Configurazione di Cisco Umbrella sulla rete tramite router serie RV34x

Introduzione

A partire dalla versione firmware 1.0.0.2.16, i router della serie RV34x supportano ora Cisco Umbrella. Umbrella utilizza il DNS come vettore o scudo di difesa contro malware e intrusioni di dati.

Dispositivi interessati

- Serie RV34x router

Versione del software

- 1.0.02.16

Requisiti

- Un account Umbrella attivo (non ne hai uno? Richiedi un preventivo o avvia una versione di valutazione gratuita)

Obiettivo

Questa guida illustra i passaggi necessari per integrare la piattaforma di sicurezza Umbrella nella rete. Prima di entrare nei dettagli grintosi risponderemo ad alcune domande che potreste porvi riguardo Umbrella.

Cos'è un ombrello?

Umbrella è una piattaforma Cisco semplice ma molto efficace per la sicurezza cloud. Umbrella opera nel cloud ed esegue molti servizi correlati alla sicurezza. Dalla minaccia emergente all'indagine post-evento. Umbrella individua e previene gli attacchi attraverso tutte le porte e i protocolli.

Come funziona?

Umbrella utilizza il DNS come vettore principale per la difesa. Quando gli utenti immettono un URL nella barra del browser e premendo Invio, Umbrella partecipa al trasferimento. Tale URL passa al resolver DNS di Umbrella e, se al dominio viene associato un avviso di sicurezza, la richiesta viene bloccata. Questi dati di telemetria vengono trasferiti e analizzati in microsecondi, senza aggiungere alcuna latenza. I dati di telemetria utilizzano registri e strumenti che tracciano miliardi di richieste DNS in tutto il mondo. Quando questi dati sono diffusi, la correlazione a livello globale consente una risposta rapida agli attacchi non appena

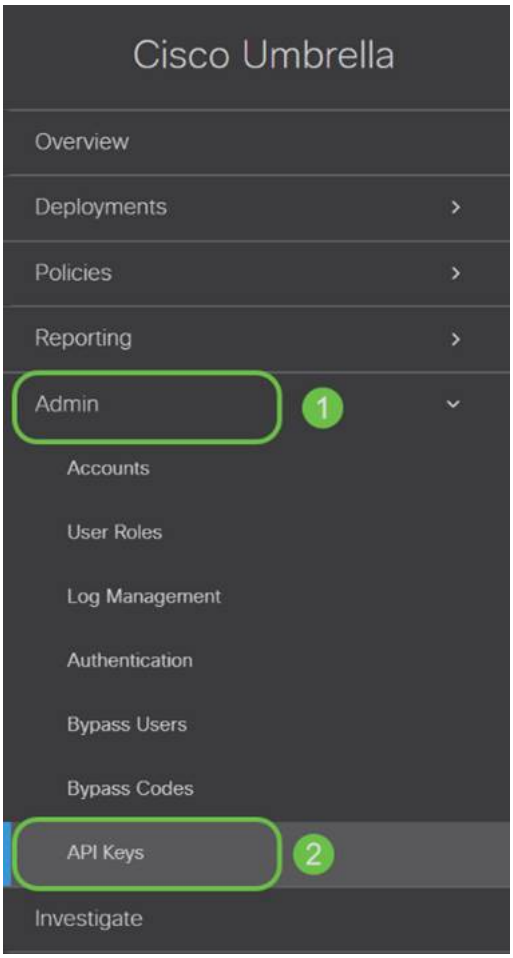
si verificano. Per ulteriori informazioni - politica completa, versione di riepilogo - vedere l'informativa sulla privacy di Cisco qui. I dati di telemetria possono essere paragonati ai dati derivati da strumenti e registri.

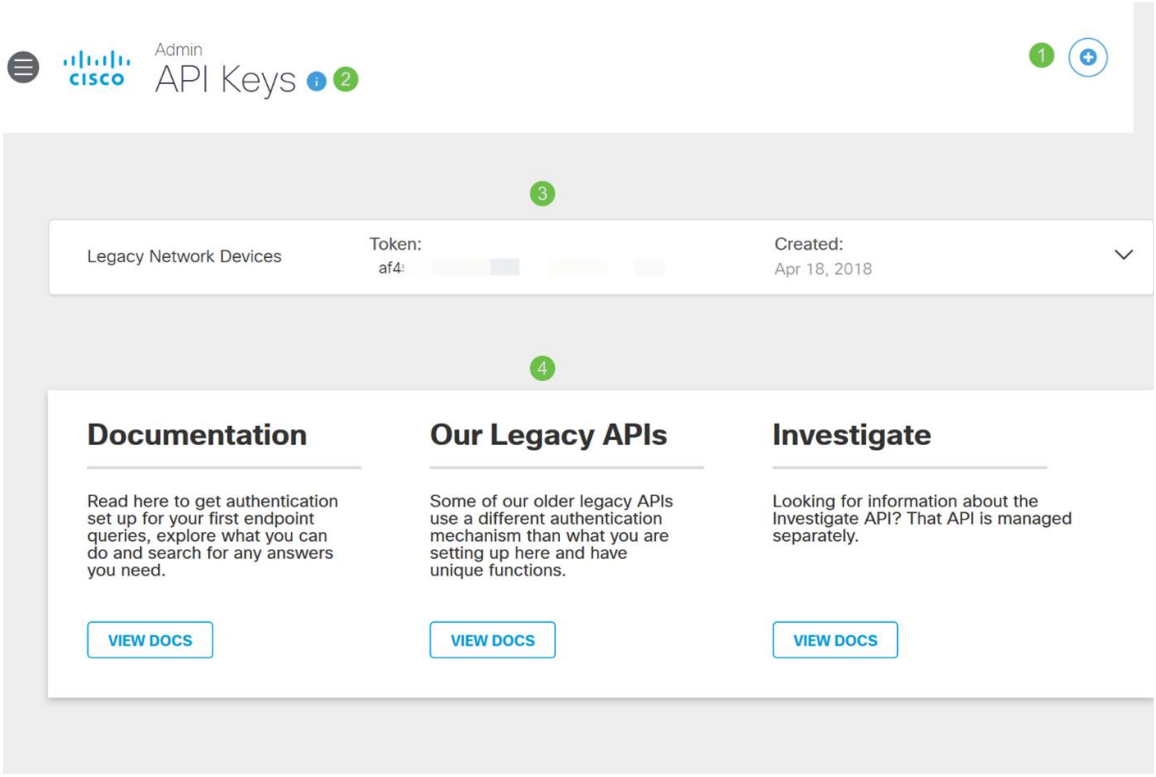
Per riassumere, in una metafora, immaginate di essere ad una festa. A questa festa tutti sono al telefono navigando in rete. Il silenzioso silenzio di gruppo è punteggiato dai partecipanti che filmano i loro schermi. Non è una grande festa, ma mentre sul vostro telefono vedete un collegamento ipertestuale a un gattino GIF che sembra irresistibile. Tuttavia, poiché l'URL appare dubbio, non si è certi di dover toccare o meno. Quindi prima di toccare il collegamento ipertestuale, si urla al resto della festa "Questo collegamento è cattivo?" Se un'altra persona alla festa fosse stata al link e avesse scoperto che era una truffa, avrebbe gridato "Si, l'ho fatto, ed è una truffa!" Ringraziate quella persona per avervi salvato, continuando la vostra nobile ricerca di immagini di animali carini. Naturalmente, nelle dimensioni di Cisco, questo tipo di richieste e di controlli di sicurezza delle richiamate vengono eseguiti milioni di volte al secondo, con vantaggi per la sicurezza della rete.

