisco debe descartar el paquete.
    - Lo más importante es que el router de extremo de Cisco también debe enviar un mensaje ICMP "Destination Unreachable - Fragmentation Needed and DF bit set" (Tipo 3, Código 4) al origen (ISE), indicando la MTU del salto siguiente (la MTU efectiva del túnel).
4. Proceso PMTUD (Path MTU Discovery): Al recibir este mensaje de ICMP "Fragmentation Needed" (Se necesita fragmentación), ISE (el sistema operativo de origen) debe reducir su

estimación de PMTU para esa ruta de destino específica. Almacenaría en caché esta información y reenviaría los datos en paquetes más pequeños que se ajusten a la PMTU recién descubierta.

Diagrama de proceso de PMTUD:



Donde se interrumpe la comunicación de PMTUD:
La PMTUD es sólida en teoría, pero puede fallar en la práctica:

- Filtrado ICMP: Los firewalls intermedios o las políticas de seguridad a menudo bloquean los mensajes ICMP, lo que impide que el mensaje "Fragmentación necesaria" llegue a ISE.
- Vigilancia del plano de control (CoPP) en el router de extremo de Cisco: Los routers Cisco Edge Router utilizan CoPP para proteger su CPU. La generación de mensajes de error ICMP es una tarea del plano de control. Bajo una carga pesada o con muchos paquetes sobredimensionados, CoPP puede limitar la velocidad o descartar la generación de ICMP. ISE nunca recibe los comentarios.
- Caídas silenciosas: Si ISE no recibe el mensaje "Fragmentation Needed" (Se necesita fragmentación) de ICMP, no tiene en cuenta la restricción de la ruta. Continúa enviando paquetes grandes con el bit DF configurado, lo que lleva a que el router de borde de Cisco de ingreso los descarte silenciosamente. Esto produce tiempos de espera y retransmisiones de la capa de aplicación (por ejemplo, RADIUS).
- Impacto en los servicios ISE: Los paquetes de aceptación de acceso RADIUS de gran tamaño (que transportan dACL, AVP extensos e información de SGT) son especialmente susceptibles. Las manifestaciones incluyen:
  - Fallos de autenticación intermitentes o completos.
  - Los terminales no reciben las políticas de acceso a la red o SGT correctas.

- Sincronización de políticas incompleta o fallida entre ISE y NAD.

Solución al Reto 2: Configuración proactiva de MTU de IP de ISE

Dada la poca fiabilidad de la PMTUD, un enfoque proactivo es mejor para servicios críticos como ISE. Configure la MTU de IP en las interfaces de red de ISE con un valor que se ajuste de forma segura a la sobrecarga de superposición de SD-WAN máxima esperada. Esto garantiza que ISE no origine paquetes IP (con el bit DF configurado) que sean inherentemente demasiado grandes para atravesar la superposición SD-WAN sin necesidad de fragmentación por parte de un dispositivo intermedio (lo que está prohibido si DF=1).

Cálculo y Configuración de la MTU IP de ISE Recomendada:

1. Establezca la MTU física base: Esto es típicamente 1500 bytes para las interfaces Ethernet estándar a lo largo de la trayectoria.
2. Determinación de la Sobrecarga Máxima de Encapsulación SD-WAN:
   - Calcule con precisión o calcule de forma conservadora la sobrecarga total introducida por su superposición SD-WAN específica (IPsec, GRE, VXLAN, MPLSoGRE, etc.). Consulte la documentación del proveedor para obtener cifras precisas de los protocolos y las opciones que haya elegido.

Componente	Ejemplo de sobrecarga (bytes)	Notas
MTU física base	1500	Ethernet estándar en enlaces físicos
Menos: Sobrecarga de SD-WAN		
Encabezado IP externo (IPv4)	20	
Encabezado UDP (para NAT-T)	8	Si ESP está encapsulado en UDP
Encabezado ESP	~8-12	
ESP IV (por ejemplo, AES-CBC)	~16	Varía con el algoritmo de cifrado
Autenticación ESP (por ejemplo, SHA256)	~12-16	Varía con el algoritmo de autenticación (por ejemplo, 96 bits para algunos)
Otras superposiciones (GRE, etc.)	Variable	Agregar si forma parte de la pila de encapsulación SD-WAN
Costes generales totales estimados	~68 - Más de 80 bytes	Suma de todos los componentes relevantes para su implementación
MTU de trayecto efectivo	~1432 - 1420 bytes	MTU física base: coste general estimado total

