meraki

White Paper

Layer 7 Visibility and Control

FEBRUARY 2013

This document highlights the foundation of Meraki's self-learning layer 7 traffic analytics engine and the rich visibility and intuitive management that it facilitates.

Table of Contents

1 Introduction

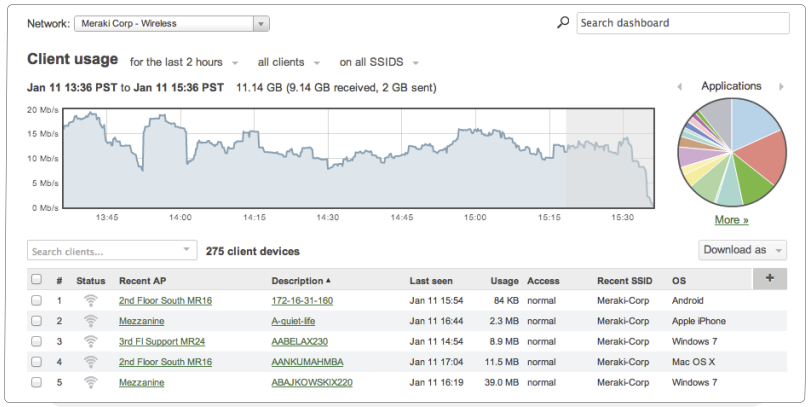
The Value of Application Visibility

An increasing reliance on Internet access for corporate productivity has created an expectation of high performance and ubiquitous connectivity in the enterprise. In parallel, bring your own device (BYOD) and cloud computing trends have led to a rapid proliferation in the number of devices and applications used in enterprise networks. These factors can strain traditional networks and create issues such as bottlenecks in network performance. It is often considered important to deliver high performance and application optimization within the context of constrained costs, finite bandwidth capacity, and an expectation to deliver a minimum quality of service (QoS) for critical applications. Meeting these requirements can be challenging for budget and time-constrained IT departments.

Two factors are critical for addressing these challenges: clear, concise insight into network performance, and an ability to enforce network policies that optimize the network's performance. Network admins must be armed with complete knowledge of network utilization, not only in terms of bandwidth, but also across all layers, even to the application level. Understanding the devices and users accessing specific applications, and the amount of time spent and traffic flowing on each, can provide valuable context to understand user behavior and prompt the design of effective network policies. Finally, a built-in toolset that allows for the creation and application of flexible policy sets can ensure that application information can be acted upon by the IT admin to help deliver optimal network performance.

An emerging use of application visibility is to leverage this data to enhance customer engagement via interactive campaigns and targeted experiences. Understanding the flow of applications, users, and time spent can help the marketing department of a retail outlet or hotspot provider answer the age-old question: 'What are my users doing?' This level of visibility and the actionable data it provides is yet another reason to require application-layer visibility in networking infrastructure.

The Value of Application Visibility (cont.)



