Guide Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance - Méfiance d'urgence des autorités de certification racine et intermédiaire eMudhra

Table des matières

Objectif

Vous trouverez ci-dessous des conseils sur Cisco Secure Firewall Threat Defense (FTD), Cisco Secure Firewall Management Center (FMC) et Adaptive Security Appliance (ASA) pour la méfiance d'urgence des autorités de certification racine et intermédiaire eMudhra.

Mises à jour du bundle de certificats de service Cisco local FMC

FMC et FTD peuvent mettre à jour automatiquement un bundle CA local utilisé pour les connexions TLS de l'appliance vers les services Cisco, y compris les mises à jour de licences et de logiciels Smart, de VDB, de SRU et de géolocalisation. Le système effectue une vérification quotidienne à une heure définie par le système. Cisco documente la disponibilité des fonctionnalités à partir de FMC/FTD 7.0.5, 7.1.0.3, 7.2.4 et 7.3.0+. Il s'agit de seuils de fonctionnalités, pas de destinations de mise à niveau recommandées ; sélectionner une cible de mise à niveau en utilisant la plate-forme exacte, la version source, les exigences de compatibilité et les conseils de version Cisco actuels. [3, 4]

Sur une CLI FMC ou FTD prise en charge, `show cert-update` signale l'état de la mise à jour automatique, le planning quotidien et l'heure de dernière modification de l'offre groupée. `configure cert-update test` vérifie si le bundle local est à jour et si la connectivité de mise à jour est prête. [4, 5, 6]

Ce bundle de services Cisco est distinct des objets/groupes d'autorité de certification approuvés configurés par FTD utilisés par le déchiffrement SSL et des points de confiance de périphériques utilisés pour les certificats d'identité ou VPN. Vous devrez vérifier qu'aucun de ces certificats n'a été ajouté manuellement à la configuration. [5, 6]

Importation automatique du pool de confiance ASA CA

Sur ASA, le pool de confiance CA et les points de confiance nommés sont des fonctionnalités de gestion de certificats distinctes. Le groupe de confiance détient des certificats CA ; un point de confiance est une configuration nommée utilisée pour l'identité de certificat et l'inscription d'autorité de certification. L'importation automatique du pool de confiance ASA est également distincte de la mise à jour du bundle de services Cisco FMC/FTD décrite ci-dessus. [8, 9]

Pour une vérification en lecture seule, exécutez `show crypto ca trustpool policy` pour examiner le nombre de certificats trustpool, l'état et le résultat de l'importation, la prochaine tentative planifiée et les détails de la stratégie effective. Exécutez la commande `show run crypto ca trustpool policy` pour examiner les lignes de stratégie trustpool configurées. Par défaut, les documents Cisco sont importés automatiquement. Lorsque cette option est activée sans remplacement, le planning documenté est une tentative toutes les 24 heures à 22:00 et l'URL Cisco par défaut est utilisée ; une heure ou une URL configurée peut modifier ces valeurs. Vérifiez le résultat réel de l'ASA plutôt que de supposer que l'importation automatique est activée ou en utilisant la planification par défaut. [8, 9]

Ces vérifications indiquent la stratégie et l'état d'importation ; ils ne fournissent pas d'inventaire certificat par certificat et n'établissent pas qu'un certificat eMudhra nommé est installé, supprimé ou n'est pas approuvé. Ne déduisez pas le comportement ASA de FMC/FTD `cert-update`, et ne traitez pas l'état trustpool comme une preuve sur les certificats configurés sous un point de confiance particulier ou un autre magasin de confiance d'application. Confirmez la version ASA exacte et le service dépendant du certificat avant de décider si une action spécifique au produit est nécessaire. [8, 9]

Solution de contournement potentielle en utilisant le FTD pour protéger vos périphériques non corrigés

