Anleitung zu Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance - Misstrauen bei der Wurzel- und Zwischenzertifizierungsstelle im Notfall

Inhalt

Zweck

Nachstehend finden Sie Anleitungen zu Cisco Secure Firewall Threat Defense (FTD), Cisco Secure Firewall Management Center (FMC) und Adaptive Security Appliance (ASA), die verhindern, dass Behörden mit Wurzel- und Zwischenzertifikaten in Notfällen misstrauen.

FMC - lokale Updates für Cisco Service-Zertifikatbündel

FMC und FTD können automatisch ein lokales CA-Paket aktualisieren, das für TLS-Verbindungen von der Appliance zu Cisco Services verwendet wird, einschließlich Smart Licensing und Software, VDB, SRU und Geolocation-Updates. Das System überprüft täglich zu einer vom System definierten Zeit. Die Dokumentverfügbarkeit von Cisco beginnt mit FMC/FTD 7.0.5, 7.1.0.3, 7.2.4 und 7.3.0+. Dies sind Schwellenwerte für Funktionen, keine empfohlenen Upgrade-Ziele. Wählen Sie ein Upgrade-Ziel unter Verwendung der genauen Plattform, der Quellversion, der Kompatibilitätsanforderungen und der aktuellen Cisco Versionshinweise aus. [3, 4]

Auf einer unterstützten FMC- oder FTD-CLI `zeigen Sie cert-update` reports automatic-update status, den täglichen Zeitplan und die Zeit der letzten Änderung des Pakets an. `configure cert-update` prüft, ob das lokale Paket aktuell ist und ob die Verbindung zum Update bereit ist. [4, 5, 6]

Dieses Cisco Service-Paket ist von den von FTD konfigurierten vertrauenswürdigen CA-Objekten/Gruppen, die per SSL-Verschlüsselung verwendet werden, und von Geräte-Vertrauenspunkten, die für Identitäts- oder VPN-Zertifikate verwendet werden, getrennt. Sie müssen sicherstellen, dass keines dieser Zertifikate manuell zur Konfiguration hinzugefügt wurde. [5, 6]

Automatischer Import von ASA CA TrustPool

Auf der ASA sind der CA-Vertrauenspool und benannte Vertrauenspunkte separate Zertifikatverwaltungsfunktionen. Der Trustpool enthält Zertifizierungsstellenzertifikate. Ein Vertrauenspunkt ist eine benannte Konfiguration, die für die Zertifikatidentität und die CA-Registrierung verwendet wird. Der automatische ASA-Trustpool-Import ist ebenfalls unabhängig vom oben beschriebenen Update für das FMC-/FTD-Cisco-Servicepaket. [8, 9]

Um eine schreibgeschützte Überprüfung durchzuführen, führen Sie `show crypto ca trustpool policy aus`, um die Anzahl der Zertifikate für trustpool, den Importstatus und das Ergebnis, den nächsten geplanten Versuch und die Details der effektiven Richtlinie zu überprüfen. Führen Sie `show run crypto ca trustpool policy` aus, um konfigurierte Richtlinienzeilen für trustpool zu überprüfen. Cisco dokumentiert den automatischen Import standardmäßig deaktiviert. Wenn der dokumentierte Zeitplan ohne Überschreibungen aktiviert ist, wird alle 24 Stunden um 22:00 Uhr versucht, und die Cisco Standard-URL wird verwendet. Eine konfigurierte Zeit oder URL kann diese Werte ändern. Überprüfen Sie die tatsächliche ASA-Ausgabe, anstatt davon auszugehen, dass der automatische Import aktiviert ist oder den Standardzeitplan verwendet. [8, 9]

Bei diesen Prüfungen werden die Grundsätze und der Einfuhrstatus angegeben; Sie stellen weder ein Inventar nach Zertifikat bereit, noch stellen sie fest, dass ein benanntes Mudhra-Zertifikat installiert, entfernt oder misstrauisch ist. Leiten Sie das ASA-Verhalten nicht aus dem FMC/FTD-`Zertifikat-Update` ab, und behandeln Sie den Trustpool-Status nicht als Beweis für Zertifikate, die unter einem bestimmten Trustpoint oder einem anderen Vertrauensspeicher für Anwendungen konfiguriert wurden. Bestätigen Sie die genaue ASA-Version und den zertifikatabhängigen Service, bevor Sie produktspezifische Maßnahmen treffen. [8, 9]

