Orientação para Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance - Desconfiança de emergência da raiz de Mudhra e autoridades de certificação intermediárias

Contents

Propósito

Veja a seguir as orientações sobre o Cisco Secure Firewall Threat Defense (FTD), o Cisco Secure Firewall Management Center (FMC) e o Adapative Security Appliance (ASA) para a desconfiança de emergência da raiz de Mudhra e das autoridades de certificação intermediárias.

Atualizações do pacote de certificados de serviço local da Cisco do FMC

O FMC e o FTD podem atualizar automaticamente um pacote de CA local usado para conexões TLS do dispositivo para os serviços da Cisco, incluindo Smart Licensing e atualizações de software, VDB, SRU e Geolocation. O sistema faz verificações diárias em um horário definido pelo sistema. Os documentos da Cisco apresentam disponibilidade iniciada com FMC/FTD 7.0.5, 7.1.0.3, 7.2.4 e 7.3.0+. Esses são limites de recursos, não destinos de atualização recomendados; selecione um destino de atualização usando a plataforma exata, a versão de origem, os requisitos de compatibilidade e as diretrizes de versão atuais da Cisco. [3, 4]

Em um FMC ou FTD CLI suportado, o comando `show cert-update` relata o status de atualização automática, a programação diária e a hora da última modificação do pacote. `configure cert-update test` verifica se o pacote local está atual e se a conectividade de atualização está pronta. [4, 5, 6]

Este pacote de serviços da Cisco é separado dos objetos/grupos de CA confiáveis configurados do FTD usados pela descriptografia SSL e dos pontos de confiança do dispositivo usados para certificados de identidade ou VPN. Você precisará verificar se nenhum desses certificados foi adicionado manualmente à configuração. [5, 6]

Importação automática do pool de confiança ASA CA

No ASA, o pool de confiança de CA e os pontos de confiança nomeados são recursos de gerenciamento de certificados separados. O conjunto confiável possui certificados CA; um ponto confiável é uma configuração nomeada usada para identidade de certificado e registro de CA. A importação automática do ASA trustpool também é separada da atualização do pacote de serviços Cisco FMC/FTD descrita acima. [8, 9]

Para uma verificação somente leitura, execute `show crypto ca trustpool policy` para revisar a contagem de certificados trustpool, o status e o resultado da importação, a próxima tentativa agendada e os detalhes efetivos da política. Execute `show run crypto ca trustpool policy` para examinar as linhas de política de pool confiável configuradas. A Cisco documenta a importação automática como desativada por padrão. Quando ativada sem substituições, a programação documentada é uma tentativa a cada 24 horas às 22:00 e o URL padrão da Cisco é usado; uma hora ou URL configurada pode alterar esses valores. Verifique a saída real do ASA em vez de pressupor que a importação automática está ativada ou usando a programação padrão. [8, 9]

Estes controlos mostram o estatuto de política e de importação; eles não fornecem um inventário certificado por certificado ou estabelecem que qualquer certificado Mudhra nomeado está instalado, removido ou não é confiável. Não inferir o comportamento do ASA a partir da `atualização de certificado do` FMC/FTD e não tratar o status do pool confiável como prova sobre certificados configurados em um determinado ponto confiável ou outro armazenamento confiável do aplicativo. Confirme a versão exata do ASA e o serviço dependente do certificado antes de decidir se é necessária alguma ação específica do produto. [8, 9]

Possível solução alternativa usando o FTD para proteger seus dispositivos sem patches

