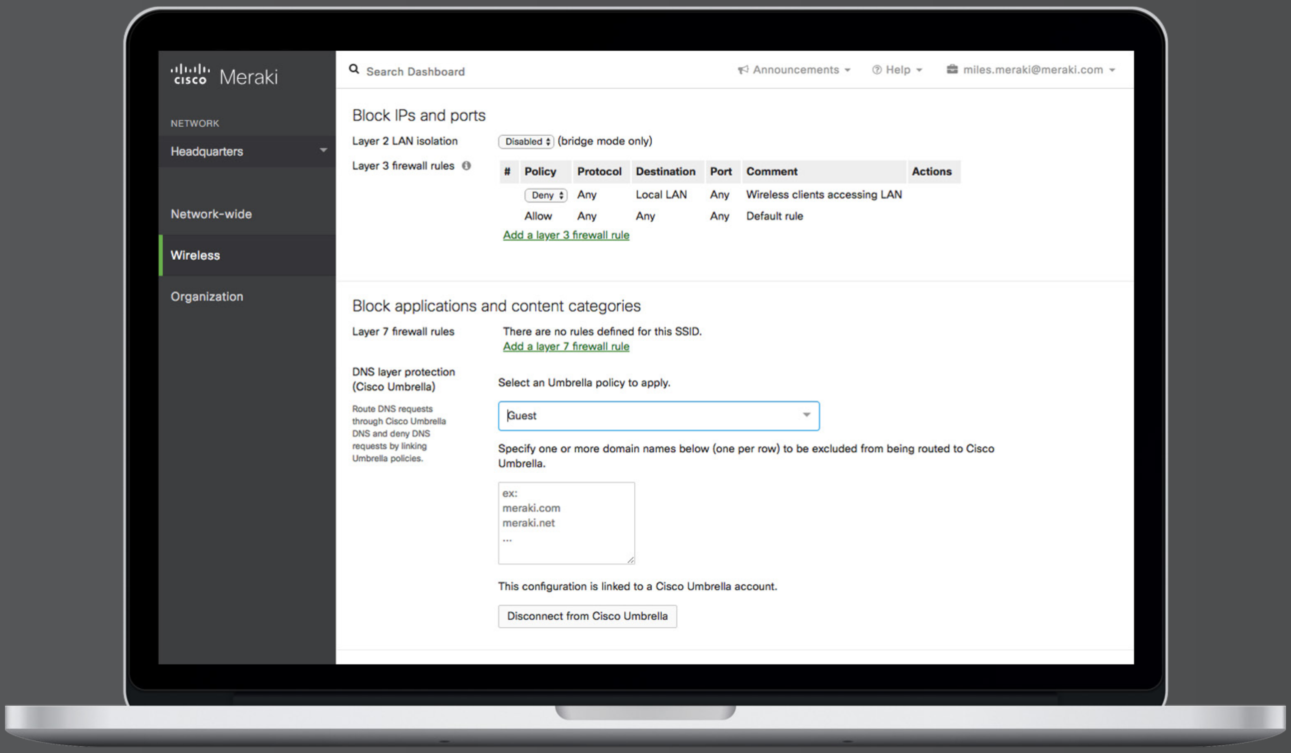


Block IPs and ports

Layer 2 LAN isolation: Disabled (bridge mode only)

Layer 3 firewall rules

#	Policy	Protocol	Destination	Port	Comment	Actions
	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

Add a layer 3 firewall rule

Block applications and content categories

Layer 7 firewall rules: There are no rules defined for this SSID.
Add a layer 7 firewall rule

DNS layer protection (Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Select an Umbrella policy to apply.

Guest

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

ex:
meraki.com
meraki.net
...

This configuration is linked to a Cisco Umbrella account.

Disconnect from Cisco Umbrella

Cisco Meraki

DNS Security with Meraki MR & Umbrella

WHITEPAPER
DECEMBER 2019

Contents

Introduction

As technology and personal computing have evolved, so too have the security threats that lurk in the dark corners of the world wide web. With 11 billion Internet-connected devices coming online in 2018, the attack vector for users with malicious intent is the largest it has ever been. Securing these devices, especially in the workplace, is of paramount importance.

The foundation of the Internet revolves largely around the Domain Name System (DNS). DNS could be considered the “phonebook for the Internet.” Akin to flipping through the phonebook to find the person or business and their phone number to call them for information, DNS is used by client devices to look up the domain name associated with a given website, and convert that name to an IP address. For example, DNS mahelps so that users can simply type in https://meraki.cisco.com instead of 104.20.40.242.

