Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance-richtlijnen - Noodsituatie: wantrouwen jegens eMudhra Root- en Intermediate Certificate Authorities

Inhoud

Doel

Hieronder vindt u de richtlijnen over Cisco Secure Firewall Threat Defense (FTD), Cisco Secure Firewall Management Center (FMC) en Adaptive Security Appliance (ASA) voor het wantrouwen van eMudhra Root en Intermediate Certificate Authorities in noodgevallen.

FMC lokale Cisco-service certificaatbundel updates

FMC en FTD kunnen automatisch een lokale CA-bundel bijwerken die wordt gebruikt voor TLS-verbindingen van het toestel naar Cisco-services, waaronder Smart Licensing en software, VDB, SRU en geolocatie-updates. Het systeem controleert dagelijks op een door het systeem gedefinieerde tijd. Cisco-documenten zijn beschikbaar vanaf FMC/FTD 7.0.5, 7.1.0.3, 7.2.4 en 7.3.0+. Dit zijn drempelwaarden voor functies, niet aanbevolen upgradebestemmingen; selecteer een upgradedoel met het exacte platform, bronrelease, compatibiliteitsvereisten en de huidige richtlijnen voor Cisco-release. [3, 4]

Op een ondersteunde FMC- of FTD-CLI `tonen cert-update` rapporten automatische-update status, de dagelijkse planning en de laatst gewijzigde tijd van de bundel. `configureer cert-update test` controleert of de lokale bundel is actueel en of update connectiviteit is klaar. [4, 5, 6]

Deze Cisco-servicebundel is gescheiden van FTD's geconfigureerde vertrouwde CA-objecten/groepen die worden gebruikt door SSL-decodering en van apparaatvertrouwenspunten die worden gebruikt voor identiteits- of VPN-certificaten. U moet controleren of geen van deze certificaten handmatig aan de configuratie is toegevoegd. [5, 6]

ASA CA trustpool automatisch importeren

Op ASA zijn de vertrouwenspool van CA en de genoemde vertrouwenspunten afzonderlijke functies voor certificaatbeheer. De trustpool heeft CA-certificaten; een trustpoint is een benoemde configuratie die wordt gebruikt voor certificaatidentiteit en CA-inschrijving. ASA trustpool auto-import is ook gescheiden van de FMC / FTD Cisco-service bundel update hierboven beschreven. [8, 9]

Voer voor een alleen-lezen controle het `beleid` van `de cryptocurrency-cartrustpool uit` om het aantal certificaten van de trustpool, de importstatus en het resultaat, de volgende geplande poging en effectieve beleidsdetails te bekijken. Voer het `beleid voor de crypto-cartrustpool uit` om de geconfigureerde regels voor het trustpool-beleid te bekijken. Cisco-documenten worden standaard automatisch als uit geïmporteerd. Wanneer ingeschakeld zonder overschrijvingen, is het gedocumenteerde schema een poging om de 24 uur om 22:00 uur en wordt de standaard Cisco-URL gebruikt; een geconfigureerde tijd of URL kan deze waarden wijzigen. Controleer de werkelijke ASA-uitvoer in plaats van aan te nemen dat automatisch importeren is ingeschakeld of het standaardschema te gebruiken. [8, 9]

Deze controles tonen het beleid en de importstatus; ze bieden geen inventarisatie per certificaat of stellen vast dat een genoemd eMudhra-certificaat is geïnstalleerd, verwijderd of gewantrouwd. Leid geen ASA-gedrag af uit FMC/FTD `cert-update`, en behandel de status van de vertrouwensgroep niet als bewijs van certificaten die zijn geconfigureerd onder een bepaald vertrouwenscentrum of een ander vertrouwensarchief voor toepassingen. Bevestig de exacte ASA-release en certificaatafhankelijke service voordat u beslist of een productspecifieke actie nodig is. [8, 9]

