Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance guidance - Mudhraルートおよび中間認証局に対する緊急不信

内容

目的

Cisco Secure Firewall Threat Defense(FTD)、Cisco Secure Firewall Management Center(FMC)、および適応型セキュリティアプライアンス(ASA)について、Mudhraルートおよび中間認証局を緊急に信頼しないためのガイダンスを次に示します。

FMCローカルCiscoサービス証明書バンドルアップデート

FMCとFTDは、アプライアンスからシスコサービスへのTLS接続に使用されるローカルCAバンドルを自動的に更新できます。これには、スマートライセンスとソフトウェア、VDB、SRU、および地理位置情報の更新が含まれます。システムは、システム定義の時刻に毎日チェックを行います。FMC/FTD 7.0.5、7.1.0.3、7.2.4、および7.3.0+以降で使用可能な機能に関するシスコのドキュメントがあります。これらは機能のしきい値であり、推奨されるアップグレード先ではありません。正確なプラットフォーム、ソースリリース、互換性要件、および最新のシスコリリースガイダンスを使用してアップグレード先を選択してください。[3、4]

サポートされているFMCまたはFTD CLIでは、`show cert-update`により、自動更新のステータス、毎日のスケジュール、およびバンドルの最終更新時刻が報告されます。`configure cert-update test`により、ローカルバンドルが最新であるかどうか、および更新接続の準備が整っているかどうかが確認されます。[4 5 6]

このCiscoサービスバンドルは、SSL復号化に使用されるFTDの設定済みの信頼できるCAオブジェクト/グループ、およびIDまたはVPN証明書に使用されるデバイスのトラストポイントから分離されています。これらの証明書が設定に手動で追加されていないことを確認する必要があります。[5、6]

ASA CA信頼プールの自動インポート

ASAでは、CAトラストプールと名前付きトラストポイントは独立した証明書管理機能です。トラストプールはCA証明書を保持します。トラストポイントは、証明書IDおよびCA登録に使用される名前付き設定です。ASAのトラストプールの自動インポートも、前述のFMC/FTDのシスコサービスバンドルのアップデートとは別です。[8、9]

読み取り専用チェックの場合、`show crypto ca trustpool policy`を実行して、トラストプール証明書の数、インポートのステータスと結果、次にスケジュールされる試行、および有効なポリシーの詳細を確認します。`show run crypto ca trustpool policy`を実行して、設定されているトラストプールポリシー行を確認します。シスコでは、デフォルトで自動インポートをオフとして文書化しています。上書きせずに有効にした場合、ドキュメントに記載されているスケジュールは24時間22:00に実行され、デフォルトのCisco URLが使用されます。設定された時間またはURLによってこれらの値が変更される場合があります。自動インポートが有効であると仮定したり、デフォルトスケジュールを使用したりするのではなく、実際のASA出力を確認します。[8、9]

これらのチェックでは、ポリシーとインポートのステータスが表示されます。証明書ごとのインベントリが提供されたり、名前付きeMudhra証明書がインストール、削除、または破棄されたりすることはありません。FMC/FTDの`cert-update`からASAの動作を推測しないでください。また、特定のトラストポイントまたは他のアプリケーションの信頼ストアで設定された証明書に関する証明としてトラストプールのステータスを扱わないでください。製品固有のアクションが必要かどうかを判断する前に、正確なASAリリースと証明書依存サービスを確認します。[8、9]

