Como: Guarda-chuva de alargamento de Cisco para proteger sua rede Wireless

Introdução

A segurança de dados é um esforço de grupo em cada organização. Os empregados são pelo menos para segurança em parte responsável eles não caem rapina aos embustes. Na prática, a Segurança é resistente e não é nenhuma maravilha porque. Porque as ferramentas da tecnologia expandem mesmas vão para os avanços do hacker, todos os barcos aumentam com a maré por assim dizer. Lido sobre para aprender como integrar a proteção do guarda-chuva em seu LAN.

Objetivo

Isto como guiar mostrar-lhe-á as etapas envolvidas na plataforma de segurança do guarda-chuva de integração em sua rede Wireless. Antes que nós obtenhamos nos detalhes do âmago nós responderemos a algumas perguntas que você pode se perguntar sobre o guarda-chuva.

Dispositivos aplicáveis

- WAP125
- WAP581

Versão de software

- 1.0.1

Requisitos

Uma conta ativa do guarda-chuva (não tenha um? Peça umas citações ou comece uma versão de avaliação gratuita)

Que é guarda-chuva?

O guarda-chuva é uma plataforma de segurança simples contudo muito eficaz da nuvem de Cisco. O guarda-chuva opera-se na nuvem e executa-se muitos serviços relativos à segurança. Da ameaça emergente para afixar a investigação do evento. O guarda-chuva descobre e impede ataques através de todas as portas e protocolo.

Como trabalha?

O guarda-chuva usa o DNS como seu vetor principal para a defesa. Quando os usuários incorporam uma URL a sua barra do navegador e a batida entra, o guarda-chuva participa em transferência. Essa URL passa ao solucionador DNS do guarda-chuva, e se um aviso da Segurança associa com o domínio, ao pedido é obstruída. Transferências de dados desta telemetria e são analisadas nos microssegundos, não adicionando quase nenhuma latência. Logs e instrumentos dos usos de dados da telemetria que seguem biliões de pedidos DNS no mundo inteiro. Quando estes dados são patentes, correlacioná-los através do globo permite a resposta

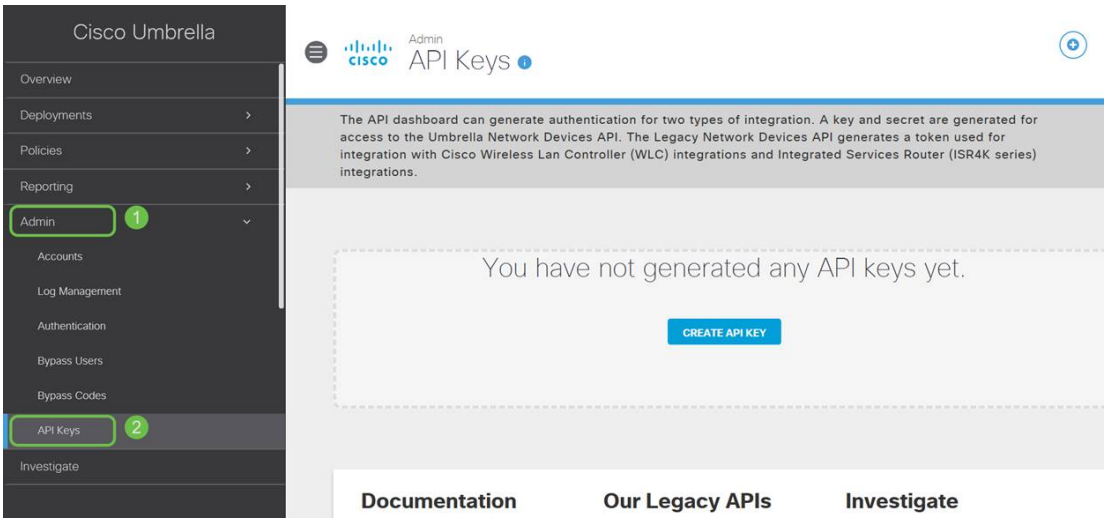
rápida aos ataques enquanto começam. Veja a política de privacidade de Cisco aqui para mais informação - política completa, versão sumária. Pense dos dados da telemetria como os dados derivados das ferramentas e dos logs.

Para resumir em uma metáfora, imagine que você está em um partido. Neste partido todos está em seu telefone que surfa a Web. O grupo-silêncio quieto é interrompido pelos partido-frequentadores que batem afastado em suas telas. Não é um grande partido, mas quando em seu próprio telefone você vir um hiperlink a um gatinho GIF que pareça irresistível. Porém você é incerto de se você bater ou não, porque a URL parece duvidosa. Assim antes que você bata o hiperlink, você grito para fora ao resto do partido “é este mau do link?” Se uma outra pessoa no partido foi ao link e descoberto lhe era um embuste, parte traseira do grito “yeah, eu fiz e é um embuste!” Você agradece a essa pessoa salvar o, continuando sua procura para imagens de animais bonitos no silêncio. Naturalmente, na escala de Cisco este tipo de verificações de segurança do pedido e da rechamada é milhões de ocorrência de épocas um o segundo.

