Guía de Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance: desconfianza de emergencia de las autoridades de certificados raíz e intermedias de eMudhra

Contenido

Propósito

A continuación se incluye la guía sobre Cisco Secure Firewall Threat Defense (FTD), Cisco Secure Firewall Management Center (FMC) y Adapative Security Appliance (ASA) para la desconfianza de emergencia de las autoridades de certificados raíz e intermedios de eMudhra.

Actualizaciones del paquete de certificados de servicio local de Cisco FMC

FMC y FTD pueden actualizar automáticamente un paquete de CA local utilizado para las conexiones TLS del dispositivo a los servicios de Cisco, incluidas las actualizaciones de licencias inteligentes y software, VDB, SRU y geolocalización. El sistema realiza comprobaciones diarias a una hora definida por el sistema. La disponibilidad de las funciones de los documentos de Cisco comienza con FMC/FTD 7.0.5, 7.1.0.3, 7.2.4 y 7.3.0+. Éstos son umbrales de funciones, destinos de actualización no recomendados; seleccione un destino de actualización utilizando la plataforma exacta, la versión de origen, los requisitos de compatibilidad y la guía de la versión actual de Cisco. [3, 4]

En una CLI FMC o FTD compatible, `show cert-update` informa del estado de la actualización automática, la programación diaria y la hora de la última modificación del paquete. `configure cert-update test` verifica si el conjunto local está actualizado y si la conectividad de actualización está lista. [4, 5, 6]

Este paquete de servicios de Cisco es independiente de los grupos/objetos de CA de confianza configurados por FTD que se utilizan para el descifrado SSL y de los puntos de confianza de

dispositivos que se utilizan para los certificados de VPN o de identidad. Deberá comprobar que ninguno de estos certificados se ha agregado manualmente a la configuración. [5, 6]

Importación automática de conjunto de confianza de CA ASA

En ASA, el conjunto de confianza de CA y los puntos de confianza con nombre son características de administración de certificados independientes. El grupo de confianza contiene certificados de CA; un punto de confianza es una configuración con nombre que se utiliza para la identidad del certificado y la inscripción de CA. La importación automática del conjunto de confianza de ASA también es independiente de la actualización del paquete de servicios de Cisco FMC/FTD descrita anteriormente. [8, 9]

Para realizar una comprobación de sólo lectura, ejecute `show crypto ca trustpool policy` para revisar el recuento de certificados de trustpool, el estado y el resultado de la importación, el siguiente intento programado y los detalles de la política efectiva. Ejecute `show run crypto ca trustpool policy` para revisar las líneas de políticas de trustpool configuradas. La importación automática de documentos de Cisco está desactivada de forma predeterminada. Cuando se habilita sin reemplazos, la programación documentada es un intento cada 24 horas a las 22:00 y se utiliza la URL predeterminada de Cisco; una hora o URL configurada puede cambiar esos valores. Verifique el resultado real de ASA en lugar de asumir que la importación automática está habilitada o que utiliza la programación predeterminada. [8, 9]

Estas comprobaciones muestran la política y el estado de la importación; no proporcionan un inventario certificado por certificado ni establecen que cualquier certificado de eMudhra designado esté instalado, eliminado o desconfiado. No inferir el comportamiento de ASA de FMC/FTD `cert-update`, y no tratar el estado de trustpool como prueba sobre los certificados configurados bajo un punto de confianza determinado u otro almacén de confianza de la aplicación. Confirme la versión exacta de ASA y el servicio dependiente de certificados antes de decidir si es necesaria alguna acción específica del producto. [8, 9]

Posible solución alternativa mediante FTD para proteger los dispositivos sin parches

