Utiliser les informations de diagnostic de la page Umbrella Block pour le dépannage

Table des matières

Introduction

Bloquer les informations de diagnostic

- Exemple de page de bloc

Définitions

- ACType
- Type de bloc
- ID d'offre
- Étiquetage de domaine
- Hôte
- Adresse IP
- ID organisation
- ID origine
- Préfs
- Requête
- Serveur
- Heure

Introduction

Ce document décrit comment accéder aux informations de diagnostic de page de bloc et les interpréter pour le test de configuration et le dépannage.

Bloquer les informations de diagnostic

Lorsque vous atteignez une page de blocage, vous pouvez développer la section des informations de diagnostic au bas de la page pour obtenir des détails supplémentaires. Utilisez ces informations pour tester votre configuration. L'assistance peut demander une capture d'écran de cette section.

Exemple de page de bloc

La capture d'écran fournie montre un exemple de page de blocage avec des informations de diagnostic développées :

Cisco Umbrella

This site is blocked due to a phishing threat.

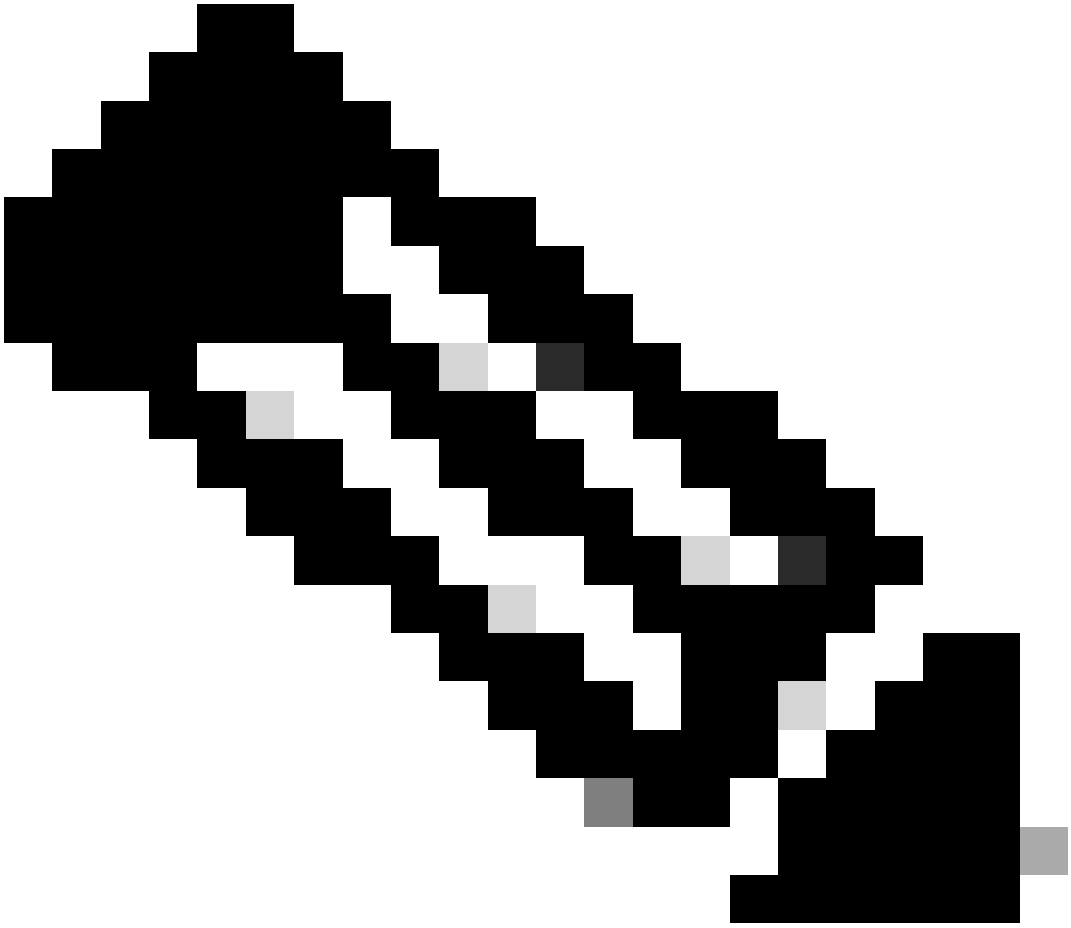
internetbadguys.com

Diagnostic Info

ACType: 0
Block Type: phish
Bundle ID: 1
Domain Tagging: -
Host: phish.opendns.com
IP Address:
Org ID:
Origin ID:
Prefs: -
Query: url=internetbadguys.com&server=ash24&prefs=&tagging=&nr
Server: ash24
Time: 2018-07-12 01:12:29.180338193 +0000 UTC
m=+3221152.293186035

Terms | Privacy Policy | Contact

diagnostic-info.png



Remarque : Pour plus d'informations sur le dépannage de la configuration des stratégies, consultez l'article Comment déterminer quelle stratégie est appliquée dans Ma configuration de parapluie.

Définitions

ACType

- ACType n'est utile que pour l'assistance.

Type de bloc

- Type de bloc indique la catégorie du bloc et la raison de la restriction de page. Les types incluent :
  - aup : Catégorie de contenu

    - domain list : Liste de destinations
    - sécurité: DNS dynamique, commande et contrôle, programmes malveillants, accès non autorisé au tunnel IP, nouveaux domaines, potentiellement dangereux, VPN de tunnellisation DNS, flux tiers (par exemple, AMP, ThreatGrid)
    - hameçonnage : Hameçonnage
    - dlink-phish : Hameçonnage via le DNS avancé D-Link

ID d'offre

- L'ID d'ensemble est l'identificateur de la stratégie appliquée.

Étiquetage de domaine

- L'étiquetage de domaine est utile uniquement pour la prise en charge.

Hôte

- L'hôte fait référence à la page de renvoi. Les valeurs possibles sont les suivantes :
    - block.opendns.com: aup, liste de domaines
    - malware.opendns.com: sécurité
    - phish.opendns.com: phish
    - www1.dlinksearch.com: dlink-phish
    - bpb.opendns.com: Bloquer le contournement de page

Adresse IP

- Adresse IP est l'adresse IP publique de l'ordinateur.

ID organisation

- L'ID d'organisation est l'ID d'organisation du réseau utilisé par l'ordinateur.

ID origine

- L'ID d'origine n'est utile que pour le support.

Préfs

- Prefs n'est utile que pour l'assistance.

Requête

- La requête n'est utile que pour le support.

Serveur

- Serveur est la ressource que l'ordinateur a utilisée pour effectuer la requête. Pour connaître

les emplacements des serveurs, reportez-vous à la ressource appropriée.

Heure

- L'heure indique quand la requête a été effectuée, en UTC.

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.