인증서 및 키

인증서 및 키

TLS 인증서 및 키는 프록시 시나리오에서 멀티 클라우드 방어 게이트웨이에 의해 사용됩니다. 인그레스(역방향 프록시) 사용자는 멀티 클라우드 방어 게이트웨이을(를) 통해 애플리케이션에 액세스하며 서비스에 대해 구성된 인증서를 제공합니다. 이그레스(정방향 프록시)의 경우 외부 호스트의 인증서가 가장되고 정의된 인증서로 서명됩니다.

인증서 본문을 멀티 클라우드 방어 컨트롤러(으)로 가져옵니다. 개인 키는 다음과 같은 방식으로 제공할 수 있습니다.

- 개인 키 콘텐츠를 가져옵니다.
- AWS 암호 관리자에 저장하고 암호 이름을 제공합니다.
- AWS KMS에 저장하고 암호 텍스트 콘텐츠를 제공합니다.
- GCP 암호 관리자에 저장하고 암호 이름을 제공합니다.
- Azure 키 저장소 및 암호에 저장하고 키 저장소 및 암호 이름을 입력합니다.

테스트 목적으로 멀티 클라우드 방어 컨트롤러에서 자체 서명 인증서를 생성할 수도 있습니다. 이는 로컬 파일 시스템에서 개인 키 콘텐츠를 가져오는 것과 유사합니다.

Note 생성된 인증서는 편집할 수 없습니다. 기존 인증서를 교체해야 하는 경우, 새 인증서를 생성하고 새 인증서를 참조하도록 암호 해독 프로파일을 편집한 다음 기존 인증서를 삭제해야 합니다.

인증서 및 개인 키를 가져올 때 멀티 클라우드 방어 컨트롤러/UI는 불일치가 있는 경우 이를 탐지할 수 있습니다. 그러나 클라우드 서비스 제공자 내에 개인 키가 저장되어 있는 다른 가져오기 방법을 사용하는 경우, 멀티 클라우드 방어 컨트롤러/UI는 불일치가 있는 경우 이를 탐지할 수 없습니다. 이는 클라우드 서비스 제공자 내에서 개인 키를 비공개로 유지하기 위한 설계입니다. 멀티 클라우드 방어 게이트웨이에서 개인 키가 필요할 때 개인 키에 액세스하여 사용되며, 불일치가 발생하면 오류가 생성됩니다.

인증서 가져오기

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Method(**방법**)**에 대한 프롬프트가 나타나면 **Import your Certificate and Private Key(**인증서 및 개인 키 가져오기**)**를 선택합니다.

단계 **4** **Certificate Body(**인증서 본문**)**에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **5** **Certificate Private Key(**인증서 개인 키**)**에 있는 개인 키의 내용을 복사합니다.

단계 **6** (선택 사항) 인증서와 체인이 다른 파일에 있는 경우 체인을 **Certificate Chain(**인증서 체인**)**으로 가져옵니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

AWS - KMS

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** Method(방법)에서 *Import AWS - KMS(AWS* 가져오기 *- KMS)*를 선택합니다.

단계 **4** 클라우드 계정 및 지역을 선택합니다.

단계 **5** *Certificate Body(*인증서 본문*)*에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **6** AWK KMS 암호화 암호 텍스트를 *Private Key Cipher Text(*프라이빗 키 암호 텍스트*)*에 복사합니다. .

단계 **7** **Save(**저장**)**를 클릭합니다.

AWS - 암호 관리자

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** Method(방법)에서 *Import AWS - Secret(AWS* 가져오기 - 암호*)*을 선택합니다.

단계 **4** 클라우드 계정 및 지역을 선택합니다.

단계 **5** *Certificate Body(*인증서 본문*)*에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **6** 개인 키가 저장된 Secret Name(비밀 이름)을 제공합니다. 개인 키 콘텐츠는 AWS Secrets Manager에서 *Other type of Secrets(*기타 유형의 비밀*)* > *Plain Text(*일반 텍스트*)*로 저장해야 합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

Azure 키 저장소

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** Method(방법)에서 *Import Azure - Key Vault Secret(Azure* 가져오기 -키 저장소 암호)을 선택합니다.

단계 **4** 클라우드 계정 및 지역을 선택합니다.

단계 **5** *Certificate Body(*인증서 본문*)*에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **6** Key Vault Name(키 저장소 이름) 및 개인 키가 저장된 암호 이름을 제공합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

GCP - 암호 관리자

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)** 클릭

단계 **3** Method(방법)에서 *Import GCP - Secret(*가져오기 *GCP* - 암호*)*을 선택합니다.

단계 **4** 클라우드 계정을 선택합니다.

단계 **5** 암호 이름(전체 경로) 및 암호 버전을 제공합니다.

단계 **6** *Certificate Body(*인증서 본문*)*에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

서버 인증서 검증

게이트웨이가 정방향 프록시로 작동할 경우에는 서버 인증서 검증이 트래픽 처리에 자동으로 포함됩니다. 트래픽을 처리하기 위해 지정된 서버 인증서 검증 작업이 필요하지는 않지만, 일반적인 보안을 향상시킬 수 있습니다. 기본적으로 서버 인증서 검증이 활성화되어 있지 않으며 유효하지 않은 서버 인증서가 있을 수 있는 서버로 이동하는 트래픽은 통과합니다. 서버 인증서 검증 작업을 활성화하여 허용해서는 안 되는 트래픽 또는 서버 인증서 검증 상태와 상관없이 신뢰해야 하는 특정 트래픽에 대한 규칙의 우선 순위를 지정합니다.

참고 이 검증 프로세스는 정방향 프록시 환경 및 암호 해독이 활성화된 경우에만 적용됩니다.

