Configure SWG Policies for Umbrella

Contents

Introduction

Background Information

Umbrella Web Policies

- Important Notes About Cloud Delivered Firewall and SWG
- Important Notes About Roaming Security Module Policies

Introduction

This document describes how to configure web policies for use with Umbrella.

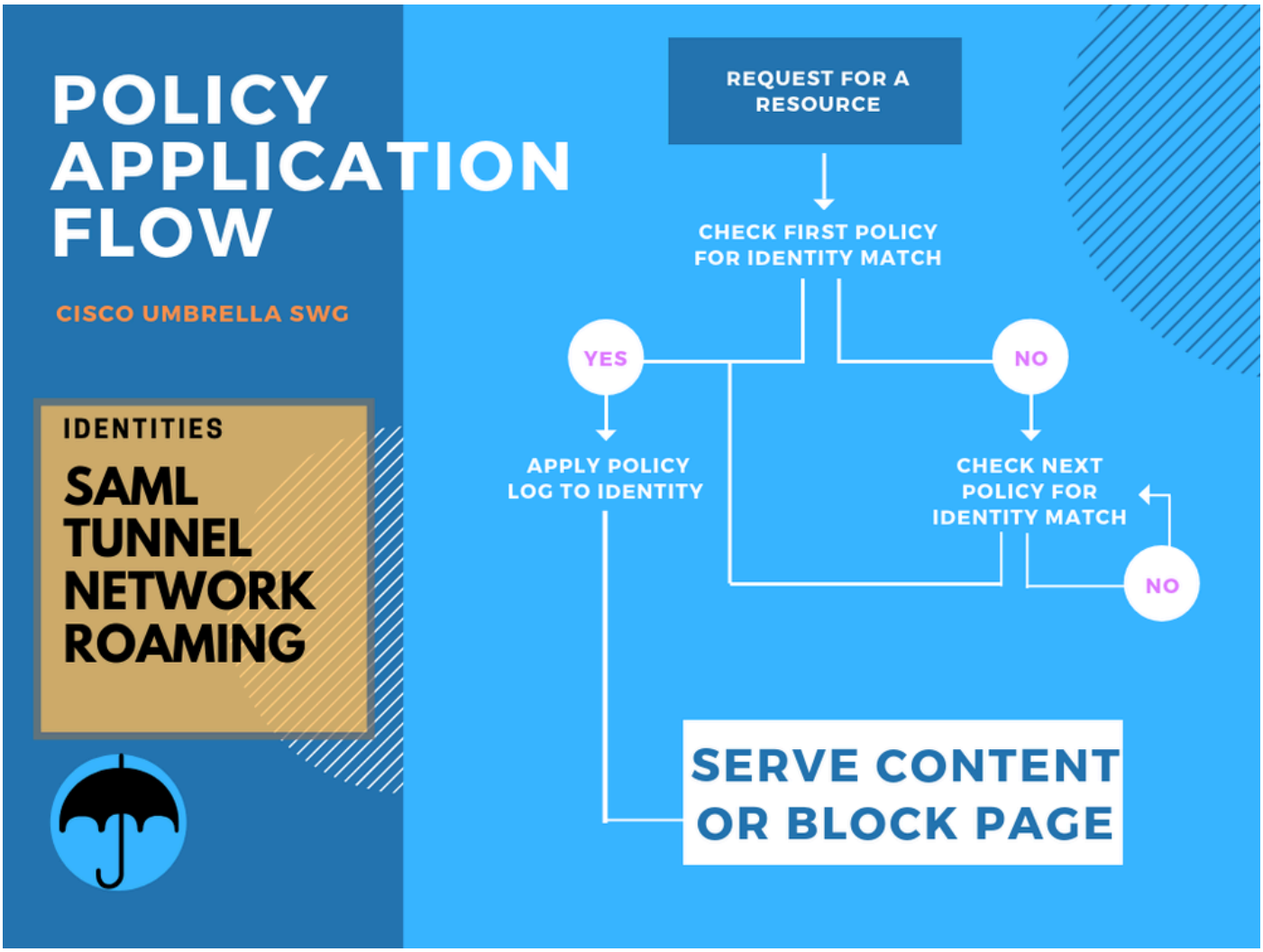
Background Information

Welcome to the Umbrella Secure Web Gateway (SWG). After deployment, the most important step is to define a web policy to ensure that the baseline behavior received is what you expect. Today, this policy flow mirrors the DNS layer policies exactly.

