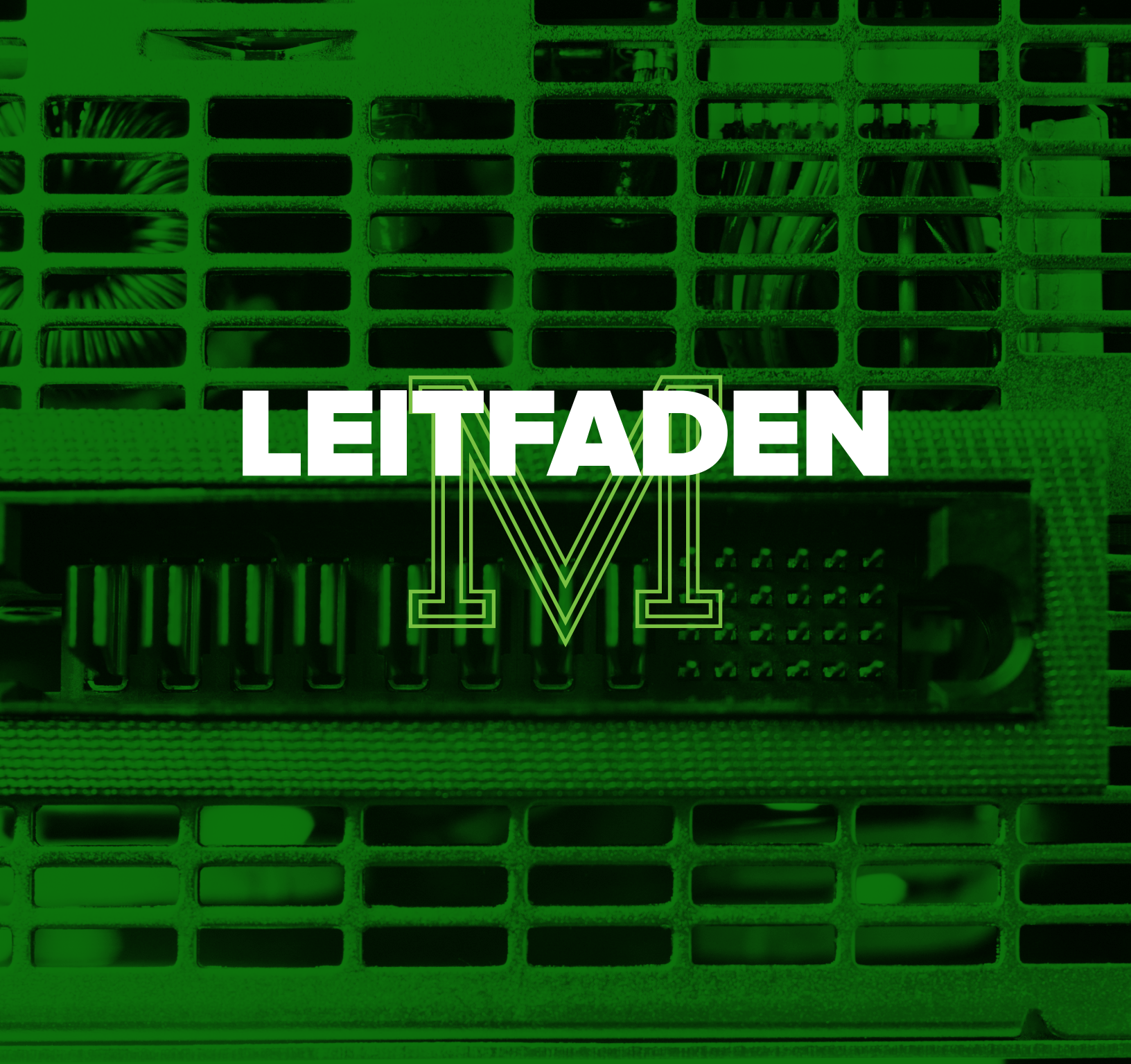


LEITFADEN IV

SICHERHEIT LEICHT GEMACHT

Inhalt

Allgemeine Übersicht

IT-Administratoren müssen Netzwerkgeräte installieren und auf dem aktuellen Stand halten, dabei aber zugleich auch das gesamte Management von Clients bis zu den Anwendungen übernehmen. Allein das ist bereits eine Herausforderung, doch dazu kommt, dass sie sich auch noch um die Sicherheit kümmern müssen. Und da geht es neben unterschiedlichsten Benutzertypen, also Mitarbeiter, Gäste, Auftragnehmer usw., die auf das Netzwerk zugreifen möchten, auch um verschiedenste Gerätetypen, nämlich Laptops, private Smartphones von Mitbareitern und auch IoT-Geräte. Zu schaffen ist das Management von Netzwerk, Geräte, Benutzerzugriff und Sicherheit nur, wenn es flexibel skalierbar ist.

Das Ergebnis: Im Versuchen, ihre Netzwerke abzusichern, implementieren IT-Teams unterschiedliche, nicht miteinander verbundene Dashboards verschiedener Hersteller und eine Vielzahl von Hardware-Produkten. So haben tatsächlich 25 % der Unternehmen Lösungen von einem bis 20 Herstellern im Einsatz, die ihr Netzwerk schützen sollen.[1] Eine solche Vielzahl unterschiedlicher Lösungen liefert jedoch keine Vereinfachung der Sicherheitslandschaft, sondern verdeckt eher den Blick darauf. Und so geben IT-Administratoren schließlich auf und implementieren eine ganz einfache Firewall. Ihnen ist der Wert eines Sicherheitsstatus, der das Netzwerk auf allen Ebenen abdeckt, zwar klar, doch fehlt es ihnen in der Regel an Personal und Zeit, um dafür geeignete Lösungen