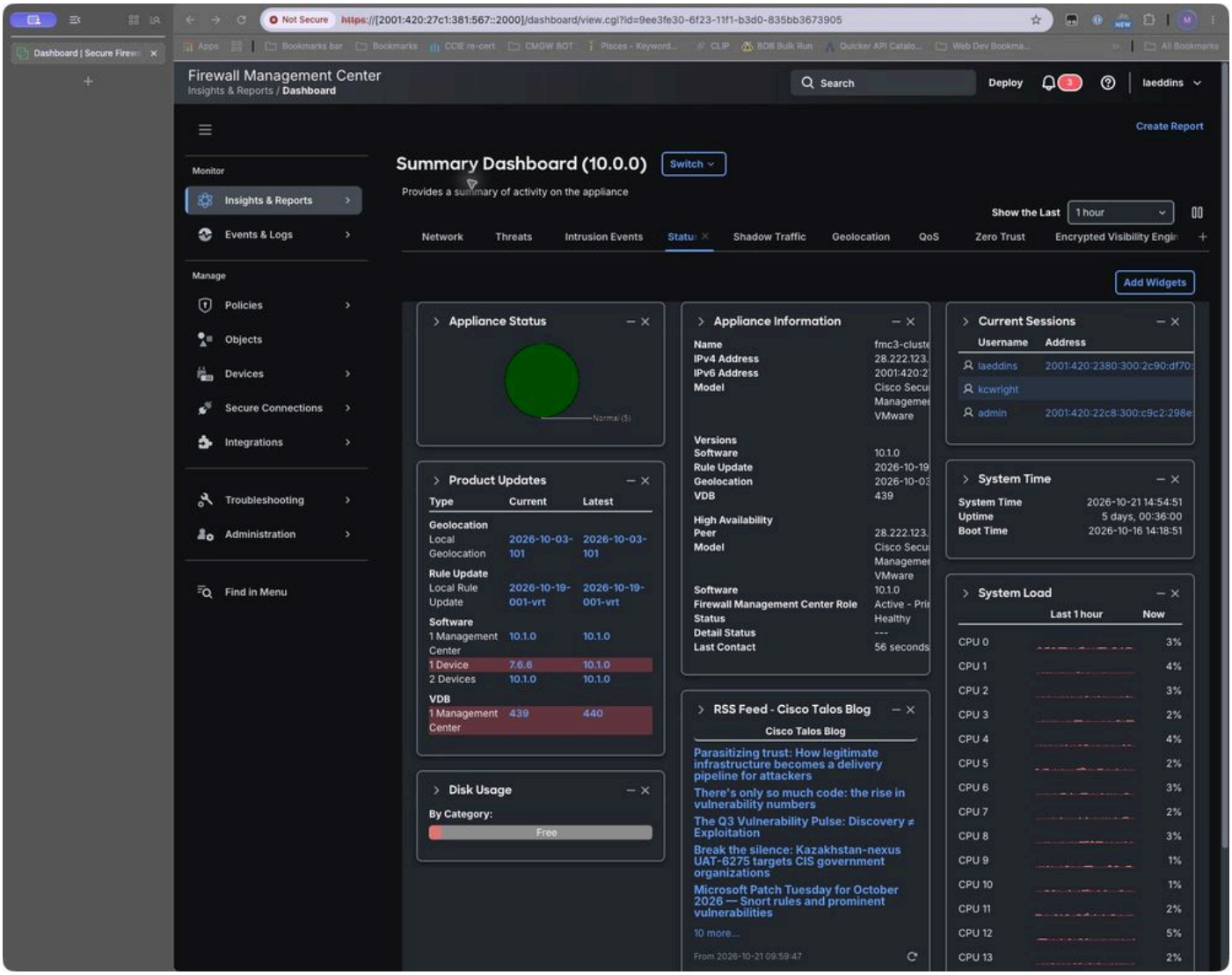
Propósito

Use o Cisco Secure Firewall Management Center (FMC) para configurar regras de política TLS que bloqueiam certificados de servidor com nomes de emissor Mudhra afetados. Esse controle pode reduzir a exposição de clientes e servidores sem cabeça cujos armazenamentos confiáveis de aplicativos ainda não receberam as atualizações necessárias, mas não bloqueia conexões em todos os cenários. Continuar a correção do repositório de confiança e a substituição do certificado. Não importe uma CA comprometida para CAs confiáveis para este procedimento.

Pré-requisitos

As telas de configuração neste artigo foram capturadas no FMC 10.1.0. O painel lista dois dispositivos gerenciados em 10.0.0 e um em 7.6.6. Nenhum teste de tráfego foi realizado. Antes da validação da imposição, registre a versão do FTD, o mecanismo Snort, o modo de imposição, a política de controle de acesso e a política TLS de destino. Confirme se o tráfego de saída afetado atinge a política desejada.