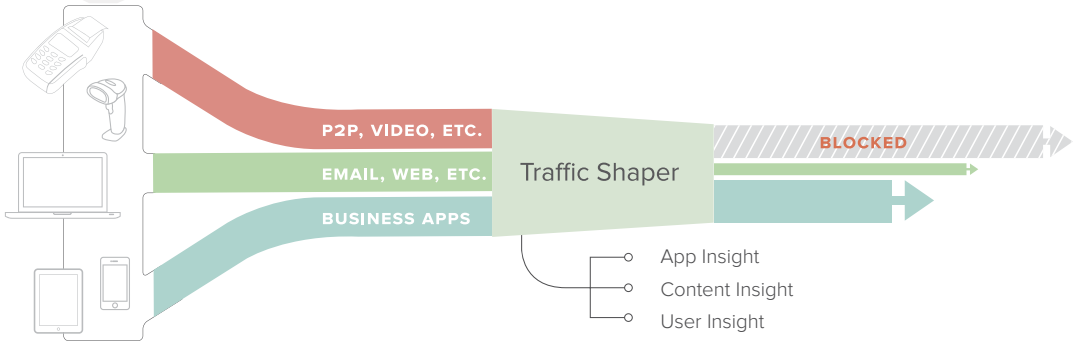


FIGURE 1

Traffic analysis and shaping engine

Meraki's unique traffic analytics engine provides visibility across all layers of the network stack, ranging from the port and protocol layer up to the application layer (e.g., Facebook and YouTube). In addition, Meraki's latest enhancements (released in 2013) include deep statistical analysis of parameters such as time spent per user and per application on a flow-by-flow basis; this provides valuable context on user behavior instead of an aggregate dump of all applications accessed on the network. Finally, Meraki's ability to create Layer 7 application firewall and traffic rules and apply these on a per-group basis provides the network admin with a rich toolbox for customization and optimization of their network based on the analytics data presented. Layer 7 traffic analysis is available across Meraki's wireless (MR), switching (MS) and security (MX) product lines, and traffic shaping is available on Meraki's MR and MX product lines. This paper takes a closer look at this innovative functionality.

2 Meraki Traffic Shaping Technology

Deep Packet Inspection and Traffic Signatures

To provide rich traffic analysis capabilities, Meraki wireless, switching, and security products perform deep-packet inspection (DPI) of traffic on the network on a flow-by-flow basis. This analysis is then uploaded in real-time to the Meraki cloud for statistical aggregation from all edge endpoints. Detailed information is made available to a network admin on their Meraki dashboard through customizable network and time formats. Meraki's capabilities include an analysis of various elements, such as IP addresses, host names, and port ranges, which is combined with a behavioral analysis of each traffic flow. This facilitates a deeper categorization of traffic beyond just port or IP-based classification; examples include peer-2-peer (P2P) file-sharing and social gaming sites that are constantly adding servers and cannot therefore be tracked simply by using IP addresses.

The inspection of thousands of traffic patterns over several years led Meraki to create a database of traffic signatures that can be used to recognize network traffic at the application level. An especially challenging task is the recognition of peer-to-peer traffic, which has traditionally been very difficult to pin down due to the constantly changing IP addresses and port ranges; via careful analysis of torrent traffic streams, Meraki created a heuristic signature that recognizes short TCP sessions across a fleeting range of IP addresses, allowing for the classification of P2P traffic. Similar heuristics are applied in the absence of any specific identifying information for a range of applications; these heuristics comprise a library of Meraki's traffic signatures, and are maintained in Meraki's cloud, allowing for rapid updates based on the discovery and analysis of new traffic patterns. In addition, the ability for the network admin to create custom signatures using host names, IP address ranges, and ports allows for tracking traffic to specific destinations. For example, an admin can create signatures to track activity such as employee access to a local web or email server.

Granular Analytics

New applications, protocols and traffic patterns are continuously emerging. While providing an overarching traffic signature can be a compelling way to reduce complexity, admins often desire deeper granularity and a more detailed breakdown of which IP addresses or host names were being accessed for traffic signatures such as 'miscellaneous web'.

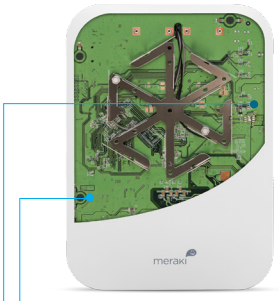
FIGURE 2
Screenshot of Meraki dashboard showing breakdown of web traffic

Destination	Protocol	Port	% Usage	Usage	Sent	Received	# clients	Active time per client ▾
mail.google.com	TCP	443	20.6%	17.77 GB	7.70 GB	10.08 GB	222	29 hours
na4.salesforce.com	TCP	443	4.6%	3.99 GB	914.0 MB	3.10 GB	167	9 hours
mops.geckoboard.com	TCP	443	<0.1%	18.3 MB	9.6 MB	8.8 MB	1	6.9 hours
docs.google.com	TCP	443	1.8%	1.58 GB	997.4 MB	616.6 MB	192	6.5 hours
0.drive.google.com	TCP	443	<0.1%	22.2 MB	18.7 MB	3.5 MB	6	6.5 hours
zcd-01.s3-external-1.amazonaws.com	TCP	443	1.3%	1.11 GB	17.2 MB	1.09 GB	1	5.1 hours
www.google.com	TCP	443	1.2%	1.05 GB	425.8 MB	648.5 MB	214	3.9 hours
d1t1fzb7fr.app02-17.join.me	TCP	443	0.4%	385.5 MB	9.6 MB	375.9 MB	1	3.9 hours

