Meraki as Cisco Cloud Services
Manage your network Where ever you are !

Marketing/Technical description for services

Scope of the Service

Cloud services can deliver big technology benefits to midsized and large organizations who don’t have the budget to buy expensive hardware and software or employ a large staff of full-time IT professionals. Cloud services can help you rapidly introduce new services to meet your business’s needs, and make you more agile and competitive.

Today world required mobility and as IT Managers you should reach and maintain your infrastructure whenever required, mean you should act indepndent of time and place.

In traditional systems, you have to spend additional effor and cost to get management and reporting tools where bring incremental budget.

What Meraki offer as Cloud based Management is like as gift for IT Admins, you can access your network resources whenever and wherever you are. Plus, it provide many report tools as default, even platform is developing everyday for fuatures and you can find additional benefery tools every month.

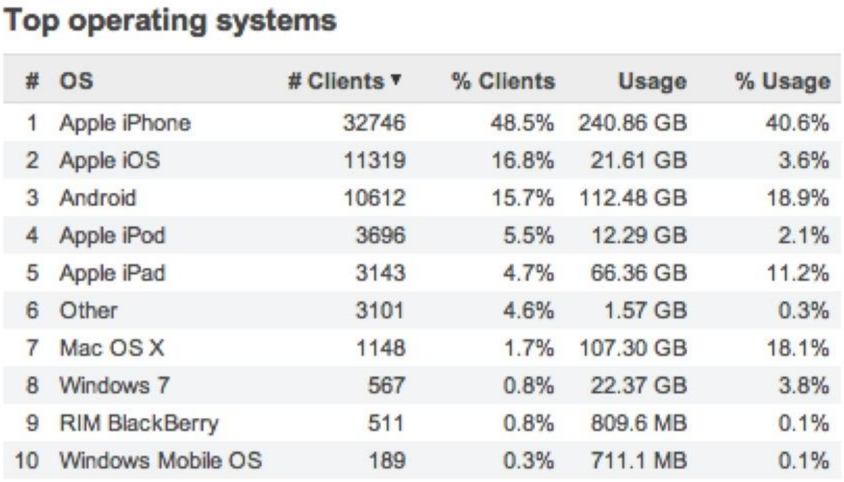
Deep packet inspection

A modular and flexible packet processing engine delivers consistent, high-performance application traffic shaping within product families and across product lines. This custom-built Layer 7 technology uses a variety of techniques to identify and control hundreds of applications.

Going far beyond IP addresses, hostnames, and ports, Layer 7 deep packet inspection uses heuristics-based identification to classify traffic based on application, even identifying evasive, dynamic, and encapsulated apps. High performance hardware enables inspection, classification, and traffic shaping at line-rate inside Cisco Meraki devices.

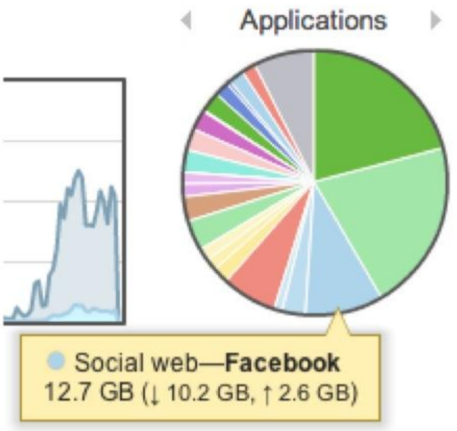
Rich, detailed analytics for deep insight

Rich analytics deliver breakthrough visibility into guest activity and shopper profiles. See detailed reports on mobile devices, web traffic, and popular smartphone applications, such as price comparison apps.



