Expressway에서 XMPP 페더레이션 구성 및 문제 해결

목차

소개

이 문서에서는 Expressway에서 XMPP(Extensible Messaging and Presence Protocol) 페더레이션의 구성 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

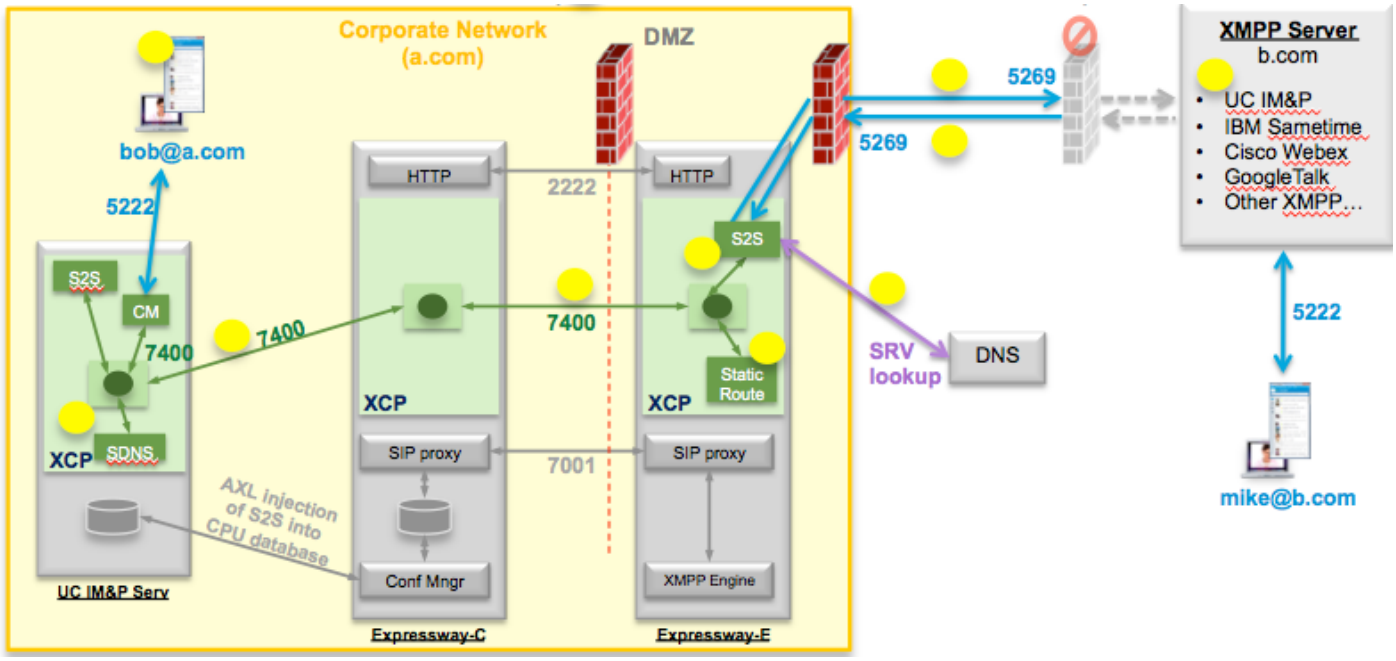
- Cisco Expressway X8.2 이상
- CM(Unified Call Manager) IM(Instant Message) 및 Presence Service 9.1.1 이상

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

잠재적인 영향을 이해해야 합니다.

배경 정보

다음 다이어그램은 상위 수준 통신을 보여줍니다.



