DNS Security with Meraki MR & Umbrella
Contents

3 Introduction

4 Lurking Threats

6 Content Categorization

7 DNS Security Made Meraki Simple

11 Umbrella and Meraki MR: A Packet’s Journey

13 Conclusion
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 (https://www.forbes.com/sites/bernardmarr/2018/01/04/the-internet-of-things-iot-will-be-massive-in-2018-here-are-the-4-predictions-from-ibm/#2d5a688fedd3). 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 yellow pages to find the person or business and mentally mapping them to a phone number, 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 makes it so users can simply type in https://meraki.cisco.com instead of 104.20.40.242.

DNS works in a hierarchical manner in order to scale to the size required to handle domain lookups for the global Internet. 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, meaning that any eavesdropper sitting between a client device and their DNS server can see the DNS queries that a client device is making, i.e. “what’s the IP address of dashboard.umbrella.com?” The DNS server that the lookup is sent to will respond with IP address(es) and upon receiving that response, the client device will then initiate a connection such as an HTTP GET to that IP address.

Given that this DNS lookup and response is unencrypted, there is potential for a malicious actor to forge a DNS response to send a user to a website that mimics their intended destination but is instead hosted by the attacker. At this point, the user is now susceptible to a variety of attacks that can 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 as RFC 882 and RFC 883, 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).

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 designed or intended as a replacement to dedicated security appliances, firewalls, or anti-virus software solutions. Instead, Umbrella is designed to block the Internet infrastructure that malware relies on to harvest data, receive commands, update itself, and spread to other devices or infrastructure. Attackers will often use the same domain names, DNS nameservers, and IP address spaces to deliver many malware variants and different attacks (https://umbrella.cisco.com/use-cases/advanced-malware-protection).
This 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. 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, Umbrella can make sure that the malware is never downloaded to begin with.

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 to the rescue yet again, as Umbrella 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.

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.

Figure 1. Block page presented from an Umbrella security policy
DNS Security Made Meraki Simple

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. Making this integration possible is the new 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 individual or groups of users connecting to the wireless network.

Bringing the two solutions together, Meraki and Umbrella have collaborated to offer a simple yet powerful integration for Meraki wireless networks to protect the connecting users via Umbrella security policies. To take advantage of the integration, an administrator must create the Umbrella Network Devices API key & secret in their Umbrella dashboard and then apply that API key & secret in a Meraki network under Network-wide > General. After applying the API key/secret, the Meraki dashboard makes an API call to Umbrella to retrieve the organization ID associated with that particular Umbrella account. The organization ID will be used as a query parameter for subsequent API calls made by the Meraki dashboard.

![Figure 2. Umbrella Network Devices API key creation in dashboard.umbrella.com](image)

![Figure 3. Applying the API key to a Meraki network in the Network-wide > General page](image)
Once the API key & secret is present in the Meraki network, administrators can then navigate to the Wireless > Firewall & Traffic Shaping page, and choose an SSID with which they’d like to link Umbrella policies to.

By clicking 'Link Umbrella policies', the Meraki Dashboard will make an API call to register the SSID as a Network Device identity in Umbrella. The naming convention for the network device identity will be `<SSID/group policy name>_<Meraki network name>`, as shown below. The same process and behavior will be seen when linking group policies to Umbrella policies.

![Figure 4. Linking Umbrella policies to a Meraki SSID](image)

![Figure 5. Viewing the network device identity and associated policy in Umbrella](image)
Upon linking Umbrella policies with an SSID or group policy, the administrator will be able to choose which security policy they wish to apply to the given SSID or group policy. Another API call is made that will list out the various security policies available to choose from that are associated with that Umbrella organization ID.

Figure 6. List of Umbrella policies for an Umbrella organization retrieved via backend API call
Upon selecting the policy and saving changes, another API call is made to link the policy with the network device in Umbrella.

![Figure 7. Dynamically reflecting the network device identity tied to a security policy in Umbrella](image)

However, the integration works both ways. Changes made regarding network device identities or policies in the Umbrella dashboard will automatically update and reflect in the Meraki dashboard as well. For example, an administrator may link an SSID to an Umbrella policy, but then decide that they want to rename that policy. Or perhaps they want to change the policy assigned to that network device, or even assign other network devices to that same policy. All of this could be done in the Umbrella dashboard, and will dynamically update the relevant configuration and UI in the Meraki dashboard as well.

Removing linked policies from an SSID or group policy in the Meraki Dashboard is done by simply clicking the ‘Disconnect from Umbrella’ button, which will trigger an API call to remove the network device associated with the SSID/group policy.
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 8. 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.

Figure 9. 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.