WAAS - SSL AO 문제 해결

장:SSL AO 문제 해결

이 문서에서는 SSL AO 문제 해결 방법에 대해 설명합니다.

목차

SSL Accelerator 개요

SSL 가속기(4.1.3 이상에서 사용 가능)는 암호화된 SSL(Secure Sockets Layer) 및 TLS(Transport Layer Security) 트래픽을 최적화합니다.SSL 가속기는 엔드 투 엔드 트래픽 최적화를 활성화하기 위해 WAAS 내에서 트래픽 암호화 및 암호 해독을 제공합니다.또한 SSL Accelerator는 암호화 인증서 및 키를 안전하게 관리합니다.

WAAS 네트워크에서 데이터 센터 WAE는 클라이언트의 SSL 요청에 대해 신뢰할 수 있는 중간 노드 역할을 합니다.개인 키와 서버 인증서는 데이터 센터 WAE에 저장됩니다.데이터 센터 WAE는 SSL 핸드셰이크에 참여하여 이 세션 키를 브랜치 WAE에 안전하게 인밴드(in-band)하여 브랜치 WAE가 클라이언트 트래픽을 해독하고, 최적화하고, 다시 암호화하고, WAN을 통해 데이터 센터 WAE로 전송할 수 있도록 합니다.데이터 센터 WAE는 원본 서버와 별도의 SSL 세션을 유지 관리합니다.

다음 서비스는 SSL/TLS 최적화와 관련이 있습니다.

- Accelerated Service - SSL 서버 또는 서버 집합에 적용할 가속화 특성을 설명하는 컨피그레이션 엔티티입니다.신뢰할 수 있는 중재자, 사용할 암호, 허용되는 SSL 버전 및 인증서 확인 설정으로 가장하는 동안 사용할 인증서 및 개인 키를 지정합니다.
- 피어링 서비스 - 지사와 데이터 센터 WAE 간의 대역 내 SSL 연결에 적용할 가속화 특성을 설명하는 컨피그레이션 엔티티입니다.이 서비스는 SSL 연결을 최적화하기 위해 데이터 센터에서 지사 WAE로 세션 키 정보를 전송하는 데 사용됩니다.
- Central Manager Admin Service - SSL Accelerator에서 직접 사용하지 않고 관리자가 SSL 가속 서비스의 구성 관리를 위해 사용합니다.SSL 가속화 서비스에 사용할 인증서 및 개인 키를 업로드하는 데에도 사용됩니다.
- Central Manager Management Service - SSL Accelerator에서 직접 사용하지 않고 애플리케이션 가속기 디바이스와 Central Manager 간의 통신에 사용됩니다.이 서비스는 컨피그레이션 관리, 보안 저장소 암호화 키 검색 및 디바이스 상태 업데이트에 사용됩니다.

중앙 관리자 보안 저장소는 모든 WAE에 대해 보안 암호화 키를 저장하기 때문에 SSL AO가 작동하려면 반드시 필요합니다.각 Central Manager를 다시 로드한 후 관리자는 cms **secure-store open** 명령을 사용하여 패스프레이즈를 제공하여 보안 저장소를 다시 열어야 합니다.WAE는 WAE가 리부팅될 때마다 Central Manager에서 보안 저장소 암호화 키를 자동으로 검색하므로 다시 로드 후 WAE에 어떤 작업도 필요하지 않습니다.

클라이언트가 HTTP 프록시 솔루션을 사용 중인 경우 초기 연결은 HTTP AO에 의해 처리되며, 이는 이를 포트 443에 대한 SSL 터널 요청으로 인식합니다. HTTP AO는 데이터 센터 WAE에 정의된 일치하는 SSL 가속 서비스를 찾고 일치 항목을 찾으면 SSL AO에 대한 연결을 해제합니다.그러나 HTTP AO가 HTTPS 프록시에 대해 SSL AO로 전달하는 트래픽은 SSL 애플리케이션이 아닌 웹 애플리케이션 통계의 일부로 보고됩니다.HTTP AO에서 일치하는 항목을 찾지 못하면 연결이 고정 HTTPS(SSL) 정책 컨피그레이션에 따라 최적화됩니다.

SSL AO는 CA 서명 인증서 대신 자체 서명 인증서를 사용할 수 있으며, 이는 POC(Proof of Concept) 시스템을 구축하고 SSL 문제를 해결하는 데 도움이 될 수 있습니다.자체 서명 인증서를 사용하면 오리진 서버 인증서를 가져올 필요 없이 WAAS 시스템을 신속하게 구축할 수 있으며 인증서를 잠재적인 문제의 소스로 제거할 수 있습니다.SSL 가속 서비스를 생성할 때 중앙 관리자에서 자체 서명 인증서를 구성할 수 있습니다.그러나 자체 서명 인증서를 사용할 경우, 클라이언트 브라우저는 인증서를 신뢰할 수 없다는 보안 경고를 표시합니다(잘 알려진 CA에서 서명하지 않았기 때문). 이 보안 경고를 방지하려면 클라이언트 브라우저의 신뢰할 수 있는 루트 인증 기관 저장소에 인증서를 설치합니다.(Internet Explorer의 보안 경고에서 **인증서 보기**를 클릭한 다음 인증서 대화 상자에서 인증서 **설치**를 클릭하고 인증서 가져오기 마법사를 완료합니다.)

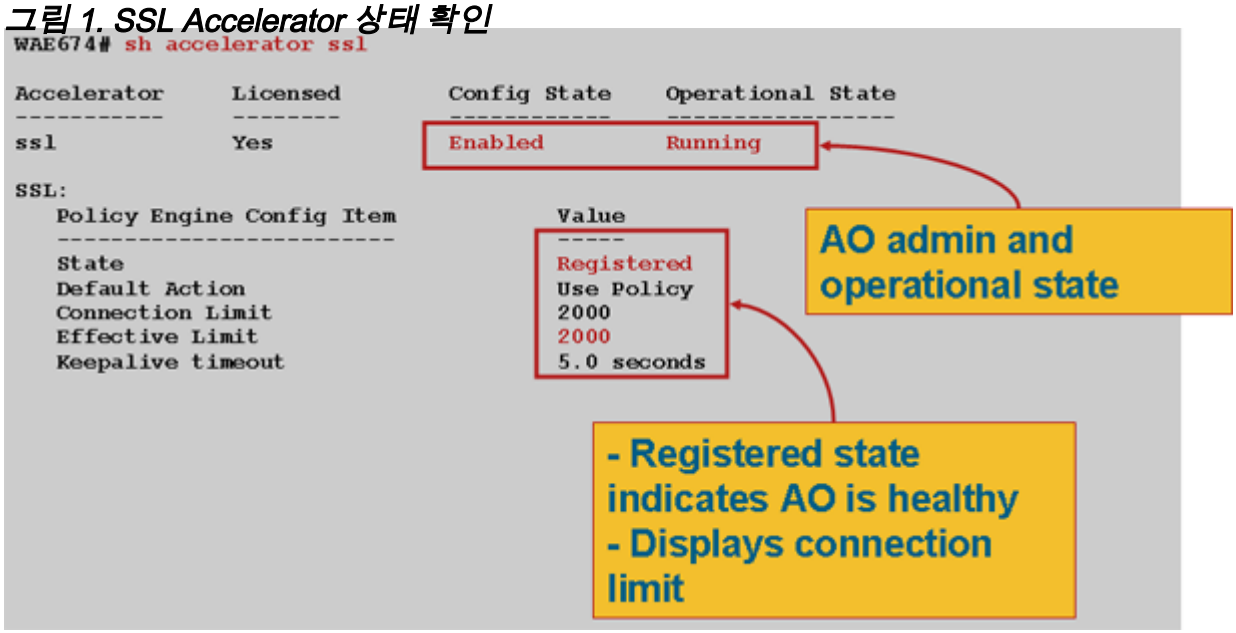
SSL Management Services 구성은 선택 사항이며, 중앙 관리자 통신에 사용되는 SSL 버전 및 암호 목록을 WAE 및 브라우저(관리 액세스용)로 변경할 수 있습니다. 브라우저에서 지원하지 않는 암호를 구성하면 중앙 관리자에 대한 연결이 끊어집니다.이 경우 CLI에서 **crypto ssl management-service** 컨피그레이션 명령을 사용하여 SSL 관리 서비스 설정을 다시 기본값으로 설정합니다.