Propósito

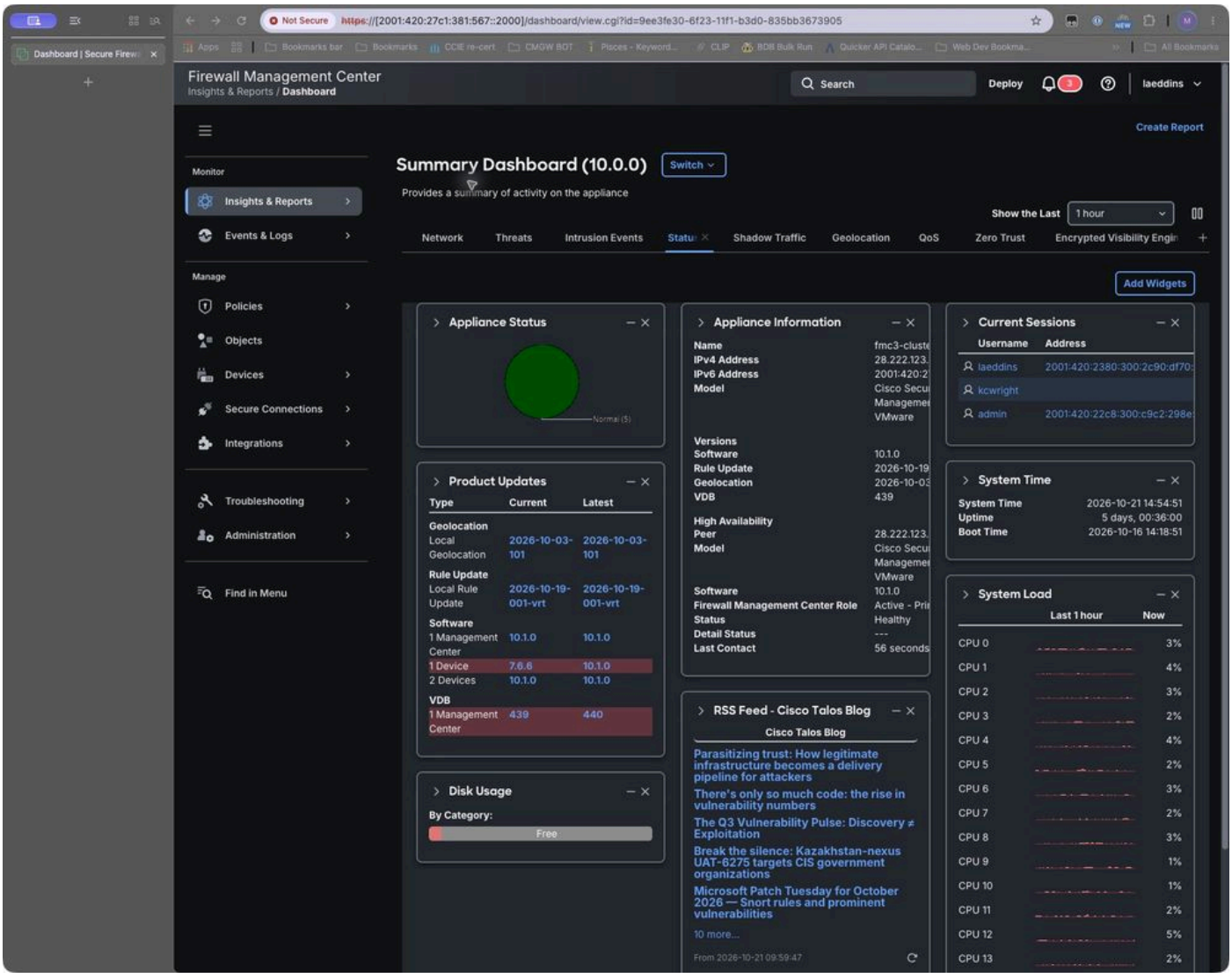
Utilice Cisco Secure Firewall Management Center (FMC) para configurar reglas de política TLS que bloqueen certificados de servidor con nombres de emisor de eMudhra afectados conocidos. Este control puede reducir la exposición de los clientes y servidores sin encabezado cuyos almacenes de confianza de aplicaciones aún no han recibido las actualizaciones necesarias, pero

no bloquea las conexiones en todos los escenarios. Continuar la corrección del almacén de confianza y la sustitución de certificados. No importe una entidad emisora de certificados comprometida en entidades emisoras de confianza para este procedimiento.

Prerequisites

Las pantallas de configuración de este artículo se capturaron en FMC 10.1.0. El panel muestra dos dispositivos administrados en 10.0.0 y uno en 7.6.6. No se realizó ninguna prueba de tráfico. Antes de la validación de la aplicación, registre la versión de FTD de destino, el motor de Snort, el modo de aplicación, la directiva de control de acceso y la directiva TLS. Confirme que el tráfico saliente afectado alcanza la política deseada.

