

# Configura la categoria di sicurezza VPN per il tunneling DNS

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica](#)

[Attivazione della VPN con tunneling DNS](#)

---

## Introduzione

In questo documento viene descritto come configurare la categoria di sicurezza VPN per il tunneling DNS in Umbrella.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano sul DNS Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Panoramica

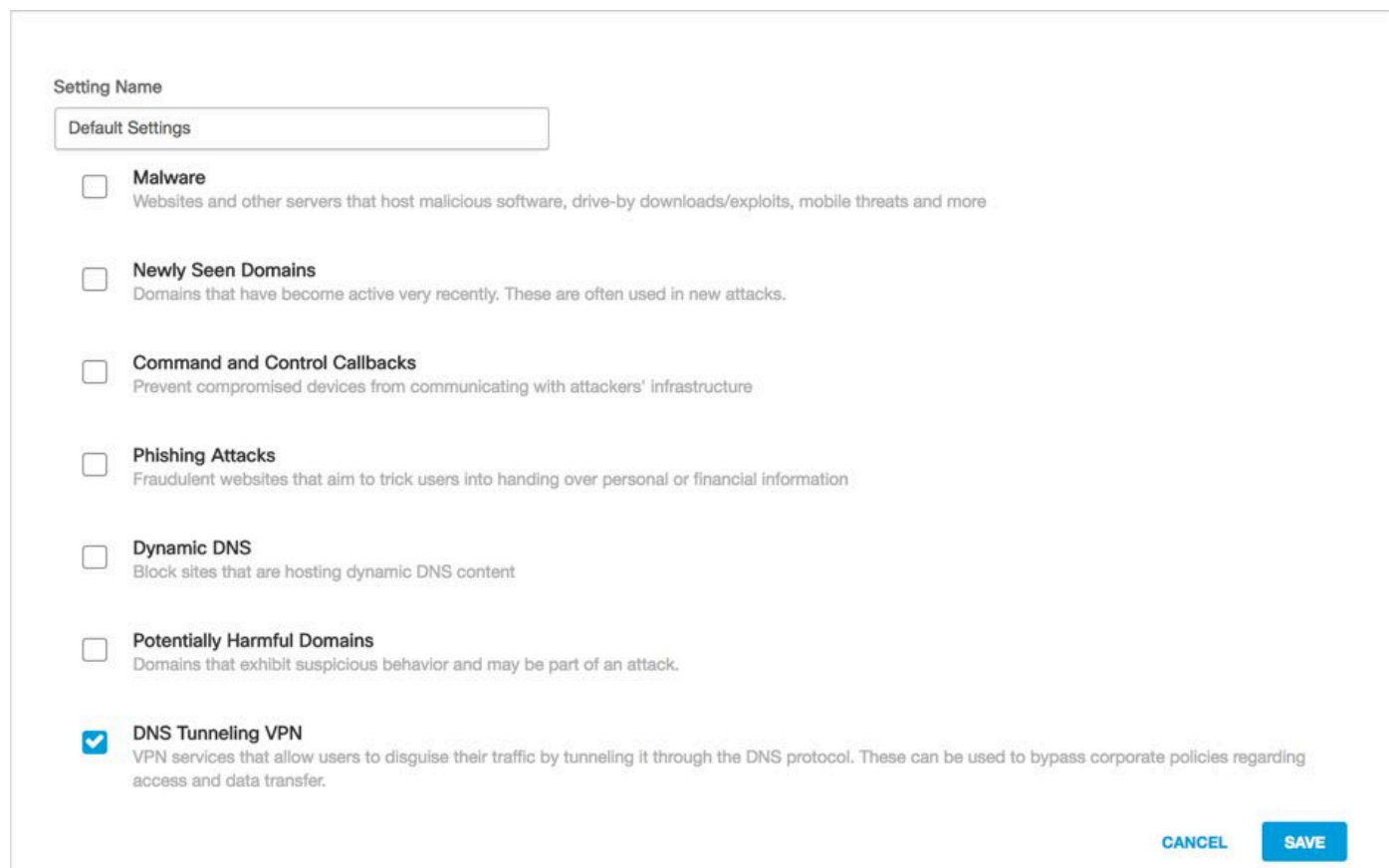
La VPN di tunneling DNS classifica i server associati ai servizi VPN di tunneling DNS in una categoria di sicurezza che è possibile bloccare o consentire e per la quale è possibile creare rapporti. Questi servizi consentono agli utenti finali di mascherare il traffico in uscita come query DNS, potenzialmente violando l'utilizzo accettabile, la prevenzione della perdita di dati o i criteri di sicurezza. Di conseguenza, questi servizi rappresentano una potenziale minaccia per la sicurezza e riducono la visibilità complessiva dell'ambiente.

Grazie a questa categoria di sicurezza che fornisce visibilità immediata, è possibile ridurre il

rischio di tunneling DNS e la potenziale perdita di dati. È possibile bloccare questa categoria in modo definitivo o semplicemente monitorare i risultati nei report; ciò fornisce la flessibilità necessaria per determinare quale sia l'approccio corretto per affrontare il problema, a seconda della tolleranza al rischio, dell'utilizzo accettabile o delle politiche delle risorse umane.

## Attivazione della VPN con tunneling DNS

Questa categoria di protezione può essere attivata come qualsiasi altra in Criteri > Impostazioni di protezione, quindi è possibile modificare un'impostazione di protezione esistente. In alternativa, è possibile eseguire questa operazione all'interno della configurazione guidata dei criteri:



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

Il tunneling DNS può essere filtrato tramite il report Ricerca attività:

## Security Categories

Select All

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

APPLY

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).