Mogelijke oplossing met FTD om uw niet-gepatchte apparaten te beschermen

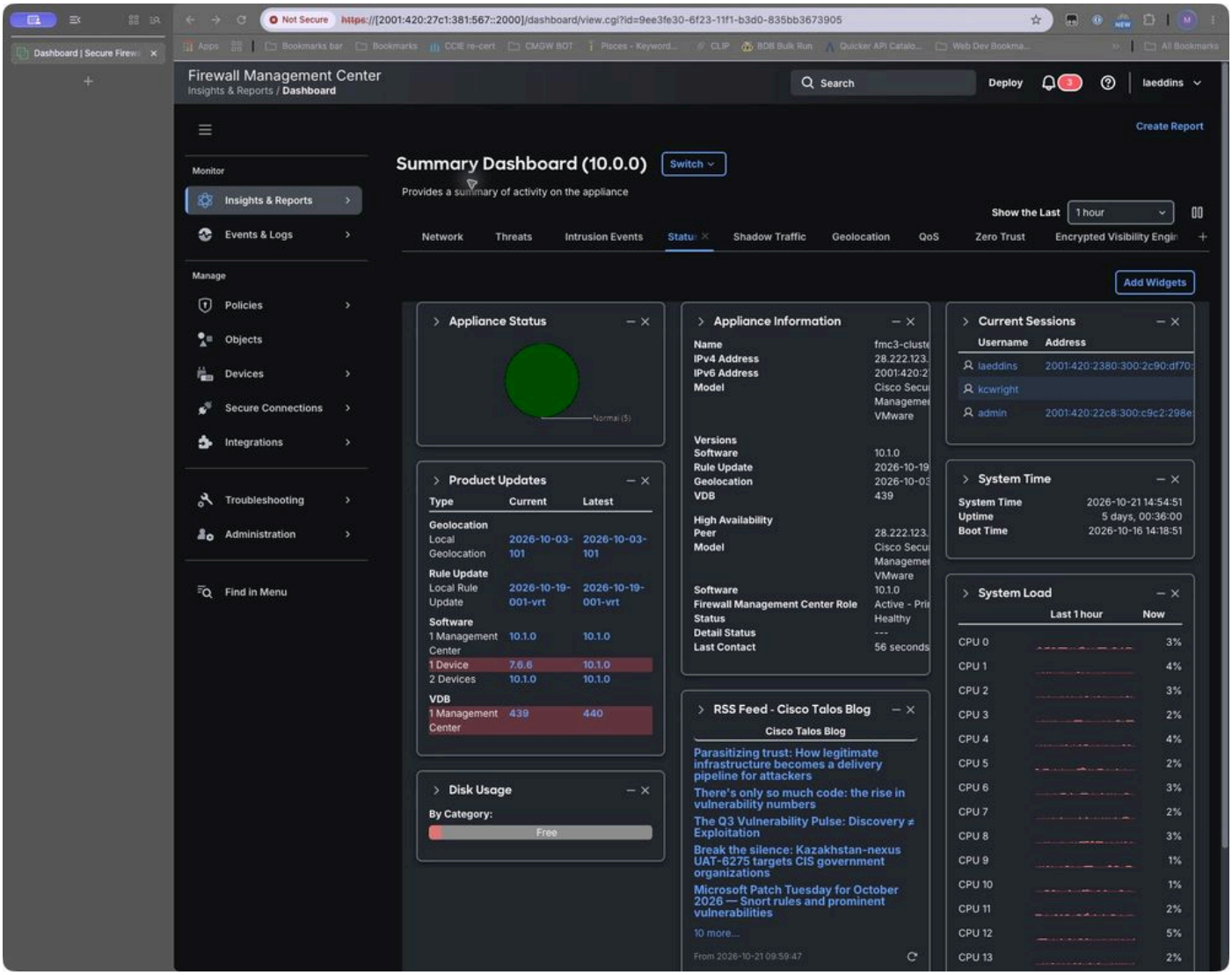
Doel

Gebruik het Cisco Secure Firewall Management Center (FMC) om TLS-beleidsregels te configureren waarmee servercertificaten worden geblokkeerd met bekende namen van de betrokken eMudra-uitgevers. Deze besturing kan de blootstelling verminderen voor headless clients en servers waarvan de applicatie vertrouwenswinkels nog niet de vereiste updates hebben ontvangen, maar het blokkeert verbindingen niet in alle scenario's. Ga door met het herstellen van vertrouwde winkels en het vervangen van certificaten. Importeer voor deze procedure geen gecompromitteerde certificeringsinstantie in vertrouwde certificeringsinstanties.

