Dépannage des objets FQDN avec domaine de base ne correspondant pas aux sous-domaines dans les politiques de contrôle d'accès FTD

Table des matières

Problème

Lors de la configuration d'objets FQDN (Fully Qualified Domain Name) dans les stratégies de contrôle d'accès Cisco Firewall Threat Defense (FTD), les entrées de domaine de base ne correspondent pas automatiquement aux sous-domaines. Par exemple, lors de la création d'une stratégie qui autorise un objet de destination configuré en tant que « exemple.com », le sous-domaine « maps.exemple.com » est bloqué au lieu d'être autorisé via la même règle de stratégie. Ce comportement pose la question de savoir si les domaines de base peuvent fonctionner comme caractères génériques pour tous les sous-domaines, et quelle est la méthode de configuration appropriée pour implémenter la correspondance de nom de domaine complet générique dans les stratégies FTD.

Environnement

- FTD version 7.2. D'autres versions peuvent également être affectées.
- FMC version 7.2. D’autres versions peuvent également être affectées.
- Objets FQDN configurés dans les stratégies de contrôle d'accès.

Résolution

- Le comportement observé correspond au fonctionnement attendu des objets FQDN.
- Dans Cisco FMC, les objets FQDN sont conçus pour correspondre à des noms de domaine

exacts et ne fonctionnent pas automatiquement comme des caractères génériques pour les sous-domaines.

- Pour configurer correctement la correspondance de sous-domaines, le filtrage d'URL et les conditions d'URL doivent être utilisés à la place des objets FQDN.

Configuration du filtrage URL pour la correspondance de sous-domaines

Pour faire correspondre un domaine et tous ses sous-domaines dans FMC, procédez comme suit :

Étape 1. Accédez à Access Control Policy Rule Configuration

Dans le FMC, accédez à Stratégies > Contrôle d'accès > Stratégie de contrôle d'accès > [Votre nom de stratégie] > Règles.

Étape 2. Créer ou modifier une règle de contrôle d’accès

Créez une nouvelle règle ou modifiez une règle de contrôle d'accès existante dans laquelle vous souhaitez mettre en oeuvre la correspondance de sous-domaines.

Étape 3 : configuration des conditions d’URL

Dans la configuration de la règle, ajoutez des conditions d'URL au lieu d'utiliser des objets FQDN. Configurez la condition d'URL pour inclure le domaine de base avec la syntaxe générique appropriée pour correspondre aux sous-domaines.

Étape 4. Application de la stratégie de filtrage des URL

Assurez-vous que le filtrage des URL est activé et correctement configuré dans la stratégie de contrôle d'accès pour traiter efficacement les conditions d'URL.

Étape 5 : déploiement de la configuration

Déployez les modifications de configuration sur les périphériques FTD cibles pour implémenter la fonctionnalité de correspondance de sous-domaine.

Autres méthodes de configuration

Si le filtrage d'URL ne convient pas à un cas d'utilisation spécifique, envisagez de créer plusieurs objets FQDN pour chaque sous-domaine qui doit être explicitement mis en correspondance, ou utilisez des objets réseau avec des plages d'adresses IP si les domaines se résolvent en espaces d'adresses IP prévisibles.

Motif

Les objets FQDN de Cisco FMC sont conçus pour effectuer une correspondance exacte des noms de domaine plutôt qu'une correspondance générique. Il s'agit du comportement souhaité du système. La fonctionnalité d'objet FQDN n'inclut pas de capacités de correspondance de sous-domaine implicites, ce qui nécessite l'utilisation de conditions de filtrage d'URL pour obtenir le comportement de correspondance de sous-domaine souhaité.

Autres informations utiles

- 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 bogue Cisco CSCwf000588
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.