Fantastico, come facciamo?

Dove si trova questa guida, inizia con l'acquisizione della chiave API e della chiave privata dal dashboard dell'account Umbrella. Dopo, accederemo al tuo router per aggiungere l'API e la chiave privata. In caso di problemi, consultare la documentazione e qui le opzioni di supporto Umbrella.

Passaggio 1. Dopo aver effettuato l'accesso all'account Umbrella, dalla schermata *Dashboard* fare clic su **Admin** > **API Keys**.

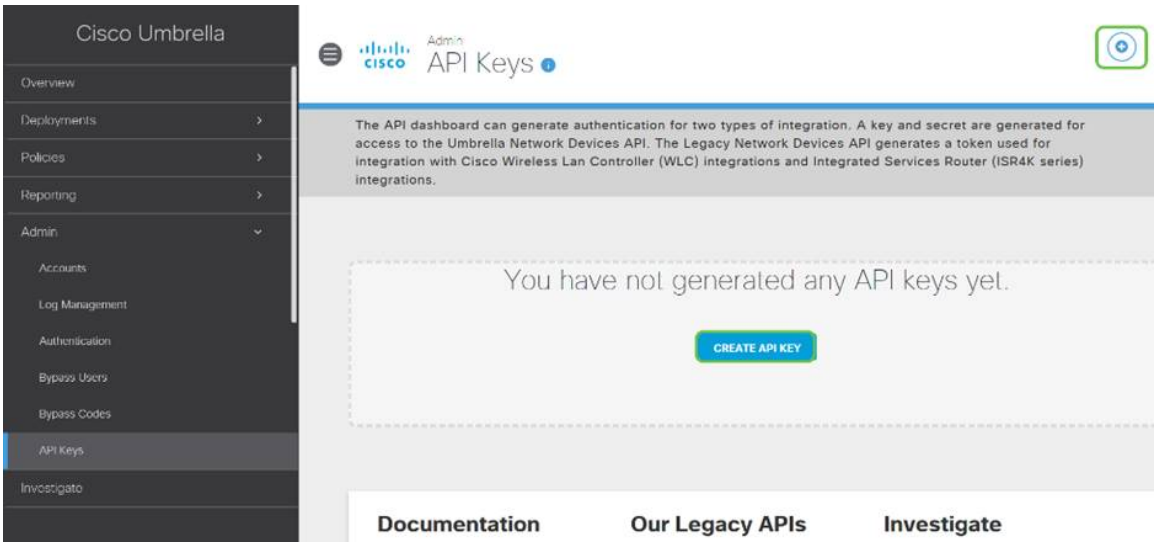




Anatomia della schermata delle chiavi API (con chiave API preesistente) -

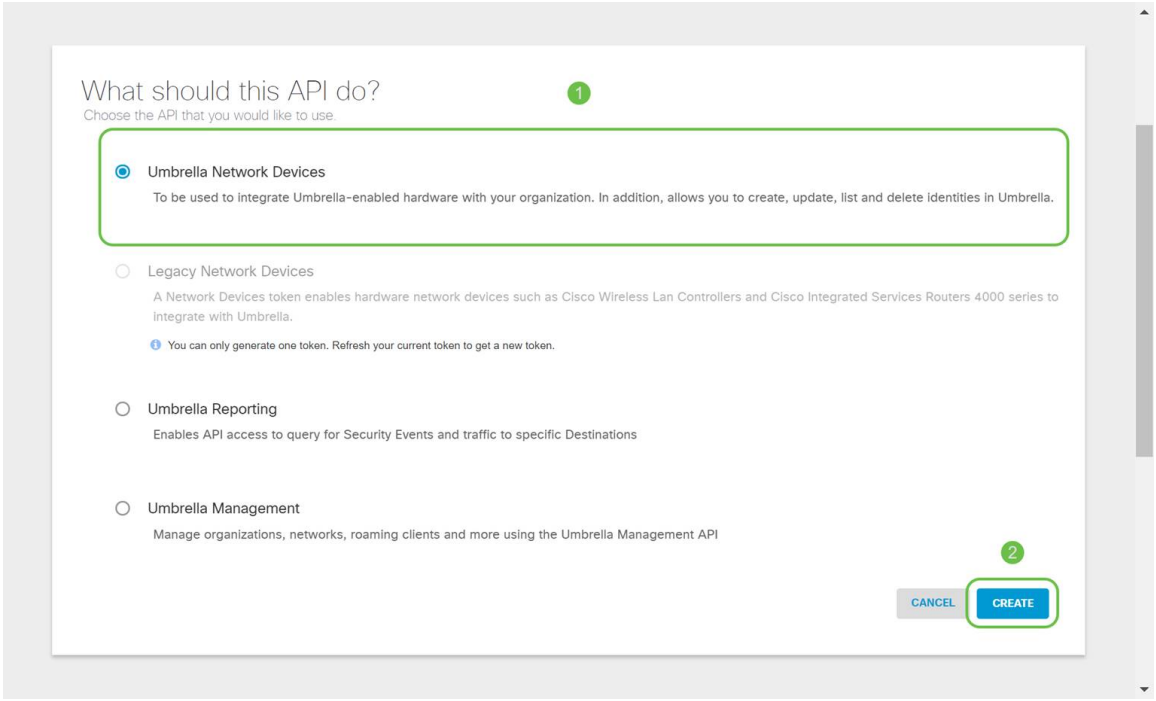
1. Add API Key (Aggiungi chiave API) - Avvia la creazione di una nuova chiave da utilizzare con l'API Umbrella.
2. Informazioni aggiuntive - Visualizza le diapositive verso il basso/verso l'alto con un'illustrazione per questa schermata.
3. Finestra Token: contiene tutte le chiavi e i token creati da questo account. (Esegue la compilazione dopo la creazione di una chiave)
4. Documenti di supporto - Collegamenti alla documentazione sul sito Umbrella relativa agli argomenti di ciascuna sezione.