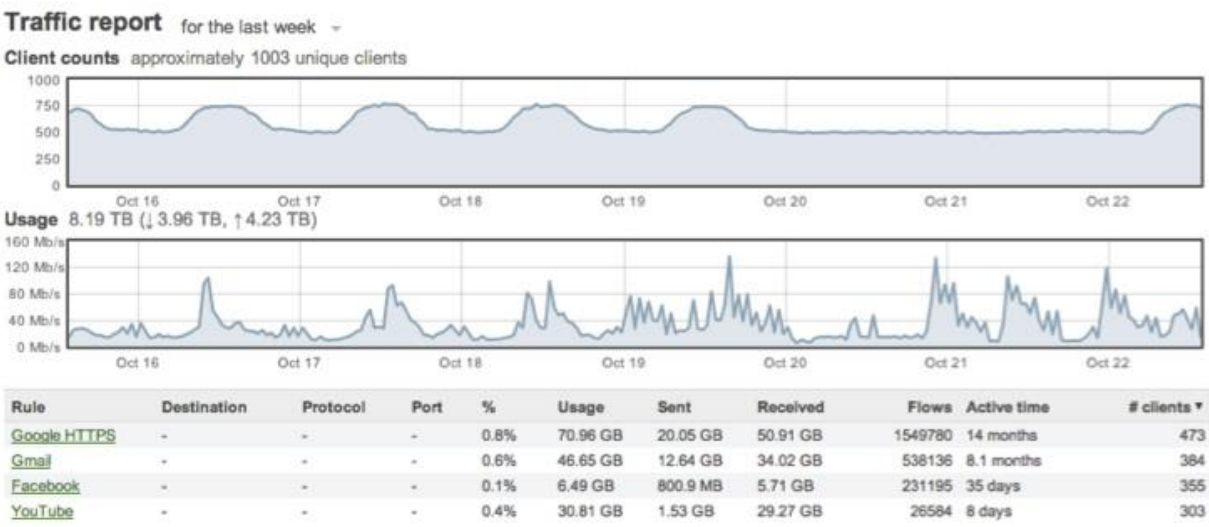
Top operating systems

#	OS	# Clients ▾	% Clients	Usage	% Usage
1	Apple iPhone	32746	48.5%	240.86 GB	40.6%
2	Apple iOS	11319	16.8%	21.61 GB	3.6%
3	Android	10612	15.7%	112.48 GB	18.9%
4	Apple iPod	3696	5.5%	12.29 GB	2.1%
5	Apple iPad	3143	4.7%	66.36 GB	11.2%
6	Other	3101	4.6%	1.57 GB	0.3%
7	Mac OS X	1148	1.7%	107.30 GB	18.1%
8	Windows 7	567	0.8%	22.37 GB	3.8%
9	RIM BlackBerry	511	0.8%	809.6 MB	0.1%
10	Windows Mobile OS	189	0.3%	711.1 MB	0.1%



User analysis and control

A detailed traffic report page identifies web sites shoppers access most frequently and reports browsing time spent on each. Track users' locations in large retail environments and monitor employee scanner or POS devices. Throttle bandwidth for high-bandwidth apps, and even block access to undesired sites, such as competitors' or online stores.