Soamos grandes, como nós retrocedemos isto fora?

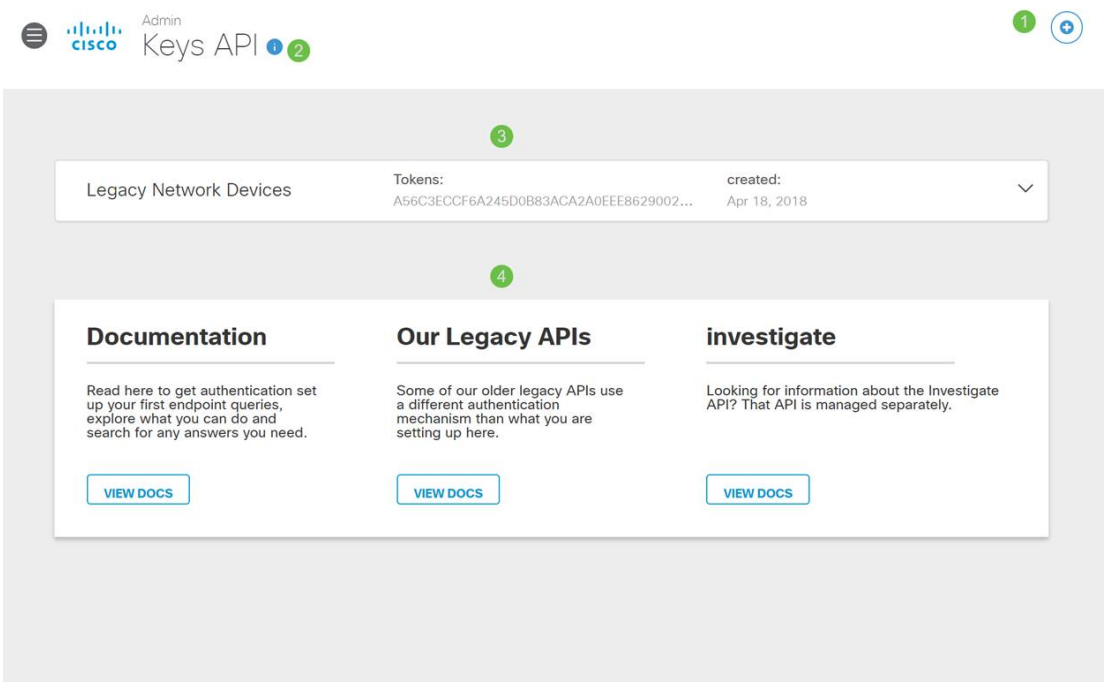
Onde este guia está navegando, começa agarrando a chave e a chave secreta API de seu painel da conta do guarda-chuva. Após, nós registraremos em seu dispositivo WAP para adicionar o API e a chave secreta. Se você é executado em quaisquer edições, verificação aqui para a documentação, e aqui para opções do apoio do guarda-chuva.

Etapa1. Após o registro em sua conta do guarda-chuva, da tela do *painel* clique sobre **Admin > chaves API**.