Mögliche Lösung mit FTD zum Schutz ungepatchter Geräte

Zweck

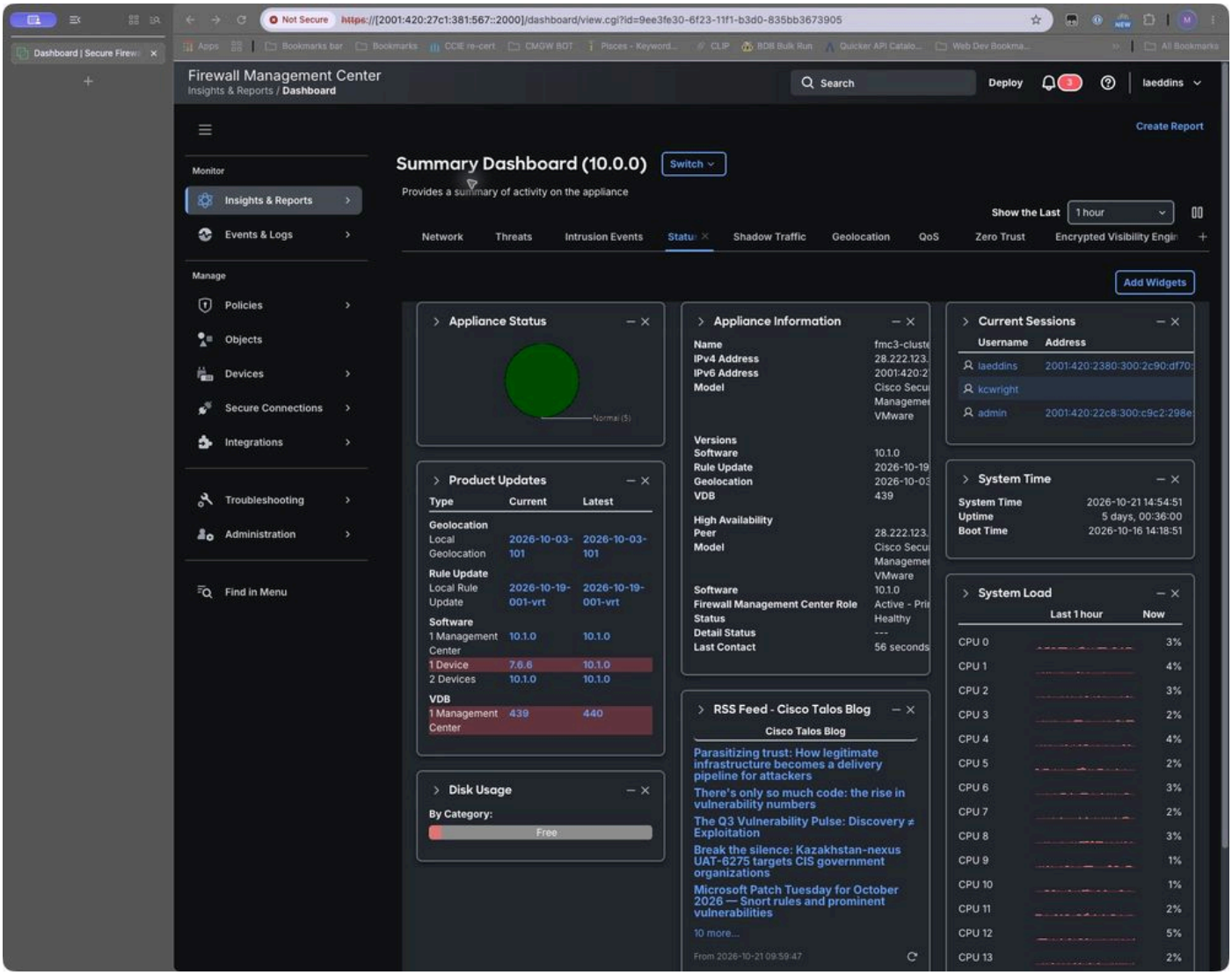
Verwenden Sie Cisco Secure Firewall Management Center (FMC), um TLS-Richtlinienregeln zu konfigurieren, die Serverzertifikate mit bekannten betroffenen Mudhra-Ausstellernamen blockieren. Diese Kontrolle kann das Risiko für kopflose Clients und Server reduzieren, deren Anwendungsvertrauensspeicher noch nicht die erforderlichen Updates erhalten hat. Verbindungen werden jedoch nicht in allen Szenarien blockiert. Setzen Sie die Wiederherstellung des Vertrauensspeichers und den Austausch von Zertifikaten fort. Importieren Sie für dieses Verfahren keine kompromittierte Zertifizierungsstelle in vertrauenswürdige Zertifizierungsstellen.