SSL AO 문제 해결

Troubleshooting Application Acceleration 기사에 설명된 대로 **show accelerator** 및 **show license** 명령을 사용하여 일반적인 AO 컨피그레이션 및 상태를 확인할 수 있습니다.SSL Accelerator 작업에는 Enterprise 라이센스가 필요합니다.

그런 다음 그림 1과 같이 **show accelerator ssl** 명령을 사용하여 데이터 센터와 지사 WAE에서 SSL AO와 관련된 상태를 확인합니다. SSL AO가 Enabled, Running 및 Registered이고 연결 제한이 표시되는지 확인합니다.Config State(컨피그레이션 상태)가 Enabled(활성화됨)이지만 Operational State(운영 상태)가 Shutdown(종료)이면 라이센싱 문제를 나타냅니다.Operational State(운영 상태)가 Disabled(비활성화됨)인 경우, 보안 저장소가 열려 있지 않거나 Central Manager에 연결할 수 없기 때문에 WAE가 Central Manager 보안 저장소에서 SSL 키를 검색할 수 없기 때문일 수 있습니다.show cms **info** 및 **ping** 명령을 사용하여 중앙 관리자에 연결할 수 있는지 확인합니다.

그림 1. SSL Accelerator 상태 확인



Operational State of Gen Crypto Params(Crypto Params의 작동 상태)가 표시되면 상태가 Running(실행 중)이 될 때까지 기다립니다. 재부팅한 후 몇 분 정도 걸릴 수 있습니다.몇 분 이상 CM에서 키 검색 상태가 표시되면 중앙 관리자의 CMS 서비스가 실행되고 있지 않거나, 중앙 관리자에 대한 네트워크 연결이 없거나, WAE 및 중앙 관리자의 WAAS 버전이 호환되지 않거나, 중앙 관리자 보안 저장소가 열려 있지 않음을 나타낼 수 있습니다.

다음과 같이 **show cms secure-store** 명령을 사용하여 중앙 관리자 보안 저장소가 초기화되고 열려 있는지 확인할 수 있습니다.

```
cm# show cms secure-store
secure-store is initialized and open.
```

보안 저장소가 초기화되거나 열리지 않으면 mstore_key_failure 및 secure-store와 같은 중요한 경보가 표시됩니다.cms **secure-store open** 명령을 사용하여 보안 저장소를 열거나 중앙 관리자에서 Admin(관리) **> Secure Store(보안 저장소)를** 선택할 수 있습니다.

팁:비밀번호를 잊은 경우 보안 저장소를 재설정할 필요가 없도록 보안 저장소 비밀번호를 문서화합니다.

WAE의 디스크 암호화에 문제가 있는 경우 SSL AO가 작동하지 않을 수도 있습니다.**show disk details** 명령을 사용하여 디스크 암호화가 활성화되었는지 확인하고 CONTENT 및 SPOOL 파티션이 마운트되었는지 확인합니다.이러한 파티션이 마운트되면 Central Manager에서 디스크 암호화 키가 성공적으로 검색되었으며 암호화된 데이터를 기록하여 디스크에서 읽을 수 있음을 나타냅니다.**show disk details** 명령에 "System is initializing(시스템 초기화 중)"이 표시되면 암호화 키가 Central Manager에서 아직 검색되지 않았고 디스크가 아직 마운트되지 않았음을 나타냅니다

.WAE는 이 상태에서 가속화 서비스를 제공하지 않습니다.WAE가 Central Manager에서 디스크 암호화 키를 검색할 수 없으면 경보가 발생합니다.

데이터 센터 WAE에서 SSL 가속화 서비스가 구성되고 해당 상태가 "Enabled(활성화됨)"인지 확인할 수 있습니다(Central Manager에서 디바이스를 선택한 다음 Configure(구성) **> Acceleration(가속화) > SSL Accelerated Services(SSL 가속화 서비스)를** 선택합니다).구성 및 활성화된 가속 서비스는 다음 조건 때문에 SSL 가속기에 의해 비활성 상태로 렌더링될 수 있습니다.

- 가속화된 서비스에 구성된 인증서가 WAE에서 삭제되었습니다.**show running-config** 명령을 사용하여 가속화된 서비스에 사용 중인 인증서를 확인한 다음 **show crypto certificates** 및 **show crypto certificate-details** 명령을 사용하여 인증서가 보안 저장소에 있는지 확인합니다.인증서가 없으면 인증서를 다시 가져옵니다.
- 가속화된 서비스 인증서가 만료되었습니다.show crypto **certificates** 및 **show crypto certificate-details** 명령을 사용하여 인증서 만료 날짜를 확인합니다.
- 가속화된 서비스 인증서의 유효 날짜는 미래부터 시작됩니다.show crypto **certificates** 및 **show crypto certificate-details** 명령을 사용하고 명령 출력의 유효성 섹션을 확인합니다.또한 WAE 클럭 및 시간대 정보가 정확한지 확인합니다.

SSL 연결에 올바른 정책이 적용되었는지 확인할 수 있습니다. 즉, 그림 2와 같이 SSL 가속화를 통한 전체 최적화가 적용되었는지 확인할 수 있습니다. Central Manager에서 WAE 디바이스를 선택한 다음 **Monitor(모니터링) > Optimization(최적화) > Connections Statistics(연결 통계)를** 선택합니다.

그림 2. SSL 연결에 대한 올바른 정책 확인

show running**-config** 명령을 사용하여 HTTPS 트래픽 정책이 올바르게 구성되었는지 확인합니다.SSL 애플리케이션 작업에 대해 **DRE**의 **최적화 없음 압축 없음**을 확인하고 다음과 같이 HTTPS 분류자에 대해 적절한 일치 조건을 표시하고자 합니다.

```
WAE674# sh run | include HTTPS
   classifier HTTPS
      name SSL classifier HTTPS action optimize DRE no compression none              <---------
----

WAE674# sh run | begin HTTPS

...skipping
   classifier HTTPS
```

```
      match dst port eq 443                                                    <---------
----
   exit
```

활성 가속 서비스는 가속화된 서비스 내에 구성된 서버 IP:port, server name:port 또는 server domain:port에 해당하는 동적 정책을 삽입합니다.**show policy-engine application dynamic** 명령을 사용하여 이러한 정책을 검사할 수 있습니다.표시된 각 정책의 Dst 필드는 가속화된 서비스와 일치하는 서버 IP 및 포트를 나타냅니다.와일드카드 도메인(예: server-domain *.webex.com 포트 443)의 경우 Dst 필드는 'Any:443'이 됩니다. 서버 이름 컨피그레이션의 경우 가속화된 서비스가 활성화되고 DNS 응답에 반환된 모든 IP 주소가 정책 엔진에 삽입될 때 정방향 DNS 조회가 수행됩니다.이 명령은 가속화된 서비스가 "서비스 안 함"으로 표시되지만 일부 다른 오류로 인해 가속화된 서비스가 비활성화된 상황을 포착하는 데 유용합니다.예를 들어 모든 가속화된 서비스는 피어링 서비스에 종속되며, 피어 서비스가 인증서 누락/삭제로 인해 비활성 상태인 경우, 가속화된 서비스는 show running-config 출력에서 "inservice"로 표시되지만 비활성 상태로 표시됩니다.**show policy-engine application dynamic** 명령을 사용하여 데이터 센터 WAE에서 SSL 동적 정책이 활성화되었는지 확인할 수 있습니다.**show crypto ssl services host-service** peering 명령을 사용하여 피어링 서비스 상태를 확인할 수 있습니다.

SSL AO 가속 서비스 컨피그레이션에는 다음과 같은 네 가지 유형의 서버 항목이 있을 수 있습니다.

- 고정 IP(server-ip) - 버전 4.1.3 이상에서 사용 가능
- 모두 탐지(server-ip any) - 4.1.7 이상에서 사용 가능
- 호스트 이름(server-name) - 4.2.1 이상에서 사용 가능
- 와일드카드 도메인(서버 도메인) - 4.2.1 이상에서 사용 가능

SSL AO에서 연결을 수신하면 최적화에 어떤 가속화된 서비스를 사용해야 할지 결정합니다.고정 IP 컨피그레이션에는 가장 높은 환경 설정이 지정되고 그 뒤에 서버 이름, 서버 도메인, 서버 ip any가 옵니다.구성 및 활성화된 가속 서비스 중 연결을 위한 서버 IP와 일치하는 서비스가 없으면 일반 AO로 연결이 푸시됩니다.SSL AO에 의해 정책 엔진에 삽입된 쿠키는 어떤 가속화된 서비스와 특정 연결에 대해 매칭되는 서버 항목 유형을 결정하는 데 사용됩니다.이 정책 엔진 쿠키는 32비트 번호이며 SSL AO에만 적용됩니다.상위 비트는 서로 다른 서버 항목 유형을 나타내는 데 사용되며 하위 비트는 다음과 같이 가속화된 서비스 인덱스를 나타냅니다.