zu implementieren. Diese Schwachstellen wiederum nutzen Angreifer aus. Mehr als 43 % der Cyberangriffe nehmen kleine und mittlere Unternehmen mit dürftig besetzten IT-Teams ins Visier, [2] und 43 % dieser Angriffe dieser Angriffe machen sich unzureichende Zugriffs- und Sicherheitsrichtlinien zunutze.[3]

Der Ausweg? Cisco Meraki! Damit erhalten Sie ein zentrales Dashboard, über das Sie nicht nur Ihr gesamtes Netzwerk verwalten, sondern auch fortschrittliche Sicherheits- und Zugriffsregeln anwenden können. Und da das Meraki-Dashboard Cloud-basiert ist, werden alle Produkte laufend mit Patches versorgt und somit auf den neuesten Stand gebracht. Außerdem ist Meraki offen ausgelegt, verfügt nämlich über weitere APIs, die weitere Integrationen mit dem Cisco Security-Portfolio ermöglichen.

1 Cisco Annual Cybersecurity Report 2018
2 Cisco Annual Cybersecurity Report 2018
3 Cisco Annual Cybersecurity Report 2018

Hardware-Updates

ÜBERBLICK

Der MS390 kombiniert die Leistung des Cisco UADP 2.0 ASIC mit der Einfachheit, die das Meraki-Dashboards für die Mikrosegmentierung von Benutzern und Geräten in einem Netzwerk bietet. Leistungsstarke Sicherheits-und Zugriffsrichtlinien lassen sich damit anwenden, die Unternehmen vor dem zweifelhaften Ruhm schützen, wegen eines Datensicherheitsvorfalls den Schlagzeilen zu landen. Mit modularen Uplinks und Netzteilen sowie einem speziell konzipierten ASIC ist der MS390 der leistungsstärkste Access Switch im Meraki-Portfolio – und einer, der IT-Administratoren von einer Vielzahl von Problemen befreit.

