Problemen met FQDN-objecten oplossen; met basisdomein dat niet overeenkomt met subdomeinen in FTD-toegangscontrolebeleid

Inhoud

uitgeven

Wanneer u FQDN-objecten (Fully Qualified Domain Name) configureert in het toegangsbeleid van Cisco Firewall Threat Defense (FTD), komen de basisdomeinvermeldingen niet automatisch overeen met subdomeinen. Wanneer u bijvoorbeeld een beleid maakt waarmee een bestemmingsobject kan worden geconfigureerd als "example.com", wordt het subdomein "maps.example.com" geblokkeerd in plaats van dat het via dezelfde beleidsregel wordt toegestaan. Dit gedrag roept vragen op over de vraag of basisdomeinen kunnen functioneren als jokertekens voor alle subdomeinen en wat de juiste configuratiemethode is voor het implementeren van wildcard FQDN-matching in FTD-beleid.

milieu

- FTD versie 7.2. Ook andere versies kunnen worden beïnvloed.
- FMC versie 7.2. Ook andere versies kunnen worden beïnvloed.
- FQDN-objecten geconfigureerd in toegangscontrolebeleid.

resolutie

- Het waargenomen gedrag is de verwachte werking van FQDN-objecten.
- In Cisco FMC zijn de FQDN-objecten ontworpen om exacte domeinnamen te matchen en functioneren ze niet automatisch als jokertekens voor subdomeinen.

- Om subdomein-matching goed te configureren, moeten URL-filtering en URL-voorwaarden worden gebruikt in plaats van FQDN-objecten.

URL-filtering configureren voor overeenkomende subdomeinen

Voer de volgende configuratiestappen uit om een domein en al zijn subdomeinen in FMC te matchen:

Stap 1. Navigeer naar Configuratie toegangscontrolebeleidsregel

Navigeer in de FMC naar Beleid > Toegangscontrole > Toegangscontrolebeleid > [Naam van beleid] > Regels.

Stap 2. Toegangsregel maken of bewerken

Maak een nieuwe regel aan of bewerk een bestaande regel voor toegangsbeheer waar u subdomein-matching wilt implementeren.

Stap 3. URL-voorwaarden configureren

Voeg in de regelconfiguratie URL-voorwaarden toe in plaats van FQDN-objecten te gebruiken. Configureer de URL-voorwaarde om het basisdomein op te nemen met de juiste jokersyntaxis die overeenkomt met subdomeinen.

Stap 4. URL-filterbeleid toepassen

Zorg ervoor dat URL-filtering is ingeschakeld en correct is geconfigureerd in het toegangscontrolebeleid om de URL-voorwaarden effectief te verwerken.

Stap 5. Configuratie implementeren

Implementeer de configuratiewijzigingen voor de beoogde FTD-apparaten om de functionaliteit

voor het matchen van subdomeinen te implementeren.

Alternatieve configuratiemethoden

Als URL-filtering niet geschikt is voor de specifieke use case, overweeg dan om meerdere FQDN-objecten te maken voor elk subdomein dat expliciet moet worden gekoppeld, of gebruik netwerkobjecten met IP-adresbereiken als de domeinen zich aanpassen aan voorspelbare IP-adresruimten.

Oorzaak

FQDN-objecten in Cisco FMC zijn ontworpen om exacte domeinnaammatching uit te voeren in plaats van jokermatching. Dit is het beoogde gedrag van het systeem. De FQDN-objectfunctionaliteit bevat geen impliciete subdomein-matchingmogelijkheden, waarvoor URL-filtervoorwaarden moeten worden gebruikt om het gewenste subdomein-matchinggedrag te bereiken.

Verwante inhoud

- 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
- Cisco bug ID CSCwf000588
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.