SSL 정책 엔진 쿠키 값

쿠키 값	서버 항목 유형	설명
0x8*xxxxxxx*	서버 IP 주소	고정 IP 주소 컨피그레이션
0x4*xxxxxxx*	서버 호스트 이름	데이터 센터 WAE는 호스트 이름에 대해 정방향 DNS 조회를 수행하고 동적 정책 컨피그레이션에 반환되는 IP 주소를 추가합니다.기본적으로 10분마다 새로 고칩니다.
0x2fffff	서버 도메인 이름	데이터 센터 WAE는 대상 호스트 IP 주소에서 역방향 DNS 조회를 수행하여 도메인과 일치하는지 확인합니다.일치하는 경우 SSL 트래픽이 가속화되고 일치하지 않으면 고정 HTTPS 정책에 따라 트래픽이 처리됩니다.
0x1*xxxxxxx*	모든 서버	모든 SSL 연결은 이 가속화된 서비스 컨피그레이션을 사용하여 가속화

예 1:서버 IP 구성을 통한 서비스 가속화:

```
WAE(config)#crypto ssl services accelerated-service asvc-ip
WAE(config-ssl-accelerated)#description "Server IP acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-ip 171.70.150.5 port 443
WAE(config-ssl-accelerated)#inservice
```

해당 정책 엔진 항목이 다음과 같이 추가됩니다.

```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
  Number:     1   Type: Any->Host (6)  User Id: SSL (4)           <----------------
    Src: ANY:ANY  Dst: 171.70.150.5:443                           <----------------
    Map Name: basic
    Flags: SSL
    Seconds: 0  Remaining: - NA -  DM Index: 32764
    Hits: 25  Flows: - NA -  Cookie: 0x80000001                   <----------------
```

예 2:서버 이름 컨피그레이션으로 서비스 가속화:

이 컨피그레이션을 사용하면 엔터프라이즈 SSL 애플리케이션을 최적화하기 위해 쉽게 구축할 수 있습니다.DNS 컨피그레이션 변경 사항에 적응할 수 있으며 IT 관리 작업을 줄일 수 있습니다.

```
WAE(config)#crypto ssl services accelerated-service asvc-name
WAE(config-ssl-accelerated)#description "Server name acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-name www.google.com port 443
WAE(config-ssl-accelerated)#inservice
```

해당 정책 엔진 항목이 다음과 같이 추가됩니다.

```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
 Number:     1   Type: Any->Host (6)  User Id: SSL (4)           <----------------
   Src: ANY:ANY  Dst: 74.125.19.104:443                          <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32762
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                    <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
 Number:     2   Type: Any->Host (6)  User Id: SSL (4)           <----------------
   Src: ANY:ANY  Dst: 74.125.19.147:443                          <----------------
```

```
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32763
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                    <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
 Number:     3   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.103:443                          <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32764
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                    <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
 Number:     4   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.99:443                           <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32765
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                    <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
```

예 3:서버-도메인 구성을 통한 서비스 가속화:

이 컨피그레이션을 통해 WAAS 디바이스는 모든 서버의 IP 주소를 알 필요가 없는 단일 와일드카드 도메인을 구성할 수 있습니다.데이터 센터 WAE는 리버스 DNS(rDNS)를 사용하여 구성된 도메인에 속한 트래픽을 확인합니다.와일드카드 도메인을 구성하면 여러 IP 주소를 구성할 필요가 없으므로 솔루션을 확장 가능하고 SaaS 아키텍처에 적용할 수 있습니다.

```
WAE(config)#crypto ssl services accelerated-service asvc-domain
WAE(config-ssl-accelerated)#description "Server domain acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-name *.webex.com port 443
WAE(config-ssl-accelerated)#inservice
```

해당 정책 엔진 항목이 다음과 같이 추가됩니다.

```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
 Number:     1   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: ANY:443                                    <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32762
   Hits: 0  Flows: - NA -  Cookie: 0x2FFFFFFF                    <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
```

예 4:서버-ip any 컨피그레이션으로 서비스 가속화:

이 컨피그레이션은 모두 탐지 메커니즘을 제공합니다.**server-ip**를 사용하여 가속화된 서비스를 활성화하면 포트 443의 모든 연결이 SSL AO에 의해 최적화됩니다.POC 중에 이 컨피그레이션을 사용하여 특정 포트의 모든 트래픽을 최적화할 수 있습니다.

```
WAE(config)#crypto ssl services accelerated-service asvc-ipany
WAE(config-ssl-accelerated)#description "Server ipany acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-ip any port 443
WAE(config-ssl-accelerated)#inservice
```

해당 정책 엔진 항목이 다음과 같이 추가됩니다.

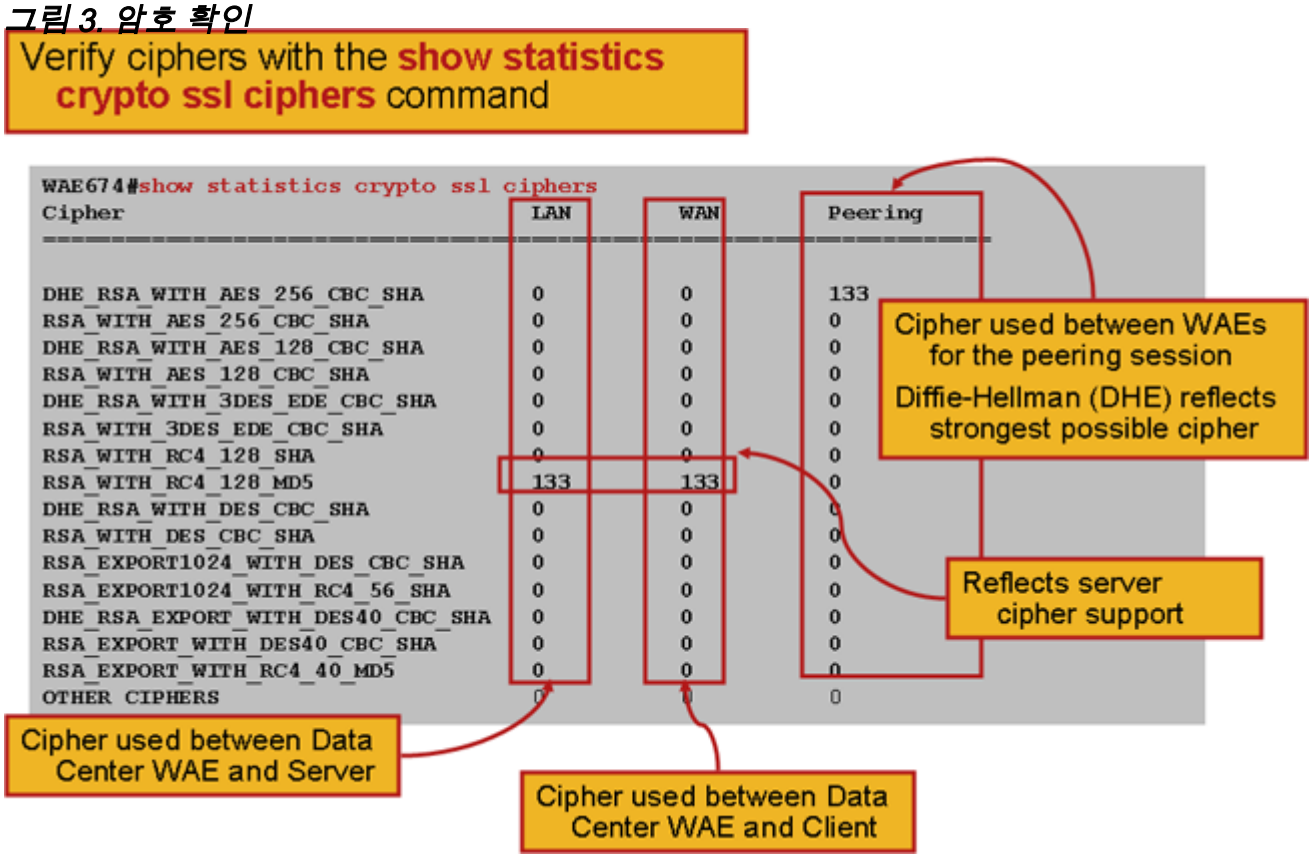
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
 Number:     1   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: ANY:443                                     <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32762
   Hits: 0  Flows: - NA -  Cookie: 0x10000004                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
```

그림 3과 같이 **show statistics crypto ssl ciphers** 명령과 함께 사용 중인 암호를 확인할 수 있습니다.

그림 3. 암호 확인



이러한 암호가 원본 서버에 구성된 암호와 일치하는지 확인할 수 있습니다.**참고:**DHE를 포함하는 암호는 Microsoft IIS 서버에서 지원되지 않습니다.

Apache 서버의 경우 httpd.conf 파일에서 SSL 버전 및 암호 세부 정보를 확인할 수 있습니다.이러한 필드는 httpd.conf에서 참조되는 별도의 파일(sslmod.conf)에도 있을 수 있습니다.다음과 같이 SSLProtocol 및 SSLCipherSuite 필드를 찾습니다.

