Configurar a MTU IP do ISE ideal em SD-WAN para implantações de SDA

Contents

Introdução

Este documento descreve como os problemas da Unidade Máxima de Transmissão (MTU - Maximum Transmission Unit) podem afetar a microssegmentação no SDA quando a SD-WAN é usada para conectar sites SDA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso definido por software (SDA) da Cisco
- Redes de longa distância definidas por software da Cisco (SD-WAN)
- Cisco Identity Services Engine (ISE)

Componentes Utilizados:

As informações neste documento são baseadas em SDA, SDWAN e ISE.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As redes empresariais modernas utilizam cada vez mais o SDA para microssegmentação granular e aplicação consistente de políticas. Para conectar locais SDA distribuídos, o Cisco SD-WAN é frequentemente empregado, oferecendo transporte ágil, seguro e otimizado através de várias redes subjacentes. Central a essa arquitetura, o ISE fornece serviços críticos de Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization, and Accounting), juntamente com a distribuição dinâmica de políticas (por exemplo, Tags de grupos de segurança (SGTs - Security Group Tags) e ACLs para download).

Embora robusta, a integração dessas tecnologias poderosas pode apresentar desafios de configuração sutis, porém impactantes. O tratamento de MTU em pontos críticos de handoff da rede e através da sobreposição de SD-WAN é uma área primordial para tais problemas. Este artigo aborda dois cenários comuns de incompatibilidade de MTU que podem interromper as operações de rede:

1. O intervalo de MTU entre os nós de borda SDA e os dispositivos de borda SD-WAN.
2. Restrições de MTU para o tráfego originado pelo ISE que atravessa a sobreposição de SD-WAN.

O alinhamento adequado de MTU é fundamental para evitar problemas de fragmentação de pacotes ou quedas silenciosas, garantindo autenticação confiável, aplicação de políticas e estabilidade geral da rede. A falha em tratá-los pode causar perturbações intermitentes na conectividade e falhas na aplicação de políticas, consumindo um esforço significativo de solução de problemas.

Sintomas comuns de MTU desalinhado

MTU desalinhado pode se manifestar de várias maneiras, geralmente levando a problemas difíceis de diagnosticar:

- Falhas intermitentes de autenticação RADIUS ou timeouts: Especialmente perceptível para políticas que geram pacotes RADIUS maiores (por exemplo, aqueles com extensos pares AV ou certificados).
- Endpoints que falham ao receber ou aplicar ACLs para download (dACLs) ou políticas TrustSec (SGTs/SGACLs): Essas políticas são frequentemente transmitidas em pacotes RADIUS grandes.
- Estabelecimento lento de sessão para clientes autenticados: Devido a retransmissões na camada de aplicação.
- Retransmissões RADIUS excessivas: Observável em registros ISE ou nos dispositivos de acesso à rede (NADs).

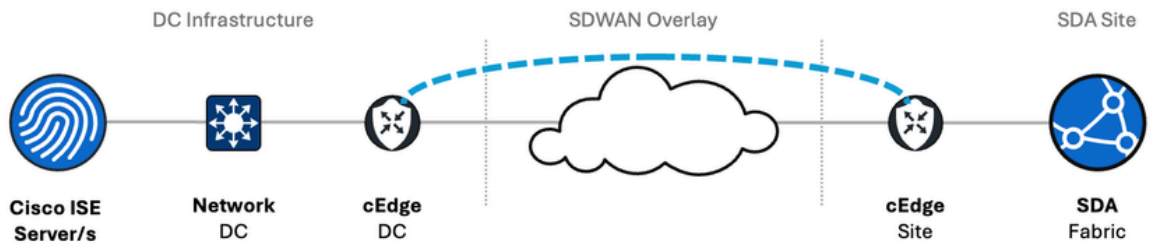
- Propagação de política inconsistente: As alterações de política feitas no ISE podem não se propagar consistentemente para todos os NADs em sites SDA remotos.
- Discrepâncias de captura de pacotes: As capturas podem mostrar o ISE enviando pacotes grandes (por exemplo, >1450 bytes) com o bit Do Not Fragment (DF) definido, mas nenhuma resposta correspondente ou erro ICMP "Fragmentation Needed" do roteador de borda da Cisco NAD ou SD-WAN.
- Incrementando contadores de queda de pacote: Observado na interface de ingresso do Roteador Cisco Edge do Data Center (DC) para tráfego originado no ISE destinado a sites SDA, ou na interface do Roteador Cisco Edge da SD-WAN voltada para a borda do SDA para tráfego no sentido inverso.