パッチ未適用のデバイスを保護するためにFTDを使用する場合の回避策

目的

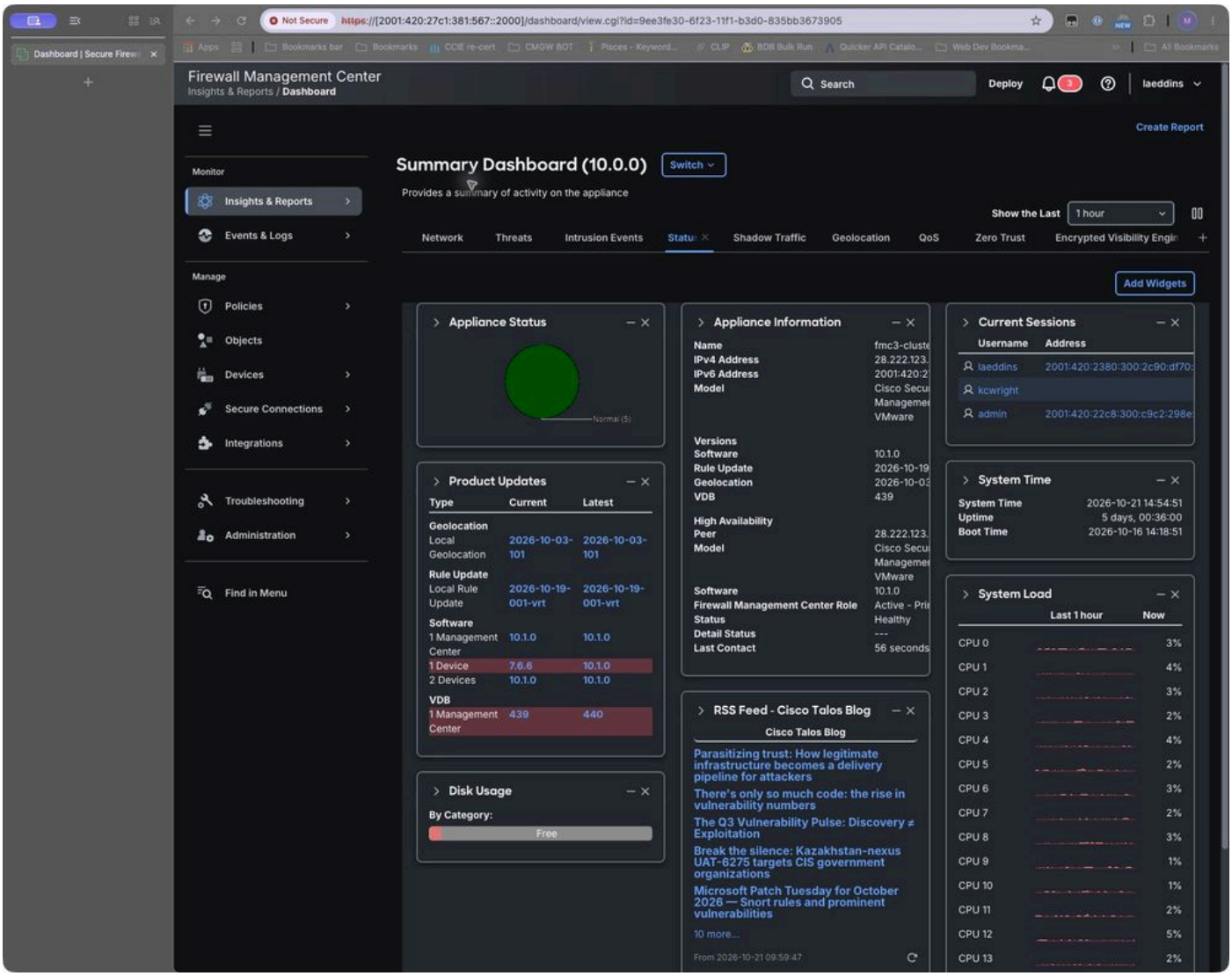
Cisco Secure Firewall Management Center(FMC)を使用して、影響を受ける既知のeMudhra発行者名を持つサーバ証明書をブロックするTLSポリシールールを設定します。この制御により、アプリケーションの信頼ストアが必要な更新をまだ受信していないヘッドレスクライアントおよびサーバの問題を減らすことができますが、すべてのシナリオで接続がブロックされるわけではありません。 信頼ストアの修復と証明書の交換を続行します。この手順では、侵害されたCAを信頼されたCAにインポートしないでください。

前提条件

この記事の設定画面は、FMC 10.1.0でキャプチャされたものです。ダッシュボードには、10.0.0の2つの管理対象デバイスと7.6.6の1つの管理対象デバイスが表示されます。トラフィックテストは実行されなかった。適用の検証を行う前に、ターゲットのFTDバージョン、Snortエンジ