Passaggio 2. Fare clic sul pulsante **Add API Key** nell'angolo in alto a destra oppure fare clic sul pulsante **Create API Key**. Funzionano entrambi allo stesso modo.

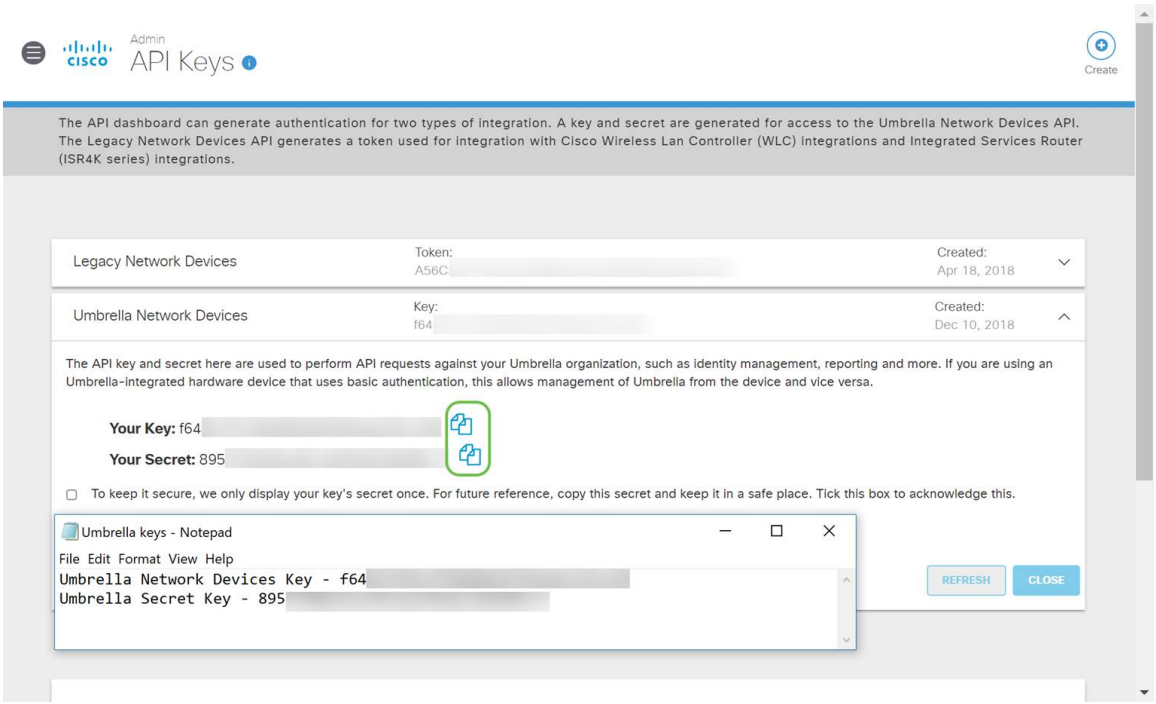


Nota: la schermata precedente sarebbe simile a quella che vedreste aprire questo menu per la prima volta.

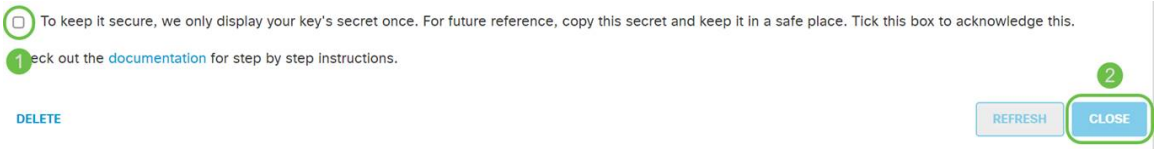
Passaggio 3. Selezionare **Umbrella Network Devices** e fare clic sul pulsante **Create**.



Passaggio 4. Aprire un editor di testo come il Blocco note, quindi fare clic sul pulsante **Copia** a destra dell'API e della *chiave privata* API. Una notifica a comparsa confermerà che la chiave è stata copiata negli Appunti. Incollare una alla volta il segreto e la chiave API nel documento, etichettandoli per riferimento futuro. In questo caso l'etichetta è "Umbrella network devices key". Salvare quindi il file di testo in una posizione sicura, facilmente accessibile in seguito.



Passaggio 5. Dopo aver copiato la chiave e la chiave segreta in un percorso sicuro, dalla *schermata API Umbrella* fare clic sulla **casella di controllo** per confermare la conferma di completamento della visualizzazione temporanea della chiave segreta, quindi fare clic sul pulsante **Chiudi**.