The need to provide deeper visibility into traffic led to the development of a new classification scheme that allows for the dynamic creation of signatures based on host names and IP addresses. Examples include a signature for 'mail.company.com' to provide visibility into unique traffic flows and a granular host name and IP address breakdown of a category such as 'Dropbox' to allow deeper inspection of the specific IP addresses and host names contributing to this application. This breakdown is especially useful for broad categories such as 'Non-web TCP', and provides a detailed breakdown of all of the websites that were visited within this category. This new learning engine allows for the dynamic creation of traffic signatures based on traffic patterns, and provides deeper visibility to admins seeking to understand what their users are doing.

Deep Packet Inspection at Line Rate

Leveraging powerful hardware components that were selected with rich capabilities such as traffic analysis in mind, Meraki products perform traffic analysis inspection and classification at line rate, ensuring no drop in performance when used in conjunction with the numerous other features available. For example, Meraki's MX security appliance can run traffic shaping in conjunction with Auto VPN to dozens of other sites in a mesh VPN topology, all at line rate whilst passing hundreds of megabits of traffic. A careful selection and design of silicon components was required to tightly integrate hardware and software for optimized performance.

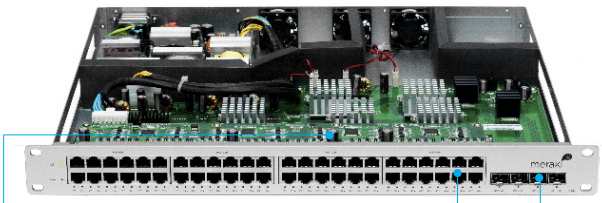


- Enhanced CPU: Layer 3-7 firewall and traffic shaping
- 3x3 MIMO, dual 802.11 radios with 3 spatial streams for up to 900 Mbps

FIGURE 3
Highly optimized hardware and software integration allows for line-rate processing

Integrated Cloud Management

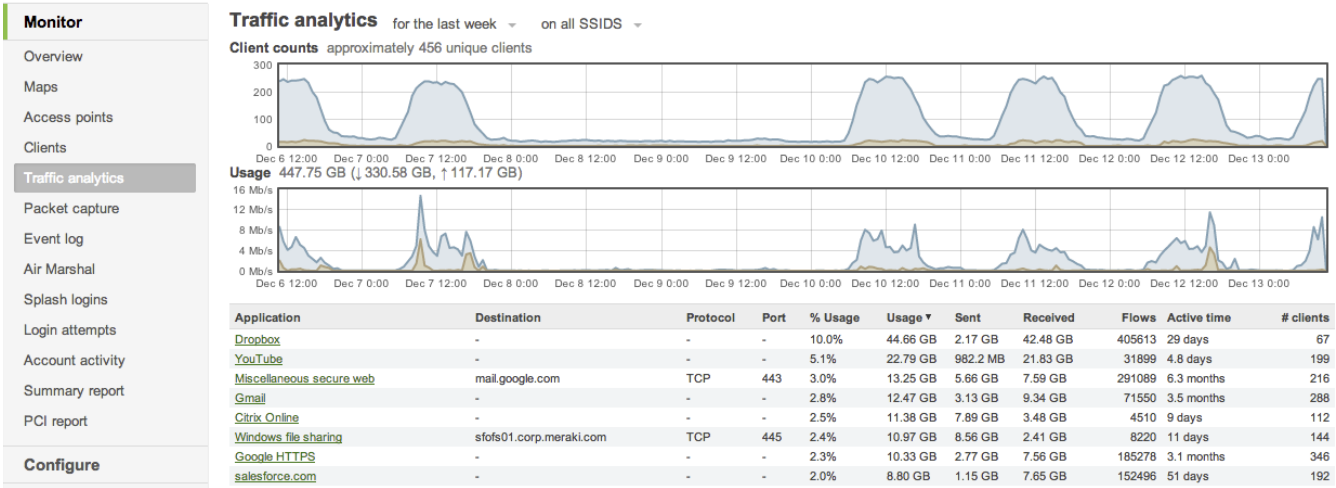
Meraki's hardware products and cloud maintain a tight feedback loop through a highly compressed 1 kbps management tunnel, which includes traffic analytics and configuration information such as network settings. In addition to traffic signatures being pushed from the cloud to the edge and traffic flows data being pushed back to the cloud, additional context information is sent on a per-flow basis, including users and applications, and the per-user average and total user time spent on each application or website.