Voorwaarden

De configuratieschermen in dit artikel zijn vastgelegd op FMC 10.1.0. Het dashboard vermeldt twee beheerde apparaten op 10.0.0 en één op 7.6.6. Er werd geen verkeerstest uitgevoerd. Vóór de validatie van de handhaving registreert u de FTD-versie van het doel, de Snort-engine, de handhavingsmodus, het toegangscontrolebeleid en het TLS-beleid. Bevestig dat het getroffen uitgaande verkeer het beoogde beleid bereikt.

Afbeelding 1. FMC 10.1.0 en inventarisatie van beheerde apparaatsoftware.



Matching van emittenten configureren

Cisco documenteert issuer-DN-voorwaarden voor het matchen van de CA die het servercertificaat heeft uitgegeven. Voeg een DN-object met Add to Issuer toe in de regeleditor. Beschikbare navigatie en labels zijn afhankelijk van de release. [1, 2]

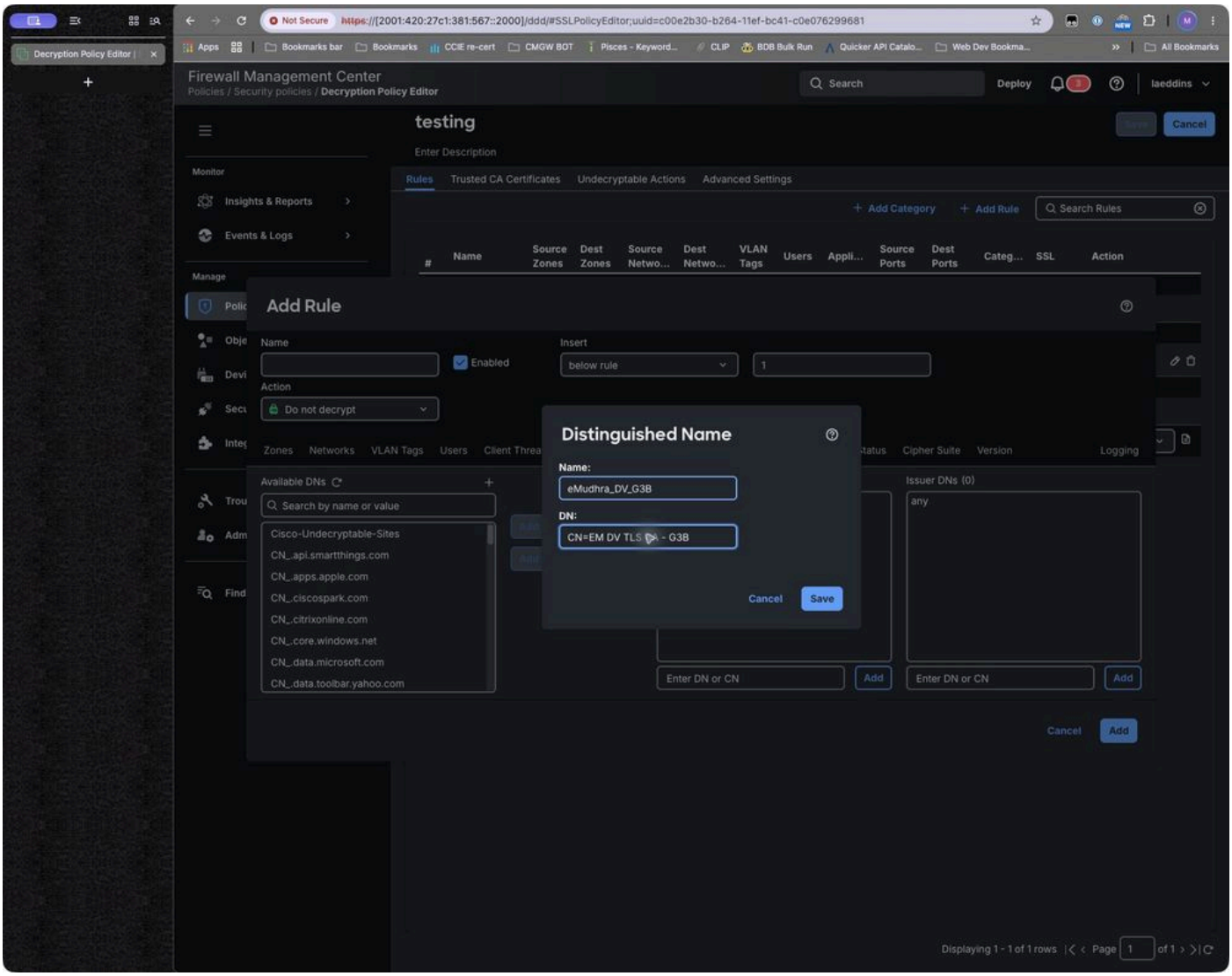
1 Maak de objecten

objecttabel

DN	Voorgestelde DN-objectnaam
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
CN=EM OV TLS CA - G3B	Mudhra_OV_G3B
CN=EM OV TLS CA - G3C	Mudhra_OV_G3C

Maak voor elk object in de bovenstaande tabel een DN-object met een smal bereik.

