

Configure the DNS Tunneling VPN Security Category

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Overview](#)

[Turning on DNS Tunneling VPN](#)

Introduction

This document describes how to configure the DNS tunneling VPN Security Category in Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Umbrella DNS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

DNS tunneling VPN classifies servers associated with DNS tunneling VPN services under a security category that you can block or allow and report on. These services allow end-users to disguise outgoing traffic as DNS queries, potentially violating acceptable use, data loss prevention, or security policies. As a result, these services present a potential security threat and reduce overall visibility in your environment.

With this security category providing immediate visibility, you can reduce the risk of DNS tunneling and potential data loss. You can block this category outright, or just monitor the results in reports; this provides the flexibility to determine what is the right approach to tackling the problem, depending on your risk tolerance, acceptable use or HR policies.

Turning on DNS Tunneling VPN

This security category can be enabled like any other under **Policies > Security Settings**, then editing an existing security setting. Or, it can be done within the policy configuration wizard itself:

Setting Name

Default Settings

- 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.

CANCEL

SAVE

115014823666

DNS Tunneling can be filtered against through the Activity Search report:

Security Categories

Select All

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

APPLY