# Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance 안내 - Mudhra 루트 및 중간 인증 기관에 대한 긴급 불신

## 목차

# 목적

아래는 Cisco FTD(Secure Firewall Threat Defense), Cisco FMC(Secure Firewall Management Center) 및 ASA(Adaptive Security Appliance)에 대한 안내로, Mudhra 루트 및 중간 인증 기관에 대한 긴급 불신을 방지합니다.

# FMC 로컬 Cisco-service 인증서 번들 업데이트

FMC 및 FTD는 어플라이언스에서 시스코 서비스로의 TLS 연결에 사용되는 로컬 CA 번들을 자동으로 업데이트할 수 있습니다(예: Smart Licensing 및 소프트웨어, VDB, SRU, 지오로케이션 업데이트). 시스템은 시스템 정의 시간에 매일 검사합니다. Cisco 문서에는 FMC/FTD 7.0.5, 7.1.0.3, 7.2.4 및 7.3.0 이상부터 제공되는 기능이 있습니다. 이는 기능 임계값이며 권장 업그레이드 대상이 아닙니다. 정확한 플랫폼, 소스 릴리스, 호환성 요구 사항 및 최신 Cisco 릴리스 지침을 사용하여 업그레이드 대상을 선택합니다. [3, 4]

지원되는 FMC 또는 FTD CLI에서 `show cert-update`는 자동 업데이트 상태, 일별 일정 및 번들의 마지막 수정 시간을 보고합니다. `configure cert-update test`는 로컬 번들의 현재 상태와 업데이트 연결이 준비되었는지 확인합니다. [4, 5, 6]

이 Cisco 서비스 번들은 SSL 해독에 사용되는 FTD의 구성된 신뢰할 수 있는 CA 객체/그룹 및 ID 또는 VPN 인증서에 사용되는 디바이스 신뢰 지점과는 별개입니다. 이러한 인증서가 구성에 수동으로 추가되지 않았는지 확인해야 합니다. [5, 6]

# ASA CA 신뢰 풀 자동 가져오기

ASA에서 CA 신뢰 풀 및 명명된 신뢰 지점은 별도의 인증서 관리 기능입니다. 신뢰 풀은 CA 인증서

를 보유합니다. 신뢰 지점은 인증서 ID 및 CA 등록에 사용되는 명명된 컨피그레이션입니다. ASA 신뢰 풀 자동 가져오기는 위에서 설명한 FMC/FTD Cisco-service 번들 업데이트와도 별개입니다. [8, 9]

읽기 전용 확인의 경우 `show crypto ca trustpool policy`를 실행하여 신뢰 풀 인증서 수, 가져오기 상태 및 결과, 다음 예약 시도, 유효한 정책 세부 정보를 검토합니다. 구성된 `trustpool 정책 라인을` 검토하려면 show run crypto ca trustpool policy를 실행합니다. Cisco는 기본적으로 자동 가져오기를 off로 문서화합니다. 재정의 없이 활성화된 경우 문서화된 일정은 22:00에 24시간마다 시도되며 기본 Cisco URL이 사용됩니다. 구성된 시간 또는 URL은 해당 값을 변경할 수 있습니다. 자동 가져오기가 활성화되었다고 가정하거나 기본 일정을 사용하는 대신 실제 ASA 출력을 확인합니다. [8, 9]

이러한 검사에는 정책 및 가져오기 상태가 표시됩니다. 인증서별 인벤토리를 제공하거나 명명된 eMudhra 인증서가 설치, 제거 또는 신뢰할 수 없음을 확인하지 않습니다. FMC/FTD `cert-update`에서 ASA 동작을 유추하지 마십시오. 또한 특정 신뢰 지점 또는 다른 애플리케이션 신뢰 저장소에 구성된 인증서에 대한 증거로 신뢰 풀 상태를 취급하지 마십시오. 제품별 조치가 필요한지 결정하기 전에 정확한 ASA 릴리스 및 인증서 종속 서비스를 확인하십시오. [8, 9]

