Configurazione dell'MTU IP ISE ottimale in SD-WAN per installazioni SDA

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati:

Premesse

Descrizione del problema

- Topologia illustrativa

Sfida 1: Il gap MTU - i confini SDA ai bordi SD-WAN

Soluzione alla sfida 1:

Sfida 2: La compressione MTU - il traffico ISE attraverso la sovrimpressione SD-WAN

- Struttura del pacchetto e sovraccarico dell'incapsulamento:

Soluzione alla sfida 2: Configurazione proattiva ISE IP MTU

- Configurazione ISE (esempio tramite CLI):

Conclusioni

- Standard e riferimenti

Introduzione

Questo documento descrive come i problemi di Maximum Transmission Unit (MTU) possono influire sulla micro-segmentazione in SDA quando SD-WAN è usato per connettere siti SDA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati:

Le informazioni fornite in questo documento si basano su SDA, SDWAN e ISE.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Le moderne reti aziendali sfruttano sempre di più l'architettura SDA per la microsegmentazione granulare e l'applicazione coerente delle politiche. Per connettere i siti SDA distribuiti, viene spesso utilizzata una Cisco SD-WAN che offre un trasporto agile, sicuro e ottimizzato su varie reti sottostanti. Elemento centrale di questa architettura, ISE offre servizi critici di autenticazione, autorizzazione e accounting (AAA), oltre a una distribuzione dinamica delle policy (ad esempio, Security Group Tags (SGT) e ACL scaricabili).

Se da un lato l'integrazione di queste potenti tecnologie può introdurre problemi di configurazione impercettibili ma di notevole impatto. La gestione dell'MTU nei punti di passaggio critici della rete e attraverso la sovrapposizione SD-WAN è un'area primaria per questi problemi. In questo articolo vengono illustrati due scenari di mancata corrispondenza MTU comuni che possono interrompere le operazioni di rete:

1. Il gap MTU tra i nodi di confine della SDA e i dispositivi periferici della SD-WAN.
2. Vincoli MTU per il traffico originato da ISE che attraversa la sovrimpressione SD-WAN.

Un corretto allineamento dell'MTU è fondamentale per evitare problemi di frammentazione dei pacchetti o perdite invisibili all'utente, garantendo un'autenticazione affidabile, l'applicazione di policy e la stabilità complessiva della rete. Se non si risolvono questi problemi, è possibile che si verifichino problemi intermittenti di connettività e errori di applicazione delle policy, con un notevole dispendio di risorse per la risoluzione dei problemi.

Sintomi comuni di MTU non allineata

L'MTU non allineata può manifestarsi in diversi modi, spesso portando a problemi di difficile diagnosi:

- Errori o timeout di autenticazione RADIUS intermittenti: Particolarmente evidente per le policy che generano pacchetti RADIUS più grandi (ad esempio, quelle con coppie AV estese o certificati).
- Endpoint che non ricevono o non applicano ACL scaricabili (dACL) o criteri TrustSec (SGT/SGACL): Questi criteri vengono spesso trasmessi in pacchetti RADIUS di grandi dimensioni.
- Sessione lenta stabilita per i client autenticati: A causa di ritrasmissioni a livello di applicazione.
- Ritrasmissioni RADIUS eccessive: Osservabile nei log ISE o nei dispositivi di accesso alla rete (NAD).
- Propagazione dei criteri incoerente: Le modifiche alle policy effettuate in ISE potrebbero non essere propagate in modo coerente a tutti i servizi NAD nei siti SDA remoti.

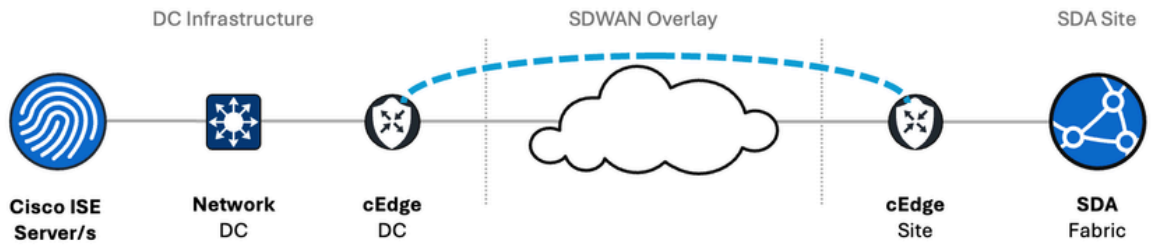
- Differenze nell'acquisizione dei pacchetti: Le acquisizioni possono mostrare l'invio di pacchetti di grandi dimensioni (ad esempio, superiori a 1450 byte) con il bit "Do Not Fragment" (DF) impostato, ma senza la risposta corrispondente o l'errore ICMP "Fragmentation Needed" (Frammentazione richiesta) dal router perimetrale NAD o SD-WAN Cisco Edge.
- Incremento dei contatori di perdita dei pacchetti: Osservato sull'interfaccia in entrata del Cisco Edge Router del data center (DC) per il traffico proveniente da ISE e destinato ai siti SDA, o sull'interfaccia del Cisco Edge Router SD-WAN rivolta verso il bordo SDA per il traffico in direzione inversa.

