Continue

دليل تكوين نقطة وصول meraki من cisco anyconnect

American cloud-managed IT company Cisco MerakiCompany typeDivisionIndustryNetworking, ITFounded2006; 19 years ago (2006) in Mountain View, California, U.S.FoundersSanjit BiswasJohn BicketHans RobertsonHeadquartersSan Francisco, California, U.S.Key peopleChris Stori (SVP, GM) Bret Hull (CTO)ParentCisco SystemsWebsitemeraki.cisco.com Cisco Meraki is a cloud-managed IT company headquartered in San Francisco, California. Their products include wireless, switching, security, enterprise mobility management (EMM) and security cameras, all centrally managed from the web. Meraki was acquired by Cisco Systems in December 2012.[1] Meraki was founded by Sanjit Biswas and John Bicket, along with Hans Robertson. The company was based in part on the MIT Roofnet project, an experimental 802.11b/g mesh network developed by the Computer Science and Artificial Intelligence Laboratory at the Massachusetts Institute of Technology. Meraki was funded by Google and Sequoia Capital. The organization started in Mountain View, California, in 2006, before relocating to San Francisco. Meraki employed people who worked on the MIT Roofnet project.[2][3][4] In 2007, Meraki selected San Francisco for their community-based Free the Net campaign.[why?] They started putting gateway devices in the Lower Haight neighborhood to provide Internet access and giving away repeaters. In the first year of the project, the growth of the network was primarily in the Mission District. By October 2007, they estimated 20,000 distinct users connected and about 5 terabytes of data transferred in this network. In July 2008, Meraki said 100,000 people in San Francisco used its "Free the Net" service. Since then, Meraki discontinued this public service, though many access points remain active, but with no connection to the Internet. On November 18, 2012, Cisco Systems announced it would acquire Meraki for an estimated $1.2 billion.[1] Table of Meraki MR Access Points Model Indoor/Outdoor Wifi Capability Ethernet Architecture System-on-Chip CPU Speed Flash-Chip Flash Size Ram Size Wireless chip End of Support MR11 Indoor Aug 30, 2017 MR12 Indoor 2x2:2 802.11n (2.4 GHz) Gigabit MIPS Atheros (AR7242/7241) 400 MHz Macronix 16MB 64MB AR9283-AL1A Oct 24, 2022 MR14 Indoor Aug 30, 2017 MR16 Indoor 2x2:2 802.11n Gigabit MIPS Atheros AR7161-BC1A 680 MHz Macronix 16MiB 64MB AR9283-AL1A May 31, 2021 MR18 Indoor 2x2:2 802.11n Gigabit MIPS Qualcomm QCA9557-AT4A 720 Hynix 128MiB (NAND) 128MB SoC AR9550 + 2x Atheros AR9582-AR1A Mar 31, 2024 MR20 Indoor 2x2:2 802.11ac Wave 2 Gigabit MR24 Indoor 3x3:3 802.11n Gigabit May 31, 2021 MR30H Indoor, In-room hotel or dormitory deployments 2x2:2 802.11ac Gigabit July 26, 2027 MR32 Indoor 2x2:2 802.11ac Gigabit Mar 31, 2024 MR33 Indoor 2x2:2 802.11ac Wave 2 Gigabit ARMv7 Qualcomm IPQ4029 716 MHz Spansion S34ML01G200TFV00 128MiB 256MB Qualcomm QCA9887 Jul 21, 2026 MR34 Indoor 3x3:3 802.11ac Wave 2 Gigabit Oct 31, 2023 MR36 Indoor 2x2:2 802.11ax Gigabit Qualcomm IPQ8070A 1.0 GHz MR36H Indoor, In-room hotel or dormitory deployments 2x2:2 802.11ax Gigabit MR42 Indoor 3x3:3 802.11ac Wave 2 Gigabit Jul 21, 2026 MR44 