SDA 구축을 위해 SD-WAN에서 최적의 ISE IP MTU 구성

목차

소개

이 문서에서는 SD-WAN을 사용하여 SDA 사이트를 연결할 때 MTU(Maximum Transmission Unit) 문제가 SDA의 마이크로 세그멘테이션에 미치는 영향에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소:

이 문서의 정보는 SDA, SDWAN 및 ISE를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

최신 엔터프라이즈 네트워크는 세분화된 마이크로 세그멘테이션 및 일관된 정책 시행을 위해 SDA를 활용하는 경우가 늘고 있습니다. 분산형 SDA 사이트를 연결하기 위해 Cisco SD-WAN을 사용하는 경우가 많습니다. Cisco SD-WAN은 다양한 언더레이 네트워크를 통해 민첩하고 안전하며 최적화된 전송을 제공합니다. 이 아키텍처의 핵심인 ISE는 동적 정책 배포(예: SGT(Security Group Tag) 및 다운로드 가능한 ACL)와 함께 중요한 AAA(Authentication, Authorization, and Accounting) 서비스를 제공합니다.

이와 같이 강력한 기술을 통합하면 강력하면서도 미묘하면서도 강력한 구성 과제를 해결할 수 있습니다. 중요한 네트워크 핸드오프 포인트에서 그리고 SD-WAN 오버레이에서 MTU를 처리하는 것이 이러한 문제의 주요 영역입니다. 이 문서에서는 네트워크 운영을 중단시킬 수 있는 두 가지 일반적인 MTU 불일치 시나리오를 다룹니다.

1. SDA 경계 노드와 SD-WAN 에지 디바이스 간의 MTU 간격.
2. SD-WAN 오버레이를 통과하는 ISE 발생 트래픽에 대한 MTU 제약 조건.

패킷 조각화 문제 또는 자동 삭제를 방지하려면 올바른 MTU 정렬이 가장 중요하며, 이를 통해 신뢰할 수 있는 인증, 정책 적용 및 전반적인 네트워크 안정성을 보장합니다. 이러한 문제를 해결하지 못하면 간헐적인 연결 및 정책 적용 실패가 발생하여 상당한 트러블슈팅 작업이 소모될 수 있습니다.

MTU 불일치의 일반적인 증상

잘못 조정된 MTU는 다양한 방법으로 나타날 수 있으며, 진단하기 어려운 문제가 발생하는 경우가 많습니다.

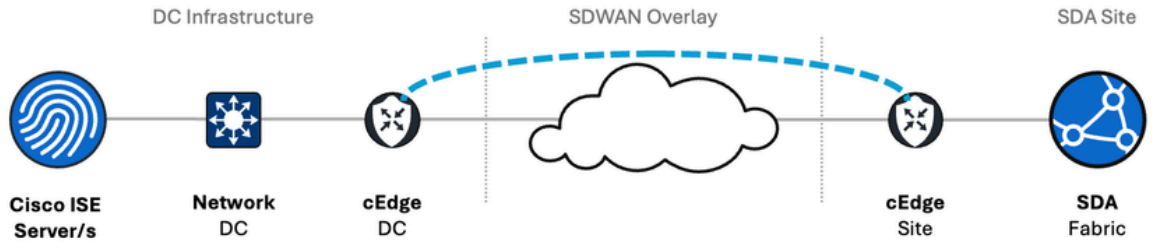
- 간헐적 RADIUS 인증 실패 또는 시간 초과: 더 큰 RADIUS 패킷을 생성하는 정책에서 특히 두드러집니다(예: 광범위한 AV 쌍 또는 인증서가 있는 정책).
- 엔드포인트에서 dACL(downloadable ACL) 또는 TrustSec 정책(SGT/SGACL)을 수신 또는 적용하지 못함: 이러한 정책은 대개 큰 RADIUS 패킷에서 전달됩니다.
- 인증된 클라이언트에 대한 느린 세션 설정: 애플리케이션 레이어에서 재전송되기 때문입니다.
- 과도한 RADIUS 재전송: ISE 로그 또는 NAD(Network Access Device)에서 확인 가능합니다.
- 일관성 없는 정책 전파: ISE에서 이루어진 정책 변경은 원격 SDA 사이트의 모든 NAD에 일관되게 전파되지 않을 수 있습니다.
- 패킷 캡처 불일치: 캡처는 DF(Do Not Fragment) 비트 세트가 있지만 NAD 또는 SD-WAN Cisco Edge Router에서 해당 응답 또는 ICMP "Fragmentation Needed" 오류가 없는 대규모 패킷(예: >1450바이트)을 전송하는 ISE를 표시할 수 있습니다.
- 패킷 삭제 카운터 증가: SDA 사이트로 향하는 ISE에서 소싱되는 트래픽에 대한 DC(Data Center) Cisco Edge Router의 인그레스(ingress) 인터페이스 또는 반대 방향의 트래픽에 대한 SDA 경계를 향하는 SD-WAN Cisco Edge Router 인터페이스에서 관찰되었습니다.