Figura 1. FMC 10.1.0 e inventario de software de dispositivos gestionados.



Configurar coincidencia de emisor

Cisco documenta las condiciones del DN del emisor para hacer coincidir la CA que emitió el certificado del servidor. Agregue un objeto DN con Agregar al emisor en el editor de reglas. La navegación y las etiquetas disponibles dependen de la versión. [1, 2]

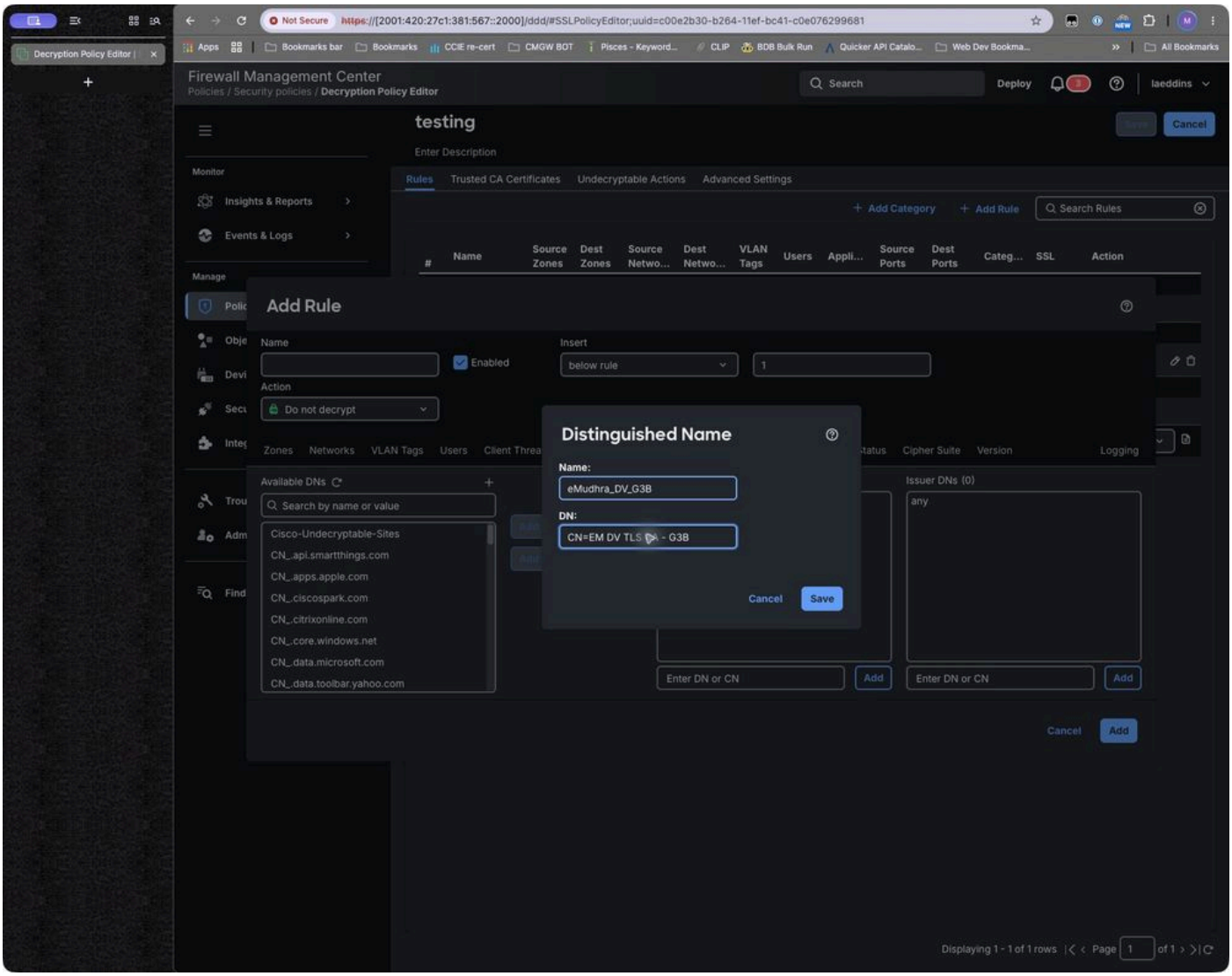
1 Crear los objetos

Tabla de objetos

DN	Nombre del objeto DN propuesto
CN=EM DV TLS CA - G3B	Mudhra_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	Mudhra_EV_G3C
CN=EM OV TLS CA - G3B	eMudhra_OV_G3B
CN=EM OV TLS CA - G3C	eMudhra_OV_G3C

Cree un objeto DN de ámbito estrecho para cada uno de los objetos de la tabla anterior.