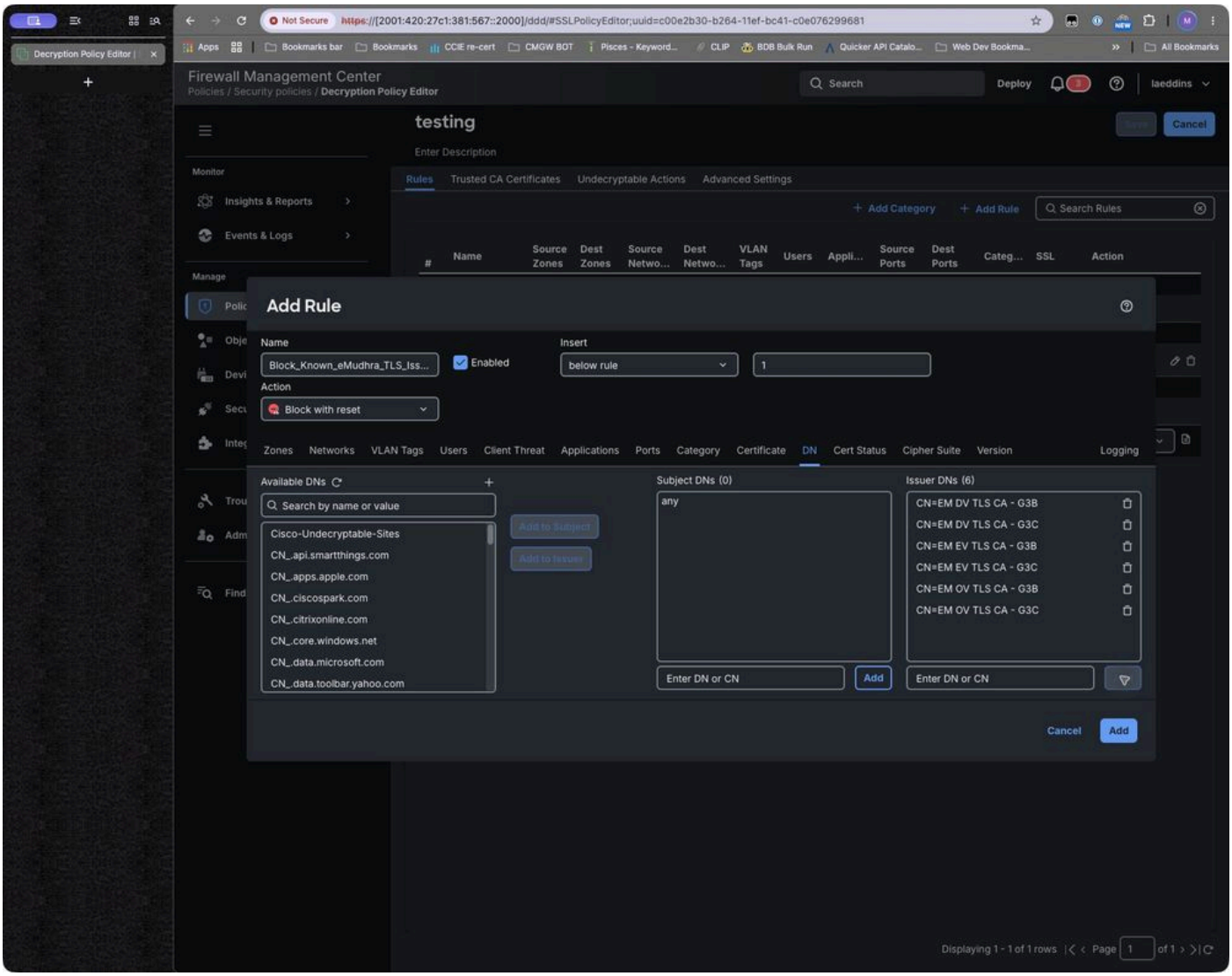
Afbeelding 2. Formulier met de velden Naam en DN. De voorbeeldwaarde is ingevoerd ter illustratie; klik op Opslaan wanneer u klaar bent.