Nota importante:se si perde o si elimina accidentalmente la chiave segreta, non sarà

necessario chiamare alcuna funzione o numero di supporto per recuperare la chiave. Tienilo segreto, tienilo al sicuro. In caso di perdita, sarà necessario eliminare la chiave e autorizzare nuovamente la nuova chiave API con ciascun dispositivo che si desidera proteggere con Umbrella.

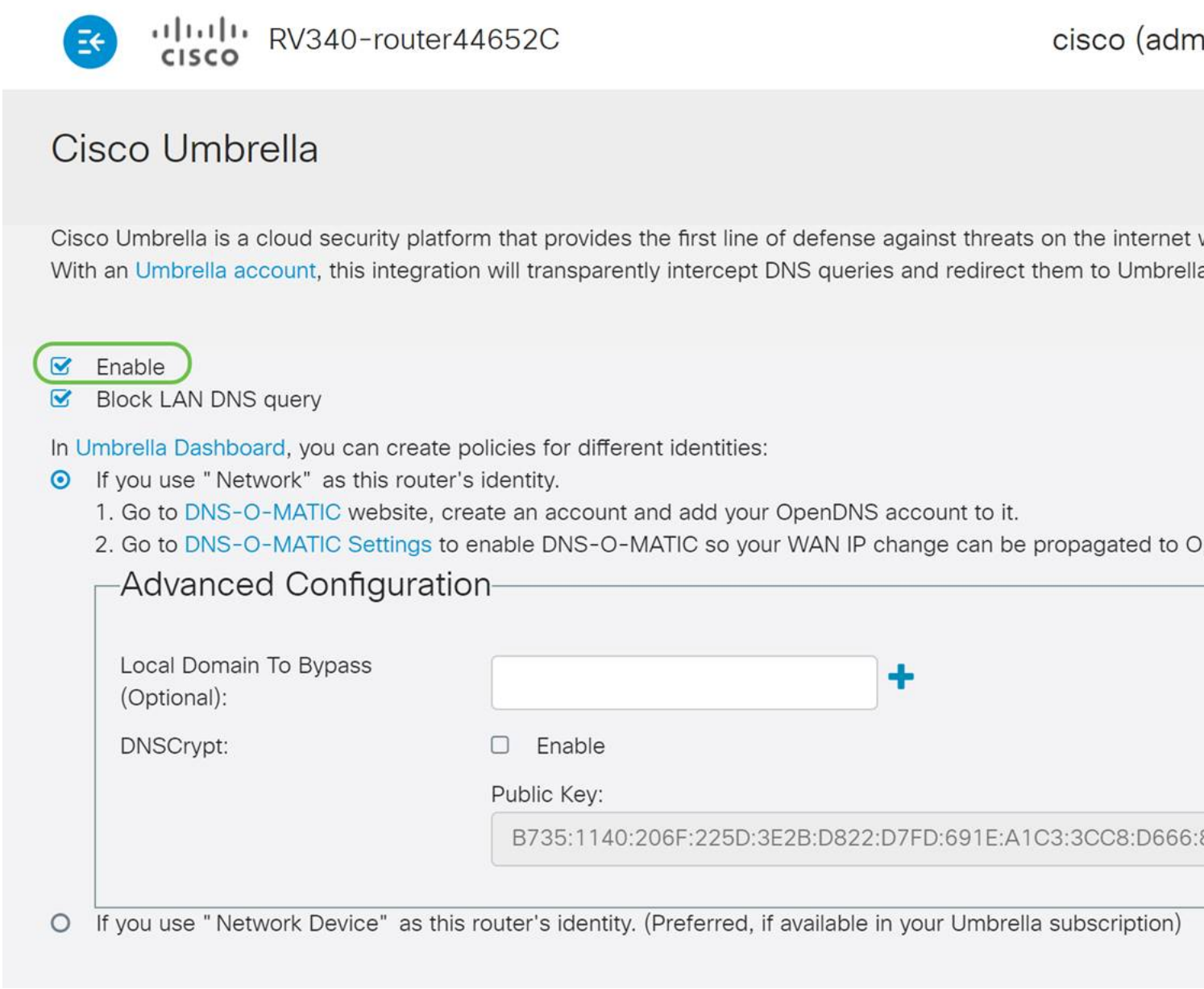
Procedure ottimali: Conservare una *singola* copia di questo documento su un dispositivo, come un'unità USB, inaccessibile da qualsiasi rete.

Configurazione di Umbrella sul dispositivo RV34x

Ora che abbiamo creato le chiavi API in Umbrella, le prenderemo e le installeremo sui nostri dispositivi RV34x. Nel nostro caso stiamo utilizzando un RV340.

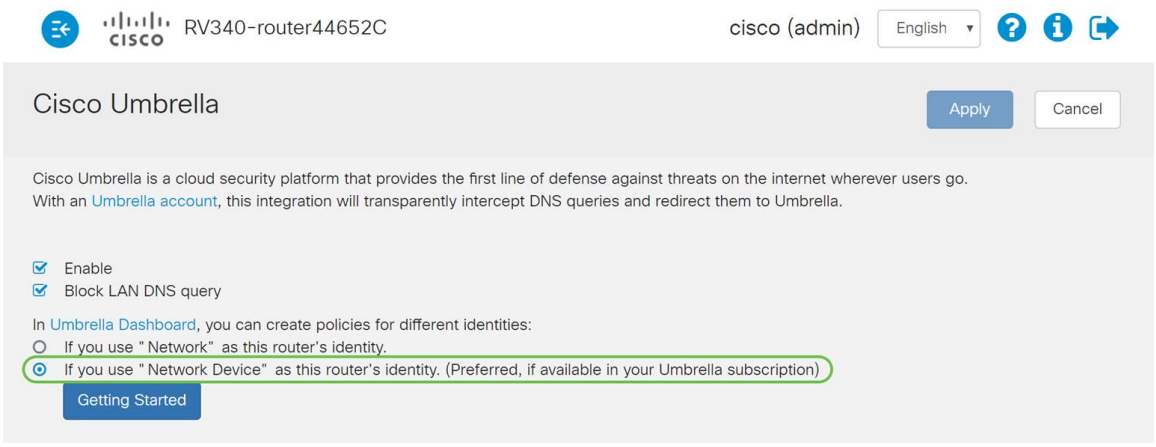
Passaggio 1. Dopo aver effettuato l'accesso al dispositivo RV34x, fare clic su **Sicurezza > Umbrella** nel menu della barra laterale.