Descrizione del problema

Un'installazione aziendale tipica
Si consideri una topologia aziendale comune:

- Server Cisco ISE: Implementato in un centro dati centralizzato (DC, Data Center) o in hub regionali, collegato all'infrastruttura di rete DC.
- Infrastruttura DC: Comprende switch di aggregazione o core DC a cui si connettono i server ISE.
- Sovrimpressione SD-WAN: I router DC Cisco Edge Router stabiliscono tunnel SD-WAN (comunemente IPsec) su una rete di trasporto sotterranea (ad esempio, Internet, MPLS) verso i router Cisco Edge nei siti SDA remoti.
- Sito SDA: I router Cisco Edge Router del sito remoto si connettono al fabric SDA locale, che include i nodi periferici del fabric, i nodi di confine, i controller WLC (Wireless LAN Controller) e, infine, gli endpoint.

Topologia illustrativa



Sfida 1: Il gap MTU - i confini SDA ai bordi SD-WAN

I principi di progettazione SDA Cisco, spesso implementati tramite l'automazione LAN, promuovono una MTU a livello di campus di 9100 byte (frame jumbo) su tutti i dispositivi fabric. Ciò include i nodi di confine Catalyst serie 9000 e garantisce che i frame jumbo Ethernet vengano trasportati in modo efficiente all'interno del fabric. Di conseguenza, l'interfaccia di handoff di layer 3 o SVI su un nodo di bordo SDA utilizza per impostazione predefinita questa MTU più grande.

Al contrario, i dispositivi periferici SD-WAN, come Catalyst serie 8000, in genere assumono come valore predefinito un'MTU dell'interfaccia di 1500 byte. Questa funzionalità è standard per le interfacce che si connettono a reti esterne come i provider di servizi Internet (ISP), dove il supporto jumbo frame è raro o non abilitato.

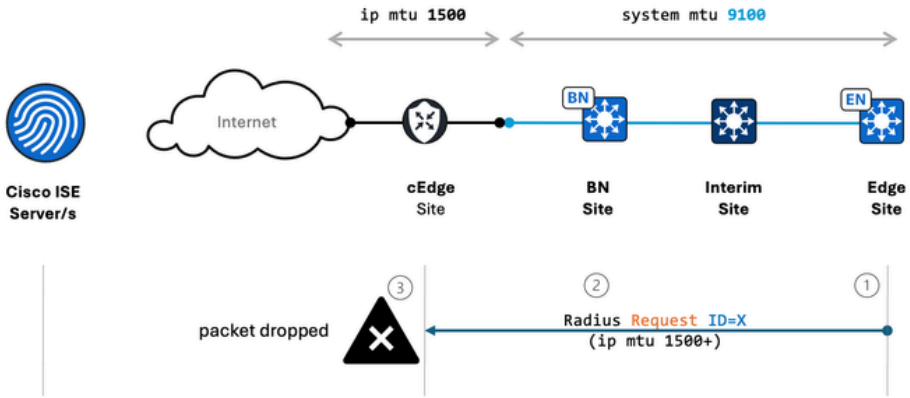
Questa disparità crea un punto immediato di potenziale fallimento: un bordo SDA che tenta di inviare un pacchetto IP più grande di 1500 byte a un bordo SD-WAN la cui interfaccia di ricezione è configurata per una MTU di 1500 byte.

Questo tipo di mancata corrispondenza MTU è un problema comune nelle distribuzioni SDA e spesso può essere ignorato durante la configurazione. Ciò che rende più difficile è che alcuni comportamenti correlati al modo in cui le richieste RADIUS vengono generate sugli switch Catalyst 9000 con Cisco IOS-XE® possono far emergere questi problemi solo in condizioni critiche e specifiche.

Ad esempio, le richieste RADIUS generate durante il processo di autenticazione dell'utente finale gestito dal processo SMD (Session Manager Daemon) vengono codificate per frammentare i pacchetti a 1396 byte. Al contrario, le richieste RADIUS coinvolte nel recupero dei criteri TrustSec, ad esempio SGACL (Security Group Access Control List), vengono generate dai sottocomponenti del daemon IOS (Cisco Internetworking Operating System Daemon). Riconoscono MTU e possono evitare di frammentare i pacchetti se le loro dimensioni non superano l'MTU del sistema (generalmente fino a 9100 byte).