- 48 x 1 GbE Ports with 802.3af/802.3at PoE/PoE+
- Enhanced CPU/ memory Meraki cloud management
- Built in 4x 10 GbE SFP+ ports for core connectivity / stacking

- Enhanced CPU: Layer 3-7 firewall and traffic shaping
- Additional memory for content filtering

FIGURE 4
Cloud-based management and reporting



Application	Destination	Protocol	Port	% Usage	Usage ▾	Sent	Received	Flows	Active time	# clients
Dropbox	-	-	-	10.0%	44.66 GB	2.17 GB	42.48 GB	405613	29 days	67
YouTube	-	-	-	5.1%	22.79 GB	982.2 MB	21.83 GB	31899	4.8 days	199
Miscellaneous secure web	mail.google.com	TCP	443	3.0%	13.25 GB	5.66 GB	7.59 GB	291089	6.3 months	216
Gmail	-	-	-	2.8%	12.47 GB	3.13 GB	9.34 GB	71550	3.5 months	288
Citrix Online	-	-	-	2.5%	11.38 GB	7.89 GB	3.48 GB	4510	9 days	112
Windows file sharing	sfofs01.corp.meraki.com	TCP	445	2.4%	10.97 GB	8.56 GB	2.41 GB	8220	11 days	144
Google HTTPS	-	-	-	2.3%	10.33 GB	2.77 GB	7.56 GB	185278	3.1 months	346
salesforce.com	-	-	-	2.0%	8.80 GB	1.15 GB	7.65 GB	152496	51 days	192