ン、適用モード、アクセスコントロールポリシー、およびTLSポリシーを記録します。影響を受ける発信トラフィックが目的のポリシーに到達することを確認します。

図 1.FMC 10.1.0および管理対象デバイスソフトウェアインベントリ



発行者の照合の構成

シスコでは、サーバ証明書を発行したCAと一致するためのissuer-DN条件を文書化しています。規則エディタで「発行者に追加」を使用してDNオブジェクトを追加します。使用可能なナビゲーションとラベルは、リリースによって異なります。[1、2]

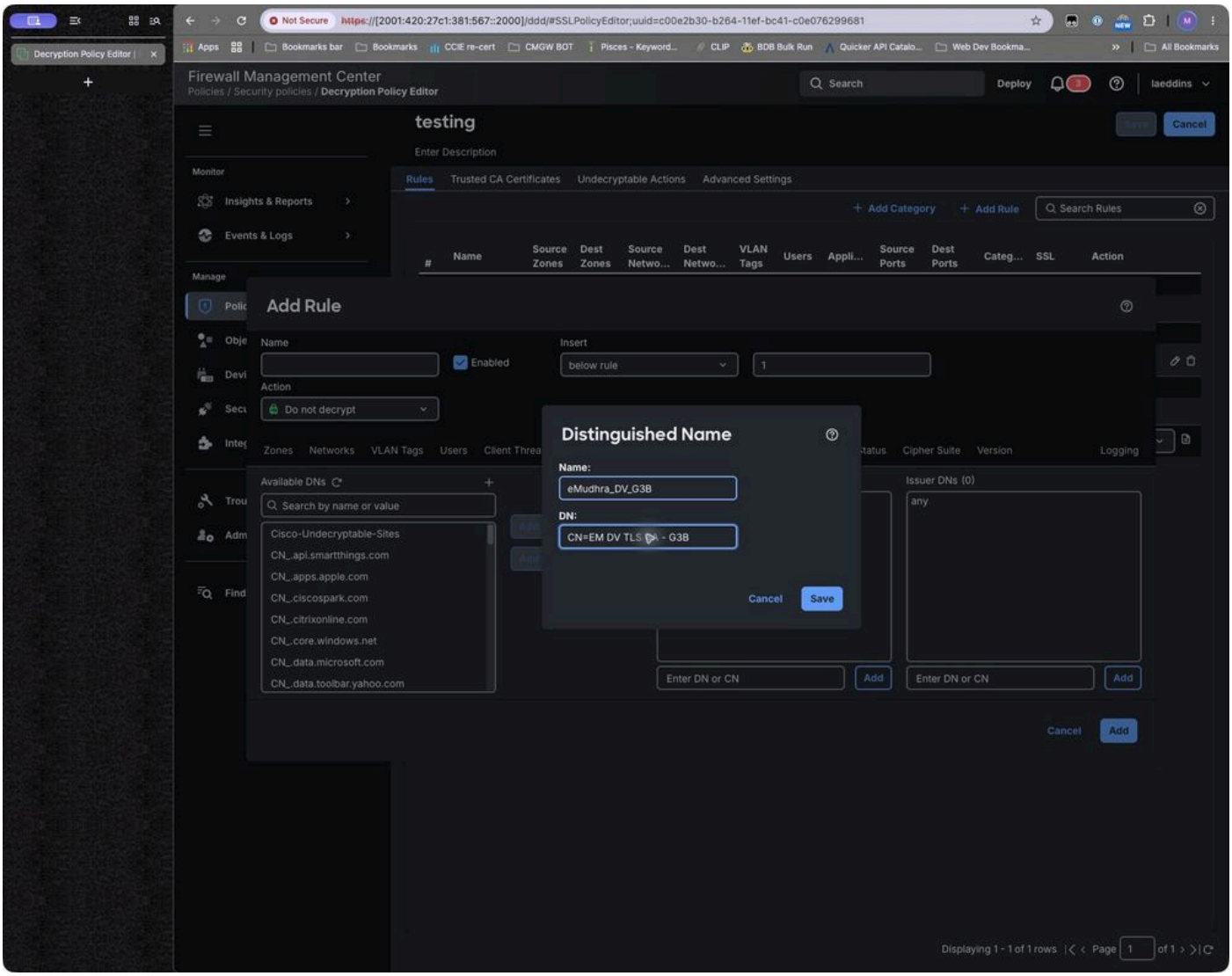
1オブジェクトの作成

オブジェクトテーブル

DN	提案されたDNオブジェクト名
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

上のテーブルの各テーブルに、狭いスコープのDNオブジェクトを1つ作成します。

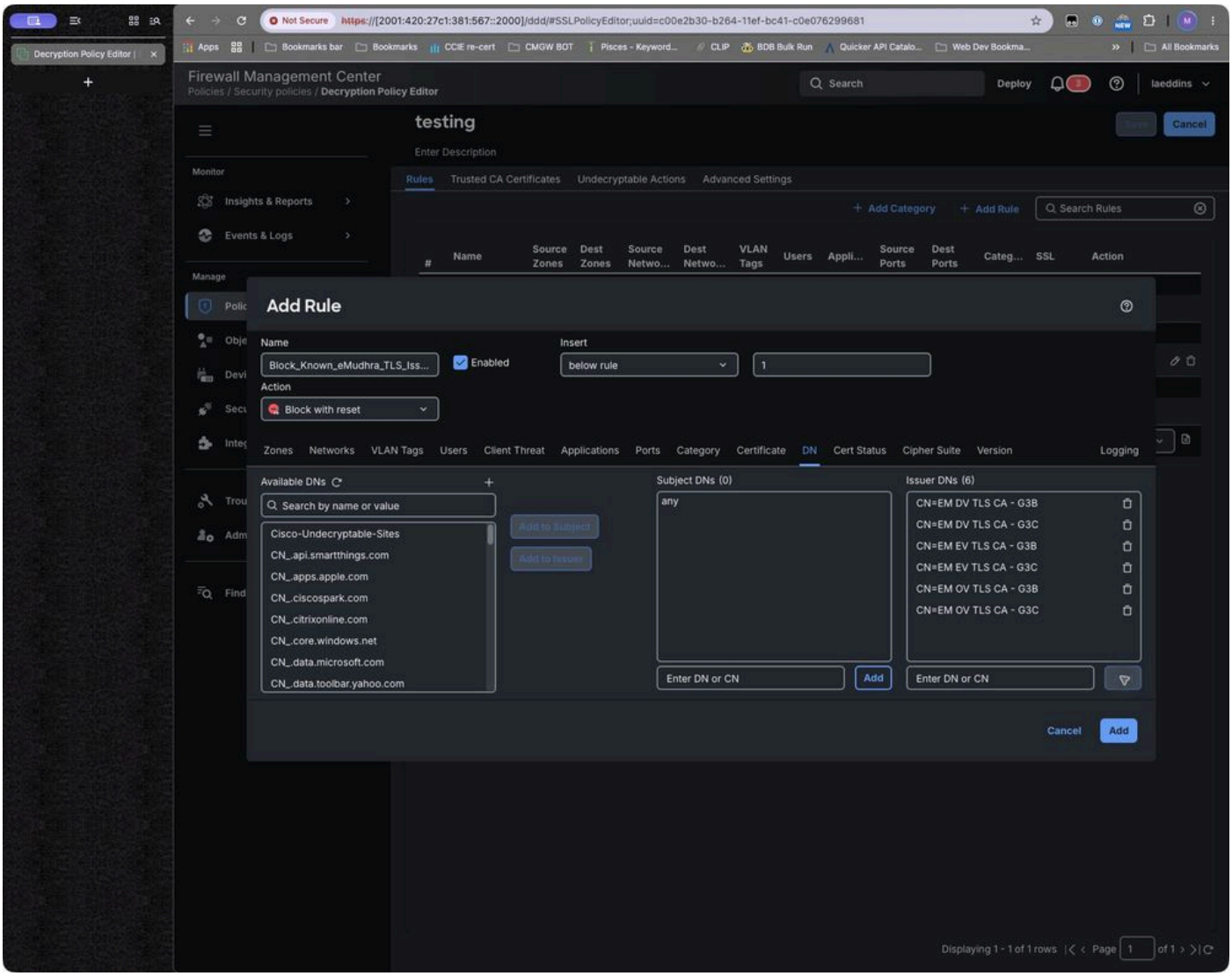
図 2：名前フィールドとDNフィールドを示す識別名フォーム。例の値は説明のために入力されています。終了したら、[保存]をクリックします。



