Cisco Meraki Cloud management (Správa cloud-u)

Prehľad
Správa Meraki založená na cloud-e poskytuje centralizovanú viditeľnosť a kontrolu nad drôtovým a bezdrôtovým sieťovým hardvérom Meraki, bez nákladov a zložitosti bezdrôtových ovládačov alebo prekrývajúcich (overlay) systémov riadenia. Meraki cloud management, integrovaný s celým produktovým portfóliom Meraki, poskytuje bohaté, škálovateľné a centralizované riadenie pre siete akejkoľvek veľkosti.

Hlavné znaky
- Jednotná viditeľnosť a kontrola celej siete cez jediný prístrojový panel (dashboard): bezdrôtové, switchové a bezpečnostné prístroje
- Zefektívnenie veľkých sietí s desaťtisícmi koncových bodov
- Provisioning bez potreby dotyku (zero touch)pre rýchle nasadenie
- Zabudované nástroje pre správu viacstránkovej siete
- Automatizované monitorovanie siete a varovania (alerts)
- Intuitívne rozhranie eliminuje náklady na školenia alebo ďalších zamestnancov
- Network tagging engine - vyhľadávanie a synchronizácia nastavení pomocou tagov
- Správa na základe rolí a kontrolovateľné záznamy (logy) o zmenách
- Stála funkcia aktualizácií prichádzajúcich z cloud-u
- Vysoká dostupnosť a bezpečnosť (PCI / HIPAA plnenie)

Siete riadené z cloud-u

Hardvérové produkty Meraki sú od podlahy postavené pre účely cloud managementu. Výsledkom je sériové riešenie s centralizovanou kontrolou, videteľnosťou 7. vrstvy pre zariadenia a aplikácie, diagnostika v reálnom čase na základe webu, monitorovanie, hlásenie a ešte oveľa viac.

Spustenie sietí Meraki prebieha rýchlo a jednoducho, bez potreby školení alebo školených zamestnancov. Naviac, Meraki poskytuje bohatú množinu funkcií, ktoré ponúkajú úplnú kontrolu nad zariadeniami, používateľmi a aplikáciami, čím sa môžu dosiahnuť flexibilné prístupové politiky a bohaté zabezpečenie bez ďalších nákladov a zbytočnej zložitosti.

Cloud management od Meraki poskytuje funkcie, bezpečnosť a škálovateľnosť pre siete akejkoľvek veľkosti. Meraki škáluje od malých stránok cez kampusy až po distribuované siete s tísíckami stránok. Zariadenia Meraki, ktoré sa samé obsluhujú cez cloud, môžu byť nasadené

na miestach bez IT. Aktualizácie firmvéru a bezpečnostného podpisu sa doručujú plynulo cez web. V cloud-e môžu pobočky automaticky zriadiť bezpečné VPN tunely medzi sebou pomocou jedného kliknutia.

Vďaka bezpečnej architektúre, ktorá je kompatibilná so štandardmi PCI a HIPAA a dizajnu odolnému voči chybám, ktorý chráni funkčnosť siete pri prípadných výpadkoch WAN, je Meraki partnerom overeným v reálnych podmienkach a kľúčových sieťových aplikáciách

Architektúra správy cloudu

Internetová architektúra Meraki poskytuje funkčne bohatú správu dát bez zariadení určených na správu v danej lokalite a bez WiFi ovládačov.

Každé Meraki zariadenie - vrátane bezdrôtových prístupových bodov, ethernetových prepínačov a bezpečnostných zariadení, sa pripája cez internet do dátových centier Meraki, ktoré bežia na báze cloudovej platformy Meraki. Tieto pripojenia, zabezpečené cez SSL, využívajú patentovaný protokol, ktorý poskytuje real-time viditeľnosť a kontrolu, ale využíva minimálnu šírku pásma (typicky 1 kB/s alebo menej.)

Namiesto tradičnej sieťovej konfigurácie na báze príkazového riadka poskytuje Meraki vyspelú webovú ovládaciu lištu, poskytujúcu prehľad a kontrolu až nad desiatkami tisíc Meraki zariadení kdekoľvek vo svete. Nástroje určené na škálovanie veľkých a distribuovaných sietí, zmeny politík, aktualizácie firmvéru, nasadzovania novej pobočky, sú jednoduché a účelné, bez ohľadu na veľkosť alebo lokalitu. Meraki protokoly bežiace v reálnom čase kombinujú bezprostrednosť prostredia aplikácie s jednoduchosťou a centralizovaným riadením cloudovej aplikácie.