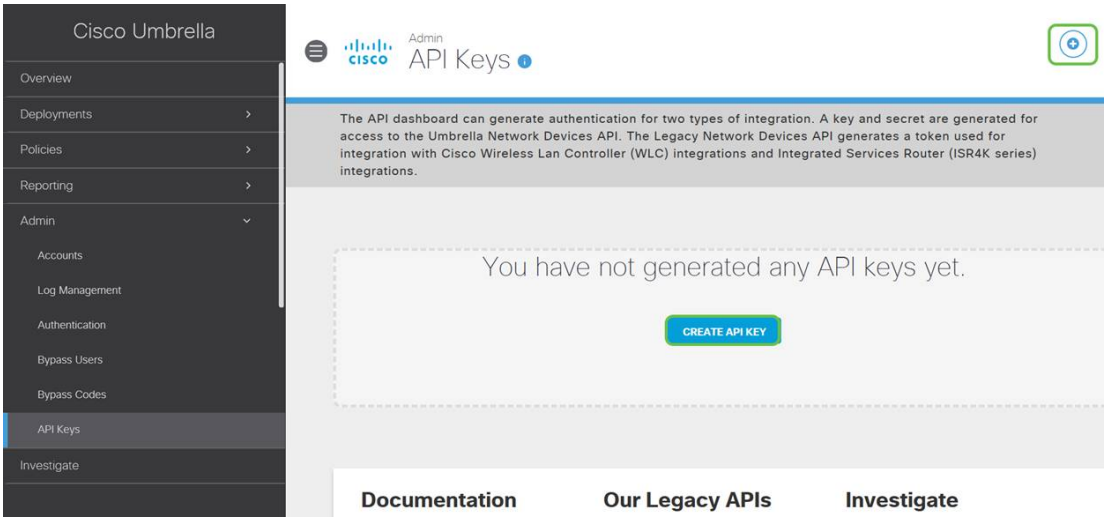


A anatomia do API fecha a tela -

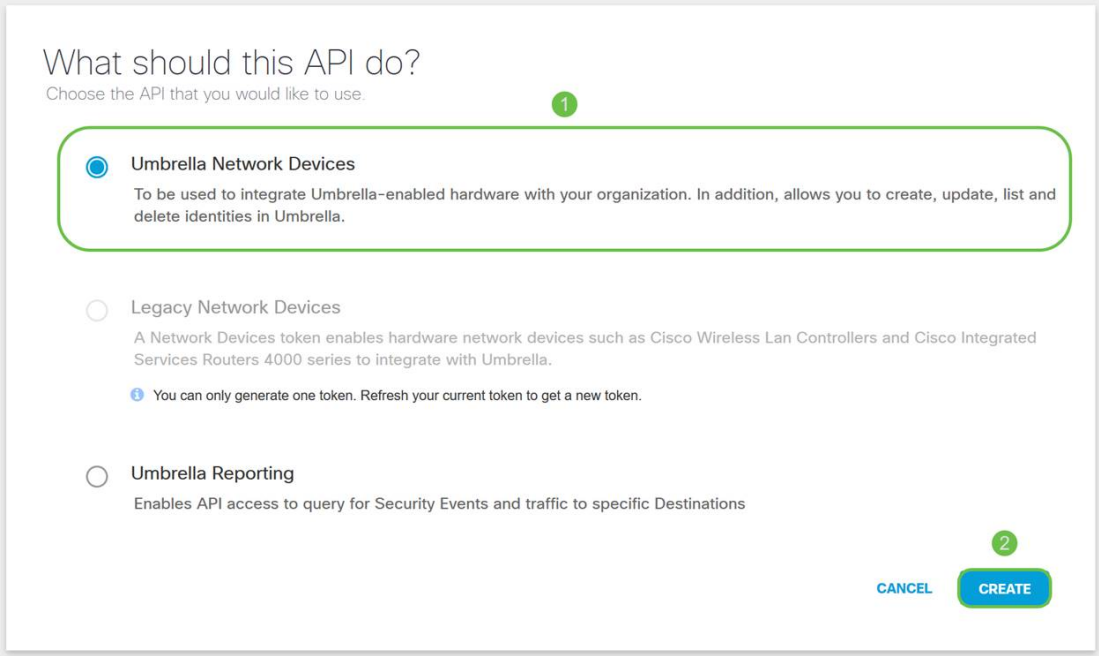
1. *Adicionar a chave API* - Inicia a criação de uma chave nova para o uso com o guarda-chuva API.
2. *Informação adicional* - Desliza down/up com uma explicação para esta tela.
3. *Poço do token* - Contém todas as chaves e tokens criados por esta conta. (Povoa uma vez que uma chave foi criada)
4. *Documentos de suporte* - Os links à documentação no guarda-chuva situam referir-se os assuntos em cada seção.



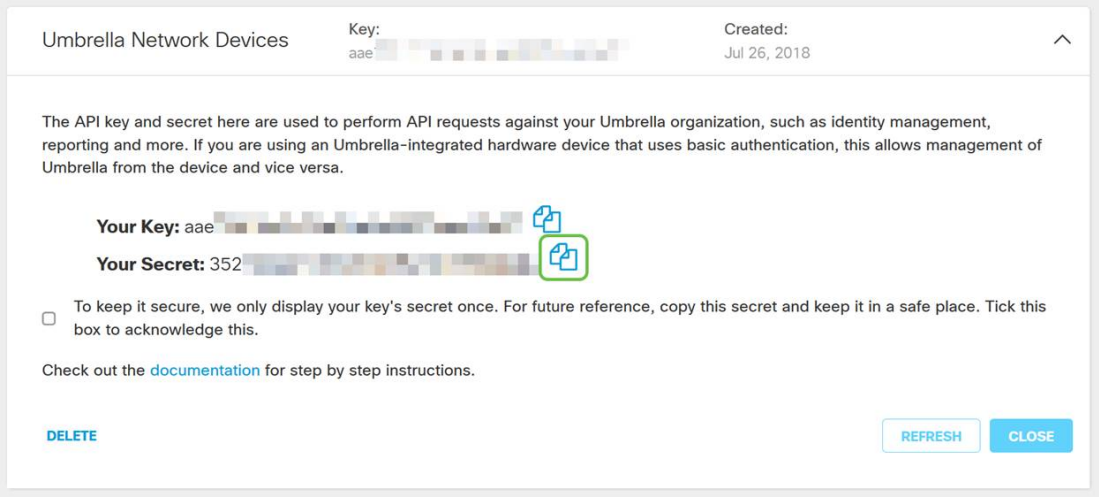
Etapa 2. Clique sobre o botão da **chave adicionar API no** canto superior-direito da mão, ou clique o botão da **chave da criação API**. Eles ambos função o mesmos.