Voraussetzungen

Die Konfigurationsbildschirme in diesem Artikel wurden mit FMC 10.1.0 erfasst. Das Dashboard

listet zwei verwaltete Geräte auf 10.0.0 und eines auf 7.6.6 auf. Es wurde kein Datenverkehrstest durchgeführt. Notieren Sie vor der Durchsetzungsvalidierung die FTD-Zielversion, die Snort-Engine, den Durchsetzungsmodus, die Zugriffskontrollrichtlinie und die TLS-Richtlinie. Vergewissern Sie sich, dass der betroffene ausgehende Datenverkehr die beabsichtigte Richtlinie erreicht.

Abbildung 1: FMC 10.1.0 und Softwarebestand für verwaltete Geräte



Ausstellerzuordnung konfigurieren

Cisco dokumentiert die Aussteller-DN-Bedingungen für die Übereinstimmung mit der Zertifizierungsstelle, die das Serverzertifikat ausgestellt hat. Fügen Sie ein DN-Objekt mit Add to Issuer im Regeleditor hinzu. Verfügbare Navigationsmöglichkeiten und Beschriftungen hängen von der jeweiligen Version ab. [1, 2]

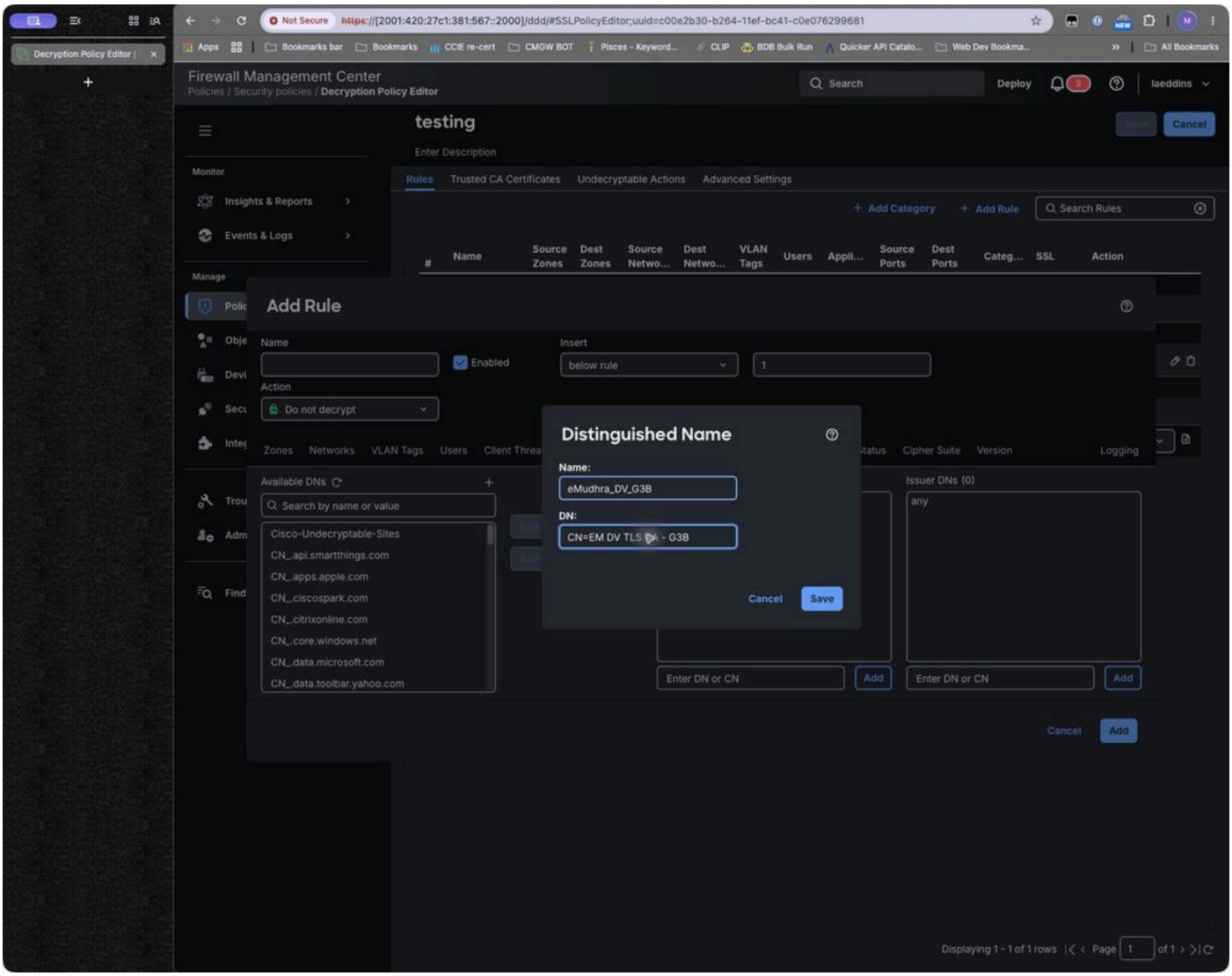
1 Objekte erstellen

Objekttabelle

DN	Name des vorgeschlagenen DN-Objekts
CN=EM DV TLS-CA - G3B	Medhra_DV_G3B
CN=EM DV TLS-CA - G3C	Medhra_DV_G3C
CN=EM EV TLS-CA - G3B	Medhra_EV_G3B
CN=EM EV TLS-CA - G3C	Medhra_EV_G3C
CN=EM OV TLS-CA - G3B	Medhra_OV_G3B
CN=EM OV TLS-CA - G3C	Medhra_OV_G3C

Erstellen Sie für jedes Objekt in der obigen Tabelle ein DN-Objekt mit engem Gültigkeitsbereich.

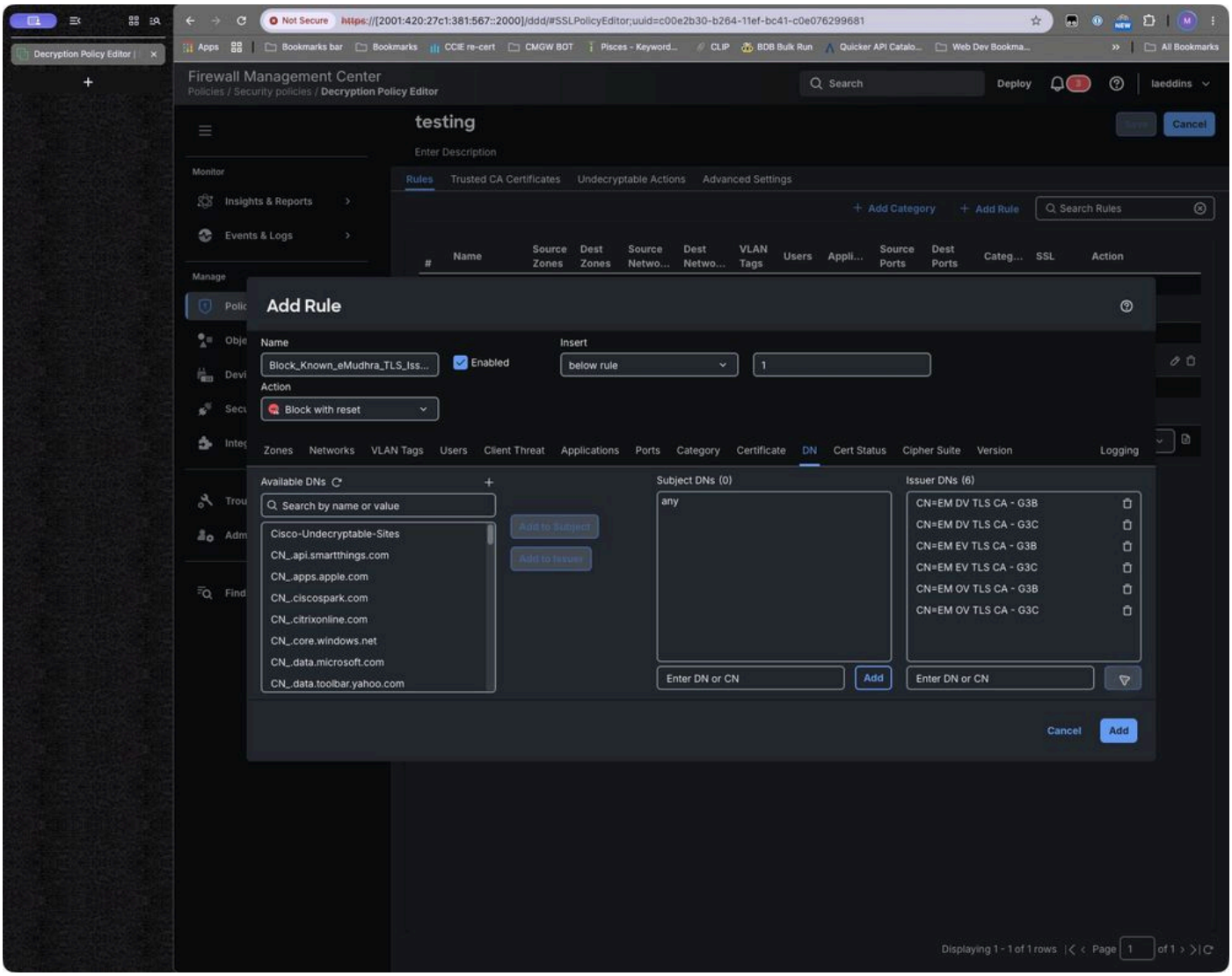
Abbildung 2: Formular für den Distinguished Name mit den Feldern Name und DN Der Beispielwert wurde zur Veranschaulichung eingegeben. Klicken Sie abschließend auf Speichern.