Figura 1. FMC 10.1.0 e inventário de software de dispositivo gerenciado.



Configurar correspondência do emissor

A Cisco documenta as condições de DN do emissor para corresponder à CA que emitiu o certificado do servidor. Adicione um objeto DN com Adicionar ao Emissor no editor de regras. A navegação e os rótulos disponíveis dependem da versão. [1, 2]

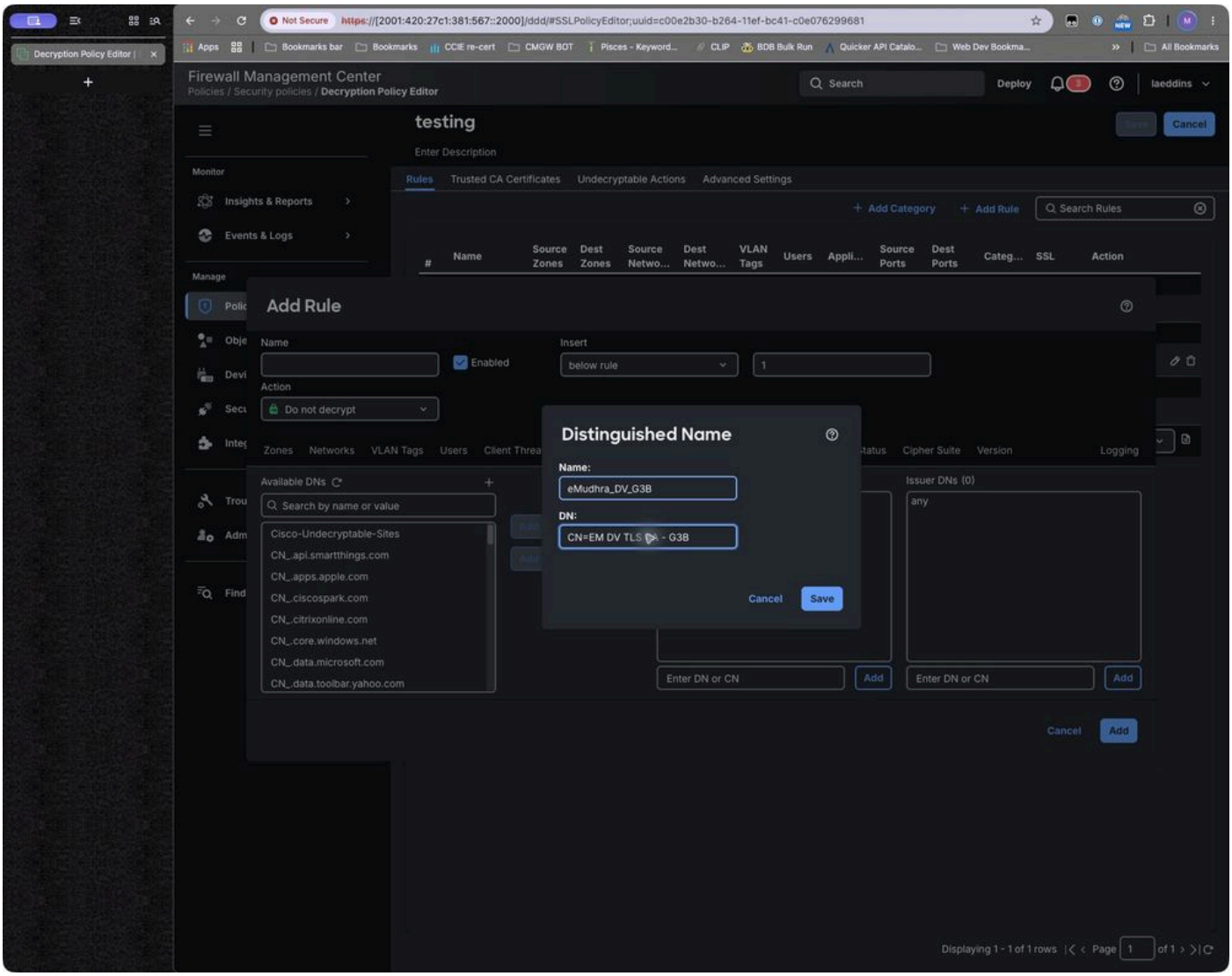
1 Criar os objetos

Tabela de Objetos

DN	Nome do objeto 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

Crie um objeto DN com escopo restrito para cada um na tabela acima.