# FTD를 사용하여 패치되지 않은 디바이스를 보호하는 잠재적인 해결 방법

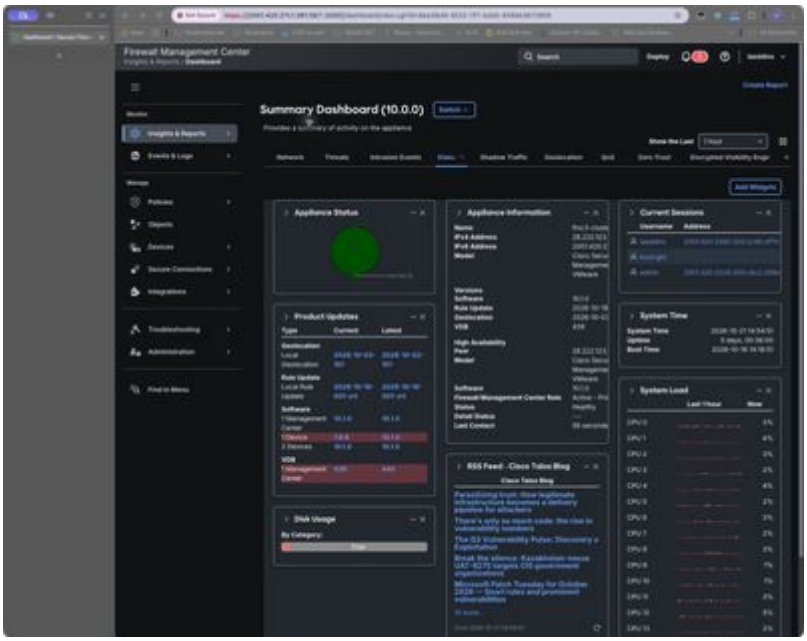
## 목적

Cisco FMC(Secure Firewall Management Center)를 사용하여 알려진 영향을 받는 eMudhra 발급자 이름으로 서버 인증서를 차단하는 TLS 정책 규칙을 구성합니다. 이 제어를 통해 애플리케이션 트러스트 저장소에서 필요한 업데이트를 아직 받지 못한 헤드리스 클라이언트 및 서버에 대한 노출을 줄일 수 있지만, 모든 시나리오에서 연결을 차단하지는 않습니다.  트러스트 저장소 교정 및 인증서 교체를 계속합니다. 이 절차를 위해 손상된 CA를 신뢰할 수 있는 CA로 가져오지 마십시오.

## 사전 요구 사항

이 문서의 컨피그레이션 화면은 FMC 10.1.0에서 캡처되었습니다. 대시보드에는 10.0.0에 관리되는 디바이스 2개와 7.6.6에 관리되는 디바이스 1개가 나열됩니다. 트래픽 테스트는 수행되지 않았습니다. 시행 검증 전에 대상 FTD 버전, Snort 엔진, 시행 모드, 액세스 제어 정책 및 TLS 정책을 기록합니다. 영향을 받는 아웃바운드 트래픽이 의도한 정책에 도달하는지 확인합니다.

그림 1. FMC 10.1.0 및 관리되는 디바이스 소프트웨어 인벤토리




# 발급자 일치 구성

Cisco는 서버 인증서를 발급한 CA와 매칭하기 위한 issuer-DN 조건을 문서화합니다. 규칙 편집기에서 Add to Issuer를 사용하여 DN 객체를 추가합니다. 사용 가능한 탐색 및 레이블은 릴리스에 따라 다릅니다. [1, 2]

## 1 개체 만들기

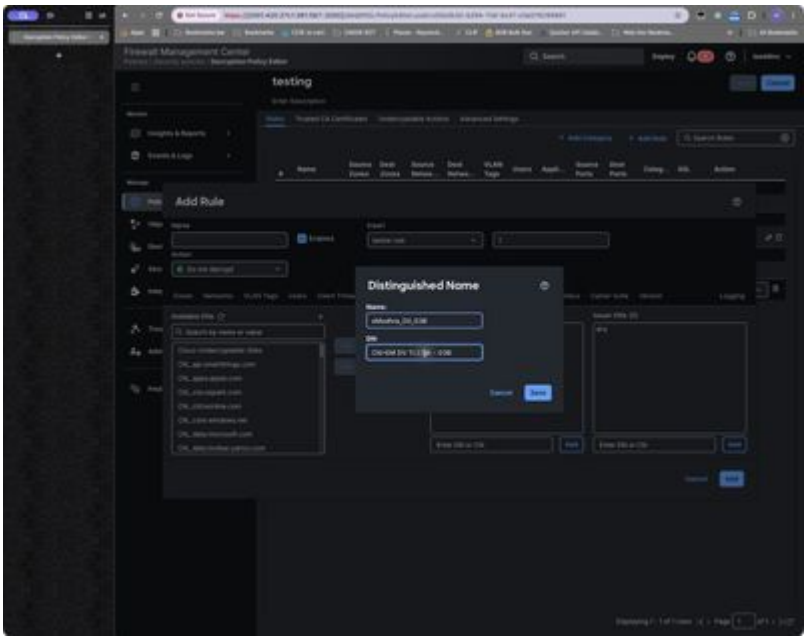
객체 테이블

| DN | 제안된 DN 객체 이름 |
|---|---|
| CN=EM DV TLS CA - G3B | Mudhra_DV_G3B |
| CN=EM DV TLS CA - G3C | Mudhra_DV_G3C |
| CN=EM EV TLS CA - G3B | Mudhra_EV_G3B |
| CN=EM EV TLS CA - G3C | Mudhra_EV_G3C |

