Blocage incohérent des pages après la migration d'Umbrella vers Cisco Secure Access

Table des matières

Problème

Après la migration d'Umbrella vers Cisco Secure Access (SSE) à l'aide de l'outil de migration, le trafic Web bloqué est redirigé de manière incohérente vers la page de blocage Umbrella héritée au lieu de la page de blocage Cisco Secure Access. Le problème se produit avec la défense DNS lorsque différents domaines déclenchent des règles de blocage, ce qui entraîne des pages d'accueil et des libellés de raison de blocage différents. Cela crée des notifications de blocage d'utilisateur final incohérentes dans toute l'entreprise.

Les symptômes spécifiques observés sont les suivants :

- Les règles de blocage redirigent les utilisateurs vers l'ancienne page de blocage Umbrella au lieu de la nouvelle page de blocage Cisco Secure Access
- Différents domaines déclenchant des règles de blocage affichent différentes pages de démarrage
- Motif de blocage incohérent présenté aux utilisateurs finaux
- Le comportement affecte la fonctionnalité de défense DNS après la migration

Environnement

- Technologie : Accès sécurisé Cisco (SSE)
- Migration : Parapluie vers SSE via l'outil de migration
- Type de service : Défense DNS
- Déploiement: Environnement post-migration
- Analyse Web : Périphériques FTD avec analyse Web activée

Résolution

L'analyse Web sur les périphériques FTD interfère avec le rendu correct des pages de renvoi personnalisées pour Cisco Secure Access. Pour résoudre ce problème, ignorez l'analyse Web sur les FTD pour les trois domaines suivants :

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

Cette solution de contournement permet aux pages de renvoi Cisco Secure Access personnalisées de s'afficher correctement au lieu d'afficher les anciennes pages de blocage Umbrella.

Étapes de vérification

Pour vérifier l'efficacité de la résolution :

Étape 1: Exécuter des tests de stratégie pour les domaines qui présentaient auparavant un comportement incohérent

Étape 2: Vérifier le comportement de la page de blocage après implémentation de la solution

Vérifiez que le trafic bloqué affiche désormais systématiquement la page de blocage de l'accès sécurisé Cisco au lieu de la page Umbrella héritée.

Étape 3: Valider la formulation cohérente du motif de bloc

Assurez-vous que tous les domaines bloqués affichent désormais un message de raison de blocage uniforme et conforme aux normes d'accès sécurisé Cisco.

Motif

Le problème est causé par la fonctionnalité d'analyse Web sur les périphériques FTD qui interfère avec le rendu correct des pages de renvoi personnalisées de Cisco Secure Access. Lorsque l'analyse Web est activée sur les FTD, elle empêche l'affichage correct des nouvelles pages de blocage, ce qui entraîne le retour du système aux anciennes pages de blocage Umbrella. Cela crée des expériences utilisateur incohérentes où différents domaines peuvent déclencher différents formats de page de blocage.

L'équipe d'ingénierie a identifié ce problème comme un problème de conception qui nécessite des modifications du point de vue de Talos. L'architecture actuelle nécessite le contournement de l'analyse Web pour des domaines Cisco spécifiques afin de garantir une fonctionnalité de page de renvoi personnalisée appropriée.

Autres informations utiles

- 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.