Due to the prevalence of DNS traffic in today’s Internet, this foundational Internet protocol has become a huge target for malicious attacks. DNS is inherently unencrypted and that allows any eavesdropper sitting between a client device and their DNS server to see DNS queries that a client device is making. But first, let’s take a step back and recall what DNS really is. It would be helpful to think of DNS as the phonebook of the internet. Every website has a specific IP address associated with it. For example, if Wells Fargo’s IP address is 151.151.29.189. DNS turns the human-readable address (wellsfargo.com) into a machine-readable address (151.151.29.189) and ensures that you always connect to the correct website. In this instance, Cisco Umbrella guarantees a user is safely routed to wellsfargo.com so that a user is not intercepted by someone else claiming to be WellsFargo who might jeopardize both the individual user’s device, or even worse, the other devices connecting to the same local network.

While DNS has largely remained the same protocol since its inception by the Internet Engineering Task Force, the way that devices connect to Internet Protocol (IP) networks has changed. Wires have largely been replaced by radios and antennas, as user mobility with laptops and smartphones has driven the meteoric rise of Wi-Fi. Cisco Meraki satisfies the needs of companies wishing to provide secure Wi-Fi connectivity to their end users with industry-leading, cloud-managed access points (APs).

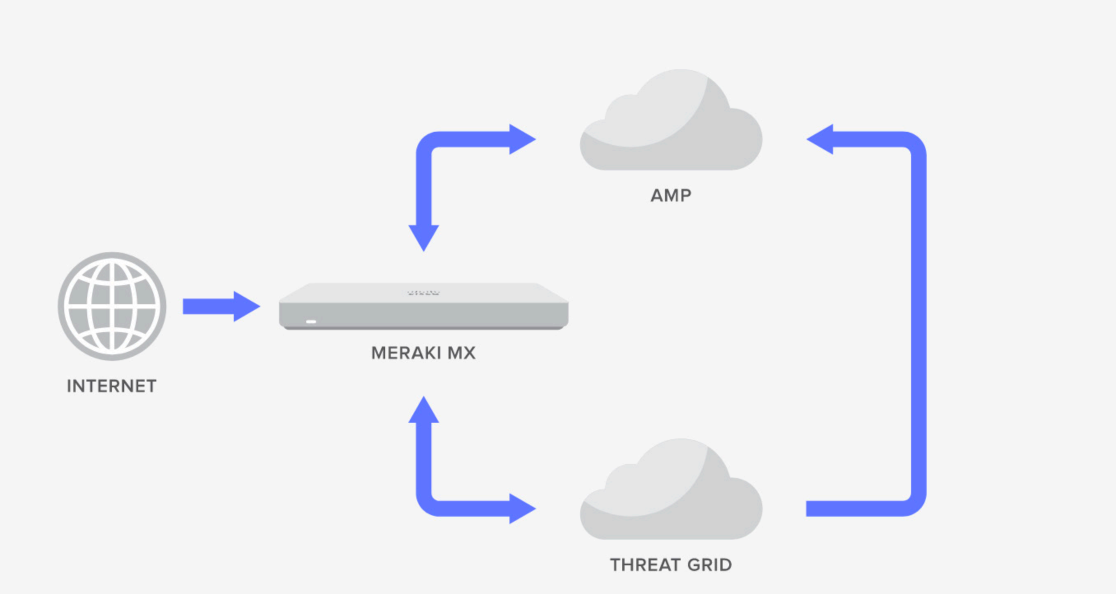
> DNS is used by client devices to look up the domain name associated with a given website, and convert that name to an IP address.

Companies can no longer sit idly by and hope that they are protected from the plethora of threats that exist. They must take action, and that action should focus around one of the original “apps” of the Internet, DNS. Now, it is easier than ever to protect the devices in your organization with Umbrella and Meraki.

Lurking Threats

Of all of the different types of computing security threats, malware is most familiar to the general population. Malware is defined as software that is intended to damage or disable computers and computer systems. Malware can take various forms, be it a computer virus, drive-by download, or a trojan. Oftentimes, network security vendors will tout their firewall as being fully capable of defending against and preventing zero-day malware attacks from being downloaded onto a network and executed. Anti-virus solutions running on personal or company-issued computers will tout the same, both with the tantalizing prospects of dynamically learning about the latest and greatest in malware and using these new 'signatures' to quickly identify malware packages soon after they were first created.