문제 설명

일반적인 엔터프라이즈 구축
공통 엔터프라이즈 토폴로지를 고려하십시오.

- Cisco ISE 서버: 중앙 집중식 DC(데이터 센터) 또는 지역 허브에 구축되며 DC 네트워크 인프라에 연결됩니다.
- DC 인프라: ISE 서버가 연결되는 DC 코어 또는 어그리게이션 스위치로 구성됩니다.
- SD-WAN 오버레이: DC Cisco Edge Router는 원격 SDA 사이트의 Cisco Edge Router 라우터에 언더레이 전송 네트워크(예: 인터넷, MPLS)를 통해 SD-WAN 터널(일반적으로 IPsec)을 설정합니다.
- SDA 사이트: 원격 사이트 Cisco Edge Router 라우터는 로컬 SDA 패브릭에 연결되며 여기에는 패브릭 에지 노드, 보더 노드, WLC(Wireless LAN Controller), 궁극적으로는 엔드포인트가 포함됩니다.

실례가 되는 토폴로지



과제 1: MTU 간격 - SD-WAN 에지에 대한 SDA 경계

LAN 자동화를 통해 구현되는 경우가 많은 Cisco SDA 설계 원칙은 모든 패브릭 디바이스에서 캠퍼스 차원의 MTU 9100바이트(점보 프레임)를 촉진합니다. 여기에는 Catalyst 9000 Series Border Node가 포함되며, 패브릭 내에서 이더넷 점보 프레임이 효율적으로 전송됩니다. 따라서 SDA 경계 노드의 레이어 3 또는 SVI 핸드오프 인터페이스는 이 더 큰 MTU를 기본값으로 설정합니다.

반대로 Catalyst 8000 Series와 같은 SD-WAN 에지 디바이스는 일반적으로 인터페이스 MTU가 1500바이트로 기본 설정됩니다. 점보 프레임 지원이 일반적이지 않거나 활성화되지 않은 ISP(Internet Service Provider)와 같은 외부 네트워크에 연결하는 인터페이스에 표준입니다.

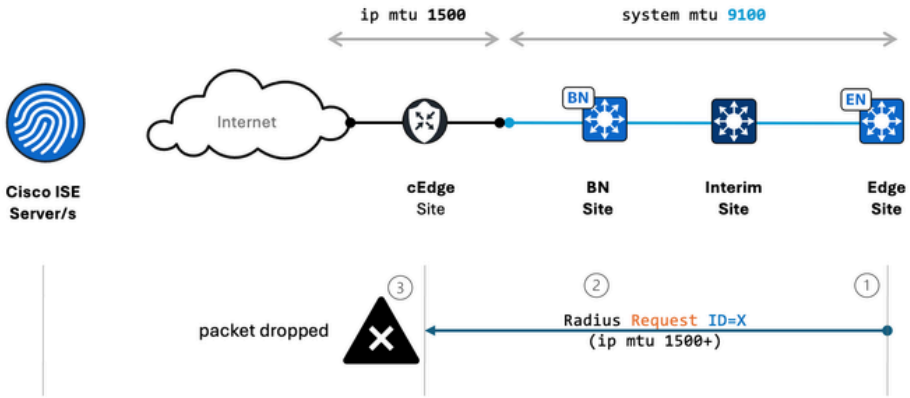
이러한 차이로 인해 장애가 발생할 수 있습니다. 수신 인터페이스가 1500바이트 MTU로 구성된 SD-WAN 에지에 1500바이트보다 큰 IP 패킷을 전송하려고 시도하는 SDA 경계입니다.

이러한 유형의 MTU 불일치는 SDA 구축에서 흔히 발생하는 문제이며 컨피그레이션 중에 간과하기 쉬운 경우가 많습니다. 더욱 어려운 점은 Cisco IOS-XE®를 실행하는 Catalyst 9000 스위치에서 RADIUS 요청이 생성되는 방식과 관련된 특정 동작이 특정 및 중요한 조건에서만 이러한 문제를 표면화할 수 있다는 것입니다.

예를 들어, SMD(Session Manager Daemon) 프로세스에서 처리하는 최종 사용자 인증 프로세스 중에 생성된 RADIUS 요청은 1396바이트로 패킷을 조각화하도록 하드코딩됩니다. 이와 달리 SGACL(Security Group Access Control List)과 같은 TrustSec 정책 검색과 관련된 RADIUS 요청은 Cisco IOSd(Internetworking Operating System daemon) 하위 구성 요소에 의해 생성됩니다. 이는 MTU를 인식하며 패킷 크기가 시스템 MTU(일반적으로 최대 9100바이트)를 초과하지 않는 한 패킷 단편화를 방지할 수 있습니다.