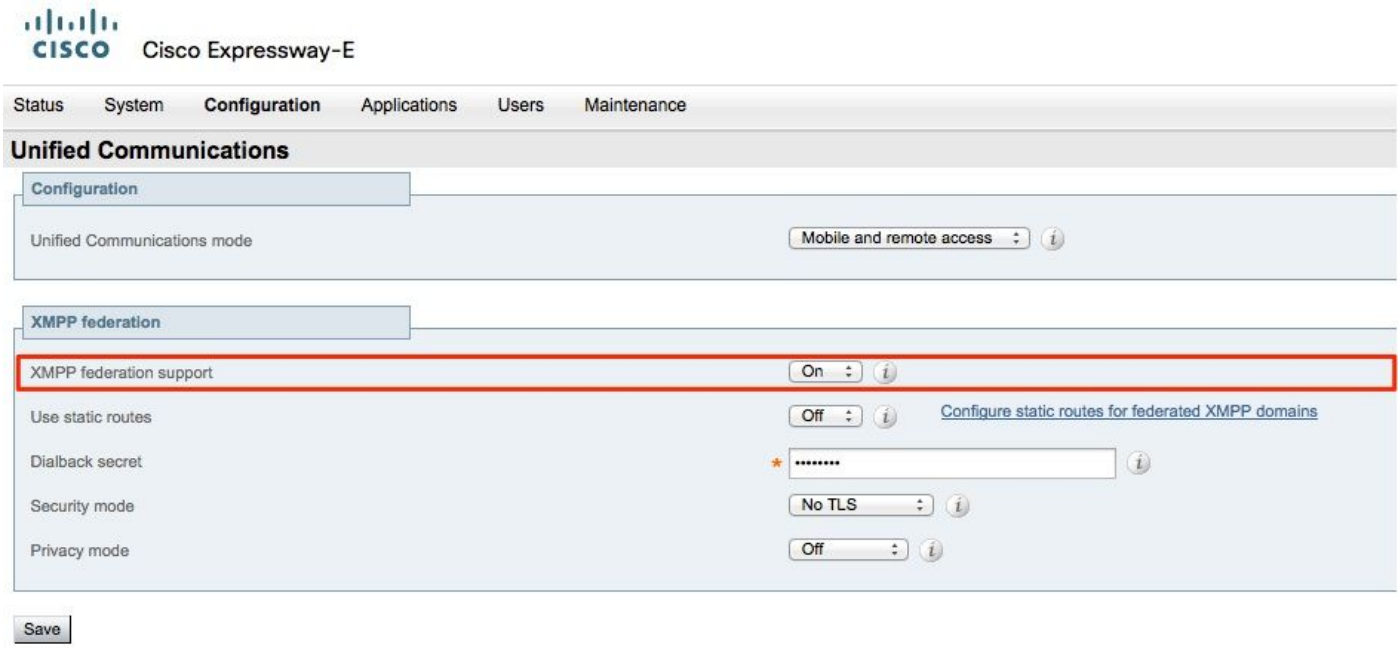
Expressway에서 XMPP Federation을 활성화하면 활성 서버가 Cisco Unified Presence(CUP)에서 Expressway Edge(Expressway E)로 이동합니다. 이 구성 요소는 페더레이션 도메인 간의 모든 XMPP 통신을 관리합니다.

- S2S는 포트 5269를 사용하여 페더레이션 도메인과 통신
- ExpresswayE, C 및 CUP의 XCP 라우터 간 내부 XMPP 트래픽은 포트 7400에서 실행됩니다.
- Expressway E의 XMPP 프로비저닝 정보는 포트 2222의 SSH 터널을 통해 Expressway C로 전송됩니다.
- Expressway C는 AXL 포트 8443을 통해 필요한 라우팅 정보로 CUP를 업데이트합니다.

구성

1단계. Expressway E에서 XMPP 페더레이션 사용

Configuration(구성) > Unified Communication(통합 커뮤니케이션) > XMPP 페더레이션 지원 > 켜기



XMPP 페더레이션을 활성화하면 다음과 같은 결과가 표시됩니다.

1. Expressway-E는 로컬 구성을 업데이트하고 Expressway Core(Expressway C)를 사용하여 이 설정을 복제합니다.

Expressway E 로그에는 다음이 표시됩니다. "Detail="xconfiguration xcpConfiguration is_federation_enabled - 다음에서 변경됨:0 ~:1"

2. Expressway-C는 CUP 데이터베이스의 "xmpps2snodes" 테이블을 Expressway E S2S 구성 요소의 영역으로 업데이트합니다.

Expressway C 로그에는 다음이 표시됩니다. "Module="network.axl" Level="INFO" Action="Send" URL="https://cups.ciscotac.net:8443/axl/" Function="executeSQLQuery"

3. 페더레이션이 필요한 모든 도메인에 대한 XMPP 서버 SRV 레코드로 공용 DNS가 업데이트되었는지 확인합니다.