3. Configuración de MTU IP de ISE recomendada:
   - Tome la MTU de Trayectoria Efectiva calculada (por ejemplo, 1420 bytes del ejemplo).
   - Reste un margen de seguridad adicional (por ejemplo, 20-70 bytes) para tener en cuenta encabezados L2 menores no contabilizados o para proporcionar un búfer.
   - Las soluciones como Cisco SD-WAN pueden realizar la detección de MTU de ruta (PMTU) de forma individual para cada túnel de sitio a sitio. Este mecanismo se ejecuta

automáticamente cada 20 minutos para probar y ajustar dinámicamente la MTU IP del túnel según las condiciones de transporte actuales en cada sitio. Como resultado, los valores de MTU pueden diferir entre los sitios y pueden cambiar con el tiempo.
- Una MTU IP generalmente segura y recomendada para las interfaces ISE en tales escenarios está entre 1350 y 1400 bytes

Una MTU IP de 1350 bytes es a menudo un punto de partida muy sólido

Configuración de ISE (ejemplo mediante CLI):

Este comando se ejecuta en la CLI del dispositivo Cisco ISE para cada interfaz de red relevante.

<#root>

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

 ip mtu 1350
!
```

Consideraciones operativas importantes para los cambios de ISE IP MTU:

- Se requiere reinicio del servicio: una vez que se aplica el comando ip mtu a una interfaz ISE, se solicita al usuario que reinicie los servicios de aplicación ISE. Se trata de un cambio que afecta al servicio y debe programarse durante un período de mantenimiento planificado. Consulte la documentación oficial de Cisco ISE para obtener detalles sobre los procedimientos.
- Aplicar a todos los nodos ISE: Este ajuste de MTU de IP debe aplicarse de forma uniforme a todos los nodos ISE de la implementación (PAN principal, PAN secundario y nodos de servicios de políticas [PSN]) que se comunican con los NAD en la SD-WAN. Una configuración de MTU incoherente provoca un comportamiento impredecible.
- Pruebas exhaustivas: Antes de realizar la implementación en producción, pruebe rigurosamente este cambio en una implementación piloto o de laboratorio. Utilice herramientas como ping con tamaños de paquete variables y el conjunto de bits DF para validar la gestión de MTU de extremo a extremo:
    - Sistemas basados en Linux:

```
ping

        -s
```

```
-M do
```

(Nota: -s especifica el tamaño de la carga ICMP. Tamaño total del paquete IP = carga útil + 8 B de Hdr ICMP + 20 B de Hdr IP para IPv4)

- Windows:

```
ping
```

```
-f -l
```

(Nota: -l especifica el tamaño de carga ICMP.)

- Cisco IOS/Cisco IOS-XE®