Descrição do problema

Uma implantação empresarial típica
Considere uma topologia corporativa comum:

- Servidores Cisco ISE: Implantado em um data center (DC) centralizado ou em hubs regionais, conectado à infraestrutura de rede do DC.
- Infraestrutura de DC: Compreende switches de agregação ou de núcleo de DC aos quais os servidores ISE se conectam.
- Sobreposição de SD-WAN: Os roteadores DC Cisco Edge Router estabelecem túneis SD-WAN (geralmente IPsec) sobre uma rede de transporte subjacente (por exemplo, Internet, MPLS) para os roteadores Cisco Edge Router em locais SDA remotos.
- Site do SDA: Os roteadores Cisco Edge Router de local remoto conectam-se à estrutura SDA local, que inclui nós de borda de estrutura, nós de borda, controladores de LAN sem fio (WLCs) e, por fim, os endpoints.

Topologia ilustrativa



Desafio 1: A lacuna de MTU - fronteiras SDA para bordas SD-WAN

Os princípios de projeto do Cisco SDA, frequentemente implementados via LAN Automation, promovem um MTU em todo o campus de 9100 bytes (quadros jumbo) em todos os dispositivos de estrutura. Isso inclui os nós de borda da série Catalyst 9000 e garante que os quadros jumbo Ethernet sejam transportados eficientemente dentro da estrutura. Consequentemente, a interface de handoff de Camada 3 ou SVI em um nó de borda SDA assume como padrão esse MTU maior.

Por outro lado, os dispositivos de borda SD-WAN, como a série Catalyst 8000, normalmente usam como padrão um MTU de interface de 1500 bytes. Esse é o padrão para interfaces que se conectam a redes externas, como provedores de serviços de Internet (ISPs), onde o suporte a quadros jumbo é incomum ou não está habilitado.

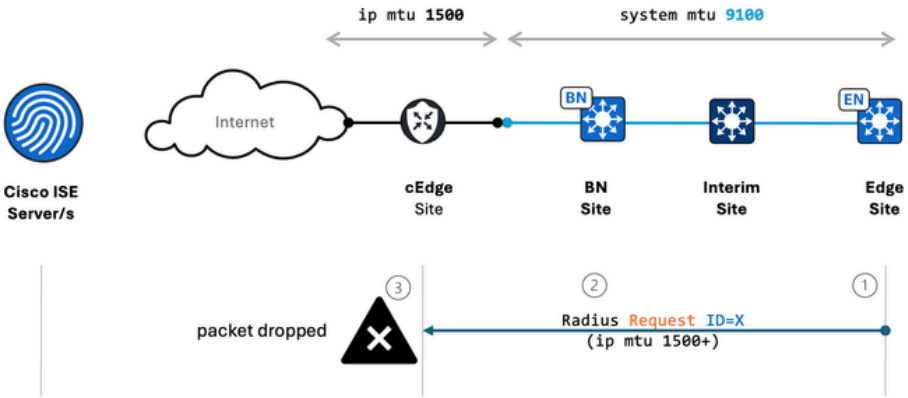
Essa disparidade cria um ponto imediato de falha potencial: uma borda SDA tentando enviar um pacote IP com mais de 1500 bytes para uma borda SD-WAN cuja interface de recebimento está configurada para uma MTU de 1500 bytes.

Esse tipo de incompatibilidade de MTU é uma armadilha comum em implantações de SDA e é frequentemente fácil de ignorar durante a configuração. O que o torna mais desafiador é que certos comportamentos relacionados à forma como as solicitações RADIUS são geradas nos switches Catalyst 9000 que executam o Cisco IOS-XE® podem fazer com que esses problemas surjam somente sob condições específicas e críticas.

Por exemplo, as solicitações RADIUS geradas durante o processo de autenticação do usuário final tratado pelo processo Session Manager Daemon (SMD) são codificadas para fragmentar pacotes a 1396 bytes. Por outro lado, as solicitações RADIUS envolvidas na recuperação de políticas TrustSec, como as Security Group Access Control List (SGACL)s, são geradas pelos subcomponentes do daemon do Cisco Internetworking Operating System (IOSd). Eles são sensíveis à MTU e podem evitar a fragmentação de pacotes, a menos que seu tamanho exceda a MTU do sistema (normalmente até 9100 bytes).

