

Configurar a Categoria de Segurança VPN de Encapsulamento DNS

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Ativando a VPN de túnel DNS](#)

Introdução

Este documento descreve como configurar a Categoria de Segurança VPN de tunelamento DNS no Umbrella.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no DNS Umbrella.

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

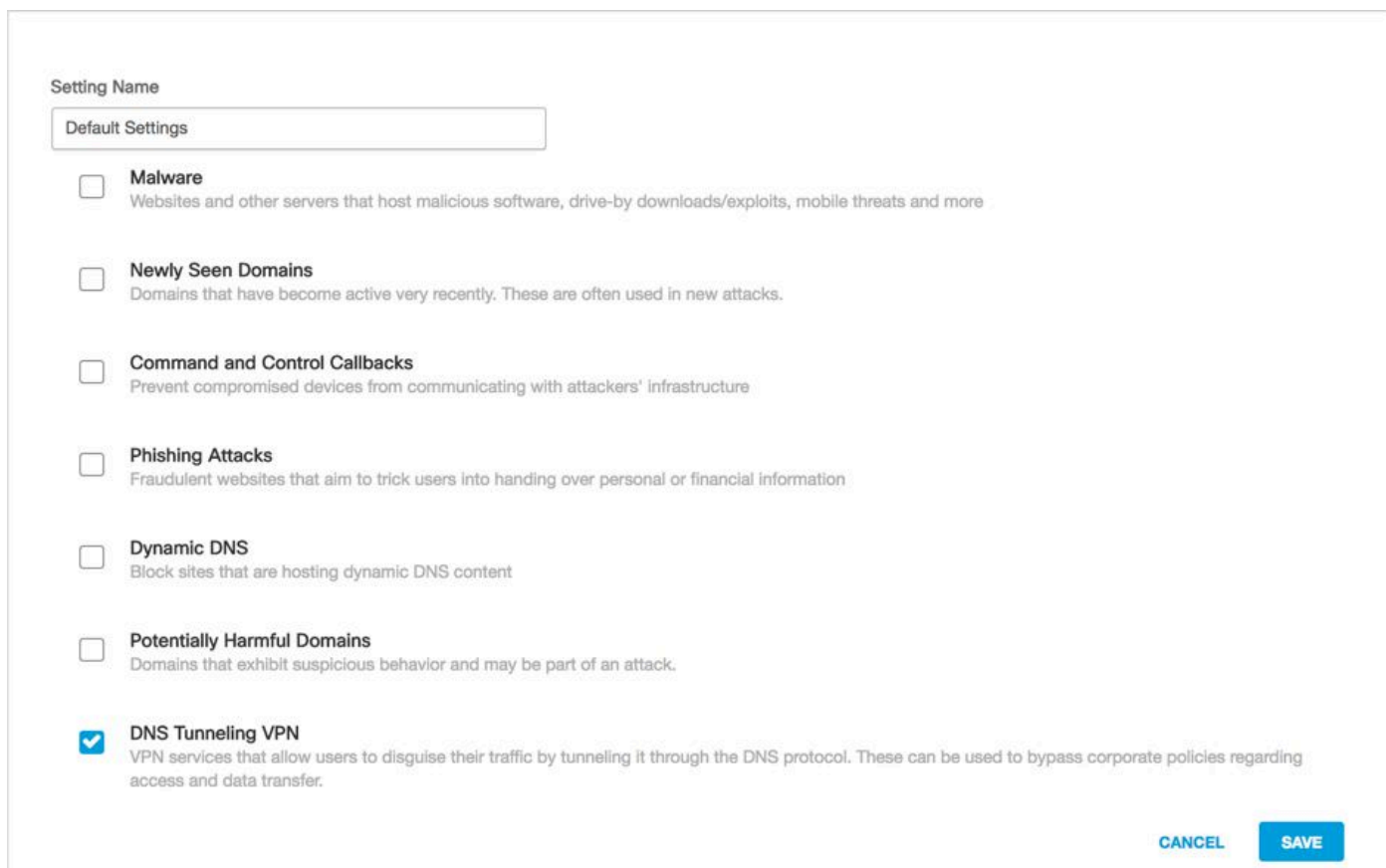
A VPN de tunelamento DNS classifica os servidores associados aos serviços VPN de tunelamento DNS em uma categoria de segurança que você pode bloquear ou permitir e relatar. Esses serviços permitem que os usuários finais disfarcem o tráfego de saída como consultas DNS, violando potencialmente o uso aceitável, a prevenção contra perda de dados ou as políticas de segurança. Como resultado, esses serviços apresentam uma ameaça potencial à segurança e reduzem a visibilidade geral em seu ambiente.

Com essa categoria de segurança fornecendo visibilidade imediata, você pode reduzir o risco de

tunelamento DNS e possível perda de dados. Você pode bloquear esta categoria imediatamente ou apenas monitorar os resultados em relatórios; isso proporciona a flexibilidade para determinar qual é a abordagem correta para lidar com o problema, dependendo da tolerância a riscos, do uso aceitável ou das políticas de RH.

Ativando a VPN de túnel DNS

Essa categoria de segurança pode ser habilitada como qualquer outra em Políticas > Security Settings e, em seguida, editar uma configuração de segurança existente. Ou pode ser feito no próprio assistente de configuração de política:



The screenshot shows a configuration window titled 'Setting Name' with a dropdown menu set to 'Default Settings'. Below the dropdown is a list of security categories, each with a checkbox and a description:

- Malware**
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more
- Newly Seen Domains**
Domains that have become active very recently. These are often used in new attacks.
- Command and Control Callbacks**
Prevent compromised devices from communicating with attackers' infrastructure
- Phishing Attacks**
Fraudulent websites that aim to trick users into handing over personal or financial information
- Dynamic DNS**
Block sites that are hosting dynamic DNS content
- Potentially Harmful Domains**
Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN**
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.

At the bottom right of the window are two buttons: 'CANCEL' and 'SAVE'.

115014823666

O tunelamento DNS pode ser filtrado por meio do relatório Activity Search:

Security Categories

Select All

- Command and Control
- Malware
- Phishing
- Unauthorized IP Tunnel Access
- Newly Seen Domains
- Potentially Harmful
- DNS Tunneling VPN**

APPLY

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.