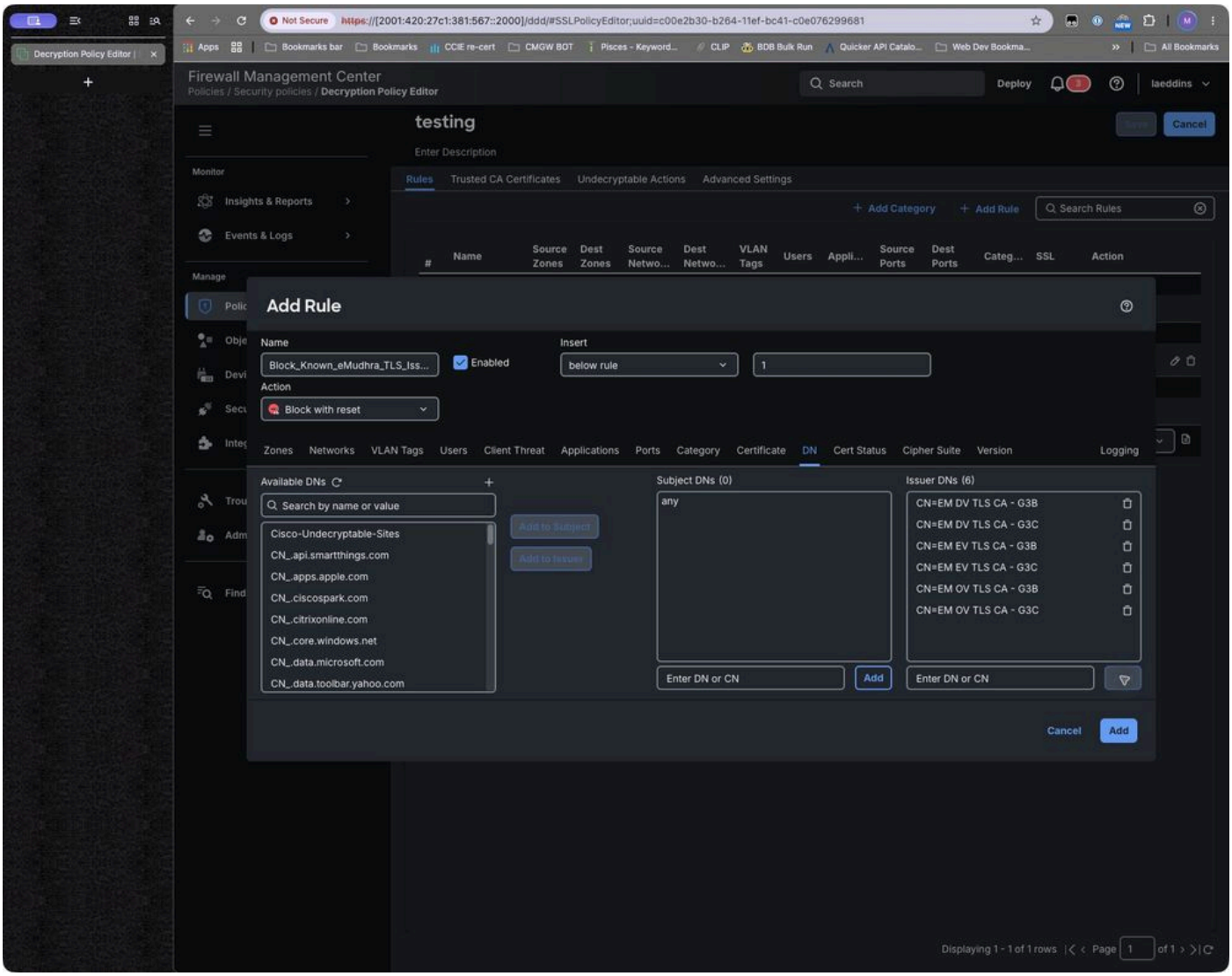
Figura 2. Formulário Nome Distinto mostrando os campos Nome e DN. O valor de exemplo foi inserido para ilustração; clique em Salvar quando terminar.