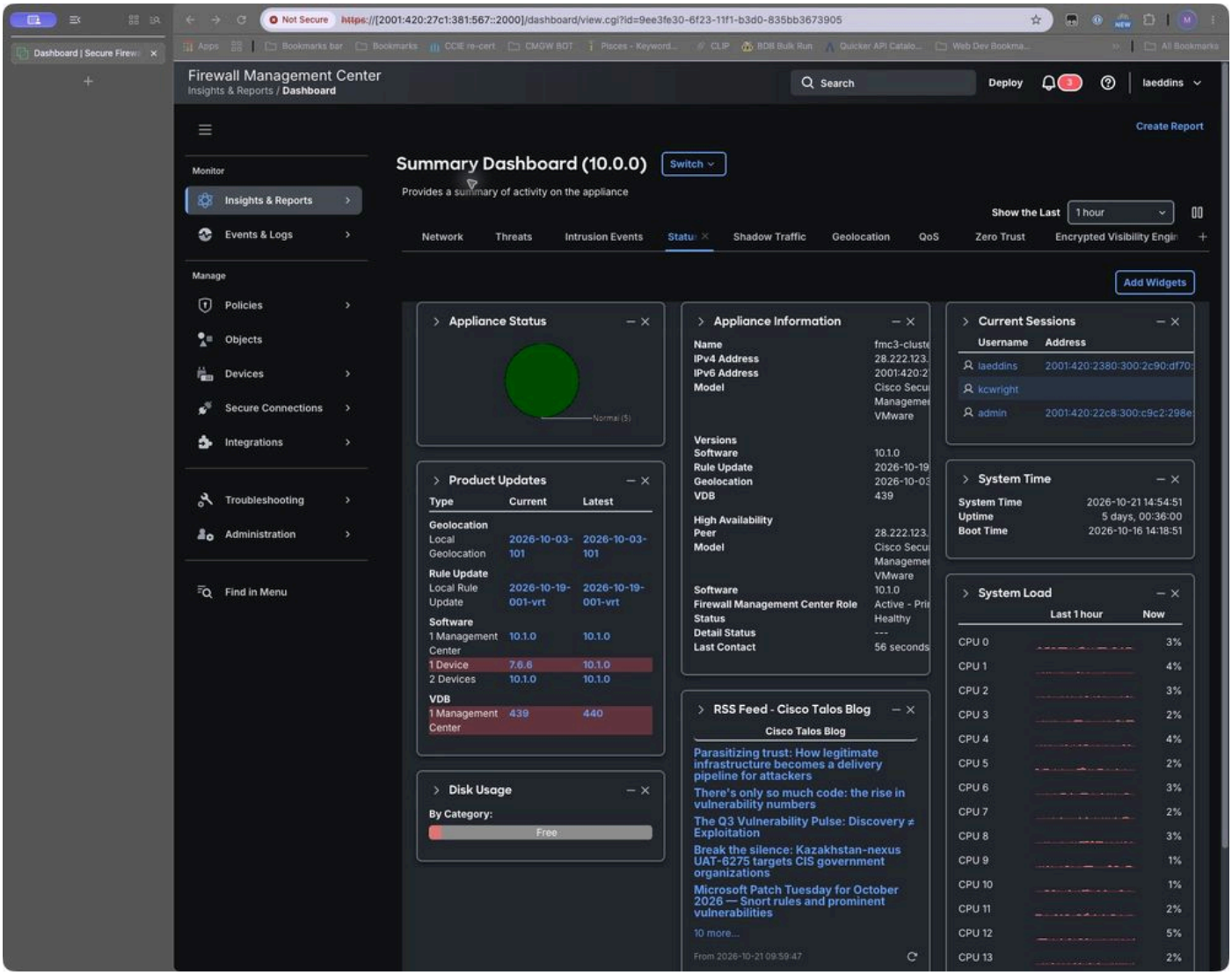
Objectif

Utilisez Cisco Secure Firewall Management Center (FMC) pour configurer des règles de stratégie TLS qui bloquent les certificats de serveur avec des noms d'émetteurs eMudhra affectés connus. Ce contrôle peut réduire l'exposition des clients et serveurs sans en-tête dont les magasins d'approbation d'applications n'ont pas encore reçu les mises à jour requises, mais il ne bloque pas les connexions dans tous les scénarios. Poursuivez la correction du magasin de confiance et le remplacement du certificat. N'importez pas d'autorité de certification compromise dans des autorités de certification approuvées pour cette procédure.

Conditions préalables

Les écrans de configuration de cet article ont été capturés sur FMC 10.1.0. Le tableau de bord répertorie deux périphériques gérés sur 10.0.0 et un sur 7.6.6. Aucun test de trafic n'a été effectué. Avant la validation de l'application, enregistrez la version FTD cible, le moteur Snort, le mode d'application, la stratégie de contrôle d'accès et la stratégie TLS. Vérifiez que le trafic sortant affecté atteint la stratégie prévue.