2 Erstellen der Blockregel

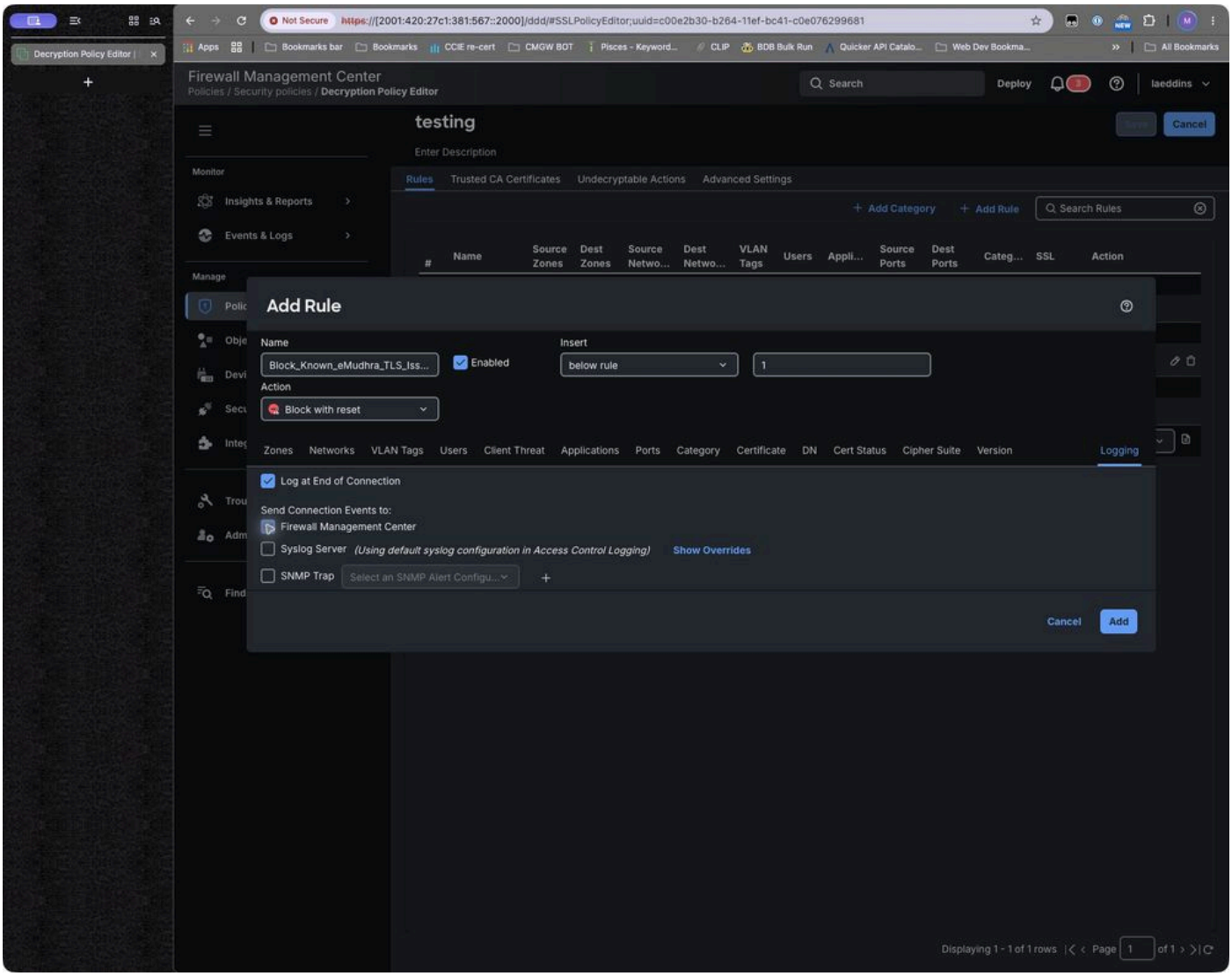
Wählen Sie in FMC 10.1.0 Richtlinien > Sicherheitsrichtlinien > Entschlüsselung aus, öffnen Sie die entsprechende Richtlinie, und klicken Sie auf Regel hinzufügen. Geben Sie der Regel den Namen Block_Known_Mudhra_TLS_Issuers. Öffnen Sie die Registerkarte DN. Fügen Sie geprüfte Objekte mit "Zum Aussteller hinzufügen" hinzu, oder geben Sie einen DN in das Feld "Aussteller-DNs" mit der Bezeichnung "DN oder CN eingeben" ein, und klicken Sie auf die Schaltfläche Hinzufügen. Bestätigen Sie, dass die Namen in den Aussteller-DNs und nicht in den Betreff-DNs angezeigt werden.

