Entender as limitações do Umbrella DNS Policy Tester

Contents

Introdução

Este documento descreve as restrições e limitações do Umbrella DNS Policy Tester.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Gateway da Web seguro
- Gateway de Internet seguro
- Guarda-chuva (camada adicionada de DNS)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

O Umbrella Policy Tester pode ser usado para determinar se um determinado destino pode ser bloqueado ou permitido pela Cisco quando visitado por uma determinada identidade. No entanto,

há algumas circunstâncias sob as quais o Policy Tester atualmente não pode retornar informações precisas (ou quaisquer) para um determinado destino. Este artigo descreve essas restrições.

Detalhes técnicos

A visão geral do verificador de políticas pode ser encontrada na documentação do Umbrella Policy Tester.

Estes resultados do Policy Tester podem estar incorretos:

Gateway da Web seguro

- Sem suporte

Gateway de Internet seguro

- Sem suporte

Guarda-chuva (camada adicionada de DNS)

- Os destinos bloqueados pelo Proxy Inteligente podem ser relatados incorretamente como "Permitidos" pelo Verificador de Políticas. Isso também inclui:
  - Listas de bloqueio de URL personalizadas
  - Domínios proxy-blocklist ou greylist
  - Blocos de inspeção de arquivo
- O tipo de destino "Aplicativo" (como Dropbox, Box, Facebook, etc. por nome) que está bloqueado pode ser incorretamente relatado como "Permitido" pelo testador de políticas.
- Quando uma rede também é aplicada a uma política da Web, a política da Web pode ser exibida incorretamente. O testador de política não tem suporte no momento para redes que também fazem parte de políticas da Web.
- Os ensaios que não forneçam todas as informações de identidade relevantes podem mostrar resultados incorretos. Por exemplo, um computador em roaming com a integração do Ative Diretory (AD) ativada enquanto estiver em uma rede protegida: o teste poderá falhar se apenas o usuário do AD for fornecido, mas o computador em roaming ganhar as decisões de política.
- Os destinos bloqueados devido a categorias de conteúdo podem ser mostrados como permitidos se forem inseridos com letras maiúsculas e minúsculas ou estiverem em maiúsculas. Por exemplo, se você estiver bloqueando a categoria "nudez", o domínio playboy.com poderá ser exibido como bloqueado, enquanto Playboy.com aparece como permitido.
- Os destinos de "DNS dinâmico" poderão ser bloqueados se essa categoria de segurança for selecionada, mas poderão ser relatados incorretamente como "Permitido" pelo testador de políticas.
- Os destinos permitidos pelo controle do aplicativo podem ser exibidos incorretamente como bloqueados no Policy Tester.
- Os destinos bloqueados pela API de imposição de guarda-chuva para integrações

personalizadas podem ser relatados incorretamente como "Permitidos" pelo testador de políticas.
- Os destinos bloqueados pela integração do Umbrella AMP Threat Grid podem ser relatados incorretamente como "Permitidos" pelo testador de políticas.
- Os destinos bloqueados devido a um CNAME podem ser incorretamente reportados como "Permitidos" pelo testador de políticas.
- Os destinos que são endereços IP não são suportados no testador de política no momento.
- Os destinos que são URLs não têm suporte noPolicy Tester neste momento.
- Destinos bloqueados para resolução em um IP mal-intencionado podem ser incorretamente reportados como "Permitidos" pelo Policy Tester.
- Destinos "potencialmente prejudiciais" podem ser bloqueados se essa categoria de segurança for selecionada, mas podem ser incorretamente relatados como "permitidos" pelo testador de políticas.
- Os destinos onde as proteções DDOS automatizadas impedem temporariamente que o DNS responda pelo domínio afetado não são visíveis pelo Policy Tester.
- Destinos bloqueados sob a categoria de conteúdo "Proteção da Juventude Alemã" podem ser incorretamente reportados como "Permitidos" pelo "Testador da Política". Esta categoria não pode ser mencionada nos resultados do testador de políticas.
- Destinos bloqueados devido à classificação de segurança "Criptomoeda" podem aparecer incorretamente como "Permitido" mesmo quando bloqueados por configurações de segurança.
- Bloqueios devido a categorias VPN de encapsulamento DNS não podem exibir corretamente resultados no testador de políticas. Eles aparecem incorretamente como permitidos.
- Os dispositivos Chromebook por trás de um dispositivo virtual podem mostrar políticas incorretas. Blocos de identidade do Chromebook (UCC) podem substituir políticas aplicadas do Virtual Appliance, mas os blocos do Virtual Appliance podem substituir as permissões do UCC.
- Os membros de grupos do AD em que o grupo não está sincronizado com o Umbrella (incluindo grupos que fazem parte de um domínio pai ou filho e grupos que são membros de grupos não sincronizados seletivamente com o Umbrella) podem ser mostrados como correspondendo à política mostrada no Testador de Política. A política de usuário não pode ser aplicada na nuvem. Confirme adicionando o usuário único à sua política e confirme se ela se aplica corretamente em 5 minutos.
- Destinos que estão na lista Domínios internos. O testador de políticas não usa a lista de domínios internos ao relatar um resultado de teste.
- As categorias que não aparecem no site de marcação de domínio da Comunidade OpenDNS não têm a garantia de mostrar a categoria correta no Policy Tester. Somente uma fonte de categorizações é representada.
- O Policy Tester é limitado a mostrar 20 resultados ao procurar uma identidade.
- Um usuário do AD é membro de um grupo do AD aninhado, mas somente o grupo do AD pai é selecionado nas identidades ao criar a política DNS. A pesquisa do testador de política pode falhar ao corresponder à política correta.
- Os destinos na lista de permissão protegida podem ser relatados incorretamente como "Bloqueados" pelo testador de políticas.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.