Figure 1. Inventaire des logiciels FMC 10.1.0 et des périphériques gérés



Configurer la correspondance des émetteurs

Cisco documente les conditions d'émetteur-DN pour la correspondance avec l'autorité de certification qui a émis le certificat de serveur. Ajoutez un objet DN avec Ajouter à l'émetteur dans l'éditeur de règles. La navigation et les étiquettes disponibles dépendent de la version. [1, 2]

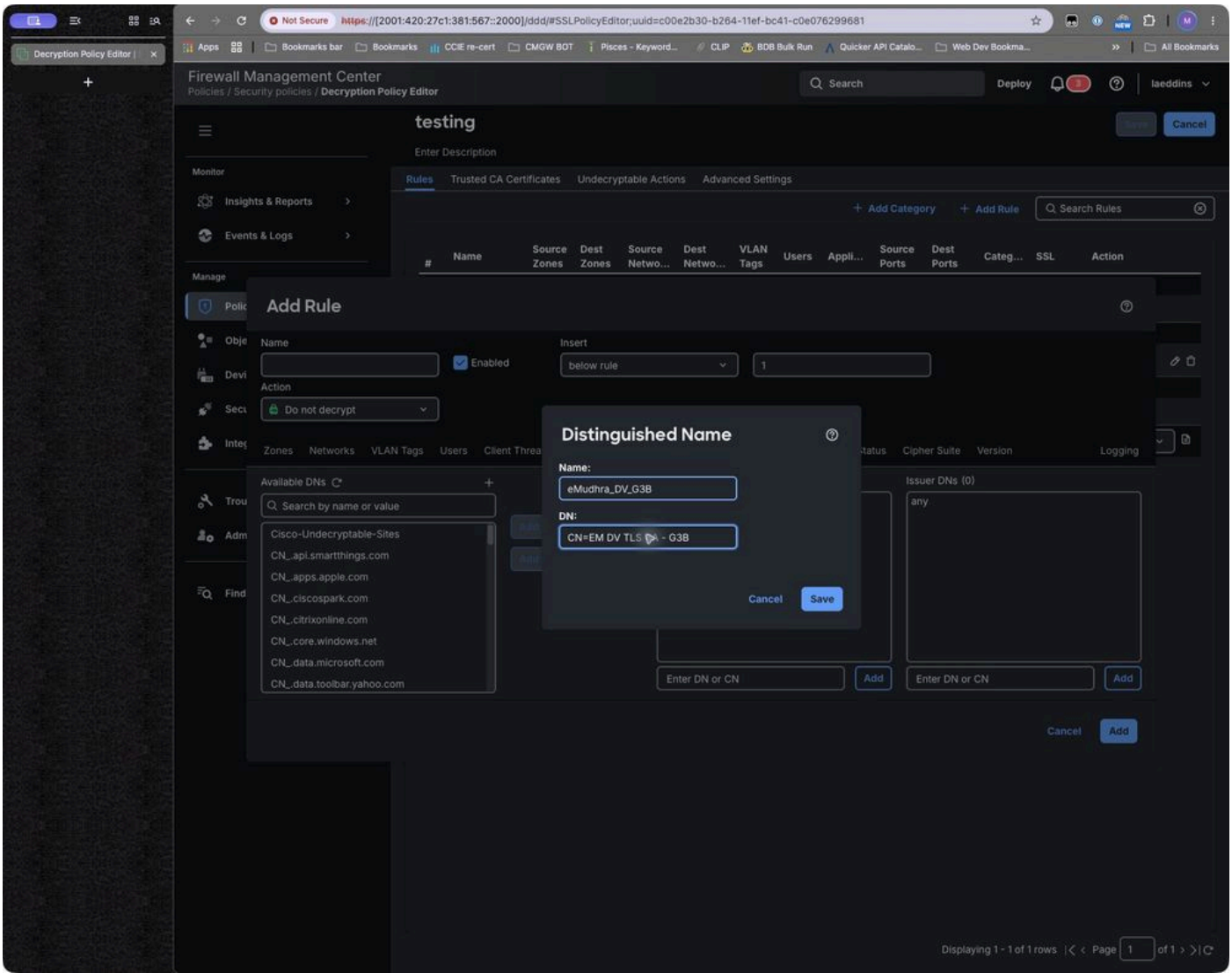
1 Création des objets

Table des objets

DN	Nom d'objet DN proposé
CN=EM DV TLS CA - G3B	eMudhra_DV_G3B
CN=EM DV TLS CA - G3C	eMudhra_DV_G3C
CN=EM EV TLS CA - G3B	eMudhra_EV_G3B
CN=EM EV TLS CA - G3C	eMudhra_EV_G3C
CN=EM OV TLS CA - G3B	eMudhra_OV_G3B
CN=EM OV TLS CA - G3C	eMudhra_OV_G3C