2ブロックルールの作成

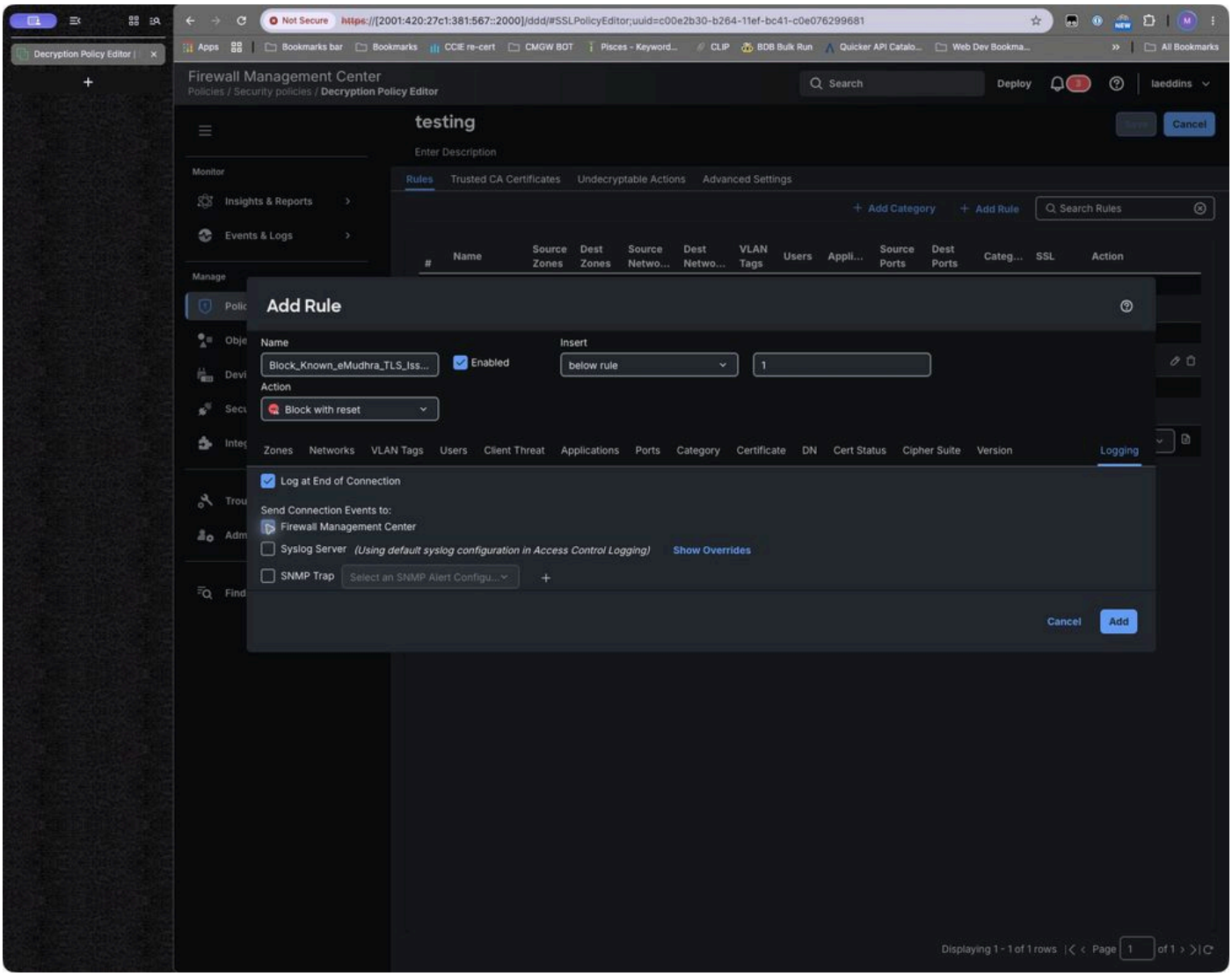
FMC 10.1.0で、Policies > Security policies > Decryptionの順に選択し、該当するポリシーを開いて、Add Ruleをクリックします。ルールにBlock_Known_Mudhra_TLS_Issuersという名前を付けます。DNタブを開きます。「Add to Issuer」を使用して検証済みオブジェクトを追加するか、「Issuer DNs」フィールドに「Enter DN or CN」というラベルの付いたDNを入力し、「Add」ボタンをクリックします。名前がサブジェクトDNではなく、発行者DNに表示されることを確認します。