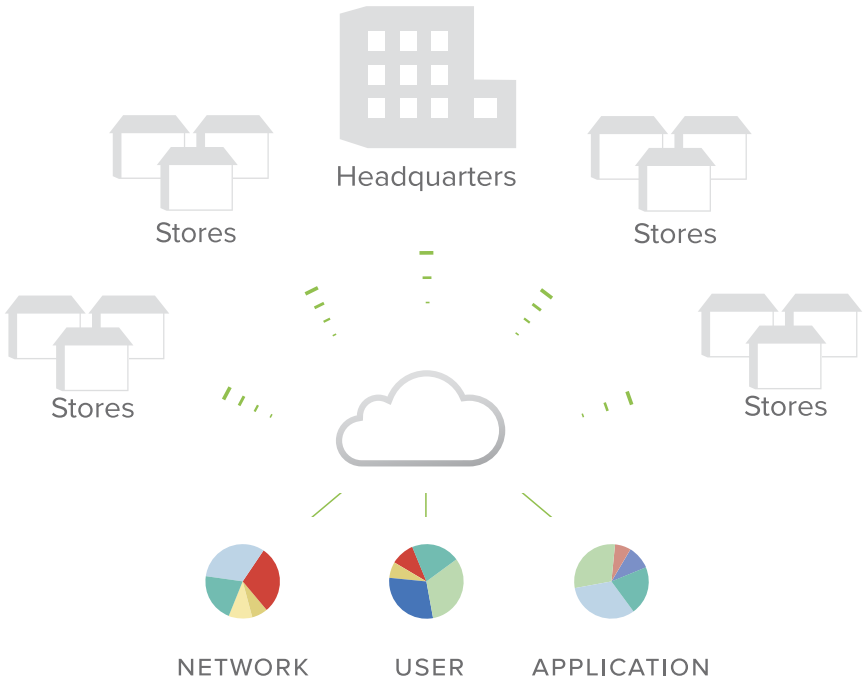


FIGURE 5
Cloud architecture facilitates traffic analysis at scale

The Meraki cloud leverages the processing capabilities of a distributed data center architecture to aggregate and display traffic analysis data on a per-network, per-SSID, or per-user basis across a customizable time period. Data aggregation allows for a consolidated view of traffic information across multiple geographic sites. Aggregated summary reports provide daily, weekly or monthly views include data on top devices, users and applications. Networks can be configured to encompass one or multiple sites for the desired reporting structure. Meraki's network tagging engine allows multiple networks to be allocated specific tags (e.g., 'Starbucks' for a group of 100 Starbucks networks), which allows for a hierarchal classification and reporting for networks in large-scale deployments.

Traditional databases would take hours to deliver a query on a per-user or per-application basis when considering a deployment of thousands of geographically dispersed end-devices and tens of thousands unique applications accessed. Meraki's cloud architecture is powered by a highly optimized software stack designed for untethered scalability (similar to the architectural design of Google and Facebook). Instead of relying on traditional databases, a proprietary database was developed in-house to facilitate rapid, real-time searches. This unique database, while powering a tremendously large data set, delivers the ability to search through and poll data within mere seconds as opposed to minutes.

Data to enhance the user experience

Traffic analysis and granular user-level data enable decision-making beyond the realm of network performance optimization. Marketing departments in retail, hospitality, and even the enterprise can use this data to make decisions on how to engage and interact with their customers more effectively. Meraki's external captive portal (EXCAP) API can be used to create custom customer onboarding experiences, and these experiences can be shaped and customized based on demographic or individual-level trends (e.g. 'my shoppers use Facebook heavily, so I should tie Facebook login with my splash servers'). Marketing departments with advertising budgets can also use this data to analyze which websites their users are trafficking, and can choose to advertise on these websites to help track and maximize the effectiveness of their own advertising strategies.

Finally, all traffic analysis information is fully opt-in, and on Meraki's MR wireless line, it is also possible to configure a group policy to opt-out a specific user or group from granular hostname-level visibility. These features are designed to provide the IT admin with greater flexibility in designing their privacy policies.

3 Management & Control

Accompanying application-level visibility is Meraki's traffic shaping engine, providing powerful management that allows for the creation and application of time and context-aware policies for QoS and prioritization based on user and network groups. Meraki's traffic shaping engine includes restrictive policies such as application firewalling or throttling and constructive policies which allow for specific classes of applications to ignore bandwidth limits and have preferred priority set across network layers using tools such as PCP and DSCP tagging. On Meraki's wireless product line, these policies can be created and applied using a range of variables through the Meraki Dashboard or via integration with a RADIUS server using RADIUS attributes. Policies can be applied across one or more users or user groups, or by network or time.

Used in conjunction with Meraki's traffic analytics capabilities, traffic and group policies can facilitate an effective classification and prioritization of application and bandwidth usage on a per-user or per-network basis. Examples include the creation of two separate SSIDs in a school environment (e.g. 'Teachers' and 'Students') with different bandwidth limits and firewalls for video traffic, and the segregation of regular employees and executives in an enterprise environment on a single 'Enterprise' SSID.

Policy Variables

1. L7 firewall/traffic shaping
2. L3 firewall
3. Bandwidth limits
4. Prioritize using PCP/DSCP tags in L2/L3

Application Variables

1. By individual user or user group
2. By device type
3. By SSID (availability can be time-based)

Application Method

1. Manually via client search in Meraki dashboard
2. Automatically via device fingerprinting
3. Via 802.1X/RADIUS server using Filter-ID or other RADIUS attribute

