Optimale ISE IP MTU configureren in SD-WAN voor SDA-implementaties

Inhoud

Inleiding

Dit document beschrijft hoe problemen met de Maximum Transmission Unit (MTU) micro-segmentatie in SDA kunnen beïnvloeden wanneer SD-WAN wordt gebruikt om SDA-sites te verbinden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten:

De informatie in dit document is gebaseerd op SDA, SDWAN en ISE.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Moderne bedrijfsnetwerken maken steeds meer gebruik van SDA voor gedetailleerde microsegmentatie en consistente beleidshandhaving. Om gedistribueerde SDA-sites te verbinden, wordt vaak Cisco SD-WAN gebruikt, dat flexibel, veilig en geoptimaliseerd transport biedt over verschillende onderliggende netwerken. Centraal in deze architectuur biedt de ISE kritische authenticatie-, autorisatie- en boekhouddiensten (AAA), samen met dynamische beleidsdistributie (bijvoorbeeld Security Group Tags (SGT's) en downloadbare ACL's).

Hoewel robuust, kan de integratie van deze krachtige technologieën subtiele maar impactvolle configuratie-uitdagingen introduceren. De MTU-afhandeling op kritieke netwerkoverdrachtspunten en over de SD-WAN-overlay is een uitstekend gebied voor dergelijke problemen. Dit artikel behandelt twee veelvoorkomende MTU-mismatchscenario's die netwerkactiviteiten kunnen verstoren:

1. De MTU-kloof tussen SDA-grensknooppunten en SD-WAN-randapparaten.
2. MTU-beperkingen voor ISE-verkeer dat de SD-WAN-overlay doorkruist.

Een goede MTU-uitlijning is van het grootste belang om problemen met de fragmentatie van pakketten of stille druppels te voorkomen, waardoor betrouwbare authenticatie, beleidshandhaving en algehele netwerkstabiliteit worden gewaarborgd. Als deze problemen niet worden aangepakt, kan dit leiden tot verwarrende onderbrekingen in de connectiviteit en fouten in de handhaving van het beleid, waardoor aanzienlijke inspanningen nodig zijn om problemen op te lossen.

Veel voorkomende symptomen van verkeerd uitgelijnde MTU

Misaligned MTU kan zich op verschillende manieren manifesteren, wat vaak leidt tot moeilijk te diagnosticeren problemen:

- Intermitterende RADIUS-verificatiefouten of time-outs: Vooral merkbaar voor beleid dat grotere RADIUS-pakketten genereert (bijvoorbeeld die met uitgebreide AV-paren of certificaten).
- Eindpunten die geen downloadbare ACL's (dACL's) of TrustSec-beleidsregels (SGT's/SGACL's) ontvangen of toepassen: Deze beleidsregels worden vaak in grote RADIUS-pakketten weergegeven.
- Trage sessie-instelling voor geverifieerde clients: vanwege hertransmissies op de toepassingslaag.
- Overmatige RADIUS-hertransmissies: Waarneembaar in ISE-logs of op de Network Access Devices (NAD's).
- Inconsistente beleidspropagatie: Beleidswijzigingen die in ISE zijn aangebracht, worden

mogelijk niet consistent doorgegeven aan alle NAD's op externe SDA-sites.

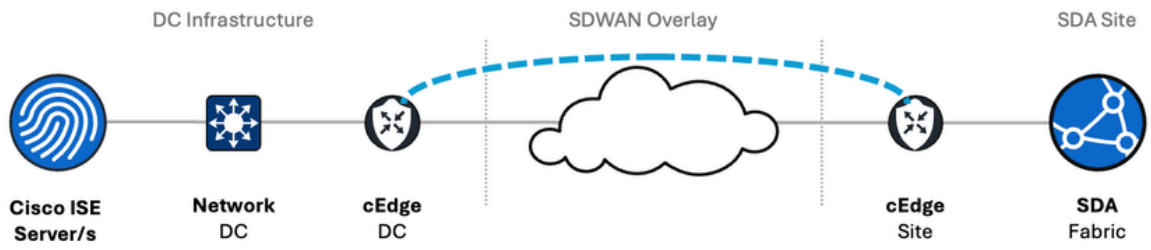
- Discrepanties in pakketopname: Opnames kunnen laten zien dat ISE grote pakketten verzendt (bijvoorbeeld >1450 bytes) met de Do Not Fragment (DF)-bitset, maar geen overeenkomstige reactie of ICMP "Fragmentation Needed"-fout van de NAD- of SD-WAN Cisco Edge Router.
- Vergroten van pakketvaltellers: waargenomen op de ingangsinterface van de Cisco Edge Router van het datacenter (DC) voor verkeer afkomstig van ISE bestemd voor SDA-sites, of op de SD-WAN Cisco Edge Router-interface gericht op de SDA-grens voor verkeer in de omgekeerde richting.