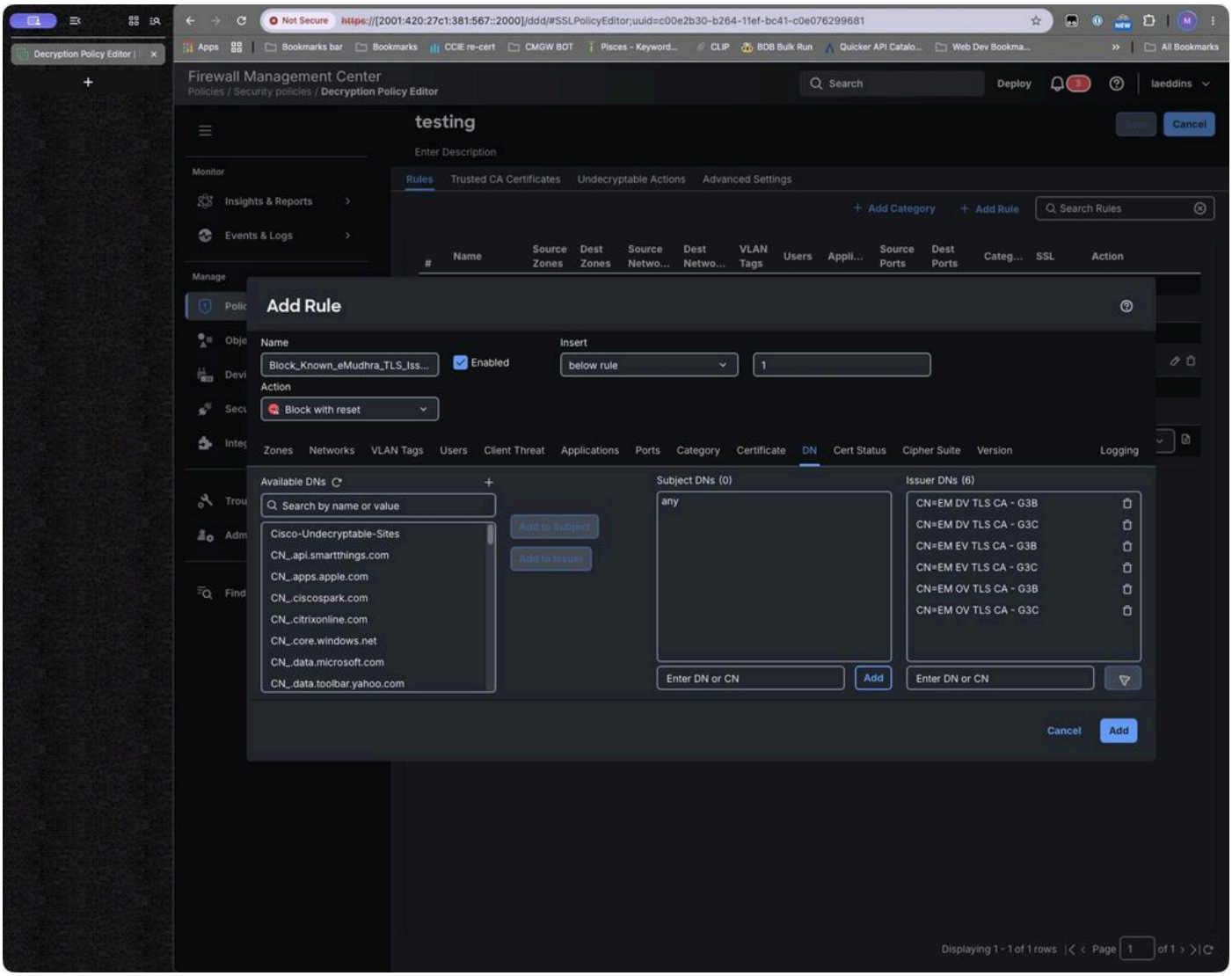
Figura 2. Formulario de nombre distinguido que muestra los campos Nombre y DN. El valor de ejemplo se ha introducido para la ilustración; haga clic en Guardar cuando termine.