따라서 MTU 불일치와 관련된 문제는 CTS(Cisco TrustSec) 다운로드 정책이 사용 중인 경우에만 명확해집니다. 또한 사용자 인증 중에 SDA 에지 디바이스에서 다운로드한 RBACL(Role-Based Access Control List) 세트는 다른 태그에 대해 어떤 SGACL 정책이 이미 존재하는지에 따라 달라질 수 있습니다. 실제로 스위치는 정책 세트의 겹치지 않는 부분만 다운로드합니다.

이러한 행동은 함께 SGACL 정책의 크기, 현재 시스템 조건, 그리고 궁극적으로 경로를 따라 MTU 오정렬에 따라 무음 실패에서 불완전한 정책 다운로드까지 예측할 수 없고 일관되지 않은 결과를 낳을 수 있습니다.



SDA Border는 SD-WAN 에지를 통해 ISE로 큰 RADIUS 패킷(예: 1600바이트)을 전달하며, 이는 다음과 같습니다.

1. SDA Border는 9100 MTU 인터페이스가 있으며 1600바이트 IP 패킷을 전송합니다.
2. SD-WAN Cisco Edge 라우터는 1500 MTU 인터페이스에서 이 패킷을 수신합니다.
3. 그러나 DF(Do Not Fragment) 비트가 이러한 RADIUS 패킷에 설정되어 있지 않으면 SD-WAN Cisco Edge Router는 구성된 인터페이스 MTU에 비해 "오버사이즈"라는 이유만으로 인그레스(ingress) 시 이를 삭제할 수 있습니다. DF 비트가 허용하는 경우 프래그먼트화를 고려할 수 있는 IP 포워딩 논리의 단계에는 도달하지 않습니다.

이러한 무음 삭제는 특히 문제가 방향성(SDA에서 SD-WAN/ISE로)이므로 심각한 트러블슈팅 문제를 초래합니다.

DC(데이터 센터) 코어 또는 리프 스위치에서도 유사한 MTU 불일치가 발생할 수 있습니다. 이 스위치는 내부 DC 트래픽 효율성을 높이기 위해 점보 프레임(예: MTU 9000+)을 지원하도록 일반적으

로 구성됩니다. 그러나 트래픽이 표준 MTU(예: 1500바이트)로 구성된 SD-WAN DC Cisco Edge Router 라우터의 LAN 연결 인터페이스로 전달되는 경우, 이러한 불일치로 인해 특히 DC 네트워크에서 SD-WAN 패브릭으로 이동하는 트래픽의 경우 프래그먼트화나 패킷 삭제가 발생할 수 있습니다.

과제 1:

SDA Border의 핸드오프 인터페이스(물리적 또는 SVI)의 IP MTU를 피어링 SD-WAN Cisco Edge Router 인터페이스(일반적으로 1500바이트)에 맞춥니다.

컨피그레이션 예(SDA Border Node):

<#root>

```
!
interface Vlan3000  // Or your physical handoff interface, for example, TenGigabitEthernet1/0/1
 description Link to SD-WAN cEdge Router
 ip address 192.168.100.1 255.255.255.252
```

ip mtu 1500

```
  // Align with SD-WAN cEdge receiving interface MTU
!
```

중요한 고려 사항: Catalyst 9000 경계의 단편화

Catalyst 9000 Series 스위치는 SDA Border Node로서 하드웨어 데이터 평면의 네이티브 IP 패킷에 대한 IP 단편화를 지원합니다. 전달 인터페이스의 ip mtu를 1500으로 줄이면 이를 필요로 하는 경계에서 시작되거나 통과하는 트래픽에 대한 소프트웨어 기반 프래그먼트화로 인한 성능 저하가 발생하지 않습니다. 이 스위치는 CPU에 펀트하지 않고 이 특정 인터페이스를 이그레스(egress)하기 전에 1500바이트보다 큰 IP 패킷을 효율적으로 프래그먼트화합니다(DF 비트가 분명한 경우).

그러나 Catalyst 9000 스위치는 일반적으로 VXLAN 캡슐화된 트래픽의 단편화를 지원하지 않습니다. 이 제한은 오버레이 트래픽에 중요하지만 SDA 보더와 외부 ISE 간의 RADIUS 통신이 일반적으로 언더레이(네이티브 IP 라우팅) 내에서 발생하므로 설명된 RADIUS 인증 시나리오에 영향을 주지 않습니다. VXLAN 오버레이에 대한 MTU 고려 사항은 별도의 복잡한 주제이며 관련 Cisco SDA 설계 가이드에서 자세히 설명합니다.

SDA 경계에서 SD-WAN Cisco Edge Router로의 사전 대응적 MTU 조정은 필수적입니다.