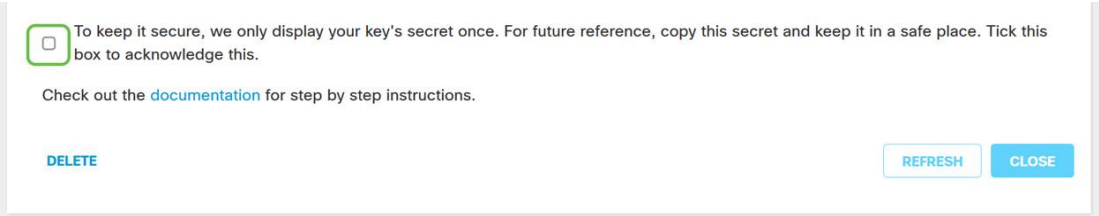
Etapa 3. Selecione **dispositivos de rede do guarda-chuva** e clique então o **botão Create**.



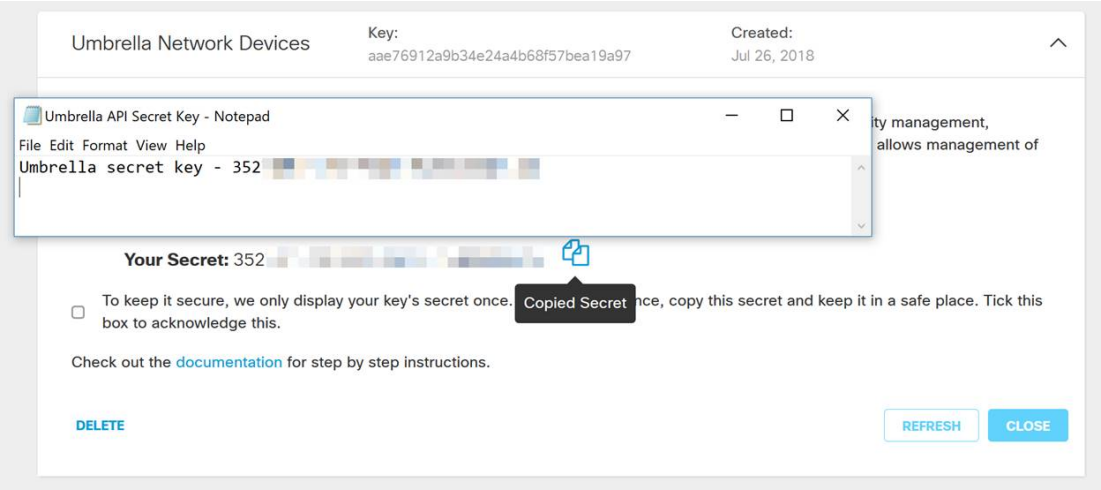
Etapa 4. Clique o **botão Copy Button** à direita de sua *chave secreta, uma* notificação do PNF- acima confirmará a chave é copiado a sua prancheta.



Depois que você copiou a chave e a chave secreta a um local segura, clique a ***caixa de seleção*** para confirmar para terminar o reconhecimento a seguir clique o **botão Close Button**.



Etapa 5. Abra um editor de texto tal como o bloco de notas e cole seu segredo e a chave API no documento, etiqueta-os para a referência futura. Neste caso sua etiqueta é do “chave secreta guarda-chuva”. Inclua a chave API com sua chave secreta junto com uma descrição breve de seu uso neste mesmo arquivo de texto. Salvar então o arquivo de texto a um lugar seguro que esteja mais atrasado de fácil acesso se você precisar.