2 Crear la regla de bloqueo

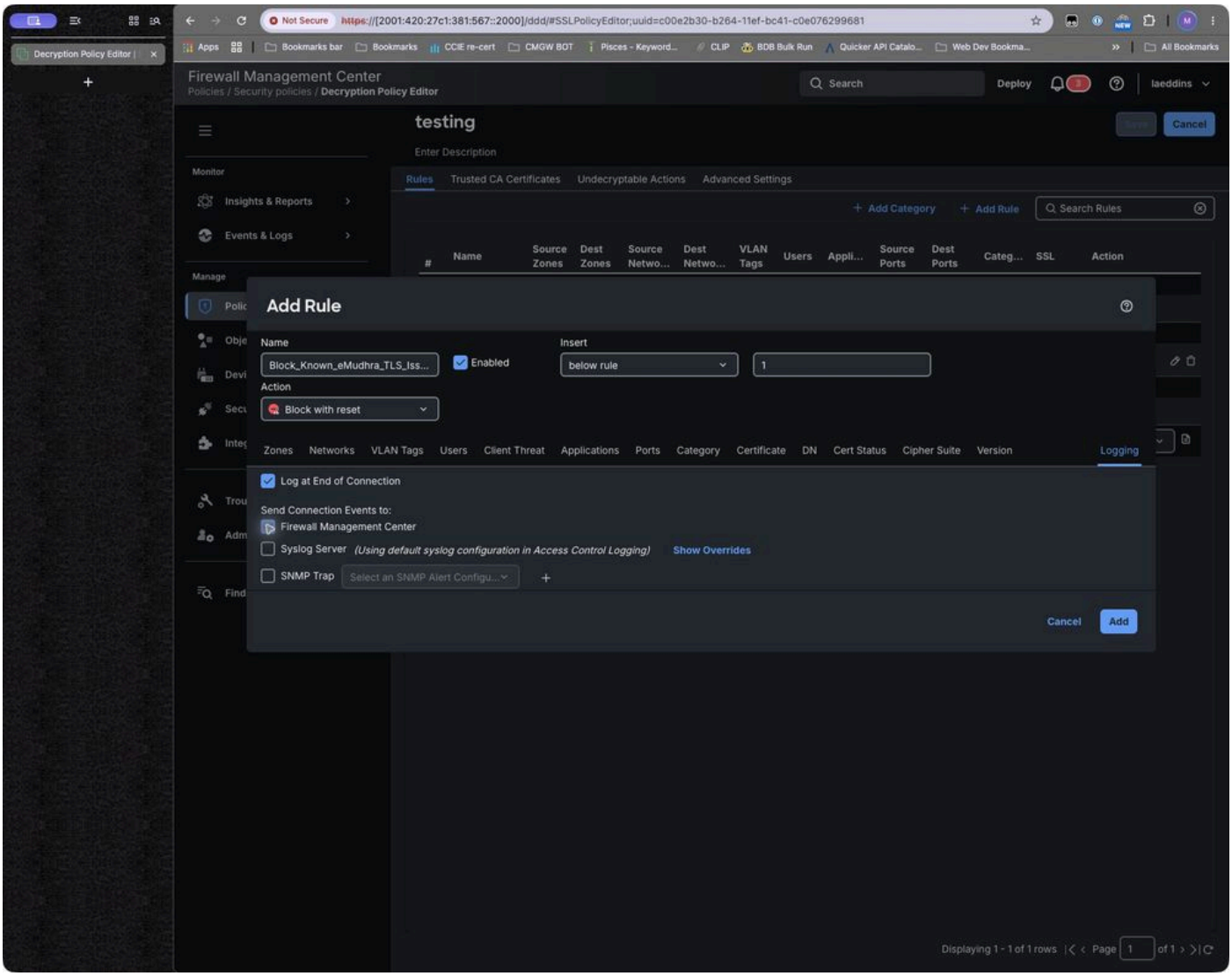
En FMC 10.1.0, seleccione Políticas > Políticas de seguridad > Descifrado, abra la política aplicable y haga clic en Agregar regla. Asigne a la regla el nombre Block_Known_Mudhra_TLS_Issuers. Abra la ficha DN. Agregue objetos verificados con Agregar al emisor o introduzca un DN en el campo DN del emisor con el nombre Introducir DN o CN y haga clic en el botón Agregar. Confirme que los nombres aparezcan en DN de emisor, no en DN de sujeto.