```
ping
```

```
size
```

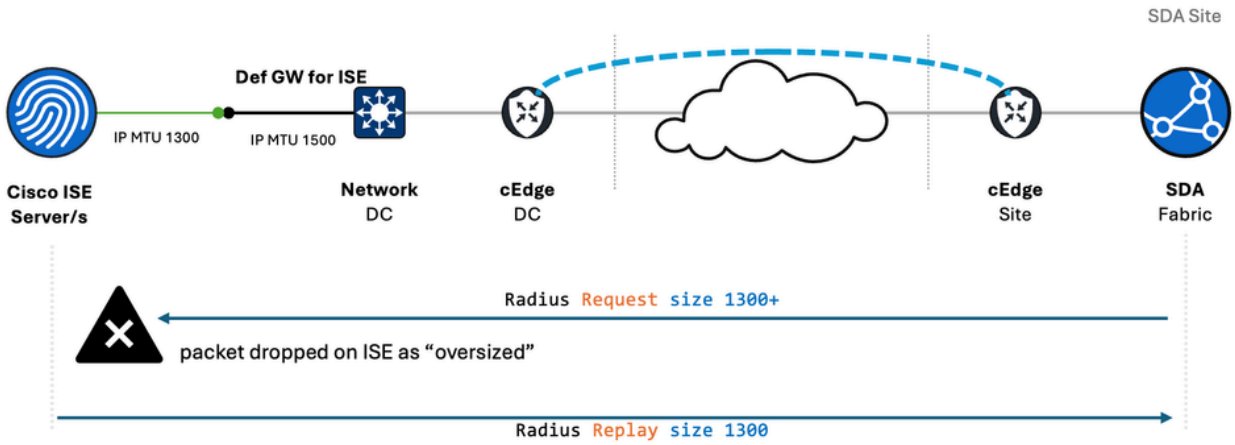
```
df-bit
```

- Primer punto de routing de ISE: al ajustar el valor de MTU de IP en la interfaz de ISE, asegúrese de que el primer punto de routing del Data Center (en concreto, la interfaz de capa 3 asociada a la subred de ISE) también esté configurado con el mismo valor de MTU de IP.
  Esto ayuda a evitar situaciones como la descrita en el Desafío 1, donde una discordancia de MTU hace que ISE trate los paquetes entrantes como sobredimensionados y los descarte.

Por ejemplo, si la interfaz ISE tiene una MTU reducida (por ejemplo, 1300), pero el primer punto de routing permanece configurado con la MTU predeterminada de 1500, los paquetes enviados a ISE que son mayores que 1300 bytes pero menores que 1500 bytes no se fragmentan y ISE los descarta, como se observa en el Desafío 1.
Además, asegúrese de que el primer punto de ruteo sea capaz de realizar la fragmentación si es necesario, y de que hacerlo no resulte en una degradación del rendimiento.

- Actualizar la MTU en toda la ruta de transmisión y en ambas direcciones: al actualizar la configuración de la MTU IP en ISE, es importante tener en cuenta la MTU en toda la ruta de transmisión y en ambas direcciones. Si el valor de MTU configurado en ISE no está alineado con la MTU en la interfaz de capa 3 del gateway de primer salto, pueden surgir problemas similares, como se describe en el Desafío #1.

  Por ejemplo, si la MTU de ISE se reduce a 1300 bytes mientras que la MTU predeterminada de 1500 bytes permanece configurada en el gateway predeterminado, ISE puede descartar paquetes de entre 1300 y 1500 bytes de tamaño, generados normalmente por dispositivos de red, por considerarlos sobredimensionados.



Para evitar este problema, asegúrese siempre de que los cambios de MTU en ISE se reflejen en el gateway de primer salto e, idealmente, en todos los hosts finales dentro del mismo segmento de capa 3. Esto ayuda a mantener la consistencia de MTU de extremo a extremo y evita caídas de paquetes inesperadas.

Conclusión

La alineación de la configuración de MTU de IP en los servidores Cisco ISE con los límites efectivos de MTU de la capa de transporte impuestos por la encapsulación SD-WAN y la alineación de MTU en el límite SDA para la transferencia del router de extremo de Cisco SD-WAN no es solo una recomendación, sino un requisito previo fundamental para garantizar la estabilidad, la fiabilidad y el rendimiento de los servicios AAA en redes empresariales modernas y segmentadas. Aunque Path MTU Discovery es un mecanismo importante, su eficacia práctica puede verse obstaculizada por factores como el filtrado ICMP o la regulación del plano de control en entornos SD-WAN.

Al configurar de forma proactiva una MTU de IP reducida en ISE (por ejemplo, 1350-1400 bytes),

los arquitectos de red y los ingenieros pueden mitigar significativamente el riesgo de caídas de paquetes relacionadas con MTU, lo que se traduce en operaciones de red más predecibles y flexibles. Esto es especialmente importante en las implementaciones de SDA de Cisco, donde ISE organiza la microsegmentación sofisticada y la aplicación de políticas dinámicas, que a menudo se basan en la entrega correcta de mensajes de plano de control potencialmente grandes. Una planificación diligente, unas pruebas exhaustivas y una configuración uniforme en todos los nodos de ISE son fundamentales para lograr una implementación correcta y sin problemas.

Estándares y referencias

Para obtener información más detallada, consulte los estándares oficiales y la documentación de Cisco:

RFC:

- RFC 1191: Descubrimiento de la MTU del trayecto
- RFC 791: Protocolo Internet (IP): define el encabezado IP, incluido el bit Do Not Fragment (DF).
- RFC 8200: Especificación de IPv6 (relevante si se utiliza IPv6, incluye conceptos similares de PMTUD).
- RFC 4459: Problemas de MTU y fragmentación con tunelación en la red (VPN): aborda directamente los problemas comunes de MTU en entornos VPN.

Documentación de Cisco:

- Guías de diseño e implementación de SDA de Cisco: Para obtener información sobre las recomendaciones de MTU de fabric y las configuraciones de nodos de borde.
- Guías de diseño y configuración de la SD-WAN de Cisco: Para obtener detalles sobre la sobrecarga de encapsulación, la MTU de interfaz de túnel y las consideraciones de PMTUD dentro del fabric SD-WAN.
- Guías de configuración de switches Catalyst de Cisco serie 9000: Para obtener detalles específicos de la plataforma sobre la configuración de MTU y las capacidades de fragmentación.
- Guías de administración y CLI de Cisco Identity Services Engine (ISE): Para obtener información sobre la configuración de la interfaz, incluido el comando ip mtu y las implicaciones de reinicio del servicio.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).