Probleembeschrijving

Een typische bedrijfsimplementatie
Overweeg een gemeenschappelijke bedrijfstopologie:

- Cisco ISE-servers: geïmplementeerd in een gecentraliseerd datacenter (DC) of regionale hubs die zijn aangesloten op de DC-netwerkinfrastructuur.
- DC-infrastructuur: omvat DC-kern- of aggregatie-switches waarmee ISE-servers verbinding maken.
- SD-WAN Overlay: DC Cisco Edge Router routers vestigen SD-WAN tunnels (meestal IPsec) over een onderliggend transportnetwerk (bijvoorbeeld internet, MPLS) naar Cisco Edge Router routers op externe SDA-sites.
- SDA-site: externe Cisco Edge-routers maken verbinding met de lokale SDA-structuur, waaronder fabric edge nodes, border nodes, draadloze LAN-controllers (WLC's) en uiteindelijk de eindpunten.

Illustratieve topologie



Uitdaging 1: De MTU-kloof – SDA-grenzen naar SD-WAN-randen

Cisco SDA-ontwerpprincipes, vaak geïmplementeerd via LAN Automation, bevorderen een campusbrede MTU van 9100 bytes (jumboframes) op alle fabric-apparaten. Dit omvat Catalyst 9000-reeks border nodes en zorgt ervoor dat Ethernet-jumbo frames efficiënt worden getransporteerd binnen de fabric. Bijgevolg is de Layer 3- of SVI-handoff-interface op een SDA-randknooppunt standaard gekoppeld aan deze grotere MTU.

Omgekeerd, SD-WAN edge apparaten, zoals de Catalyst 8000-serie, meestal standaard naar een interface MTU van 1500 bytes. Dit is standaard voor interfaces die verbinding maken met externe netwerken zoals Internet Service Providers (ISP's), waar ondersteuning voor jumbo-frames ongebruikelijk is of niet is ingeschakeld.

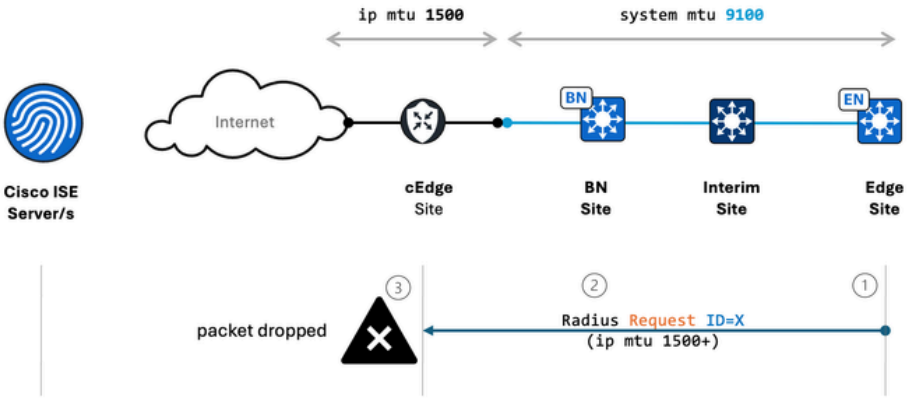
Deze ongelijkheid creëert een onmiddellijk punt van potentiële mislukking: een SDA-rand die probeert een IP-pakket groter dan 1500 bytes te verzenden naar een SD-WAN-rand waarvan de ontvangende interface is geconfigureerd voor een 1500-byte MTU.

Dit type MTU-mismatch is een veel voorkomende valkuil in SDA-implementaties en is vaak gemakkelijk over het hoofd te zien tijdens de configuratie. Wat het uitdagender maakt, is dat bepaalde gedragingen met betrekking tot de manier waarop RADIUS-verzoeken worden gegenereerd op Catalyst 9000-switches met Cisco IOS-XE® ertoe kunnen leiden dat deze problemen alleen onder specifieke en kritieke omstandigheden aan de oppervlakte komen.

RADIUS-verzoeken die worden gegenereerd tijdens het eindgebruikersverificatieproces dat wordt afgehandeld door het Session Manager Daemon-proces (SMD), zijn bijvoorbeeld hardcoded om pakketten te fragmenteren op 1396 bytes. RADIUS-verzoeken die betrokken zijn bij het ophalen van TrustSec-beleid, zoals Security Group Access Control List (SGACL), worden daarentegen gegenereerd door Cisco Internetworking Operating System daemon (IOSd)-subcomponenten. Deze zijn MTU-bewust en kunnen fragmentatie van pakketten voorkomen, tenzij hun grootte groter is dan het systeem MTU (meestal tot 9100 bytes).