Figura 3. Regla que muestra Bloque con restablecimiento, la ficha DN, seis DN de emisor y ninguna restricción de DN de asunto. Haga clic en Agregar cuando haya terminado.



Seleccione Bloquear o Bloquear con restablecimiento. Limite las zonas o redes de origen al ámbito acordado. Si lo desea, en la ficha Registro, seleccione Registro al final de la conexión y compruebe que Firewall Management Center está seleccionado. No agregar un requisito Válido = Sí: el bloque de emisor previsto no debe depender de que el certificado pase la validación de confianza.

Figura 4. Regla que muestra Registro al final de la conexión y Centro de administración de firewall seleccionados. Haga clic en Agregar cuando termine



3 Revisar el orden de las reglas y la asociación de políticas

Sitúe la regla por delante de reglas más amplias que podrían gestionar el mismo tráfico en primer lugar. Confirme la asociación de la política TLS con la política de control de acceso asignada a los dispositivos de destino. Revise el prefiltro y otras rutas de desvío antes de realizar la prueba.

Figura 5. Tabla de reglas de políticas de prueba existentes. Muestra sólo la interfaz de pedidos.

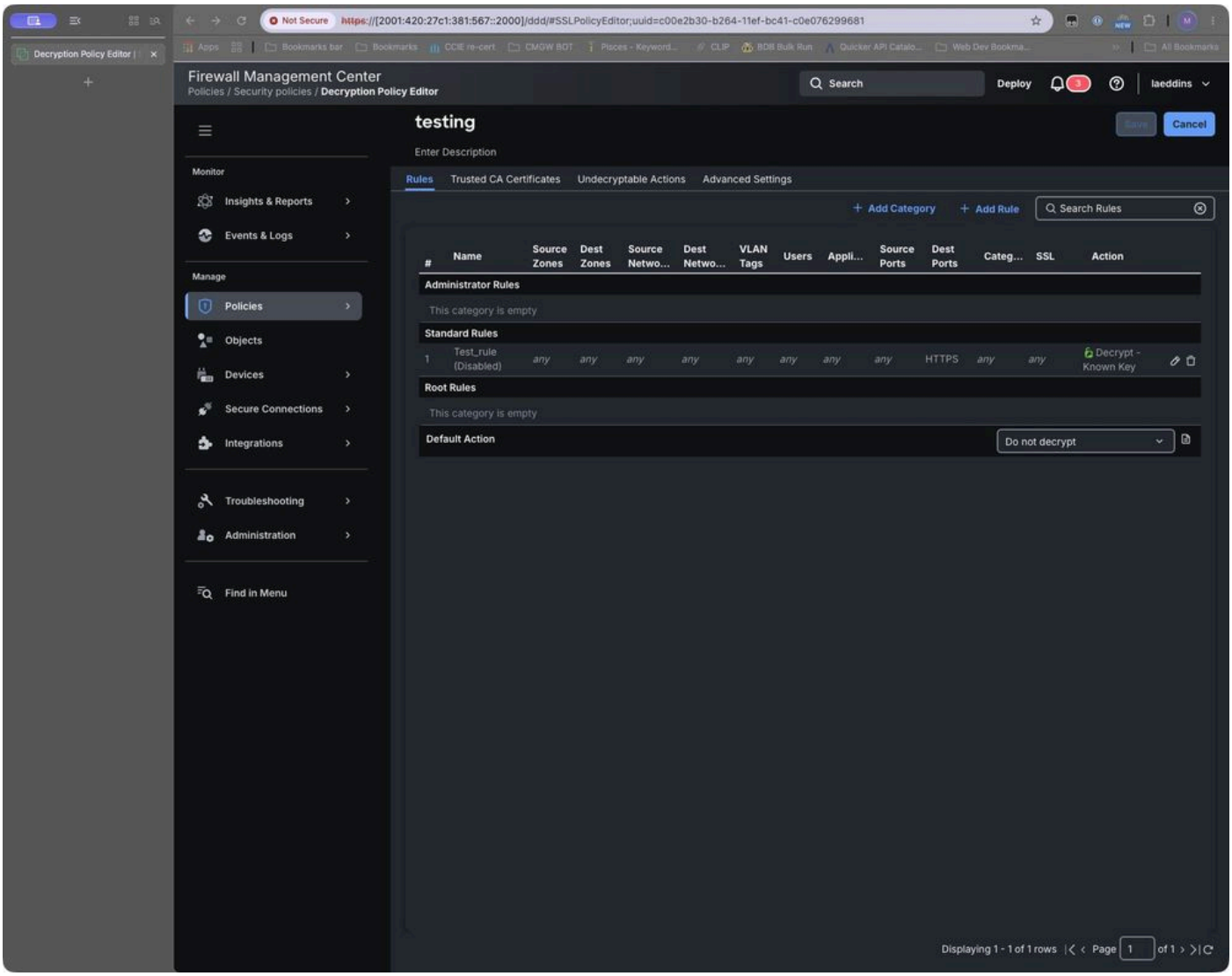
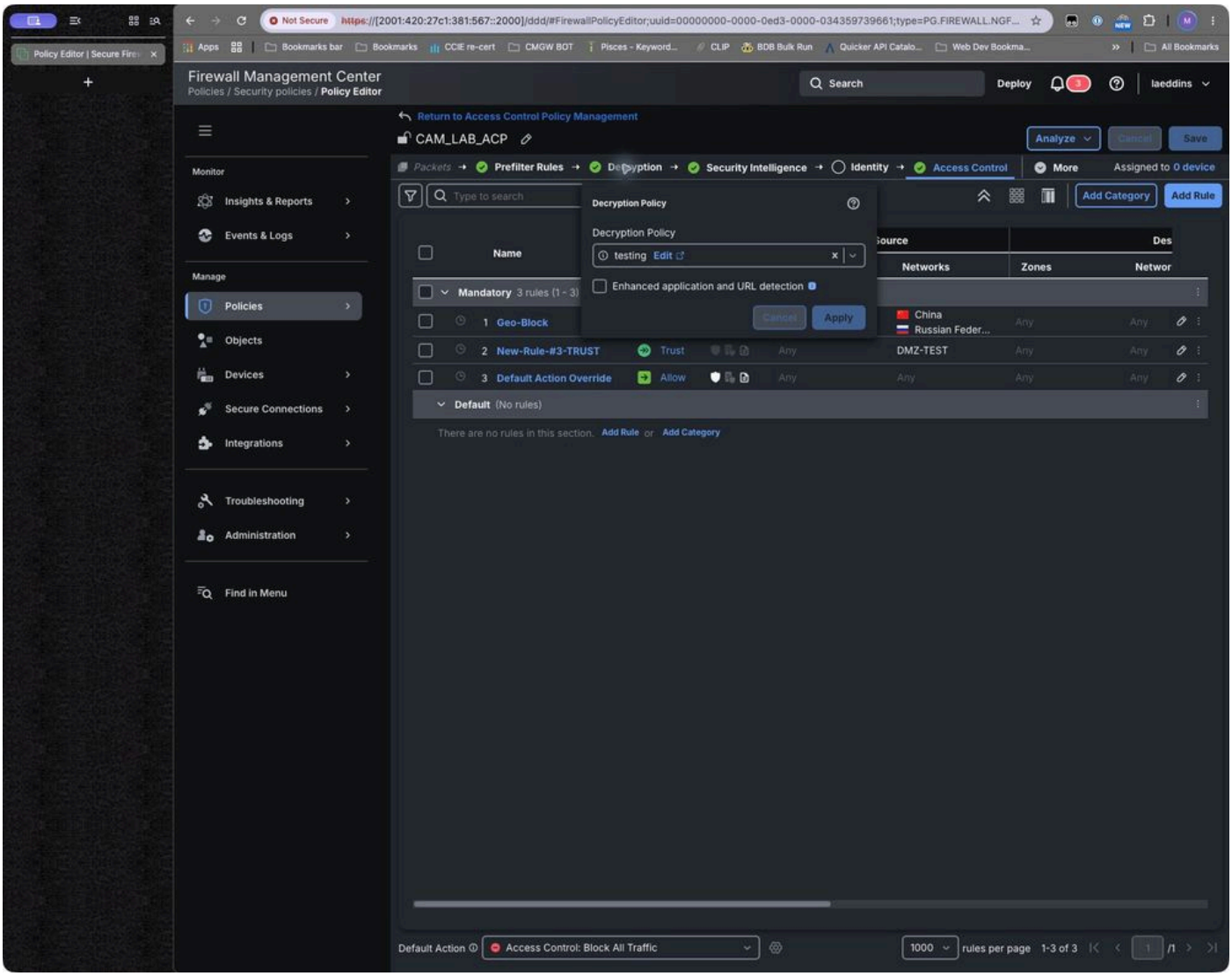