2 De blokregel maken

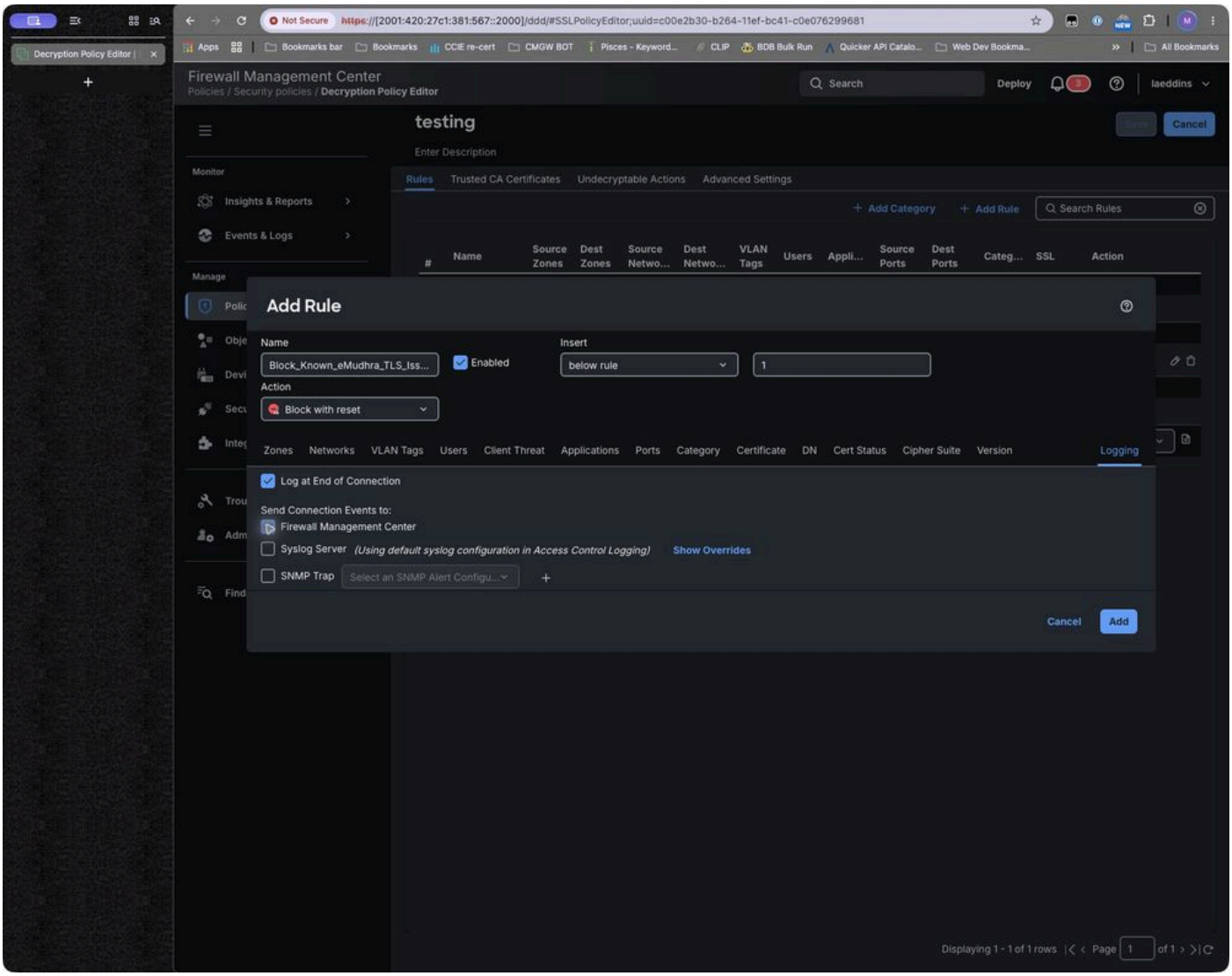
Selecteer in FMC 10.1.0 de optie Beleid > Veiligheidsbeleid > Decryptie, open het toepasselijke beleid en klik op Regel toevoegen. Noem de regel Block_Known_Mudhra_TLS_Issuers. Open het tabblad DN. Voeg geverifieerde objecten toe met Toevoegen aan Uitgever of voer een DN in het veld Uitgever-DN's met de naam Voer DN of CN in en klik op de knop Toevoegen. Bevestig dat de namen worden weergegeven in Issuer DN's, niet in Subject DN's.