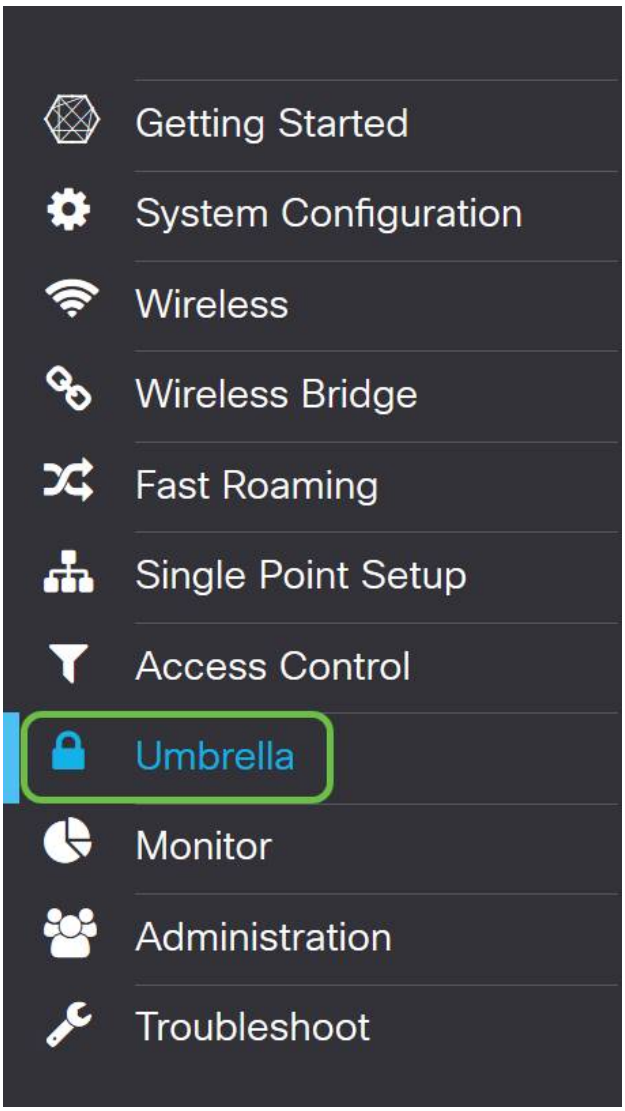
Nota importante: Se você perde ou acidentalmente não suprime da chave secreta lá é nenhum função ou número do apoio para chamar para recuperar esta chave. Mantenha-a segredo, mantenha-a segura. Se perdido, você precisará de suprimir da chave e re-de autorizar a chave API com cada dispositivo que WAP você deseja proteger com guarda-chuva.

Melhor prática: Mantenha apenas uma *cópia única d*este documento em um dispositivo, como uma movimentação do polegar USB, inacessível de toda a rede.

Configurando o guarda-chuva em seu dispositivo WAP

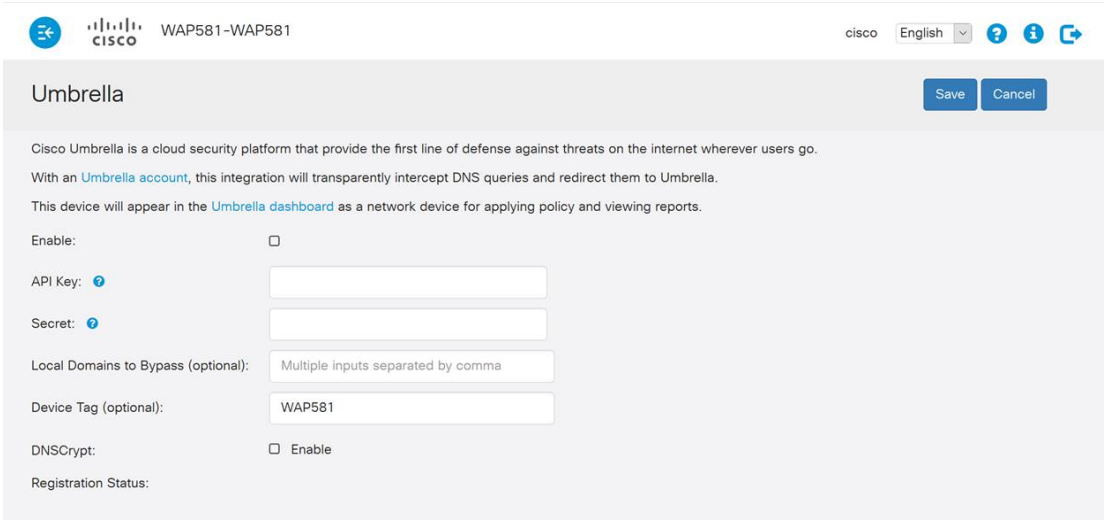
Agora que nós criamos chaves API dentro do guarda-chuva, nós tomaremos aquelas chaves e instalá-las-emos em nossos dispositivos WAP. Em nosso caso nós estamos usando um WAP581.

Etapa1. Após o registro em seu dispositivo WAP, clique sobre o **guarda-chuva no** menu do sidebar.

