Ecole Lemania

Schweizer Schule nutzt komplettes cloud-managed Portfolio von Cisco Meraki für verlässliches Networking in Klassenzimmern und Wohnheimen

- Mehrsprachige Schweizer Schule mit Schülern aus der ganzen Welt
- Zuverlässiges und leistungsfähiges Netzwerk durch Meraki APs, Switches und Security
- Abgestimmte Kontrolle der Endbenutzergeräte durch benutzerdefinierte Richtlinien

LEMANIA
Ecole Lémania - Lausanne

Die Ecole Lémania ist zu Recht stolz auf ihr ganzheitliches Bildungsangebot, mit dem Schüler und Studenten jeden Alters darauf vorbereitet werden, mithilfe ihres erworbenen Wissens die Zukunft zu gestalten. Zur Umsetzung dieses Ziels benötigen Dozenten und Schüler Zugriff auf Technologie und die erforderlichen Ressourcen, um aktuelle gesellschaftliche Trends zu gestalten. Die Bereitstellung eines zuverlässigen Netzwerks zur Unterstützung der täglichen Anforderungen der Schule ist für Leonard Jan, IT-Manager an der Ecole Lémania, von entscheidender Bedeutung.

Die Schule ist am Ufer des Genfer Sees in Lausanne (Schweiz) gelegen. Hier werden über 400 Schüler im Alter zwischen 12 und 18 Jahren an einem mehrsprachigen Gymnasium unterrichtet, und 900 Erwachsene absolvieren jährlich Kurse, die sich beispielsweise mit den Bereichen Wirtschaftswissenschaften, Rechnungswesen und Handel befassen. Aufgrund von Beschwerden vieler Benutzer wusste Jan, dass das bisherige System alles andere als ideal war. Das System stürzte oft alle paar Tage oder sogar alle paar Stunden ab. „Vor der Einführung von Meraki war unser Netzwerk ein absoluter Albtraum“, erläutert Jan. „Zwei Internatsschüler haben wegen dieses unzuverlässigen Netzwerks sogar die Schule verlassen!“

Früher bestand das WLAN der Schule aus handelsüblichen Access Points auf jedem Stockwerk. In zwei Hauptgebäuden herrschten jedoch äußerst schwierige WLAN-Bedingungen: sehr dicke Mauern in einem Gebäude aus dem Jahr 1908 und Stahlbeton in einem Gebäude aus den 1970er Jahren. Wenn die Endbenutzergeräte einmal die Signale erkannten, funktionierte zumeist die Datenübertragung nicht. Und bei über 400 gleichzeitigen Client-Verbindungen war ein sinnvolles Arbeiten nicht wirklich möglich. Jan suchte nach anderen Lösungen.

Bei seinen Recherchen, wie Universitäten, Krankenhäuser und andere Branchen ähnliche Herausforderungen meisterten, stieß er dann auf die Cisco Meraki-Lösung. Ein paar Stunden nach der Kontaktaufnahme mit Meraki erhielt Jan von einem lokalen Partner in der Schweiz Informationen zu der über die Cloud verwalteten Lösung. Jan hatte zwar auch andere Lösungen in Erwägung gezogen, aber als Meraki kostenlose Netzwerkgeräte zum Testen in der Schule bereitstellte und gemeinsam mit ihm optimale Konfigurationen ausarbeitete, war er überzeugt. „Meraki verstand unsere spezielle Situation als Bildungsträger. Und die angebotene Lösung ist benutzerfreundlich“, so Jan.

Basierend auf der Ortsbesichtigung eines Partners der beiden Hauptgebäude kaufte die Schule mehr als zwanzig Meraki 802.11n/802.11ac Access Points, sechs Switches mit 24 und 48 Ports sowie eine zentrale UTM Security Appliance. Die Elektriker installierten drei bis vier Tage lang neue Ethernet-Kabel in den Gebäuden. Die eigentliche Installation aller Geräte erfolgte jedoch innerhalb eines einzigen Tages. „Dank der automatischen Funktionen von Meraki war der Installationsaufwand minimal“, meint Jan.

Die zentrale Überwachung und Verwaltung der auf die Gebäude verteilten Netzwerkgeräte war für Jan das ausschlaggebende Kaufargument.

Das Cisco Meraki Dashboard bietet Jan viele Konfigurationsmöglichkeiten für das Netzwerk, wie beispielsweise die vollständige Trennung des WLAN vom Security- und Switching-Fabric. Mithilfe der integrierten Reporting-Funktion können die über 1.300 Wireless-Clients, die pro Woche mehr als 3 TB an Daten übertragen, problemlos überwacht werden.

