

Configurando o Cisco Umbrella em sua rede via roteadores série RV34x

Introduction

A partir da versão do firmware 1.0.0.2.16, os roteadores da série RV34x agora suportam o Cisco Umbrella. A Umbrella usa o DNS como um vetor ou escudo de defesa contra malware e invasões de dados.

Dispositivos aplicáveis

- RV34x Series Router

Versão de software

- 1.0.02.16

Requirements

- Uma conta guarda-chuva ativa (não tem uma? [Solicite um orçamento](#) ou inicie uma [avaliação gratuita](#))

Objetivo

Este guia mostra as etapas envolvidas na integração da plataforma de segurança da Umbrella na sua rede. Antes de falarmos sobre os detalhes gerais, responderemos a algumas perguntas que você pode estar se fazendo sobre o Umbrella.

O que é guarda-chuva?

A Umbrella é uma plataforma de segurança de nuvem simples, mas muito eficaz, da Cisco. A Umbrella opera na nuvem e executa muitos serviços relacionados à segurança. Da ameaça emergente à investigação pós-evento. O Umbrella detecta e impede ataques em todas as portas e protocolos.

Como funciona?

O Umbrella usa o DNS como seu principal vetor de defesa. Quando os usuários inserem uma URL na barra do navegador e pressionam Enter, o Umbrella participa da transferência. Essa URL passa para o resolvidor DNS da Umbrella e, se um aviso de segurança estiver associado ao domínio, a solicitação será bloqueada. Essa telemetria transfere dados e é analisada em microssegundos, praticamente sem latência. Os dados de telemetria usam logs e instrumentos para rastrear bilhões de solicitações de DNS em todo o mundo. Quando esses dados estão difundidos, correlacioná-los em todo o mundo permite uma resposta

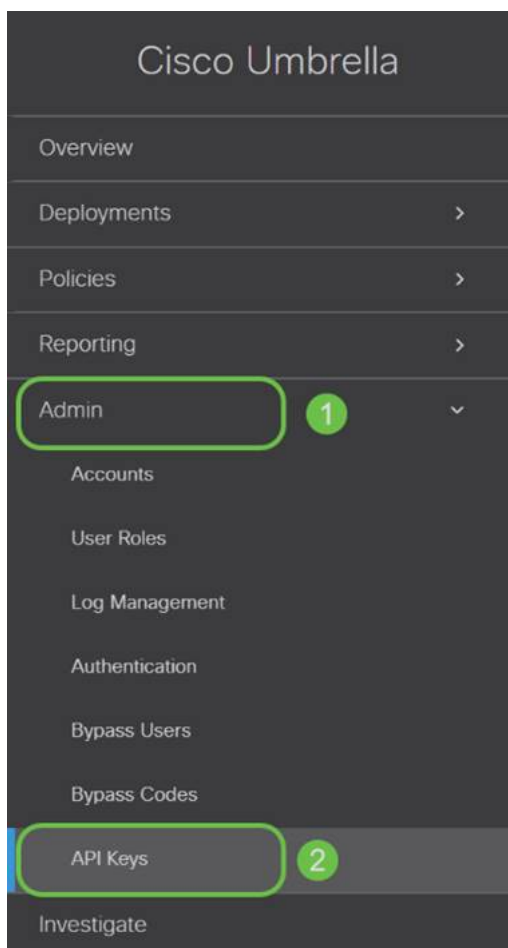
rápida aos ataques no início. Consulte a política de privacidade da Cisco aqui para obter mais informações - [política completa, versão resumida](#). Pense nos dados de telemetria como dados derivados de ferramentas e registros.