2 Criar a regra de bloqueio

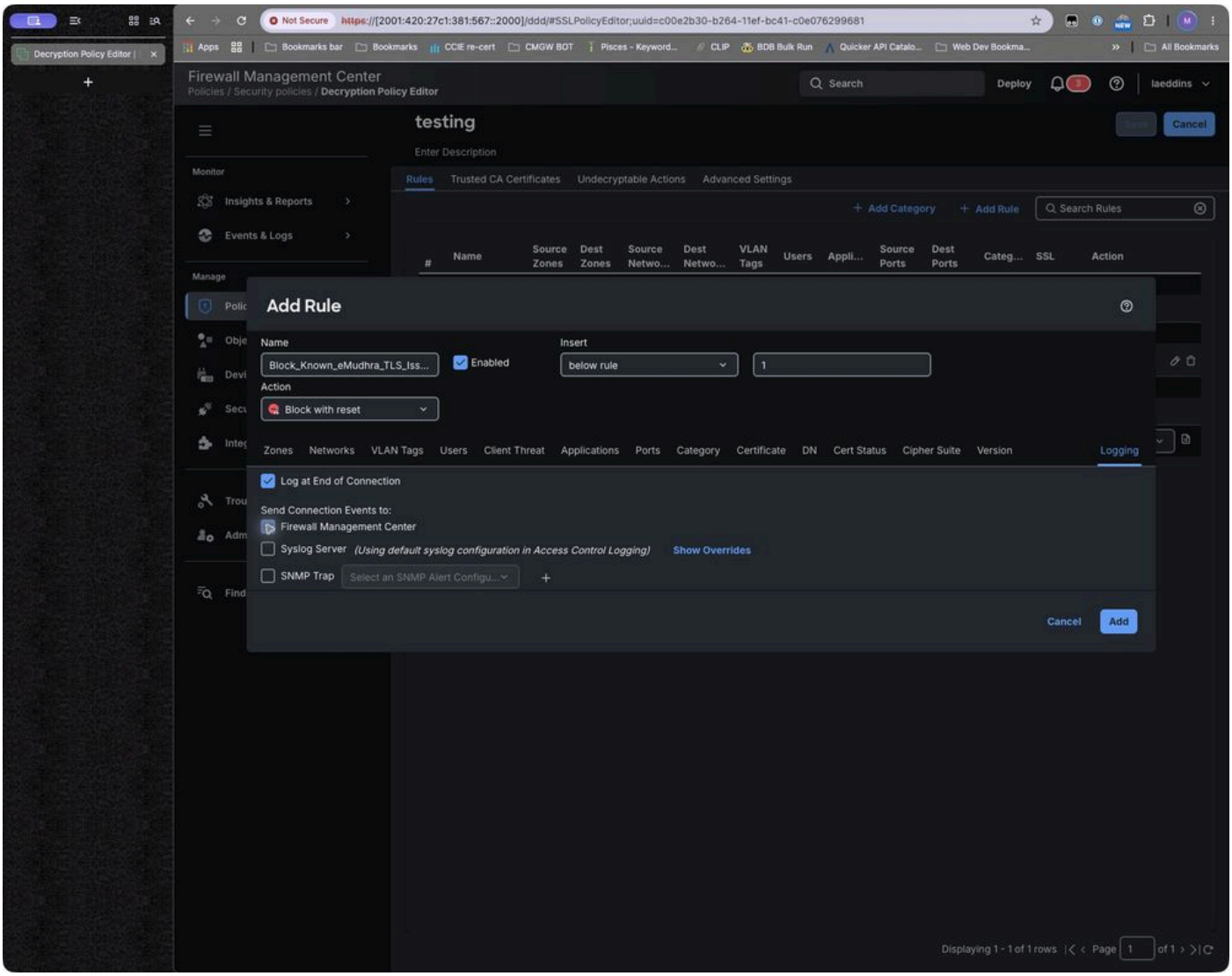
No FMC 10.1.0, selecione Policies > Security policies > Decryption, abra a política aplicável e clique em Add Rule. Nomeie a regra Block_Known_Mudhra_TLS_Issuers. Abra a guia DN. Adicione objetos verificados com Adicionar ao Emissor ou insira um DN no campo DNs do Emissor rotulado como Inserir DN ou CN e clique no botão Adicionar. Confirme se os nomes aparecem nos DNs do Emissor, não nos DNs do Assunto.