Passaggio 2. La schermata dell'API Umbrella presenta una serie di opzioni. Per iniziare ad abilitare Umbrella, fare clic sulla casella di controllo **Abilita**.

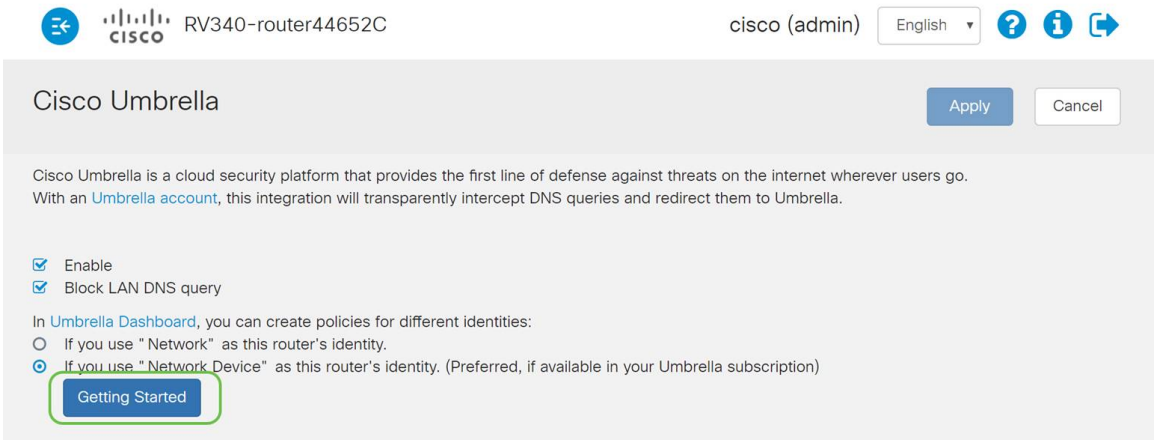


Passaggio 3. (Facoltativo) Se per impostazione predefinita è selezionata la casella Blocca query DNS LAN, questa funzionalità pulita crea automaticamente elenchi di controllo di accesso sul router che impedirà al traffico DNS di uscire su Internet. Questa funzione forza tutte le richieste di traduzione del dominio a essere indirizzate attraverso RV34x ed è una buona idea per la maggior parte degli utenti.

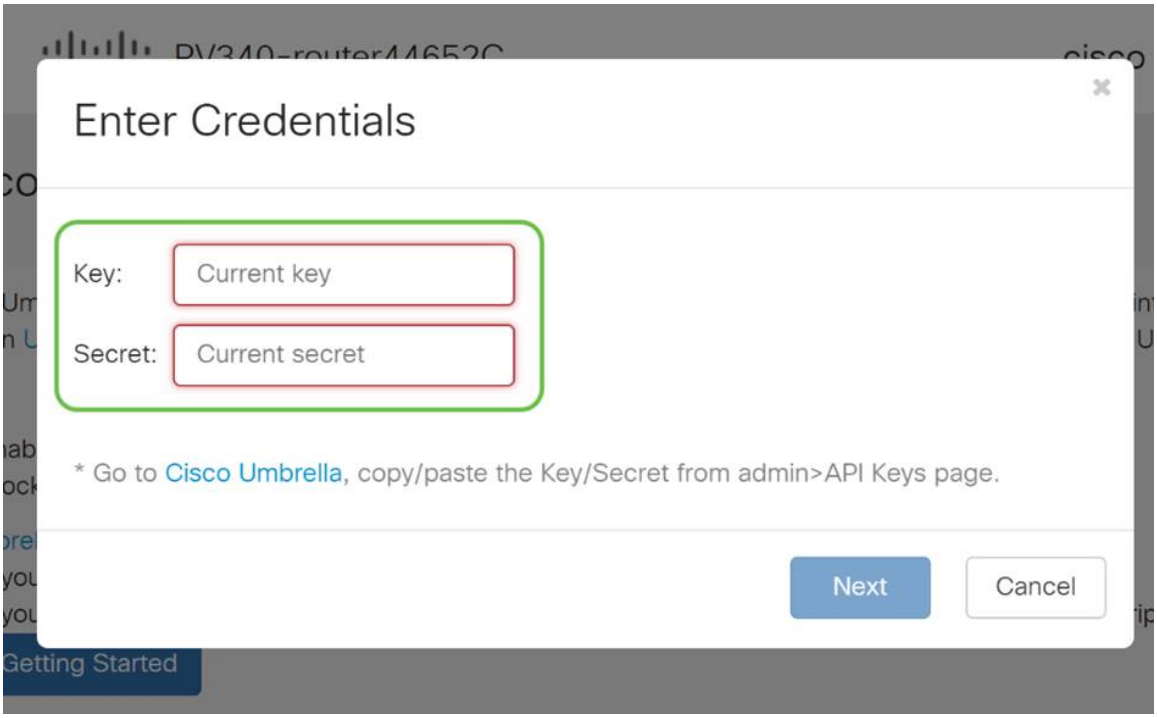
Passaggio 4. Il passaggio successivo viene eseguito in due modi diversi. Entrambi dipendono dalla configurazione della rete. Se si utilizza un servizio come DynDNS o NoIP, è necessario lasciare lo schema di denominazione predefinito "Network". Sarà quindi necessario accedere a tali account per garantire l'interfaccia Umbrella con tali servizi in quanto fornisce protezione. Per i nostri scopi stiamo facendo affidamento su "Network Device", fare clic sul pulsante radiale inferiore.



