Cisco Umbrella Bible

Overview:

Top right is a time interval. Before looking at the overview page, change the time interval to your desired time. The schedule button in the top right will go through the process of scheduling reports based off of security block events.

The overview page will show you a summary of what is being seen in your network. It shows you any messages, deployment health, network breakdown, security categories, app discovery, security requests, and more.

Deployments:

Networks:

This is where all of your networks will be located and created. This consists of naming the network, the public IP address, as well as the policy that is attached to the networks. Adding a network to Umbrella will extend protection to any devices that connects to the internet behind that public IP.

Network Devices:

These will be any physical devices that will send DNS requests to Umbrella. Acts like a virtual appliance but it is a physical device instead of a virtual device. Any network devices will act like the VA however, which will forward DNS queries and return results based on policies. The integration is typically done by inputting an API key from Umbrella on the device itself, which should populate a status in the dashboard.

Roaming Computers:

Roaming clients are a great add on for companies as well as a work around for some sites. Essentially, the roaming clients act the exact same as VAs (Resolve DNS queries and send them up to the cloud to sift through policies) however the difference is that the computer that has the roaming client will resolve DNS queries locally on their own machine. Instead of the “normal” behavior of reaching out to the VA, sending DNS to the cloud, returning back to the VA, then to your PC… It will resolve the DNS query locally, send to the cloud, and then will be sent back to the PC.

In situations where VAs is living on a site where other sites cannot reach or hit internally, we can set up roaming clients on PCs for those sites to stay protected by Umbrella. Also, if you want your client to be protected when not inside the network (Lets say the PC is a laptop, and he is taking it to surf the internet at a coffee shop) his umbrella roaming client/module will still protect his web surfing since the traffic is resolving on his PC.

Note \* Because DNS is resolving locally, this will use some resource on the PC end, but not much.

To deploy the roaming client, on Deployments > Roaming Computers, there is a download button on the top left named “Roaming Client”. You can click it, and then download whatever option works best. (There is a client for Windows and Mac. Also a roaming security module that can be attached to an AnyConnect Profile.)

The first two are easy to set up, as you just download it onto the client machine. For the AnyConnect module, follow these steps here: <https://docs.umbrella.com/deployment-umbrella/docs/the-anyconnect-plugin-umbrella-roaming-security-client-administrator-guide>

Mobile Devices:

You can configure an MDM with the Umbrella Profile data provided below for IOS or Andriod.

IOS: <https://docs.umbrella.com/deployment-umbrella/docs/cisco-mobile-security-setup-guide>

Android: <https://docs.umbrella.com/deployment-umbrella/docs/umbrella-module-for-anyconnect-android-os>

On the top right under Manage, you will be able to download your configuration files here. For Android, you have one generic config file. For IOS, you have many such as Cisco Meraki, Apple, IBM, Microsoft Intune, Jamf, MobiConnect, MobileIron, and Workspace ONE.

Chromebook Users:

For Chromebook users specifically, there is a roaming client for directly made for Chromebooks. Here is the deployment guide:

<https://docs.umbrella.com/deployment-umbrella/docs/cisco-umbrella-chromebook-client-deployment-guide>

To protect your Chromebook, in the upper right corner, there is a configure button. Click that, and download your organizations configuration file, install the Chromebook client software by following the setup guide, and then sign in with super admin email id of your Google Admin console to sync GSuite identities into Umbrella.

Users and Groups:

In this area, you will be able to provision and users and groups from your identity providers. In most cases, your users and groups will be under the active directory section. You will then be able to view AD users and groups that have been synced by your connector.

Domain Management:

This is a crucial area to configure, as any domains created in this section will route DNS traffic to your DNS server as your resolver. For instance, you route a DNS request that is resolving towards an internal website hosted within your domain. We would want to have the domain configured in the domain management section, so when the DNS traffic hits your virtual appliances they know to send the DNS request to your DNS server. If there is no config in your domain management, all your DNS requests will be sent to the cloud to resolve which will not be good as traffic destined to resolve specifically on your DNS server will not happen. (Lose access to hit your internal resources.)

Sites and Active Directory:

This area is another area that is important to configure. You will be able to see the status of any VA, Domain Controller, AD connector, etc that you install. On the top right corner, there is an Add button. Here, you will be able to start the process to integrate either a DC, Windows Event Log Collector, or Domain with Umbrella. If we click the Download button on the top right, it will give you the active directory components as well as the virtual appliance components to download and install. The active directory components will be installed on the DC and the VA components will be installed on either VMWare or Hyper-V. A good resource I use to help remind me how to run the install processes is…

<https://www.youtube.com/watch?v=e6dS-ZpBgQo&t=1841s>

Generally, the steps to install that I usually take are:

1. Active Directory config script + connector for DC
2. Any Domain Controller Components Scripts
3. Virtual Appliance Install process
4. Give it time to sync everything (Generally an hour is sufficient)

Internal Networks:

Here, we can get super granular and apply policies to specific internal VLANs/subnets. (These will be non-routable) Generally we do not do this in the setup, however customers can come in and create more detailed policies that attach to specific subnets.

Root Certificate:

Umbrellas Block page presents an SSL cert to browsers that hit the page. The cert is signed by Cisco Root Certificate Authority (CA).

Service Account Exceptions:

You can explicitly tell the connector to ignore logon events from specific service accounts. When you add a User/Group/IP, it will add it to the exceptions lists that disables the tracking of events from that source.