Di conseguenza, i problemi relativi alla mancata corrispondenza delle MTU diventano evidenti solo quando vengono utilizzati i criteri di download di Cisco TrustSec (CTS). Inoltre, l'insieme di RBACL (Role-Based Access Control List) scaricati da un dispositivo periferico SDA durante l'autenticazione utente può variare a seconda dei criteri SGACL già presenti per altri tag. In pratica, lo switch scarica solo le parti non sovrapposte dei set di criteri.

Insieme, questi comportamenti possono produrre risultati imprevedibili e incoerenti, che vanno dagli errori automatici ai download di criteri incompleti, a seconda delle dimensioni del criterio SGACL, delle condizioni di sistema correnti e, in ultima analisi, dei disallineamenti MTU lungo il percorso.



SDA Border inoltra un pacchetto RADIUS di grandi dimensioni (ad esempio, 1600 byte) verso l'ISE passando per il bordo SD-WAN, ed ecco cosa succede:

1. Il bordo SDA, con la sua interfaccia di 9100 MTU, invia il pacchetto IP da 1600 byte.
2. Il router perimetrale Cisco SD-WAN riceve questo pacchetto sull'interfaccia 1500 MTU.
3. Tuttavia, se il bit "non frammentare" (DF, Do Not Fragment) non è impostato su questi pacchetti RADIUS, il router perimetrale Cisco SD-WAN può spesso eliminarli all'ingresso semplicemente perché sono "di dimensioni eccessive" rispetto alla MTU dell'interfaccia configurata. Non arriva alla fase della logica di inoltro IP in cui può prendere in considerazione la frammentazione (se il bit DF lo consente).

Questa perdita invisibile all'utente comporta notevoli problemi nella risoluzione dei problemi, soprattutto se il problema è direzionale (da SDA a SD-WAN/ISE).

Una mancata corrispondenza MTU simile può verificarsi sugli switch core o foglia del data center (DC), che sono in genere configurati per supportare frame jumbo (ad esempio, MTU 9000+) per migliorare l'efficienza del traffico interno DC. Tuttavia, se il traffico viene consegnato all'interfaccia con connessione LAN di un router Cisco Edge DC SD-WAN configurato con una MTU standard (ad esempio, 1500 byte), la mancata corrispondenza può causare la frammentazione o la perdita di pacchetti, in particolare per il traffico che fluisce dalla rete DC al fabric SD-WAN.

Soluzione alla sfida 1:

Allineare l'MTU IP sull'interfaccia handoff del bordo SDA (fisica o SVI) con l'interfaccia peer SD-WAN Cisco Edge Router, in genere da 1500 byte.