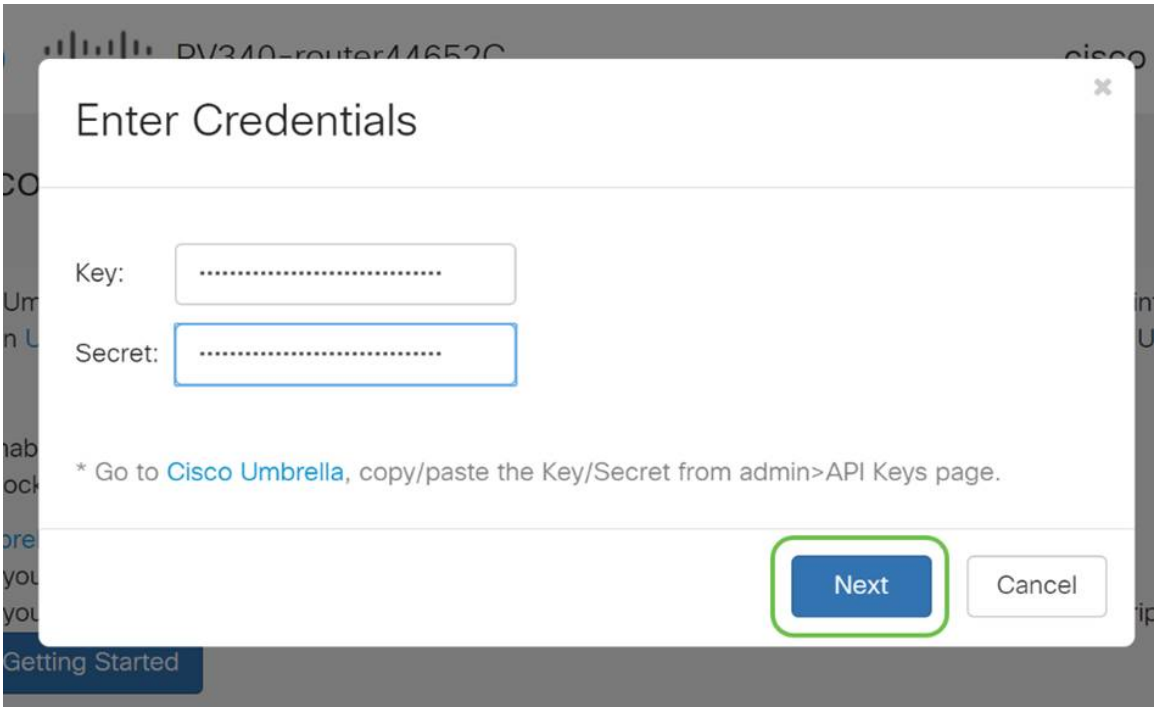
Passaggio 5. Fare clic su **Riquadro attività iniziale** per avviare la procedura guidata.



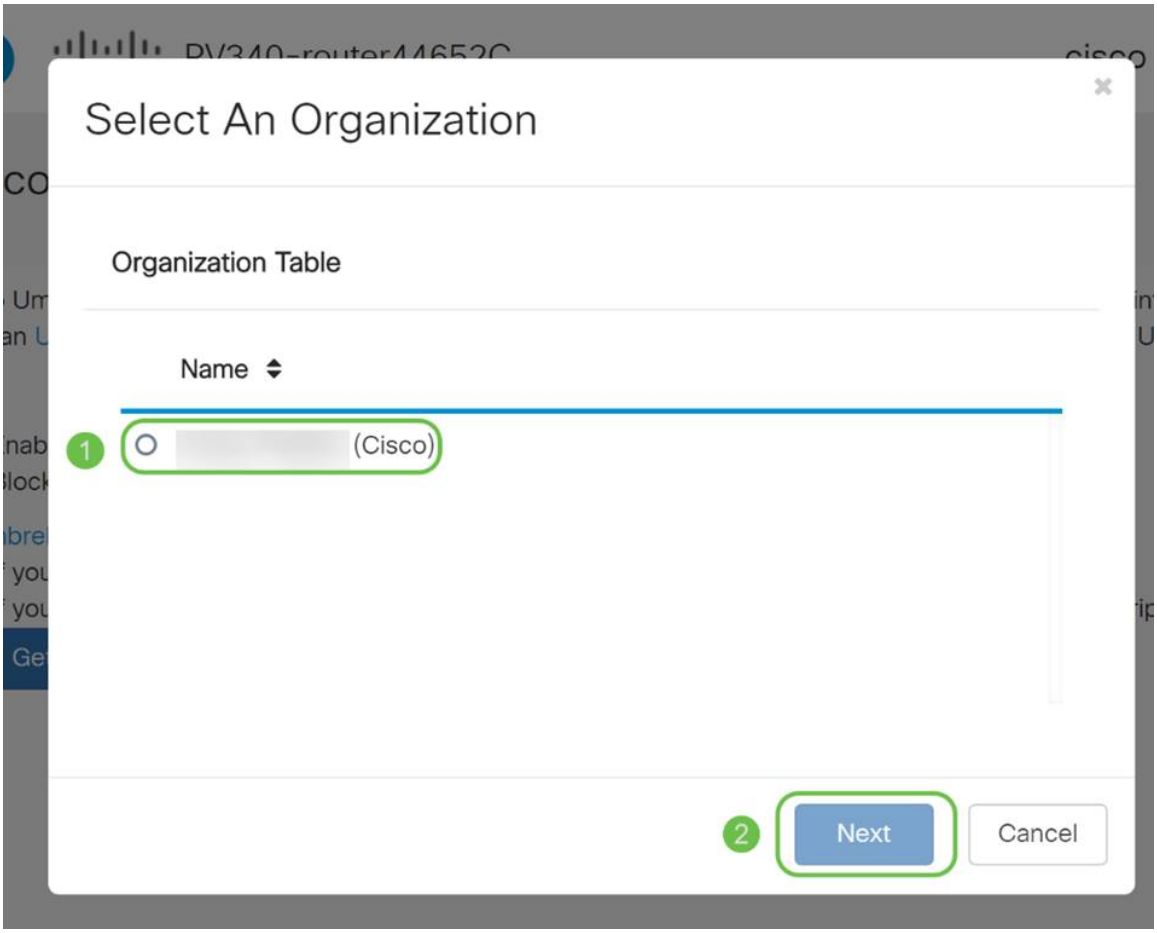
Passaggio 6. Immettere la **chiave API** e la **chiave privata** nelle caselle di testo.