Umbrella Web Policies

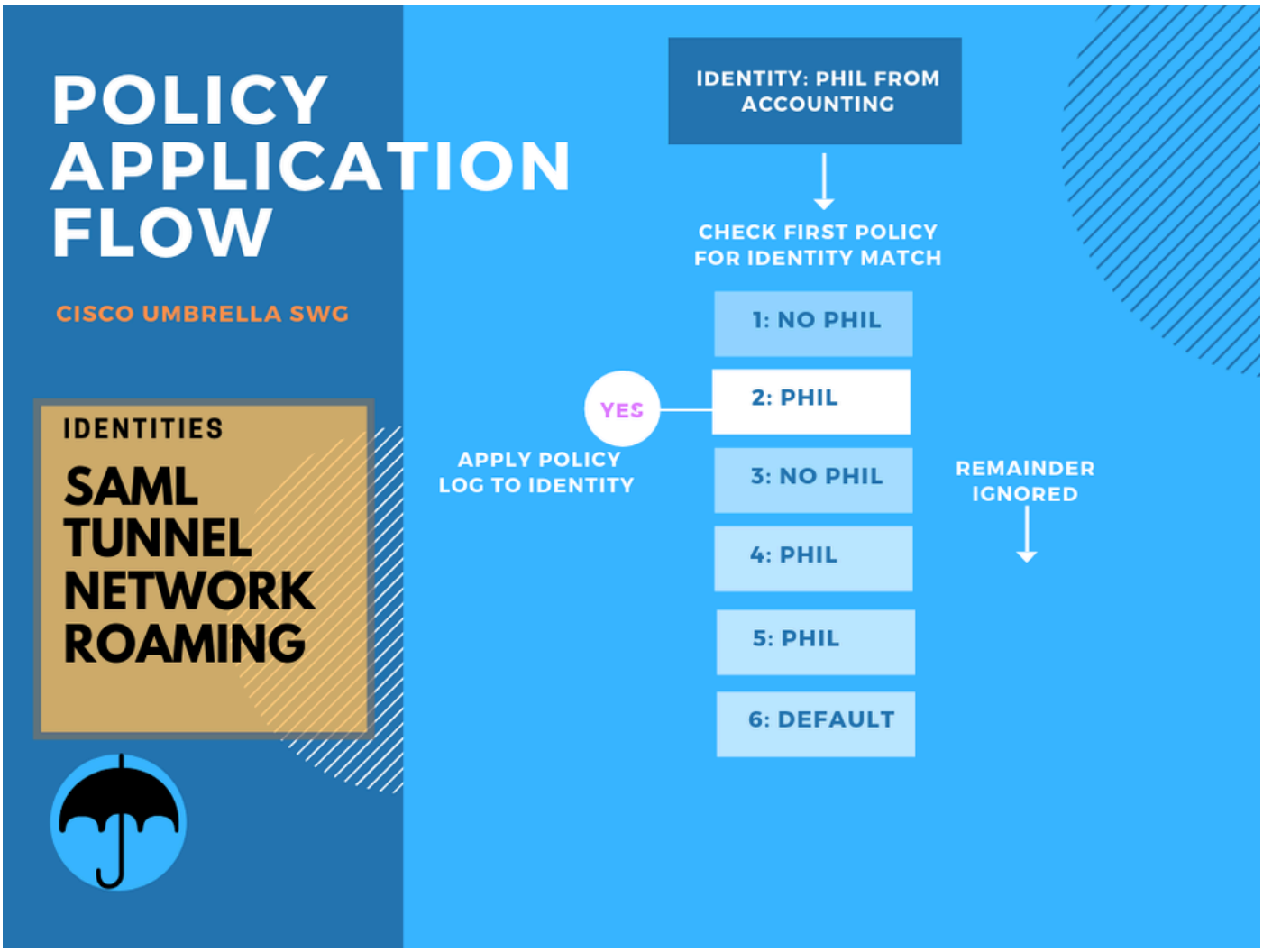
Umbrella Web policies function with a top match application algorithm. That is, the first policy to match the current set of identities is applied, and all subsequent policy matches are ignored. This is the basis for all Umbrella policies and can differ from any pre-existing expectations on proxy-based web policies.

Policy functions as displayed in this flow chart. The first **policy** match to any identity included in the query is applied without considering any further policies.



Flowchart-SWG.png

Since this flow is new to those not coming from Umbrella DNS policies, here is an example of a set of policies where several policies apply to the same user or group. Note how only the first policy applying to Phil (or Phil's user group) is used, and all remaining matches are ignored. Additional matches are not aggregated in Umbrella policy, just simply ignored.