Esempio di configurazione (su nodo di bordo 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
!
```

Considerazioni importanti: Frammentazione sui bordi di Catalyst 9000

Gli switch Catalyst serie 9000, in quanto nodi del bordo SDA, supportano la frammentazione IP per i pacchetti IP nativi nel piano dati hardware. la riduzione dell'mtu ip sull'interfaccia dell'handoff a 1500 non causa un calo delle prestazioni dovuto alla frammentazione basata su software del traffico in entrata o in uscita dal confine che lo richiede. Lo switch frammenta in modo efficiente pacchetti IP più grandi di 1500 byte (se il bit DF non è impostato) prima di uscire da questa interfaccia specifica, senza puntare alla CPU.

Tuttavia, è importante notare che gli switch Catalyst 9000 in genere non supportano la frammentazione del traffico incapsulato VXLAN. Questa limitazione è fondamentale per il traffico di sovrimpressione, ma non influisce sullo scenario di autenticazione RADIUS descritto, in quanto la comunicazione RADIUS tra il bordo SDA e un ISE esterno in genere si verifica nell'underlay (routing IP nativo). (Le considerazioni sull'MTU per le sovrapposizioni VXLAN sono un argomento distinto e complesso, descritto in dettaglio nelle guide alla progettazione Cisco SDA).

L'allineamento proattivo MTU al bordo SDA per il collegamento del router Cisco Edge SD-WAN è essenziale.

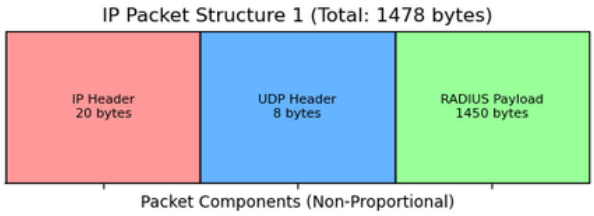
Sfida 2: La compressione MTU - il traffico ISE attraverso la sovrimpressione SD-WAN

Anche se le singole interfacce fisiche, come le schede di interfaccia di rete (NIC, Network Interface Card) ISE, le porte degli switch o le interfacce del router sono impostate su una MTU IP standard di 1500 byte, la sovrapposizione SD-WAN stessa introduce il sovraccarico dell'incapsulamento. Questo sovraccarico consuma una parte del limite di 1500 byte, riducendo l'MTU effettiva disponibile per il pacchetto IP originale (il "payload" dalla prospettiva di ISE).

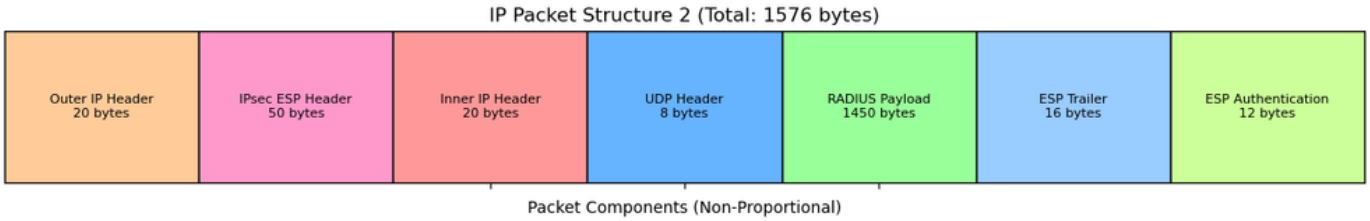
Struttura del pacchetto e sovraccarico dell'incapsulamento:

Quando un pacchetto IP proveniente da un server ISE (ad esempio, un pacchetto RADIUS Access-Accept) viene inviato a un dispositivo NAD (Network Access Device) in un sito SDA, attraversa la sovrimpressione SD-WAN e viene incapsulato. Uno stack di incapsulamento comune include IPsec in modalità tunnel, potenzialmente su UDP per NAT traversal (NAT-T).

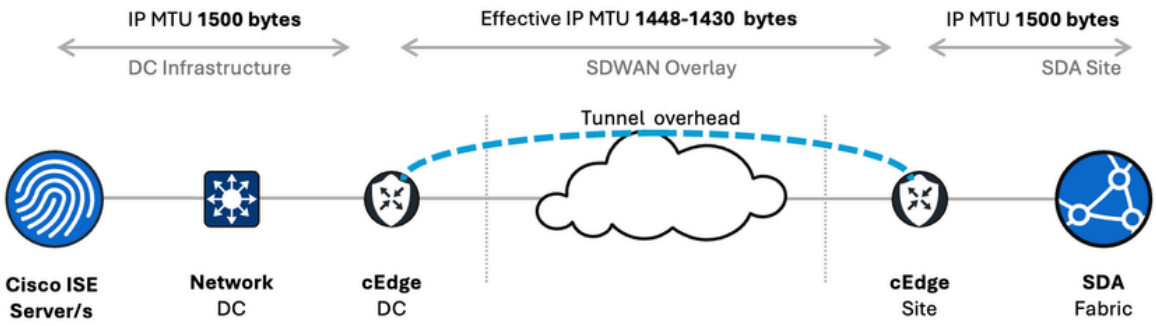
- Pacchetto originale da ISE (pacchetto interno):
  Ad esempio, un pacchetto RADIUS con un payload di 1450 byte + 8B UDP + 20B IP interno = 1478 byte.



- Prendere in considerazione IPsec ESP in modalità tunnel, potenzialmente con incapsulamento UDP per NAT-T:



- Il sovraccarico totale può variare in base alla cifratura IPsec specifica, ai meccanismi di autenticazione e ad altre funzionalità di sovrimpressione (ad esempio, GRE, se utilizzato). Un tipico calcolo:
    - Intestazione IP esterna (IPv4): 20 byte
    - Intestazione UDP (se ESP over UDP per NAT-T): 8 byte
    - Intestazione ESP: Circa 8 byte
    - ESP IV (ad esempio, per AES-CBC): ~16 byte (se applicabile)
    - Autenticazione ESP (ad esempio, HMAC-SHA256 troncato): Circa 12-16 byte
    - Sovraccarico IPsec stimato comune: ~52-70 byte (maggiore, fino a ~80 byte o più con tutte le opzioni).



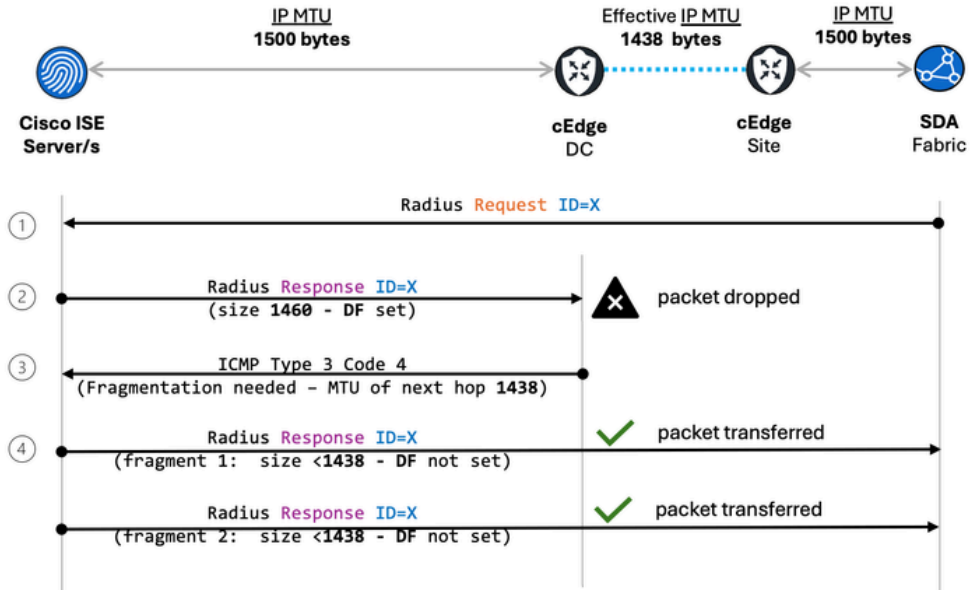
Se l'MTU del collegamento fisico è 1500 byte, la MTU del payload disponibile per il pacchetto IP originale dell'ISE diventa: 1500 byte - Sovraccarico SD-WAN.
Ad esempio, 1500 - 70 = 1430 byte.

Comportamento quando i pacchetti superano l'MTU effettiva:

1. ISE Genera un pacchetto (l'anomalia del bit DF):
    - Per impostazione predefinita, il sistema operativo Linux sottostante di un'appliance ISE imposta il bit Do Not Fragment (DF) nell'intestazione IP di tutti i pacchetti da cui ha origine che sono inferiori o uguali alla MTU IP dell'interfaccia configurata (ad esempio, 1500 byte).