Indoor 2.5Gig MR45 Indoor 4x4:4 802.11ax 2.5Gig MR46 Indoor 4x4:4 802.11ax 2.5Gig MR52 Indoor 4x4:4 802.11ac Wave 2 2 x Gigabit Jul 21, 2026 MR53 Indoor 4x4:4 802.11ac Wave 2 2.5Gig+Gigabit MR55 Indoor 8x8:8 802.11ax 5Gig Aug 1, 2028 MR56 Indoor 8x8:8 802.11ax 5Gig MR57 Indoor 4x4:4 802.11ax 2,4 GHz, 5 GHz, 6 GHz (Wi-Fi 6E) 2 x 5Gig MR58 Outdoor Oct 30, 2017 MR66 Outdoor 2x2:2 802.11n Gigabit Jun 9, 2024 MR70 Outdoor 2x2:2 802.11n Gigabit MR72 Outdoor 2x2:2 802.11ac Wave 2 Gigabit Apr 30, 2024 MR74 Outdoor 2x2:2 802.11ac Wave 2 Gigabit Jul 21, 2026 MR76 Outdoor 2x2:2 802.11ax Gigabit MR84 Outdoor 4x4:4 802.11ac Wave 2 2.5Gig+Gigabit Jul 21, 2026 MR86 Outdoor 4x4:4 802.11ax 5Gig Series[5] Deployment type Interfaces Uplinks PoE capabilities Power configuration Stacking capabilities Routing capabilities Models MS120-8 Compact 8 x 1GbE RJ45 2 x 1GbE SFP Fixed 67W (LP model) 124W (FP model) External PSU (non-PoE, LP model) Internal (FP Model) Virtual only DHCP Relay MS120-8-HW MS120-8LP-HW MS120-8FP-HW MS225 Branch & small campus 24 / 48 x 1GbE RJ45 4 x SFP+ Fixed 370W (LP model) 740W (FP model) Internal Yes, 80G physical + virtual DHCP Relay MS225-24-HW MS225-24P-HW MS225-48-HW MS225-48LP-HW MS225-48FP-HW MS355 Branch & small campus 24 / 48 x 1GbE RJ45 8 x XGbE RJ45 (24X only) 2 × 40G (QSFP+) Fixed 740W (24 port, X2 models) 740W (48 port, X2 models) Removable PSU 400G physical + virtual Static + Dynamic DHCP Server + Relay MS355-24-HW MS355-24X-HW MS355-48-HW MS355-48X-HW MS355-48X2-HW MS390 High-performance campus & branch 24 / 48 x 1GbE RJ45 24 / 48x XGbE RJ45 (in select models)* 4/8 x 10GbE SFP+ 2 x 40GbE QSFP Modular 830W (24 port models) 822W (48 port models) Removable PSU Compatible only with MS390 480G physical + virtual Static + Dynamic DHCP Server + Relay MS390-24-HW MS390-24P-HW MS390-24U-HW MS390-24UX-HW MS390-48-HW MS390-48P-HW MS390-48U-HW MS390-48UX-HW MS390-48UX2-HW MS450 10G fiber aggregation 12x 40GbE QSFP+ 2 x 100GbE QSFP28 N/A Modular Redundant PSU optional (sold separately) Front-port 160G + virtual Static + Dynamic DHCP Server + Relay Warm spare (VRRP) MS450-12-HW Table of Meraki MX Security Appliances Model Wifi Model Interfaces Stateful Firewall Throughput Architecture CPU Speed End of Sale End of support Z1[6] Yes 5 x GbE 50 Mbit/s Z3[7] Yes 5 x GbE 100 Mbit/s Z4[8] Yes WAN: 1 x GbE RJ45 LAN: 4 x GbE RJ45 (1 x PoE) 500 Mbit/s MX60[9] MX60W 5 x GbE 100 Mbit/s MX64[10] MX64W WAN: 1 x GbE RJ45 LAN: 4 x GbE RJ45 250 Mbit/s July 26, 2022 July 26, 2027 MX65 MX65W WAN: 2 x GbE RJ45 LAN: 10 x GbE RJ45 250 Mbit/s May 28, 2019 May 28, 2026 MX67 MX67W MX68 MX68W MX75 N/A WAN: 2 x GbE RJ45 1 x SFP LAN: 10 x GbE RJ45 (2 x PoE) 1 Gbit/s MX80 N/A 5 x GbE 250 Mbit/s Aug 30, 2016 Aug 30, 2023 MX84 N/A 5 x GbE 500 Mbit/s Oct 31, 2021 Oct 31, 2026 MX85 N/A WAN: 2 x GbE RJ45 2 x SFP LAN: 8 x GbE RJ45 2 x SFP 1000 Mbit/s MX90 N/A 9 x GbE, 2 x GbE (SFP) 500 Mbit/s MX95 N/A WAN: 2 x 2.5GbE RJ45 2 x SFP+ LAN: 4 x GbE RJ45 2 x SFP+ 2 Gbit/s MX100 N/A 9 x GbE, 2 x GbE (SFP) 750 Mbit/s Feb 1, 2022 Feb 1, 2027 MX105 N/A WAN: 2 x 2.5GbE RJ45 2 x SFP+ LAN: 4 x GbE RJ45 2 x SFP+ 3 Gbit/s MX250 N/A WAN: 2 x 10GbE (SFP+) LAN: 8 x GbE (RJ45), 8 x GbE (SFP), 8 x 10GbE (SFP+) 4 Gbit/s MX400 N/A 8 x GbE (RJ45), 8 GbE (SFP), 4 x 10GbE (SFP+) 1 Gbit/s May 20, 2018 May 20, 2025 MX450 N/A 6 Gbit/s MX600 N/A 8 x GbE (RJ45), 8 GbE (SFP), 4 x 10GbE (SFP+) 2 Gbit/s May 20, 2018 May 20, 2025 On August 3, 2017, the engineering team made changes to the North American object storage service; the change caused some deletion of customer data. Cisco stated that the change was due to the application of "an erroneous policy". The data loss mostly affected media files uploaded by customers. Lost data included: Systems Manager – Custom enterprise apps and contact images. Meraki Communications – IVR audio files, hold music, contact images and VM greetings. Wireless Device Dashboard – Custom floor plans, device placement photos, custom logos used for interface branding and reports and custom splash themes. On August 7 Meraki announced that some data on the cache service could be recovered. On August 9 customers were informed that recovery efforts were still underway but that they "do not expect to be able to recover most assets".[11][12][13][14][15][16] Cisco Systems List of networking hardware vendors ^ a b Constine, Josh (18 November 2012). "Cisco Acquires Enterprise Wi-Fi Startup Meraki For $1.2 Billion In Cash". TechCrunch. Retrieved 2016-11-17. ^ "Sequoia – Companies". Sequoia Capital. Retrieved 2016-11-17. ^ Fehrenbacher, Katie (2006-08-02). "Meraki Cooks Up Wireless Mesh Router". gigaom.com. Archived from the original on 2022-01-27. Retrieved 2016-11-17. ^ Goodin, Dan (15 August 2007). "Google-Funded startup to offer free WiFi in San Francisco". The Register. Retrieved 10 April 2019. ^ "Meraki MS Series Switches Family Datasheet". Meraki MS Series Switches Family Datasheet. 17 May 2021. Archived from the original on 2021-02-25. Retrieved 17 May 2021. ^ "Cisco Meraki Z1 Datasheet" (PDF). Cisco Meraki. Retrieved 23 May 2020. ^ "Meraki Z-Series Datasheet" (PDF). Cisco Meraki. Retrieved 23 May 2020. ^ "Z4 Datasheet". Cisco Meraki. Retrieved 11 Feb 2025. ^ "MX Cloud Managed Security Appliance Series Datasheet" (PDF). Cisco Meraki. Retrieved 23 May 2020. ^ "Meraki MX Cloud-Managed Security and SD-WAN Datasheet" (PDF). Cisco Meraki. Retrieved 23 May 2020. ^ "North American Object Storage Service Impact". Cisco Meraki. 4 August 2017. Retrieved 10 April 2019. ^ "Cisco Meraki suffers data loss caused by human error". The Stack. 7 August 2017. Archived from the original on 4 December 2018. Retrieved 10 April 2019 – via Techerati. ^ Marzouk, Zach (7 August 2017). "Cisco Meraki loses customer data in engineering gaffe". CloudPro. Retrieved 10 April 2019. ^ Hardcastle, Jessica Lyons (7 August 2017). "Cisco Meraki Data Loss Reveals Need for Oversight". SDX Central. Retrieved 10 April 2019. ^ Sharwood, Simon (6 August 2017). "Cisco loses customer data in Meraki cloud muckup". The Register. Retrieved 10 April 2019. ^ "North American Object Storage Service Impact (8-4-2017)". Cisco Meraki Documentation. 5 October 2020. Retrieved 2024-05-29. Official website Retrieved from " إجراء نقل الموقع المقدمة يصف هذا المستند A Access Point (AP) 1 إلى ملف التعريف الموصى به (AB & CD) و AP2 المتطلبات توصي المتطلبات الأساسية للوصول ...