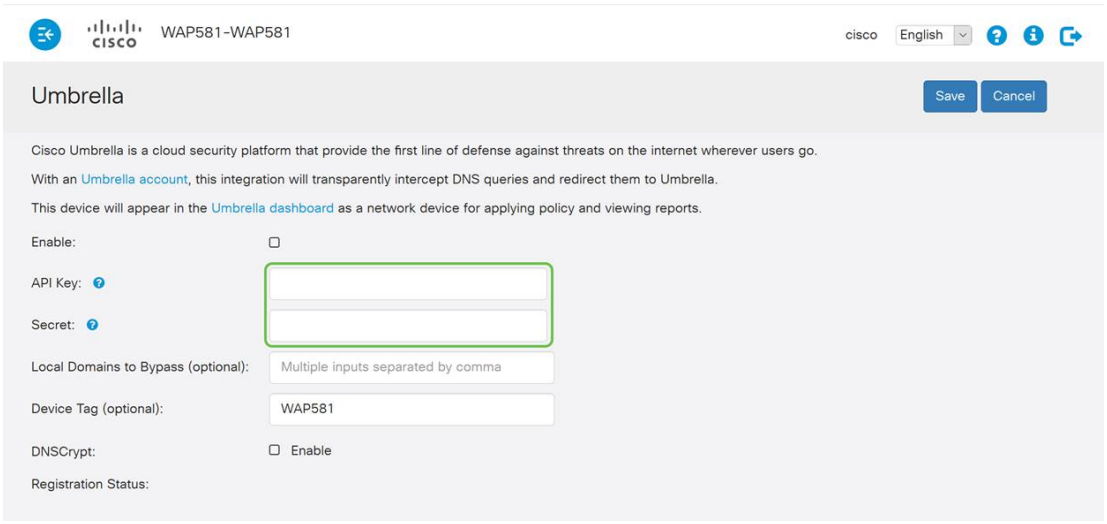


Etapa 2. A tela do guarda-chuva é direta, mas há um valor de dois campos que define aqui:

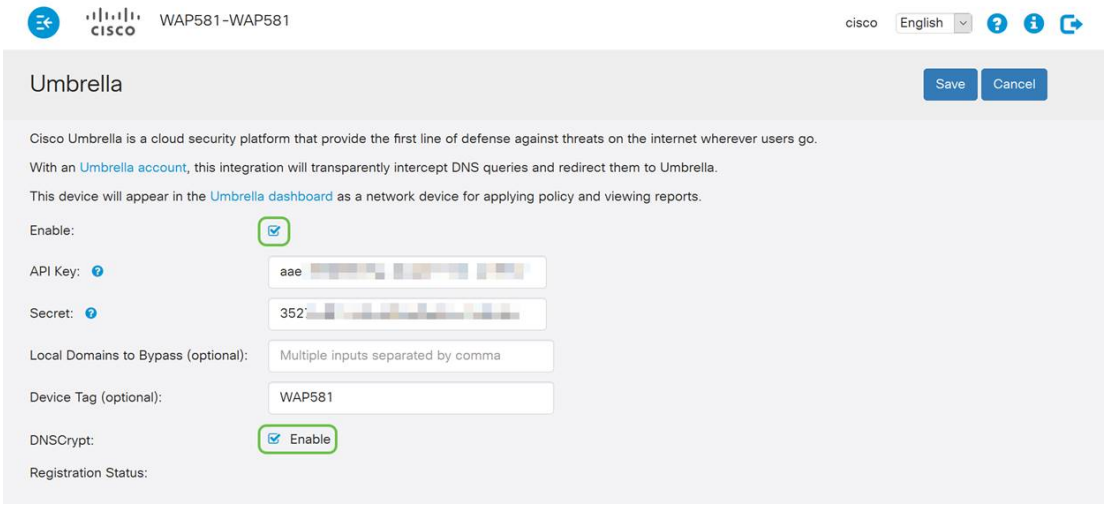
- *Domínios locais a contornear* - Este campo contém seus domínios internos que você gostaria de ser excluído do serviço do guarda-chuva.
- *DNSCrypt* - Fixa transferência dos pacotes entre o cliente de DNS e o solucionador DNS. Esta característica está ligada à revelia, desabilitando esta característica fará sua rede menos segura.



