Guida di Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance - Attendibilità di emergenza delle autorità di certificazione principali e intermedie di Mudhra

Sommario

Scopo

Di seguito sono riportate le linee guida su Cisco Secure Firewall Threat Defense (FTD), Cisco Secure Firewall Management Center (FMC) e Adapative Security Appliance (ASA) per la sfiducia in caso di emergenza delle autorità di certificazione principali e intermedie di Mudhra.

Aggiornamenti del bundle dei certificati Cisco locali FMC

FMC e FTD possono aggiornare automaticamente un bundle CA locale utilizzato per le connessioni TLS dall'accessorio ai servizi Cisco, inclusi gli aggiornamenti di software e licenze Smart, VDB, SRU e geolocalizzazione. Il sistema esegue controlli giornalieri a un'ora definita dal sistema. La disponibilità dei documenti Cisco inizia con FMC/FTD 7.0.5, 7.1.0.3, 7.2.4 e 7.3.0+. Si tratta di soglie di funzionalità, non di destinazioni di aggiornamento consigliate; selezionare una destinazione dell'aggiornamento usando la piattaforma, la release di origine, i requisiti di compatibilità e le linee guida correnti di Cisco release. [3, 4]

In una CLI FMC o FTD supportata, `show cert-update` segnala lo stato di aggiornamento automatico, la pianificazione giornaliera e l'ora dell'ultima modifica del bundle. `configura test cert-update` verifica se il bundle locale è corrente e se la connettività di aggiornamento è pronta. [4, 5, 6]

Questo bundle Cisco-service è separato dagli oggetti/gruppi CA trusted configurati dell'FTD e utilizzati dalla decrittografia SSL e dai trust dispositivo utilizzati per i certificati di identità o VPN. Sarà necessario verificare che nessuno di questi certificati sia stato aggiunto manualmente alla configurazione. [5, 6]

Importazione automatica trust pool CA ASA

Nell'appliance ASA, il trust pool CA e i trust point denominati sono funzionalità di gestione dei certificati separate. Il pool di trust contiene certificati CA; un trust point è una configurazione denominata utilizzata per l'identità del certificato e la registrazione della CA. L'importazione automatica del trust pool ASA è inoltre distinta dall'aggiornamento del bundle Cisco-service FMC/FTD descritto sopra. [8, 9]

Per un controllo di sola lettura, eseguire `show crypto ca trustpool policy` per esaminare il conteggio dei certificati trustpool, lo stato e il risultato dell'importazione, il successivo tentativo pianificato e i dettagli dei criteri effettivi. Eseguire il comando `show run crypto ca trustpool policy` per esaminare le righe dei criteri di trust pool configurate. Per impostazione predefinita, l'importazione automatica dei documenti Cisco è disattivata. Se abilitata senza override, la pianificazione documentata è un tentativo ogni 24 ore alle 22:00 e viene utilizzato l'URL Cisco predefinito; un'ora o un URL configurato può modificare questi valori. Controllare l'output effettivo dell'ASA invece di presupporre che l'importazione automatica sia abilitata o usare la pianificazione predefinita. [8, 9]

Tali controlli mostrano la politica e lo stato delle importazioni; non forniscono un inventario certificato per certificato né accertano che qualsiasi certificato eMudhra denominato sia installato, rimosso o non attendibile. Non dedurre il comportamento ASA da FMC/FTD `cert-update` e non considerare lo stato del trust pool come prova di certificati configurati in un determinato trust point o altro trust store applicazioni. Prima di decidere se un'azione specifica sul prodotto è necessaria, verificare l'esatta versione dell'ASA e il servizio basato sui certificati. [8, 9]