Policies:

All Policies:

You will be able to see all of your policies created here. It will be sorted by order of enforcement, meaning your policies will be hit by top down. Any granular policies will be on top of the list, while your generic/default global policies will be on the bottom. Within each of the policies will be your identities that it will be applied to as well as all of your policy components listed below.

Destination Lists:

You will have a Global Allow list as well as a Global Block list. I generally keep these defaults and add certain domains/IPs when events occur. If something is being blocked that shouldn’t be blocked, I will through the domain/IP in the allow list which is applied to all of my parent policies.

Content Categories:

These categories can get super granular. I will sit down with the customer and give our best practice list (Adult, Illegal Activities, Nudity, Terrorism and Violent Extremism, Peer File Transfer, and pornography.) After these categories are attached, any other ones that the customer wants, will be put in. Talos on the back end has databases filled with IPs/Domains that are linked to each category. The more categories that are checked, the more room for false positives. After a policy is applied and the clients are running DNS requests through the policies, it will be smart to keep an eye on the reporting section to ensure what is being blocked is supposed to be blocked.

Application Settings:

Application settings are super similar to content categories except, these do not have to be malicious. This can be any application you want to limit access to for your users. There are many different categories in here from backup and recovery applications, cloud storage applications, etc etc. Usually our best practice contains sites in social networking, P2P, Games, and anonymizers. (Please see Ceriums list for a best practice within our environment) We can then see what the customer needs/wants and apply changes based off needs.

Security Settings:

This section is less granular and more generic. Here we can block any categories such as malware, potentially harmful domains, crypto mining, etc. Usually we block every category except Newly Seen Domains, DNS tunneling VPN, and Dynamic DNS. These cause a lot of false positives that is not worth the effort unless you have a distinguished SOC or IT staff that can monitor Umbrella traffic all the time.

Block Page Appearance:

We usually keep the generic block page however customers can go in on their own and create a custom block page for their users to see if trying to access a domain that is against their policies.

Integrations:

We can tie other pieces of software into Umbrella. Integrations currently are Check Point, Cisco AMP Threat Grid, FireEye, ThreatConnect, ThreatQ, and ZeroFOX. Usually to enable these integrations, you just need to connect to an API key that can be found on the third-party tool.

Reporting:

Security Activity:

General overview page of the security activity happening within your network. (DNS/Umbrella related only) You can see different event types relating to antivirus, Cisco AMP, and other integrations. You will be able to see the security category that was blocked, the user trying to access the domain/site, and the date of the event. As we see on the top right as well, we can schedule reports to be sent based on the security activity seen.

Activity Search:

This is the number one section you will spend most your time in. Here, we will be able to see all the DNS traffic that Umbrella sees, Allowed or blocked. We can also specify protocols like HTTP and HTTPS while filtering through event types, identity types, security categories, content categories, etc. At the bottom of the page, there is a search options button. We want to include all the traffic when looking into security events, which will show the high traffic domains like CDNs and reverse lookups.

After specifying our parameters, we will be able to see the specific requests. The request, identity, policy, destination, internal IP, external IP, action, category, application, & date/time will be shown on each event. We can see what exactly is being blocked, which will lead to actions such as IPs/Domains going into destination lists, finding false positives, and understanding who/what in your environment is searching for malicious domains.

Application Discovery:

Here, we can see applications found through DNS requests. There will be a list of apps you can see is being accessed in your environment as well as any flagged categories, anonymizers, P2P, etc. We can then see graphs showing DNS requests by APP risk and APPS by category and Risk.

Top Threats:

Here, you will be able to see any reported threats that have happened in your environment. You can schedule reports to “report” off this page as well.

Total Requests:

Similar to Activity Search, you will be able to see the total requests of traffic that Umbrella has seen within your environment. This can be DNS, web, or IP-Layer Enforcement traffic. We can then go even more granular to see the different types of traffic, identities, response, etc.

Activity Volume:

Requests separated by security, categories, destination lists, permitted, and total. We can then see allowed, blocked, total, and % of the total allowed vs blocked requests.

Top Destinations:

These will be your most visited destinations in the network. You will be able to go through all of the categories to search through your data similar to activity volume.

Top Categories:

Same as Top Destinations, but for categories.

Top Identities:

Same as Top Categories and Top Destinations, except this section shows the most traffic out of certain identities.

Exported Reports:

This category shows any reports that you have exported. We can also download the reports here as well as delete any not used reports.

Scheduled Reports:

We can see any reports that were made, such as weekly reports, monthly reports, daily reports, etc.

Admin Audit Log:

Here we can see any audit logs for specific Users, IP addressed, and identities.

Investigate:

Smart Search:

We can search hostnames, URLs, ASNs, IPs, or email addresses to bring up the identities traffic to investigate.

<https://docs.umbrella.com/investigate-ui/docs>

Pattern Search:

It is a RegEx search. Uses investigate pattern searching.

<https://docs.umbrella.com/investigate-ui/docs>

API Keys:

This area allows you to create an API key to help write scripts as well as integrate other solutions. Umbrella investigate API is organized around the principles of REST.

<https://docs.umbrella.com/investigate-ui/docs>

We can see any access tokens created that show integrations between secure X, AMP, etc. We can also create new Tokens at the top right.

Admin:

In this section, we will be able to see the Admin capabilities. This includes managing accounts, giving accounts “User Roles”, seeing Log management as well as authentication requests. We can Bypass Users and codes, assign API keys, and review our current licensing scheme.