Konfigurieren der VPN-Sicherheitskategorie für DNS-Tunneling

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der VPN-Sicherheitskategorie für DNS-Tunneling unter Umbrella beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Umbrella DNS.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

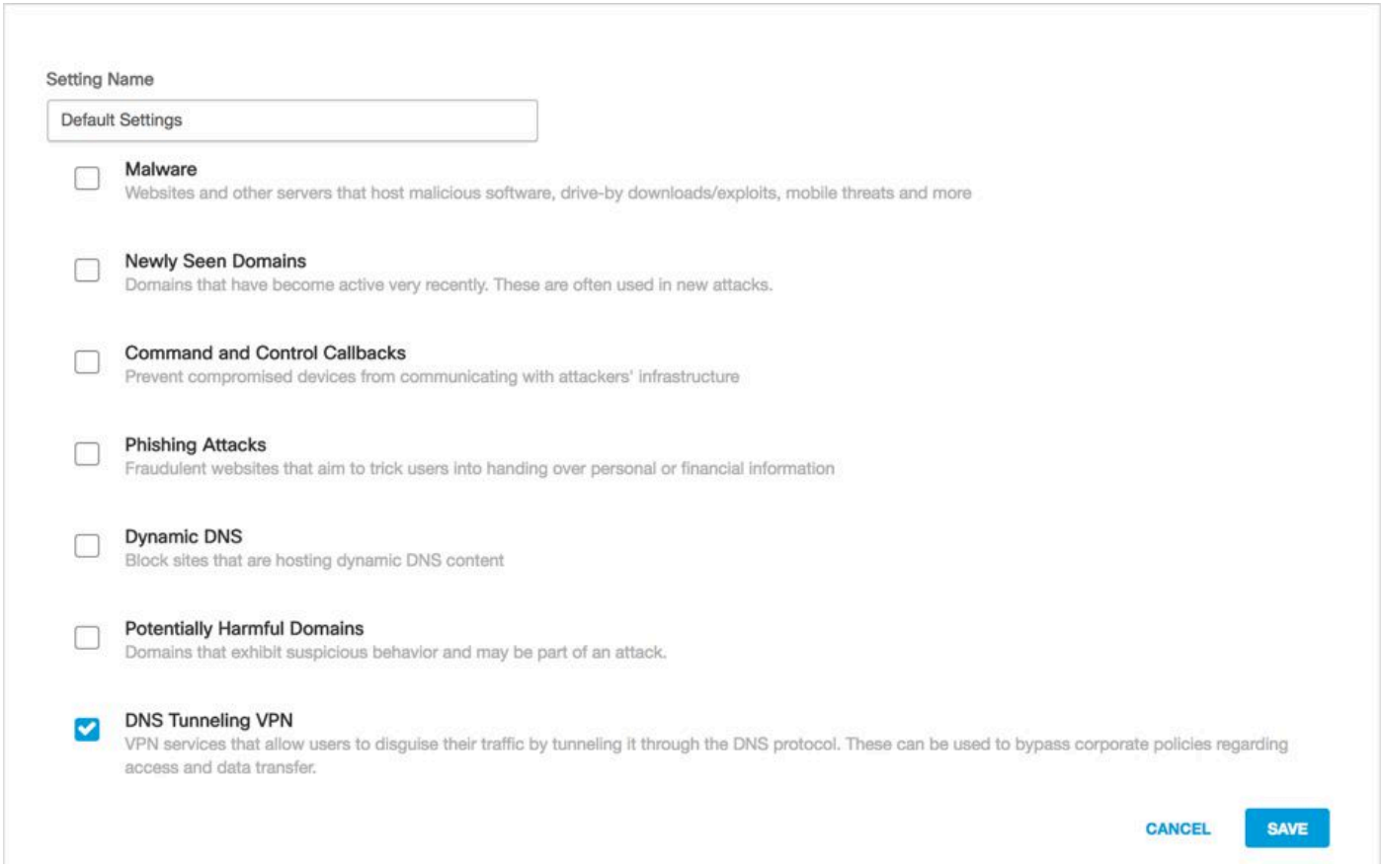
Das DNS-Tunneling-VPN klassifiziert Server, die DNS-Tunneling-VPN-Services zugeordnet sind, unter einer Sicherheitskategorie, die Sie blockieren oder zulassen und melden können. Mit diesen Services können Endbenutzer ausgehenden Datenverkehr als DNS-Abfragen tarnen und damit möglicherweise gegen akzeptable Nutzungsbedingungen, Schutz vor Datenverlust oder Sicherheitsrichtlinien verstoßen. Daher stellen diese Services ein potenzielles Sicherheitsrisiko dar und reduzieren die Gesamttransparenz in Ihrer Umgebung.