Als gevolg hiervan worden problemen met betrekking tot MTU-mismatches pas duidelijk wanneer het downloadbeleid van Cisco TrustSec (CTS) wordt gebruikt. Bovendien kan de set RBACL's (Role-Based Access Control List) die tijdens de gebruikersverificatie door een SDA edge-apparaat worden gedownload, variëren, afhankelijk van het SGACL-beleid dat al voor andere tags aanwezig is. In de praktijk downloadt de switch alleen de niet-overlappende delen van beleidssets.

Samen kunnen deze gedragingen onvoorspelbare en inconsistente resultaten opleveren, variërend van stille mislukkingen tot onvolledige beleidsdownloads, afhankelijk van de omvang van het SGACL-beleid, de huidige systeemomstandigheden en, uiteindelijk, MTU-misalignementen langs het pad.



SDA Border stuurt een groot RADIUS-pakket (bijvoorbeeld 1600 bytes) naar de ISE via de SD-WAN-rand, dit is wat er gebeurt:

1. De SDA Border, met zijn 9100 MTU-interface, verzendt het 1600-byte IP-pakket.
2. De SD-WAN Cisco Edge Router ontvangt dit pakket op zijn 1500 MTU-interface.
3. Als de Do Not Fragment (DF)-bit echter niet op deze RADIUS-pakketten is ingesteld, kan de SD-WAN Cisco Edge Router ze vaak laten vallen bij binnendringen, simpelweg omdat ze "oversized" zijn ten opzichte van de geconfigureerde MTU-interface. Het komt niet in het stadium van IP-doorstuurlogica waar het kan overwegen ze te fragmenteren (als DF-bit dit toestaat).

Deze stille daling leidt tot aanzienlijke problemen bij het oplossen van hoofdpijn, vooral omdat het probleem directioneel is (SDA naar SD-WAN / ISE).

Een soortgelijke MTU-mismatch kan optreden bij de kern van het datacenter (DC) of de leaf-switches, die doorgaans zijn geconfigureerd om jumboframes (bijvoorbeeld MTU 9000+) te ondersteunen om de efficiëntie van het interne DC-verkeer te verbeteren. Als het verkeer echter wordt overgedragen aan de LAN-interface van een SD-WAN DC Cisco Edge Router die is geconfigureerd met een standaard MTU (bijvoorbeeld 1500 bytes), kan deze mismatch leiden tot fragmentatie of pakketdalingen, met name voor verkeer dat van het DC-netwerk naar de SD-WAN-structuur stroomt.

Oplossing voor uitdaging 1:

Lijn de IP MTU uit op de overdrachtsinterface van de SDA Border (fysiek of SVI) met de aangrijpende SD-WAN Cisco Edge Router-interface, meestal 1500 bytes.

Voorbeeld van configuratie (op SDA-grensknooppunt):