Solutions such as Cisco's Threat Grid take this one step further by identifying suspicious files or traffic behaviors on a network and even placing suspicious files into a 'sandbox' to execute the file and analyze the resulting behavior. A signature is then developed and uploaded to a centralized storage of known malware signatures so that Unified Threat Managers such as MX security appliances can learn about the threat before ever seeing the file, and further secure users with functionality like Advanced Malware Protection (AMP).



Umbrella isn't intended as a replacement to dedicated security appliances, firewalls, or anti-virus software solutions. Instead, Umbrella is more efficient because it stops the majority of threats at the DNS layer before a connection is ever made, and thus reduces the traffic volume and inspection tasks that are required by downstream security tools and personnel. Umbrella is built into the foundation of the internet and therefore is better able to block internet-based threats. Attackers will often use the same domain names, DNS nameservers, and IP address spaces to deliver many malware variants and different attacks.

This ability is extremely important in today's age of rapid software development because attackers are able to test their engineered threats against a number of different, existing security solutions quickly. This allows the attacker to adapt the malware to get around firewalls and security appliances so that the malicious data can be downloaded and executed on an unsuspecting user's machine. However, there's a lot that goes into preparing malware for consumption by users. The attacker will need to prepare the necessary internet infrastructure in order to host the malicious content for users to access. This may require preparing a redirect or link to a malicious web domain, or sending a malicious attachment in an email. If the attacker has embedded malware into a compromised site, perhaps via means of malvertising (injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages), or has simply inserted a hyperlink into the site that would redirect to the domain where the malware is hosted, then a user is immediately susceptible and will begin downloading the malicious content once their computer performs a DNS lookup of the domain to resolve the IP address. This is where Cisco Umbrella comes into play. By blocking those domain lookups of exploit and phishing domains at the earliest point, Umbrella can make sure that the malware is never downloaded to begin with. Umbrella enforces 7M+ malicious domains and IPs at the time a DNS request is being processed without adding any latency.

As mentioned previously, the attacker may instead initiate an attack via email attachments or direct downloads. A common technique with these attacks is that once downloaded, the malware will "call home" and begin exfiltrating data back to its central command center, perhaps on a large scale in tandem with other computers as part of what's called a "botnet." Of course, in order for the malware to find its home, it's going to lookup via DNS where home resides on the internet. Umbrella comes to the rescue yet again, as it is able to identify where these domains are hosted and will block the DNS requests to prevent what could be confidential company data from leaking out of the local network.

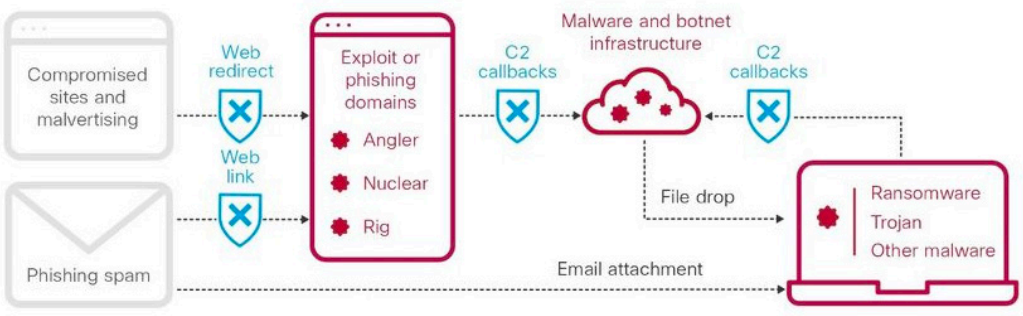
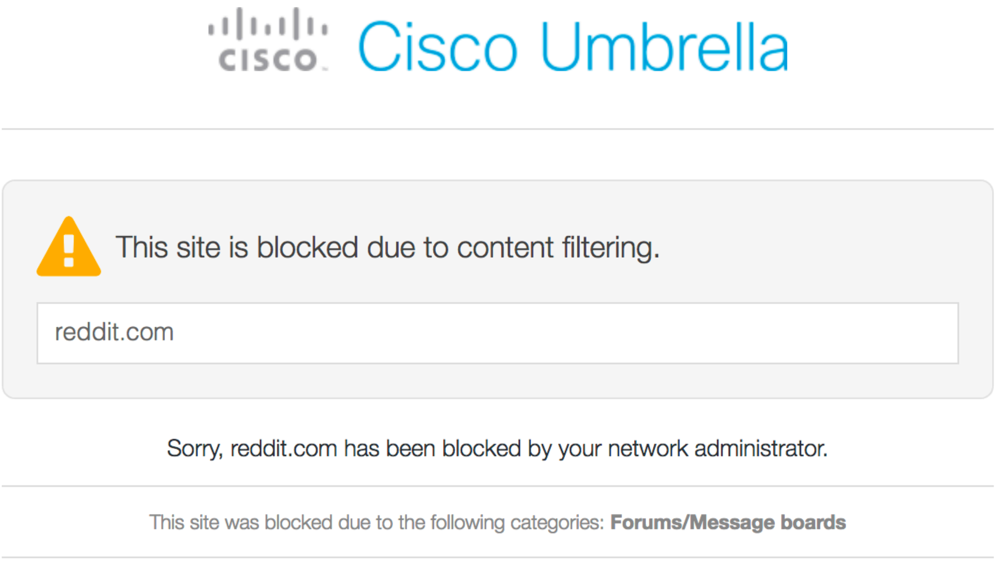