Como resultado, problemas relacionados a incompatibilidades de MTU só se tornam aparentes quando as políticas de download do Cisco TrustSec (CTS) estão em uso. Além disso, o conjunto de Role-Based Access Control List (RBACL)s baixado por um dispositivo de borda SDA durante a autenticação do usuário pode variar dependendo de quais políticas SGACL já estão presentes para outras tags. Na prática, o switch baixa apenas as partes não sobrepostas dos conjuntos de políticas.

Juntos, esses comportamentos podem produzir resultados imprevisíveis e inconsistentes, variando de falhas silenciosas a downloads incompletos de políticas, dependendo do tamanho da política SGACL, das condições atuais do sistema e, por fim, dos desalinhamentos de MTU ao longo do caminho.



A borda SDA encaminha um pacote RADIUS grande (por exemplo, 1600 bytes) em direção ao ISE através da borda SD-WAN. Isso é o que ocorre:

1. A borda SDA, com sua interface MTU 9100, envia o pacote IP de 1600 bytes.
2. O Roteador Cisco Edge SD-WAN recebe esse pacote em sua interface MTU 1500.
3. No entanto, se o bit Do Not Fragment (DF) não estiver definido nesses pacotes RADIUS, o Roteador Cisco Edge SD-WAN pode frequentemente descartá-los no ingresso simplesmente porque eles são "superdimensionados" em relação à sua interface MTU configurada. Ele não chega ao estágio da lógica de encaminhamento IP em que pode considerar a fragmentação deles (se o bit DF permitir).

Essa queda silenciosa leva a problemas de cabeça significativos, especialmente porque o problema é direcional (SDA para SD-WAN/ISE).

Uma incompatibilidade de MTU semelhante pode ocorrer no núcleo do data center (DC) ou nos switches leaf, que são normalmente configurados para suportar quadros jumbo (por exemplo, MTU 9000+) para melhorar a eficiência do tráfego de DC interno. No entanto, se o tráfego for transferido para a interface de LAN de um roteador de borda DC SD-WAN configurado com um MTU padrão (por exemplo, 1500 bytes), essa incompatibilidade pode levar à fragmentação ou quedas de pacotes, particularmente para o tráfego que flui da rede DC para a estrutura SD-WAN.

Solução para o desafio 1:

Alinhe o IP MTU na interface de handoff da borda SDA (física ou SVI) com a interface do roteador de borda da Cisco de SD-WAN de troca de tráfego (peering), normalmente 1500 bytes.