일반 규칙 작업의 TLS 암호 해독 프로파일에서 서버 인증서 검증 작업을 활성화하는 것이 좋습니다. TLS 암호 해독 선택을 재정의해야 하는 경우 FQDN 서비스 개체를 수정하여 검증 작업을 활성화할 수 있습니다. 두 가지 방법으로 서버 인증서 검증을 포함하고 활성화할 수 있습니다.

- TLS 암호 해독 프로파일의 서버 인증서 검증
- FQDN 서비스 개체의 서버 인증서 검증

TLS 암호 해독 프로파일의 서버 인증서 검증

TLS 암호 해독 프로파일 내에서 서버 인증서 검증을 위한 작업을 선택하는 경우, 이 암호 해독 프로파일을 사용하는 모든 규칙 집합에서 이 작업이 사용됩니다. 기본적으로 검증 작업은 서버 인증서의 유효 여부에 관계없이 모든 트래픽을 허용하도록 구성되며 멀티 클라우드 방어은(는) HTTP 로그 내에 알림을 생성하지 않습니다.

참고 **Log(**로그**)**에 대한 검증 확인을 활성화한 경우 **Investigate(**조사**)** > **Flow Analytics(**플로우 분석**)** > **HTTPS Logs(HTTPS** 로그**)**에서 로그를 찾습니다.

다음 절차를 사용하여 TLS 암호 해독 프로파일에서 서버 인증서 검증을 활성화합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Profiles(**프로파일**)** > **Decryption(**암호 해독**)**으로 이동합니다.

단계 **2** 서버 인증서 검증을 추가할 TLS 암호 해독 프로파일을 선택합니다. 프로파일이 준비되지 않았다면 여기에서 생성하십시오. 자세한 내용은 암호 해독 프로파일를 참조하십시오.

단계 **3** 암호 해독 프로파일을 편집합니다.

단계 **4** **Profile Properties(**프로파일 속성**)** 섹션에서 **Invalid Server Certificate Action(**유효하지 않은 서버 인증서 작업**)** 드롭다운 목록을 확장합니다.

단계 **5** 다음 옵션 중 하나를 선택합니다.

- **Deny Log(**거부 로그**)** - 이 옵션은 검증된 서버 인증서를 제공하지 않는 연결을 자동으로 삭제하고 인시던트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)**- 이 옵션은 검증된 서버 인증서를 제공하지 않으며 인시던트를 로깅하지 않는 연결을 자동으로 삭제합니다.
- **Allow Log(**허용 로그**)** - 이 옵션은 검증된 서버 인증서를 제공하지 않는 연결의 통과를 허용하고 인시던트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**)**- 이 옵션은 검증된 서버 인증서를 제공하지 않는 연결이 통과하도록 허용하며, 인시던트를 로깅하지 않습니다. 이것이 기본 작업 선택 사항입니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

TLS 암호 해독 프로파일이 전달 프록시 서비스 개체와 올바르게 연결되어 있는지 확인하십시오. 자세한 내용은 전달 프록시 서비스 개체(이그레스/이스트-웨스트)를 참조하십시오.

TLS 암호 해독 프로파일이 서비스 개체에 포함되면 정책 내의 규칙 순서가 원하는 트래픽 처리 방법을 지원하는 순서로 지정되었는지 확인합니다.

FQDN 서비스 개체의 서버 인증서 검증

FQDN 서비스 개체 내 잘못된 서버 인증서 검증은 선택 사항입니다. 지정된 경우 TLS 암호 해독 프로파일에 지정된 동작을 재정의합니다. 여기서 선택 항목을 지정하지 않으면 추가 작업이 없거나 재정의 작업이 수행되지 않습니다. FQDN 서비스 개체 내에서 유효하지 않은 서버 인증서 검증을 사용하여 특정 서버로 향하는 트래픽을 차단하거나 허용할 수 있습니다. 다른 방법으로는 TLS 암호 해독 프로파일에 의해 차단되거나 허용될 수 있습니다.

로그 검증 확인을 활성화하면 이러한 로그는 **Investigate(**검사**)** > **Flow Analytics(**플로우 분석**)** > **HTTPS Logs(HTTPS** 로그**)**에 위치합니다.

FQDN 서비스 개체에 서버 인증서 검증 작업을 포함하려면 다음 절차를 사용합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Security Profile(**보안 프로필**)** > **FQDNs**로 이동합니다.

단계 **2** 수정할 FQDN 서비스 개체를 선택합니다.

단계 **3** 선택한 FQDN 서비스 개체를 편집합니다.

단계 **4** 규칙 집합에 포함된 FQDN 서비스 개체의 목록에서 **Invalid Server Certificate Action(**유효하지 않은 서버 인증서 작업**)** 드롭다운 메뉴를 확장하고 다음 옵션 중 하나를 선택합니다.

- **Deny Log(**거부 로그**)** - 검증된 서버 인증서를 제공하지 않는 연결을 자동으로 삭제하고 인시던트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)** - 검증된 서버 인증서를 제공하지 않으며 인시던트를 로깅하지 않는 연결을 자동으로 삭제합니다.

- **Allow Log(**허용 로그**) -** 검증된 서버 인증서를 제공하지 않는 연결의 통과를 허용하고 인시던트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**) -** 서버 인증서를 제공하지 않는 연결이 통과하도록 허용하며, 인시던트를 로깅하지 않습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

FQDN 서비스 개체가 규칙 또는 규칙 집합과 올바르게 연결되어 있는지 확인하십시오. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

FQDN 서비스 개체가 정책에 설정된 규칙 또는 규칙과 성공적으로 연결되면 정책의 규칙 순서가 원하는 트래픽 처리 방법을 지원하는 순서로 지정되어 있는지 확인합니다.