<#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
!
```

Belangrijke overweging: fragmentatie van de grenzen van Catalyst 9000

Catalyst-switches uit de 9000-reeks, zoals SDA Border Nodes, ondersteunen IP-fragmentatie voor native IP-pakketten in het hardwaredatapier. Het verlagen van de IP MTU op de overdrachtsinterface tot 1500 leidt niet tot een verslechtering van de prestaties als gevolg van op software gebaseerde fragmentatie voor verkeer dat afkomstig is van of doorgaat naar de grens die het nodig heeft. De switch fragmenteert efficiënt IP-pakketten groter dan 1500 bytes (als de DF-bit leeg is) voordat deze specifieke interface wordt geëgreneerd, zonder naar de CPU te wijzen.

Het is echter belangrijk op te merken dat Catalyst 9000-switches over het algemeen geen fragmentatie van VXLAN-ingekapseld verkeer ondersteunen. Deze beperking is van cruciaal belang voor overlappend verkeer, maar heeft geen invloed op het beschreven RADIUS-verificatiescenario, aangezien RADIUS-communicatie tussen de SDA-grens en een externe ISE doorgaans plaatsvindt binnen de onderlaag (native IP-routering). (MTU-overwegingen voor VXLAN-overlays zijn een afzonderlijk, complex onderwerp, dat wordt beschreven in de relevante Cisco SDA-ontwerphandleidingen).

Proactieve MTU-uitlijning bij de SDA Border naar SD-WAN Cisco Edge Router-overdracht is essentieel.

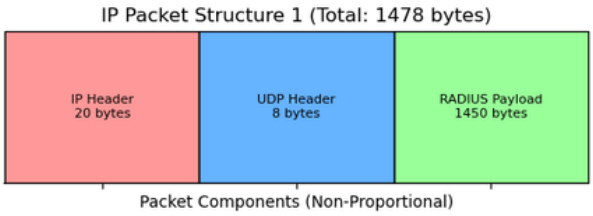
Uitdaging 2: De MTU Squeeze – ISE-verkeer over de SD-WAN-overlay

Zelfs als individuele fysieke interfaces, zoals ISE Network Interface Card (NIC)'s, switch-poorten of routerinterfaces zijn ingesteld op een standaard 1500-byte IP MTU, introduceert de SD-WAN-overlay zelf inkapselingsoverhead. Deze overhead verbruikt een deel van de limiet van 1500 bytes, waardoor de effectieve MTU die beschikbaar is voor het oorspronkelijke IP-pakket (de "payload" vanuit het perspectief van ISE) wordt verminderd.

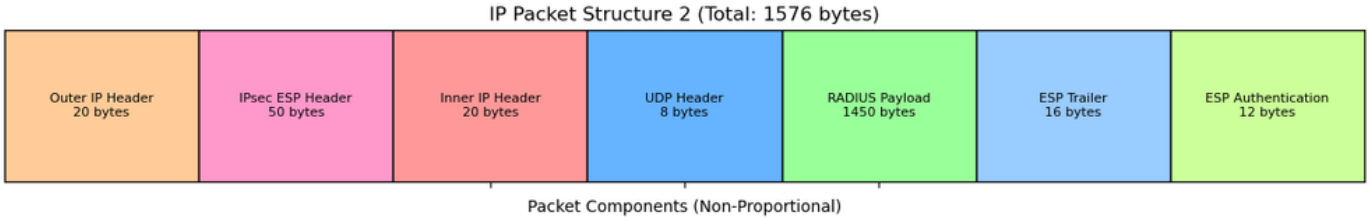
Pakketstructuur en inkapselingsoverhead:

Wanneer een IP-pakket van een ISE-server (bijvoorbeeld een RADIUS Access-Accept-pakket) wordt verzonden naar een Network Access Device (NAD) in een SDA-site, doorkruist het de SD-WAN-overlay en wordt ingekapseld. Een gemeenschappelijke inkapselingsstapel omvat IPsec in tunnelmodus, mogelijk meer dan UDP voor NAT-traversal (NAT-T).

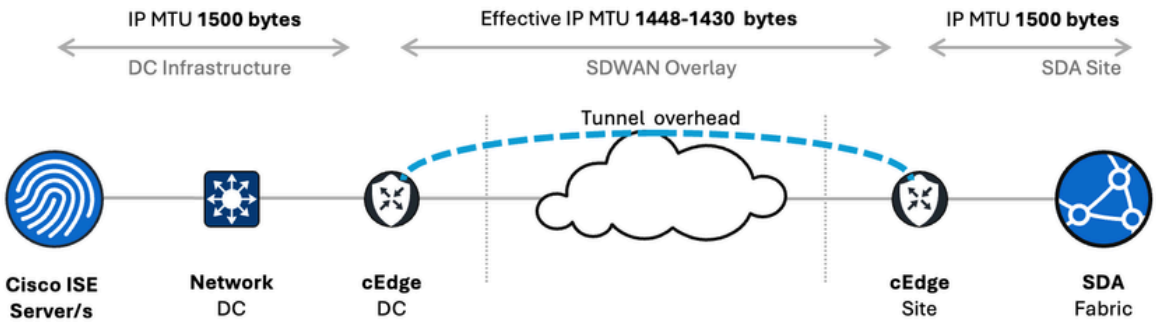
- Origineel pakket van ISE (Inner Packet):
  Bijvoorbeeld een RADIUS-pakket met een payload van 1450 bytes + 8B UDP + 20B Inner IP = 1478 bytes.



- Overweeg IPsec ESP in tunnelmodus, mogelijk met UDP-inkapseling voor NAT-T:



- De totale overhead kan variëren op basis van de specifieke IPsec-coderingen, authenticatiemechanismen en andere overlayfuncties (zoals GRE indien gebruikt). Een typische berekening:
  - Externe IP-header (IPv4): 20 bytes
  - UDP-header (indien ESP over UDP voor NAT-T): 8 bytes
  - ESP-header: ~8 bytes
  - ESP IV (bijvoorbeeld voor AES-CBC): ~16 bytes (indien van toepassing)
  - ESP-verificatie (bijvoorbeeld HMAC-SHA256 afgekapt): ~12-16 bytes
  - Gemeenschappelijke geschatte IPsec-overhead: ~52-70 bytes (kan hoger zijn, tot ~80 bytes of meer met alle opties).

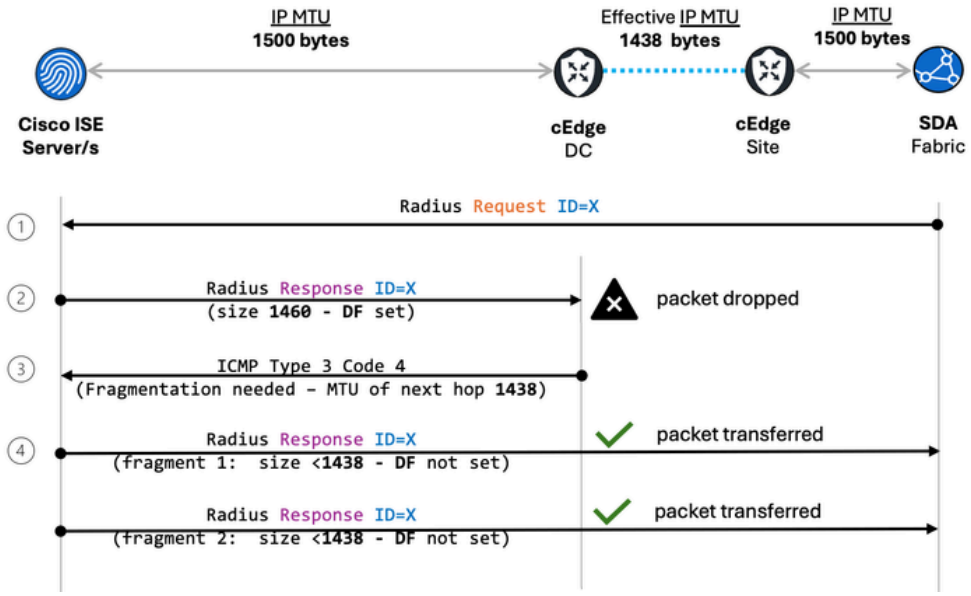


Als de fysieke link MTU 1500 bytes is, wordt de beschikbare payload MTU voor het originele IP-pakket van ISE: 1500 bytes - SD-WAN Overhead.
Bijvoorbeeld 1500 - 70 = 1430 bytes.

Gedrag wanneer pakketten de effectieve MTU overschrijden:

1. ISE initieert een pakket (de DF-bitanomalie):