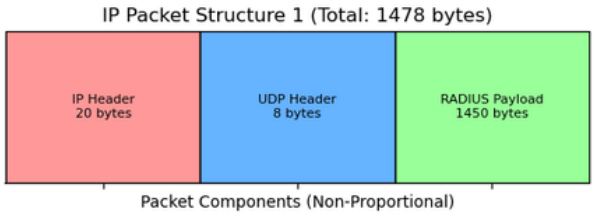
과제 2: MTU 스퀴즈 - SD-WAN 오버레이의 ISE 트래픽

ISE NIC(Network Interface Card), 스위치 포트 또는 라우터 인터페이스와 같은 개별 물리적 인터페이스가 표준 1500바이트 IP MTU로 설정된 경우에도 SD-WAN 오버레이 자체에 캡슐화 오버헤드가 생깁니다. 이 오버헤드는 1500바이트 제한의 일부를 소비하므로 원래 IP 패킷에 사용 가능한 유효 MTU(ISE의 관점에서 "페이로드")가 감소합니다.

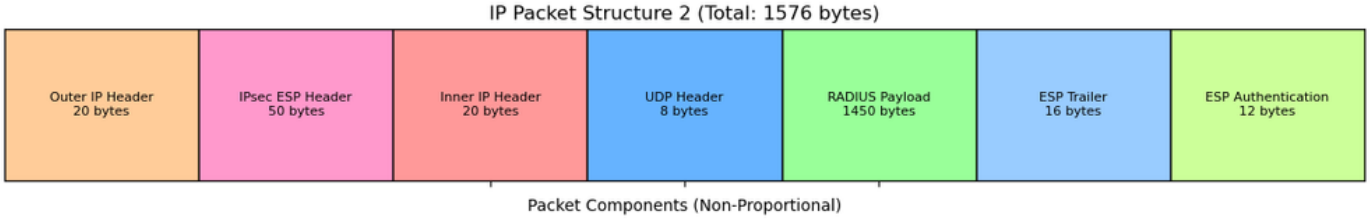
패킷 구조 및 캡슐화 오버헤드:

ISE 서버의 IP 패킷(예: RADIUS Access-Accept 패킷)이 SDA 사이트의 NAD(Network Access Device)에 전송될 때 SD-WAN 오버레이를 통과하여 캡슐화됩니다. 공통 캡슐화 스택은 터널 모드에서 IPsec을 포함하며, 잠재적으로 NAT-T(NAT traversal)를 위해 UDP를 통해 수행됩니다.

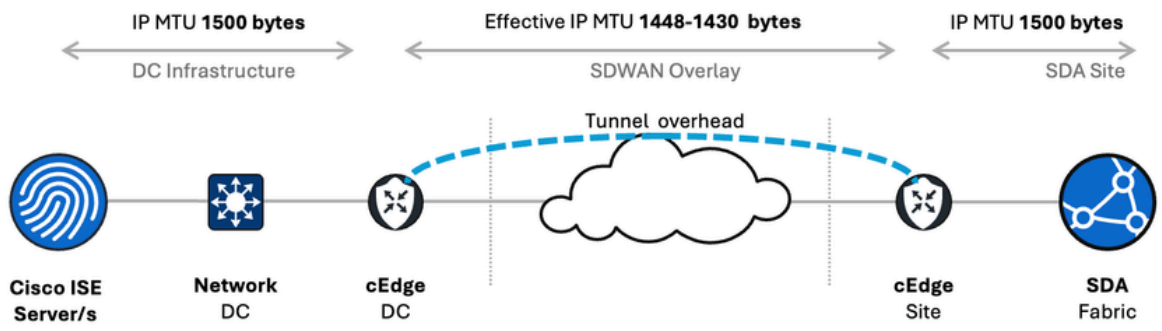
- ISE의 원래 패킷(내부 패킷):
  예를 들어, 1450바이트 페이로드 + 8B UDP + 20B 내부 IP = 1478바이트의 RADIUS 패킷입니다.



- 터널 모드에서 IPsec ESP를 고려하십시오. 잠재적으로 NAT-T에 대한 UDP 캡슐화를 사용할 수 있습니다.



- 총 오버헤드는 특정 IPsec 암호, 인증 메커니즘 및 기타 오버레이 기능(예: GRE 사용)에 따라 달라질 수 있습니다. 일반적인 계산:
  - 외부 IP 헤더(IPv4): 20바이트
  - UDP 헤더(NAT-T에 대해 ESP over UDP인 경우): 8바이트
  - ESP 헤더: ~8바이트
  - ESP IV(예: AES-CBC): ~16바이트(해당되는 경우)
  - ESP 인증(예: HMAC-SHA256 잘림): ~12-16바이트
  - 일반적인 예상 IPsec 오버헤드: ~52-70바이트(모든 옵션을 사용할 경우 최대 ~80바이트 이상 더 높을 수 있음).



물리적 링크 MTU가 1500바이트이면 ISE의 원래 IP 패킷에 사용 가능한 페이로드 MTU는 다음과 같이 됩니다. 1500바이트 - SD-WAN 오버헤드.
예를 들어 1500 - 70 = 1430바이트입니다.