```
SSLProtocol -all +TLSv1 +SSLv3
SSLCipherSuite HIGH:MEDIUM:!aNULL:+SHA1:+MD5:+HIGH:+MEDIUM
. . .
SSLCertificateFile /etc/httpd/ssl/server.crt
SSLCertificateKeyFile /etc/httpd/ssl/server.key
```

Apache 서버에서 인증서 발급자를 확인하려면 다음과 같이 openssl 명령을 사용하여 인증서를 읽습니다.

```
> openssl x509 -in cert.pem -noout -issuer -issuer_hash
issuer= / C=US/ST=California/L=San
Jose/O=CISCO/CN=tools.cisco.com/emailAddress=webmaster@cisco.com be7cee67
```

브라우저에서 인증서 및 세부 정보를 보고 인증서 체인, 버전, 암호화 키 유형, 발급자 CN(Common Name) 및 주체/사이트 CN을 확인할 수 있습니다.Internet Explorer에서 자물쇠 아이콘을 클릭하고 **인증서 보기**를 클릭한 다음 세부 정보 및 인증 경로 탭에서 이 정보를 확인합니다.

대부분의 브라우저에서는 클라이언트 인증서가 X509 PEM 형식이 아닌 PKCS12 형식이어야 합니다.X509 PEM 형식을 PKCS12 형식으로 내보내려면 Apache 서버에서 다음과 같이 openssl 명령을 사용합니다.

```
> openssl pkcs12 -export -in cert.pem -inkey key.pem -out cred.p12
Enter Export Password:
Verifying - Enter Export Password:
```

개인 키가 암호화된 경우 내보내기에 암호가 필요합니다.내보내기 비밀번호는 WAAS 디바이스로 자격 증명을 가져오는 데 다시 사용됩니다.

show statistics accelerator **ssl** 명령을 사용하여 SSL AO 통계를 확인합니다.

```
WAE7326# show statistics accelerator ssl
SSL:

  Global Statistics
  -----------------
  Time Accelerator was started:                     Mon Nov 10     15:28:47 2008
  Time Statistics were Last Reset/Cleared:          Mon Nov 10    15:28:47 2008
  Total Handled Connections:                                        17                <-------
---------
  Total Optimized Connections:                                      17                <-------
---------
  Total Connections Handed-off with Compression Policies Unchanged:  0                <-------
---------
  Total Dropped Connections:                                        0                 <-------
---------
  Current Active Connections:                                       0
  Current Pending Connections:                                      0
  Maximum Active Connections:                                       3
  Total LAN Bytes Read:                                             25277124          <-------
---------
  Total Reads on LAN:                                               5798              <-------
```

```
---------
  Total LAN Bytes Written:                                  6398            <-------
---------
  Total Writes on LAN:                                      51              <-------
---------
  Total WAN Bytes Read:                                     43989           <-------
---------
  Total Reads on WAN:                                       2533            <-------
---------
  Total WAN Bytes Written:                                  10829055        <-------
---------
  Total Writes on WAN:                                      3072            <-------
---------
. . .
```

실패한 세션 및 인증서 확인 통계는 문제 해결에 유용할 수 있으며 show statistics accelerator ssl 명령에서 다음 필터를 사용하여 보다 쉽게 검색할 수 있습니다.

```
WAE# show statistics accelerator ssl | inc Failed
  Total Failed Handshakes:                                  47
  Total Failed Certificate Verifications:                   28
  Failed certificate verifications due to invalid certificates:    28
  Failed Certificate Verifications based on OCSP Check:     0
  Failed Certificate Verifications (non OCSP):              28
  Total Failed Certificate Verifications due to Other Errors:       0
  Total Failed OCSP Requests:                               0
  Total Failed OCSP Requests due to Other Errors:           0
  Total Failed OCSP Requests due to Connection Errors:      0
  Total Failed OCSP Requests due to Connection Timeouts:    0
  Total Failed OCSP Requests due to Insufficient Resources:         0
```

DNS 관련 통계는 서버 이름 및 와일드카드 도메인 컨피그레이션의 문제를 해결하는 데 유용할 수 있습니다.이러한 통계를 검색하려면 다음과 같이 **show statistics accelerator ssl** 명령을 사용합니다 .

```
WAE# show statistics accelerator ssl
 . . .
 Number of forward DNS lookups issued:                      18
 Number of forward DNS lookups failed:                      0
 Number of flows with matching host names:                  8
 Number of reverse DNS lookups issued:                      46
 Number of reverse DNS lookups failed:                      4
 Number of reverse DNS lookups cancelled:                   0
 Number of flows with matching domain names:                40
 Number of flows with matching any IP rule:                 6
 . . .
 Pipe-through due to domain name mismatch:                  6
 . . .
```

SSL 재핸드셰이크 관련 통계는 문제 해결에 유용할 수 있으며 **show statistics accelerator ssl** 명령에서 다음 필터를 사용하여 검색할 수 있습니다.

```
WAE# show statistics accelerator ssl | inc renegotiation
  Total renegotiations requested by server:                 0
  Total SSL renegotiations attempted:                       0
  Total number of failed renegotiations:                    0
  Flows dropped due to renegotiation timeout:               0
```

show statistics **connection optimized ssl** 명령을 사용하여 WAAS 디바이스에서 최적화된 SSL 연결을 설정하는지 확인합니다.연결에 대한 Accel 열에 "TDLS"가 나타나는지 확인합니다."S"는 SSL AO가 다음과 같이 사용되었음을 나타냅니다.

```
WAE674# sh stat conn opt ssl
Current Active Optimized Flows:                       3
   Current Active Optimized TCP Plus Flows:           3
   Current Active Optimized TCP Only Flows:           0
   Current Active Optimized TCP Preposition Flows:    1
Current Active Auto-Discovery Flows:                  0
Current Active Pass-Through Flows:                    0
Historical Flows:                                     100

D:DRE,L:LZ,T:TCP Optimization,
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID  Local IP:Port         Remote IP:Port        PeerID             Accelerator
342     10.56.94.101:3406    10.10.100.100:443      0:1a:64:d3:2f:b8   TDLS                 <---
--Look for "S"
```

show statistics connection closed ssl 명령을 사용하여 닫힌 연결에 대한 연결 통계를 확인할 수 있습니다.

연결이 최적화되지 않는 경우 WCCP/PBR이 올바르게 구성되고 작동하는지 확인하고 비대칭 라우팅을 확인합니다.

show statistics connection optimized ssl detail 명령을 사용하여 SSL 연결 통계를 볼 수 있습니다. 여기서 구성된 SSL 가속 서비스에서 발생하는 동적 정책을 확인할 수 있습니다.**참고:**구성된 정책은 TFO 최적화만 적용되지만 구성된 SSL 서비스의 결과로 전체 최적화가 적용됩니다.