    - Standaard stelt het onderliggende Linux-besturingssysteem van een ISE-toestel het Do Not Fragment (DF) in de IP-header in voor alle pakketten die het voortbrengt en die kleiner zijn dan of gelijk zijn aan de geconfigureerde interface IP MTU (bijvoorbeeld, 1500 bytes).
    - Doel van deze DF-bit: ISE (via het besturingssysteem) stelt proactief de DF-bit in om voornamelijk gebruik te maken van het Path MTU Discovery (PMTUD) -proces, dat later wordt beschreven. Hierdoor kan ISE de eigenlijke PMTU dynamisch naar een bestemming leren als deze kleiner is dan zijn eigen MTU-interface.
    - Gedrag voor pakketten groter dan interface MTU: Als ISE een IP-pakket moet verzenden dat groter is dan de geconfigureerde interface IP MTU, is het gedrag afhankelijk van het Linux-besturingssysteem. Doorgaans kan het besturingssysteem het pakket vóór verzending fragmenteren en de DF-bit wissen (DF=0 instellen) op deze resulterende fragmenten. Deze fragmentatie is een functie op besturingssysteemniveau, die niet rechtstreeks wordt aangestuurd door de ISE-toepassingscode zelf.
    - Belangrijk onderscheid met netwerkapparaten: Dit standaardgedrag van ISE (het instellen van DF=1, zelfs voor niet-gefragmenteerde pakketten die binnen de MTU-interface passen) verschilt aanzienlijk van veel traditionele netwerkapparaten (routers, switches). Netwerkapparaten stellen de DF-bit vaak niet in op pakketten die ze genereren of doorsturen, tenzij dit expliciet is geconfigureerd, of als het pakket dat wordt doorgestuurd al de DF-bit heeft ingesteld, of voor specifieke protocollen die het mandaat geven. Ze staan standaard fragmentatie toe als een pakket de next-hop MTU (en DF=0) overschrijdt.
    - Problemen oplossen Complexiteit: Deze asymmetrie, waarbij ISE-naar-NAD-verkeer standaard vaak DF=1 heeft, terwijl NAD-naar-ISE-verkeer DF=0 kan hebben (tenzij de NAD het om een reden instelt), kan een extra laag complexiteit introduceren tijdens het oplossen van problemen. Ingenieurs kunnen verschillende fragmentatiegedragingen en PMTUD-interacties observeren, afhankelijk van de richting van de verkeersstroom.
2. Packet Reaches Ingress Cisco Edge Router (DC): De DC Cisco Edge Router ontvangt het IP-pakket van ISE.
3. Inkapseling en MTU-controle door Cisco Edge Router: De Cisco Edge Router probeert het pakket voor de SD-WAN-tunnel in te kapselen.
    - Als de oorspronkelijke pakketgrootte groter is dan de SD-WAN-inkapselingsoverhead (bijvoorbeeld 1500 bytes) en de DF-bit is ingesteld op het oorspronkelijke (binnenste) pakket van ISE, mag de Cisco Edge Router het binnenste pakket niet fragmenteren.
    - De Cisco Edge Router moet het pakket laten vallen.
    - Van cruciaal belang is dat de Cisco Edge Router ook een ICMP-bericht "Destination Unreach - Fragmentation Needed and DF bit set" (Type 3, Code 4) terugstuurt naar de bron (ISE), met vermelding van de MTU van de volgende hop (de effectieve MTU van de tunnel).
4. Path MTU Discovery (PMTUD)-proces: na ontvangst van dit ICMP-bericht "Fragmentatie vereist" moet ISE (het bronbesturingssysteem) de PMTU-schatting voor dat specifieke bestemmingspad verlagen. Het zou deze informatie opslaan en de gegevens opnieuw verzenden in kleinere pakketten die passen binnen de nieuw ontdekte PMTU.

PMTUD-procesdiagram:



Waar PMTUD-communicatie uiteenvalt:
PMTUD is in theorie robuust, maar kan in de praktijk falen:

- ICMP-filtering: Intermediaire firewalls of beveiligingsbeleid blokkeren vaak ICMP-berichten, waardoor het bericht "Versnippering nodig" ISE niet kan bereiken.
- Control Plane Policing (CoPP) op Cisco Edge Router: Cisco Edge Routers gebruiken CoPP om hun CPU te beschermen. Het genereren van ICMP-foutberichten is een controleplantaak. Onder zware belasting of met veel te grote pakketten kan CoPP de ICMP-generatie beperken of verlagen. ISE krijgt nooit feedback.