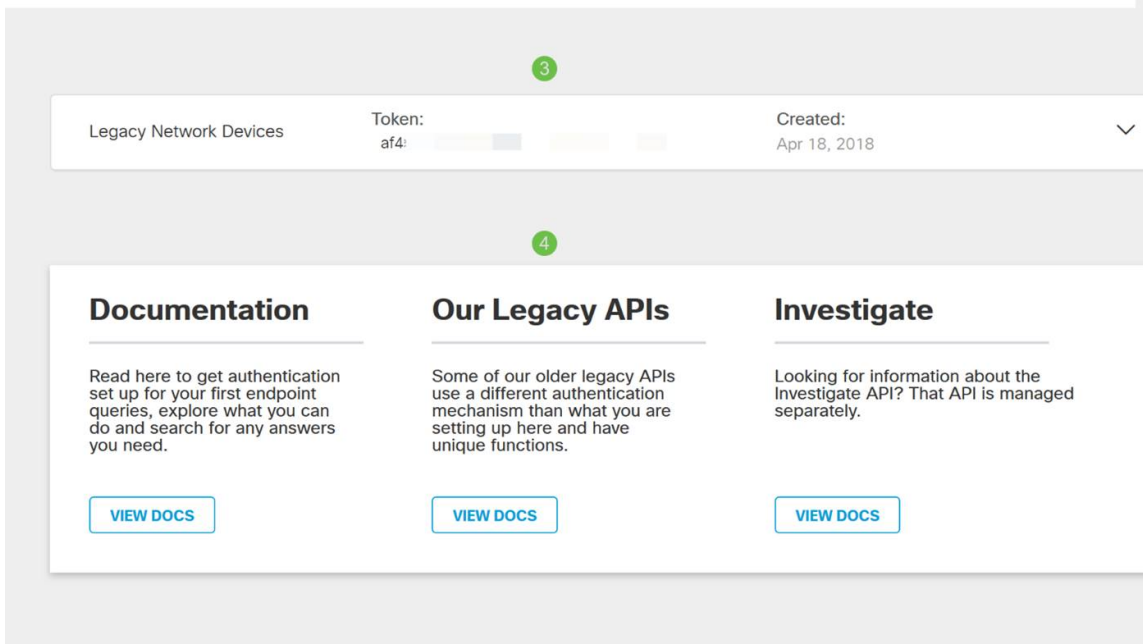
Para resumir em uma metáfora, imagine que você está em uma festa. Nesta festa, todos estão ao telefone navegando na Web. O silêncio em grupo é pontuado pelos participantes da festa tocando em suas telas. [Não é uma festa ótima](#), mas, enquanto você está em seu próprio telefone, você vê um hiperlink para um GIF de gatinho que parece irresistível. No entanto, a URL parece questionável, portanto, você não sabe se deve tocar ou não. Então, antes de tocar no hiperlink, você grita para o resto da festa "Esse link não funciona bem?" Se outra pessoa na festa estivesse no link e descobrisse que era uma fraude, gritaria "Sim, eu fiz e é uma fraude!" Você agradece a essa pessoa por salvá-lo, continuando sua nobre busca por fotos de animais bonitos. É claro que, na escala da Cisco, esse tipo de solicitação e verificações de segurança de retorno de chamada estão ocorrendo milhões de vezes por segundo, e isso é para o benefício da segurança em sua rede.

Parece ótimo, como vamos começar isso?

Onde este guia está navegando, o começa pegando a chave de API e a chave secreta do painel da conta Umbrella. Depois, faremos login no dispositivo do roteador para adicionar a API e a chave secreta. Se tiver algum problema, [verifique a documentação aqui](#) e [as opções de suporte do Umbrella](#).

Etapa 1. Depois de fazer login na sua conta Umbrella, na tela *Dashboard*, clique em **Admin > API Keys**.