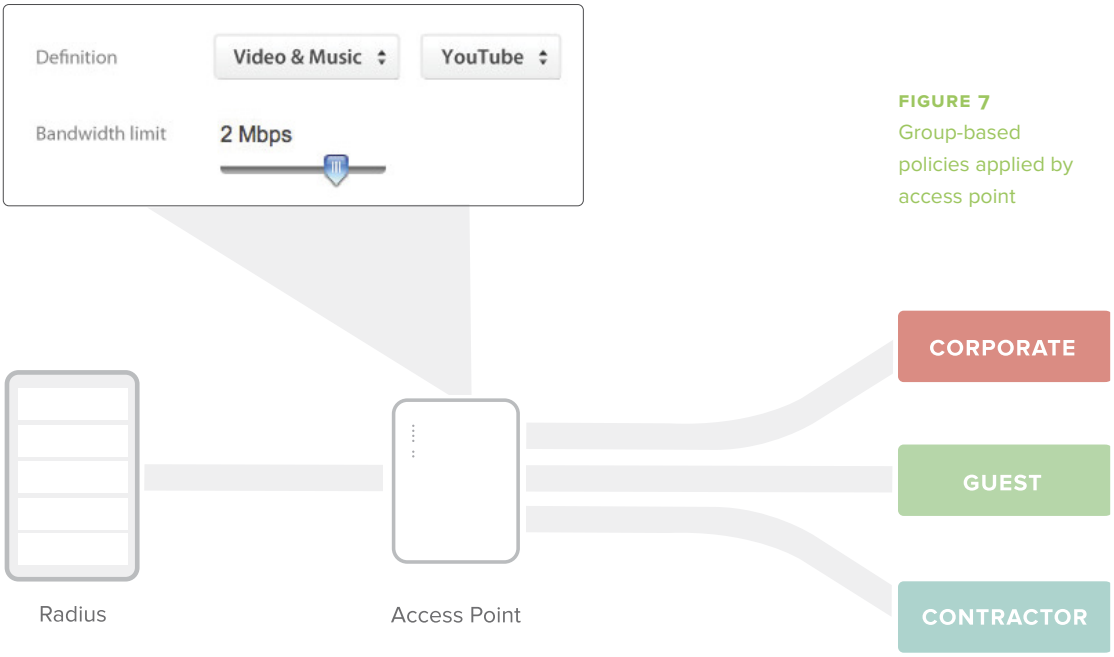


FIGURE 7
Group-based policies applied by access point

Meraki, Inc. | 660 Alabama St, San Francisco, CA 94110 | (415) 432-1000 | sales@meraki.com

Create Group Policies with Different Traffic Rules

Apply Policies to Groups of Users

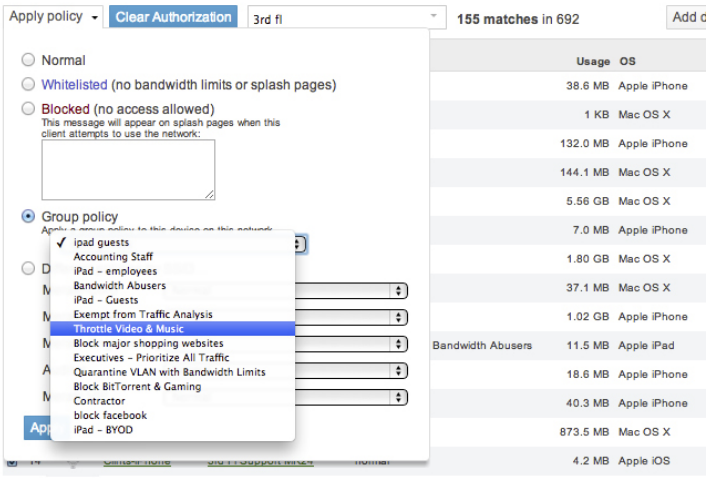
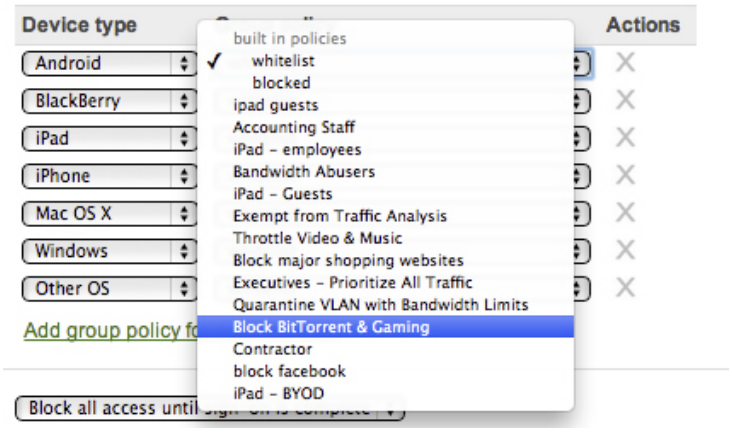