WIR PRÄSENTIEREN

Der MS390, der bis dato leistungsfähigste Access Switch von Meraki, vereint die Einfachheit von Cloud-Managed IT mit der Power von speziell konzipierter Chip-Technologie von Cisco. Zusätzlich zu klassischen Switching-Funktionen ermöglicht es der MS390, komplexe Sicherheits-und Zugriffsrichtlinien durch Mikrosegmenterung einzelner Benutzergruppen anstatt über sperrige, schwer lesbare IP-Adressen einzurichten. Darüber hinaus zeichnet er sich insbesondere aus durch:

- Unterstützung von Kunden bei der Erfüllung anspruchsvollster Quality-of-Service-Anforderungen dank des speziell konzipieren UADP 2.0 ASIC
- Durchsatz von 480 Gbit/s – dreimal mehr als sein Vorgänger, der MS350 – und eine vollständige 48-Port-mGig-SKU mit Hot-Swap-fähigen modularen Uplinks, unter denen Kunden im Zuge der Überholung ihres Netzwerk zwischen 1, 10 oder 40 Gbit/s auswählen können.
- Verbesserungen beim physisches Stacking reduzieren die Latenz auf weniger als eine Sekunde, was die für Bereitstellungen in Großunternehmen so wichtige schnellere Stack-Konvergenz ermöglicht
- StackPower, das alle verfügbaren Stromversorgungen zu einer zusätzlichen redundanten Stromversorgung bündelt.

WICHTIGE SCHLUSSFOLGERUNGEN

Der UDAP 2.0 ASIC der Switches der MS390-Serie macht eine standortunabhängige Bereitstellung von Intent-based Networking einfacher. Denn statt auf Basis ihres Standorts können Benutzern eigene Mikrosegmente zugeordnet werden, auf die dann fortschrittliche Zugriffs- und Sicherheitsrichtlinien angewendet werden. Der umfangreiche Funktionsumfang der MS390-Hardware bietet zudem ein einfacheres Stack-Management und ein effizientes Energiemanagement mit der unübertroffenen Einfachheit des Meraki-Dashboards.

Updates bei Software und Funktionen

Adaptive Policy

ÜBERBLICK

Ergänzt ein Unternehmen im Zuge seines Wachstums neue Geräte, Benutzer und Anwendungen, müssen die IP-Adressen im Netzwerk neu zugewiesen werden. Nach klassischer Methode ist das jedoch äußerst mühsam. Darüber hinaus beinhalten IP-Adressen keine Informationen zu Benutzern, Geräten und Anwendungen. Mit Adaptive Policy steht vor allem anderen die Sicherheit im Mittelpunkt, indem sie die IP-Adressen bei jeder Kommunikationsverbindung durch Informationen dazu ergänzt, auf wen und auf was sie sich bezieht und wann die Verbindung aufgebaut wurde – das alles, ohne die Ressourcen und Kapazitäten der Switch-Hardware einzuschränken.

WIR PRÄSENTIEREN

Adaptive Policy ist eine Softwarefunktion, die den MS390 mit einer zusätzlichen Sicherheitsebene basierend auf der Absicht von Benutzer, Gerät und Anwendung ausstattet. Sie implementiert Netzwerkrichtlinien, die sich automatisch an die jeweilige Umgebung anpassen, basierend auf der Absicht des Clients, der Benutzeranwendung oder des Geräts.

WICHTIGE SCHLUSSFOLGERUNGEN

Adaptive Policy geht die Probleme der Netzwerke von heute durch effektive Sicherheit, reduzierte Betriebskosten, leistungsstarke Automatisierung, mehr Transparenz, höhere Effizienz der Hardware sowie eine höhere geschäftliche Produktivität an.

SecureConnect

ÜBERBLICK

Netzwerkhardware ist anfällig für potenzielle Bedrohungen. SecureConnect ist die einfachste und effektivste Art, Switch-Ports zu absichern und Gerätekonfigurationen zu automatisieren. Bei keinem anderen Hersteller wird dieses Maß an Sicherheit mit nur ein paar Klicks ermöglicht.

WIR PRÄSENTIEREN

SecureConnect ist eine Softwarefunktion, die für alle MS-Modelle ab MS210 oder höher sowie alle 802.11ac- und 802.11ax-konformen MR-Modelle verfügbar ist. Mithilfe von SecureConnect erkennen und verifizieren die MS, dass der mit dem Port verbundene MR zum selben Unternehmen gehört, auf den sie dann automatisch Konfigurationen übertragen.