Possibile soluzione utilizzando FTD per proteggere i dispositivi senza patch

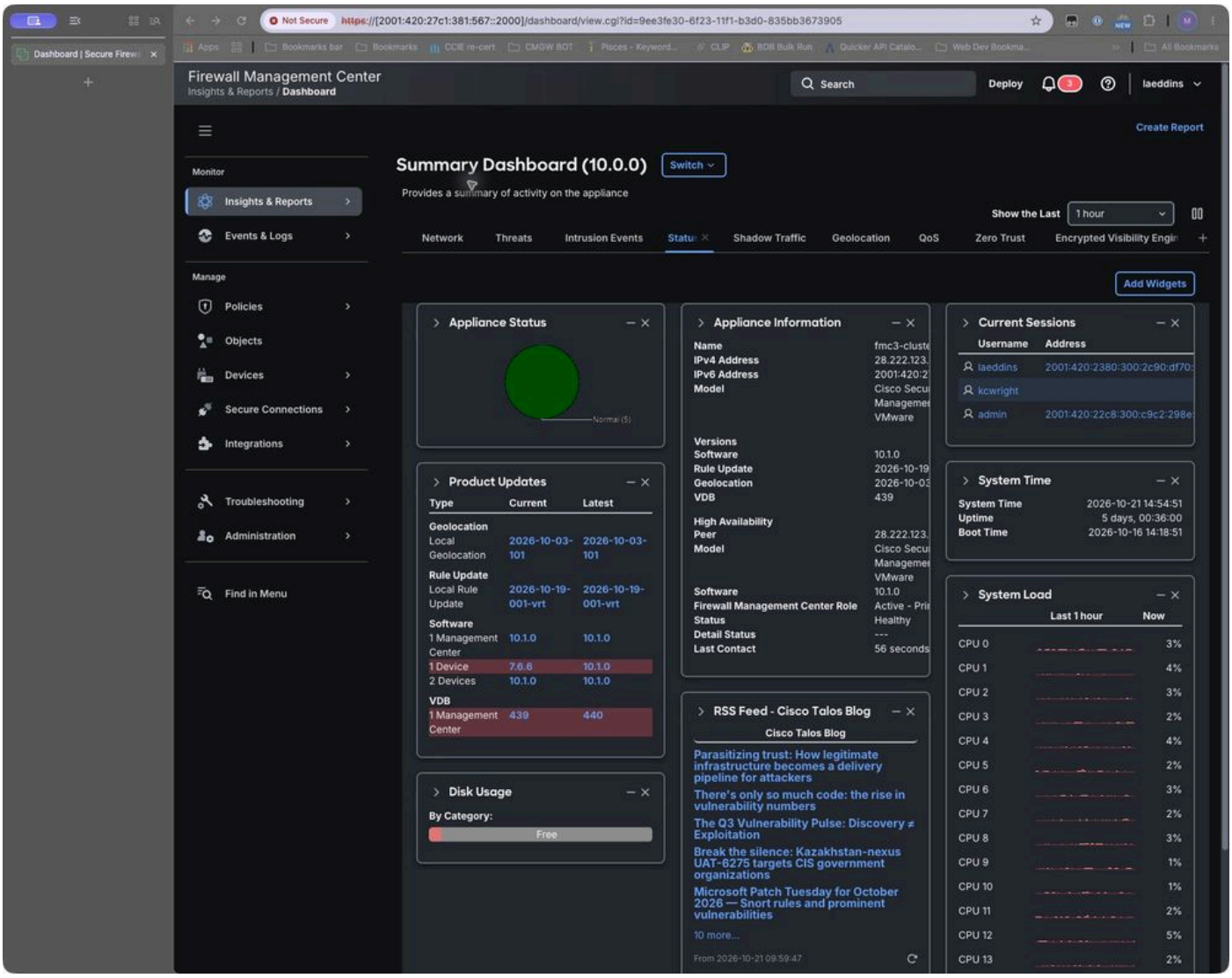
Scopo

Utilizzare Cisco Secure Firewall Management Center (FMC) per configurare le regole dei criteri TLS che bloccano i certificati server con nomi di autorità di certificazione eMudhra note interessate. Questo controllo può ridurre l'esposizione per i client e i server headless i cui archivi attendibilità applicazioni non hanno ancora ricevuto gli aggiornamenti necessari, ma non blocca le connessioni in tutti gli scenari. Continua il monitoraggio e l'aggiornamento dell'archivio di attendibilità e la sostituzione dei certificati. Non importare una CA compromessa in CA attendibili per questa procedura.

Prerequisiti

Le schermate di configurazione in questo articolo sono state acquisite in FMC 10.1.0. Il dashboard elenca due dispositivi gestiti in 10.0.0 e uno in 7.6.6. Non è stato eseguito alcun test del traffico. Prima della convalida dell'imposizione, registrare la versione FTD di destinazione, il motore Snort, la modalità di imposizione, i criteri di controllo di accesso e i criteri TLS. Confermare che il traffico in uscita interessato raggiunga il criterio desiderato.