Flowchart-flow.png

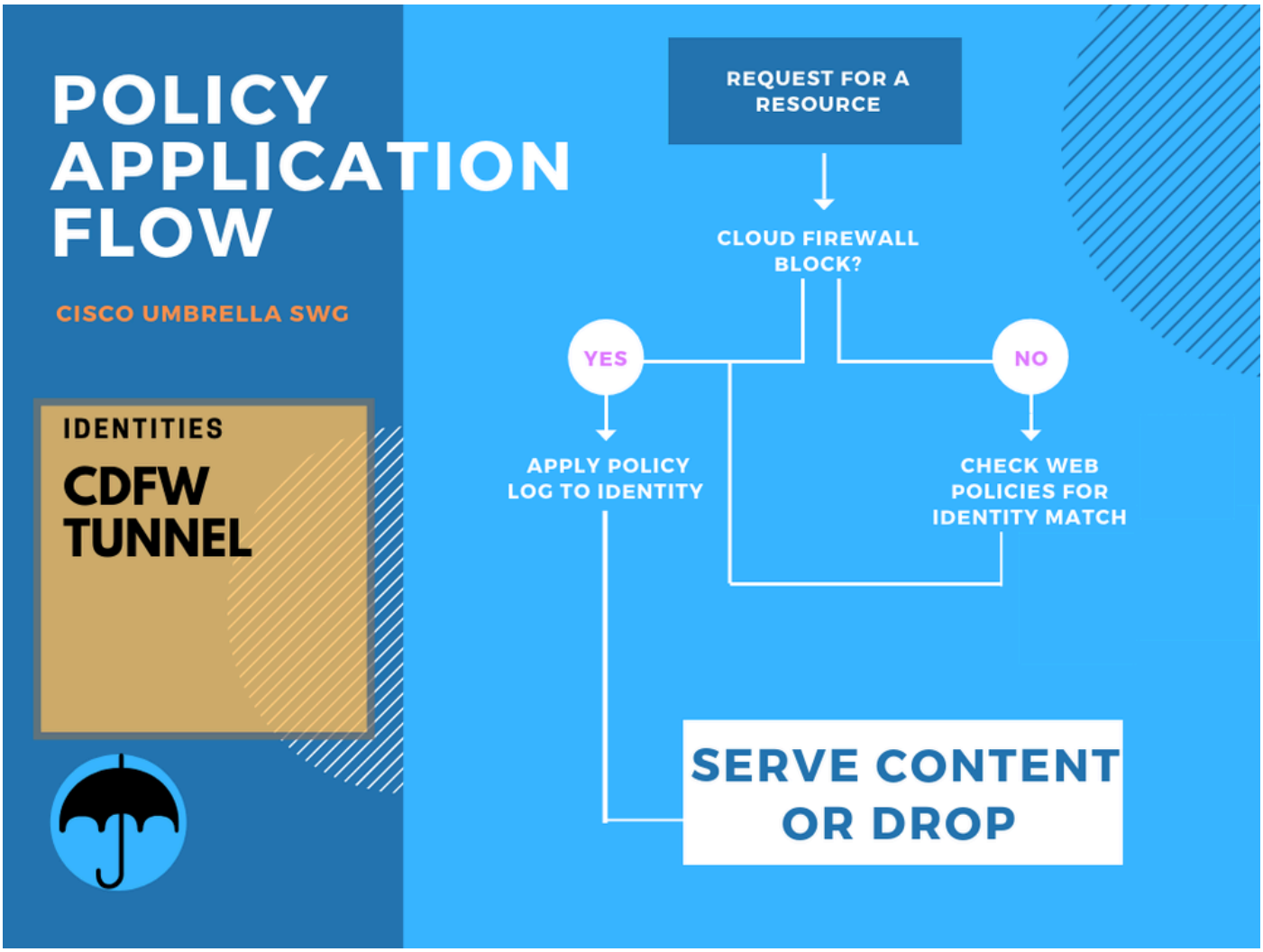
As a result, these are not available with Umbrella SWG policy:

- Nested policies
- Allow and block exclusions for an application or website that transverse any policy
    - Example: Policy exclusions for Phil is on allow Facebook, allow Instagram, and allow Dropbox exclusion but Phillis is only on allow Facebook and allow Instagram.
        - In Umbrella policy, this would be two unique policies.
            - Allow Facebook, Instagram, Dropbox applying to Phil
            - Allow Facebook, Instagram applying to Phillis
        - Each combination of allowed or blocked individual applications must have a new policy created with the applicable users added to the policy.

Additionally, any traffic that is not HTTP/S receives DNS layer policy for this type of traffic.

Important Notes About Cloud Delivered Firewall and SWG

The Umbrella CDFW sends any allowed HTTP/S traffic through the Umbrella SWG and therefore also apply policy. Once a policy is defined, policy application flow works the same as the SWG flow.