포트 5269의 _xmpp-server._tcp.domain.com

Expressway에서 XMPP 컨피그레이션 확인

1단계. CUP CLI(Command Line Interface)에서 이 쿼리를 실행하여 IM&P 서버에서 데이터베이스 변경 내용을 성공적으로 승인했는지 확인합니다.

관리:xmpps2snodes에서 sql select * 실행
pkid cp_id
==========
055c13d9-943d-459d-a3c6-af1d1176936d cm-2_s2scp-1.eft-xwye-a-coluc-com
관리자:

2단계. IM&P 서버에서 XMPP 페더레이션이 꺼져 있는지 확인합니다.

Presence > Inter-Domain Federation > XMPP Federation > Settings > XMPP Federation Node

Status > Off

Expressway C 및 Expressway E에서 XMPP 페더레이션 문제 해결

1단계..DEBUG 수준 로그를 활성화합니다.

Expressway-E에서:

유지 관리 > 진단 > 고급 > 지원 로그 구성 > developer.clusterdb.restapi

Expressway-C:

유지 관리 > 진단 > 고급 > 지원 로그 구성 > developer.clusterdb.restapi

유지 관리 > 진단 > 고급 > 네트워크 로그 구성 > network.axl

2단계. Expressway-C 및 Expressway-E에서 진단 로그 및 TCP 덤프를 시작합니다.

네트워크 문제가 CLI에서 IM&P 측에서 패킷 캡처를 수행하는 것으로 의심되는 경우:

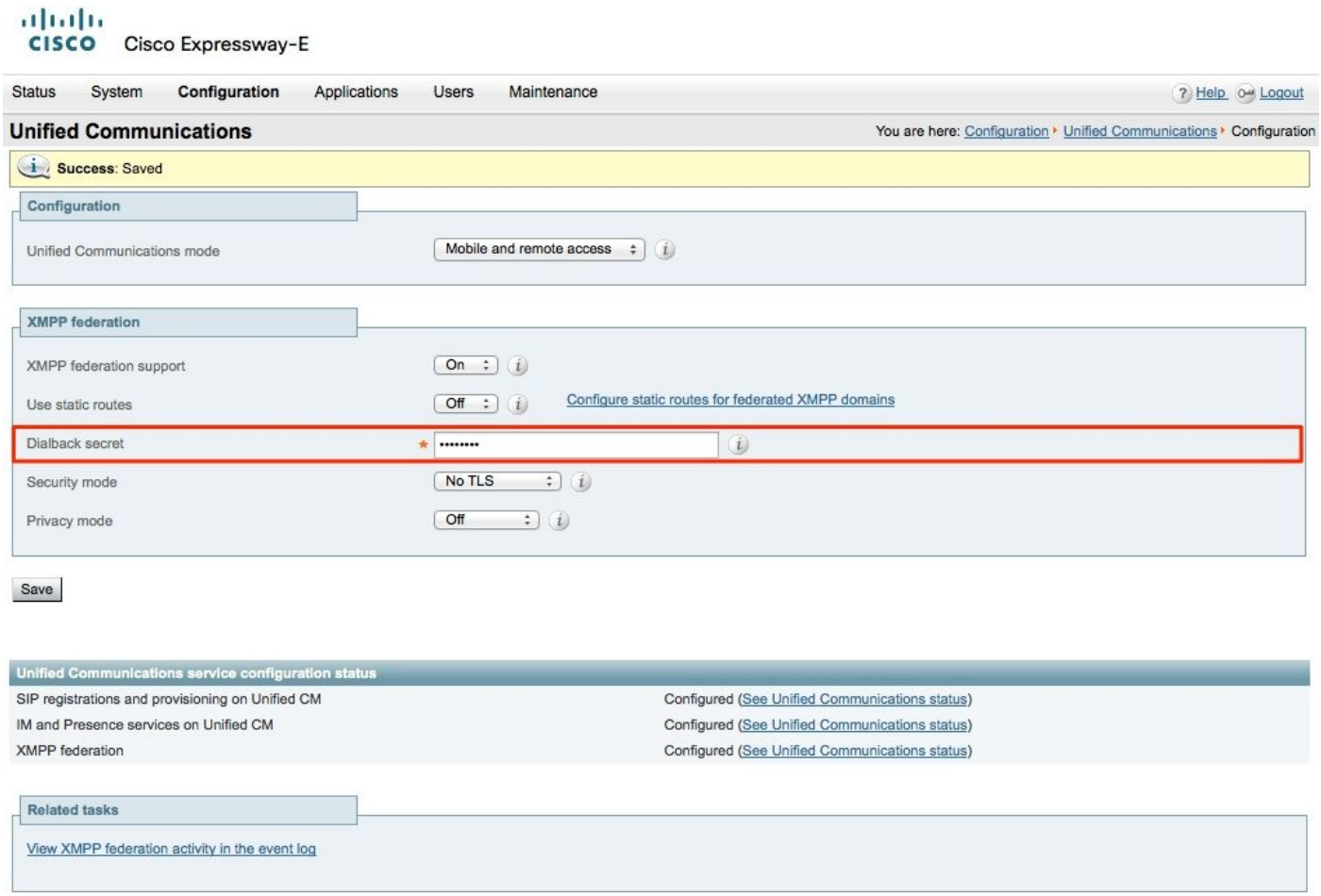
"utils network capture eth0 file axl_inject.pcap count 1000000 size all"