Figura 1. FMC 10.1.0 e inventario software dei dispositivi gestiti.



Configura corrispondenza emittente

Cisco documenta le condizioni DN emittente per la corrispondenza con la CA che ha emesso il certificato del server. Aggiungere un oggetto DN con Aggiungi all'autorità emittente nell'editor delle regole. La navigazione e le etichette disponibili dipendono dalla versione. [1, 2]

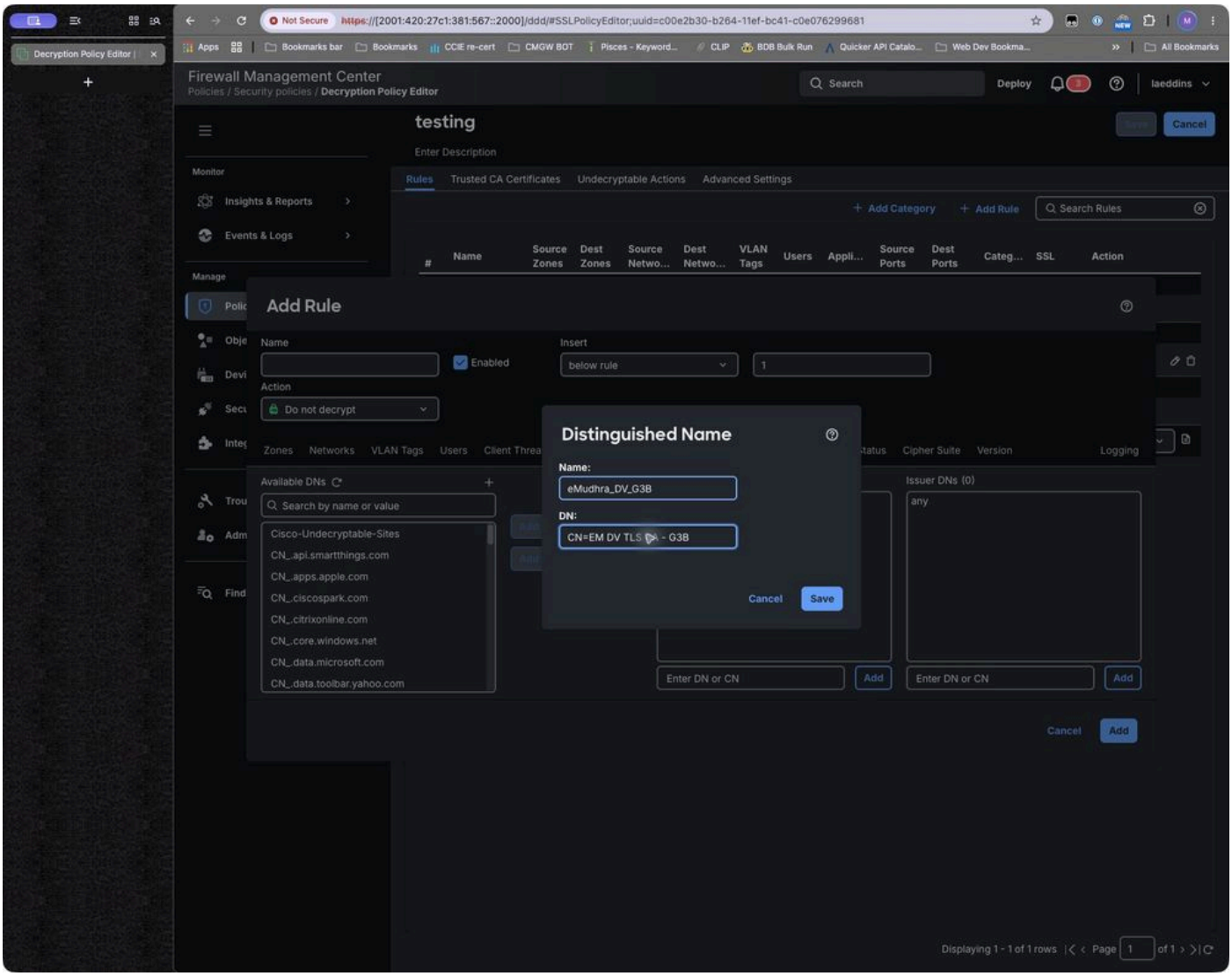
1 Creare gli oggetti

Tabella oggetti

DN	Nome oggetto DN proposto
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

Creare un oggetto DN con ambito ristretto per ciascuno di essi nella tabella precedente.