    - Scopo del bit DF:ISE (tramite il sistema operativo) imposta proattivamente il bit DF in modo da usare il processo di rilevamento della MTU del percorso (PMTUD), descritto più avanti. Questo consente ad ISE di imparare dinamicamente la PMTU effettiva su una destinazione se è più piccola della MTU della propria interfaccia.
    - Comportamento per pacchetti più grandi dell'MTU dell'interfaccia:se ISE deve inviare un pacchetto IP più grande della MTU IP dell'interfaccia configurata, il comportamento dipende dal sistema operativo Linux in uso. In genere, il sistema operativo frammenta il pacchetto prima della trasmissione e cancella il bit DF (impostando DF = 0) su questi frammenti risultanti. Questa frammentazione è una funzione a livello di sistema operativo, non guidata direttamente dal codice dell'applicazione ISE.
    - Distinzione dei tasti dai dispositivi di rete:questo comportamento predefinito di ISE (impostando DF=1 anche per pacchetti non frammentati che si adattano alla MTU dell'interfaccia) è notevolmente diverso da quello di molti dispositivi di rete tradizionali (router, switch). I dispositivi di rete spesso non impostano il bit DF sui pacchetti da essi originati o inoltrati a meno che non siano stati configurati esplicitamente a tale scopo o se per il pacchetto da inoltrare il bit DF è già impostato o è stato impostato per protocolli specifici che lo richiedono. In genere, permettono la frammentazione per impostazione predefinita se un pacchetto supera l'MTU dell'hop successivo (e DF = 0).
    - Complessità della risoluzione dei problemi: questa asimmetria, in cui per impostazione predefinita il traffico da ISE a NAD ha spesso DF=1, mentre il traffico da NAD a ISE può avere DF=0 (a meno che non venga impostato da NAD per un motivo), può introdurre un ulteriore livello di complessità durante la risoluzione dei problemi. I tecnici possono osservare comportamenti di frammentazione diversi e interazioni PMTUD a seconda della direzione del flusso del traffico.
2. Il pacchetto raggiunge il Cisco Edge Router (DC) in entrata:il router Cisco Edge DC riceve il pacchetto IP da ISE.
3. Incapsulamento e controllo MTU da parte di Cisco Edge Router:Cisco Edge Router cerca di incapsulare il pacchetto per il tunnel SD-WAN.
    - Se le dimensioni del pacchetto originale più il sovraccarico dell'incapsulamento SD-WAN supera l'MTU dell'interfaccia fisica in uscita del router Cisco Edge (ad esempio, 1500 byte) E il bit DF è impostato sul pacchetto (interno) originale dell'ISE, il router Cisco Edge non deve frammentare il pacchetto interno.
    - Il Cisco Edge Router deve rilasciare il pacchetto.
    - In termini critici, il router Cisco Edge deve anche inviare un messaggio ICMP "Destination Unreachable - Fragmentation Needed and DF bit set" (Tipo 3, Codice 4) all'origine (ISE), indicando la MTU dell'hop successivo (la MTU effettiva del tunnel).
4. Processo di rilevamento della MTU del percorso (PMTUD): Dopo aver ricevuto il messaggio ICMP "Frammentazione richiesta", l'ISE (il sistema operativo di origine) deve ridurre la sua stima PMTU per il percorso di destinazione specifico. Memorizza nella cache queste

informazioni e invia nuovamente i dati in pacchetti più piccoli che rientrano nella PMTU appena rilevata.

Diagramma processo PMTUD:



Dove la comunicazione PMTUD si interrompe:
La funzionalità PMTUD è solida in teoria, ma può fallire in pratica:

- Filtro ICMP: I firewall intermedi o le policy di sicurezza spesso bloccano i messaggi ICMP, impedendo al messaggio "frammentazione richiesta" di raggiungere ISE.
- Control Plane Policing (CoPP) su Cisco Edge Router: I router Cisco Edge Router utilizzano il protocollo CoPP per proteggere la CPU. La generazione di messaggi di errore ICMP è un'attività del control plane. In condizioni di carico elevato o con molti pacchetti di dimensioni eccessive, il protocollo CoPP può limitare la velocità di generazione o eliminare il protocollo ICMP. ISE non riceve mai il feedback.