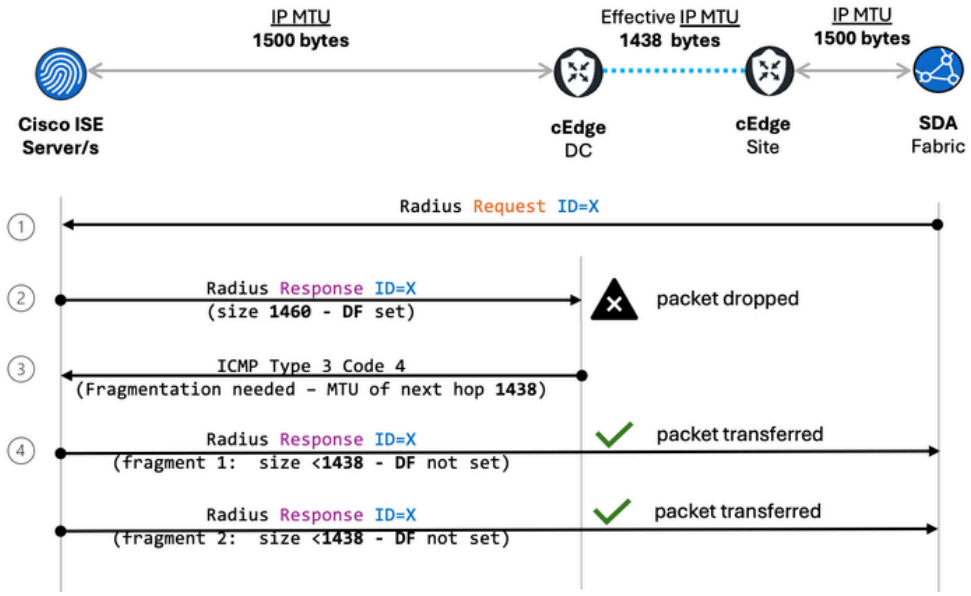
패킷이 유효 MTU를 초과하는 경우의 동작:

1. ISE에서 패킷(DF 비트 이상) 시작:
   - 기본적으로 ISE 어플라이언스의 기본 Linux 운영 체제는 생성된 모든 패킷의 IP 헤더에 구성된 인터페이스 IP MTU(예: 1500바이트)보다 작거나 같은 DF(Do Not Fragment)를 설정합니다.
   - 이 DF 비트의 목적: ISE는 (OS를 통해) DF 비트를 주도적으로 설정하여 PMTUD(Path MTU Discovery) 프로세스를 활용합니다. 이에 대해서는 나중에 설명합니다. 이렇게 하면 ISE가 자체 인터페이스 MTU보다 작은 경우 대상에 대한 실제 PMTU를 동적으로 학습할 수 있습니다.
   - 인터페이스 MTU보다 큰 패킷에 대한 동작: ISE가 구성된 인터페이스 IP MTU보다 큰 IP 패킷을 전송해야 하는 경우, 동작은 Linux 운영 체제에 따라 달라집니다. 일반적으로 OScanfragment the packetbeforetransmission 및 이러한 결과 프래그먼트에 대한 DF 비트(설정 DF=0)를 지웁니다. 이 프래그먼트화는 ISE 애플리케이션 코드 자체에 의해 직접 구동되지 않는 OS 레벨 기능입니다.
   - 네트워크 디바이스와의 주요 차이점: ISE의 이 기본 동작(인터페이스 MTU 내에 피팅되는 프래그먼트화되지 않은 패킷에 대해서도 DF=1 설정)은 많은 기존 네트워킹 디바이스(라우터, 스위치)와 크게 다릅니다. 네트워크 디바이스는 명시적으로 구성되지 않는 한, 또는 전달 중인 패킷에 이미 DF 비트가 설정되어 있거나 이를 요구하는 특정 프로토콜에 대해 DF 비트가 설정되어 있는 경우, DF 비트를 시작하거나 전달하는 패킷에서 DF 비트를 설정하지 않는 경우가 많습니다. 일반적으로 패킷은 다음 홉 MTU(및 DF=0)를 초과할 경우 기본적으로 프래그먼트화를 허용합니다.
   - 문제 해결 복잡성: ISE-to-NAD 트래픽은 DF=1인 경우가 많은 반면, NAD-to-ISE 트래픽은 DF=0인 경우가 많습니다(NAD에서 어떤 이유로 설정하지 않는 한). 이러한 비대칭성은 문제 해결 중에 추가적인 복잡성 계층을 유발할 수 있습니다. 엔지니어는 트래픽 흐름의 방향에 따라 다양한 프래그먼트화 동작 및 PMTUD 상호 작용을 관찰할 수 있습니다.
2. 패킷이 인그레스 Cisco Edge Router(DC)에 도달함: DC Cisco Edge Router는 ISE에서 IP 패킷을 수신합니다.
3. Cisco Edge Router의 캡슐화 및 MTU 확인: Cisco Edge Router는 SD-WAN 터널용 패킷을 캡슐화하려고 시도합니다.