Figure 1: DNS layer security from Cisco Umbrella

Content Categorization

Beyond protecting users from malicious content, Umbrella also provides top-notch content categorization. This allows network administrators and security teams to dictate which types of websites can be accessed by users on the network. Administrators can select between default content category filtering levels of high, medium, and low; each with their own rule set allowing for quick and easy DNS-based content security. An administrator may also choose a custom ruleset, in which upwards of 100 different categories can be selected. If a user's DNS query is destined to a website that has been categorized by Umbrella as a blocked website category, then a block page is presented to the user. The block page may be the default Umbrella block page as shown below, or one with custom text and images and perhaps subtle messaging to guide a user back towards more work-related web browsing on company time.



Cisco Umbrella

This site is blocked due to content filtering.

reddit.com

Sorry, reddit.com has been blocked by your network administrator.

This site was blocked due to the following categories: **Forums/Message boards**

Figure 2. Block page presented from an Umbrella security policy

DNS Security Made Simple with Meraki

With Wi-Fi being the primary means, and sometimes the only means, of connecting to a company's network for access to resources as well as the Internet, it makes perfect sense to bring the power of Umbrella's cloud-based DNS security solution to Meraki's cloud-based MR wireless access point portfolio.

Depending on the user's needs, there are two ways to integrate with Cisco Umbrella:

Manual Integration: Customers who want to build custom policies for content and security and then push them to the Meraki MR will need to pursue this route. It offers a great range of flexibility and also access to the Umbrella dashboard.

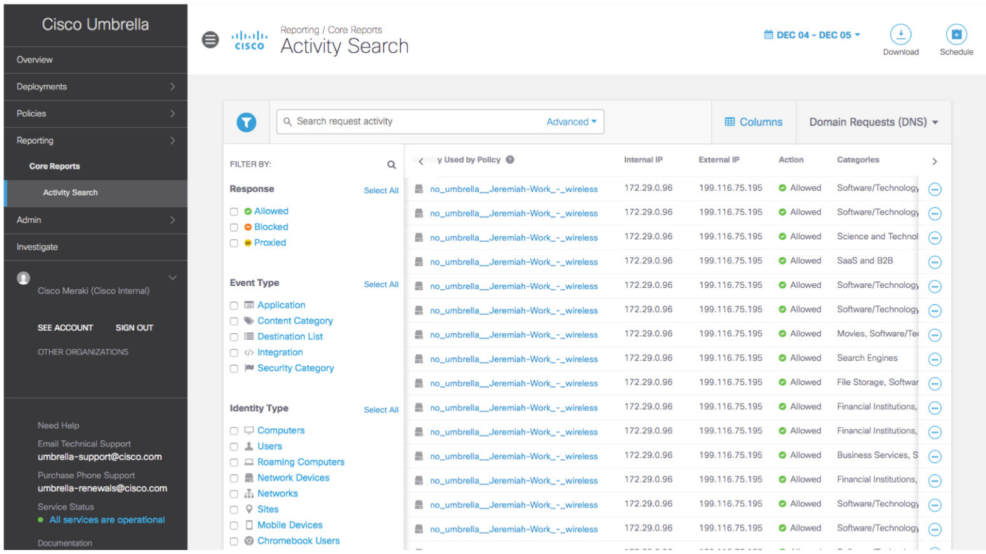
Automated Integration: Customers who want a turn-key solution provision DNS-layer security will choose this integration. This also simplifies licensing for MR and Umbrella while giving access to blocked events inside the Meraki dashboard along with seven pre-defined policies.