3단계. Expressway-E에서 XMPP 페더레이션 활성화

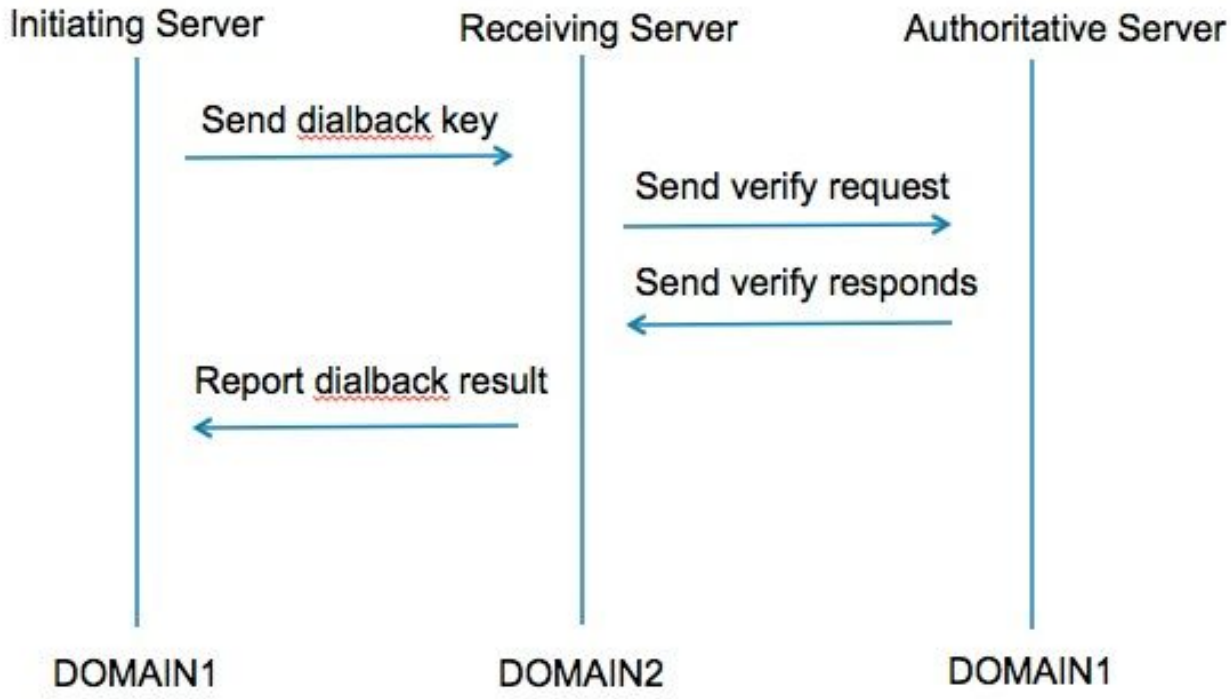
30초 기다렸다가 "Verify the XMPP Configuration on Expressway(Expressway에서 XMPP 컨피그레이션 확인)"에 설명된 단계를 진행합니다.