```
WAE674# sh stat connection optimized ssl detail
Connection Id:             1633
   Peer Id:                   00:14:5e:84:24:5f
   Connection Type:           EXTERNAL CLIENT
   Start Time:                Wed Jul 15 06:35:48 2009
   Source IP Address:         10.10.10.10
   Source Port Number:        2199
   Destination IP Address:    10.10.100.100
   Destination Port Number:   443
   Application Name:          SSL
   Classifier Name:           HTTPS
   Map Name:                  basic
   Directed Mode:             FALSE
   Preposition Flow:          FALSE
   Policy Details:
          Configured:         TCP_OPTIMIZE                                          <------TFO only
is configured
             Derived:         TCP_OPTIMIZE + DRE + LZ
                Peer:         TCP_OPTIMIZE
          Negotiated:         TCP_OPTIMIZE + DRE + LZ
             Applied:         TCP_OPTIMIZE + DRE + LZ                               <------Full
optimization applied
   Accelerator Details:
               Configured:    None
                  Derived:    None
                  Applied:    SSL                                                   <------SSL
acceleration applied
                     Hist:    None
```

```
                                        Original           Optimized
                                   ------------------- -------------------
   Bytes Read:                                1318                 584
   Bytes Written:                              208                1950
. . .
```

이 출력의 뒷부분에서는 확장 SSL 세션 레벨 세부사항이 다음과 같이 표시됩니다.

```
. . .
SSL : 1633

  Time Statistics were Last Reset/Cleared:                          Tue Jul 10 18:23:20 2009
  Total Bytes Read:                                                 0         0
  Total Bytes Written:                                              0         0
  Memory address:                                                   0x8117738
  LAN bytes read:                                                   1318
  Number of reads on LAN fd:                                        4
  LAN bytes written out:                                            208
  Number of writes on LAN fd:                                       2
  WAN bytes read:                                                   584
  Number of reads on WAN fd:                                        23
  WAN bytes written out:                                            1950
  Number of writes on WAN fd:                                       7
  LAN handshake bytes read:                                         1318
  LAN handshake bytes written out:                                  208
  WAN handshake bytes read:                                         542
  WAN handshake bytes written out:                                  1424
  AO bytes read:                                                    0
  Number of reads on AO fd:                                         0
  AO bytes written out:                                             0
  Number of writes on AO fd:                                        0
  DRE bytes read:                                                   10
  Number of reads on DRE fd:                                        1
  DRE bytes written out:                                            10
  Number of writes on DRE fd:                                       1
  Number of renegotiations requested by server:                     0
  Number of SSL renegotiations performed:                           0
  Flow state:                                                       0x00080000
  LAN work items:                                                   1
  LAN conn state:                                                   READ
  LAN SSL state:                                                    SSLOK (0x3)
  WAN work items:                                                   0
  WAN conn state:                                                   READ
  WAN SSL state:                                                    SSLOK (0x3)
  W2W work items:                                                   1
  W2W conn state:                                                   READ
  W2W SSL state:                                                    SSLOK (0x3)
  AO  work items:                                                   1
  AO  conn state:                                                   READ
  DRE work items:                                                   1
  DRE conn state:                                                   READ
  Hostname in HTTP CONNECT:                                                    <-----
```

```
Added in 4.1.5
  IP Address in HTTP CONNECT:                                                    <-----
Added in 4.1.5
  TCP Port in HTTP CONNECT:                                                      <-----
Added in 4.1.5
```

HTTP AO에서 SSL AO 핸드오프 연결 문제 해결

클라이언트가 HTTPS 서버에 연결하기 위해 프록시를 통과해야 하는 경우 클라이언트의 요청은 먼저 프록시에 대한 HTTP CONNECT 메시지(CONNECT 메시지에 포함된 실제 HTTPS 서버 IP 주소 포함)로 이동합니다. 이 시점에서 HTTP AO는 피어 WAE에서 이 연결을 처리합니다.프록시는 클라이언트와 서버 포트 간에 터널을 생성하고 클라이언트와 해당 서버 IP 주소 및 포트 간에 후속 데이터를 릴레이합니다.프록시는 클라이언트에 다시 응답하고 "200 OK" 메시지를 표시하며 클라이언트가 SSL을 통해 서버와 통신하려고 하므로 SSL AO에 대한 연결을 해제합니다.그런 다음 클라이언트는 프록시에 의해 설정된 TCP 연결(터널)을 통해 SSL 서버와의 SSL 핸드셰이크를 시작합니다.

핸드오프 연결 문제를 해결할 때 다음 사항을 확인합니다.

- **show statistics accelerator http** 명령의 출력을 확인하여 연결이 HTTP AO에 의해 처리되었는지 확인한 다음 SSL AO로 전달합니다.Total Handled Connections(처리된 총 연결 수) 및 Total Connections Handshed-off to SSL 카운터를 확인합니다.문제가 있는 경우 다음을 확인합니다.
  - HTTP AO가 활성화되고 피어 WAE에서 실행 중인 상태입니다.
  - SSL 가속화 서비스는 클라이언트가 CONNECT URL에서 사용하는 포트(또는 HTTPS를 사용하는 경우 묵시적 포트 443)로 구성됩니다. 프록시 포트가 CONNECT URL 포트와 다른 경우가 많으며 이 프록시 포트는 SSL 가속 서비스에서 구성하지 않아야 합니다.그러나 프록시 포트는 HTTP AO에 매핑된 트래픽 분류자에 포함되어야 합니다.
- **show statistics accelerator http** 명령의 출력을 확인하여 이 연결이 SSL AO에 의해 처리되고 최적화되었는지 확인합니다.Total Handled Connections(총 처리된 연결 수) 및 Total Optimized Connections(총 최적화된 연결 수) 카운터를 확인합니다.통계 카운터가 올바르지 않으면 이전 섹션에서 설명한 대로 기본 SSL 문제 해결을 수행합니다.
- 데이터 센터 WAE에서 **show statistics connection optimized detail** 명령 출력에 실제 SSL 서버의 호스트 이름, IP 주소 및 TCP 포트가 표시되는지 확인합니다.이러한 필드가 올바르게 설정되지 않은 경우 다음을 확인하십시오.
  - 클라이언트 브라우저 프록시 설정이 올바른지 확인합니다.
  - DNS 서버가 데이터 센터 WAE에 구성되어 있고 연결할 수 있는지 확인합니다.**ip name-server** ***A.B.C.D*** 명령을 사용하여 WAE에서 DNS 서버를 구성할 수 있습니다.

서버 인증서 확인 문제 해결

서버 인증서를 확인하려면 데이터 센터 WAE로 올바른 CA 인증서를 가져와야 합니다.

서버 인증서 확인을 트러블슈팅하려면 다음 단계를 수행합니다.

1. 서버 인증서를 검사하고 발급자 이름을 검색합니다.서버 인증서 내의 이 발급자 이름은 일치하는 CA 인증서 내의 주체 이름과 일치해야 합니다.PEM 인코딩 인증서가 있는 경우 openssl이 설치된 서버에서 다음 openssl 명령을 사용할 수 있습니다.

```
> openssl x509 -in cert-file-name -noout -text
```

2. show running-**config** 명령을 사용하여 데이터 센터 WAE에 일치하는 암호화 pki ca 컨피그레이션이 있는지 확인합니다.확인 프로세스에서 WAE에서 사용할 CA 인증서의 경우 가져온 각 CA 인증

서에 대해 crypto pki ca 컨피그레이션 항목이 필요합니다.예를 들어 CA 인증서 company1.ca를 가져오는 경우 데이터 센터 WAE에서 다음 컨피그레이션을 수행해야 합니다.

```
crypto pki ca company1
   ca-certificate company1.ca
   exit
```

참고: Central Manager GUI를 사용하여 CA 인증서를 가져오는 경우 Central Manager는 가져온 CA 인증서를 포함하도록 위의 crypto pki ca 컨피그레이션을 자동으로 추가합니다.그러나 CLI를 통해 CA 인증서를 가져오는 경우 위 컨피그레이션을 수동으로 추가해야 합니다.

3. 확인 중인 인증서에 인증서 체인이 포함되어 있는 경우 인증서 체인이 일치하고 가장 높은 발급자의 CA 인증서를 WAE에서 가져오는지 확인합니다.openssl verify 명령을 **사용하여** 인증서를 먼저 별도로 확인합니다.

4. 확인이 계속 실패하면 SSL 가속기 디버그 로그를 검사합니다.다음 명령을 사용하여 디버그 로깅을 활성화합니다.