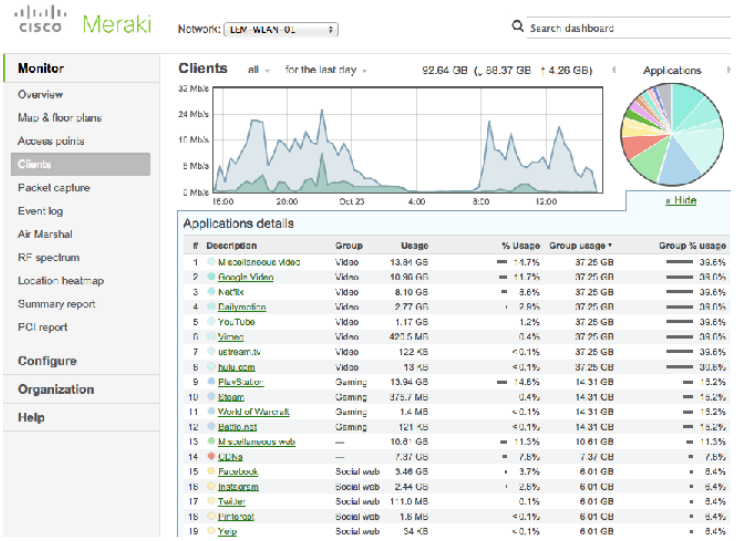
Jan kann mit den integrierten Dashboard-Funktionen bei der Überwachung sogar noch einen Schritt weiter gehen. Die Ecole Lémania hat als Schule verschiedene Netzwerkanforderungen, die speziell für den Bildungssektor gelten, insbesondere dass die Schüler geschützt werden müssen. Mit den Layer-7-Firewall- und Traffic-Shaping-Funktionen kann Jan Beschränkungen festlegen, um den Zugriff auf Peer-to-Peer-Datenverkehr sowie auf jugendgefährdende Inhalte und Softwarepiraterie zu sperren. „Wir können die Geräte der Schüler überwachen und sie bei etwaigen Problemen warnen“, erläutert Jan. „Ignoriert der Schüler die Warnung, können wir eine spezielle Richtlinie auf das Gerät des Schülers anwenden, wodurch der Internetzugriff beschränkt wird.“

“Dank der Berichte im Dashboard können wir die Bandbreitennutzung problemlos überwachen, Missbrauch bei hohem Datenaufkommen verhindern und den Schülern während Ausfallzeiten ‘mehr Freiheiten’ gewähren.”

– Leonard Jan, IT Manager, Ecole Lemania

Durch die Möglichkeit, im Meraki Dashboard jederzeit benutzerdefinierte Richtlinien zu erstellen und zuzuweisen, wird die Verwaltung der verschiedenen BYOD-Geräte, die der Schule, den Mitarbeitern oder den Schülern gehören, für Jan sogar noch einfacher. Eine einzige SSID wird im Zusammenhang mit den verschiedenen Richtlinien verwendet, die je nach Richtlinie Videos, Musik, Spiele, Social-Media-Datenverkehr usw. beschränken. „Dank der Berichte im Dashboard können wir die Bandbreitennutzung problemlos überwachen, Missbrauch bei hohem Datenaufkommen verhindern und den Schülern während Ausfallzeiten ‘mehr Freiheiten’ gewähren“, stellt Jan fest.

Diese Transparenz und die einfache Verwaltung über das Dashboard gelten auch für die Meraki Switches und die Security-Appliance, auf denen das WLAN basiert. Alle APs sind über Cisco Meraki Switches vor Ort verbunden. Für Jan ist es äußerst einfach, im Remote-Modus Konfigurationsänderungen für einzelne Ports über die Cloud-Management-Plattform vorzunehmen. Mit dem Virtual Stacking kann er, ohne den Switch jemals zu berühren, individuell abgestimmte und umfangreiche Änderungen vornehmen, um neuen Anforderungen n in den Unterrichtsräumen Rechnung zu tragen.



Darüber hinaus sind zahlreiche automatische Warnungen konfiguriert, um ihn über mögliche Fehler beim Switch-Fabric zu informieren.

Diese Fehler können von einem Offline-Gerät, über ein fehlerhaftes Kabel bis hin zu einem neu gefundenen DHCP-Server reichen.

Die Meraki Security Appliance befindet sich am Netzwerk-Edge und bietet Jan UTM-Services. Es ist deshalb nicht erforderlich, zahlreiche Switch-Boxes zu beschaffen, und außerdem kann er Kosten einsparen. Wenn Datenanforderungen zwischen Endbenutzergeräten und Endzielen übertragen werden, müssen sie erst die im Dashboard definierten Prüfstufen bestehen. Mit ein paar Mausklicks implementierte Jan Einstellungen wie beispielsweise automatische Malware-Erkennung und IDS mithilfe von Sourcefire, Content-Filterungsregeln zum Blockieren jugendgefährdender Inhalte, Whitelisting zulässiger Websites, Konfiguration von Layer-3-Firewall-Regeln für ausgehenden Datenverkehr, Einrichtung des Mobilfunk-Failovers und Erstellung von VLAN-spezifischen Konfigurationen.

Die vollständige Transparenz, vom Benutzergerät bis hin zum Netzwerk-Core, mithilfe einer umfassenden, intuitiven Benutzeroberfläche ermöglicht Jan eine proaktive Herangehensweise beim Netzwerkmanagement. Das Dashboard eröffnet für Jan bisher unbekannte Möglichkeiten beim Netzwerkmanagement. Beispielsweise kann ein potenzielles Problem identifiziert und behoben werden, bevor es vom Endbenutzer gemeldet wird, oder ein infiziertes Gerät kann ermittelt und der Benutzer gewarnt werden.

„Alle sind mehr als zufrieden. Vor der Einführung von Meraki war das WLAN unbrauchbar oder bestenfalls bescheiden. Jetzt funktioniert alles bestens“, erläutert Jan. „Und damit meine ich auch wirklich alles. Nicht nur die Nutzung durch die Schule, sondern auch durch die Schüler: Skype, Big Data-Downloads, Spiele usw.“

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com