- Cadute invisibili all'utente: Se ISE non riceve il messaggio ICMP "Frammentazione richiesta", non è a conoscenza della restrizione del percorso. Continua a inviare pacchetti di grandi dimensioni con bit DF impostato e li scarta automaticamente in entrata dal Cisco Edge Router. Ciò determina timeout e ritrasmissioni a livello di applicazione (ad esempio RADIUS).
- Impatto sui servizi ISE: Particolarmente sensibili sono i pacchetti RADIUS Access-Accept di grandi dimensioni (che contengono dACL, AVP estesi, informazioni SGT). Le manifestazioni includono:
  - Errori di autenticazione intermittenti o completi.
  - Endpoint che non ricevono i criteri di accesso alla rete o i servizi SGT corretti.
  - Sincronizzazione dei criteri incompleta o non riuscita tra ISE e NAD.

Soluzione alla sfida 2: Configurazione proattiva ISE IP MTU

Data l'inaffidabilità della funzionalità PMTUD, un approccio proattivo è il migliore per servizi critici come ISE. Configurare l'MTU IP sulle interfacce di rete ISE su un valore che soddisfi in modo sicuro il massimo sovraccarico previsto per SD-WAN. Ciò assicura che ISE non generi pacchetti IP (con bit DF impostato) che sono intrinsecamente troppo grandi per attraversare la sovrapposizione SD-WAN senza dover essere frammentati da un dispositivo intermedio (condizione vietata se DF = 1).

Calcolo e impostazione dell'MTU IP ISE consigliata:

1. Stabilire l'MTU fisica di base: si tratta in genere di 1500 byte per le interfacce Ethernet standard sul percorso.
2. Determinare il sovraccarico massimo di incapsulamento SD-WAN:
    - Calcolare accuratamente o stimare in modo prudente il sovraccarico totale introdotto dalla sovrimpressione SD-WAN specifica (IPsec, GRE, VXLAN, MPLSoGRE e così via). Per informazioni dettagliate sulle opzioni e i protocolli scelti, consultare la documentazione del fornitore.

Componente	Esempio di sovraccarico (byte)	Note
MTU fisica base	1500	Ethernet standard sui collegamenti fisici
Meno: Overhead SD-WAN		
Intestazione IP esterna (IPv4)	20	
UDP Header (per NAT-T)	8	Se ESP è incapsulato in UDP
Intestazione ESP	~8-12	
ESP IV (ad esempio, AES-CBC)	~16	Varia a seconda dell'algoritmo di crittografia
Autenticazione ESP (ad esempio, SHA256)	~12-16	Varia con l'algoritmo di autenticazione (ad esempio, 96 bit per alcuni)
Altre sovrapposizioni (GRE, ecc.)	Variabile	Da aggiungere se parte dello stack di incapsulamento SD-WAN
Totale costi comuni stimati	~68 - 80+ byte	Somma di tutti i componenti rilevanti per la distribuzione
MTU percorso effettivo	Circa 1432 - 1420 Byte	MTU fisica base - Totale stimato sovraccarico

3. Configurazione consigliata ISE IP MTU:
    - Prendere l'MTU del percorso effettivo calcolata (ad esempio, 1420 byte dall'esempio).
    - Sottrarre un margine di sicurezza aggiuntivo (ad esempio, 20-70 byte) per tenere conto delle intestazioni L2 secondarie non contabilizzate o per fornire un buffer.
    - Soluzioni come Cisco SD-WAN possono eseguire il rilevamento della MTU del percorso (PMTU) singolarmente per ogni tunnel da sito a sito. Questo meccanismo viene eseguito automaticamente ogni 20 minuti per verificare e regolare dinamicamente l'MTU IP del tunnel in base alle condizioni di trasporto correnti in ciascun sito. Di conseguenza, i valori MTU possono variare da sito a sito e possono variare nel tempo.
    - In questi scenari, un'MTU IP generalmente sicura e consigliata per le interfacce ISE è

compresa tra 1350 e 1400 byte

Una MTU IP di 1350 byte è spesso un punto di partenza molto solido

Configurazione ISE (esempio tramite CLI):

Questo comando viene eseguito sulla CLI dell'appliance Cisco ISE per ciascuna interfaccia di rete rilevante.

<#root>

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

 ip mtu 1350
!
```