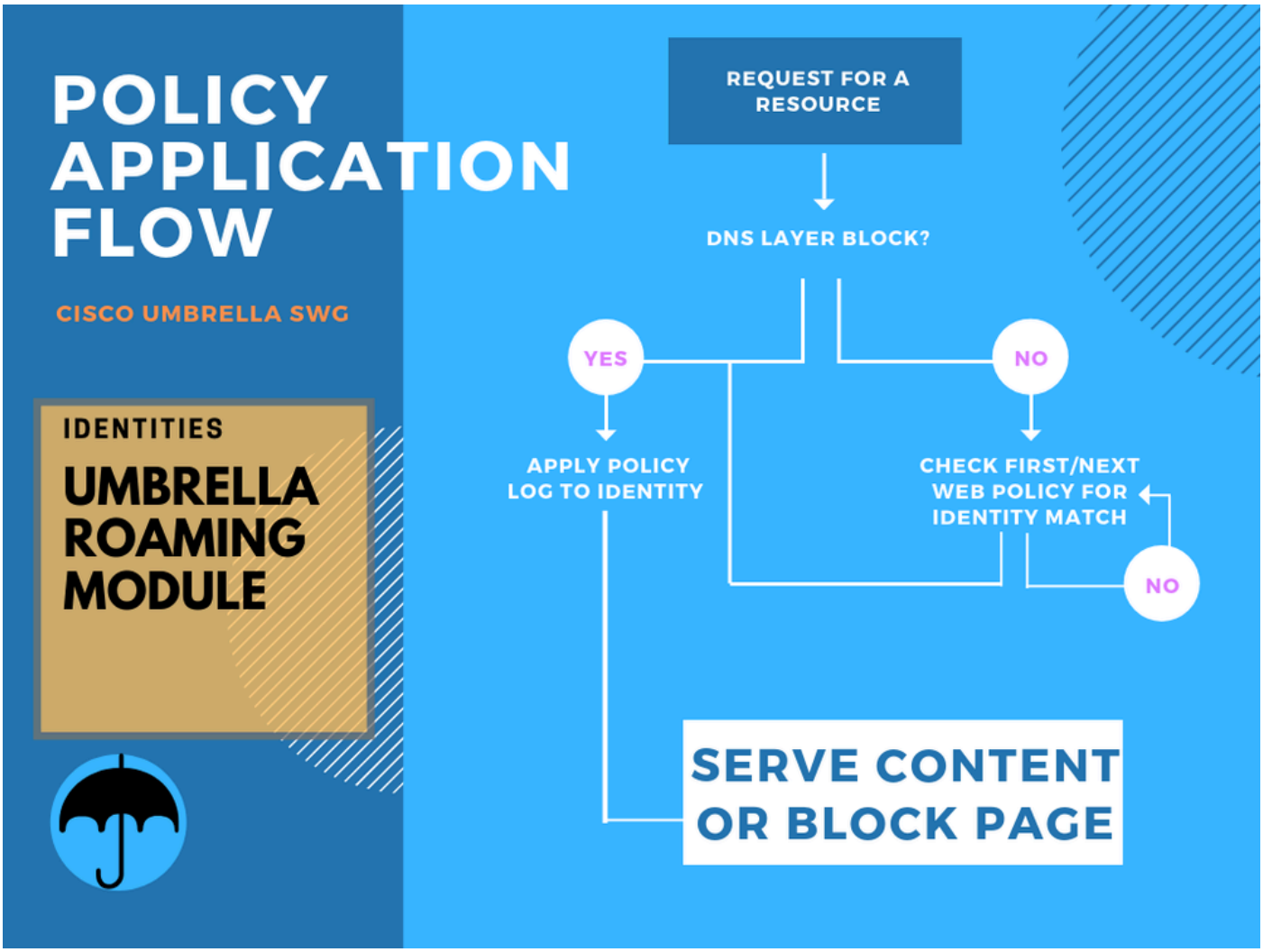
Flowchart-cdfw.png

Important Notes About Roaming Security Module Policies

With the Umbrella Roaming Module, policy is in effect differently than on-network policies. The roaming module is not compatible with on-network proxy configurations or PAC files and supports only the off-network use case. It can be disabled when on network.

While using the roaming module with a SWG policy, DNS policy takes effect first for any blocks including security blocks. If the result of the DNS policy is not a block, the proxy policy applies. Additionally, for any traffic that is not HTTP/S traffic, DNS policies are exclusively applied. Therefore, policy is applied in this order:

1. DNS Policy (for blocks)
2. SWG policy



Flowchart-module.png

Want to learn more? Check out our tutorial video: Umbrella Web Policies.