図 3：リセットされたブロック、DNタブ、6つの発行者DN、およびサブジェクトDN制約がないことを示すルール。完了したら、Addをクリックします。



[ブロック]または[リセット付きブロック]を選択します。ソースゾーンまたはネットワークを、合意された範囲に制限します。必要に応じて、[ログ]タブで[接続の最後にログを記録]を選択し、[ファイアウォール管理センター]が選択されていることを確認します。Valid = Yesの要件を追加しないでください。目的の発行者ブロックは、信頼検証を渡す証明書に依存してはいけません。

図 4：接続の最後にログを示すルールとファイアウォール管理センターが選択されました。完了したらAddをクリックします



3ルールの順序とポリシーの関連付けの確認

同じトラフィックを最初に処理できるより広範なルールの前にルールを配置します。ターゲットデバイスに割り当てられたアクセスコントロールポリシーとのTLSポリシーの関連付けを確認します。テストを行う前に、プレフィルタおよびその他のバイパスパスを確認します。

図 5.既存のtest-policyルールテーブル。これは注文インターフェイスのみを表示します。

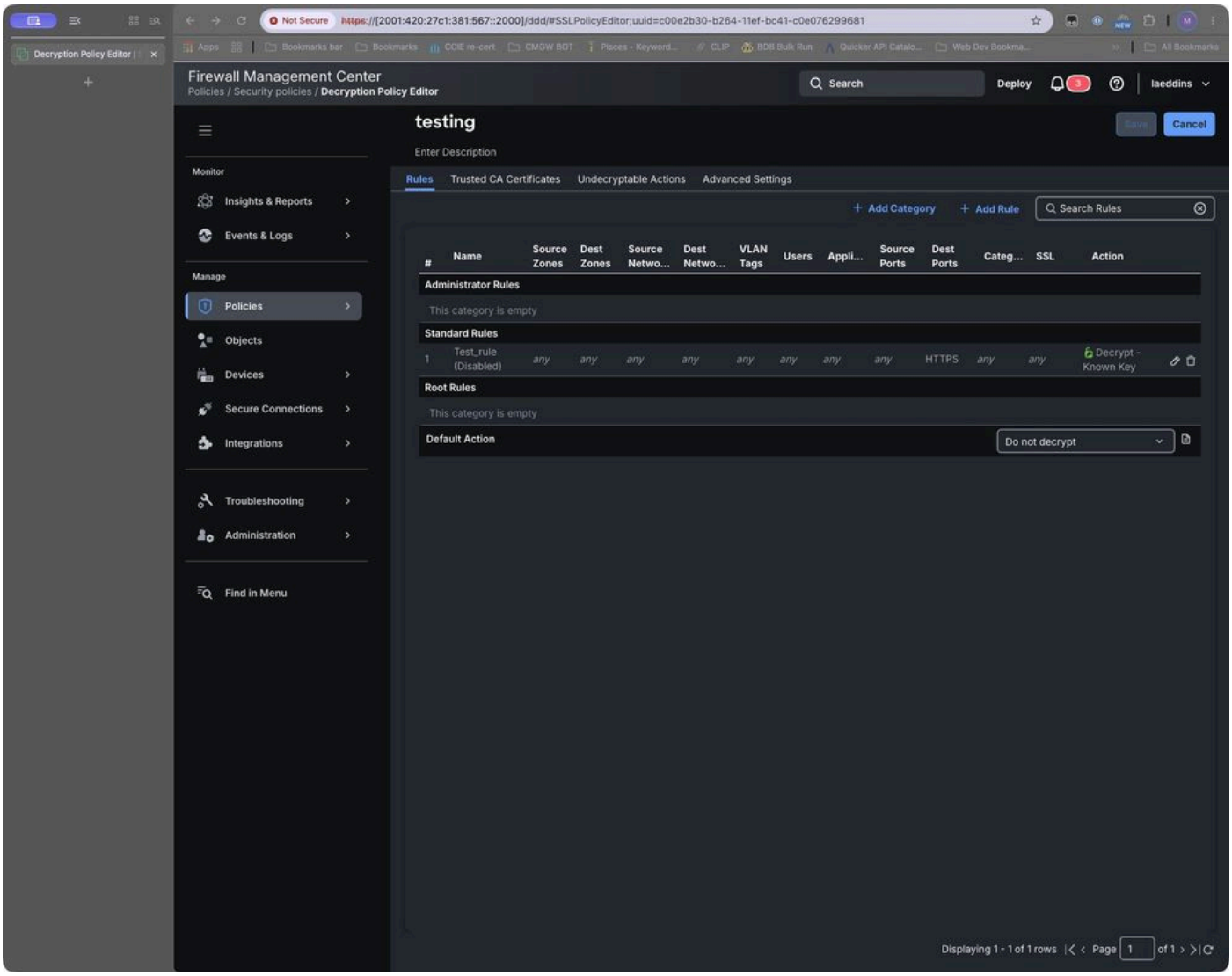
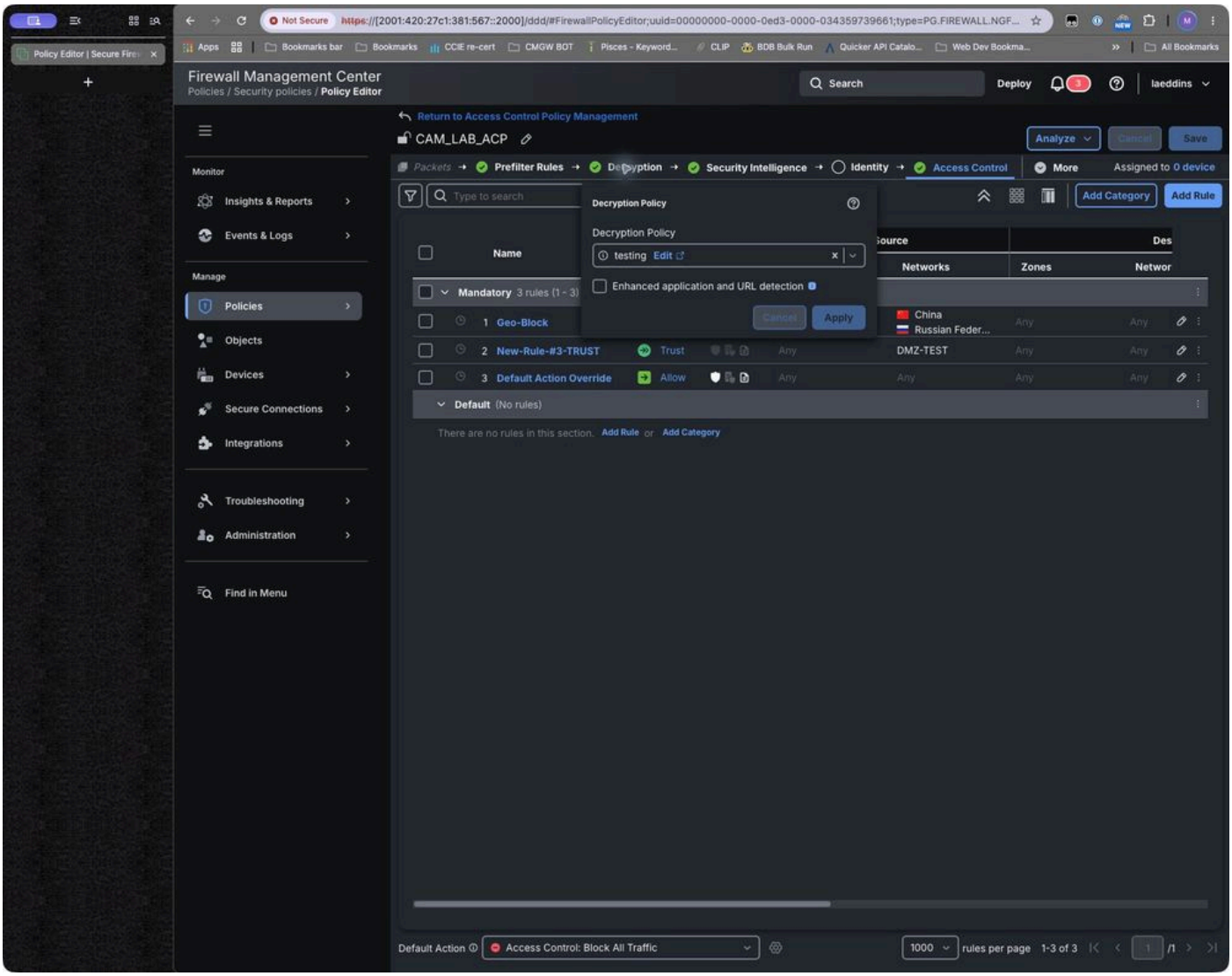