Meraki المشكلة يلزم تغيير ملف تعريف نقطة الوصول في ... Profile_18Mbps_40MHz_EXCLUDE_161، ثم قم بتحرير الإعدادات >تعيين ملف تخصيص أختر AP2 ميجاهرتز، انقر على التالي ثم احفظ انتقل إلى الشبكة > معرف الموقع > لاسلكي >إعدادات الراديو أختر كلا الجهازين اللاسلكيين لنقطة الوصول ... تأثير التغيير: إذا قمت بفصل الاتصال بالشبكة المحلية اللاسلكية ... رؤية المرضى. MX Appliance. MX is running the wrong firmware version. Ensure your MX is running the correct firmware version. The firmware section on the Appliance Status page should say MX 16.X** version. If your MX is running firmware versions MX14 or MX15, contact Meraki Support to upgrade your MX. The connection request did not make it to the MX (AnyConnect server). If your MX is behind a router or firewall, confirm traffic is forwarded to your MX. Requests from the AnyConnect client could be reaching the upstream router or firewall device but not your MX (AnyConnect server). Take a packet capture on the WAN to confirm traffic is forwarding as expected. If you are using a port other than the default 443, for example 1443, ensure the new port is appended to the end of the DDNS hostname. For example: "xyz.dynamic-m.com:1443" Wrong AnyConnect client version "The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again." This error might occur when a user tries to connect with an AnyConnect client version 4.7 or lower. AnyConnect client version 4.8 or higher is required to connect to the MX (AnyConnect server). Unable to connect due to captive portal "The service provider in your current location is restricting access to the Internet. You need to log on with the service provider before you can establish a VPN session. You can try this by visiting any website with your browser." This error occurs when a captive portal is enabled on the user's network. If the error occurs on a network where no captive portal is enabled, disable captive portal detection in the AnyConnect client preferences. Look at the event log and filter by "AnyConnect authentication failures" and try testing with different username and password or try updating your credentials. When authenticating with RADIUS or Active Directory (if offline), after entering your username and password, your AnyConnect client will look like screenshots below. When the RADIUS or AD server responds immediately with authentication failure, the user will get a prompt to reenter their password immediately. If the user does not get a prompt to reenter their credentials, the server is not responding or the response from the server is not making it back to the MX for some reason. You may even see error messages indicating an issue with the server certificate, although the issue really is that the Active Directory or RADIUS server did not respond to the authentication request. Ping the RADIUS or AD server to see if it is online Ensure your MX is listed as a RADIUS client, if authenticating via RADIUS Take a packet capture on LAN/VPN/WAN depending on where the authentication server resides to see if authentication requests and replies are seen been the MX and the authentication server "Certificate Validation Failure" This error occurs when certificate authentication is enabled and none of the certificates presented by the authenticating client were issued by the root CA whose certificate was uploaded to the MX when certificate authentication was configured. The uploaded trusted CA certificate needs to be in PEM format. Check the User > Personal > Certificates folder of the client to verify that there is a valid certificate that was issued by the Trusted CA certificate uploaded to the Dashboard for certificate authentication. "Security Warning: Untrusted Server Certificate! AnyConnect cannot verify server: Certificate does not match the server name. Certification is from an untrusted source." By default, configuring AnyConnect