Exemplo de configuração (no nó de borda 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
!
```

Consideração importante: Fragmentação nas fronteiras do Catalyst 9000

Os switches Catalyst 9000 Series, como nós de borda SDA, suportam fragmentação IP para pacotes IP nativos no plano de dados do hardware. A redução do ip mtu na interface de handoff para 1500 não causa degradação de desempenho devido à fragmentação baseada em software para o tráfego que se origina ou que transita pela borda que precisa dele. O switch fragmenta eficientemente pacotes IP maiores que 1500 bytes (se o bit DF estiver limpo) antes de sair dessa interface específica, sem apontar para a CPU.

No entanto, é importante observar que os switches Catalyst 9000 geralmente não suportam a fragmentação do tráfego encapsulado de VXLAN. Essa limitação é crucial para tráfego de sobreposição, mas não afeta o cenário de autenticação RADIUS descrito, pois a comunicação RADIUS entre a borda SDA e um ISE externo geralmente ocorre dentro da base (roteamento de IP nativo). (As considerações de MTU para sobreposições de VXLAN são um tópico separado e complexo, detalhado nos guias de design relevantes do Cisco SDA).

O alinhamento pró-ativo de MTU na borda do SDA para a entrega do roteador de borda da Cisco SD-WAN é essencial.

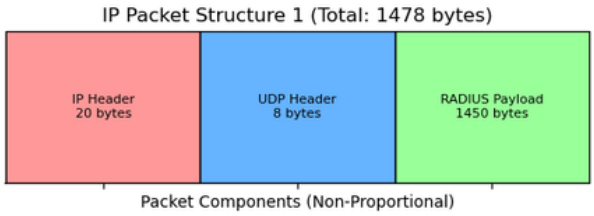
Desafio 2: O compactação de MTU - tráfego ISE na sobreposição de SD-WAN

Mesmo que as interfaces físicas individuais, como as placas de interface de rede (NICs) do ISE, as portas do switch ou as interfaces do roteador sejam definidas para um MTU IP padrão de 1.500 bytes, a própria sobreposição de SD-WAN introduz a sobrecarga de encapsulamento. Essa sobrecarga consome uma parte do limite de 1.500 bytes, reduzindo o MTU efetivo disponível para o pacote IP original (o "payload" da perspectiva do ISE).

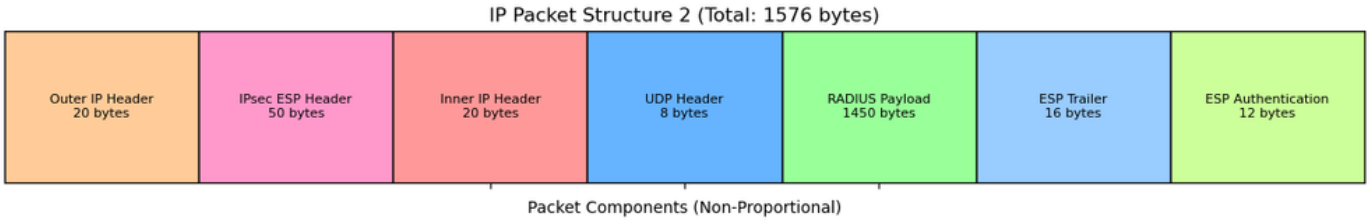
Sobrecarga de encapsulamento e estrutura de pacote:

Quando um pacote IP de um servidor ISE (por exemplo, um pacote RADIUS Access-Accept) é enviado a um dispositivo de acesso à rede (NAD) em um local SDA, ele atravessa a sobreposição de SD-WAN e é encapsulado. Uma pilha de encapsulamento comum envolve IPsec no modo de túnel, potencialmente sobre UDP para NAT traversal (NAT-T).

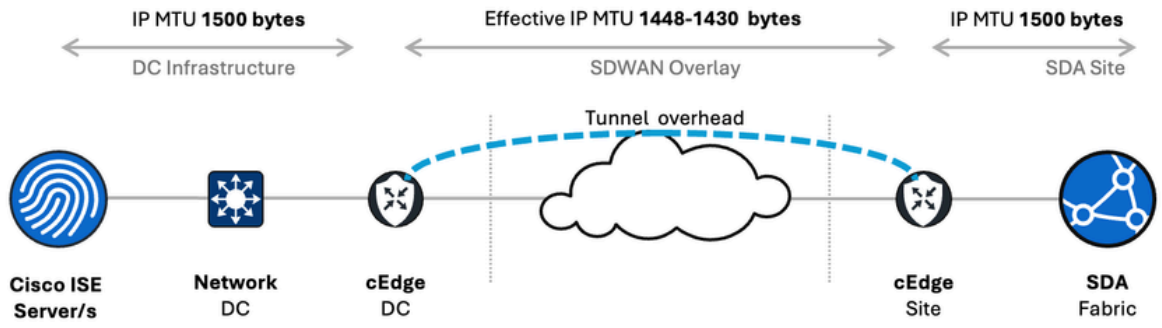
- Pacote original do ISE (pacote interno):
  Por exemplo, um pacote RADIUS com payload de 1.450 bytes + 8B UDP + 20B IP interno = 1.478 bytes.



- Considere o ESP IPsec em modo de túnel, possivelmente com encapsulamento UDP para NAT-T:



- A sobrecarga total pode variar com base nas cifras IPsec específicas, nos mecanismos de autenticação e em outros recursos de sobreposição (como GRE, se usado). Um cálculo típico:
    - Cabeçalho IP Externo (IPv4): 20 bytes
    - Cabeçalho UDP (se ESP sobre UDP para NAT-T): 8 bytes
    - Cabeçalho ESP ~8 bytes
    - ESP IV (por exemplo, para AES-CBC): ~16 bytes (se aplicável)
    - Autenticação ESP (por exemplo, HMAC-SHA256 truncado): ~12-16 bytes
    - Sobrecarga estimada comum de IPsec: ~52-70 bytes (pode ser maior, até ~80 bytes ou mais com todas as opções).

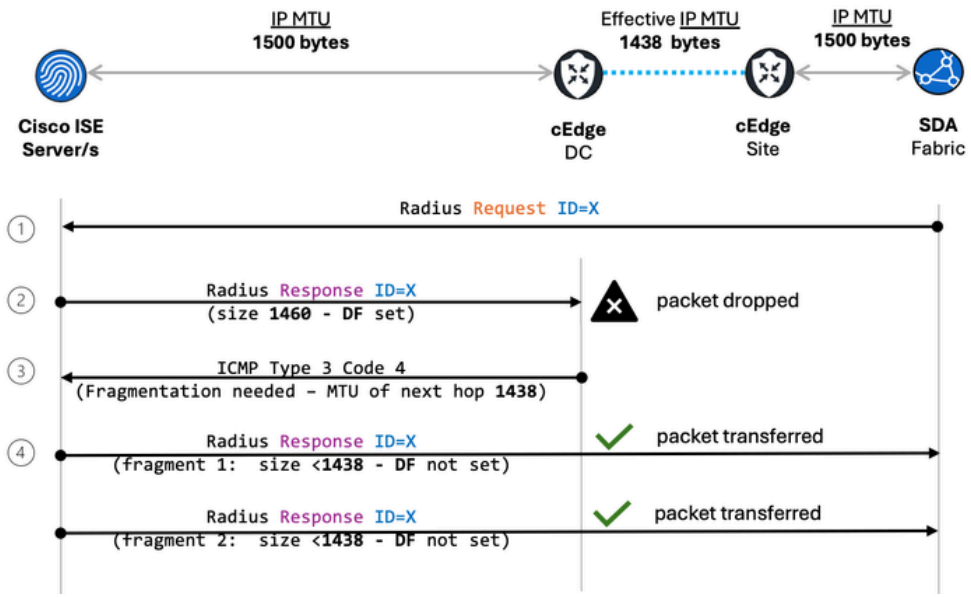


Se o MTU do link físico for de 1500 bytes, o MTU do payload disponível para o pacote IP original do ISE será: 1500 bytes - carga adicional de SD-WAN.
Por exemplo, 1500 - 70 = 1430 bytes.

Comportamento quando os pacotes excedem o MTU efetivo:

1. O ISE origina um pacote (a anomalia de bit DF):
    - Por padrão, o sistema operacional Linux subjacente de um dispositivo ISE define oNão Fragmentar (DF) no cabeçalho IP para todos os pacotes que ele origina que são menores ou iguais a sua interface IP MTU configurada (por exemplo, 1500 bytes).