MANUAL INTEGRATION

Making this integration possible is the Umbrella Network Devices API key. This API key allows for network devices with access to the API key to register themselves as Network Device identities in Umbrella. Administrators can then configure security policies assigned to those Network Device identities for protecting DNS traffic being sourced from those identities.

On the Meraki side of the house, much of the wireless network configuration (Access Control settings, Firewall & Traffic Shaping) takes place on an individual SSID basis. To override those configuration settings and get more granular at a per-user level, similar settings can be applied via Group Policies and assigned to individuals or groups of users connecting to the wireless network.

Here are the steps involved in setting up a manual integration between Umbrella and the Meraki MR: [Manually integrating Cisco Umbrella with Meraki MR]



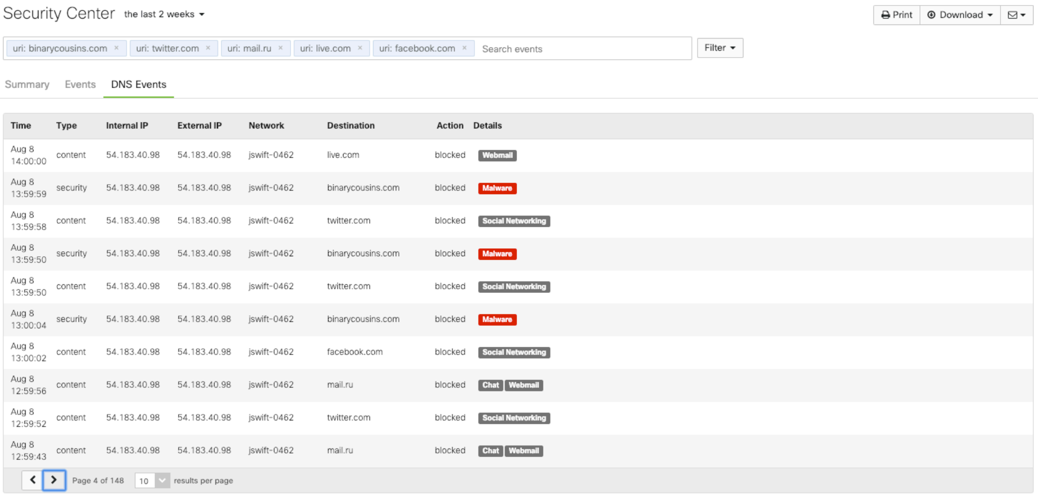
Identity Used by Policy	Internal IP	External IP	Action	Categories
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Software/Technology
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Software/Technology
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Science and Technol
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	SaaS and B2B
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Software/Technology
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Software/Technology
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Movies, Software/Te
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Search Engines
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	File Storage, Softwar
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Financial Institutions,
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Financial Institutions,
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Business Services, S
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Financial Institutions,
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Software/Technology
no_umbrella__Jeremiah-Work_-_wireless	172.29.0.96	199.116.75.195	Allowed	Software/Technology

Figure 3. Users have access to complete Umbrella dashboard with the Manual Integration

AUTOMATED INTEGRATION

IT admins can secure their wireless network by combining the power of Cisco Umbrella's DNS security solution with the simplicity of the Meraki dashboard. The new MR Advanced and Upgrade licenses automatically enable Meraki-defined policies at the DNS layer across their entire network. With the new license, IT admins also get access to the industry-leading "Security Center" under the Meraki dashboard which helps them gain granular visibility into blocked events. Existing MR customers easily upgrade their existing MR using the Upgrade License to combine their MR and Umbrella licenses. New Meraki MR customers can opt for the Advanced License which covers both the MR and the Cisco Umbrella subscription.