WICHTIGE SCHLUSSFOLGERUNGEN

Mit SecureConnect erhalten Kunden zuverlässige Sicherheit und erweiterbare Automatisierung, mit der sie ihre Produktivität steigern und potenzielle Konfigurationsfehler beseitigen. Es baut auf die Vorteile des Meraki-Lizenzierungsmodells und die Vorteile der Meraki-Cloud auf, über die es auch in Zukunft Sicherheitsfunktionen liefert, die unsere Kunden benötigen. Auch weiterhin adressiert Meraki die Anforderungen von Kunden an starke Sicherheit mit produktübergreifenden Funktionen, sodass jeder, der in Meraki investiert hat, auch in Zukunft davon profitiert.

Trusted Access

ÜBERBLICK

Zu wissen, wer sich mit dem Netzwerk verbindet, mit welchem Gerät, und wann ist alles andere als die Realität des IT-Administrators von heute. Mit Meraki Trusted Access haben sie einen transparenten Überblick über Benutzer und Geräte und sind zudem in der Lage, sicheren Netzwerkzugriff nahtlos zu ermöglichen.

WIR PRÄSENTIEREN

Meraki Trusted Access ist eine Softwarefunktion, mit der eine sichere Netzwerkverbindung zwischen Unternehmensressourcen und privaten Geräten aufgebaut wird, ohne dass ein MDM-Agent/-Profil installiert werden muss. Um Trusted Access nutzen zu können, sind MR und SM (Systems Manager) erforderlich. Verfügbar ist die Funktion für iOS, macOS und Android-Geräte.

WICHTIGE SCHLUSSFOLGERUNGEN

Meraki Trusted Access liefert Kunden flexible Authentifizierungsverfahren kombiniert mit erweiterter Sicherheit. Die Lösung bietet außerdem ein besseres Benutzererlebnis ebenso wie einen transparenten Überblick über Benutzer und Geräte. Sie trägt ferner dazu bei, das Geräte-Onboarding sowie die Durchsetzung von Richtlinien zu automatisieren und ermöglicht zudem individuell angepasste Integrationen anhand von APIs.

Trustworthy Systems

ÜBERBLICK

Das Cisco Meraki-Portfolio hebt als kompletter durch die Cisco Trustworthy Systems abgedeckter Hardware-Stack (MR Access Points, MS Switches und MX SD-WAN Security Appliances) im Markt ab.

WIR PRÄSENTIEREN

Trustworthy Systems, also vertrauenswürdige Systeme, sind eine Suite von Cisco Lösungen, die sicherstellen, dass der Code, der auf diesen Hardwareplattformen ausgeführt wird, authentisch ist, nicht manipuliert wurde und nur die Aktionen ausführt, für die er vorgesehen ist. Hinter dem Konzept stehen Technologien wie Image Signing, Secure Booth und das Cisco Trust Anchor Module (TAm). Dieser mehrschichtige Ansatz beinhaltet einen auf Hardwareebene integrierten Nachweis der Vertrauenswürdigkeit, eine eindeutige Geräteidentität und die Validierung aller Softwareebenen beim Systemstart. Dadurch wird eine durchgehende Kette der Vertrauenswürdigkeit im gesamten System hergestellt. Cisco Meraki-Hardwareprodukte werden ab sofort durch alle Cisco Trustworthy Systems abgedeckt.

WICHTIGE SCHLUSSFOLGERUNGEN

Mit Cisco Trustworthy Systems sind Sicherheit und Vertrauenswürdigkeit für alle abgedeckten Hardwareprodukte gewährleistet und damit optimaler Schutz vor gefälschte Produkten und Cyberangriffen sichergestellt. Das Meraki-Komplettportfolio liefert unternehmen eine umfassende Lösung für eine vertrauenswürdige Netzwerkinfrastruktur gestützt auf die Trustworthy Systems.

Umbrella + MR-Lizenz

ÜBERBLICK

Kunden können zum Schutz ihrer Netzwerke ab sofort die Vorteile der im Rahmen von Cisco Umbrella verfügbaren DNS-Sicherheitslösung mit der Einfachheit des Meraki-Dashboards kombinieren. Möglich wir dies mit der MR Advanced- und der MR Upgrade-Lizenz, die Meraki-definierte Richtlinien automatisch auf DNS-Ebene im Netzwerk integriert. Mit der neuen Lizenz werden Kunden im Meraki-Dashboard zudem blockierte DNS-Ereignisse angezeigt. Eine manuelle Integration von Umbrella mit den MR Access Points seitens IT-Administratoren ist dabei nicht mehr nötig. Das bedeutet auch, dass sie Sicherheitsbereitstellungen nunmehr innerhalb weniger Minuten über mehrere Standorte hinweg skalieren können.