Créez un objet DN d'étendue étroite pour chacun des objets du tableau ci-dessus.

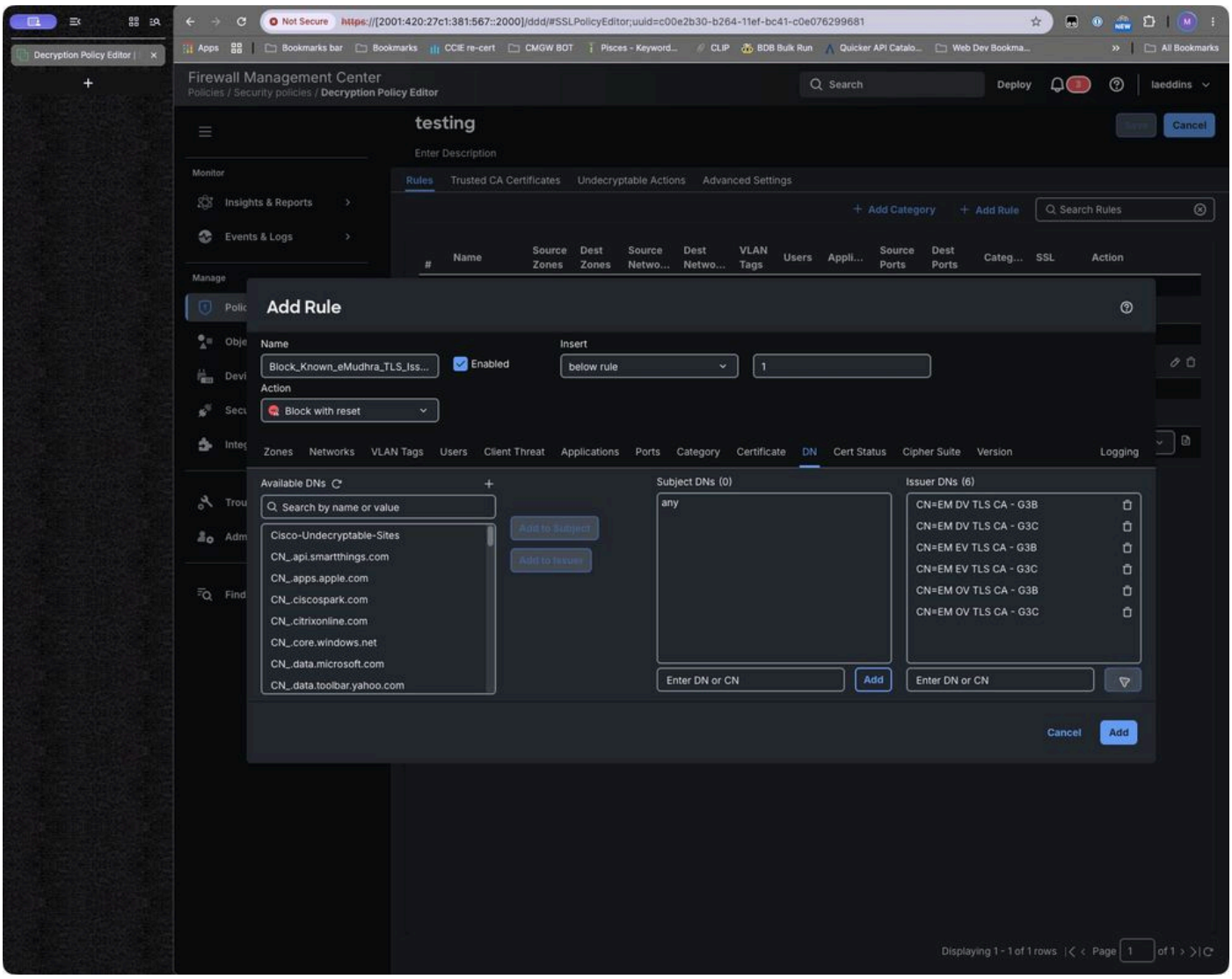
Figure 2. Formulaire de nom distinctif affichant les champs Nom et DN. L'exemple de valeur a été saisi pour l'illustration ; cliquez sur Enregistrer lorsque vous avez terminé.