図 5b. 既存のCAM_LAB_ACPポリシーは、テスト用の復号化ポリシーを参照します。



導入と検証

対象のデバイスに変更を適用します。 可能であれば、問題のCAによって発行された証明書を使用しているWebサイトでテストします。

予期しない結果のトラブルシューティング

トラフィックが通過した場合は、展開ステータス、トラフィックの範囲、ポリシーの関連付け、ルールの順序、発行者のスペルとフィールドのエンコーディング、およびデバイスに証明書情報があるかどうかを確認します。別のルールまたはバイパスパスでフローが処理されたかどうかを確認します。同等のカバレッジを要求する前に、テスト済みリリースでTLS 1.3の可視性を確認します。

追加のTLS 1.3検証：FMC 7.6では、TLS 1.3復号化は個別の復号化ポリシーの詳細設定です。こ

の設定を無効にすると、復号化ルールはTLS 1.2以下にのみ適用されます。TLS 1.3の復号化を有効にすると、適応型のサーバIDプローブが有効になり、証明書がキャッシュされていない場合にIssuer DN条件によってプローブがトリガーされる可能性があります。関連付けられたアクセスコントロールポリシーのTLS 1.3 Server Identity Discovery設定が優先されます。シスコでは、これらの高度な設定は、7.1より前のデバイスまたはSnort 2を実行するデバイスでは無視され、AWSにデプロイされたFTDvでは適応型ID検出はサポートされていないと述べています。TLS 1.3カバレッジを要求する前に、対象のソフトウェア/プラットフォームと証明書の可視性を検証します。ルールのTLSバージョンセレクタ自体は、TLS 3.0からTLS 1.2までをリストします。TLS 1.3については、このセレクタに依存しません。 [7]

無関係なトラフィックが失敗した場合は、実際に一致するルールと発行者を特定します。必要に応じてDNまたはトラフィックの範囲を狭め、該当するテストと該当しないテストの両方を繰り返します。回避策として、証明書の検証を無効にしないでください。

カバレッジと運用上の制限

このソリューションは、すべてのシナリオをブロックしたり、他のサービスを更新する必要性を置き換えたりするものではありません。

ロールバックとルールの削除

ルールが許容できない影響を及ぼす場合は、通常の変更プロセスで新しいルールを無効にし、再展開します。イベントを保存し、証拠をテストします。廃止の前に、影響を受けるワークロードが現在の信頼ポリシーを適用していることを確認し、否定的な証明書検証テストを繰り返し、一時的な封じ込めを削除するための変更オーナーの承認を取得します。

参考資料

[1] FMC 7.2復号ルール

[2] FMC 10.xルールベースの復号ルール

[3]リリースごとのセキュアファイアウォール管理センターの新機能

[4] FMCおよびFDMのCAバンドルの自動更新の設定

[5] FMC 7.6証明書

[6] FDM 7.6証明書

[7] FMC 7.6復号ポリシーおよびTLS 1.3ガイダンス

[8] Cisco Secure Firewall ASA 9.22 General Operations CLIコンフィギュレーションガイド – デジタル証明書

[9] Cisco Secure Firewall ASAシリーズコマンドリファレンス – crypto ca trustpool policy

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。