Importanti considerazioni operative per le modifiche dell'MTU IP ISE:

- Riavvio del servizio richiesto: se il comando ip mtu viene applicato a un'interfaccia ISE, all'utente viene richiesto di riavviare i servizi dell'applicazione ISE. Si tratta di una modifica che influisce sui servizi e deve essere pianificata durante un intervento di manutenzione pianificato. Per i dettagli procedurali, consultare la documentazione ufficiale di Cisco ISE.
- Applica a tutti i nodi ISE: Questa regolazione dell'MTU IP deve essere applicata in modo coerente a tutti i nodi ISE nell'implementazione (PAN primario, PAN secondario, Policy Service Nodes (PSN)) che comunicano con i NAD nella SD-WAN. Impostazioni MTU incoerenti causano comportamenti imprevedibili.
- Test approfonditi: Prima dell'implementazione in produzione, testare rigorosamente questa modifica in un'installazione di laboratorio o pilota. Utilizzare strumenti come ping con dimensioni dei pacchetti diverse e bit DF impostato per convalidare la gestione dell'MTU end-to-end:
    - Sistemi basati su Linux:

```
ping

        -s

         -M do
```

(Nota: -s specifica le dimensioni del payload ICMP. Dimensioni totali pacchetto IP = payload + 8B (ICMP Hdr + 20B IP Hdr per IPv4)

- Windows:

```
ping

        -f -l
```

(Nota: -l specifica le dimensioni del payload ICMP.)

- Cisco IOS/Cisco IOS-XE®

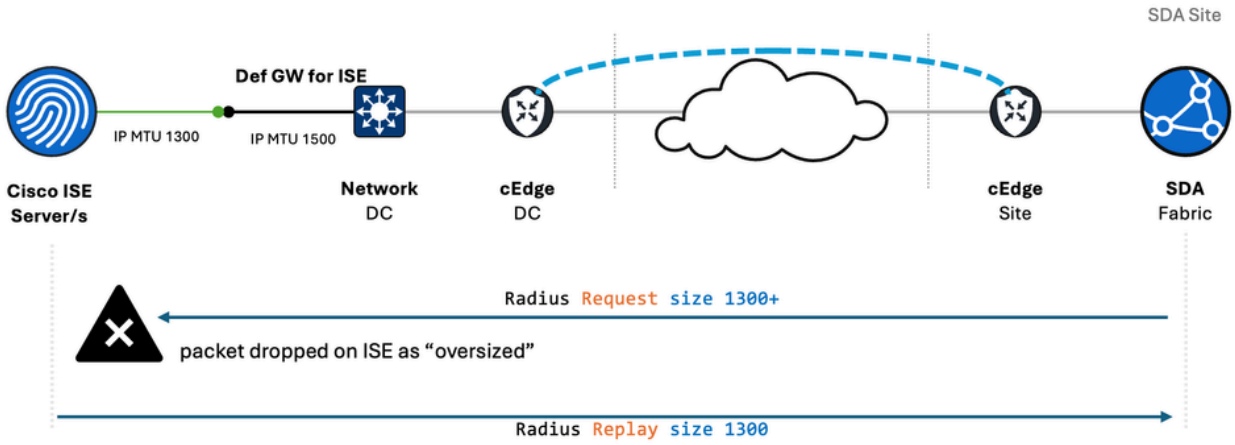
```
ping

        size

         df-bit
```