| DN | 제안된 DN 객체 이름 |
|---|---|
| CN=EM OV TLS CA - G3B | Mudhra_OV_G3B |
| CN=EM OV TLS CA - G3C | Mudhra_OV_G3C |

위의 표에서 각각에 대해 좁게 범위가 지정된 DN 객체를 하나 생성합니다.

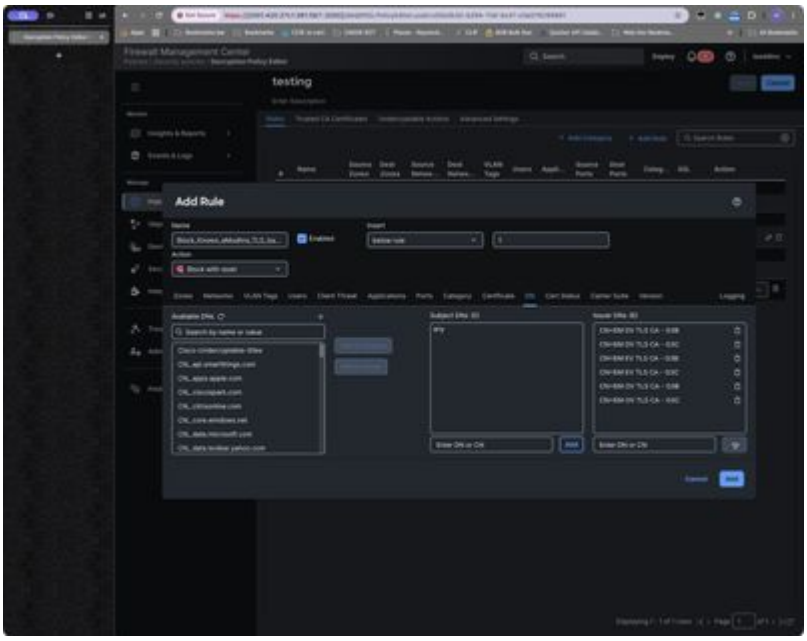
그림 2. Name 및 DN 필드를 보여 주는 Distinguished Name 양식입니다. 예시 값이 그림에 대해 입력되었습니다. 완료되면 Save(저장)를 클릭합니다.




## 2 블록 규칙 만들기

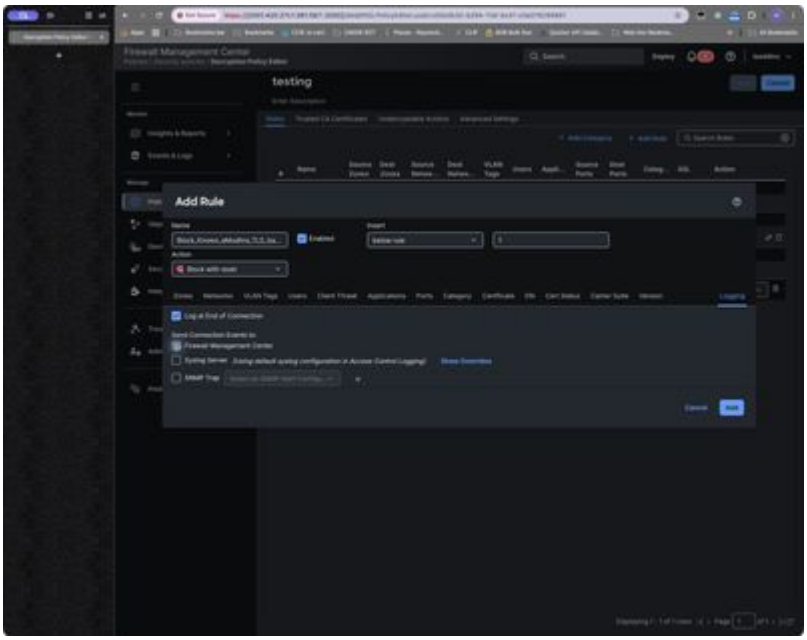
FMC 10.1.0에서 Policies > Security policies > Decryption을 선택하고 해당 정책을 연 다음 Add Rule을 클릭합니다. 규칙의 이름을 Block_Known_Mudhra_TLS_Issuers로 지정합니다. DN 탭을 엽니다. Add to Issuer(발급자에 추가)로 확인된 객체를 추가하거나 Enter DN or CN(DN 또는 CN 입력)이라는 Issuer DNs(발급자 DN) 필드에 DN을 입력하고 Add(추가) 버튼을 클릭합니다. 이름이 주체 DN이 아니라 발급자 DN에 나타나는지 확인합니다.