2 Créer la règle de blocage

Dans FMC 10.1.0, sélectionnez Stratégies > Stratégies de sécurité > Déchiffrement, ouvrez la stratégie applicable et cliquez sur Ajouter une règle. Nommez la règle Block_Known_Mudhra_TLS_Issuers. Ouvrez l'onglet DN. Ajoutez des objets vérifiés à l'aide de l'option Ajouter à l'émetteur ou saisissez un DN dans le champ DN de l'émetteur intitulé Entrer DN ou CN et cliquez sur le bouton Ajouter correspondant. Confirmez que les noms apparaissent dans les DN de l'émetteur et non dans les DN de l'objet.

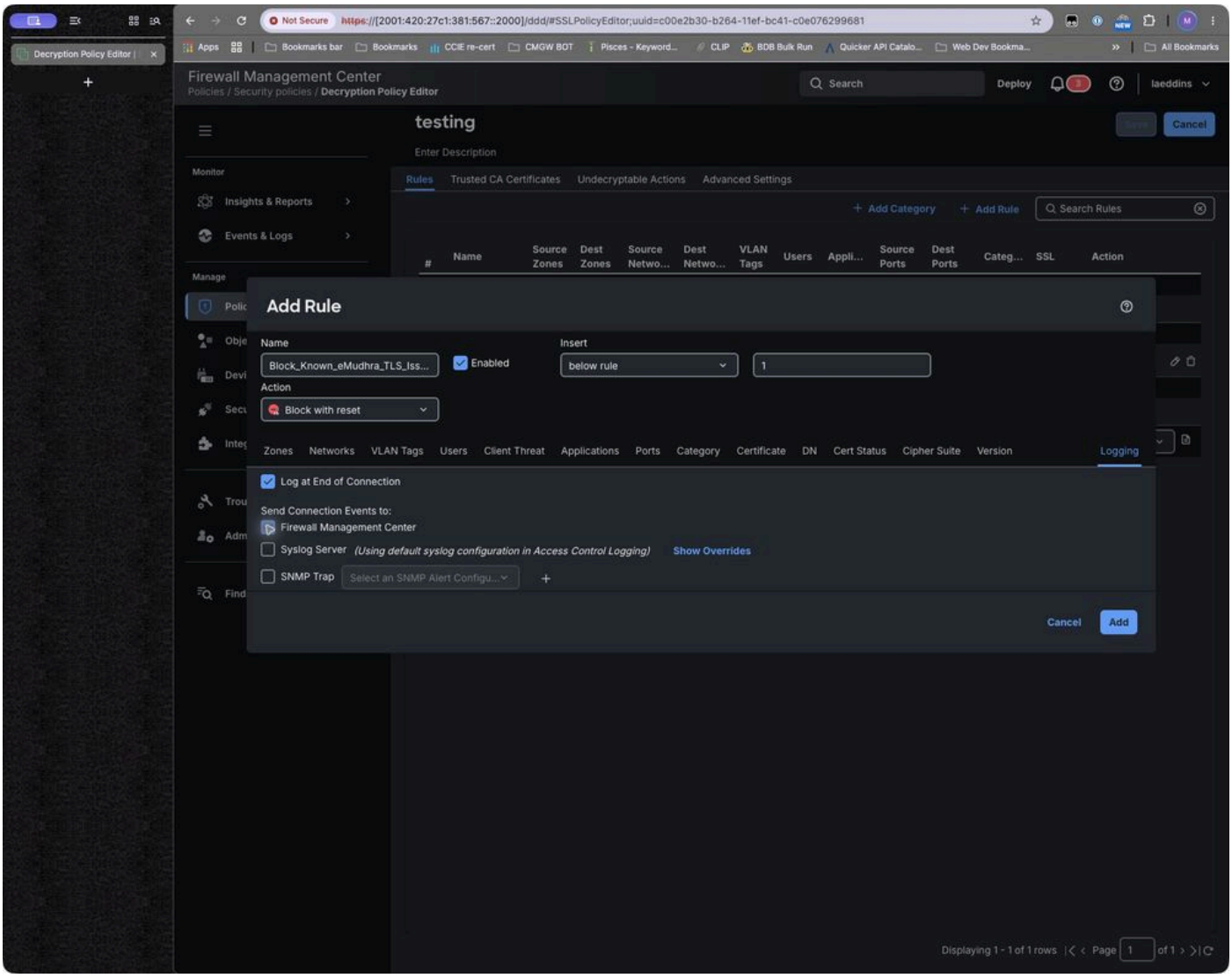
Figure 3. Règle affichant Block with reset, l'onglet DN, six DN d'émetteur et aucune contrainte de DN d'objet. Cliquez sur Ajouter lorsque vous avez terminé.