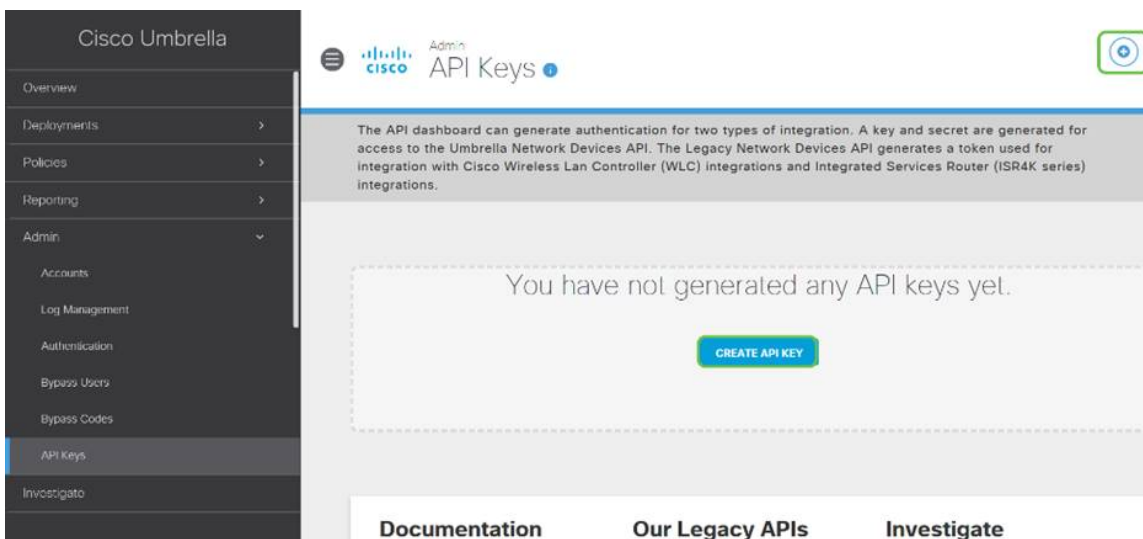




Anatomia da tela de chaves de API (com chave de API preexistente) -

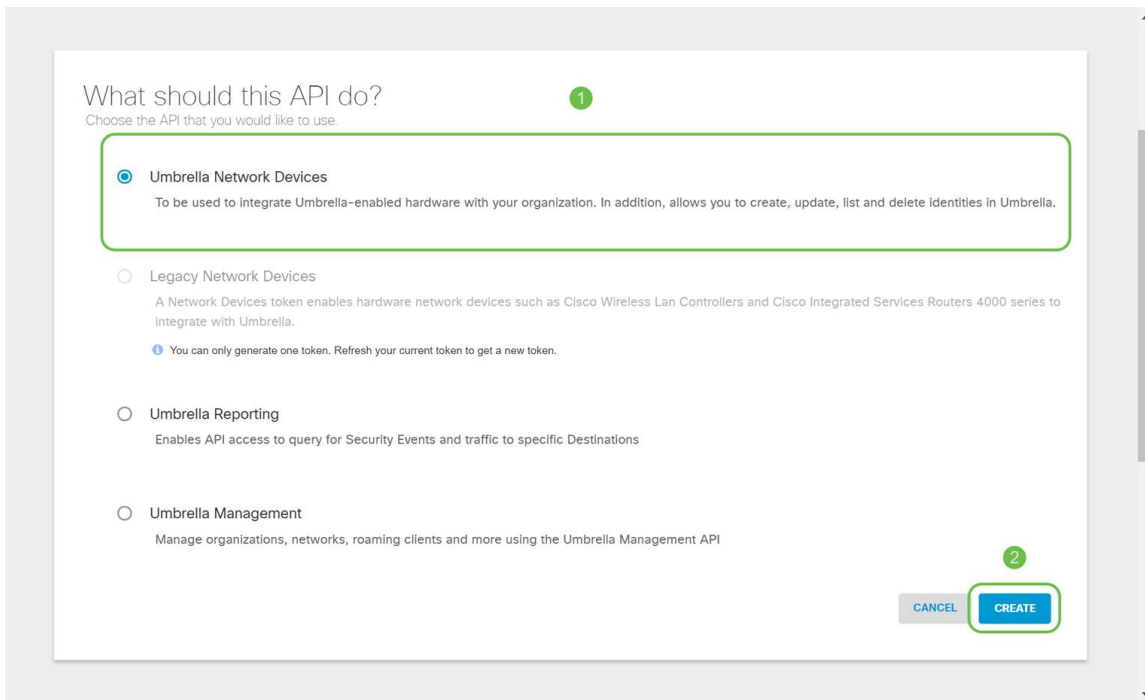
1. Adicionar chave de API - Inicia a criação de uma nova chave para uso com a API Umbrella.
2. Informações adicionais - desliza para baixo/para cima com um explicador para esta tela.
3. Compartimento Token - Contém todas as chaves e tokens criados por esta conta. (Preenche quando uma chave é criada)
4. Documentos de suporte - Links para a documentação no site do Umbrella referente aos tópicos em cada seção.

Etapa 2. Clique no botão **Add API Key** no canto superior direito ou no botão **Create API Key**. Ambos funcionam da mesma forma.

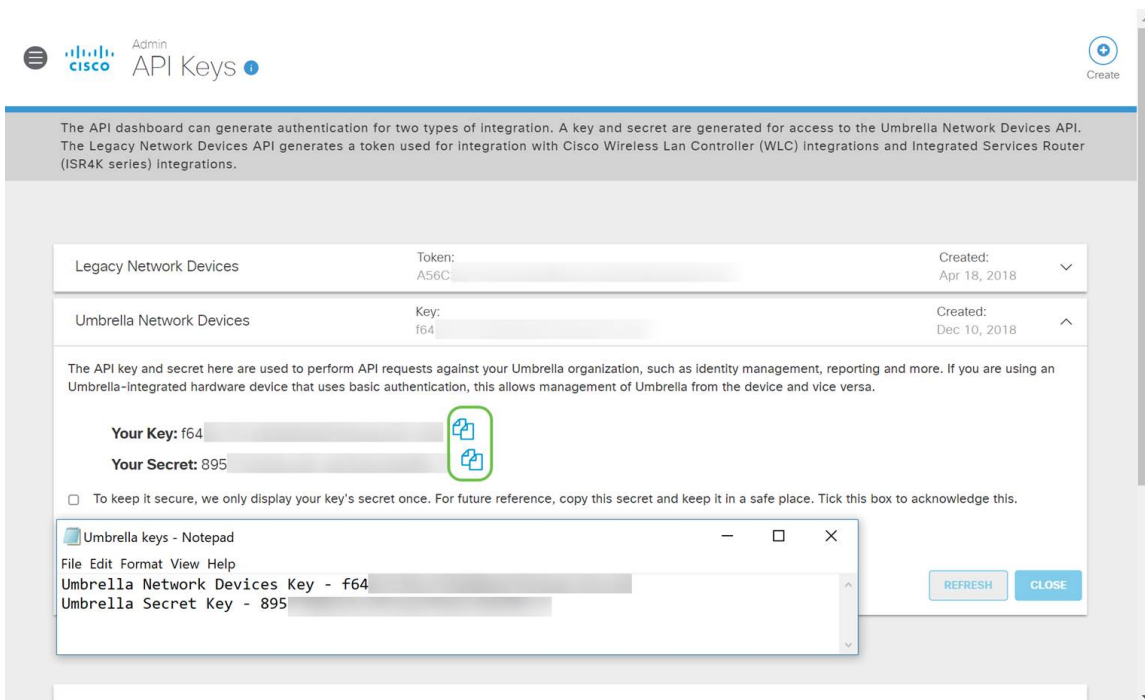


Note: a captura de tela acima seria semelhante ao que você veria abrindo este menu pela primeira vez.