2단계. 다이얼백 암호 구성

Configuration(컨피그레이션) > Unified Communication(통합 커뮤니케이션) > Dialback Secret(다이얼백 암호)



다이얼 백 작동 방식



1단계. 시작 서버는 다이얼백 결과를 구성한 암호를 기반으로 계산하여 수신 서버로 전송합니다.

2단계. 수신 서버는 시작 도메인의 권한 있는 서버로 이 결과를 검증합니다.

3단계. 권한 있는 서버가 동일한 다이얼 백 암호를 공유하므로 결과를 검증할 수 있습니다.

4단계. 유효성을 검사하면 수신 서버가 시작 서버의 XMPP를 수락합니다.

5단계. 시작 서버가 _xmpp-server._tcp.<target domain>에 대해 조회를 수행하여 수신 서버를 찾습니다.

6단계. 수신 서버는 _xmpp-server._tcp.<orginening domain>에 대해 조회를 수행하여 권한 있는 서버를 찾습니다.

7단계. 권한 있는 서버는 시작 서버와 같을 수 있습니다.

다이얼 백 암호 확인

Expressway는 시작 서버인 경우 이 디버그를 표시합니다.

XCP_CM2[12122]:..Level="INFO " CodeLocation="stanza.component.out" Detail="xcoder=34A9B60C8 전송:<db:result from='coluc.com' to='vngtp.lab'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:result>"

XCP_CM2[12122]:..Level="DEBUG" CodeLocation="stream.out" Detail="(0000000-0000-0000-0000000000000000, coluc.com:vngtp.lab, OUT) xcoder=34A9B60C0Scheduling 30초 후 시간 초과"

XCP_CM2[12122]:..Level="INFO " CodeLocation="ConnInfoHistory" Detail="연결 상태 변경 :PENDING->CONNECTED:...

Expressway는 수신 서버인 경우 이 디버그를 표시합니다.

XCP_CM2[22992]:..Level="VBOSE" CodeLocation="stanza.component.in" Detail="xcoder=05E295A2B 수신:
<db:result from='coluc.com'
to='vngtp.lab'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:result>"

XCP_CM2[22992]:..Level="INFO " CodeLocation="Resolver.cpp:128" Detail= "'coluc.com:puny=coluc.com:service=_xmpp-server._tcp:defport=0'에 대한 해결 프로그램 조회를 시작합니다."

XCP_CM2[22992]:..Level="INFO " CodeLocation="debug" Detail="(e5b18d01-fe24-4290-bba1-a57788a76468, vngtp.lab:coluc.com, IN)
host=coluc.com method=SRV dns-tigings=(TOTAL:0.003157 SRV:0.002885)"에 대해 확인된 다이얼백 주소

XCP_CM2[22992]:..Level="INFO " CodeLocation="DBVerify.cpp:270" Detail="(e5b18d01-fe24-4290-bba1-a57788a76468, vngtp.lab:coluc.com, IN)
DBVerify 스트림이 열려 있습니다.db 전송:확인 패킷:<db:verify from='vngtp.lab' id='05E295A2B' to='coluc.com'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:verify>"

XCP_CM2[22992]:..Level="INFO " CodeLocation="DBVerify.cpp:282" Detail="(e5b18d01-fe24-4290-bba1-a57788a76468, vngtp.lab:coluc.com, IN)
DBVerify 패킷 수신: <db:verify from='coluc.com' id='05E295A2B' to='vngtp.lab' type='valid'>d780f198ac34a6dbd795fcdaf8762eaf52a9b03</db:verify>

