Solucionar problemas de objetos FQDN con dominio base que no coincide con subdominios en políticas de control de acceso FTD

Contenido

Problema

Al configurar objetos de nombre de dominio completo (FQDN) en las directivas de control de acceso de Cisco Firewall Threat Defence (FTD), las entradas de dominio base no coinciden automáticamente con los subdominios. Por ejemplo, al crear una política que permite un objeto de destino configurado como "ejemplo.com", el subdominio "maps.ejemplo.com" se bloquea en lugar de permitirse a través de la misma regla de política. Este comportamiento plantea preguntas sobre si los dominios base pueden funcionar como comodines para todos los subdominios y cuál es el método de configuración adecuado para implementar la coincidencia de FQDN con comodines en las políticas de FTD.

Entorno

- FTD versión 7.2. Otras versiones también pueden verse afectadas.
- FMC versión 7.2. Otras versiones también pueden verse afectadas.
- Objetos FQDN configurados en directivas de control de acceso.

Resolución

- El comportamiento observado es la operación esperada de los objetos FQDN.
- En Cisco FMC, los objetos FQDN están diseñados para coincidir con los nombres de dominio exactos y no funcionan automáticamente como comodines para los subdominios.

- Para configurar correctamente la coincidencia de subdominios, se deben utilizar el filtrado de URL y las condiciones de URL en lugar de los objetos FQDN.

Configuración del Filtrado de URL para la Coincidencia de Subdominios

Para hacer coincidir un dominio y todos sus subdominios en FMC, siga estos pasos de configuración:

Paso 1. Acceda a Configuración de Reglas de Política de Control de Acceso

En el FMC, navegue hasta Políticas > Control de acceso > Política de control de acceso > [Su nombre de política] > Reglas.

Paso 2. Crear o editar regla de control de acceso

Cree una nueva regla o edite una regla de control de acceso existente en la que desee implementar la coincidencia de subdominios.

Paso 3. Configuración de las condiciones de URL

En la configuración de la regla, agregue condiciones de URL en lugar de utilizar objetos FQDN. Configure la condición de URL para incluir el dominio base con la sintaxis comodín adecuada para que coincida con los subdominios.

Paso 4. Aplicar política de filtrado de URL

Asegúrese de que el filtrado de URL esté habilitado y configurado correctamente dentro de la política de control de acceso para procesar las condiciones de URL de manera eficaz.

Paso 5. Implementación de la configuración

Implemente los cambios de configuración en los dispositivos FTD de destino para implementar la

funcionalidad de coincidencia de subdominios.

Métodos de configuración alternativos

Si el filtrado de URL no es adecuado para el caso práctico específico, considere la posibilidad de crear varios objetos FQDN para cada subdominio que deba coincidir explícitamente, o utilice objetos de red con intervalos de direcciones IP si los dominios se resuelven en espacios de direcciones IP predecibles.

Causa

Los objetos FQDN de Cisco FMC están diseñados para realizar la coincidencia exacta de nombres de dominio en lugar de la coincidencia de comodines. Este es el comportamiento esperado del sistema. La funcionalidad del objeto FQDN no incluye capacidades implícitas de coincidencia de subdominios, lo que requiere el uso de condiciones de filtrado de URL para lograr el comportamiento de coincidencia de subdominios deseado.

Contenido relacionado

- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214698-understand-fqdn-feature-on-firepower-thr.html
- https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/214505-configure-fqdn-based-object-for-access-c.html
- ID de bug de Cisco CSCwf000588
- Soporte técnico y descargas de Cisco

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).