- Silent Drops: Als ISE het ICMP-bericht "Fragmentation Needed" niet ontvangt, blijft het zich niet bewust van de padbeperking. Het blijft grote pakketten verzenden met de DF-bitset, waardoor ze stilletjes worden weggelaten door de Cisco Edge Router. Dit resulteert in time-outs en heruitzendingen van de toepassingslaag (bijvoorbeeld RADIUS).
- Impact op ISE-services: grote RADIUS Access-Accept-pakketten (met dACL's, uitgebreide AVP's, SGT-informatie) zijn bijzonder gevoelig. Manifestaties omvatten:
    - Intermitterende of volledige verificatiefouten.
    - Eindpunten die geen correct netwerktoegangsbeleid of SGT's ontvangen.
    - Onvolledige of mislukte beleidssynchronisatie tussen ISE en NAD.

Oplossing voor uitdaging 2: proactieve ISE IP MTU-configuratie

Gezien de onbetrouwbaarheid van PMTUD is een proactieve aanpak het beste voor kritieke services zoals ISE. Configureer de IP MTU op de netwerkinterfaces van ISE op een waarde die veilig de maximale verwachte SD-WAN-overlay-overhead herbergt. Dit zorgt ervoor dat ISE geen

IP-pakketten (met de DF-bitset) produceert die inherent te groot zijn om door de SD-WAN-overlay te gaan zonder fragmentatie door een tussenliggend apparaat (wat verboden is als DF=1).

De aanbevolen ISE IP MTU berekenen en instellen:

1. Vaststellen van fysieke basis-MTU: Dit is meestal 1500 bytes voor standaard Ethernet-interfaces langs het pad.
2. Bepaal de maximale SD-WAN-inkapselingsoverhead:
    - Bereken of schat nauwkeurig de totale overhead die door uw specifieke SD-WAN-overlay wordt geïntroduceerd (IPsec, GRE, VXLAN, MPLSoGRE, enzovoort). Raadpleeg de documentatie van de leverancier voor precieze cijfers voor de door u gekozen protocollen en opties.

component	Voorbeeld overhead (bytes)	Opmerkingen
Basis fysieke MTU	1500	Standaard Ethernet op fysieke koppelingen
Minder: SD-WAN-overhead		
Externe IP-header (IPv4)	20	
UDP-header (voor NAT-T)	8	Als ESP is ingekapseld in UDP
ESP-koptekst	~8-12	
ESP IV (bijvoorbeeld AES-CBC)	~16	Varieert met het coderingsalgoritme
ESP Auth (bijvoorbeeld, SHA256)	~12-16	Varieert met het verificatiealgoritme (bijvoorbeeld 96-bits voor sommige)
Andere overlays (GRE, enzovoort)	veranderlijk	Voeg een deel van uw SD-WAN-inkapselingsstapel toe
Totale geschatte overheadkosten	~68 - 80+ bytes	Som van alle relevante onderdelen voor uw implementatie
Effectief pad MTU	~1432 - 1420 bytes	Basis fysieke MTU - totale geschatte overhead

3. Aanbevolen MTU-configuratie van ISE IP:
    - Neem het berekende effectieve pad MTU (bijvoorbeeld 1420 bytes uit het voorbeeld).
    - Trek een extra veiligheidsmarge (bijvoorbeeld 20-70 bytes) af om rekening te houden met kleine, niet-verantwoorde L2-headers of om een buffer te bieden.
    - Oplossingen zoals Cisco SD-WAN kunnen Path MTU (PMTU)-detectie individueel uitvoeren voor elke site-to-site tunnel. Dit mechanisme werkt automatisch elke 20 minuten om de IP MTU van de tunnel te testen en dynamisch aan te passen aan de huidige transportomstandigheden op elke locatie. Hierdoor kunnen MTU-waarden tussen sites verschillen en in de loop van de tijd veranderen.
    - Een over het algemeen veilige en aanbevolen IP MTU voor ISE-interfaces in dergelijke scenario's is tussen 1350 en 1400 bytes

Een IP MTU van 1350 bytes is vaak een zeer robuust uitgangspunt

ISE-configuratie (voorbeeld via CLI):

Deze opdracht wordt uitgevoerd op de Cisco ISE-appliance CLI voor elke relevante

netwerkinterface.

<#root>

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

 ip mtu 1350
!
```