FIGURE 6
Creating and applying group policies in the Meraki Dashboard

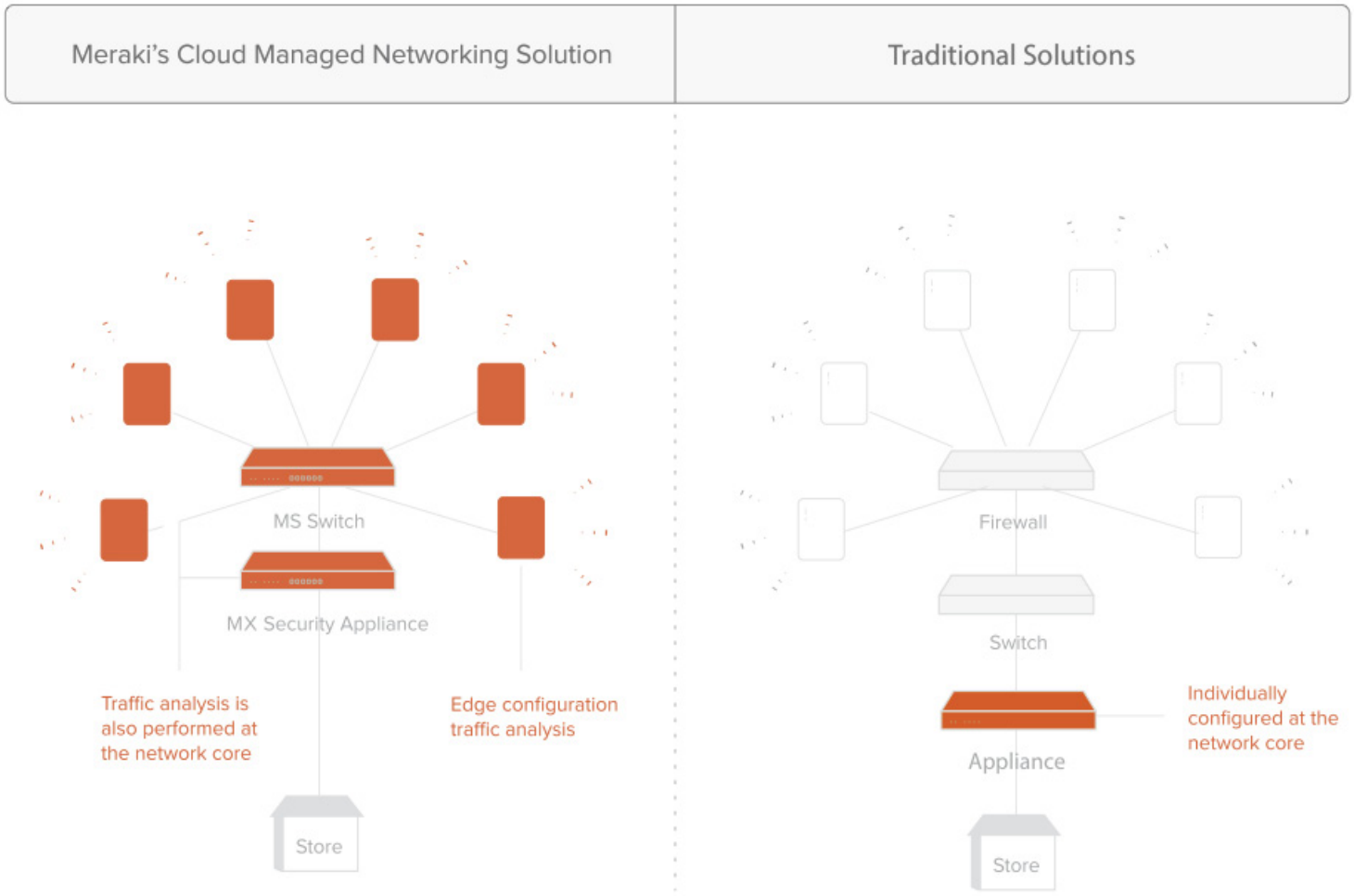
Apply Policies by Device Type



Meraki, Inc. | 660 Alabama St, San Francisco, CA 94110 | (415) 432-1000 | sales@meraki.com

4 Comparison With Traditional Solutions

Application-level visibility is not a new concept; several companies have built solutions for delivering Layer 7 visibility to provide administrators with insight into network performance. Similarly, tools are available that provide the ability to create and apply application-level firewalls and shaping rules. However, Meraki's approach is an industry-first in multiple regards, ranging from scalable processing power at the edge across both wired and wireless product lines, to leveraging the cloud databases for big data processing and indexing to deliver statistics in customizable formats. These benefits make Meraki the optimal solution for traffic visibility and policy management.



Meraki, Inc. | 660 Alabama St, San Francisco, CA 94110 | (415) 432-1000 | sales@meraki.com

Meraki's application-layer analysis is performed at the edge across our wired or wireless product lines, whereas traditional solutions have required a consolidated and dedicated appliance somewhere within the network core. The requirement to have a centrally positioned appliance can present numerous disadvantages, including (a) the need to specifically architect the network such that all traffic flows through this appliance, (b) the creation of a single point of failure, and (c) limited scalability due to constrained CPU from a single appliance. Separate appliances also come with a high cost and are often licensed on an endpoint basis, which can lead to spiralling costs if there are large numbers of edge devices (e.g. 1000 APs). Meraki's traffic analysis capabilities are baked into the cost of an Enterprise Cloud license (and so are the recent analytics upgrades).