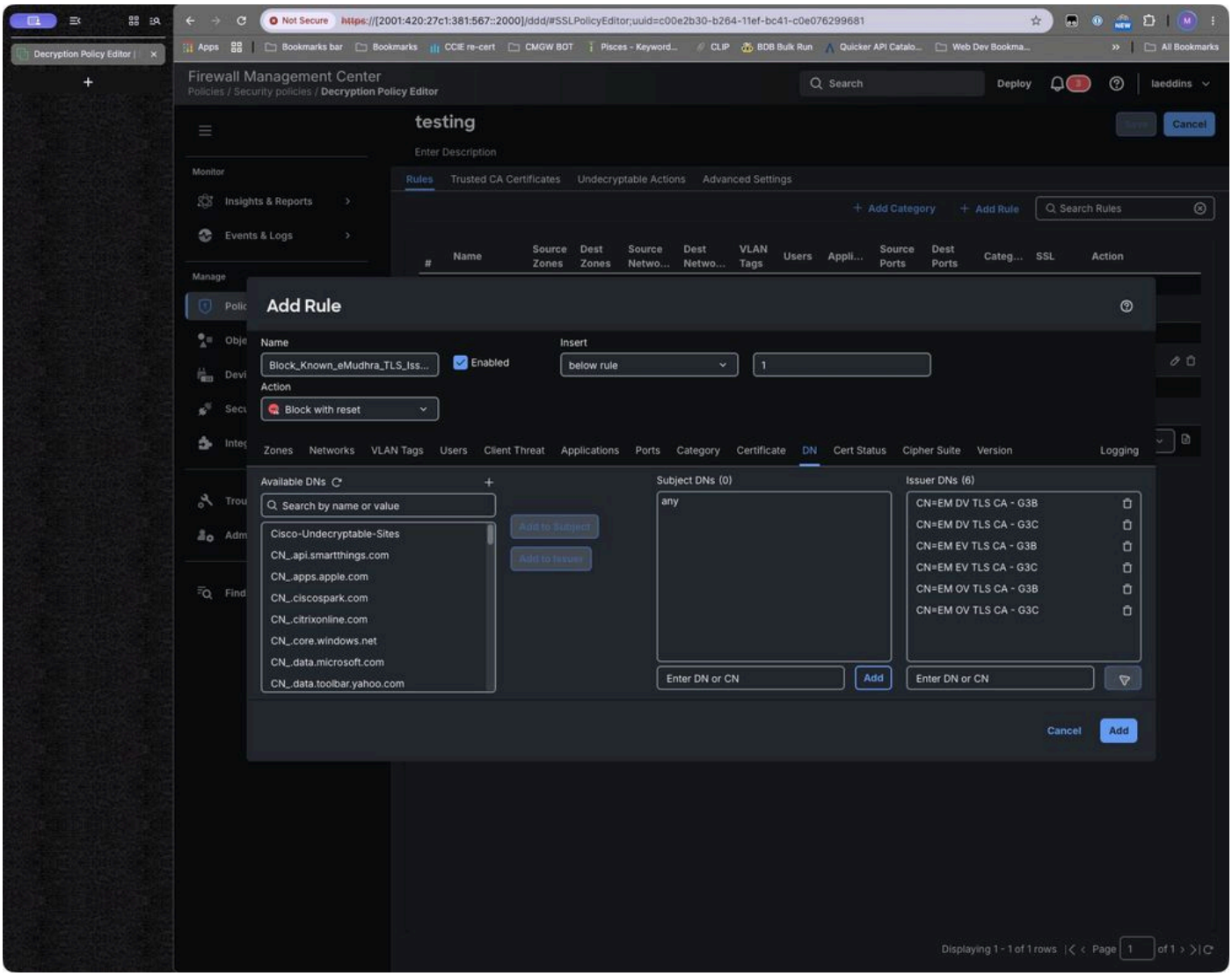
Figura 2. Maschera Nome distinto con i campi Nome e DN. Il valore di esempio è stato inserito a scopo illustrativo; al termine, fare clic su Salva.