Figura 3. Regra mostrando Bloco com redefinição, a guia DN, seis DNs Emissores e nenhuma restrição de DN Assunto. Clique em Adicionar ao terminar.



Selecione Bloquear ou Bloquear com redefinição. Limite as zonas de origem ou redes ao escopo acordado. Se desejar, na guia Registro, selecione Registro no fim da conexão e verifique se Firewall Management Center está selecionado. Não adicione um requisito Válido = Sim: o bloco do emissor pretendido não deve depender da aprovação do certificado na validação de confiança.

Figura 4. Regra que mostra o Log no Fim da Conexão e o Centro de Gerenciamento de Firewall selecionado. Clique em Adicionar quando terminar



3 Revisar a ordem das regras e a associação das políticas

Coloque a regra à frente de regras mais amplas que poderiam lidar primeiro com o mesmo tráfego. Confirme a associação da política TLS com a política de controle de acesso atribuída aos dispositivos de destino. Revise o pré-filtro e outros caminhos de bypass antes do teste.

Figura 5. Tabela de regras de política de teste existente. Mostra apenas a interface de pedidos.

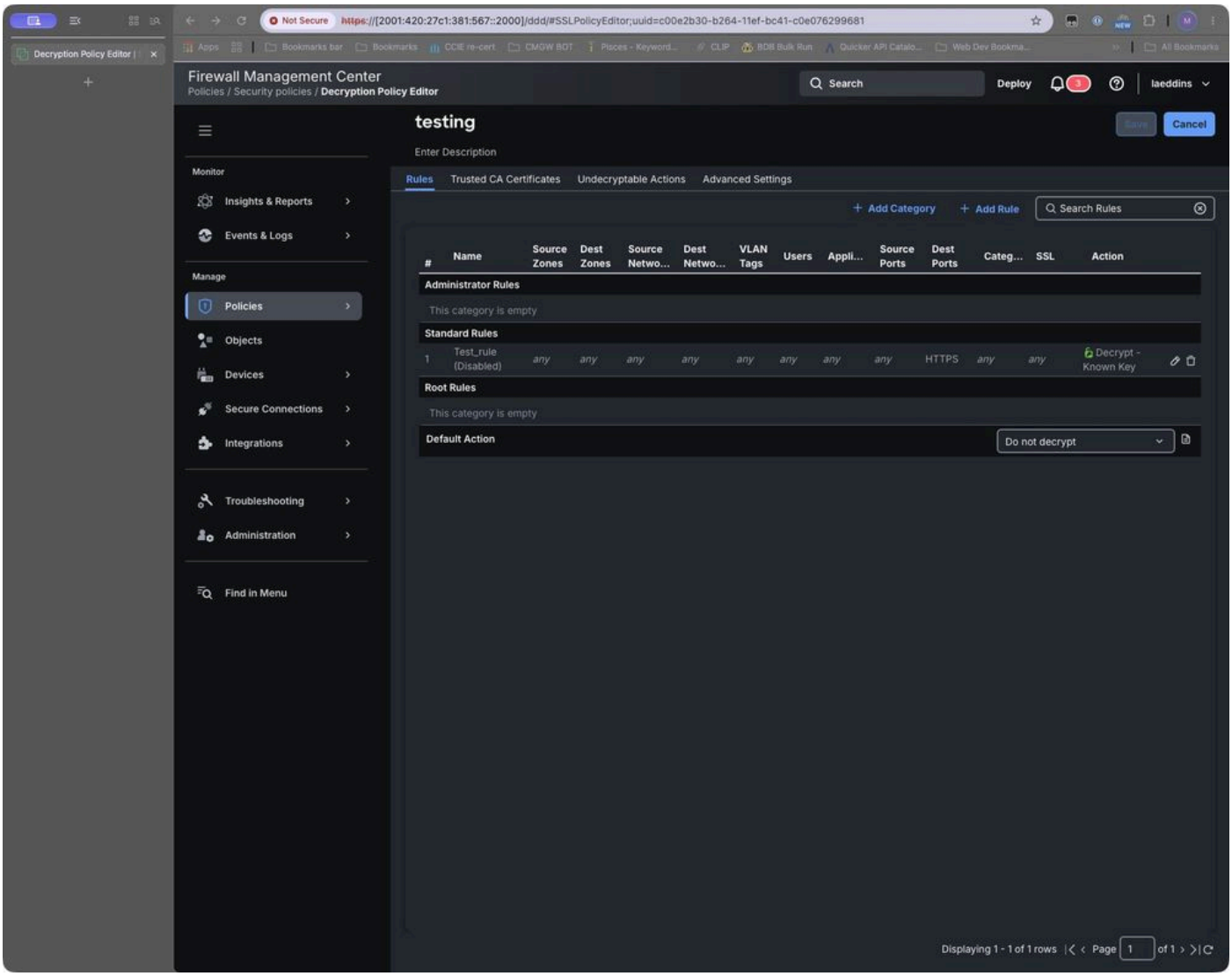
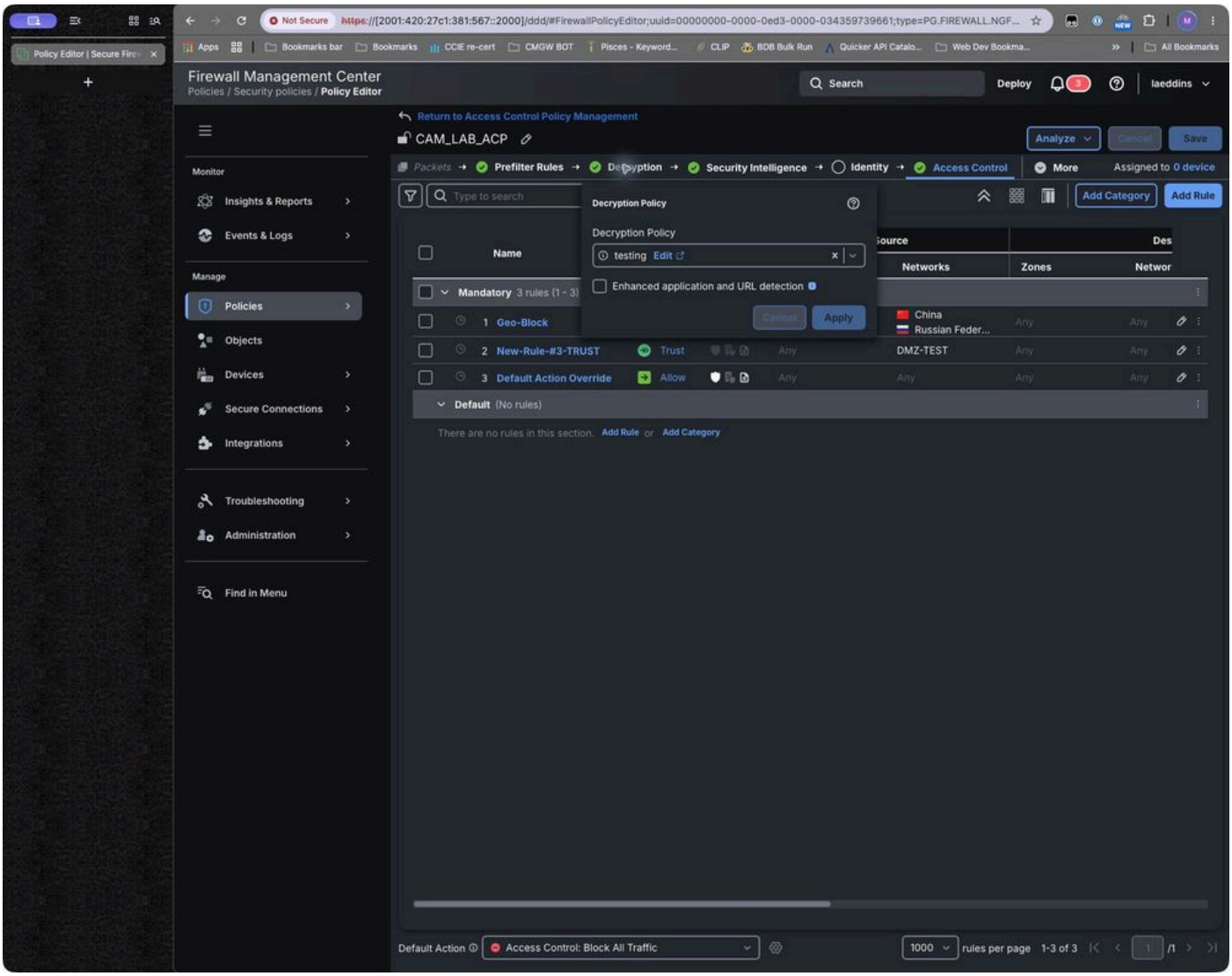