- 원래 패킷의 크기가 플러스되고 SD-WAN 캡슐화 오버헤드가 Cisco Edge Router의 아웃바운드 물리적 인터페이스 MTU(예: 1500바이트)를 초과하며 DF 비트가 ISE의 원래(내부) 패킷에 설정된 경우, Cisco Edge Router는 내부 패킷을 프래그먼트화하지 않아야 합니다.
- Cisco Edge Router에서 패킷을 삭제해야 합니다.
- 또한 Cisco Edge Router는 다음 홉의 MTU(터널의 유효 MTU)를 나타내는 ICMP "Destination Unreachable - Fragmentation Needed and DF bit set"(Type 3, 코드 4) 메시지를 소스(ISE)로 다시 보내야 합니다.

4. 경로 MTU 검색(PMTUD) 프로세스: 이 ICMP "Fragmentation Needed(조각화가 필요함)" 메시지를 수신하면 ISE(소스 OS)는 해당 특정 대상 경로에 대한 PMTU 추정치를 줄여야 합니다. 이 정보는 캐시되며 새로 검색된 PMTU에 맞는 더 작은 패킷으로 데이터를 재전송합니다.

PMTUD 프로세스 다이어그램:



PMTUD 통신이 중단되는 경우:
PMTUD는 이론상 강력하지만 실제로는 실패할 수 있습니다.

- ICMP 필터링: 중간 방화벽 또는 보안 정책은 종종 ICMP 메시지를 차단하여 "Fragmentation Needed" 메시지가 ISE에 도달하지 못하게 합니다.

- Cisco 에지 라우터의 CoPP(Control Plane Policing): Cisco Edge 라우터 라우터는 CoPP를 사용하여 CPU를 보호합니다. ICMP 오류 메시지 생성은 컨트롤 플레인 작업입니다. 로드가 많거나 크기가 큰 패킷이 많은 경우 CoPP는 ICMP 생성을 속도 제한하거나 삭제할 수 있습니다. ISE는 피드백을 받지 않습니다.

- 자동 삭제: ISE는 ICMP "Fragmentation Needed(조각화가 필요함)" 메시지를 수신하지 못하면 경로 제한을 알지 못합니다. DF 비트가 설정된 대용량 패킷을 계속 전송하므로 인그레스 Cisco Edge Router에서 무음으로 패킷을 삭제합니다. 그러면 애플리케이션 레이어 시간 초과 및 재전송(예: RADIUS)이 발생합니다.

- ISE 서비스에 미치는 영향: 대규모 RADIUS 액세스 수락 패킷(dACL, 광범위한 AVP, SGT 정보 전달)은 특히 민감합니다. 매니페스트에는 다음이 포함됩니다.

- 간헐적이거나 완전한 인증 실패입니다.
- 엔드포인트가 올바른 네트워크 액세스 정책 또는 SGT를 수신하지 않습니다.
- ISE와 NAD 간의 정책 동기화가 완료되지 않았거나 실패했습니다.

당면 과제 2: 사전 대응적 ISE IP MTU 컨피그레이션

PMTUD의 신뢰성이 떨어지면 ISE와 같은 중요한 서비스에 대해 사전 대응적 접근 방식이 가장 적합합니다. ISE의 네트워크 인터페이스에서 IP MTU를 최대 예상 SD-WAN 오버레이 오버헤드를 안전하게 수용하는 값으로 구성합니다. 이렇게 하면 ISE가 중간 디바이스에 의한 프래그먼트화 없이 SD-WAN 오버레이를 통과하기에 너무 큰(DF=1인 경우 금지됨) IP 패킷(DF 비트 세트 포함)을 시작하지 않습니다.

권장 ISE IP MTU 계산 및 설정:

1. 기본 물리적 MTU 설정: 경로를 따라 표준 이더넷 인터페이스의 경우 일반적으로 1500바이트입니다.
2. 최대 SD-WAN 캡슐화 오버헤드 결정:
   - 특정 SD-WAN 오버레이(IPsec, GRE, VXLAN, MPLSoGRE 등)에서 발생하는 총 오버헤드를 정확하게 계산하거나 신중하게 추정합니다. 선택한 프로토콜 및 옵션에 대한 정확한 수치는 공급업체 설명서를 참조하십시오.

구성 요소	오버헤드 예(바이트)	참고
기본 물리적 MTU	1500	물리적 링크의 표준 이더넷
절감: SD-WAN 오버헤드		
외부 IP 헤더(IPv4)	20	
UDP 헤더(NAT-T용)	8	ESP가 UDP로 캡슐화된 경우
ESP 헤더	~8-12	
ESP IV(예: AES-CBC)	~16	암호화 알고리즘에 따라 다름
ESP 인증(예: SHA256)	~12-16	인증 알고리즘에 따라 다름(예: 일부는 96비트)
기타 오버레이(GRE 등)	변수	SD-WAN 캡슐화 스택의 일부인 경우 추가
총 예상 오버헤드	~68~80바이트 이상	구축과 관련된 모든 구성 요소의 합계
유효 경로 MTU	~1432 - 1420바이트	기본 물리적 MTU - 총 예상 오버헤드