WIR PRÄSENTIEREN

Meraki liefert Kunden im Rahmen einer neuen Lizenz ab sofort einen umfassenden, transparenten Überblick über blockierte DNS-Ereignisse, indem das Security Center direkt im Meraki-Dashboard verfügbar gemacht wird. Dabei lassen sich auch vordefinierte Richtlinien lassen ohne manuelle Eingriffe integrieren. Durch die Integration des Security Center in das Meraki-Dashboard können Kunden ihre Wireless-Netzwerke auch auf DNS-Ebene überwachen, absichern und etwaige Fehler beheben. Neukunden erhalten diese kombinierten Funktionen über die SKU der Advanced-Lizenz. Bestehende Wireless-Kunden wiederum können die SKU der Upgrade-Lizenz erwerben, um die DNS-Sicherheit von Umbrella in Ihrem Meraki-Netzwerk zu aktivieren.

WICHTIGE SCHLUSSFOLGERUNGEN

Die neue kombinierte Lizenz für Umbrella und MR liefert beispiellose Einfachheit und Zentralisierung. Für Kunden bedeutet das: Sie können Sicherheit auf DNS-Ebene für alle Meraki Access Points über die Cloud und somit ganz ohne zusätzliche Hardware oder virtuelle Systeme bereitstellen. Ebenfalls bietet Meraki API-Endpunkte, mit deren Hilfe vordefinierte Richtlinien abgerufen und bereitgestellt werden können, die Schutz vor den meisten Internetbedrohungen schützen. Damit können IT-Administratoren Sicherheit auf DNS-Ebene in großem Maßstab über verschiedenste Netzwerke hinweg bereitstellen und so eine einfache und sichere digitale Arbeitsumgebung schaffen.

API-Integration der MX mit Cisco Defense Orchestrator (CDO)

ÜBERBLICK

Cisco Defense Orchestrator (CDO) ist eine Cloud-basierte Management-Lösung, mit der Sicherheitsrichtlinien und Konfigurationen mühelos über alle Cisco Security-Produkte hinweg, einschließlich der Meraki MX, verwaltet werden können.

WIR PRÄSENTIEREN

Der CDO unterstützt ab sofort auch die Meraki MX. Dieser sorgt für starke Sicherheit, da mit sich ihm Richtlinien unternehmensweit anpassen lassen, unabhängig davon, auf welchem Cisco Security-Produkt. Dadurch wird das Management von Sicherheitsrichtlinien über mehrere Cisco Security-Produkte hinweg vereinfacht und Inkonsistenzen oder Lücken vermieden. Kunden, die verschiedene Cisco Security-Produkte einschließlich der Meraki MX im Einsatz haben, liefert der CDO Mehrwert durch die Möglichkeit, Richtlinien an allen Standorten des Unternehmens einheitlich zu gestalten, zu verwalten und zu aktualisieren.

WICHTIGE SCHLUSSFOLGERUNGEN

Der CDO vereint das Sicherheitsmanagement in auf Cisco und Meraki basierenden Hybrid-Infrastrukturen in einer leistungsstarken Lösung.

Identity Pre-Shared Key (iPSK)