- ISE First Routing Point: quando si regola il valore MTU IP sull'interfaccia ISE, verificare che anche il primo punto di routing nel data center, in particolare l'interfaccia di layer 3 associata alla subnet ISE, sia configurato con lo stesso valore MTU IP.
  Questo aiuta a prevenire situazioni come quella descritta nella Sfida 1, in cui una mancata corrispondenza MTU fa sì che ISE consideri i pacchetti in arrivo come di dimensioni eccessive e li scarti.
  Ad esempio, se l'interfaccia ISE ha una MTU ridotta (ad esempio, 1300), ma il primo punto di routing rimane configurato con la MTU predefinita di 1500, i pacchetti inviati all'ISE che sono più grandi di 1300 byte ma più piccoli di 1500 byte non vengono frammentati e vengono scartati dall'ISE, come mostrato nella sfida 1.
  Inoltre, accertarsi che il primo punto di routing sia in grado di eseguire la frammentazione, se

necessario, e che questa operazione non determini una riduzione delle prestazioni.

- Aggiornare l'MTU sull'intero percorso di trasmissione e in entrambe le direzioni - quando si aggiornano le impostazioni dell'MTU IP sull'ISE, è importante considerare l'MTU sull'intero percorso di trasmissione e in entrambe le direzioni. Se il valore MTU configurato sull'ISE non è allineato con l'MTU dell'interfaccia di layer 3 del gateway del primo hop, possono verificarsi problemi simili, come descritto nel passaggio 1.

  Ad esempio, se l'MTU ISE è ridotta a 1300 byte e l'MTU predefinita da 1500 byte rimane configurata sul gateway predefinito, i pacchetti di dimensioni comprese tra 1300 e 1500 byte, generalmente generati dai dispositivi di rete, possono essere scartati dall'ISE perché di dimensioni eccessive.



  Per evitare questo problema, verificare sempre che le modifiche MTU sull'ISE vengano riflesse sul gateway del primo hop e, idealmente, su tutti gli host terminali all'interno dello stesso segmento di layer 3. Ciò contribuisce a mantenere la coerenza MTU end-to-end e impedisce la perdita imprevista di pacchetti.

Conclusioni

L'allineamento delle impostazioni MTU IP sui server Cisco ISE con i limiti MTU del livello di trasporto effettivi imposti dall'incapsulamento SD-WAN e dall'allineamento MTU al confine SDA per il trasferimento del router Cisco Edge SD-WAN non è solo una raccomandazione, ma anche un prerequisito critico per garantire la stabilità, l'affidabilità e le prestazioni dei servizi AAA nelle moderne reti aziendali segmentate. Anche se il rilevamento dell'MTU del percorso è un meccanismo importante, la sua efficacia pratica può essere ostacolata da fattori come il filtro ICMP o il Control Plane Policing negli ambienti SD-WAN.

Configurando in modo proattivo una MTU IP ridotta sull'ISE (ad esempio, 1350-1400 byte), i progettisti e i tecnici della rete possono ridurre in modo significativo il rischio di perdite di pacchetti correlate alla MTU, consentendo operazioni di rete più prevedibili e resilienti. Questo è particolarmente importante nelle implementazioni Cisco SDA dove ISE coordina una sofisticata microsegmentazione e l'applicazione dinamica delle policy, che spesso si basano sulla distribuzione efficace di messaggi control-plane potenzialmente grandi. Una pianificazione accurata, test completi e una configurazione coerente su tutti i nodi ISE sono fondamentali per

un'implementazione efficace e senza problemi.

Standard e riferimenti

Per una comprensione più approfondita, consultare gli standard ufficiali e la documentazione Cisco:

RFC:

- RFC 1191: Rilevamento MTU percorso
- RFC 791: Protocollo Internet (IP): definisce l'intestazione IP, incluso il bit "non frammentare" (DF, Do Not Fragment).
- RFC 8200: Specifica IPv6 (rilevante se si utilizza IPv6, include concetti di PMTUD simili).
- RFC 4459: Problemi di MTU e frammentazione con il tunneling in rete (VPN) - Risolve direttamente i problemi di MTU comuni negli ambienti VPN.

Documentazione Cisco:

- Guide alla progettazione e all'installazione Cisco SDA: Per informazioni sui consigli relativi all'MTU dell'infrastruttura e sulle configurazioni dei nodi di confine.
- Guide alla progettazione e alla configurazione Cisco SD-WAN: Per i dettagli sul sovraccarico dell'incapsulamento, l'MTU dell'interfaccia del tunnel e le considerazioni sulla funzionalità PMTUD all'interno del fabric SD-WAN.
- Guide alla configurazione degli switch Cisco Catalyst serie 9000: Per i dettagli specifici della piattaforma sulle impostazioni MTU e le funzionalità di frammentazione.
- Guide per l'amministratore e la CLI di Cisco Identity Services Engine (ISE): Per informazioni sulla configurazione dell'interfaccia, tra cui le implicazioni del comando ip mtu e del riavvio del servizio.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).