3. 권장 ISE IP MTU 구성:
   - 계산된 유효 경로 MTU를 가져옵니다(예: 에에서 1420바이트).
   - 미계상 L2 헤더를 계산하거나 버퍼를 제공하기 위해 추가 안전 마진(예: 20-70바이트)을 뺍니다.
   - Cisco SD-WAN과 같은 솔루션은 각 사이트 간 터널에 대해 개별적으로 경로 MTU(PMTU) 검색을 수행할 수 있습니다. 이 메커니즘은 20분마다 자동으로 실행되어 각 사이트의 현재 전송 조건에 따라 터널의 IP MTU를 테스트하고 동적으로 조정합니다. 따라서 MTU 값은 사이트 간에 다를 수 있으며 시간이 지남에 따라 변경될 수 있습니다.
   - 이러한 시나리오에서 ISE 인터페이스에 대해 일반적으로 안전하고 권장되는 IP MTU는 1350~1400바이트입니다

IP MTU 1350바이트는 매우 강력한 시작점입니다

ISE 컨피그레이션(예: CLI):

이 명령은 Cisco ISE 어플라이언스 CLI에서 각 관련 네트워크 인터페이스에 대해 실행됩니다.

```
<#root>

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

 ip mtu 1350

!
```

ISE IP MTU 변경에 대한 중요한 운영 고려 사항:

- 서비스 재시작 필요: ip mtu 명령이 ISE 인터페이스에 적용되면 사용자에게 ISE 애플리케이션 서비스를 재시작하라는 프롬프트가 표시됩니다. 이는 서비스에 영향을 미치는 변경이며, 계획된 유지 관리 기간 중에 예약해야 합니다. 절차 세부 사항은 공식 Cisco ISE 문서를 참조하십시오.
- 모든 ISE 노드에 적용: 이 IP MTU 조정은 SD-WAN을 통해 NAD와 통신하는 구축의 모든 ISE 노드(기본 PAN, 보조 PAN, PSN(Policy Service Node))에 일관되게 적용해야 합니다. MTU 설정이 일치하지 않으면 예측할 수 없는 동작이 발생합니다.
- 철저한 테스트: 프로덕션 환경에서 구현하기 전에 랩 또는 파일럿 구축에서 이 변경 사항을 엄격하게 테스트합니다. 다양한 패킷 크기와 DF 비트가 설정된 ping과 같은 툴을 사용하여 엔드 투 엔드 MTU 처리를 검증합니다.
    - Linux 기반 시스템:

```
ping

        -s

         -M do
```

(참고: -s는 ICMP 페이로드 크기를 지정합니다. 총 IP 패킷 크기 = 페이로드 + 8B ICMP Hdr + IPv4용 20B IP Hdr)

- 창:

```
ping

        -f -l
```

(참고: -l ICMP 페이로드 크기를 지정합니다.)

- Cisco IOS/Cisco IOS-XE®

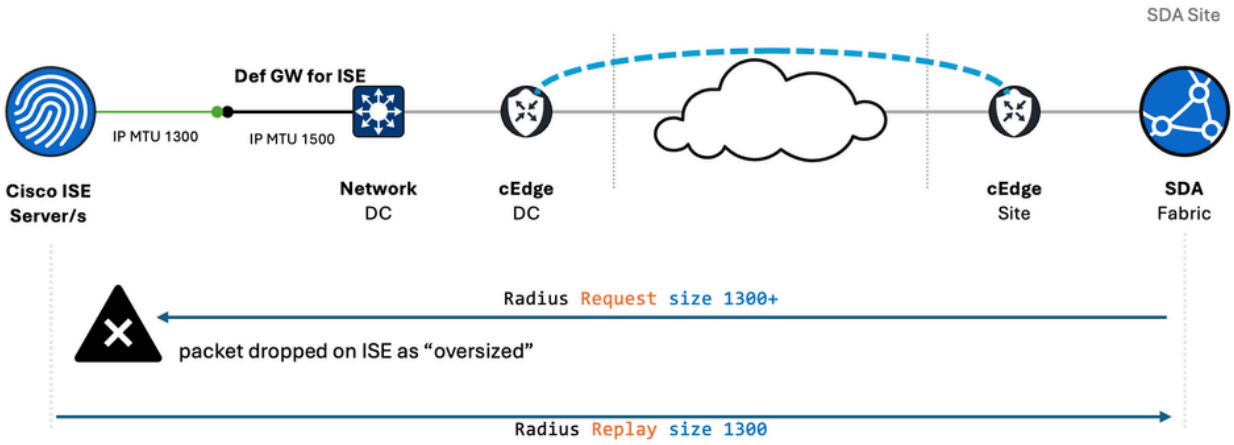
```
ping

        size

         df-bit
```