ÜBERBLICK

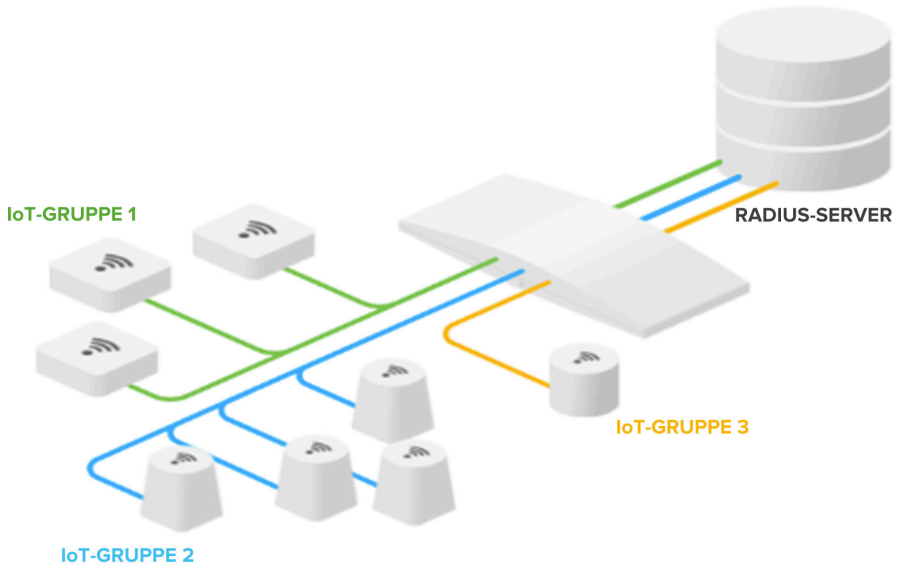
Mit dem Vormarsch des IoT müssen Netzwerkadministratoren mit einem exponentiellen Zuwachs an Systemen fertig werden, die sich mit Wireless-Netzwerken verbinden. Die Authentifizierung dieser Geräte gestaltet sich jedoch bisweilen schwierig, da hierfür nicht alle den 802.1X-Standard unterstützen. Das WPA-PSK-Verfahren bietet heute zwar eine Alternative, doch bei ihm kann es vorkommen, dass ein Schlüssel an nicht autorisierte Benutzer weitergegeben wird. Eine deutlich einfachere Absicherung des Wireless-Netzwerks liefert der iPSK (Identity Pre-Shared Key) .

WIR PRÄSENTIEREN

Der iPSK ist eine neue Funktion des MR, die eine sicherere Authentifizierung für Wireless-Geräte ermöglicht als frühere Verfahren wie etwa WPA-PSK. Zusätzliche Zertifikate werden dafür ebenso wenig benötigt wie 802.1X. Statt einen einzelnen Pre-Shared Key an jedes Gerät herauszugeben, das sich mit einer SSID verbindet, wird ein eindeutiger PSK mit der MAC-Adresse des Geräts korreliert und über einen RADIUS-Server authentifiziert. Diese Funktion ermöglicht also die Zuweisung separater Gruppenrichtlinien innerhalb einer einzelnen, auf dem PSK basierenden SSID. So erhalten alle Geräte, die etwa den PSK „Meraki123“ verwenden, automatisch die Gruppenrichtlinie 1. Geräten, die dagegen den PSK „Meraki456“ verwenden, wird automatisch die Gruppenrichtlinie 2 zugewiesen.

WICHTIGE SCHLUSSFOLGERUNGEN

Mit dieser Funktion können Unternehmen ihre Netzwerke auch ohne de Einrichtung mehrerer SSIDs schützen, die ihre Wireless-Leistung beeinträchtigen könnten. Auf ihrem Weg zur digitalen Transformation erhalten Unternehmen mit dieser Lösung zusätzliche Sicherheit.



Firewall-Objektgruppen

ÜBERBLICK

Firewall-Objektgruppen ermöglichen die Zuordnung von Netzwerkentitäten wie Telefonie-Geräte, Drucker und mehr zu einer IP-Adresse oder einem Subnetz. Diese Netzwerkobjekte lassen sich dann in Gruppen zusammenfassen, was zur Vereinfachung der Firewall-Regeln auf der MX beiträgt.

WIR PRÄSENTIEREN

Firewall-Objektgruppen sind eine neue Funktion der MX, mit der verschiedene Firewall-Regeln auf einfache Weise erstellt und verwaltet werden können.

WICHTIGE SCHLUSSFOLGERUNGEN

Die Erstellung und das Management von Firewall-Regeln gestaltet sich jetzt einfacher als je zuvor. Mit diesem neuen Prozess wird die MX noch leistungsfähiger, was sich in einer Vereinfachung des Netzwerkmanagements niederschlägt.

cisco Meraki