Here are the steps involved in setting up an automated integration between Umbrella and the Meraki MR: Advanced and Upgrade License for Cisco Meraki and Umbrella



Time	Type	Internal IP	External IP	Network	Destination	Action	Details
Aug 8 14:00:00	content	54.183.40.98	54.183.40.98	jswift-0462	live.com	blocked	Webmail
Aug 8 13:59:59	security	54.183.40.98	54.183.40.98	jswift-0462	binarycousins.com	blocked	Malware
Aug 8 13:59:58	content	54.183.40.98	54.183.40.98	jswift-0462	twitter.com	blocked	Social Networking
Aug 8 13:59:50	security	54.183.40.98	54.183.40.98	jswift-0462	binarycousins.com	blocked	Malware
Aug 8 13:59:50	content	54.183.40.98	54.183.40.98	jswift-0462	twitter.com	blocked	Social Networking
Aug 8 13:00:04	security	54.183.40.98	54.183.40.98	jswift-0462	binarycousins.com	blocked	Malware
Aug 8 13:00:02	content	54.183.40.98	54.183.40.98	jswift-0462	facebook.com	blocked	Social Networking
Aug 8 12:59:56	content	54.183.40.98	54.183.40.98	jswift-0462	mail.ru	blocked	Chat Webmail
Aug 8 12:59:52	content	54.183.40.98	54.183.40.98	jswift-0462	twitter.com	blocked	Social Networking
Aug 8 12:59:43	content	54.183.40.98	54.183.40.98	jswift-0462	mail.ru	blocked	Chat Webmail

Figure 4. Users can view their events inside the Meraki dashboard under the "Security Center" with the Automated Integration

Which one should you choose ?

MANUAL INTEGRATION	AUTOMATED INTEGRATION
Benefits: • Access to all Umbrella policies & custom features • Granular visibility into network events • Access to the Umbrella dashboard	**Benefits:** • Turn-key solution, no integration required • Faster provisioning and simplified licensing • View threat events in the Meraki dashboard
Challenges: • Manual API integration • Managed using two dashboards • Events only visible in Umbrella dashboard	**Challenges:** • No option to create custom policies • Access to Umbrella dashboard is not available • No granular visibility into events
For: • Customers who want to use all of Umbrella's policies • Customers who want to deploy custom policies for compliance	**For:** • Customers seeking to deploy basic DNS layer security • Customers who want to provide secure guest Wi-Fi with ease

Umbrella and Meraki MR: A Packet's Journey

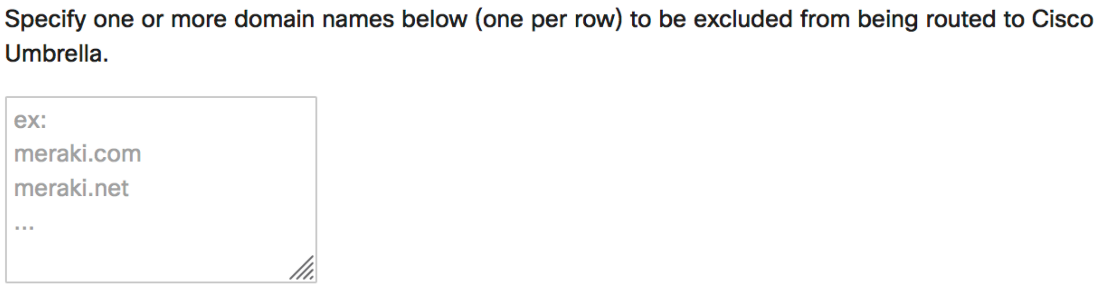
The integration between Umbrella and Meraki was designed with powerful capabilities, but the simple to configure user interface is true to Meraki's mantra of technology that simply works. As outlined above, the administrator only needs to copy and paste their Umbrella Network Devices API key & secret into the Meraki Dashboard network, and then choose which policies apply to which SSIDs. Meanwhile, all of the heavy lifting of the configuration is taking place behind the scenes with API calls to and from the Umbrella and Meraki backends. It's also important to outline what the actual traffic flow looks like for the DNS queries.

When the user connects to an SSID that has an Umbrella policy enforced, their device will start to send DNS queries in an attempt to identify IP address destinations. The MR access point will listen for these DNS queries, and if a query is received from a wireless client on an Umbrella-policed SSID, then the MR will encrypt the DNS query using DNScrypt.