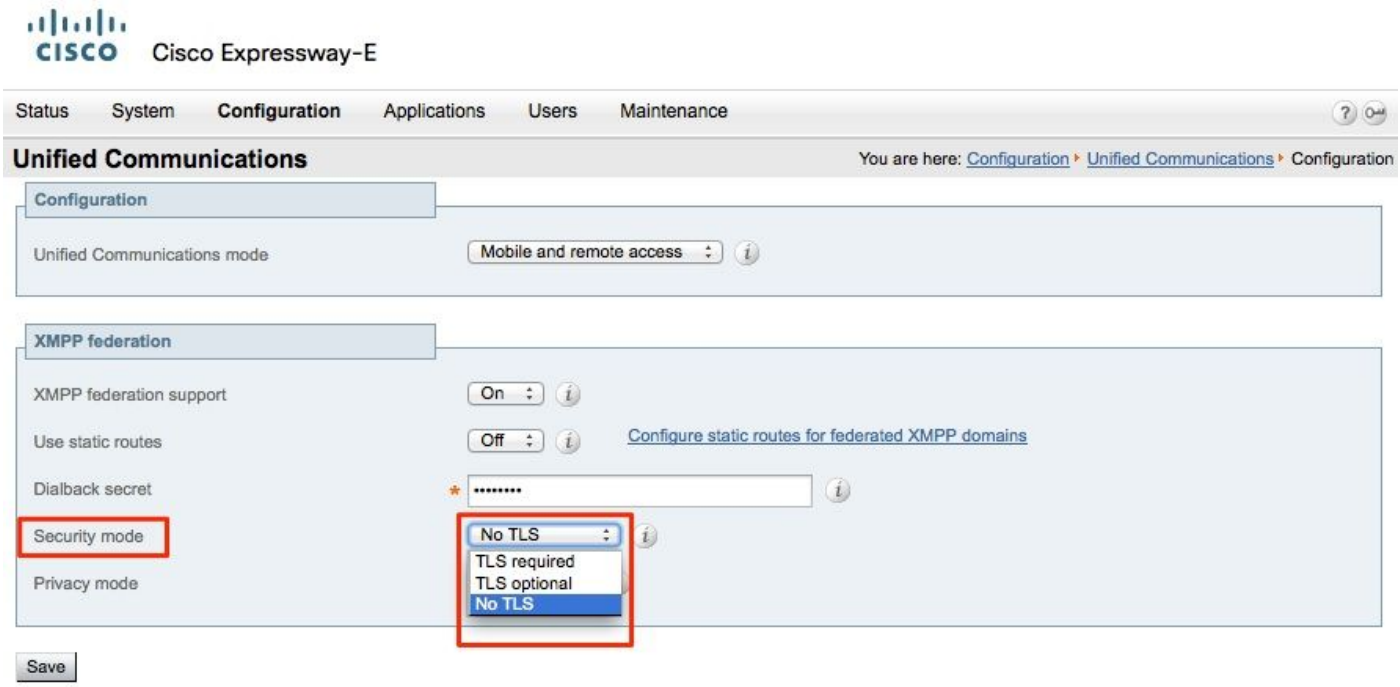
Expressway는 권한 있는 서버인 경우 이 디버그를 표시합니다.

XCP_CM2[5164]:..Level="INFO " CodeLocation="debug" Detail="xcoder=94A9B60C8 onStreamOpen:
<stream:stream from='vngtp.lab' id='1327B794B' to='coluc.com' 버전='1.0' xml:lang='en-US.UTF-8' xmlns='jabber:server' xmlns:db='jabber:server:dialns' xmlns:stream='stream='http://etherx.jabber.org/streams'/>"

XCP_CM2[5164]:..Level="VBOSE" CodeLocation="stanza.component.in" Detail="xcoder=94A9B60C8 수신:
<db:verify from='vngtp.lab' id='05E295A2B' to='coluc.com'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:verify>"

XCP_CM2[5164]:..Level="INFO " CodeLocation="stream.in" Detail="xcoder=94A9B60C8 닫는 스트림(dialback 전용)"