Abbildung 3. Regel für Block mit Zurücksetzen, Registerkarte DN, sechs Aussteller-DNs und keine Einschränkung für Betreff-DN. Klicken Sie abschließend auf Hinzufügen.



Wählen Sie Blockieren oder Blockieren mit Zurücksetzen. Begrenzen Sie Quellzonen oder Netzwerke auf den vereinbarten Umfang. Wählen Sie bei Bedarf auf der Registerkarte Protokollierung die Option Am Ende der Verbindung protokollieren aus, und überprüfen Sie, ob Firewall Management Center ausgewählt ist. Fügen Sie keine Valid = Yes-Anforderung hinzu: Der beabsichtigte Ausstellerblock darf nicht von dem Zertifikat abhängen, das die Vertrauensüberprüfung besteht.

Abbildung 4. Regel mit ausgewähltem Protokoll am Ende der Verbindung und ausgewähltem Firewall-Verwaltungscenter. Klicken Sie abschließend auf Hinzufügen



3 Überprüfen der Regelreihenfolge und Richtlinienzuweisung

Stellen Sie die Regel breiteren Regeln vor, die denselben Datenverkehr zuerst behandeln könnten. Bestätigen Sie die Zuordnung der TLS-Richtlinie zur den Zielgeräten zugewiesenen Zugriffskontrollrichtlinie. Überprüfen Sie vor dem Testen die Vorfilter- und andere Umgehungspfade.

Abbildung 5: Vorhandene Regeltabelle für Testrichtlinien. Es wird nur die Bestellschnittstelle angezeigt.