- ISE First Routing Point - ISE 인터페이스에서 IP MTU 값을 조정할 때 데이터 센터의 첫 번째 라우팅 포인트, 특히 ISE 서브넷과 연결된 레이어 3 인터페이스도 동일한 IP MTU 값으로 구성되어야 합니다.
  이렇게 하면 MTU 불일치로 인해 ISE가 수신 패킷을 오버사이징으로 간주하고 삭제하는 Challenge 1에 설명된 것과 같은 상황을 방지할 수 있습니다.
  예를 들어, ISE 인터페이스의 MTU가 감소했지만(예: 1300) 첫 번째 라우팅 포인트가 기본 MTU인 1500으로 구성된 상태로 남아 있는 경우, 1300바이트보다 크지만 1500바이트보다 작은 ISE로 전송된 패킷은 프래그먼트화되지 않으며 ISE에서 폐기됩니다. Challenge 1에서 관찰된 내용입니다.
  또한 필요한 경우 첫 번째 라우팅 포인트에서 프래그먼트화를 수행할 수 있는지, 그렇게 해도 성능이 저하되지 않는지 확인합니다.
- 전체 전송 경로 및 양방향으로 MTU 업데이트 - ISE에서 IP MTU 설정을 업데이트할 때는 전체 전송 경로 및 양방향으로 MTU를 고려하는 것이 중요합니다. ISE에 구성된 MTU 값이 첫 번째 홉 게이트웨이의 레이어 3 인터페이스에 있는 MTU와 일치하지 않을 경우, Challenge #1에 설명된 것과 유사한 문제가 발생할 수 있습니다.

예를 들어 기본 1500바이트 MTU가 기본 게이트웨이에 구성된 상태로 유지되는 동안 ISE MTU가 1300바이트로 축소되면, 일반적으로 네트워크 디바이스에서 생성되는 1300바이트와 1500바이트 사이의 패킷은 ISE에서 오버사이징으로 삭제될 수 있습니다.



이 문제를 방지하려면 항상 ISE의 MTU 변경 사항이 첫 번째 홉 게이트웨이에 미러링되고, 이상적으로는 동일한 레이어 3 세그먼트 내의 모든 종단 호스트에 반영되도록 해야 합니다. 이를 통해 엔드 투 엔드 MTU 일관성을 유지하고 예기치 않은 패킷 삭제를 방지할 수 있습니다.

결론

Cisco ISE 서버의 IP MTU 설정을 SD-WAN 캡슐화 및 SDA 경계에서 SD-WAN Cisco Edge Router 핸드오프에 적용된 효과적인 전송 레이어 MTU 제한과 일치시키는 것은 현대적이고 세분화된 엔터프라이즈 네트워크에서 AAA 서비스의 안정성, 안정성 및 성능을 보장하기 위한 중요한 전제조건일 뿐 아니라 중요한 전제조건입니다. 경로 MTU 검색은 중요한 메커니즘이지만, SD-WAN 환경의 ICMP 필터링 또는 제어 평면 정책과 같은 요인으로 인해 그 실질적인 효과가 저해될 수 있습니다.

네트워크 설계자와 엔지니어는 ISE에서 감소된 IP MTU(예: 1350-1400바이트)를 사전 대응적으로 구성함으로써 MTU 관련 패킷 삭제의 위험을 크게 완화할 수 있으며, 이는 네트워크 운영의 예측 가능성과 복원력을 향상시킵니다. 이는 ISE가 정교한 마이크로 세그멘테이션 및 동적 정책 시행을 오케스트레이션하는 Cisco SDA 구축에서 특히 중요하며, 대규모의 제어 평면 메시지의 성공적인 전달에 의존하는 경우가 많습니다. 모든 ISE 노드에서 성실한 계획, 포괄적인 테스트, 일관된 컨피그레이션이 성공적이고 문제 없는 구축의 핵심입니다.

표준 및 참조

자세한 내용은 공식 표준 및 Cisco 설명서를 참조하십시오.

RFC:

- RFC 1191: 경로 MTU 검색
- RFC 791: IP(Internet Protocol) - DF(Do Not Fragment) 비트를 포함하여 IP 헤더를 정의합니다.

- RFC 8200: IPv6 사양(IPv6를 사용하는 경우 관련, 유사한 PMTUD 개념 포함).
- RFC 4459: VPN(In-the-Network Tunneling)의 MTU 및 프래그먼트화 문제 - VPN 환경에서 일반적인 MTU 문제를 직접 해결합니다.

Cisco 설명서:

- Cisco SDA 설계 및 구축 설명서: 패브릭 MTU 권장 사항 및 보더 노드 컨피그레이션에 대한 자세한 내용
- Cisco SD-WAN 설계 및 컨피그레이션 가이드: 캡슐화 오버헤드, 터널 인터페이스 MTU, SD-WAN 패브릭 내 PMTUD 고려 사항에 대한 자세한 내용을 보려면
- Cisco Catalyst 9000 Series 스위치 컨피그레이션 가이드: MTU 설정 및 조각화 기능에 대한 플랫폼별 세부 정보
- Cisco ISE(Identity Services Engine) 관리자 및 CLI 가이드: 인터페이스 컨피그레이션에 대한 자세한 내용은 ip mtu 명령 및 서비스 재시작과 관련된 사항을 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.