2 Creare la regola di blocco

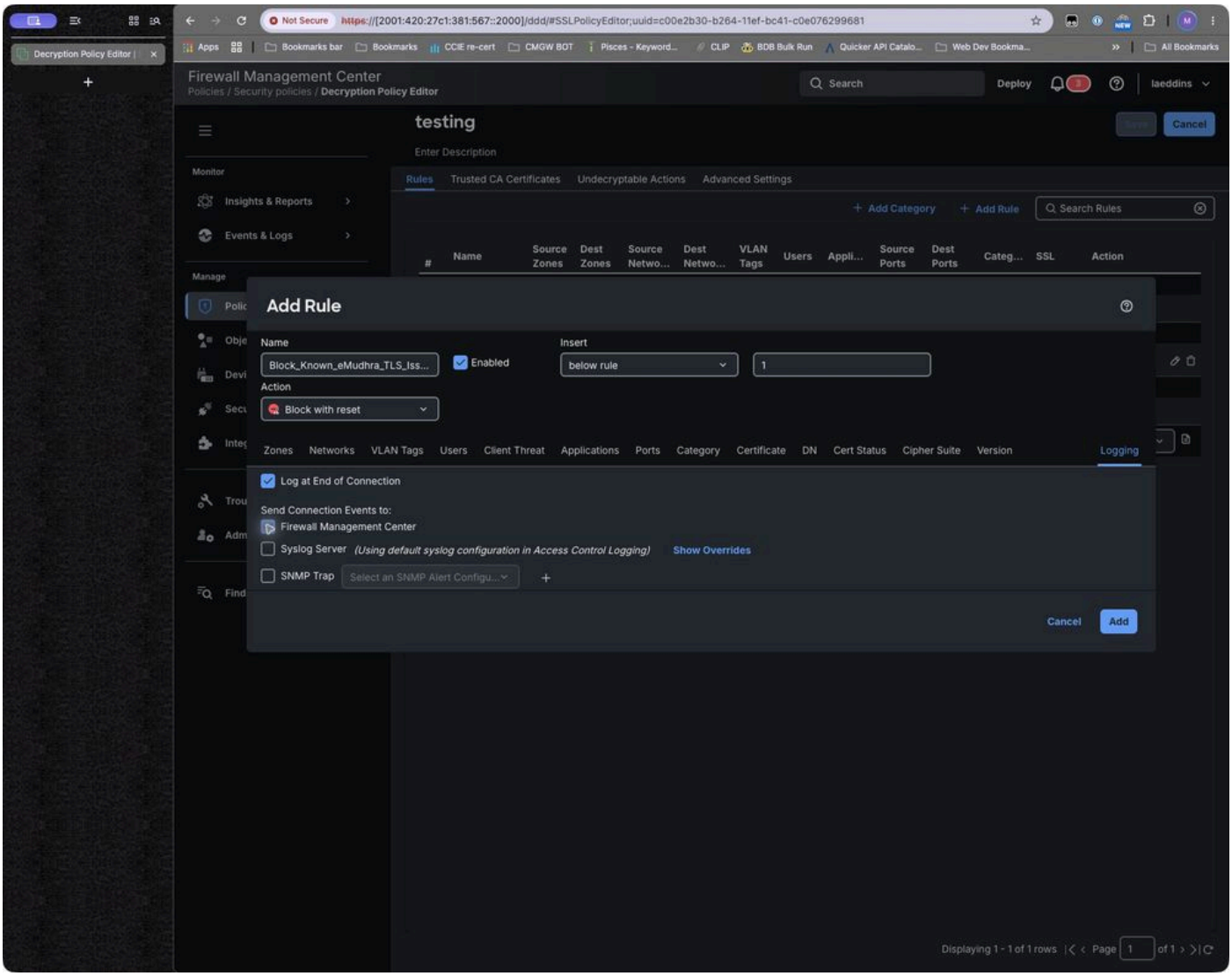
In FMC 10.1.0, selezionare Criteri > Criteri di sicurezza > Decrittografia, aprire il criterio applicabile e fare clic su Aggiungi regola. Denominare la regola Block_Known_Mudhra_TLS_Issuers. Aprire la scheda DN. Aggiungere gli oggetti verificati tramite Aggiungi all'autorità emittente oppure immettere un DN nel campo DN autorità emittente con l'etichetta Immettere DN o CN e fare clic sul relativo pulsante Aggiungi. Confermare che i nomi siano visualizzati nei DN autorità emittente e non nei DN oggetto.