Figura 5b. La política CAM_LAB_ACP existente hace referencia a la política de descifrado de prueba.



Implementación y verificación

Implemente los cambios en los dispositivos en cuestión. Si está disponible, pruebe con un sitio web que sepa que está utilizando un certificado emitido por una de las CA en cuestión.

Solucionar resultados inesperados

Si pasa el tráfico, compruebe el estado de implementación, el ámbito del tráfico, la asociación de directivas, el orden de las reglas, la ortografía del emisor y la codificación de campos, así como si el dispositivo tenía información de certificados. Determine si otra regla o ruta de omisión controló el flujo. Revise la visibilidad de TLS 1.3 en la versión probada antes de solicitar una cobertura equivalente.

Validación adicional de TLS 1.3: en FMC 7.6, el descifrado de TLS 1.3 es una configuración

avanzada de política de descifrado independiente; si está inhabilitado, las reglas de descifrado se aplican sólo a TLS 1.2 o inferior. La activación del descifrado de TLS 1.3 habilita la sonda de identidad de servidor adaptable, y una condición de DN de emisor puede activar una sonda cuando el certificado no está almacenado en caché. La configuración de detección de identidad de servidor TLS 1.3 de la directiva de control de acceso asociada tiene prioridad. Cisco afirma que estas configuraciones avanzadas se ignoran en dispositivos anteriores a la versión 7.1 o que ejecutan Snort 2, y que la detección de identidad adaptativa no es compatible con FTDv implementado en AWS. Valide el software/plataforma de destino y la visibilidad de certificados antes de solicitar la cobertura de TLS 1.3. El selector de versión de TLS de la regla en sí muestra SSL 3.0 a TLS 1.2; no confíe en ese selector para TLS 1.3. [7]

Si falla el tráfico no relacionado, identifique la regla de coincidencia real y el emisor. Limite el DN o el ámbito de tráfico según sea necesario y, a continuación, repita las pruebas afectadas y no afectadas. No deshabilite la validación de certificados como solución alternativa.

Cobertura y límites operativos

Esta solución no bloquea todos los escenarios ni sustituye la necesidad de actualizar otros servicios.

Reversión y retirada de reglas

Si la regla provoca un impacto inaceptable, desactive la nueva regla mediante el proceso de cambio normal y vuelva a implementarla. Preservar eventos y pruebas de prueba. Antes de la retirada, confirme que las cargas de trabajo afectadas aplican la directiva de confianza actual, repita las pruebas negativas de validación de certificados y obtenga la aprobación del propietario del cambio para eliminar la contención temporal.

Referencias

[1] FMC 7.2 Reglas de descifrado

[2] Reglas de descifrado basadas en reglas FMC 10.x

[3] Nuevas funciones de Secure Firewall Management Center por versión

[4] Configuración de la actualización automática de los paquetes de CA para FMC y FDM

[5] Certificados FMC 7.6

[6] Certificados de FDM 7.6

[7] FMC 7.6 Políticas de descifrado y guía de TLS 1.3

[8] Guía de configuración de Cisco Secure Firewall ASA 9.22 General Operations CLI: certificados digitales

[9] Referencia de Comandos de la Serie ASA de Cisco Secure Firewall: política crypto ca trustpool

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).