Secondly, Meraki is able to leverage the power of its cloud platform for rapid aggregation, analysis and customized presentation of statistics based on adjustable variables. Examples include being able to view consolidated statistics in a single view across multiple geographical sites, along with per-network, per-user and per-application breakdowns with the ability to sort and customize the data that is being viewed. Leveraging Meraki's rapidly growing custom databases and geographic data-center spread, 'big data' processing is possible, which allows for a large-scale synthesis and presentation of network statistics that would not be possible in single-box or enterprise-hosted architectures.

Finally, Meraki's MR and MX wireless and security appliance lines come coupled with the ability to create and apply custom application signatures and traffic shaping policies, which allow for network optimization based on perceived network trends. Leveraging Meraki's powerful device fingerprinting and real-time client searches, it is possible to filter and apply policies to custom groups of users quickly. Following the policy creation and application, an ability to measure the policy impact in terms of application and network usage is also key. Measuring the impacts of policy changes is also intuitive via the Meraki Dashboard, and this visibility facilitates quick adjustments to policies to help administrators track and optimize their network performance in a manner not otherwise possible with traditional enterprise equipment.

Conclusion

Providing greater visibility beyond simple network management allows admins to understand user behavior and network utilization on their infrastructure. Meraki's policy management tools facilitate the creation of application-aware firewall and traffic shaping rules that can be used to optimize network performance and deliver a high quality of experience for end-users. By using Meraki, administrators can now count on rich application-layer insights across their edge access layer to fully understand user behavior. They can then leverage a flexible policy toolkit that allows for the creation and application of specific application policies down to a per-user basis. Both traditional IT staff and marketing departments can use Meraki's MX, MS and MR product lines to obtain the visibility required to optimize network performance, and ultimately build a scalable application-aware architecture that is built to last for the new BYOD and cloud apps era.

Meraki, Inc. | 660 Alabama St, San Francisco, CA 94110 | (415) 432-1000 | sales@meraki.com