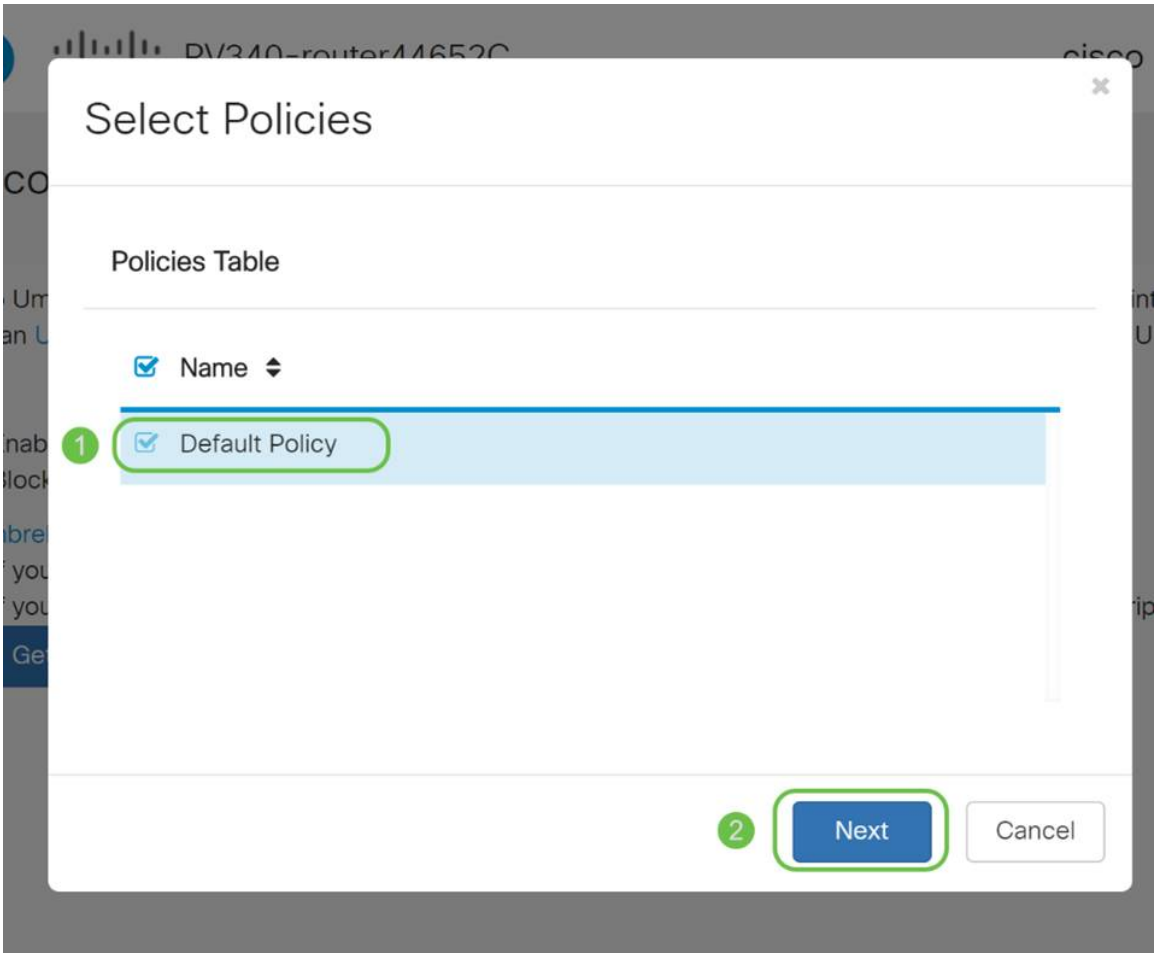
Passaggio 7. Dopo aver inserito l'API e la chiave privata, fare clic sul pulsante **Next** (Avanti).



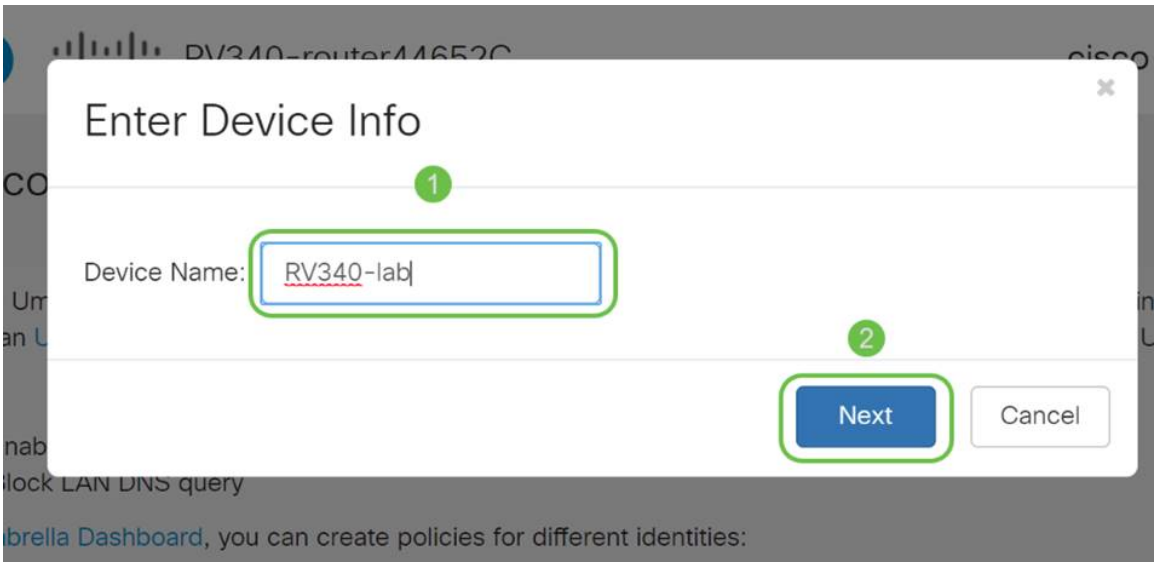
Passaggio 8. Nella schermata successiva selezionare l'**organizzazione** che si desidera associare al router, quindi fare clic su **Avanti**.