Sélectionnez Bloquer ou Bloquer avec réinitialisation. Limitez les zones sources ou les réseaux à la portée convenue. Si vous le souhaitez, dans l'onglet Journalisation, sélectionnez Fichier journal à la fin de la connexion et vérifiez que Firewall Management Center est sélectionné. N'ajoutez pas de condition Valide = Oui : le bloc d'émetteurs prévu ne doit pas dépendre du certificat passant la validation de confiance.

Figure 4. Règle indiquant le journal à la fin de la connexion et le Centre de gestion du pare-feu

sélectionné. Cliquez sur Ajouter lorsque vous avez terminé



3 Examiner l'ordre des règles et l'association des stratégies

Placez la règle au-dessus de règles plus larges qui pourraient gérer le même trafic en premier. Confirmez l'association de la stratégie TLS avec la stratégie de contrôle d'accès attribuée aux périphériques cibles. Vérifiez le préfiltre et les autres chemins de contournement avant de tester.

Figure 5. Table de règles de stratégie de test existante. Affiche uniquement l'interface de commande.

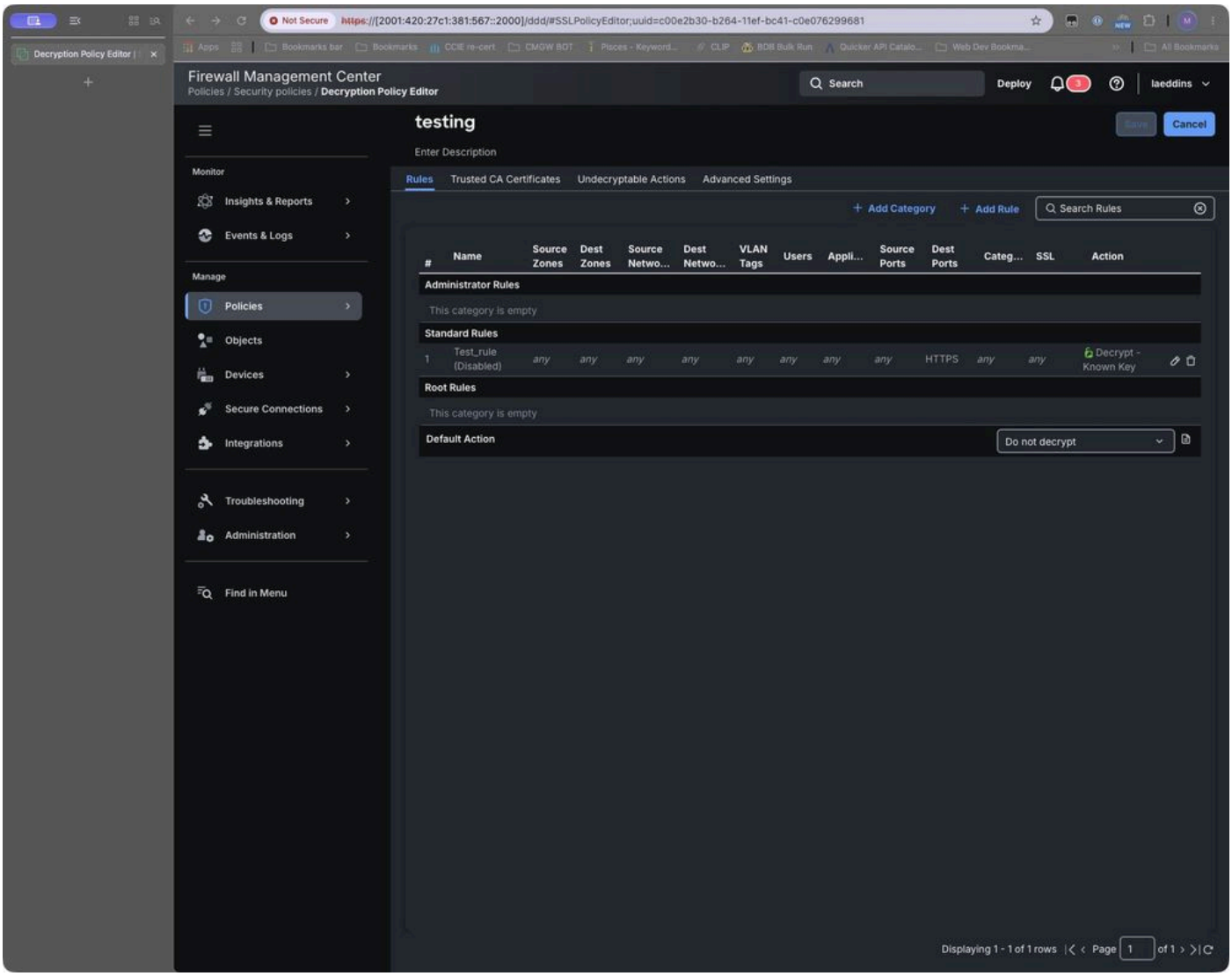
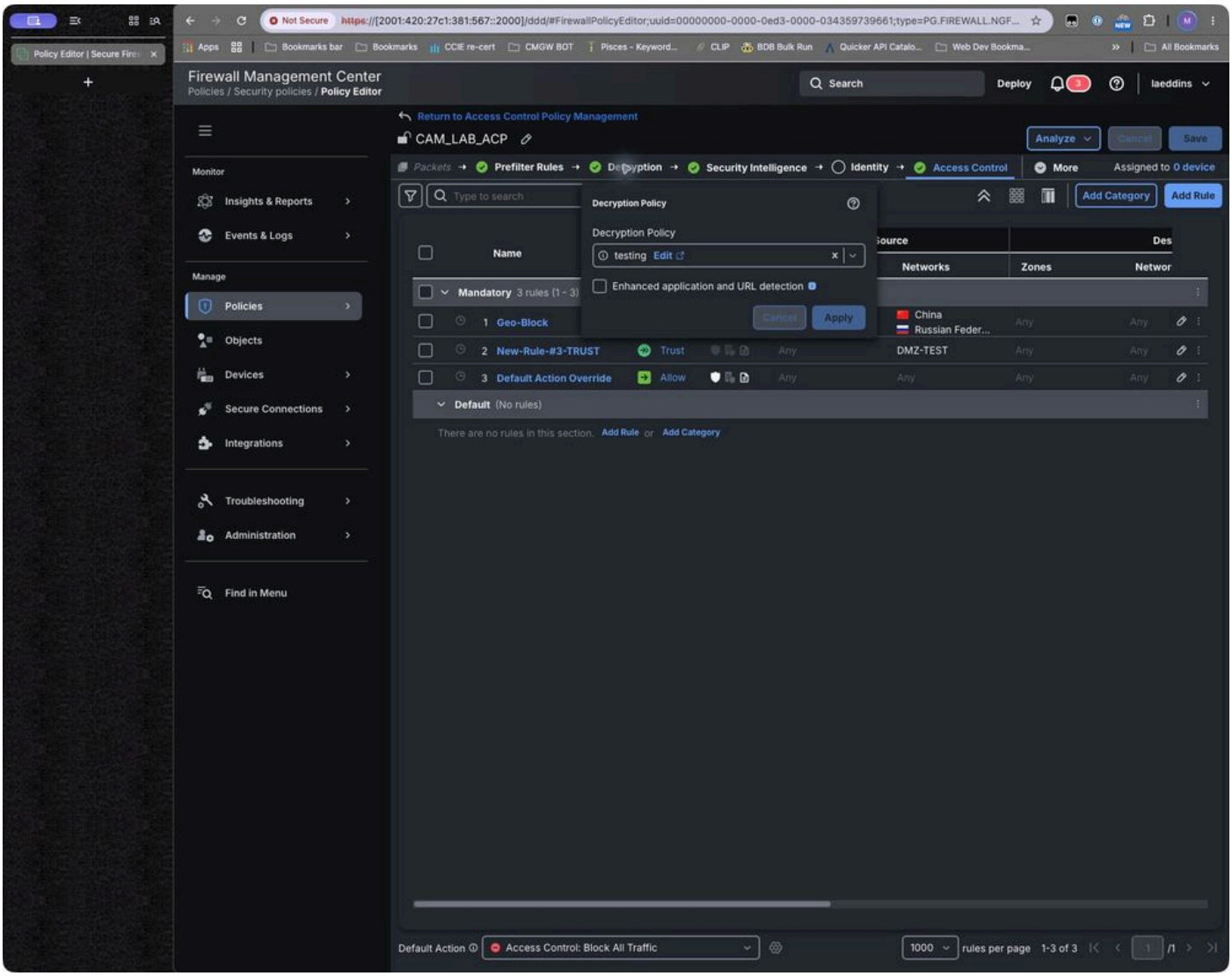