Figura 3. Regola che mostra Blocco con reimpostazione, scheda DN, sei DN emittente e nessun vincolo DN oggetto. Al termine, fare clic su Aggiungi.



Selezionare Blocca o Blocca con reimpostazione. Limitare le zone di origine o le reti all'ambito concordato. Se lo si desidera, nella scheda Registrazione selezionare Registra alla fine della connessione e verificare che sia selezionato Centro gestione firewall. Non aggiungere un requisito Valido = Sì: il blocco emittente desiderato non deve dipendere dal certificato che ha superato la convalida dell'attendibilità.

Figura 4. Regola che mostra il registro alla fine della connessione e centro di gestione dei firewall selezionato. Al termine, fare clic su Aggiungi



3 Esaminare l'associazione tra l'ordine e i criteri delle regole

Posizionare la regola prima delle regole più ampie che potrebbero gestire lo stesso traffico. Confermare l'associazione tra il criterio TLS e il criterio di controllo di accesso assegnato ai dispositivi di destinazione. Prima di eseguire il test, esaminare il prefiltro e gli altri percorsi di bypass.

Figura 5. Tabella delle regole dei criteri di test esistente. Mostra solo l'interfaccia di ordinazione.

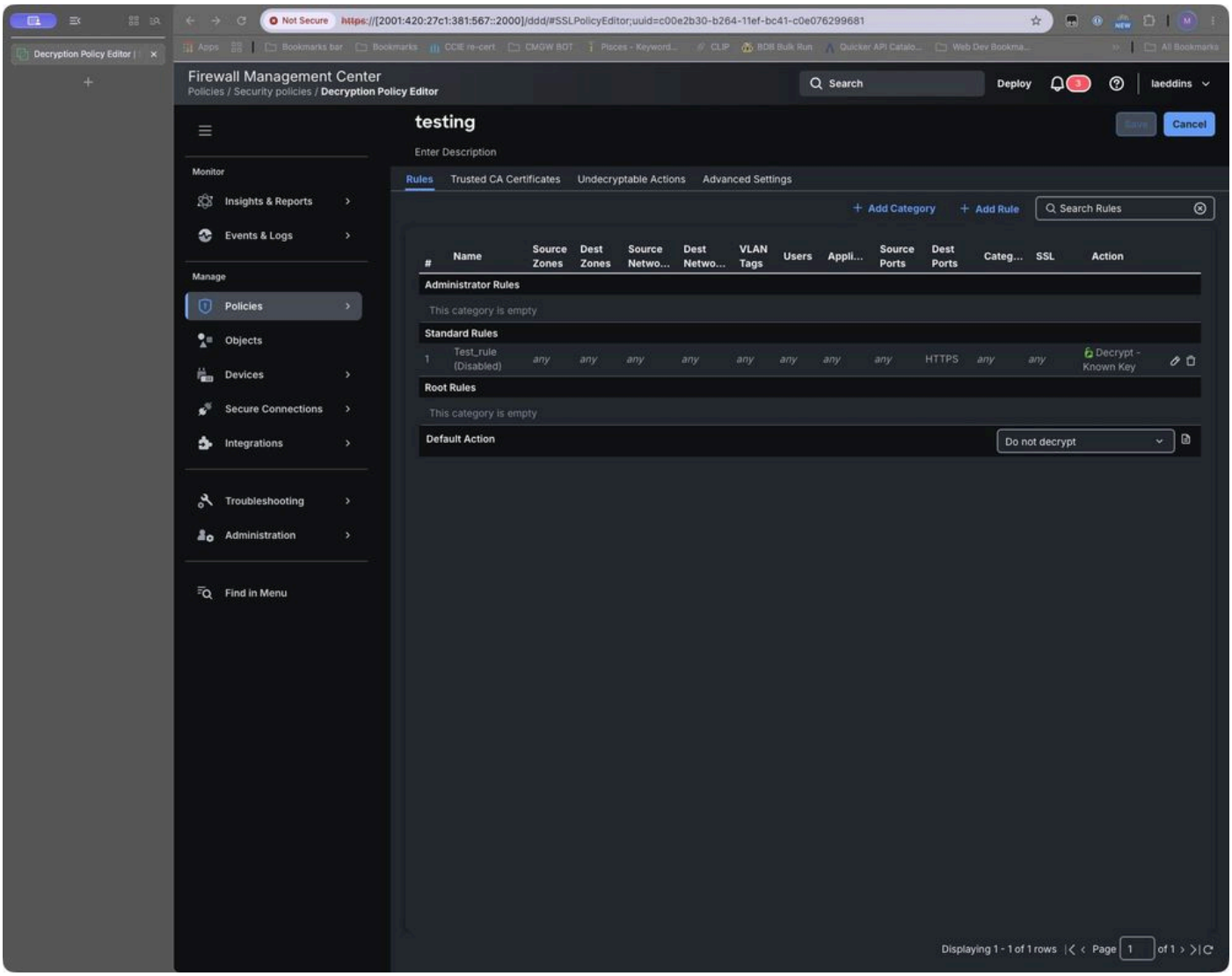
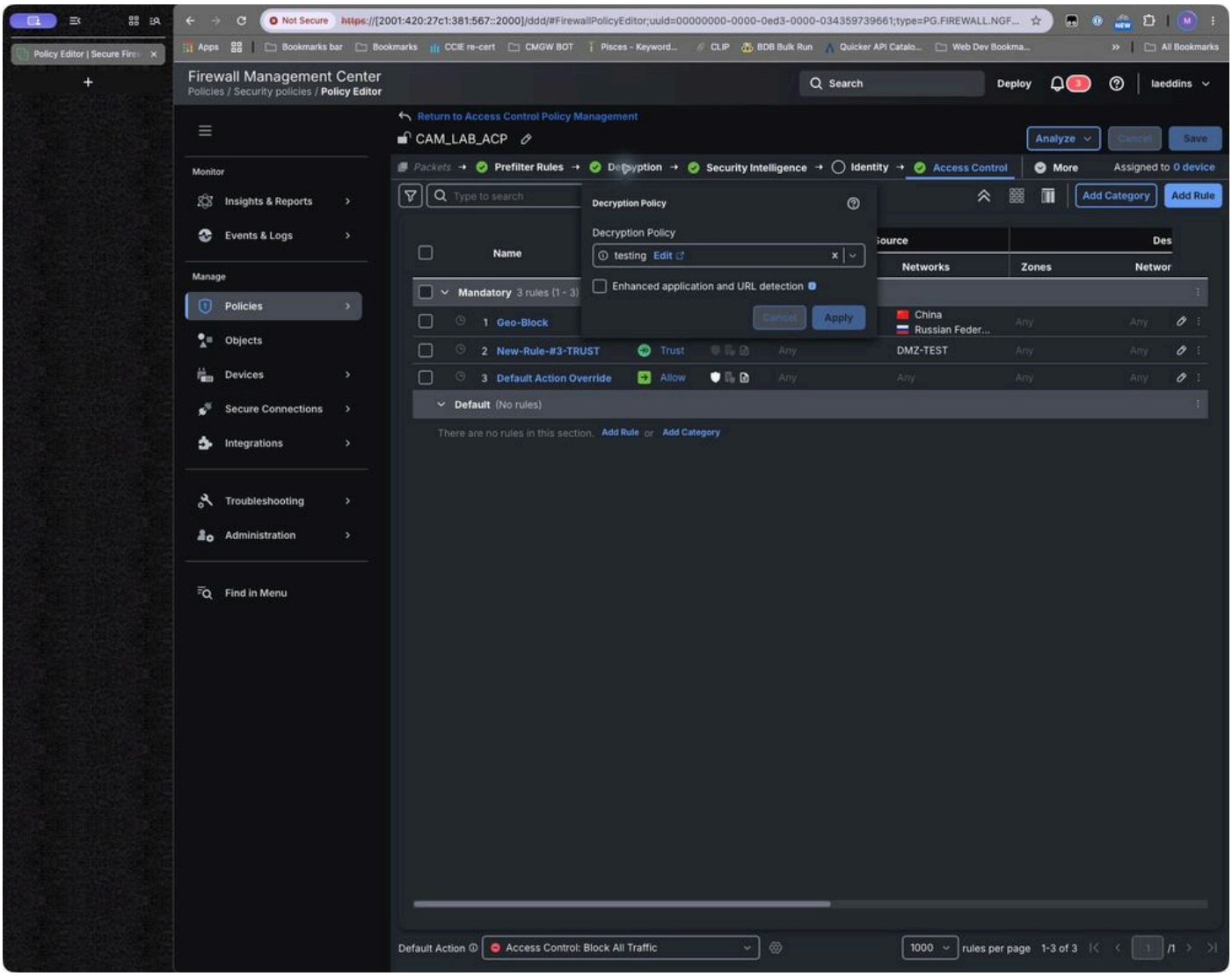