Figura 5b. A política CAM_LAB_ACP existente faz referência à política de descriptografia de teste.



Implantar e verificar

Implante as alterações nos dispositivos em questão. Se disponível, teste com um site que você sabe que está usando um certificado emitido por uma das CAs em questão.

Solucionar resultados inesperados

Se o tráfego passar, verifique o status da implantação, o escopo do tráfego, a associação da política, a ordem das regras, a ortografia do emissor e a codificação do campo, e se o dispositivo tinha informações de certificado. Determine se outra regra ou caminho de desvio manipulou o fluxo. Revise a visibilidade do TLS 1.3 na versão testada antes de solicitar cobertura equivalente.

Validação TLS 1.3 adicional: no FMC 7.6, a descriptografia TLS 1.3 é uma configuração avançada separada para a política de descriptografia; se estiver desabilitado, as regras de descriptografia

se aplicam somente ao TLS 1.2 ou inferior. Habilitar a descriptografia TLS 1.3 permite a sondagem adaptável de identidade do servidor, e uma condição de DN do Emissor pode disparar uma sonda quando o certificado não está em cache. A configuração de Descoberta de identidade do servidor TLS 1.3 da política de controle de acesso associada tem precedência. A Cisco diz que essas configurações avançadas são ignoradas em dispositivos anteriores à versão 7.1 ou que executam o Snort 2, e a descoberta de identidade adaptável não é suportada no FTDv implantado no AWS. Valide o software/plataforma de destino e a visibilidade do certificado antes de solicitar a cobertura TLS 1.3. O próprio seletor de Versão TLS da regra lista SSL 3.0 a TLS 1.2; não confiam nesse seletor para TLS 1.3. [7]

Se o tráfego não relacionado falhar, identifique a regra de correspondência real e o emissor. Restrinja o DN ou o escopo do tráfego conforme necessário e repita os testes afetados e não afetados. Não desabilite a validação do certificado como uma solução alternativa.

Cobertura e limites operacionais

Essa solução não bloqueia todos os cenários nem substitui a necessidade de atualizar outros serviços.

Reversão e descontinuação de regra

Se a regra causar um impacto inaceitável, desative a nova regra por meio do processo normal de alteração e reimplante. Preservar eventos e evidências de teste. Antes da desativação, confirme se as cargas de trabalho afetadas aplicam a diretiva de confiança atual, repita testes negativos de validação de certificado e obtenha a aprovação do proprietário da alteração para remover a contenção temporária.

Referências

[1] Regras de descriptografia do FMC 7.2

[2] Regras de descriptografia baseadas em regras do FMC 10.x

[3] Secure Firewall Management Center Novos recursos por versão

[4] Configure a atualização automática de pacotes CA para FMC e FDM

[5] Certificados FMC 7.6.

[6] Certificados FDM 7.6

[7] FMC 7.6 - Políticas de Descriptografia e orientações TLS 1.3.

[8] Cisco Secure Firewall ASA 9.22 General Operations CLI Configuration Guide — Certificados Digitais

[9] Referência de comandos do Cisco Secure Firewall ASA Series - política crypto ca trustpool

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.