그림 3. Block with reset, DN 탭, 6개의 Issuer DN 및 no Subject DN 제약 조건을 보여주는 규칙. 완료되면 Add(추가)를 클릭합니다.




Block(차단) 또는 Block with reset(차단 후 초기화)을 선택합니다. 소스 영역 또는 네트워크를 합의된 범위로 제한합니다. 원하는 경우 Logging(로깅) 탭에서 Log at End of Connection(연결 종료 시 로그)을 선택하고 Firewall Management Center(방화벽 관리 센터)가 선택되었는지 확인합니다. Valid = Yes 요구 사항을 추가하지 마십시오. 의도한 발급자 블록은 신뢰 검증을 통과하는 인증서에 의존해서는 안 됩니다.

그림 4. 선택한 End of Connection 및 Firewall Management Center의 로그를 보여주는 규칙. 완료되면 Add(추가)를 클릭합니다




## 3 규칙 순서 및 정책 연결 검토

동일한 트래픽을 먼저 처리할 수 있는 더 넓은 규칙보다 먼저 규칙을 배치합니다. 대상 장치에 할당된 액세스 제어 정책과의 TLS 정책 연결을 확인합니다. 테스트 전에 프리필터 및 기타 우회 경로를 검토하십시오.

그림 5. 기존 테스트 정책 규칙 테이블 주문 인터페이스만 표시됩니다.

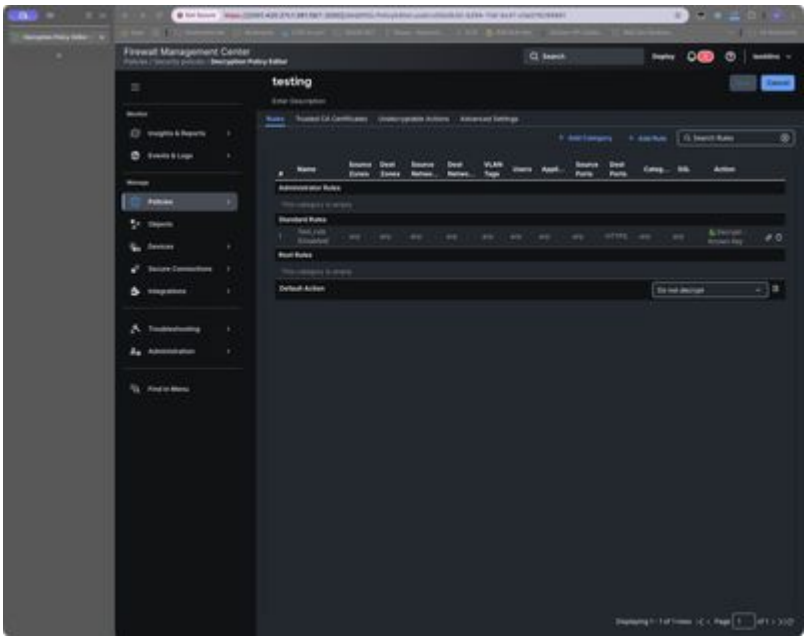
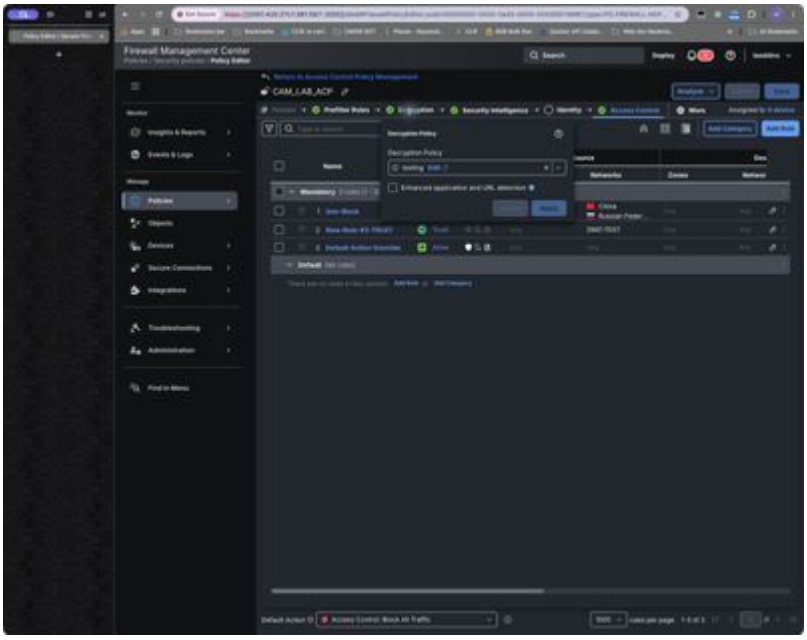