```
wae# config
wae(config)# logging disk priority debug
wae(config)# logging disk enable
wae(config)# exit
wae# undebug all
wae# debug accelerator ssl verify
wae# debug tfo connection all
```

5. 테스트 연결을 시작한 다음 /local/local1/errorlog/sslao-errorlog.current 로그 파일을 검사합니다.이 파일은 서버 인증서에 포함된 발급자 이름을 나타내야 합니다.이 발급자 이름이 CA 인증서의 주체 이름과 정확히 일치하는지 확인합니다.

로그에 다른 내부 오류가 있는 경우 추가 디버그 옵션을 활성화하는 것이 도움이 될 수 있습니다.

6. 발급자 이름과 주체 이름이 일치하더라도 CA 인증서가 올바르지 않을 수 있습니다.이 경우 서버 인증서가 잘 알려진 CA에서 발급되면 브라우저를 사용하여 WAAS 없이 서버에 직접 연결할 수 있습니다.브라우저에서 연결을 설정할 때 브라우저 창의 오른쪽 아래에 나타나는 잠금 아이콘 또는 브라우저의 주소 표시줄 내에서 인증서를 검사할 수 있습니다.인증서 세부 정보는 이 서버 인증서와 일치하는 적절한 CA 인증서를 나타낼 수 있습니다.CA 인증서 내에서 Serial Number(일련 번호) 필드를 선택합니다.이 일련 번호는 데이터 센터 WAE에서 가져오는 인증서의 일련 번호와 일치해야 합니다.

7. OCSP 폐기 검사를 사용하도록 설정한 경우 이를 비활성화하고 자체 인증서 확인이 작동하는지 확인합니다.OCSP 설정 문제 해결에 대한 자세한 내용은 "OCSP 해지 확인 문제 해결" 섹션을 참조하십시오.

클라이언트 인증서 확인 문제 해결

클라이언트 인증서 확인은 원본 서버 및/또는 데이터 센터 WAE에서 활성화될 수 있습니다.WAAS를 사용하여 SSL 트래픽을 가속화할 경우 원본 서버에서 받은 클라이언트 인증서는 데이터 센터 WAE 또는 데이터 센터 WAE 머신 자체 서명 인증서의 crypto ssl **services global-settings** 명령에 지정된 machine-cert-key에 표시된 인증서입니다.따라서 원본 서버에서 클라이언트 인증서 확인이 실패할 경우 데이터 센터 WAE 머신 인증서가 원본 서버에서 확인되지 않기 때문일 수 있습니다.

데이터 센터 WAE에 대한 클라이언트 인증서 검증이 작동하지 않는 경우 클라이언트 인증서와 일

치하는 CA 인증서를 데이터 센터 WAE에서 가져오지 않기 때문일 수 있습니다.WAE에서 올바른 CA 인증서를 가져왔는지 확인하는 방법에 대한 지침은 "서버 인증서 확인 문제 해결" 섹션을 참조하십시오.

피어 WAE 인증서 확인 문제 해결

피어 인증서 확인 문제를 해결하려면 다음 단계를 수행하십시오.

1. 확인 중인 인증서가 CA 서명 인증서인지 확인합니다.한 WAE에 의한 자체 서명 인증서는 다른 WAE에 의해 확인되지 않습니다.기본적으로 WAE는 자체 서명 인증서로 로드됩니다.자체 서명 인증서는 crypto ssl **services global-settings machine-cert-key** 명령을 사용하여 구성해야 합니다.

2. 인증서를 확인하는 디바이스에 올바른 CA 인증서가 로드되었는지 확인합니다.예를 들어 데이터 센터 WAE에 peer-cert-verify가 구성된 경우 지사 WAE 인증서가 CA 서명 및 데이터 센터 WAE에서 동일한 서명 CA의 인증서를 가져와야 합니다.CLI를 통해 수동으로 인증서를 가져오는 경우 가져온 인증서를 사용하기 위해 crypto pki ca 명령을 사용하여 CA를 만드는 것을 잊지 마십시오.Central Manager GUI에서 가져오면 Central Manager는 일치하는 암호화 PKI 구성을 자동으로 생성합니다.

3. 피어 WAE의 확인이 여전히 실패하는 경우 "SSL AO 로깅" 섹션에 설명된 대로 디버그 로그를 확인합니다.

OCSP 해지 확인 문제 해결

시스템에서 OCSP(Online Certificate Status Protocol) 폐기 검사를 활성화하여 SSL 연결에 문제가 있는 경우 다음 문제 해결 단계를 수행하십시오.

1. OCSP responder 서비스가 responder 서버에서 실행 중인지 확인합니다.
2. WAE와 responder 간의 올바른 연결을 보장합니다.WAE에서 **ping** 및 **텔넷** 명령(해당 포트에 대한)을 사용하여 확인합니다.
3. 검증 중인 인증서가 실제로 유효한지 확인합니다.만료 날짜 및 올바른 응답자 URL은 일반적으로 문제가 있는 영역입니다.
4. WAE에서 OCSP 응답용 인증서를 가져왔는지 확인합니다.OCSP 응답자의 응답도 서명되며 OCSP 응답과 일치하는 CA 인증서가 WAE에 있어야 합니다.
5. show statistics accelerator **ssl** 명령 출력을 확인하여 OCSP 통계를 확인하고 OCSP 장애에 해당하는 카운터를 확인합니다.
6. OCSP HTTP 연결이 HTTP 프록시를 통과하는 경우 프록시를 비활성화하여 도움이 되는지 확인합니다.도움이 되는 경우 프록시 컨피그레이션에서 연결 실패를 유발하지 않는지 확인합니다.프록시 컨피그레이션이 정상인 경우 HTTP 헤더의 특성 중 일부가 있을 수 있으며, 이로 인해 프록시와 호환되지 않을 수 있습니다.추가 조사를 위해 패킷 추적을 캡처합니다.
7. 다른 모든 작업이 실패하면 추가 디버깅을 위해 발신 OCSP 요청의 패킷 추적을 캡처해야 할 수 있습니다.예비 WAAS 문제 해결 기사의 "패킷 캡처 및 분석" 섹션에 설명된 대로 tcpdump 또는 **tethereal** 명령을 사용할 수 있습니다.

데이터 센터 WAE에서 OCSP 응답자에게 연결하는 데 사용하는 URL은 다음 두 가지 방법 중 하나로 파생됩니다.

- crypto pki **global-settings** 컨피그레이션 명령으로 구성된 고정 OCSP URL
- 확인 중인 인증서에 지정된 OCSP URL

확인 중인 인증서에서 URL이 파생되는 경우 URL에 연결할 수 있는지 확인해야 합니다.SSL 가속기 OCSP 디버그 로그를 활성화하여 URL을 확인한 다음 응답자에 대한 연결을 확인합니다.디버그 로그 사용에 대한 자세한 내용은 다음 섹션을 참조하십시오.

DNS 구성 문제 해결

시스템이 서버 이름 및 서버 도메인 구성을 사용하여 SSL 연결을 최적화하는 데 문제가 있는 경우 다음 트러블슈팅 단계를 수행하십시오.

1. WAE에 구성된 DNS 서버에 연결할 수 있고 이름을 확인할 수 있는지 확인합니다.구성된 DNS 서버를 확인하려면 다음 명령을 사용합니다.

```
WAE# sh running-config | include name-server
ip name-server 2.53.4.3

Try to perform DNS or reverse DNS lookup on the WAE using the following commands:

WAE# dnslookup www.cisco.com
The specified host/domain name is unknown !
```

이 응답은 구성된 이름 서버에서 이름을 확인할 수 없음을 나타냅니다.

구성된 이름 서버에 대해 ping/traceoute를 사용하여 연결 가능성 및 왕복 시간을 확인합니다.

```
WAE# ping 2.53.4.3
PING 2.53.4.3 (2.53.4.3) 56(84) bytes of data.
--- 2.53.4.3 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4008ms


WAE# traceroute 2.53.4.3
traceroute to 2.53.4.3 (2.53.4.3), 30 hops max, 38 byte packets
1  2.53.4.33 (2.53.4.33)  0.604 ms  0.288 ms  0.405 ms
2  * * *
3  * * *
4  * * *
5  * * *
```

2. DNS 서버에 연결할 수 있고 이름을 확인할 수 있지만 SSL 연결이 최적화되지 않는 경우 지정된 도메인 또는 호스트 이름을 구성하는 가속화된 서비스가 활성 상태이고 SSL AO에 대한 경보가 없는지 확인합니다.다음 명령을 사용합니다.