on your MX generates a temporary self-signed certificate. Then the MX initiates enrollment for a publicly-trusted certificate based on the Dynamic DNS (DDNS) hostname. This enrollment process takes approximately 10 minutes after AnyConnect is enabled to complete. If attempting to make a connection before a publicly-trusted certificate is available, you will see the "Untrusted Server Certificate" message. After the public certificate enrollment is complete, the AnyConnect server will replace the self-signed certificate with the publicly-trusted certificate. If this message is encountered after the enrollment process is complete: Ensure the device is online in the dashboard Ensure Dynamic DNS is enabled and resolves to the MX IP Ensure you are connecting with the DDNS hostname not the IP of the MX--connecting with the IP will cause a certificate error even if there is a publicly trusted certificate on the MX Connect to the MX with different devices to see if they all report the MX as an "Untrusted Server" Devices should have HydrantID Server CA O1 certificates by default If this is seen on some devices, check the Trusted CA folder on your client device If you do not see the HydrantID certificates, update your browser to the latest version It might be necessary to download the Root CA certificate and push it to the end device in order for it to trust the AnyConnect Server certificate To identify what Root CA to download, try connecting to the DDNS hostname or IP of the MX When the Untrusted Server message appears, click details Look at the Issuer field to identify the Root CA required The Root CA certificate can then be downloaded from the internet and pushed to the client Check traffic settings on MX or routes on your AnyConnect client. Verify the destinations have routes configured under Secured Routes in the Route Details on the client. If the destination routes are not configured, modify the traffic setting on the AnyConnect Settings page and reconnect to the AnyConnect server to update your routes.   Firewall rules or group policy. Check the firewall rules on the MX to ensure traffic to the destination is not being blocked from your AnyConnect client IP or subnet. Do not include port number when adding the Meraki hostname to DUO configuration. e.g. Use meraki-hostname.com instead of meraki-hostname.com:443 According to DUO Support, the global port numbers are not required and may result in the following behavior if used: User is able to enter credentials and goes through the second factor authentication (if enabled). DUO app reports an authentication confirmation, and user is presented with a "You are successfully authenticated" page. Secure Client reports a warning saying "Please complete the authentication process in the AnyConnect Login window", and client is not able to access internal resources. Dashboard's Event Log reports Admin State: Auth reply timer expired at XXXX waiting for response.   Take packet captures on the AnyConnect VPN interface. Packet captures taken on the AnyConnect VPN interface can verify if traffic is making it to the MX. To take packet captures, navigate to: Dashboard > Network > Packet captures > Select AnyConnect VPN interface. If traffic from the expected client is not in the packet capture, and the routing appears to be configured correctly on each end of the tunnel, contact AnyConnect TAC. When initializing a tunnel, the AnyConnect client will attempt to connect using both TLS, and DTLS (Datagram TLS) over TCP and UDP 443 respectively. If it is unable to form a tunnel using the latter, it will fall back to TLS, but this requires a reinitialization of the connection, leading to a brief drop and reconnection right after the initial connection is established. More details on the problem, and ways to resolve it can be found here Ensure that a Filter-ID attribute is being