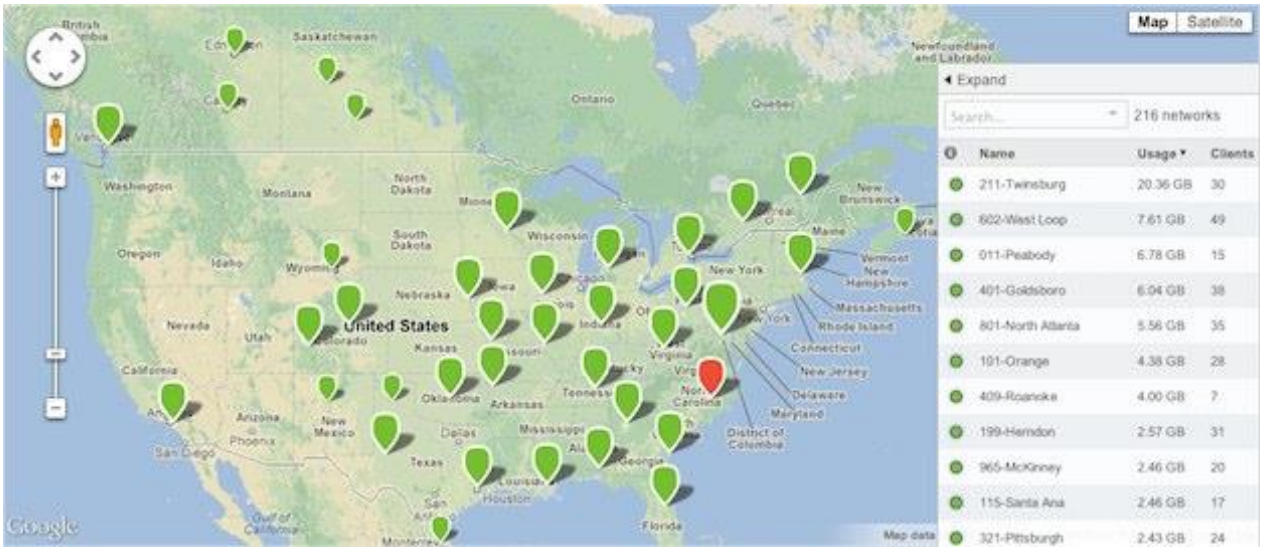


Rule	Destination	Protocol	Port	%	Usage	Sent	Received	Flows	Active time	# clients ▾
Google HTTPS	-	-	-	0.8%	70.96 GB	20.05 GB	50.91 GB	1549780	14 months	473
Gmail	-	-	-	0.6%	46.65 GB	12.64 GB	34.02 GB	538136	8.1 months	384
Facebook	-	-	-	0.1%	6.49 GB	800.9 MB	5.71 GB	231195	35 days	355
YouTube	-	-	-	0.4%	30.81 GB	1.53 GB	29.27 GB	26584	8 days	303

Centralized multi-site management via the cloud

The Cisco Meraki cloud-managed architecture enables plug and play branch deployments and provides centralized visibility and control across any number of distributed locations.

Since Cisco Meraki networks are managed entirely through the Cisco Meraki web-based dashboard, configuration and diagnostics can be performed remotely just as easily as they can be performed on-site, eliminating costly field visits.



	Name	Usage ▾	Clients
●	211-Twinsburg	20.36 GB	30
●	602-West Loop	7.61 GB	49
●	011-Peabody	6.78 GB	15
●	401-Goldsboro	6.04 GB	38
●	801-North Atlanta	5.56 GB	35
●	101-Orange	4.38 GB	28
●	409-Roanoke	4.00 GB	7
●	199-Herndon	2.57 GB	31
●	965-McKinney	2.46 GB	20
●	115-Santa Ana	2.46 GB	17
●	321-Pittsburgh	2.43 GB	24

Zero-touch remote site deployment

Cisco Meraki devices self-provision, enabling branch deployments without on-site IT.

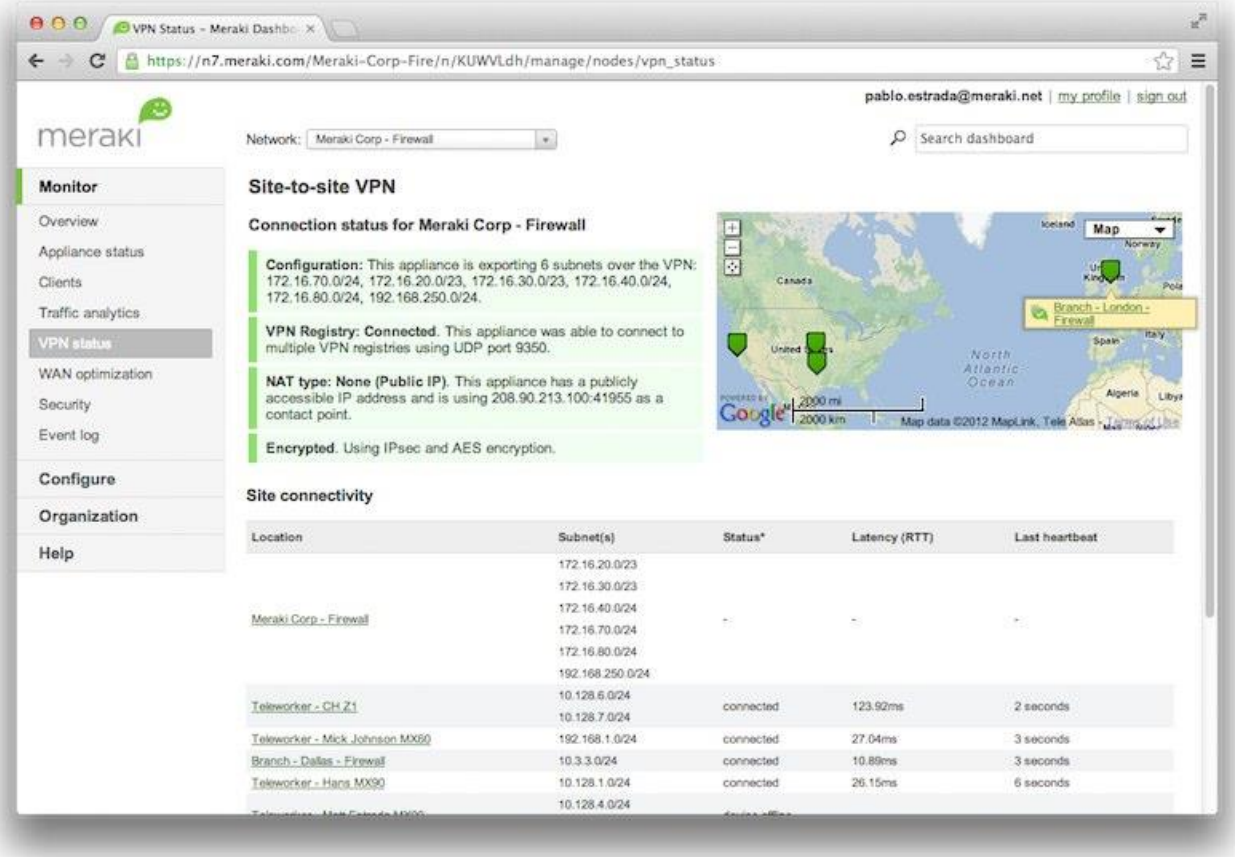
Each device downloads its configuration via the Cisco Meraki cloud, applying your network and security policies automatically so you don’t have to provision on-site. Wireless APs optimize their RF configuration based on the environment, and switches integrate seamlessly into existing RSTP domains.