    - Finalidade deste bit DF:o ISE (através de seu SO) define proativamente o bit DF principalmente para aproveitar o processo Path MTU Discovery (PMTUD), que é descrito mais adiante. Isso permite que o ISE aprenda dinamicamente o PMTU real para um destino se ele for menor que o MTU de sua própria interface.
    - Comportamento para Pacotes Maiores que o MTU da Interface:Se o ISE precisar enviar um pacote IP maior que o MTU IP da interface configurada, o comportamento dependerá do sistema operacional Linux. Normalmente, o OS pode fragmentar o pacote antes da transmissão e limpar o bit DF (definindo DF=0) nesses fragmentos resultantes. Essa fragmentação é uma função no nível do SO, não diretamente acionada pelo próprio código do aplicativo ISE.
    - Principal distinção dos dispositivos de rede:esse comportamento padrão do ISE (definindo DF=1 mesmo para pacotes não fragmentados que se encaixam em sua interface MTU) é significativamente diferente de muitos dispositivos de rede tradicionais (roteadores, switches). Os dispositivos de rede geralmente não definem o bit DF nos pacotes que originam ou encaminham, a menos que explicitamente configurados para fazê-lo, ou se o pacote que está sendo encaminhado já tem o bit DF definido, ou para protocolos específicos que exigem isso. Normalmente, eles permitem a fragmentação por padrão se um pacote exceder o MTU do próximo salto (e DF=0).
    - Complexidade de Troubleshooting:Essa assimetria, em que o tráfego ISE para NAD geralmente tem DF=1 por padrão, enquanto o tráfego NAD para ISE pode ter DF=0 (a menos que o NAD o defina por um motivo), pode introduzir uma camada adicional de complexidade durante o troubleshooting. Os engenheiros podem observar diferentes comportamentos de fragmentação e interações PMTUD, dependendo da direção do fluxo de tráfego.
2. O pacote alcança o Cisco Edge Router (DC) de entrada:o roteador DC Cisco Edge Router recebe o pacote IP do ISE.
3. Encapsulamento e verificação de MTU pelo Cisco Edge Router:o Cisco Edge Router tenta encapsular o pacote para o túnel SD-WAN.
    - Se o tamanho do pacote original mais a sobrecarga de encapsulamento SD-WAN exceder o MTU da interface física de saída do Cisco Edge Router (por exemplo, 1500 bytes), E o bit DF estiver definido no pacote original (interno) do ISE, o Cisco Edge Router não deve fragmentar o pacote interno.
    - O Cisco Edge Router deve descartar o pacote.
    - Criticamente, o Cisco Edge Router também deve enviar uma mensagem ICMP "Destination Unreachable - Fragmentation Needed and DF bit set" (Type 3, Code 4) de volta à origem (ISE), indicando a MTU do próximo salto (a MTU efetiva do túnel).
4. Processo de Path MTU Discovery (PMTUD): Ao receber essa mensagem ICMP "Fragmentation Needed", o ISE (o SO de origem) deve reduzir sua estimativa de PMTU para esse caminho de destino específico. Ele armazenaria em cache essas informações e reenviaria os dados em pacotes menores que se encaixassem no PMTU recém-descoberto.

Diagrama do processo PMTUD:



Onde a comunicação PMTUD for interrompida:
O PMTUD é robusto em teoria, mas pode falhar na prática:

- Filtragem ICMP: Firewalls intermediários ou políticas de segurança geralmente bloqueiam mensagens ICMP, evitando que a mensagem "Fragmentação necessária" atinja o ISE.
- Política de plano de controle (CoPP) no Cisco Edge Router: Os roteadores Cisco Edge Router usam CoPP para proteger a CPU. A geração de mensagens de erro ICMP é uma tarefa do plano de controle. Sob carga pesada ou com muitos pacotes grandes demais, o CoPP pode limitar a taxa ou descartar a geração de ICMP. O ISE nunca recebe o feedback.
