

# Pagine di blocco incoerenti dopo la migrazione da Umbrella a Cisco Secure Access

## Sommario

---

---

## Problema

Dopo la migrazione da Umbrella a Cisco Secure Access (SSE) utilizzando lo strumento di migrazione, il traffico Web bloccato viene reindirizzato in modo incoerente alla pagina di blocco Umbrella legacy anziché alla pagina di blocco Cisco Secure Access. Il problema si verifica con la difesa DNS quando domini diversi attivano regole di blocco, determinando pagine di avvio e parole relative al motivo del blocco diverse. In questo modo vengono create notifiche incoerenti di blocco degli utenti finali nell'intera organizzazione.

I sintomi specifici osservati includono:

- Le regole di blocco reindirizzano gli utenti alla vecchia pagina di blocco Umbrella anziché alla nuova pagina di blocco Cisco Secure Access
- Domini diversi che attivano le regole di blocco visualizzano pagine iniziali diverse
- Presentazione agli utenti finali di una formulazione incoerente per il motivo del blocco
- Il comportamento influisce sulla funzionalità di difesa DNS dopo la migrazione

## Ambiente

- Tecnologia: SSE (Cisco Secure Access)
- Migrazione: Umbrella a SSE utilizzando lo strumento di migrazione
- Tipo di servizio: Difesa DNS
- Implementazione: Ambiente post-migrazione
- Scansione Web: Dispositivi FTD con scansione Web abilitata

# Risoluzione

La scansione Web sui dispositivi FTD interferisce con il rendering corretto delle pagine iniziali personalizzate per Cisco Secure Access. Per risolvere il problema, ignorare la scansione Web sugli FTD per i seguenti tre domini:

- `opendns.com`
- `cisco-secure.com`
- `sse.cisco.com`

Questa soluzione consente di eseguire correttamente il rendering delle pagine iniziali personalizzate di Cisco Secure Access anziché visualizzare le pagine precedenti che bloccano Umbrella.

## Fasi di verifica

Per verificare l'efficacia della risoluzione:

Passaggio 1: Esegui test dei criteri per i domini che in precedenza mostravano un comportamento incoerente

Passaggio 2: Verificare il comportamento della pagina di blocco dopo l'implementazione della soluzione alternativa

Confermare che il traffico bloccato ora visualizzi in modo coerente la pagina di blocco di Cisco Secure Access anziché la pagina Umbrella legacy.

Passaggio 3: Convalida la formulazione coerente del motivo del blocco

Verificare che tutti i domini bloccati visualizzino ora un motivo di blocco uniforme allineato agli standard Cisco Secure Access.

## Causa

Il problema è causato dalla funzionalità di scansione Web sui dispositivi FTD che interferisce con il rendering corretto delle pagine iniziali personalizzate di Cisco Secure Access. Quando la scansione Web è abilitata sui FTD, impedisce la corretta visualizzazione delle nuove pagine bloccanti, causando il fallback del sistema alle pagine di blocco Umbrella legacy. In questo modo si creano situazioni incoerenti in cui domini diversi possono attivare formati di pagina di blocco diversi.

Il team di progettazione ha identificato questo problema come un problema a livello di progettazione che richiede modifiche dal punto di vista di Talos. L'architettura corrente richiede che venga ignorata la scansione Web per domini Cisco specifici per garantire la corretta funzionalità della pagina di destinazione personalizzata.

## Contenuto correlato

- [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).