Afbeelding 3. Regel die Blok met reset, het DN-tabblad, zes Issuer DN's en geen Subject DN-beperking toont. Klik op Toevoegen wanneer u klaar bent.



Selecteer Blokkeren of Blokkeren met reset. Beperk bronzones of netwerken tot het overeengekomen bereik. Selecteer op het tabblad Logboekregistratie desgewenst Log aan het einde van de verbinding en controleer of Firewall Management Center is geselecteerd. Voeg geen Geldig = Ja-vereiste toe: het beoogde emittentenblok mag niet afhankelijk zijn van het certificaat dat de vertrouwensvalidatie doorstaat.

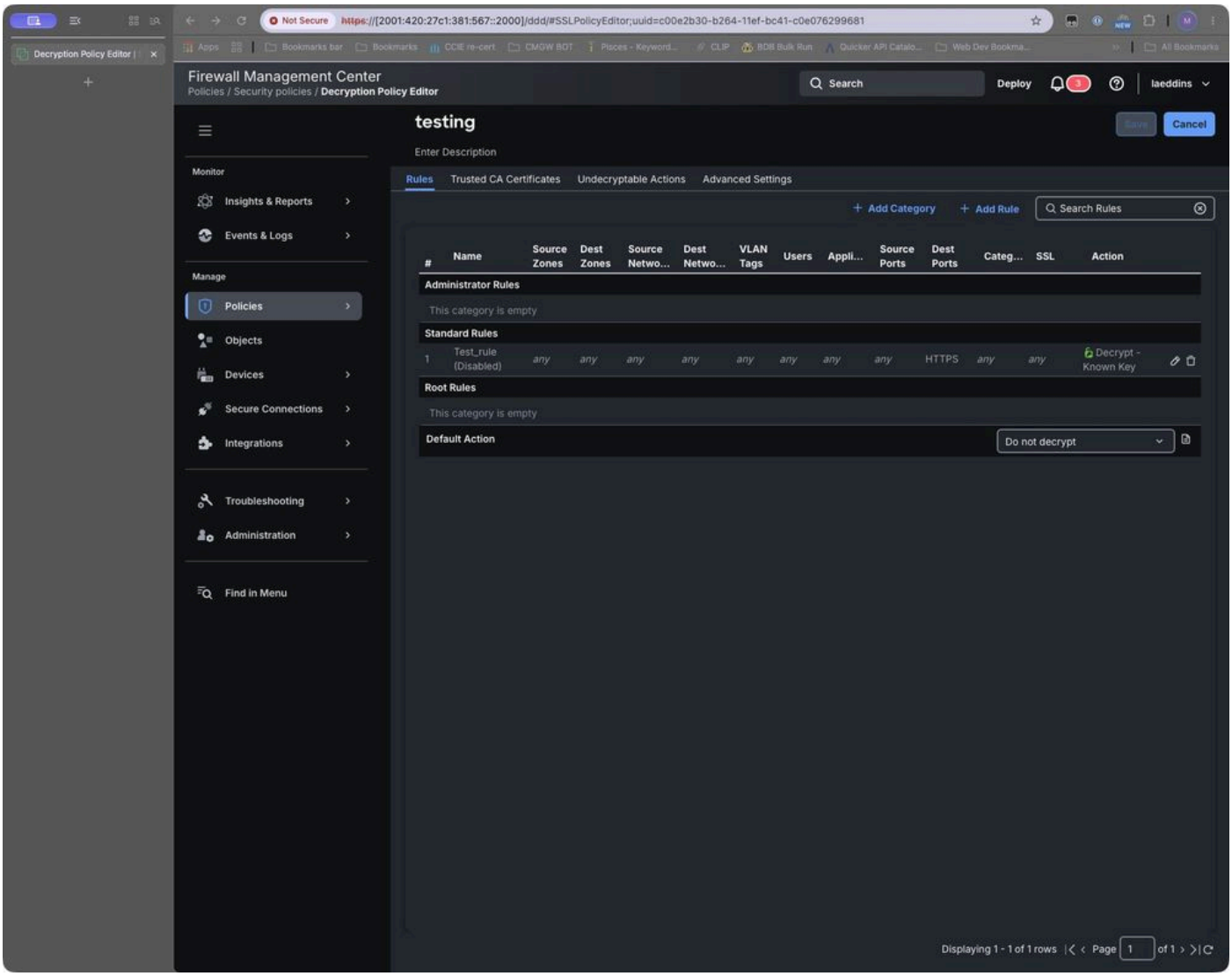
Afbeelding 4. Regel voor het weergeven van het logbestand aan het einde van de verbinding en het Firewall Management Center geselecteerd. Klik op Toevoegen wanneer u klaar bent