- Quedas silenciosas: Se o ISE não receber a mensagem ICMP "Fragmentation Needed" (Fragmentação necessária), ele não saberá da restrição do caminho. Ele continua a enviar pacotes grandes com o bit DF definido, fazendo com que eles sejam descartados silenciosamente pelo Cisco Edge Router de entrada. Isso resulta em tempos limite e retransmissões da camada de aplicação (por exemplo, RADIUS).
- Impacto nos serviços do ISE: Pacotes RADIUS Access-Accept grandes (transportando dACLs, AVPs extensivos, informações de SGT) são particularmente susceptíveis. As manifestações incluem:
    - Falhas de autenticação intermitentes ou completas.
    - Os endpoints não estão recebendo as políticas de acesso à rede ou SGTs corretos.
    - Sincronização de política incompleta ou com falha entre ISE e NADs.

Solução para o desafio 2: Configuração proativa de MTU IP do ISE

Devido à falta de confiabilidade da PMTUD, uma abordagem proativa é melhor para serviços críticos como o ISE. Configure o IP MTU nas interfaces de rede do ISE para um valor que acomode com segurança a sobrecarga de SD-WAN máxima esperada. Isso garante que o ISE não origine pacotes IP (com o bit DF definido) que são inerentemente grandes demais para atravessar a sobreposição de SD-WAN sem precisar de fragmentação por um dispositivo intermediário (que é proibido se DF=1).

Calculando e configurando o MTU IP recomendado do ISE:

1. Estabelecer MTU Físico Básico: Normalmente, são 1500 bytes para interfaces Ethernet padrão ao longo do caminho.
2. Determine a sobrecarga máxima de encapsulamento de SD-WAN:
    - Calcule com precisão ou estime de forma conservadora a sobrecarga total introduzida por sua sobreposição de SD-WAN específica (IPsec, GRE, VXLAN, MPLSoGRE e assim por diante). Consulte a documentação do fornecedor para obter números precisos sobre os protocolos e as opções escolhidas.

Componente	Exemplo de carga adicional (bytes)	Notas
MTU Físico Base	1500	Ethernet padrão em links físicos
Menos: Carga adicional de SD-WAN		
Cabeçalho IP externo (IPv4)	20	
Cabeçalho UDP (para NAT-T)	8	Se o ESP for encapsulado em UDP
Cabeçalho ESP	~8-12	
ESP IV (por exemplo, AES-CBC)	~16	Varia com o algoritmo de criptografia
ESP Auth (por exemplo, SHA256)	~12-16	Varia com o algoritmo de autenticação (por exemplo, 96 bits para alguns)
Outras Sobreposições (GRE e assim por diante)	Variável	Adicione se for parte da sua pilha de encapsulamento SD-WAN
Custo total estimado	~68 a mais de 80 bytes	Soma de todos os componentes relevantes para sua implantação
MTU de Caminho Efetivo	~1432 a 1420 bytes	MTU Físico Base - Total de Sobrecarga Estimada

3. Configuração recomendada de MTU IP do ISE:
    - Tome o MTU de caminho efetivo calculado (por exemplo, 1420 bytes do exemplo).
    - Subtraia uma margem de segurança adicional (por exemplo, 20-70 bytes) para considerar cabeçalhos L2 secundários não lançados ou para fornecer um buffer.
    - Soluções como Cisco SD-WAN podem executar a descoberta de MTU de caminho (PMTU) individualmente para cada túnel de site para site. Esse mecanismo é executado automaticamente a cada 20 minutos para testar e ajustar dinamicamente o MTU IP do túnel de acordo com as condições de transporte atuais em cada local. Como resultado, os valores de MTU podem diferir entre os locais e podem mudar com o tempo.
    - Um MTU IP geralmente seguro e recomendado para interfaces ISE nesses cenários é entre 1350 e 1400 bytes

Um IP MTU de 1350 bytes é geralmente um ponto de partida muito robusto

Configuração do ISE (exemplo via CLI):

Esse comando é executado na CLI do dispositivo Cisco ISE para cada interface de rede relevante.

<#root>

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

 ip mtu 1350

!
```