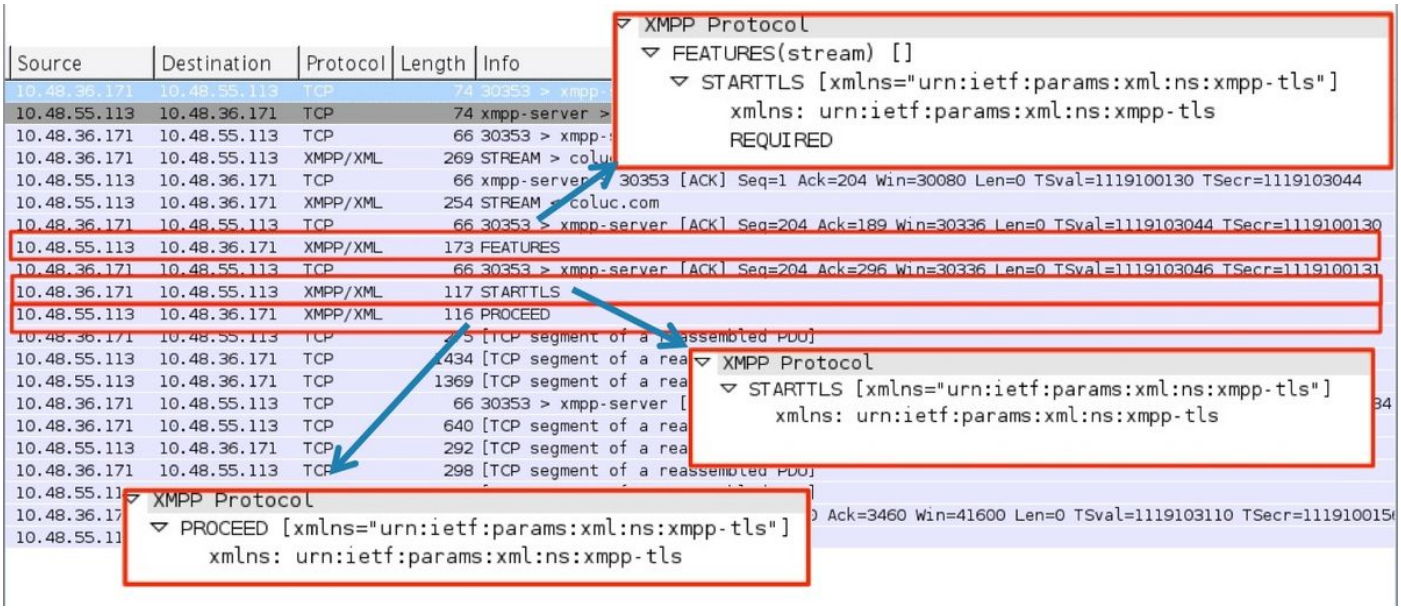
3단계. 보안 모드 구성



보안 모드 문제 해결

- Wireshark를 사용하여 문제 해결
- TLS(Transport Layer Security)가 필요한지, OPTIONAL(선택 사항) 또는 No TLS(TLS 없음)가 필요한지 여부를 표시하는 기능

이 패킷 캡처 연습은 TLS가 필요한 경우의 예를 보여줍니다.



SSL로 디버깅하면 TLS 핸드셰이크가 표시됩니다.

Source	Destination	Protocol	Length	Info
10.48.36.171	10.48.55.113	TCP	74	30353 > xmpp-server [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1119103043 TSecr=0 W
10.48.55.113	10.48.36.171	TCP	74	xmpp-server > 30353 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=1119100129
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1119103043 TSecr=1119100129
10.48.36.171	10.48.55.113	TLSv1.2	269	Continuation Data
10.48.55.113	10.48.36.171	TCP	66	xmpp-server > 30353 [ACK] Seq=1 Ack=204 Win=30080 Len=0 TSval=1119100130 TSecr=1119103044
10.48.55.113	10.48.36.171	TLSv1.2	254	Continuation Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=189 Win=30336 Len=0 TSval=1119103044 TSecr=1119100130
10.48.55.113	10.48.36.171	TLSv1.2	173	Continuation Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=204 Ack=296 Win=30336 Len=0 TSval=1119103046 TSecr=1119100131
10.48.36.171	10.48.55.113	TLSv1.2	117	Continuation Data
10.48.55.113	10.48.36.171	TLSv1.2	116	Continuation Data
10.48.36.171	10.48.55.113	TLSv1.2	275	Client Hello
10.48.55.113	10.48.36.171	TLSv1.2	1434	Server Hello
10.48.55.113	10.48.36.171	TLSv1.2	1369	Certificate, Server Hello Done
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=464 Ack=3017 Win=36096 Len=0 TSval=1119103049 TSecr=1119100134
10.48.36.171	10.48.55.113	TLSv1.2	640	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10.48.55.113	10.48.36.171	TLSv1.2	292	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
10.48.36.171	10.48.55.113	TLSv1.2	298	Application Data
10.48.55.113	10.48.36.171	TLSv1.2	283	Application Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1270 Ack=3460 Win=41600 Len=0 TSval=1119103110 TSecr=1119100156
10.48.55.113	10.48.36.171	TLSv1.2	113	Application Data
10.48.36.171	10.48.55.113	TCP	66	30353 > xmpp-server [ACK] Seq=1270 Ack=3507 Win=41600 Len=0 TSval=1119103110 TSecr=1119100195
10.48.36.171	10.48.55.113	TLSv1.2	190	Application Data
10.48.55.113	10.48.36.171	TCP	66	xmpp-server > 30353 [ACK] Seq=3507 Ack=1394 Win=33408 Len=0 TSval=1119100236 TSecr=1119103110
10.48.55.113	10.48.36.171	TLSv1.2	218	Application Data