Belangrijke operationele overwegingen voor ISE IP MTU-wijzigingen:

- Opnieuw opstarten van de service vereist: zodra de opdracht ip mtu wordt toegepast op een ISE-interface, wordt de gebruiker gevraagd om de ISE-toepassingsservices opnieuw op te starten. Dit is een wijziging die gevolgen heeft voor de service en moet worden gepland tijdens een gepland onderhoudsvenster. Raadpleeg de officiële Cisco ISE-documentatie voor procedurele details.
- Toepassen op alle ISE-nodes: deze aanpassing van de IP MTU moet consequent worden toegepast op alle ISE-nodes in de implementatie (primaire PAN, secundaire PAN, Policy Service Nodes (PSN's)) die communiceren met NAD's via het SD-WAN. Inconsistente MTU-instellingen leiden tot onvoorspelbaar gedrag.
- Grondig testen: test deze verandering grondig in een laboratorium of proefopstelling voordat deze in productie wordt genomen. Gebruik tools zoals ping met verschillende pakketgroottes en de DF-bit set om end-to-end MTU handling te valideren:
    - Linux-gebaseerde systemen:

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

(Opmerking: -s geeft de grootte van de ICMP-payload op. Totale IP-pakketgrootte = payload + 8B ICMP Hdr + 20B IP Hdr voor IPv4)

- Windows:

```
ping

        -f -l
```

(Opmerking: -l geeft de grootte van de ICMP-payload op.)

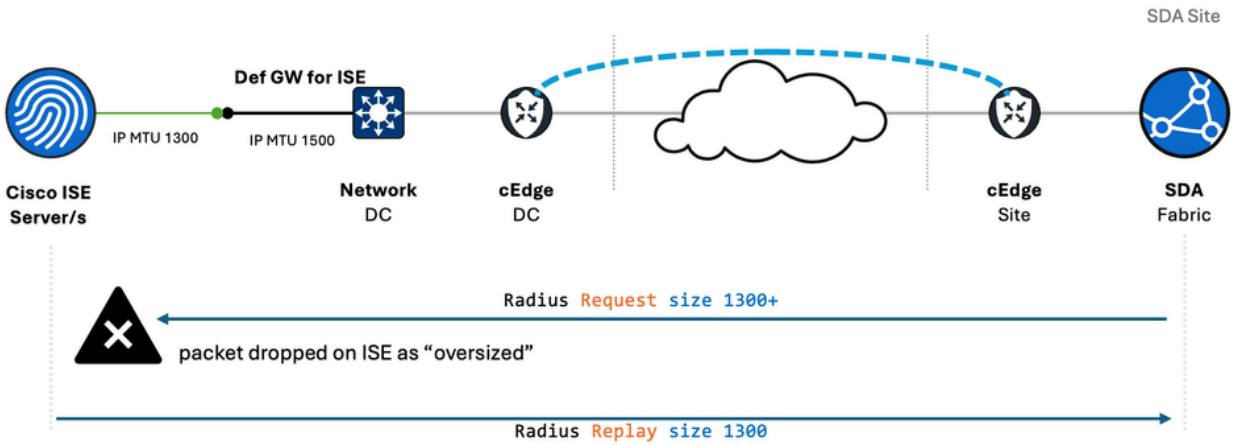
- Cisco IOS/Cisco IOS-XE®

```
ping

        size

         df-bit
```