Considerações operacionais importantes para alterações de MTU IP do ISE:

- Reinicialização do serviço necessária: quando o comando ip mtu é aplicado a uma interface do ISE, isso solicita que o usuário reinicie os serviços do aplicativo ISE. Esta é uma alteração que afeta o serviço e deve ser agendada durante uma janela de manutenção planejada. Consulte a documentação oficial do Cisco ISE para obter detalhes dos procedimentos.
- Aplicar a todos os nós do ISE: Esse ajuste de MTU de IP deve ser aplicado consistentemente a todos os nós do ISE na implantação (PAN primário, PAN secundário, nós de serviço de política (PSNs)) que se comunicam com NADs através da SD-WAN. Configurações de MTU inconsistentes levam a um comportamento imprevisível.
- Teste completo: Antes de implementar na produção, teste rigorosamente essa alteração em uma implantação de laboratório ou piloto. Use ferramentas como ping, com tamanhos de pacotes variáveis e o conjunto de bits DF para validar o tratamento de MTU fim-a-fim:
    - Sistemas baseados em Linux:

```
ping

        -s

         -M do
```

(Nota: -s especifica o tamanho do payload ICMP. Tamanho total do pacote IP = payload + 8B ICMP Hdr + 20B IP Hdr para IPv4)

- Windows:

```
ping

        -f -l
```

(Nota: -l especifica o tamanho do payload ICMP.)

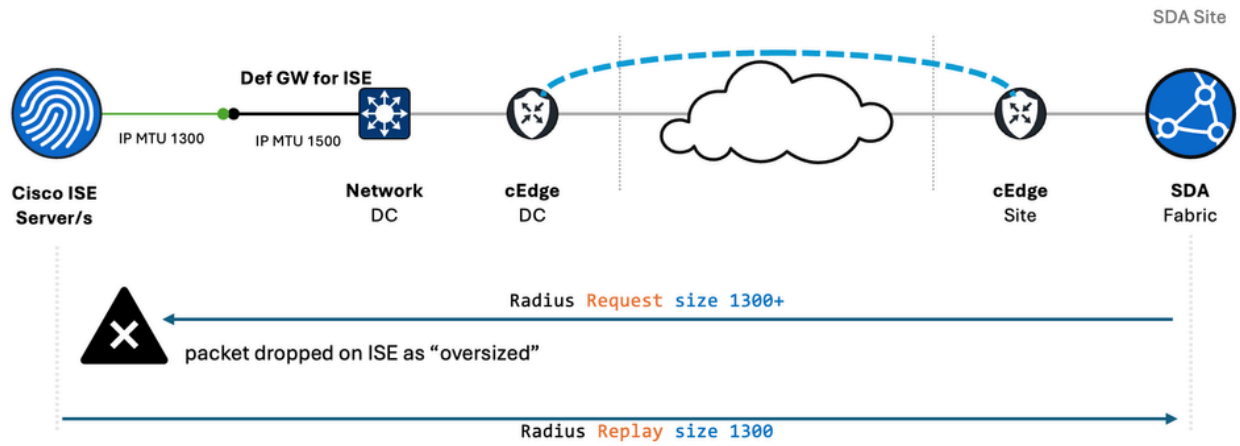
- Cisco IOS/Cisco IOS-XE®

```
ping

        size

         df-bit
```