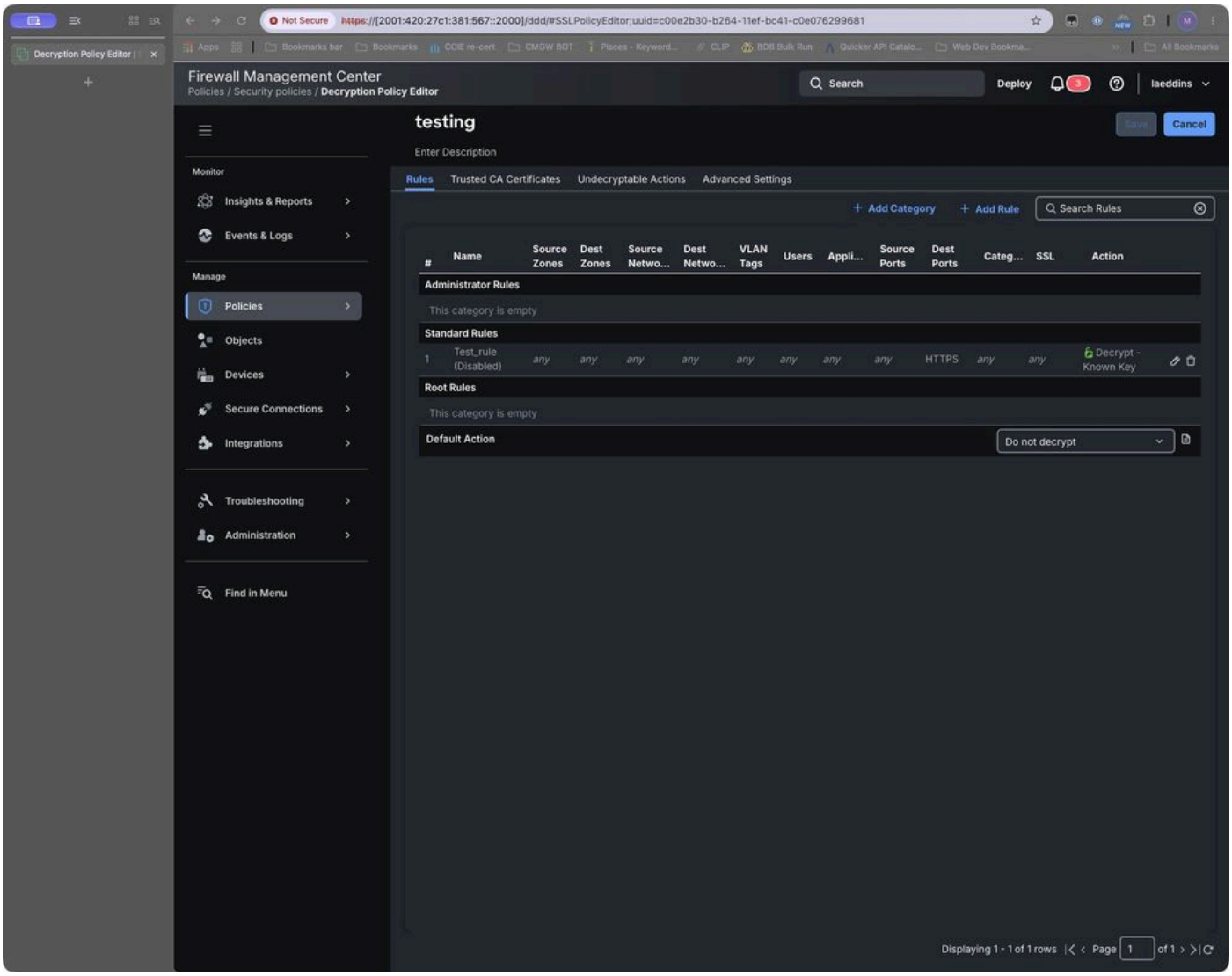
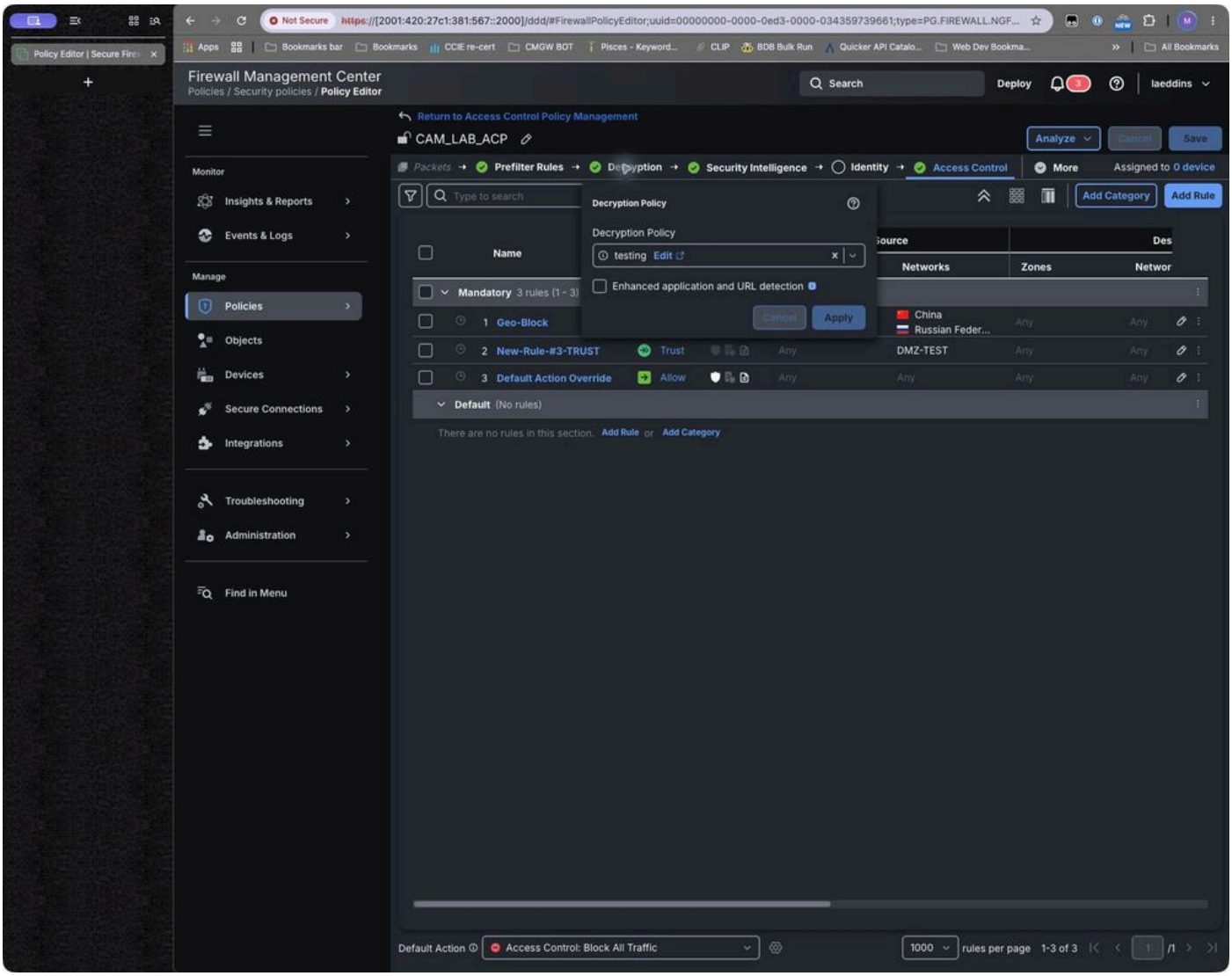


Abbildung 5b. Die vorhandene CAM_LAB_ACP-Richtlinie referenziert die Test-Entschlüsselungsrichtlinie.