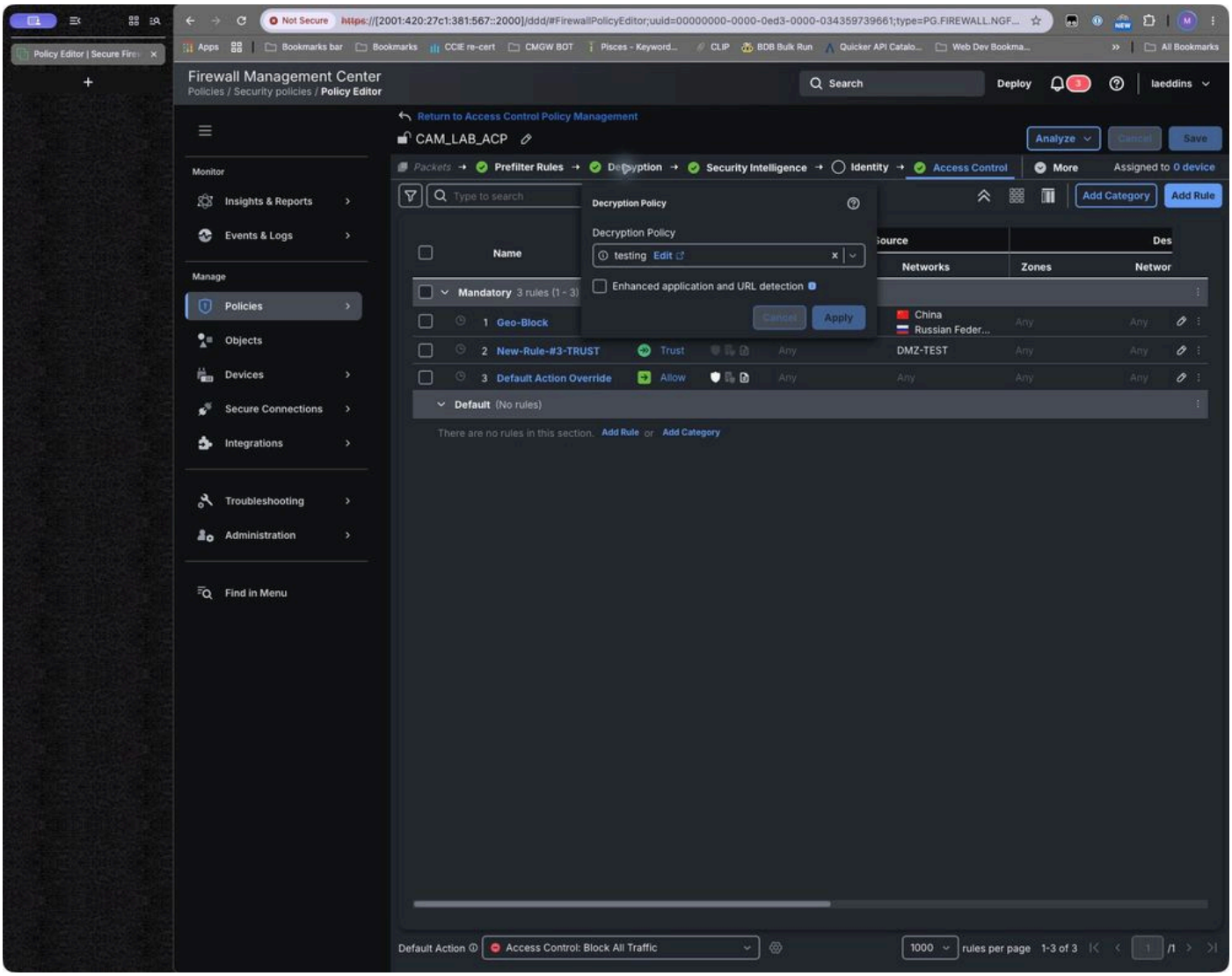
3 Regelvolgorde en beleidsassociatie controleren

Plaats de regel vóór bredere regels die hetzelfde verkeer als eerste kunnen verwerken. Bevestig de TLS-beleidsassociatie met het toegangsbeheerbeleid dat is toegewezen aan de doelapparaten. Controleer het voorfilter en andere bypass-paden voordat u het test.