- Primeiro ponto de roteamento do ISE - Ao ajustar o valor de MTU de IP na interface do ISE, certifique-se de que o primeiro ponto de roteamento no data center, especificamente a interface de Camada 3 associada à sub-rede do ISE, também esteja configurado com o mesmo valor de MTU de IP.
  Isso ajuda a evitar situações como a descrita no Desafio 1, em que uma incompatibilidade de MTU faz com que o ISE trate os pacotes recebidos como grandes demais e os descarte. Por exemplo, se a interface do ISE tiver uma MTU reduzida (por exemplo, 1300), mas o primeiro ponto de roteamento permanecer configurado com a MTU padrão de 1500, os pacotes enviados ao ISE que forem maiores que 1300 bytes, mas menores que 1500 bytes, não serão fragmentados e serão descartados pelo ISE — como observado no Desafio 1. Além disso, certifique-se de que o primeiro ponto de roteamento seja capaz de executar a fragmentação, se necessário, e que isso não resulte em degradação do desempenho.
- Atualizar MTU em todo o caminho de transmissão e em ambas as direções - Ao atualizar as

configurações de MTU IP no ISE, é importante considerar a MTU em todo o caminho de transmissão e em ambas as direções. Se o valor de MTU configurado no ISE não estiver alinhado com o MTU na interface de Camada 3 do gateway do primeiro salto, podem surgir problemas semelhantes, conforme descrito na #1 de desafio.

Por exemplo, se o MTU do ISE for reduzido para 1300 bytes enquanto o MTU padrão de 1500 bytes permanecer configurado no gateway padrão, os pacotes entre 1300 e 1500 bytes de tamanho, geralmente gerados pelos dispositivos de rede, podem ser descartados pelo ISE como grandes demais.



Para evitar esse problema, certifique-se sempre de que as alterações de MTU no ISE sejam espelhadas no gateway do primeiro salto e, idealmente, refletidas em todos os hosts finais dentro do mesmo segmento de Camada 3. Isso ajuda a manter a consistência de MTU de ponta a ponta e evita quedas inesperadas de pacotes.

Conclusão

O alinhamento das configurações de MTU IP nos servidores Cisco ISE com os limites de MTU da camada de transporte efetivos impostos pelo encapsulamento SD-WAN e o alinhamento de MTU na borda SDA para a transferência do Cisco Edge Router SD-WAN não é apenas uma recomendação, mas um pré-requisito crítico para garantir a estabilidade, confiabilidade e desempenho dos serviços AAA em redes empresariais modernas e segmentadas. Embora a Path MTU Discovery seja um mecanismo importante, sua eficácia prática pode ser prejudicada por fatores como filtragem ICMP ou Política de plano de controle em ambientes SD-WAN.

Ao configurar proativamente um MTU IP reduzido no ISE (por exemplo, 1350-1400 bytes), os arquitetos e engenheiros de rede podem reduzir significativamente o risco de quedas de pacotes relacionados ao MTU, levando a operações de rede mais previsíveis e resilientes. Isso é particularmente vital nas implantações do Cisco SDA, onde o ISE orquestra a microssegmentação sofisticada e a aplicação dinâmica de políticas, que frequentemente dependem da entrega bem-sucedida de mensagens de plano de controle potencialmente grandes. Planejamento diligente, testes abrangentes e configuração consistente em todos os nós do ISE são essenciais para uma implantação bem-sucedida e sem problemas.

Padrões e Referências

Para uma compreensão mais profunda, consulte os padrões oficiais e a documentação da Cisco:

RFCs:

- RFC 1191: Descoberta da MTU do caminho
- RFC 791: Internet Protocol (IP) - Define o cabeçalho IP, incluindo o bit Do Not Fragment (DF).
- RFC 8200: Especificação IPv6 (relevante se o IPv6 for usado, inclui conceitos PMTUD semelhantes).
- RFC 4459: Problemas de MTU e de Fragmentação com In-the-Network Tunneling (VPNs) - Aborda diretamente problemas comuns de MTU em ambientes VPN.

Documentação da Cisco:

- Guias de design e implantação do Cisco SDA: Para obter informações sobre recomendações de MTU de estrutura e configurações de nó de borda.
- Guias de design e configuração da Cisco SD-WAN: Para obter detalhes sobre a sobrecarga de encapsulamento, a interface de túnel MTU e as considerações de PMTUD na estrutura SD-WAN.
- Guias de configuração do switch Cisco Catalyst 9000 Series: Para obter detalhes específicos da plataforma sobre configurações de MTU e recursos de fragmentação.
- Guias do administrador e da CLI do Cisco Identity Services Engine (ISE): Para obter informações sobre a configuração da interface, incluindo o comando ip mtu e as implicações da reinicialização do serviço.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.