Etapa 3. Cole seus API e chave secreta nos campos correspondentes

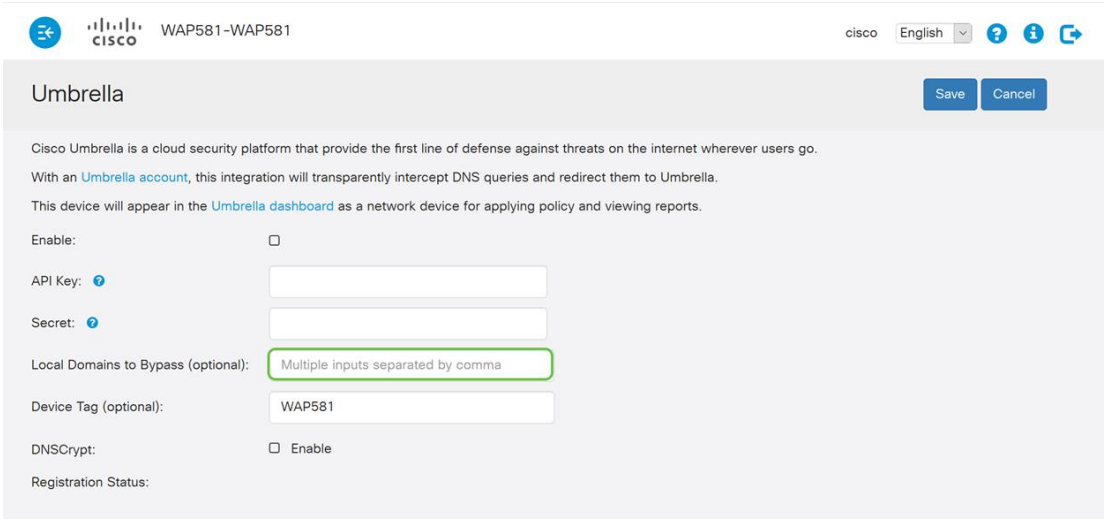


Etapa 4. Assegure-se de que as caixas de seleção para **Enable** e **DNSCrypt** estejam firmadas o estado da verificação.



Nota: DNSCrypt fixa uma comunicação DNS entre um cliente de DNS e um solucionador DNS. O padrão é permitido.

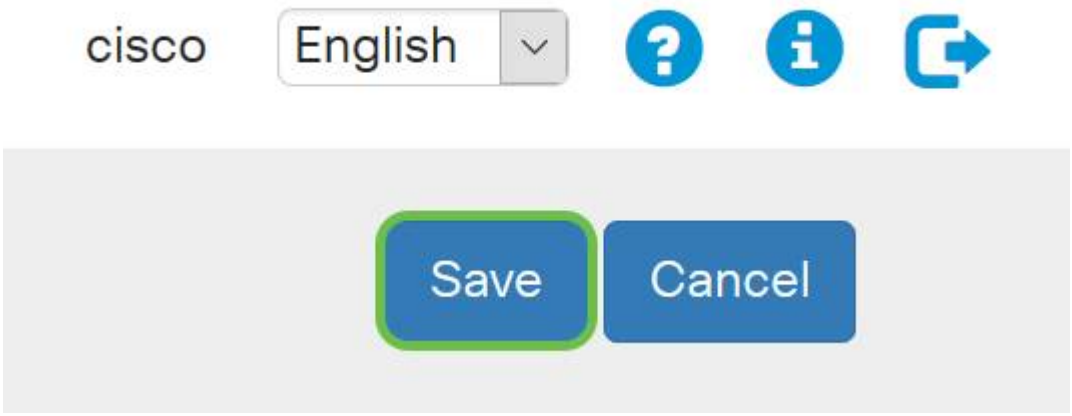
Etapa 5. (opcional) entra nos domínios locais que você gostaria do guarda-chuva de permitir com o processo da resolução de DNS.



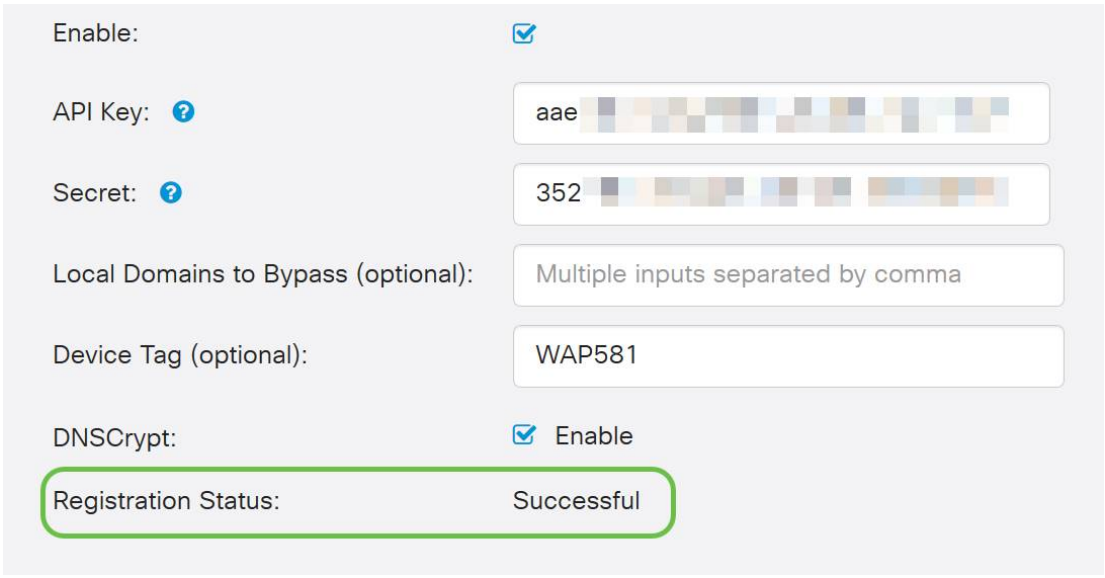
Nota: Isto é exigido para todos os domínios do intranet e domínios do DNS em divisão. Se sua rede exige o uso de domínios da área local distribuindo, você precisará de contactar o apoio do

guarda-chuva para obter esta característica em serviço. A maioria de usuários não precisarão de usar esta opção.