Adding new sites to a network takes minutes, not hours or days, and there’s no need to train additional staff to monitor or manage the remote networks.

Self-provisioning VPN networks

Cisco Meraki’s unique auto provisioning site-to-site VPN connects branches securely with complete simplicity. Using IPsec over any wide area network, MX Security Appliances seamlessly link your branches to headquarters and to one another.

Site-to-site connectivity is established through a single click in the Cisco Meraki dashboard. Gone are the configuration headaches of traditional site-to-site VPNs: route discovery, authentication, and security policies are all handled automatically from the cloud. Full- and split-tunnel VPNs are configured with a single drop-down, and new sites are added with a few simple clicks.


VPN Status - Meraki Dashbo
https://n7.meraki.com/Meraki-Corp-Fire/n/KUWVLdh/manage/nodes/vpn_status
meraki
pablo.estrada@meraki.net | my profile | sign out
Network: Meraki Corp - Firewall
Search dashboard
Monitor
Overview
Appliance status
Clients
Traffic analytics
VPN status
WAN optimization
Security
Event log
Configure
Organization
Help
Map
Iceland
Norway
Canada
United States
Spain
Italy
Algeria
Libya
North Atlantic Ocean
Branch - London - Firewall
2000 mi
2000 km
Map data ©2012 MapLink, Tele Atlas - Terms of Use

Site-to-site VPN

Connection status for Meraki Corp - Firewall

Configuration: This appliance is exporting 6 subnets over the VPN: 172.16.70.0/24, 172.16.20.0/23, 172.16.30.0/23, 172.16.40.0/24, 172.16.80.0/24, 192.168.250.0/24.

VPN Registry: Connected. This appliance was able to connect to multiple VPN registries using UDP port 9350.

NAT type: None (Public IP). This appliance has a publicly accessible IP address and is using 208.90.213.100:41955 as a contact point.