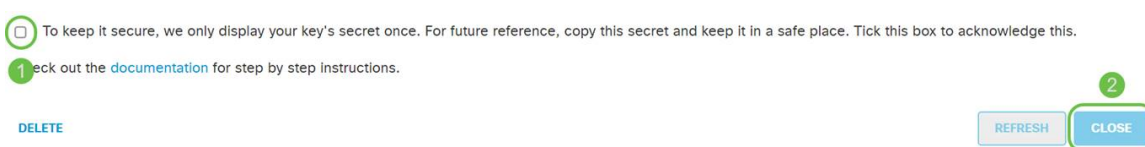
Etapa 3. Selecione **Umbrella Network Devices** e clique no botão **Create**.



Etapa 4. Abra um editor de texto, como o notepad, e clique no botão **Copy** à direita da sua API e da *chave secreta da API*. Uma notificação pop-up confirmará que a chave foi copiada para a área de transferência. Cole seu segredo e a chave de API no documento, rotulando-os para referência futura. Nesse caso, seu rótulo é "Umbrella network devices key". Em seguida, salve o arquivo de texto em um local seguro e de fácil acesso posteriormente.



Etapa 5. Depois de copiar a chave e a chave secreta para um local seguro, na tela *Umbrella API*, clique na **caixa de seleção** para confirmar a exibição temporária da chave secreta e clique no botão **Fechar**.



Nota importante: Se você perder ou acidentalmente excluir a chave secreta, não haverá função ou número de suporte para ligar para recuperar essa chave. [Mantenha em segredo, em segurança](#). Se perder, você precisará excluir a chave e autorizar novamente a nova

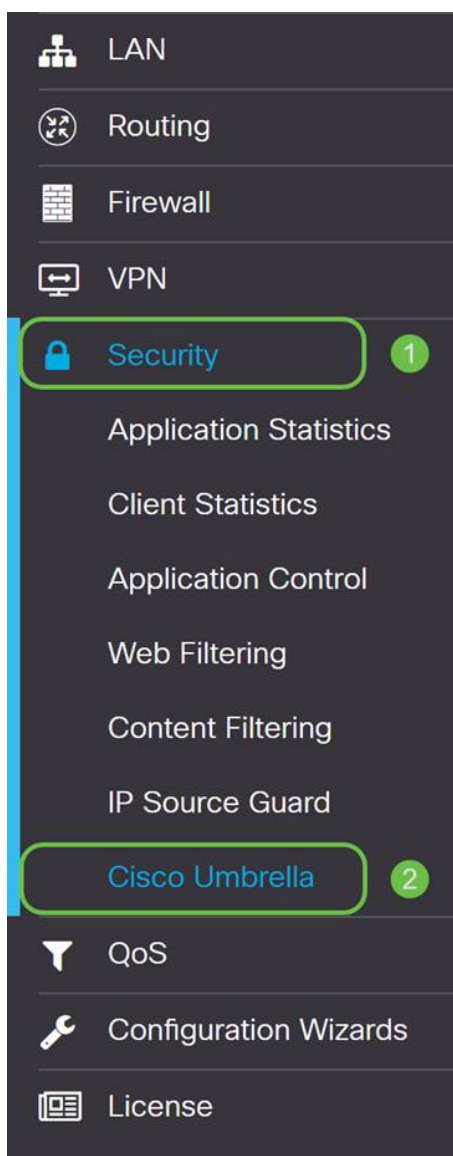
chave de API com cada dispositivo que deseja proteger com o Umbrella.

Prática recomendada: Mantenha apenas uma *única* cópia deste documento em um dispositivo, como um pen drive USB, inacessível de qualquer rede.

Configurando o Umbrella em seu dispositivo RV34x

Agora que criamos chaves de API no Umbrella, vamos pegá-las e instalá-las em nossos dispositivos RV34x. No nosso caso, estamos usando um RV340.

Etapa 1. Depois de fazer login no seu dispositivo RV34x, clique em **Security > Umbrella** no menu da barra lateral.



Etapa 2. A tela da API do Umbrella tem uma variedade de opções, comece a ativar o Umbrella clicando na caixa de seleção **Habilitar**.



Cisco Umbrella

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

- Enable
- Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
 - Go to [DNS-O-MATIC](#) website, create an account and add your OpenDNS account to it.
 - Go to [DNS-O-MATIC Settings](#) to enable DNS-O-MATIC so your WAN IP change can be propagated to O

Advanced Configuration

Local Domain To Bypass
(Optional):



DNSEncrypt:

Enable

Public Key:

B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8

- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Etapa 3. (Opcional) Por padrão, a caixa Block LAN DNS Queries (Bloquear consultas de DNS da rede local) está selecionada. Esse recurso limpo cria automaticamente listas de controle de acesso no roteador, o que impedirá que o tráfego de DNS saia para a Internet. Este recurso força todas as solicitações de tradução de domínio a serem direcionadas através do RV34x e é uma boa ideia para a maioria dos usuários.

Etapa 4. A próxima etapa é executada de duas maneiras diferentes. Ambos dependem da configuração da sua rede. Se você usar um serviço como DynDNS ou NoIP, você deixará o esquema de nomenclatura padrão de "Rede". Em seguida, você precisará fazer login nessas contas para garantir que o Umbrella faça interface com esses serviços, pois ele oferece proteção. Para nossos propósitos, estamos confiando em "Dispositivo de rede", clique no botão de opção inferior.

Cisco Umbrella

Apply

Cancel

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

- Enable
- Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Getting Started

Etapa 5. Agora clique em **Introdução** para iniciar o miniassistente.

Cisco Umbrella

Apply

Cancel

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

- Enable
- Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Getting Started

Etapa 6. Agora, insira a **chave de API** e a **chave secreta** nas caixas de texto.

Enter Credentials

Key:

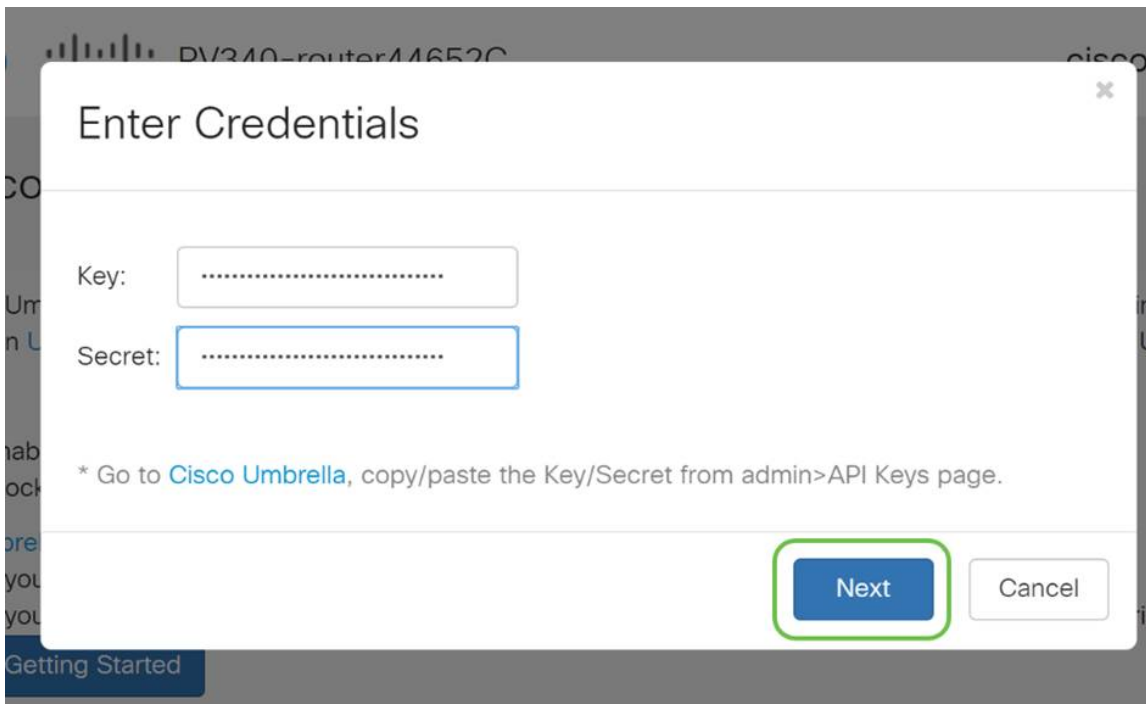
Secret:

* Go to [Cisco Umbrella](#), copy/paste the Key/Secret from admin>API Keys page.

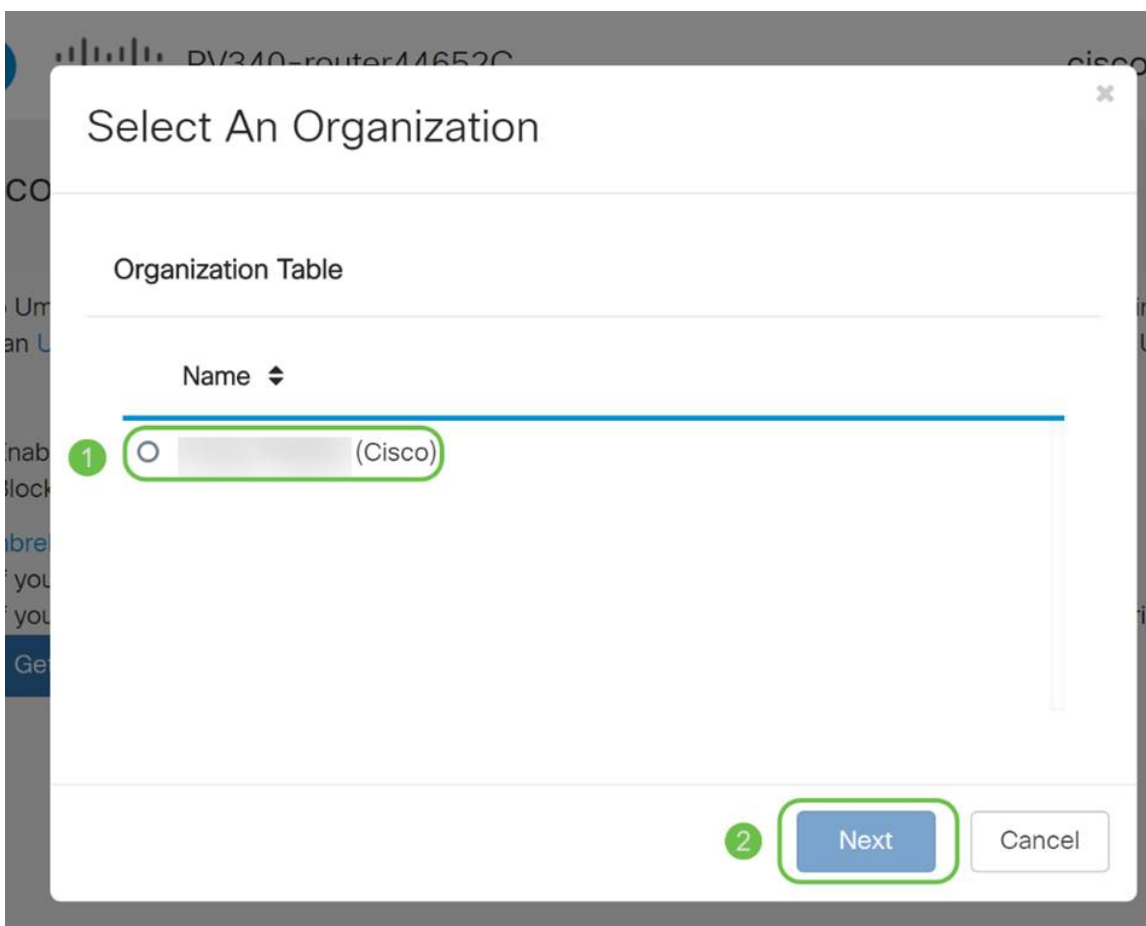
Next

Cancel

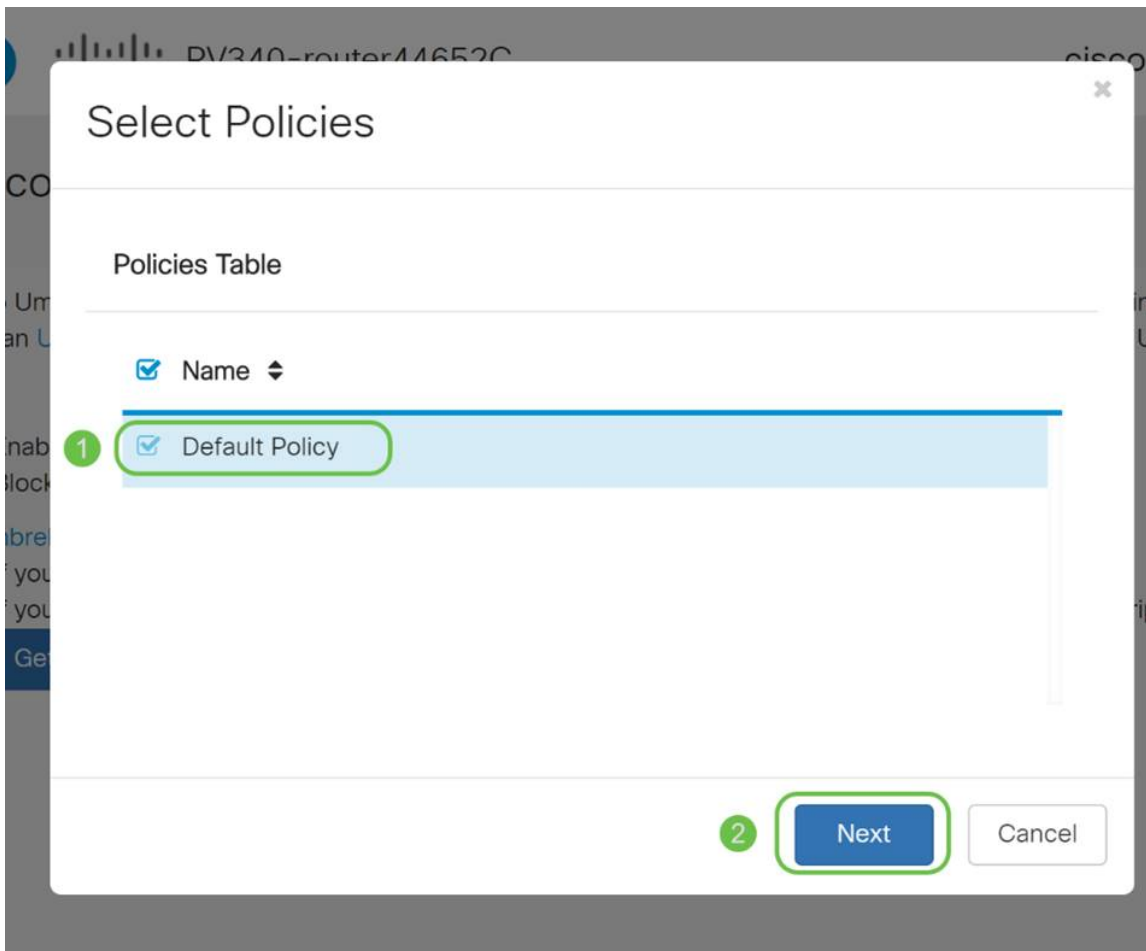
Etapa 7. Depois de inserir a API e a chave secreta, clique no botão **Next**.



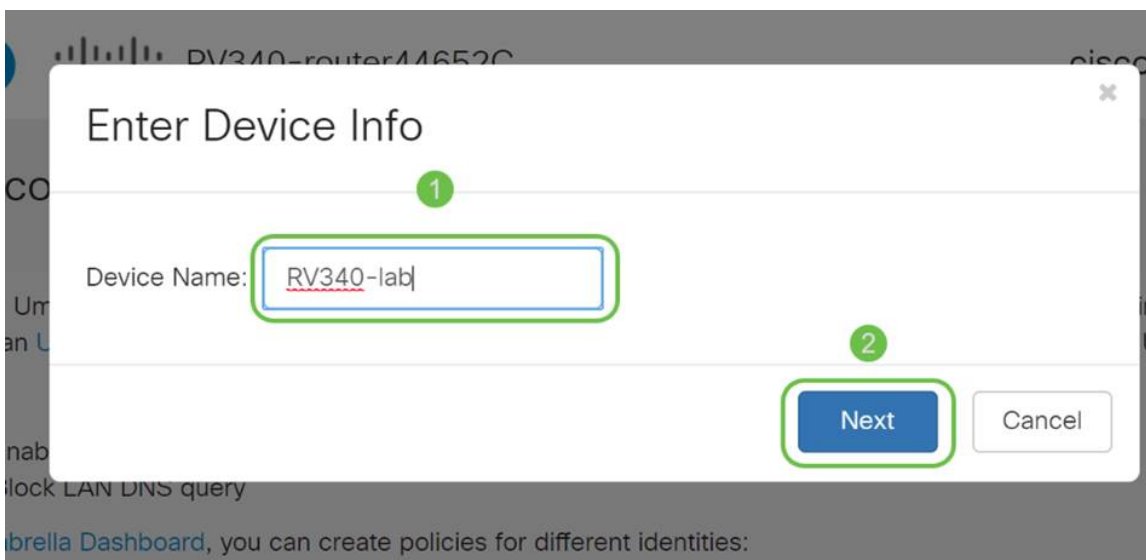
Etapa 8. Na próxima tela, selecione a **organização** que deseja associar ao roteador e clique em **Avançar**.



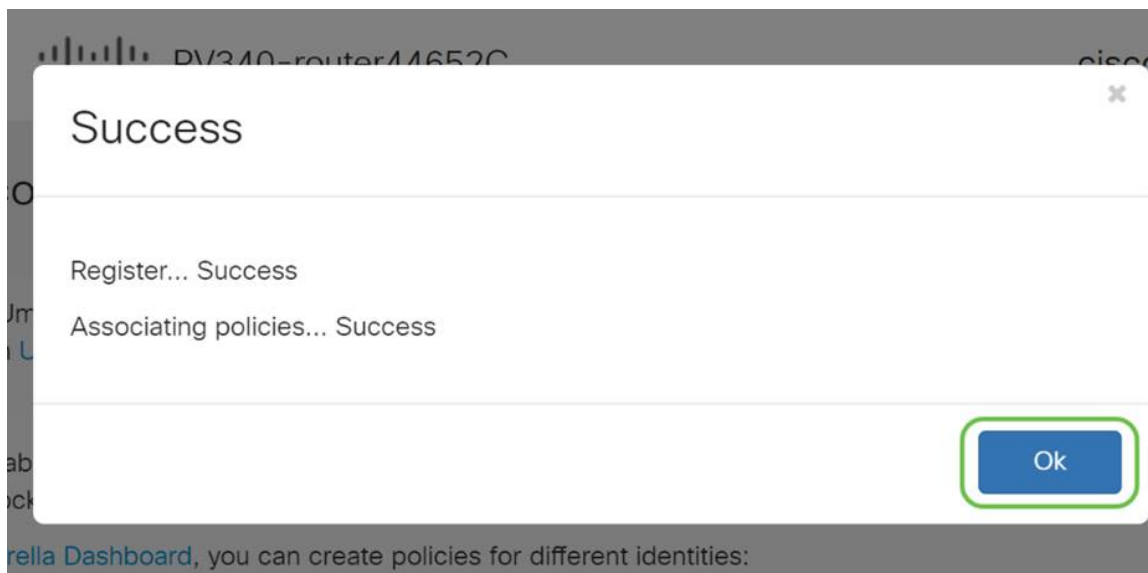
Etapa 9. Agora, selecione a política a ser aplicada ao tráfego roteado pelo RV34x. Para a maioria dos usuários, a política padrão fornecerá cobertura suficiente.



Etapa 10. **Atribua um nome** ao dispositivo para que ele possa ser designado nos relatórios do Umbrella. Em nossa configuração, atribuímos "RV340-lab".



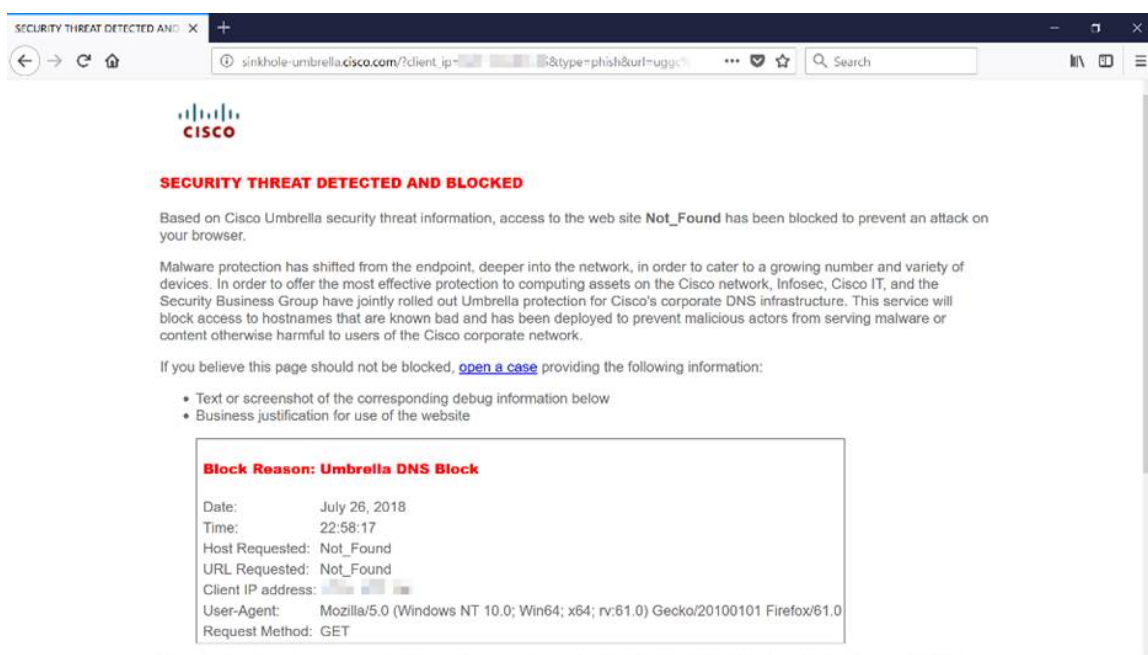
Etapa 11. A próxima tela validará as configurações escolhidas e fornecerá uma atualização; quando associada com êxito, clique em **OK**.



Confirmando que tudo está no lugar certo

Parabéns, agora você está protegido pelo Umbrella da Cisco. Ou você está? Vamos ter certeza, verificando duas vezes com um exemplo ao vivo, que a Cisco criou um site dedicado a determinar isso tão rapidamente quanto a página é carregada. [Clique aqui](#) ou digite <https://InternetBadGuys.com> na barra do navegador.

Se o Umbrella estiver configurado corretamente, você será recebido por uma tela semelhante a esta!



Exibir um vídeo relacionado a este artigo...

[Clique aqui para ver outras palestras técnicas da Cisco](#)

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.