일반적인 문제:

증상 1:단방향 메시징외부 인터넷이 작동하지 않습니다.IM&P 상태가 활성 상태입니다.

Expressway-C 로그에서:

"함수="executeSQLQuery" 상태="401" 이유="없음"

원인 1: Expressway-C 측의 IM&P 사용자에 대한 자격 증명이 잘못되었습니다.

이 URL을 실행하고 Expressway C에 구성된 자격 증명으로 로그인하여 확인할 수도 있습니다

Configuration(구성) > Unified Communications > IM and Presence Server(IM and Presence 서버)

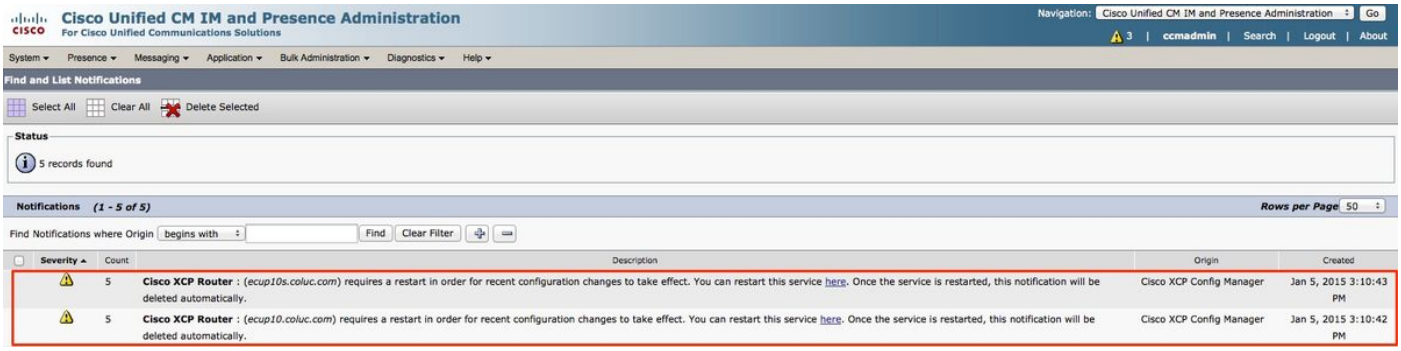
https://cups_address.domain.com:8443/axl

솔루션 1:암호 업데이트, CUP 서버 검색 새로 고침

증상 2:페더레이션 실패, CUP의 XCP 라우터가 패킷을 반송합니다.

원인 2:CUP의 XCP 라우터가 다시 시작되지 않았습니다.

이는 CUP **관리**에서 Notifications 페이지에서 확인할 수 **있습니다**.



솔루션 2:CUP에서 XCP 라우터 재시작

어떤 때는 알림이 없지만 CUP의 XCP 라우터 로그에서는 여전히 패킷을 반송합니다. XCP 라우터 서비스를 다시 시작해도 해결되지 않으면 IM&P 클러스터를 다시 부팅해도 문제가 해결되지 않습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems