# Risolvere i problemi relativi agli oggetti FQDN con dominio di base non corrispondente ai sottodomini nei criteri di controllo di accesso FTD

## Sommario

## Problema

Quando si configurano oggetti FQDN (Fully Qualified Domain Name) nei criteri di controllo di accesso di Cisco Firewall Threat Defense (FTD), le voci del dominio di base non corrispondono automaticamente ai sottodomini. Ad esempio, quando si crea un criterio che consente un oggetto di destinazione configurato come "example.com", il sottodominio "maps.example.com" viene bloccato invece di essere consentito attraverso la stessa regola. Questo comportamento solleva dubbi sulla possibilità che i domini di base possano funzionare come caratteri jolly per tutti i sottodomini e sul metodo di configurazione appropriato per implementare la corrispondenza FQDN dei caratteri jolly nei criteri FTD.

## Ambiente

- FTD versione 7.2. Possono essere interessate anche altre versioni.
- FMC versione 7.2. Possono essere interessate anche altre versioni.
- Oggetti FQDN configurati nei criteri di controllo di accesso.

## Risoluzione

- Il comportamento osservato è il funzionamento previsto degli oggetti FQDN.
- In Cisco FMC gli oggetti FQDN sono progettati per corrispondere a nomi di dominio esatti e non funzionano automaticamente come caratteri jolly per i sottodomini.

- Per configurare correttamente la corrispondenza del sottodominio, è necessario utilizzare il filtro URL e le condizioni URL al posto degli oggetti FQDN.

## Configurazione del filtro URL per la corrispondenza del sottodominio

Per creare una corrispondenza tra un dominio e tutti i relativi sottodomini in FMC, eseguire la procedura di configurazione seguente:

Passaggio 1. Passare alla configurazione della regola dei criteri di controllo di accesso

Nel FMC, selezionare Policies > Access Control > Access Control Policy > [Your Policy Name] > Rules (Policy > Controllo di accesso > Policy di controllo di accesso > [Nome criterio] > Regole).

Passaggio 2. Creare o modificare la regola di controllo d'accesso

Creare una nuova regola o modificare una regola di controllo d'accesso esistente in cui si desidera implementare la corrispondenza del sottodominio.

Passaggio 3. Configurazione delle condizioni dell'URL

Nella configurazione della regola aggiungere condizioni URL anziché utilizzare oggetti FQDN. Configurare la condizione dell'URL in modo da includere il dominio di base con la sintassi dei caratteri jolly appropriata per la corrispondenza dei sottodomini.

Passaggio 4. Applicazione dei criteri di filtro URL

Verificare che il filtro URL sia abilitato e configurato correttamente nei criteri di controllo di accesso per elaborare le condizioni dell'URL in modo efficace.

Passaggio 5. Distribuire la configurazione

Distribuire le modifiche di configurazione ai dispositivi FTD di destinazione per implementare la

funzionalità di corrispondenza del sottodominio.

### Metodi di configurazione alternativi

Se il filtro URL non è adatto allo scenario di utilizzo specifico, è consigliabile creare più oggetti FQDN per ogni sottodominio a cui deve corrispondere in modo esplicito oppure utilizzare oggetti di rete con intervalli di indirizzi IP se i domini si risolvono in spazi di indirizzi IP prevedibili.

## Causa

Gli oggetti FQDN in Cisco FMC sono progettati per eseguire la corrispondenza esatta dei nomi di dominio anziché dei caratteri jolly. Questo è il comportamento previsto del sistema. La funzionalità dell'oggetto FQDN non include funzionalità di corrispondenza implicita tra sottodomini, che richiedono l'utilizzo di condizioni di filtro URL per ottenere il comportamento di corrispondenza desiderato per i sottodomini.

## Contenuto correlato

- 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 bug Cisco CSCwf00588
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).