Mit dieser Sicherheitskategorie, die sofortige Transparenz bietet, können Sie das Risiko von DNS-

Tunneling und potenziellen Datenverlusten reduzieren. Sie können diese Kategorie vollständig sperren oder die Ergebnisse nur in Berichten überwachen. So können Sie flexibel festlegen, welcher Ansatz zur Problemlösung am besten geeignet ist, und zwar abhängig von Ihrer Risikotoleranz, Ihrer akzeptablen Nutzung oder Ihren HR-Richtlinien.

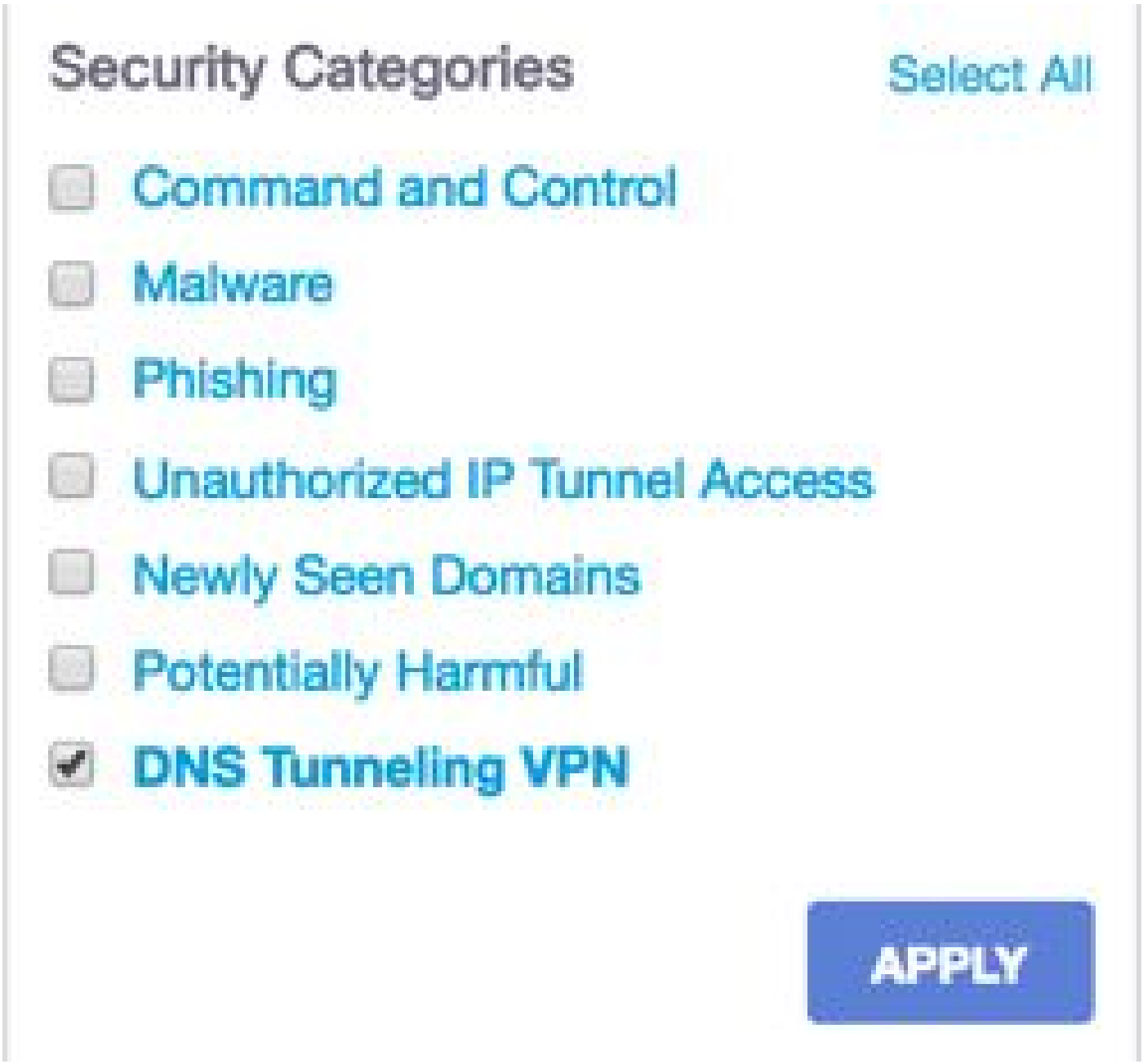
Aktivieren von DNS Tunneling VPN

Diese Sicherheitskategorie kann wie jede andere Sicherheitskategorie unter Richtlinien > Sicherheitseinstellungen aktiviert werden. Anschließend können Sie eine vorhandene Sicherheitseinstellung bearbeiten. Dies kann auch im Assistenten zur Richtlinienkonfiguration selbst durchgeführt werden:



115014823666

DNS-Tunneling kann mithilfe des Aktivitätssuchberichts gefiltert werden:



115015008983

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.