Etapa 6. Depois que você é satisfeito com as mudanças ou adicionou seus próprios *domínios locais para contornear*, clique o **botão Save Button no** canto superior-direito da mão.



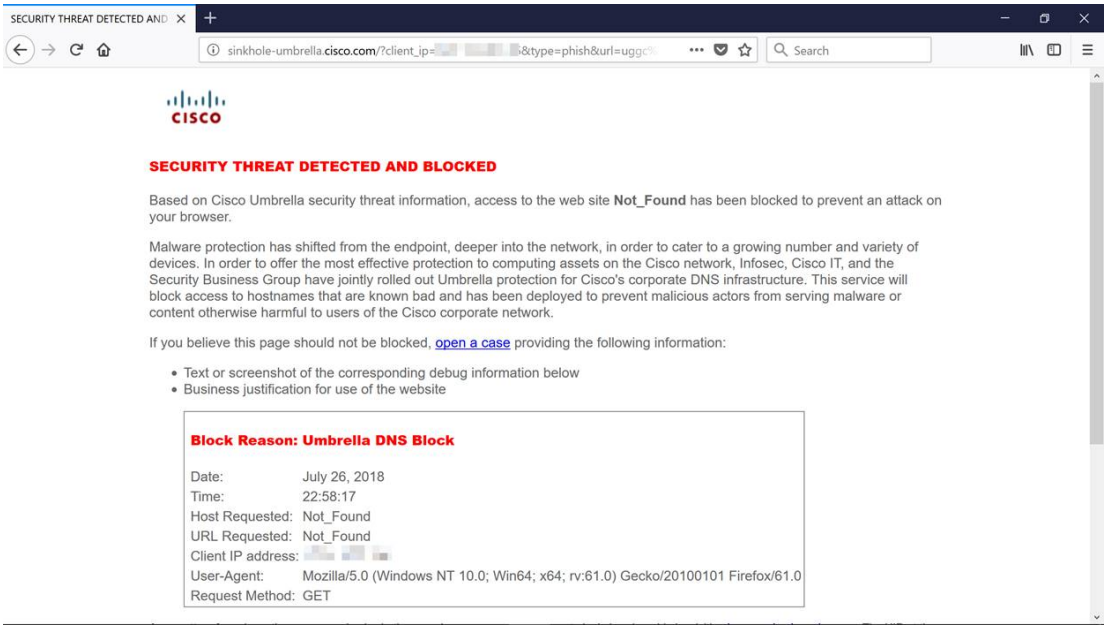
Passo 7. Quando as mudanças estão completas, o *status de registro do* campo lerá “bem sucedido”.



Confirmar tudo está em seu local correto

Felicitações, você é agora o guarda-chuva de Cisco protegido. Ou é você? Deixe-nos ser certos, Cisco criou um Web site dedicado a determinar isto tão rapidamente quanto as cargas da página. Clique aqui ou datilografe https://InternetBadGuys.com na barra do navegador.

Se o guarda-chuva é configurado corretamente você estará cumprimentado por uma tela similar a esta!


SECURITY THREAT DETECTED AND
sinkhole-umbrella.cisco.com/?client_ip=
&type=phish&url=ugg
Search
CISCO
SECURITY THREAT DETECTED AND BLOCKED
Based on Cisco Umbrella security threat information, access to the web site Not_Found has been blocked to prevent an attack on your browser.
Malware protection has shifted from the endpoint, deeper into the network, in order to cater to a growing number and variety of devices. In order to offer the most effective protection to computing assets on the Cisco network, Infosec, Cisco IT, and the Security Business Group have jointly rolled out Umbrella protection for Cisco's corporate DNS infrastructure. This service will block access to hostnames that are known bad and has been deployed to prevent malicious actors from serving malware or content otherwise harmful to users of the Cisco corporate network.
If you believe this page should not be blocked, open a case providing the following information:
Text or screenshot of the corresponding debug information below
Business justification for use of the website
Block Reason: Umbrella DNS Block
Date: July 26, 2018
Time: 22:58:17
Host Requested: Not_Found
URL Requested: Not_Found
Client IP address:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Request Method: GET