```
WAE#  show alarms
Critical Alarms:
----------------
      Alarm ID                 Module/Submodule              Instance
  ---------------            --------------------          ---------------
  1 accl_svc_inactive         sslao/ASVC/asvc-host         accl_svc_inactive
  2 accl_svc_inactive         sslao/ASVC/asvc-domain       accl_svc_inactive

Major Alarms:
-------------
None

Minor Alarms:
-------------
None
```

"accl_svc_inactive" 경보가 있는 것은 가속화된 서비스 컨피그레이션에 일부 불일치가 있으며 서버 항목에 대한 컨피그레이션이 겹치는 하나 이상의 가속화된 서비스가 있을 수 있음을 나타냅니다.가속화된 서비스 컨피그레이션을 확인하고 컨피그레이션이 올바른지 확인합니다.다음 명령을 사용하

여 컨피그레이션을 확인합니다.

```
WAE# show crypto ssl accelerated service
Accelerated Service     Config State    Oper State      Cookie
-------------------     ------------    -----------     ------
asvc-ip                  ACTIVE          ACTIVE          0
asvc-host                ACTIVE          INACTIVE        1
asvc-domain              ACTIVE          INACTIVE        2
```

특정 가속화된 서비스에 대한 세부 정보를 확인하려면 다음 명령을 사용합니다.

```
WAE# show crypto ssl accelerated service asvc-host
 Name: asvc-host
   Config state: ACTIVE, Oper state: INACTIVE, Cookie: 0x3, Error vector: 0x0
   No server IP addresses are configured
   The following server host names are configured:
     lnxserv.shilpa.com port 443
         Host 'lnxserv.shilpa.com' resolves to following IPs:
         --none--
   No server domain names are configured
```

가속화된 서비스의 작동 상태가 INACTIVE일 수 있는 이유 중 하나는 DNS 실패입니다.예를 들어 가속화된 서비스 컨피그레이션에 서버 호스트 이름이 있고 WAE가 서버 IP 주소를 확인할 수 없는 경우 적절한 동적 정책을 구성할 수 없습니다.

3. "도메인 이름이 일치하지 않아 파이프스루"에 대한 통계 카운터가 증가하는 경우 최적화를 위해 구성된 서버에 대한 SSL 연결임을 나타냅니다.다음 명령을 사용하여 정책 엔진 항목을 확인합니다.

```
WAE#sh policy-engine application dynamic
       Number:     1   Type: Any->Host (6)  User Id: SSL (4)
       Src: ANY:ANY  Dst: 2.53.4.2:443
       Map Name: basic
       Flags: TIME_LMT DENY
       Seconds: 10  Remaining: 5  DM Index: 32767
       Hits: 1  Flows: - NA -  Cookie: 0x2EEEEEE
       DM Ref Index: - NA -  DM Ref Cnt: 0
```

show statistics connection 명령을 사용하여 연결 상태를 확인합니다.첫 번째 연결은 TSGDL의 가속기와 후속 연결을 표시해야 합니다. TIME_DENY 정책 항목의 수명이 TDL이어야 합니다.

4. 데이터 센터 WAE와 관련하여 DNS 서버가 WAN을 통해 있거나 역방향 DNS 응답 시간이 너무 긴 경우 일부 연결이 삭제될 수 있습니다.클라이언트 시간 초과 및 rDNS 응답 시간에 따라 달라집니다.이 경우 "Number of reverse DNS lookups cancelled(역방향 DNS 조회 수 취소됨)"에 대한 카운터가 증가하고 연결이 삭제됩니다.이 상황은 DNS 서버가 응답하지 않거나 매우 느리거나 WAAS의 NSCD가 작동하지 않음을 나타냅니다.**show alarms** 명령을 사용하여 NSCD 상태를 확인할 수 있습니다.대부분의 구축에서 DNS 서버가 데이터 센터 WAE와 동일한 LAN에 있을 것으로 예상되기 때문에 이러한 일이 발생할 가능성은 매우 낮습니다.

HTTP에서 SSL AO 체이닝 문제 해결

참고:HTTP-SSL AO 체이닝이 WAAS 버전 4.3.1에 도입되었습니다. 이 섹션은 이전 WAAS 버전에는 적용되지 않습니다.

체이닝 기능을 사용하면 AO는 플로우의 수명 동안 언제든지 다른 AO를 삽입할 수 있으며, 두 AO는 플로우에 독립적으로 AO별 최적화를 적용할 수 있습니다.AO 체이닝은 4.3.1 이전 릴리스에서 WAAS가 제공하는 AO 핸드오프 기능과 다릅니다. AO 체이닝으로 인해 첫 번째 AO는 계속 흐름을 최적화하기 때문입니다.

SSL AO는 두 가지 유형의 연결을 처리합니다.

- Byte-0 SSL:SSL AO는 먼저 연결을 수신하고 SSL 핸드셰이크를 완료합니다.페이로드의 초기 부분을 구문 분석하여 HTTP 메서드를 확인합니다.페이로드가 HTTP를 나타내는 경우 HTTP AO를 삽입합니다.그렇지 않은 경우 일반 TSDL 최적화를 적용합니다.
- 프록시 연결:HTTP AO는 먼저 연결을 수신합니다.클라이언트의 요청에서 CONNECT 헤더 방법을 식별하고 프록시가 200 OK 메시지로 확인한 후 SSL AO를 삽입합니다.

SSL AO는 다음 HTTP 방법을 탐지하는 경량 HTTP 파서를 사용합니다.GET, HEAD, POST, PUT, OPTIONS, TRACE, COPY, LOCK, BCOPY, BMOVE, MCOL, DELETE, SEARCH, UNLOCK, BDELETE, PROPFIND, PROPPATCH, SUBSCRIBE, BPROPPATCH, UNSUBSCRIBE, AND_MS_ENUMATTS.**debug accelerator ssl parser** 명령을 사용하여 파서와 관련된 문제를 디버깅할 수 있습니다.show stat accel **ssl payload http/other** 명령을 사용하여 페이로드 유형에 따라 분류된 트래픽의 통계를 볼 수 있습니다.

문제 해결 팁:

1. HTTP AO에서 소유하므로 HTTP AO 컨피그레이션에서 HTTPS 기능이 활성화되어 있는지 확인합니다.자세한 내용은 HTTP AO 문제 해결 문서를 참조하십시오.
2. **show stat connection** 명령을 사용하여 연결 상태를 확인합니다.올바르게 최적화된 경우 TCP, HTTP, SSL 및 DRE-LZ 최적화를 나타내는 THSDL을 표시해야 합니다.이러한 최적화 중 하나라도 없으면 해당 최적화 프로그램(SSL, HTTP 등)에서 추가로 디버깅합니다. 예를 들어 연결 상태가 THDL을 표시하는 경우 SSL 최적화가 연결에 적용되지 않았음을 의미합니다.다음은 SSL AO와 관련된 디버깅 문제에 대한 세부 정보입니다.
3. SSL AO가 활성화되어 있고 실행 중 상태인지 확인합니다("SSL AO 문제 해결" 섹션 참조).
4. **show alarms** 명령을 사용하여 경보가 없는지 확인합니다.
5. SSL 트래픽이 최적화되지 않는 경우 가속화된 서비스의 일부로 서버 IP 주소, 호스트 이름 또는 도메인 이름 및 포트 번호가 추가되어야 합니다.
6. 가속화된 서비스가 **show crypto ssl services accelerated-service *ASVC-name*** 명령을 사용하여 ACTIVE **상태인지** 확인합니다("Troubleshooting DNS Configuration" 섹션 참조).
7. **show policy-engine application dynamic** 명령을 사용하여 정책 엔진에 이 서버 및 포트에 대한 항목이 있는지 확인합니다.
8. 목적지 서버가 기본이 아닌 포트에서 SSL을 사용하는 경우(기본값은 443) 정책 엔진 컨피그레이션에 이 항목이 반영되었는지 확인합니다.Central Manager는 SSL 트래픽 데이터를 보고하기 위해 이 정보를 사용합니다.
9. 구성된 호스트 이름이 **show crypto ssl services accelerated-service *ASVC-name*** 명령을 사용하여 유효한 IP 주소***로 확인되는지 확인합니다***.IP 주소를 찾을 수 없는 경우 이름 서버가 올바르게 구성되었는지 확인합니다.또한 dnslookup ***IP-address*** 명령의 출력을 확인합니다.

