セキュアアクセスで「Continue」をクリックした後のSWG Warnページ404エラー

内容

お問い合わせ内容

Secure Web Gateway(SWG)の警告ページで「Continue」をクリックした後、意図したとおりに許可されずに断続的に404エラーが発生する。この問題は、SWG警告ページがトリガーされたときに通常のポリシーフローで発生し、ユーザのWebアクセスに影響を与えます。この問題は、ユーザが目的のポリシー実装を介してSWG警告ページにアクセスした場合に発生しますが、「Continue」をクリックすると、ユーザは目的の宛先に進まずに404個のエラーを受信します。

環境

- テクノロジー：ソリューションサポート（SSPT – 契約が必要）
- サブテクノロジー：セキュアなアクセス
- 製品ファミリ：SECACCS
- 影響を受けるドメイン：block.sse.cisco.com

解決策

この問題は、CCO(Cisco Connection Online)で入手可能なCSCバージョン5.1.16で解決されています。 この問題の解決には、影響を受けるドメインのDNS処理と応答処理の変更が含まれていました。

解決手順

ステップ1:CSC 5.1.16へのアップグレード

CCOからCSCバージョン5.1.16をダウンロードしてインストールします。このバージョンには、DNSレコード処理問題の修正が含まれています。

手順2: DNS応答の変更を確認する

block.sse.cisco.comのDNS AAAA応答が、マッピングされたIPを使用しないように変更されたため、問題の根本原因が排除されました。

ステップ3:SWG警告ページ機能をテストする

ユーザが404エラーが発生せずにSWG警告ページの「Continue」を正常にクリックできることを確認します。

データ収集のトラブルシューティング

問題が解決しない場合、または診断目的の場合は、次のログを収集します。
https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

- 最大デバッグが有効なDARTログ
- ネットワークパケットキャプチャ(pcap)
- KDFログ
- ブラウザセッションからのHAR（HTTPアーカイブ）ファイル

原因

この問題は、ランダム化されたTTL（存続可能時間）値を持つ重複したDNSレコードによって上書きされた、内部DNSキャッシュ内のblock.sse.cisco.comのDNSレコードが原因で発生しました。 このDNSの破損により、SWGの警告ページリダイレクトメカニズムが失敗し、ユーザが警告ページを続行しようとしたときに404エラーが発生しました。DNS処理の不整合により、警告ページ機能に使用されるドメインが適切に解決されませんでした。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。