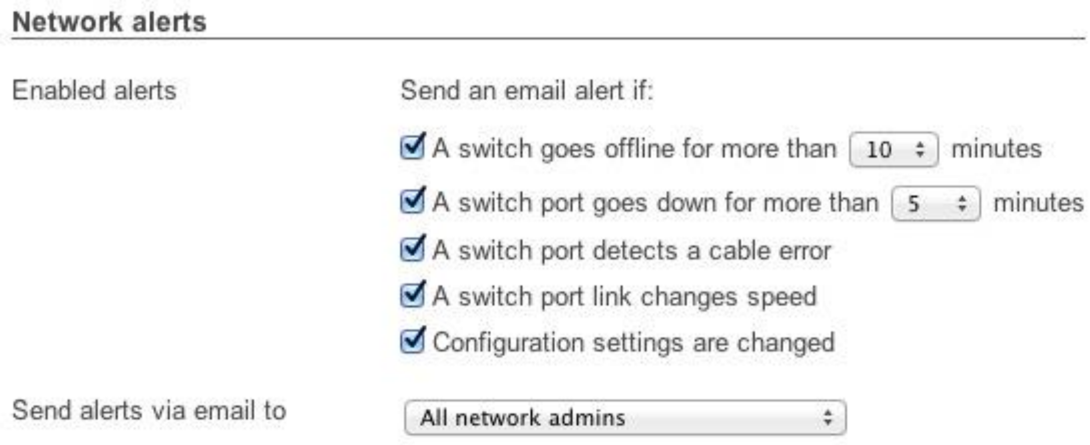
Encrypted. Using IPsec and AES encryption.

Site connectivity

Location	Subnet(s)	Status*	Latency (RTT)	Last heartbeat
Meraki Corp - Firewall	172.16.20.0/23 172.16.30.0/23 172.16.40.0/24 172.16.70.0/24 172.16.80.0/24 192.168.250.0/24	-	-	-
Teleworker - CH Z1	10.128.6.0/24 10.128.7.0/24	connected	123.92ms	2 seconds
Teleworker - Mick Johnson MX60	192.168.1.0/24	connected	27.04ms	3 seconds
Branch - Dallas - Firewall	10.3.3.0/24	connected	10.89ms	3 seconds
Teleworker - Hans MX90	10.128.1.0/24	connected	26.15ms	6 seconds
	10.128.4.0/24			

Automated monitoring and alerts

Each Cisco Meraki device is automatically monitored from the cloud, with continuous testing for WAN connectivity, latency, and more. The Cisco Meraki dashboard notifies you of problems via email alerts, and provides rich web-based diagnostics to troubleshoot your network from any web browser.



Network alerts

Enabled alerts

Send an email alert if:

☑ A switch goes offline for more than 10 minutes

☑ A switch port goes down for more than 5 minutes

☑ A switch port detects a cable error

☑ A switch port link changes speed

☑ Configuration settings are changed

Send alerts via email to: All network admins

Dedicated radio for continuous monitoring

Cisco Meraki access points feature a third radio dedicated to continuously and automatically monitoring surroundings to maximize Wi-Fi performance. By measuring channel utilization, signal strength, throughput, signals from non-Meraki APs, and non-WiFi interference, Cisco Meraki APs automatically optimize WiFi performance of individual APs and maximize system-wide performance.

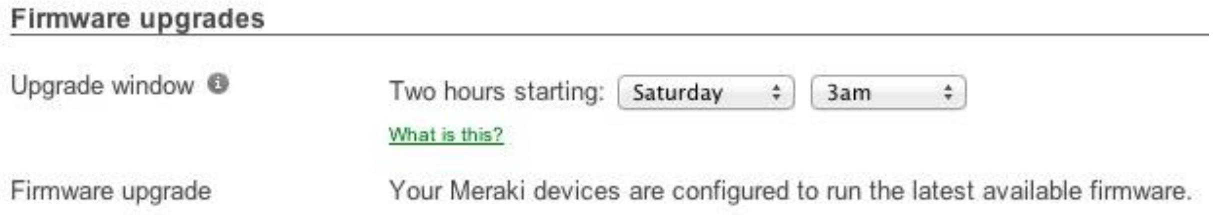
Adaptive configuration for optimal performance

Real-time and historical metrics ensure maximum system-wide performance. Wireless channels, AP output power, and client connection settings are automatically adapted to changing performance and interference conditions, eliminating the need for tedious manual adjustment of dozens of independent parameters.

Seamless firmware updates

Firmware updates are delivered seamlessly from the cloud to Cisco Meraki devices. When firmware updates are available, an administrator simply schedules an appropriate time for devices to download and install the new version, eliminating insecure and out of date firmware.

Maintain compliance with security requirements without deciphering compatibility matrices, performing time consuming manual updates, or visiting branch locations to upgrade hardware.



Firmware upgrades

Upgrade window	Two hours starting: Saturday 3am
Firmware upgrade	Your Meraki devices are configured to run the latest available firmware.

For more information :
https://meraki.cisco.com/solutions/branch-networking