```
wae# sh run no-policy
. . .
crypto ssl services accelerated-service sslc
  version all
  server-cert-key test.p12
  server-ip 2.75.167.2 port 4433
```

```
  server-ip any port 443
  server-name mail.yahoo.com port 443
  server-name mail.google.com port 443
  inservice


wae# sh crypto ssl services accelerated-service sslc
Name: sslc
Config state: ACTIVE, Oper state: ACTIVE, Cookie: 0x0, Error vector: 0x0

   The following server IP addresses are configured:
     2.75.167.2 port 4433
     any port 443

   The following server host names are configured:
     mail.yahoo.com port 443
         Host 'mail.yahoo.com' resolves to following IPs:
         66.163.169.186

     mail.google.com port 443
         Host 'mail.google.com' resolves to following IPs:
         74.125.19.17
         74.125.19.18
         74.125.19.19
         74.125.19.83


wae# dnslookup mail.yahoo.com
Official hostname: login.lga1.b.yahoo.com
         address: 66.163.169.186
Aliases: mail.yahoo.com
Aliases: login.yahoo.com
Aliases: login-global.lgg1.b.yahoo.com

wae# dnslookup mail.google.com
Official hostname: googlemail.l.google.com
         address: 74.125.19.83
         address: 74.125.19.17
         address: 74.125.19.19
         address: 74.125.19.18
Aliases: mail.google.com
```

SSL AO 로깅

다음 로그 파일은 SSL AO 문제를 해결하는 데 사용할 수 있습니다.

- 트랜잭션 로그 파일:/local1/logs/tfo/working.log(및 /local1/logs/tfo/tfo_log_*.txt)
- 디버그 로그 파일:/local1/errorlog/sslao-errorlog.current(및 sslao-errorlog*)

디버깅을 보다 쉽게 하려면 먼저 패킷을 하나의 호스트로 제한하기 위해 ACL을 설정해야 합니다.

```
WAE674(config)# ip access-list extended 150 permit tcp host 10.10.10.10 any
WAE674(config)# ip access-list extended 150 permit tcp any host 10.10.10.10
```

트랜잭션 로깅을 활성화하려면 다음과 같이 **transaction-logs** 컨피그레이션 명령을 사용합니다.

```
wae(config)# transaction-logs flow enable
wae(config)# transaction-logs flow access-list 150
```

다음과 같이 **type-tail** 명령을 사용하여 트랜잭션 로그 파일의 끝을 볼 수 있습니다.

```
wae# type-tail tfo_log_10.10.11.230_20090715_130000.txt
Wed Jul 15 14:35:48 2009 :1633 :10.10.10.10 :2199 :10.10.100.100 :443 :OT :START  :EXTERNAL
CLIENT :00.14.5e.84.24.5f :basic
 :SSL :HTTPS :F :(TFO) (DRE,LZ,TFO) (TFO) (DRE,LZ,TFO) (DRE,LZ,TFO) :<None> :(None) (None)
(SSL) :<None> :<None>  :0 :332
Wed Jul 15 14:36:06
2009 :1633 :10.10.10.10 :2199 :10.10.100.100 :443 :SODRE :END :165 :15978764 :63429 :10339 :0
Wed Jul 15 14:36:06 2009 :1633 :10.10.10.10 :2199 :10.10.100.100 :443 :OT :END :EXTERNAL
CLIENT :(SSL) :468 :16001952 :80805 :27824
```

SSL AO의 디버그 로깅을 설정하고 활성화하려면 다음 명령을 사용합니다.

참고:디버그 로깅은 CPU를 많이 사용하며 대량의 출력을 생성할 수 있습니다.생산 환경에서 현명하게 그리고 드물게 사용하십시오.

다음과 같이 디스크에 대한 자세한 로깅을 활성화할 수 있습니다.

```
WAE674(config)# logging disk enable
WAE674(config)# logging disk priority detail
```

다음과 같이 ACL에서 연결에 대한 디버그 로깅을 활성화할 수 있습니다.

```
WAE674# debug connection access-list 150
```

SSL AO 디버깅 옵션은 다음과 같습니다.

```
WAE674# debug accelerator ssl ?
 accelerated-svc   enable accelerated service debugs
 alarm             enable SSL AO alarm debugs
 all               enable all SSL accelerator debugs
 am                enable auth manager debugs
 am-generic-svc    enable am generic service debugs
 bio               enable bio layer debugs
 ca                enable cert auth module debugs
 ca-pool           enable cert auth pool debugs
 cipherlist        enable cipherlist debugs
 client-to-server  enable client-to-server datapath debugs
 dataserver        enable dataserver debugs
 flow-shutdown     enable flow shutdown debugs
 generic           enable generic debugs
 ocsp              enable ocsp debugs
 oom-manager       enable oom-manager debugs
 openssl-internal  enable opnessl internal debugs
 peering-svc       enable peering service debugs
 session-cache     enable session cache debugs
 shell             enable SSL shell debugs
 sm-alert          enable session manager alert debugs
 sm-generic        enable session manager generic debugs
 sm-io             enable session manager i/o debugs
 sm-pipethrough    enable sm pipethrough debugs
 synchronization   enable synchronization debugs
 verify            enable certificate verification debugs
 waas-to-waas      enable waas-to-waas datapath debugs
```

SSL 연결에 대한 디버그 로깅을 활성화한 다음 디버그 오류 로그의 끝을 다음과 같이 표시할 수 있

습니다.

```
WAE674# debug accelerator ssl all
WAE674# debug connection all
Enabling debug messages for all connections.
Are you sure you want to do this? (y/n) [n]y
WAE674# type-tail errorlog/sslao-errorlog.current follow
```

NME 및 SRE 모듈의 인증서 만료 경보 문제 해결

SSL AO는 자체 서명된 시스템 인증서가 만료되었거나 만료 후 30일 이내인 경우 WAAS 디바이스에 맞춤형 글로벌 머신 인증서가 구성되지 않은 경우 경보를 생성합니다.WAAS 소프트웨어는 WAAS 장치의 첫 번째 시작으로부터 5년 만료 날짜의 공장 자체 서명 인증서를 생성합니다.

모든 WAAS NME 및 SRE 모듈의 시계는 NME 또는 SRE 모듈이 더 최신 버전인 경우에도 처음 시작 시 2006년 1월 1일로 설정됩니다.이로 인해 자체 서명 인증서가 2011년 1월 1일에 만료되고 디바이스에서 인증서 만료 경보를 생성합니다.

기본 팩터리 인증서를 전역 인증서로 사용하지 않고 SSL AO에 사용자 지정 인증서를 사용하는 경우 이 예기치 않은 만기가 발생하지 않으며 만료될 때마다 사용자 지정 인증서를 업데이트할 수 있습니다.또한 NME 또는 SME 모듈을 새 소프트웨어 이미지로 업데이트하여 시계를 최신 날짜로 동기화한 경우 이 문제가 발생하지 않을 수 있습니다.

인증서 만료 증상은 다음 경보 중 하나입니다(**show alarms** 명령의 출력에 표시됨).

```
Major Alarms:
-------------
       Alarm ID                 Module/Submodule               Instance
  ---------------             --------------------          ---------------
  1 cert_near_expiration      sslao/SGS/gsetting           cert_near_expiration
```

또는

```
      Alarm ID                 Module/Submodule               Instance
  ---------------             --------------------          ---------------
  1 cert_expired              sslao/SGS/gsetting           cert_expired
```

Central Manager GUI에서 다음과 같은 경보를 보고합니다."Certificate__waas-self__.p12가 만료에 가까워졌습니다. 전역 설정에서 머신 인증서로 구성됩니다."

다음 솔루션 중 하나를 사용하여 이 문제를 해결할 수 있습니다.

- 전역 설정에 대해 다른 인증서를 구성합니다.

```
SRE# crypto generate self-signed-cert waas-self.p12 rsa modulus 1024
SRE# config
SRE(config)# crypto ssl services global-settings machine-cert-key waas-self.p12
```

- 나중에 만료 날짜를 사용하여 자체 서명 팩토리 인증서를 업데이트합니다.이 솔루션에는 Cisco TAC에 문의하여 얻을 수 있는 스크립트가 필요합니다.

참고:이 문제는 WAAS 소프트웨어 버전 4.1.7b, 4.2.3c 및 4.3.3에서 릴리스된 주의 사항 CSCte05426의 해결에 의해 수정되었습니다. 인증 만료일은 2037로 변경됩니다.