passed by your RADIUS server to the MX in an Access-Accept packet. This can be accomplished by taking a packet capture on the appropriate interface, validating that the attribute exists, and that its value exactly matches the name of the policy defined in the dashboard. Dynamic split tunneling is a client-side feature. The AnyConnect server on MX/Z devices is responsible only for pushing the list of included and/or excluded domains to the client. For other issues related to functionality, contact AnyConnect TAC. To verify if clients are receiving the expected lists, review the Dynamic Tunnel Exclusion and Inclusion fields under the VPN tab of the Statistics window of the AnyConnect Client. If you need to change your list of URLs during production hours, you will need your clients to disconnect any active VPN sessions they have before the updates will propagate to them. المقدمةيصف هذا المستند كيفية تكوين الوصول الآمن من Cisco باستخدام Meraki MX للتوافر العالي باستخدام فحوصات الصحة.المتطلبات الأساسيةالمتطلبات يجب أن يكون Meraki MX يتم دعم نفق واحد ... Meraki التي تمنع تغيير IP للتحقق من الصحة، مما يجعل NAT مطلوبا لأنفاق SPA (Secure Private Access) الإضافية. لا ينطبق هذا عند إستخدام SIA المكونات المستخدمة) الوصول الآمن إلى الإنترنت). حدد بوضوح الشبكات الفرعية أو الموارد الداخلية التي يتم توجيهها عبر النفق لتأمين الوصول. Cisco Secure Access جهاز أمان Meraki MX (لوحة معلومات Meraki 19.7.1 الإصدار من البرنامج الثابت أو إصدار أحدث)

... الأنفاق الثابتة، مع فهم أن مجموعة نفق الشبكة فقط يمكنها دعم فحوصات الحماية والتوفر العالي. وتعمل أنفاق إضافية من دون مراقبة الصحة أو التكرار. التكوينتكوين شبكة BGP المتعددة بحاجة إلى الاتصال للوصول الآمن للوصول الخاص، فيجب عليك إما إستخدام Meraki MX الصحي، يتم دعم مجموعة نفق واحدة فقط في وضع الوصول الخاص. إذا كانت أجهزة Next انقر Passphrase وTunnel ID Format قم بتكوين Next انقر Device Type وTunnel Group Name، Region التكوين Add + فوقNetwork Tunnel Groups تحت النقر Connect > Network Connections انقر فوق Secure Access. على الوصول الآمنانتقل إلى لوحة الإدارة الخاصة ب VPN للتوجيه الديناميكي أو تكوين الأنفاق الثابتة، مع فهم أن

أختر الشبكات التي قمت بتحديدها لإرسال حركة مرور البيانات إلى الوصول الآمن:إختيار فيVPN إعدادات.Hub من موقع إلى موقعاختر VPN شبكةSecurity & SD-WAN > Site-to-site VPN وانقر فوق Meraki MX انتقل إلىMeraki MX على VPN تكوين شبكة.Meraki Non-Meraki VPN Peers المفكرة، أستخدم هذه المعلومات لاستكمال التكوين في Secure Access ملاحظة: يستجيب هذا المجال فقط عند الوصول إليه عبر نفق من موقع إلى موقع مع Add health Check+ انقر فوق Configure Health Checks لتوجيه حركة المرور إلى الوصول الآمن:انقر فوق Meraki أنت تحتاج إلى تكوين فحوصات الصحة التي تستخدمهاMeraki غير VPN تلقائيأقران شبكاتNAT Traversalأختر الشبكات التي قمت بتحديدها

1.0.0.0/0 ... Remote Access VPN IP Pool و ال cgnat 100.64.0.0/10 ... Meraki ... واحد فقط، فيمكنك ... All Networks. إذا كان لديك أجهزة متعددة، فتأكد من تحديد شبكة Meraki ... إعداد Umbrella ثم انقر Save.انقر فوق: الرئيسي بالنفق الخاصة الخيارات قائمة فوق انقر ،الثانوي النفق تكوين + Add Secondary peer انقر فوقInherit primary peer configurations فق ثم بعد ذلك يمكنك النقر

Traffic Shaping قم بالتمرير لأسفل إلى Local Internet Breakout المقطع وانقر فوق Add+ ثم قم بإنشاء المجازة بناءا على Custom Expressions أو Major Applications:Custom Expressions - ProtocolCustom Expressions - DNSMajor Applicationsإستبعاد شبكات: تكوين قواعد إستبعاد شبكات، يرجى زيارة الموقع: لمزيد من المعلومات، VPN (IP/Port/DNS/APP) انقر فوقالتحقق من الحالة في: الرجاء التحقق من الحالة في: التحقق من الصحةللتحقق مما إذا كانت الأنفاق قيد التشغيل، Security & SD-WAN> VPN Status في لوحة معلومات Meraki. انقر فوق Non-Meraki peers: إذا تم عرض حالات الشبكات الخاصة الظاهرية (VPN) للتحقق مما إذا كانت عمليات التحقق من سلامة حقق من الصحة

up ... هذا السلوك متوقع ... يعني حاليا عم يمر ويشغل حركة مرور. يظهر التحقق من صحة النفق الثانوي الحالة: فنزولا، ليس لأن النفق غير متاح، بل لأن الخط الأساسي صحي ومستخدم بنشاط.