Figura 5b. Il criterio CAM_LAB_ACP esistente fa riferimento al criterio di decrittografia di prova.



Installazione e verifica

Distribuire le modifiche ai dispositivi in questione. Se disponibile, eseguire il test con un sito Web che si è certi stia utilizzando un certificato rilasciato da una delle CA in questione.

Risoluzione dei problemi relativi a risultati imprevisti

Se il traffico viene superato, verificare lo stato della distribuzione, l'ambito del traffico, l'associazione ai criteri, l'ordine delle regole, l'ortografia dell'autorità emittente e la codifica dei campi e verificare se il dispositivo dispone di informazioni sul certificato. Determinare se un'altra regola o un percorso di bypass ha gestito il flusso. Esaminare la visibilità di TLS 1.3 sulla release testata prima di richiedere la copertura equivalente.

Convalida TLS 1.3 aggiuntiva: in FMC 7.6, la decrittografia TLS 1.3 è un'impostazione avanzata

separata per la politica di decrittografia; se è disabilitata, le regole di decrittografia si applicano solo a TLS 1.2 o versioni precedenti. L'attivazione della decrittografia TLS 1.3 consente il probe adattivo dell'identità del server e una condizione del DN dell'autorità emittente può attivare una sonda quando il certificato non è memorizzato nella cache. L'impostazione TLS 1.3 Server Identity Discovery del criterio di controllo dell'accesso associato ha la precedenza. Cisco afferma che queste impostazioni avanzate vengono ignorate sui dispositivi precedenti alla versione 7.1 o che eseguono Snort 2 e che il rilevamento adattivo dell'identità non è supportato su FTDv distribuito in AWS. Convalidare la visibilità del software/piattaforma di destinazione e del certificato prima di richiedere la copertura TLS 1.3. Il selettore di versione TLS della regola elenca da SSL 3.0 a TLS 1.2; non utilizzare questo selettore per TLS 1.3. [7]

Se il traffico non correlato ha esito negativo, identificare la regola di corrispondenza effettiva e l'autorità emittente. Limitare l'ambito del DN o del traffico in base alle esigenze, quindi ripetere i test interessati e non interessati. Non disabilitare la convalida del certificato come soluzione alternativa.

Copertura e limiti operativi

Questa soluzione non blocca tutti gli scenari né sostituisce la necessità di aggiornare altri servizi.

Rollback e ritiro delle regole

Se la regola causa un impatto inaccettabile, disabilitarla tramite il normale processo di modifica e ridistribuirla. Conservare gli eventi e testare le prove. Prima del ritiro, verificare che i carichi di lavoro interessati applichino il criterio di attendibilità corrente, ripetano i test di convalida dei certificati negativi e ottengano l'approvazione del proprietario della modifica per rimuovere il contenimento temporaneo.

Riferimenti

[1] Regole di decrittografia FMC 7.2

[2] Regole di decrittografia basate su regole di FMC 10.x

[3] Nuove funzionalità di Secure Firewall Management Center per release

[4] Configurare l'aggiornamento automatico dei pacchetti CA per FMC e FDM

[5] Certificati FMC 7.6

[6] Certificati FDM 7.6

[7] Politiche di decrittazione del CCP 7.6 e orientamenti TLS 1.3

[8] Guida alla configurazione della CLI per Cisco Secure Firewall ASA 9.22 General Operations - Digital Certificates

[9] Guida di riferimento ai comandi di Cisco Secure Firewall serie ASA - Criterio Crypto CA trustpool

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).