Figure 5b. La stratégie CAM_LAB_ACP existante fait référence à la stratégie de déchiffrement de test.



Déployer et vérifier

Déployez les modifications sur les périphériques en question. Le cas échéant, effectuez un test sur un site Web dont vous savez qu'il utilise un certificat délivré par l'une des autorités de certification en question.

Dépanner les résultats inattendus

Si le trafic réussit, vérifiez l'état du déploiement, l'étendue du trafic, l'association des stratégies, l'ordre des règles, l'orthographe de l'émetteur et le codage des champs, et si le périphérique disposait d'informations de certificat. Déterminez si une autre règle ou un chemin de contournement a traité le flux. Vérifiez la visibilité de TLS 1.3 sur la version testée avant de demander une couverture équivalente.

Validation TLS 1.3 supplémentaire : sur FMC 7.6, le décryptage TLS 1.3 est un paramètre avancé

de stratégie de décryptage distinct ; si elle est désactivée, les règles de décodage s'appliquent uniquement à TLS 1.2 ou version antérieure. L'activation du déchiffrement TLS 1.3 active l'analyse adaptative de l'identité du serveur et une condition DN de l'émetteur peut déclencher une analyse lorsque le certificat n'est pas mis en cache. Le paramètre Détection des identités du serveur TLS 1.3 de la stratégie de contrôle d'accès associée est prioritaire. Cisco indique que ces paramètres avancés sont ignorés sur les périphériques antérieurs à la version 7.1 ou exécutant Snort 2, et que la détection d'identité adaptative n'est pas prise en charge sur FTDv déployé sur AWS. Validez le logiciel/la plate-forme cible et la visibilité sur les certificats avant de demander la couverture TLS 1.3. Le sélecteur de version TLS de la règle répertorie lui-même SSL 3.0 à TLS 1.2 ; ne vous fiez pas à ce sélecteur pour TLS 1.3. [7]

Si le trafic non lié échoue, identifiez la règle de correspondance et l'émetteur. Réduisez l'étendue du DN ou du trafic selon les besoins, puis répétez les tests affectés et non affectés. Ne désactivez pas la validation de certificat comme solution de contournement.

Couverture et limites opérationnelles

Cette solution ne bloque pas tous les scénarios et ne remplace pas la mise à jour d'autres services.

Restauration et retrait des règles

Si la règle a un impact inacceptable, désactivez la nouvelle règle par le biais du processus de modification normal et redéployez. Préserver les événements et tester les preuves. Avant la mise hors service, vérifiez que les charges de travail affectées appliquent la stratégie d'approbation actuelle, répétez les tests de validation de certificat négatifs et obtenez l'approbation du propriétaire de la modification pour supprimer la rétention temporaire.

Références

[1] Règles de décodage FMC 7.2

[2] Règles de décodage basées sur les règles FMC 10.x

[3] Secure Firewall Management Center Nouvelles fonctionnalités par version

[4] Configurer la mise à jour automatique des ensembles CA pour FMC et FDM

[5] Certificats FMC 7.6

[6] Certificats FDM 7.6

[7] FMC 7.6 Politiques de décodage et TLS 1.3

[8] Guide de configuration de l'interface de ligne de commande des opérations générales de Cisco Secure Firewall ASA 9.22 — Certificats numériques

[9] Référence des commandes de la gamme Cisco Secure Firewall ASA — crypto ca trustpool policy

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.