- ISE eerste routeringspunt – Zorg er bij het aanpassen van de IP MTU-waarde op de ISE-interface voor dat het eerste routeringspunt in het datacenter — met name de Layer 3-interface die is gekoppeld aan het ISE-subnet — ook is geconfigureerd met dezelfde IP MTU-waarde.
  Dit helpt situaties te voorkomen zoals beschreven in Challenge 1, waarbij een MTU-mismatch ervoor zorgt dat ISE binnenkomende pakketten als te groot behandelt en laat vallen.
  Als de ISE-interface bijvoorbeeld een verlaagde MTU heeft (bijvoorbeeld 1300), maar het eerste routeringspunt blijft geconfigureerd met de standaard MTU van 1500, worden pakketten die naar ISE worden verzonden en groter zijn dan 1300 bytes maar kleiner dan 1500 bytes, niet gefragmenteerd en worden ze door ISE verwijderd - zoals waargenomen in uitdaging 1.
  Zorg er bovendien voor dat het eerste routeringspunt in staat is om fragmentatie uit te voeren als dat nodig is en dat dit niet leidt tot verslechtering van de prestaties.
- Update MTU over het hele transmissiepad, en in beide richtingen - Bij het bijwerken van de IP MTU-instellingen op ISE, is het belangrijk om de MTU over het hele transmissiepad te

overwegen, en in beide richtingen. Als de MTU-waarde die op ISE is geconfigureerd, niet is afgestemd op de MTU op de Layer 3-interface van de first-hop-gateway, kunnen zich vergelijkbare problemen voordoen zoals beschreven in uitdaging nr. 1.

Als de ISE MTU bijvoorbeeld wordt gereduceerd tot 1300 bytes terwijl de standaard 1500-byte MTU op de standaardgateway blijft geconfigureerd, kunnen pakketten met een grootte tussen 1300 en 1500 bytes, die gewoonlijk worden gegenereerd door netwerkapparaten, door ISE als te groot worden weggelaten.



Om dit probleem te voorkomen, moet u er altijd voor zorgen dat MTU-wijzigingen op ISE worden gespiegeld op de first-hop-gateway en idealiter worden weerspiegeld op alle eindhosts binnen hetzelfde Layer 3-segment. Dit helpt de end-to-end MTU consistentie te behouden en voorkomt onverwachte pakketdruppels.

Conclusie

Het afstemmen van de IP MTU-instellingen op Cisco ISE-servers met de effectieve MTU-limieten voor transportlagen die worden opgelegd door SD-WAN-inkapseling en MTU-uitlijning aan de SDA Border op SD-WAN Cisco Edge Router-overdracht is niet alleen een aanbeveling, maar een essentiële voorwaarde voor het waarborgen van de stabiliteit, betrouwbaarheid en prestaties van AAA-services in moderne, gesegmenteerde bedrijfsnetwerken. Hoewel Path MTU Discovery een belangrijk mechanisme is, kan de praktische effectiviteit ervan worden belemmerd door factoren zoals ICMP-filtering of Control Plane Policing in SD-WAN-omgevingen.

Door proactief een verlaagde IP MTU op ISE te configureren (bijvoorbeeld 1350-1400 bytes), kunnen netwerkarchitecten en ingenieurs het risico op MTU-gerelateerde pakketdalingen aanzienlijk verminderen, wat leidt tot meer voorspelbare en veerkrachtige netwerkactiviteiten. Dit is met name van vitaal belang in Cisco SDA-implementaties waar ISE geavanceerde micro-segmentatie en dynamische beleidshandhaving orkestreert, die vaak afhankelijk zijn van de succesvolle levering van potentieel grote control-plane-berichten. Zorgvuldige planning, uitgebreide tests en consistente configuratie voor alle ISE-knooppunten zijn de sleutel tot een succesvolle en probleemloze implementatie.

Normen en referenties

Raadpleeg voor meer informatie de officiële standaarden en de documentatie van Cisco:

RFC's:

- RFC 1191: Path MTU Discovery
- RFC 791: Internet Protocol (IP) - Definieert de IP-header, inclusief de Do Not Fragment (DF)-bit.
- RFC 8200: IPv6-specificatie (relevant indien IPv6 wordt gebruikt, omvat soortgelijke PMTUD-concepten).
- RFC 4459: MTU and Fragmentation Issues with In-the-Network Tunneling (VPN's) - richt zich rechtstreeks op veelvoorkomende MTU-problemen in VPN-omgevingen.

Cisco-documentatie:

- Ontwerp- en implementatiehandleidingen voor Cisco SDA: voor informatie over MTU-aanbevelingen voor verbindingen en configuraties van randknooppunten.
- Ontwerp- en configuratiehandleidingen voor Cisco SD-WAN: voor meer informatie over inkapselingsoverhead, tunnelinterface MTU en PMTUD-overwegingen binnen de SD-WAN-structuur.
- Cisco Catalyst 9000 Series Switch Configuration Guides: voor platformspecifieke informatie over MTU-instellingen en fragmentatiemogelijkheden.
- Cisco Identity Services Engine (ISE) Administrator and CLI Guides: Voor informatie over de configuratie van de interface, inclusief de implicaties van de ip mtu-opdracht en het opnieuw opstarten van de service.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.