Bereitstellung und Überprüfung

Stellen Sie die Änderungen an den betreffenden Geräten bereit. Falls verfügbar, testen Sie mit einer Website, von der Sie wissen, dass sie ein von einer der betreffenden Zertifizierungsstellen ausgestelltes Zertifikat verwendet.

Fehlerbehebung bei unerwarteten Ergebnissen

Wenn der Datenverkehr weitergeleitet wird, überprüfen Sie den Bereitstellungsstatus, den Datenverkehrsbereich, die Richtlinienzuordnung, die Regelreihenfolge, die Rechtschreibung des Ausstellers, die Feldcodierung und ob das Gerät Zertifikatinformationen enthält. Bestimmt, ob der Fluss von einer anderen Regel oder einem Umgehungspfad verarbeitet wurde. Überprüfen Sie die TLS 1.3-Transparenz für die getestete Version, bevor Sie eine gleichwertige Abdeckung beantragen.

Zusätzliche TLS 1.3-Validierung: Bei FMC 7.6 ist die TLS 1.3-Entschlüsselung eine separate erweiterte Entschlüsselungsrichtlinieneinstellung. Wenn sie deaktiviert ist, gelten die Entschlüsselungsregeln nur für TLS 1.2 oder niedriger. Durch die Aktivierung der TLS 1.3-Entschlüsselung wird die adaptive Serveridentitätsprüfung aktiviert, und eine Issuer DN-Bedingung kann eine Überprüfung auslösen, wenn das Zertifikat nicht zwischengespeichert wird. Die Einstellung für die TLS 1.3-Serveridentitätserkennung der zugeordneten Zugriffssteuerungsrichtlinie hat Vorrang. Laut Cisco werden diese erweiterten Einstellungen auf Geräten vor 7.1 oder Snort 2 ignoriert, und die adaptive Identitätserkennung wird auf FTDv, das auf AWS bereitgestellt wird, nicht unterstützt. Validieren Sie die Transparenz von Zielsoftware/Plattform und Zertifikat, bevor Sie eine TLS 1.3-Abdeckung beantragen. Der TLS-Versionsselektor der Regel selbst führt SSL 3.0 bis TLS 1.2 auf. verlassen sich nicht auf diesen Selektor für TLS 1.3. [7]

Wenn der nicht verknüpfte Datenverkehr fehlschlägt, geben Sie die zutreffende Regel und den Aussteller an. Schränken Sie den DN oder den Datenverkehrsbereich nach Bedarf ein, und wiederholen Sie dann sowohl die betroffenen als auch die nicht betroffenen Tests. Deaktivieren Sie die Zertifikatsvalidierung nicht als Problemumgehung.

Abdeckung und betriebliche Beschränkungen

Diese Lösung blockiert nicht jedes Szenario und ersetzt nicht die Notwendigkeit, andere Services zu aktualisieren.

Rollback und Außerbetriebnahme von Regeln

Wenn die Regel unannehmbare Auswirkungen hat, deaktivieren Sie die neue Regel über den normalen Änderungsprozess, und stellen Sie sie erneut bereit. Bewahren Sie Ereignisse auf, und testen Sie Beweise. Überprüfen Sie vor der Einstellung, ob die betroffenen Workloads die aktuelle Vertrauensrichtlinie durchsetzen, wiederholen Sie die Tests zur negativen Zertifikatvalidierung, und holen Sie die Genehmigung des Eigentümers der Änderung ein, um die temporäre Beschränkung zu entfernen.

Referenzen

[1] FMC 7.2 Entschlüsselungsregeln

[2] Regelbasierte Entschlüsselungsregeln für FMC 10.x

[3] Neue Funktionen von Secure Firewall Management Center nach Version

[4] Automatische Aktualisierung von CA-Paketen für FMC und FDM konfigurieren

[5] FMC 7.6 Zertifikate

[6] FDM 7.6 Zertifikate

[7] FMC 7.6 Entschlüsselungsrichtlinien und TLS 1.3-Richtlinien

[8] Cisco Secure Firewall ASA 9.22 General Operations CLI Configuration Guide — Digital Certificates

[9] Cisco Secure Firewall ASA Series Command Reference — crypto ca trustpool policy

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.