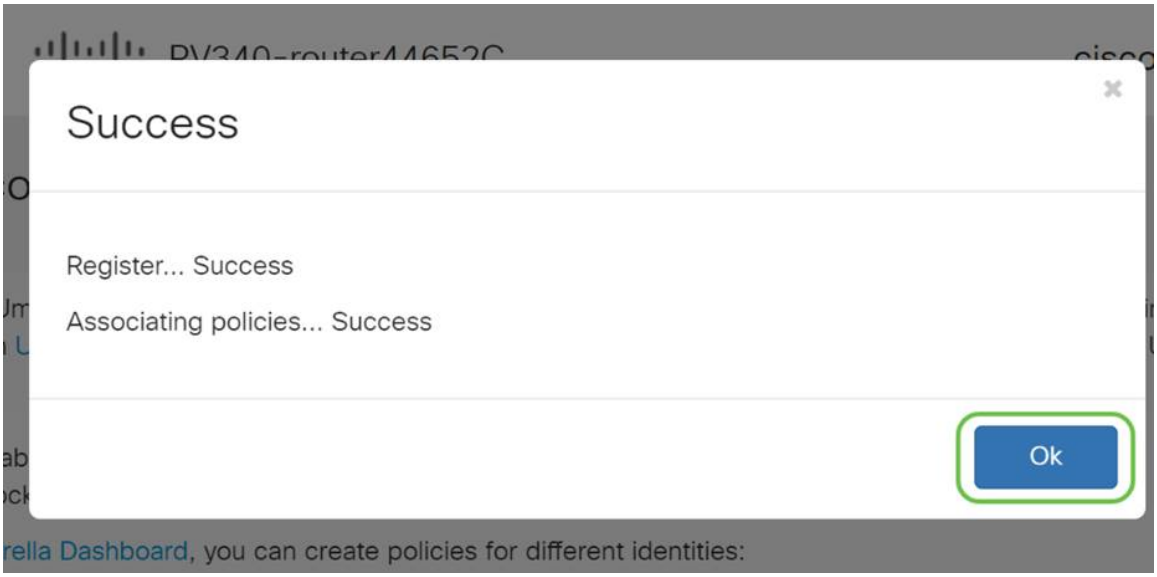
Passaggio 9. Selezionare la policy da applicare al traffico instradato dalla RV34x. Per la maggior parte degli utenti, il criterio predefinito fornisce una copertura sufficiente.



Passaggio 10. **Assegnare un nome** al dispositivo in modo che possa essere designato in Umbrella reporting. Nella configurazione è stato assegnato "RV340-lab".



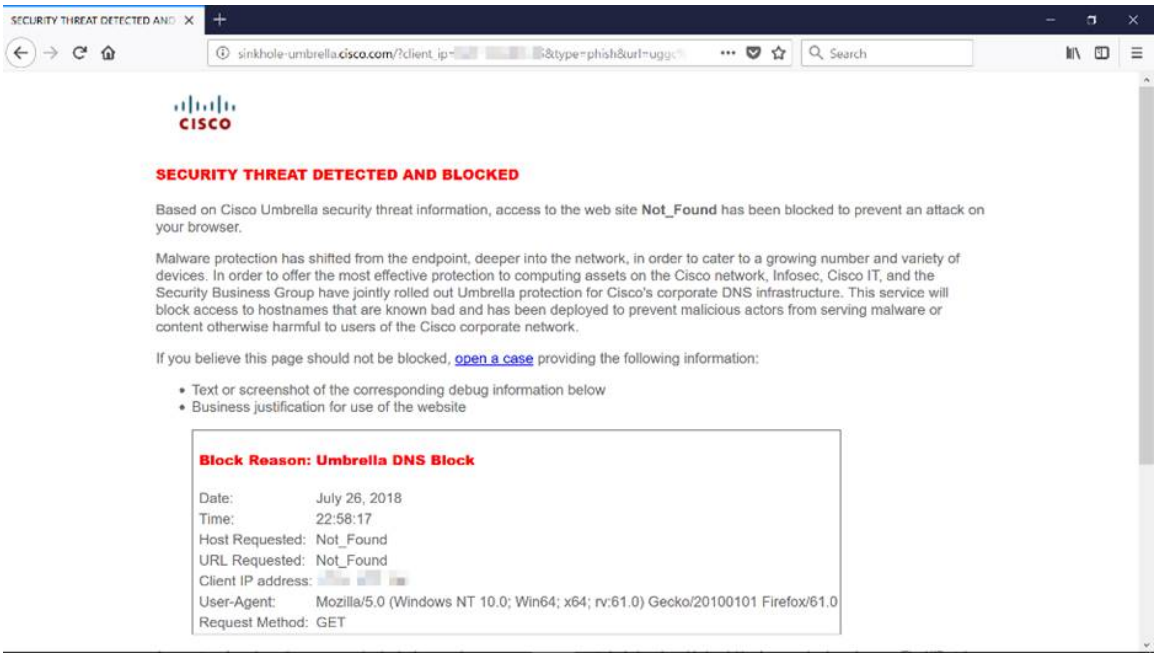
Passaggio 11. La schermata successiva convaliderà le impostazioni scelte e fornirà un aggiornamento, quando associato correttamente fare clic su **OK**.



Confermare che tutto è al posto giusto

Congratulazioni, ora sei protetto da Cisco's Umbrella. O lo sei? Sicuramente, facendo un doppio controllo con un esempio dal vivo, Cisco ha creato un sito web dedicato a determinare questa situazione non appena la pagina viene caricata. Fare clic qui o digitare https://InternetBadGuys.com nella barra del browser.

Se Umbrella è configurato correttamente, sarete accolti da uno schermo simile a questo!



Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco

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).