Afbeelding 5. Bestaande tabel met regels voor testbeleid. Dit toont alleen de bestelinterface.



Figuur 5b. Het bestaande CAM_LAB_ACP-beleid verwijst naar het beleid voor het decoderen van tests.



Implementeren en verifiëren

Implementeer de wijzigingen in de apparaten in kwestie. Indien beschikbaar, test met een website waarvan u weet dat deze een certificaat gebruikt dat is uitgegeven door een van de betrokken bevoegde autoriteiten.

Problemen met onverwachte resultaten oplossen

Als het verkeer passeert, controleert u de implementatiestatus, het verkeersbereik, de beleidsassociatie, de regelvolgorde, de spelling van de emittent en de veldencodering en of het apparaat certificaatgegevens had. Bepaal of een andere regel of bypass-pad de stroom heeft verwerkt. Controleer de zichtbaarheid van TLS 1.3 op de geteste release voordat u een gelijkwaardige dekking claimt.

Aanvullende TLS 1.3-validatie: op FMC 7.6 is TLS 1.3-decryptie een afzonderlijke geavanceerde decryptie-instelling; als deze is uitgeschakeld, zijn de decryptieregels alleen van toepassing op TLS 1.2 of lager. Als u TLS 1.3-decodering inschakelt, kunt u de identiteit van de server aanpassen en kan een DN-voorwaarde van de emittent een sonde activeren wanneer het certificaat niet in de cache is opgeslagen. De instelling TLS 1.3 Server Identity Discovery van het bijbehorende toegangsbeheerbeleid heeft voorrang. Cisco zegt dat deze geavanceerde instellingen worden genegeerd op apparaten die eerder zijn dan 7.1 of waarop Snort 2 wordt uitgevoerd, en dat adaptieve identiteitsdetectie niet wordt ondersteund op FTDv die is geïmplementeerd in AWS. Valideer de zichtbaarheid van de doelsoftware/het doelplatform en het certificaat voordat u TLS 1.3-dekking claimt. De TLS-versieselector van de regel vermeldt zelf SSL 3.0 tot en met TLS 1.2; vertrouw niet op die selector voor TLS 1.3. [7]

Als niet-gerelateerd verkeer mislukt, identificeert u de werkelijke matchingsregel en de emittent. Verklein de DN- of verkeersruimte indien nodig en herhaal vervolgens zowel de getroffen als de niet-getroffen tests. Schakel certificaatvalidatie niet uit als een tijdelijke oplossing.

Dekking en operationele limieten

Deze oplossing blokkeert niet elk scenario of vervangt de noodzaak om andere services bij te werken.

Terugdraaiing en pensioenregeling

Als de regel een onaanvaardbare impact heeft, schakelt u de nieuwe regel uit via het normale wijzigingsproces en herschikt u deze. Bewaar gebeurtenissen en test bewijs. Bevestig vóór uw pensionering dat de betreffende werklasten het huidige vertrouwensbeleid afdwingen, herhaal negatieve certificaatvalidatietests en verkrijg de goedkeuring van de eigenaar van de wijziging om tijdelijke insluiting te verwijderen.

Referenties

[1] Decryptieregels FMC 7.2

[2] FMC 10.x Regelgebaseerde decoderingsregels

[3] Nieuwe functies van Secure Firewall Management Center per release

[4] Automatische update van CA-bundels voor FMC en FDM configureren

[5] FMC 7.6-certificaten

[6] FDM 7.6-certificaten

[7] FMC 7.6 Decryptiebeleid en TLS 1.3-richtsnoeren

[8] Cisco Secure Firewall ASA 9.22 General Operations CLI Configuration Guide — Digitale certificaten

[9] Cisco Secure Firewall ASA Series Command Reference — crypto-cartrustpool-beleid

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.