그림 5b. 기존 CAM_LAB_ACP 정책이 테스트 암호 해독 정책을 참조합니다.




# 구축 및 확인

해당 장치에 변경 사항을 배포합니다. 가능한 경우 문제의 CA 중 하나가 발급한 인증서를 사용하고 있는 웹 사이트로 테스트합니다.

# 예기치 않은 결과 트러블슈팅

트래픽이 통과되면 배포 상태, 트래픽 범위, 정책 연결, 규칙 순서, 발급자 맞춤법 및 필드 인코딩, 장치에 인증서 정보가 있는지 확인합니다. 다른 규칙 또는 우회 경로가 흐름을 처리했는지 여부를 확인합니다. 동일한 지원 범위를 청구하기 전에 테스트된 릴리스에서 TLS 1.3 가시성을 검토하십시오
.

추가 TLS 1.3 검증: fmc 7.6에서 TLS 1.3 암호 해독은 별도의 암호 해독 정책 고급 설정입니다. 비활성화되어 있으면 암호 해독 규칙은 TLS 1.2 이하에만 적용됩니다. TLS 1.3 암호 해독을 활성화하면 적응형 서버 ID 프로브가 활성화되며, 인증서가 캐시되지 않은 경우 발급자 DN 조건이 프로브를 트리거할 수 있습니다. 연결된 액세스 제어 정책의 TLS 1.3 Server Identity Discovery 설정이 우선합니다. Cisco에서는 이러한 고급 설정이 7.1 이전 디바이스나 Snort 2를 실행하는 디바이스에서는 무시되며, AWS에 배포된 FTDv에서는 적응형 ID 검색이 지원되지 않습니다. TLS 1.3 지원 범위를 청구하기 전에 대상 소프트웨어/플랫폼 및 인증서 가시성을 검증합니다. 규칙의 TLS Version Selector에는 SSL 3.0~TLS 1.2가 나열됩니다. TLS 1.3에 대해 이 선택기를 사용하지 마십시오. [7]

관련되지 않은 트래픽이 실패한 경우, 실제 일치하는 규칙 및 발급자를 확인합니다. 필요에 따라 DN 또는 트래픽 범위를 좁힌 다음 영향받는 테스트와 영향받지 않는 테스트를 모두 반복합니다. 해결 방법으로 인증서 검증을 비활성화하지 마십시오.

# 커버리지 및 운영 제한

이 솔루션은 모든 시나리오를 차단하거나 다른 서비스를 업데이트해야 하는 필요성을 대체하는 것은 아닙니다.

# 롤백 및 규칙 폐기

규칙이 허용되지 않는 영향을 초래하는 경우, 일반적인 변경 프로세스를 통해 새 규칙을 비활성화하고 재구축합니다. 이벤트 및 테스트 증거 보존 종료 전에 영향을 받는 워크로드가 현재 신뢰 정책을 시행하는지 확인하고, 부정적인 인증서 검증 테스트를 반복하고, 변경 소유자의 승인을 얻어 임시 억제를 제거합니다.

# 참조


[1] FMC 7.2 암호 해독 규칙

[2] FMC 10.x 규칙 기반 암호 해독 규칙

[3] Secure Firewall Management Center 릴리스별 새로운 기능

[4] FMC 및 FDM용 CA 번들의 자동 업데이트 구성

[5] FMC 7.6 인증서

[6] FDM 7.6 인증서

[7] FMC 7.6 암호 해독 정책 및 TLS 1.3 지침

[8] Cisco Secure Firewall ASA 9.22 일반 운영 CLI 컨피그레이션 가이드 — 디지털 인증서

[9] Cisco Secure Firewall ASA Series 명령 참조 — crypto ca trustpool 정책

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.