DNScrypt is used to encrypt the DNS lookups between the local network and Umbrella's DNS resolvers. This is done to ensure that individuals with malicious intent cannot "sit in" on the traffic between a user and their DNS server. This eliminates the threat of a Man in the Middle (MITM) attack, and prevents attackers from forging DNS responses to unsuspecting user queries to redirect users to malicious sites. As such, the DNS lookup that leaves the user's device as a plaintext DNS query arrives at the MR, the MR attaches additional identifiable information to the DNS packet, gets encrypted, and then subsequently is redirected as UDP 443 traffic to Umbrella's DNS resolvers.

Upon receiving the encrypted DNS packet, Umbrella's resolvers decrypt the packet, inspect the EDNS information denoting the proper network device identity, check the lookup to see if it matches on the configured security policy and if the query is allowed through or not, and sends back a block page if the queried domain is blocked. Assuming the domain is not blocked, then the query is resolved and sent back to the client device as normal.

There may be instances where administrators do not want all DNS lookups sent to Umbrella. For example, there may be internal domain services that employees use in their day-to-day operations. In these cases, administrators can effectively exclude domain names from being redirected to Umbrella. Instead, DNS queries for these domains will be forwarded unencrypted onto the ethernet destined to the DNS server IP configured on the client.

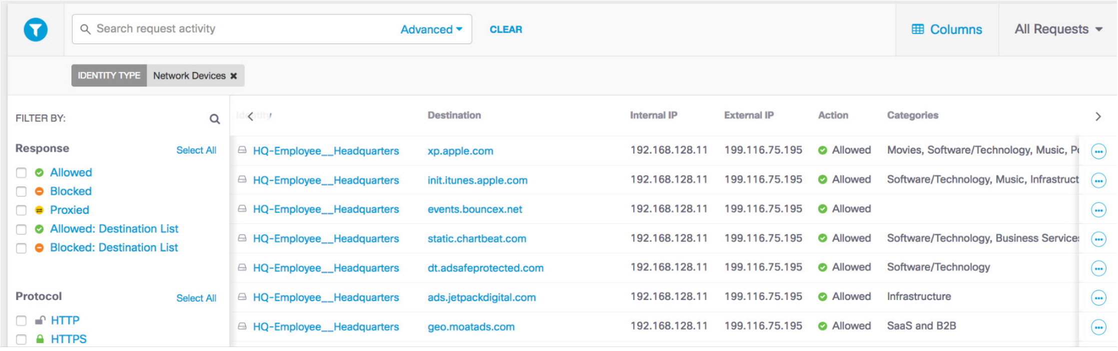


Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

ex:
meraki.com
meraki.net
...

Figure 5. Umbrella domain exclusion textbox in Wireless > Firewall & Traffic Shaping

Once Umbrella policies are linked to Meraki SSIDs and group policies, reporting information will begin to populate in the Umbrella Dashboard. Administrators will be able to easily delineate where lookups are coming from, who's making the request, and type of traffic the domain lookups are getting categorized as.



Identity	Destination	Internal IP	External IP	Action	Categories
HQ-Employee__Headquarters	xp.apple.com	192.168.128.11	199.116.75.195	Allowed	Movies, Software/Technology, Music, Po
HQ-Employee__Headquarters	init.itunes.apple.com	192.168.128.11	199.116.75.195	Allowed	Software/Technology, Music, Infrastruct
HQ-Employee__Headquarters	events.bouncex.net	192.168.128.11	199.116.75.195	Allowed	
HQ-Employee__Headquarters	static.chartbeat.com	192.168.128.11	199.116.75.195	Allowed	Software/Technology, Business Service
HQ-Employee__Headquarters	dt.adsafeprotected.com	192.168.128.11	199.116.75.195	Allowed	Software/Technology
HQ-Employee__Headquarters	ads.jetpackdigital.com	192.168.128.11	199.116.75.195	Allowed	Infrastructure
HQ-Employee__Headquarters	geo.moatads.com	192.168.128.11	199.116.75.195	Allowed	SaaS and B2B

Figure 6. Sample activity search report in Umbrella

Conclusion

Both the Umbrella and Meraki organizations pride ourselves on bringing powerful, secure solutions to our customers. The recent integration between Umbrella and Meraki MR access points shows the best of both worlds in being able to leverage the best DNS security that the industry has to offer, in combination with the fast, reliable, enterprise Wi-Fi solution that the MR product line is known for. Network administrators and security administrators can now rejoice in unison with the fact that bulletproof security has been brought to the wireless edge, protecting the employees, as well as the companies they work for, from the omnipresent threat of cybersecurity attacks.