Každé zariadenie Meraki je navrhnuté za účelom fungovania v prostredí cloudu. Konkrétne to znamená, že zariadenia Meraki sú navrhnuté s pamäťou a CPU zdrojmi tak, aby mohli vykonávať spracovanie paketov QoS, zabezpečenia vo vrstve 3-7, šifrovanie, atď. na okraji siete. V dôsledku toho sieťová prevádzka neprechádza cez cloud, takže cloud poskytuje funkcionalitu mimo trasu dát. Táto architektúra umožňuje horizontálnu škálovateľnosť siete pridaním kapacity jednoducho tým, že pridá viac koncových bodov, bez obáv o centralizované prekážky lebo spomalenia. Rovnako dôležité je, že všetky pakety sa spracovávajú na požiadanie a funkcionalita koncového používateľa nie je ohrozená, ak sa preruší pripojenie do cloudu.

Cloudová platforma Meraki slúži k rozloženiu výpočtov a úložiska po nezávislých zoskupeniach serverov v geograficky izolovaných dátových centrách. Ktorýkoľvek server alebo dátové centrum môže zlyhať bez ovplyvnenia zákazníkov alebo zvyšku systému. Navyše, dizajn dátových centier Meraki je osvedčený v praxi, keďže poskytuje podporu desaťtisícom koncových bodov.

	Camppus /HQ
	Pobočky

	Maloobchodné predajne
	Pracovníci call centier
	Správa cloudových služieb
	Správa údajov
	On Prime Meraki hardvér
	Správa založená na prehliadačoch

Účinné nástroje pre prehľad a riešenie problémov

Cloudová architektúra Meraki poskytuje účinný prehľad a zahŕňa 5 nástrojov integrovaných priamo do ovládacej lišty a poskytuje tak okamžitú analýzu výkonu, pripojenia a mnohé iné charakteristiky. Pomocou živých nástrojov už správcovia siete neumožňujú byť prítomní fyzicky za účelom vykonania testov na riešenie problémov. Viditeľnosť do zariadení, užívateľov a aplikácií dáva správcom informácie potrebné na uplatňovanie politiky zabezpečenia a umožňuje vykonávanie potrebných úloh v dnešnom náročnom sieťovom prostredí.

Nástroje na riešenie problémov, ako je ping, traceroute, priepustnosť a dokonca live packet zachytenia sú integrované priamo do ovládacej lišty Meraki, čo dramaticky znižuje čas na vyriešenie problému a umožňuje jeho riešenie aj na vzdialených lokalitách bez nutnosti prítomnosti IT pracovníka.

Splnenie požiadaviek na súkromie a ochranu osobných údajov v EÚ

Cisco Meraki sa zaväzuje k ochrane osobných údajov, súkromia, bezpečnosti a dodržiavaniu príslušných regulačných rámcov v USA aj v zahraničí. Cloudová architektúra Meraki je navrhnutá od základu s ochranou dát, súkromia a bezpečnosti.

Technická architektúra Cisco Meraki a jej interné administratívne a procesné záruky pomáhajú zákazníkom s návrhom a nasadením riešení cloudových sietí, ktoré sú v súlade s predpismi na ochranu osobných údajov v EÚ, dokonca aj prípadoch mimo rámca dohody bezpečného prístavu (Safe Harbor). Základnými kameňmi architektúry Meraki s vhodným dizajnom sú:

- **Rovina riadenia Out-of-band (z externého pásma)** — zo zariadenia do cloudu Meraki prúdia len informácie na správu siete (nie užívateľské dáta), čo výrazne obmedzuje množstvo osobných údajov, ktoré sa prenášajú na cloud Meraki.
- **Cloud EÚ** — siete konfigurované na prevádzku v cloude EÚ zabezpečujú, že informácie pre správu siete sa ukladajú iba v Európskom hospodárskom priestore (EHP), vrátane obnovy a zálohovania. Zavedením osvedčených postupov zákazníci môžu zabrániť prenosu niektorých osobných údajov mimo EHP.
- **Dodatok o spracovaní údajov (Data Processing Addendum, DPA)** — Cisco Meraki umožňuje svojim zákazníkom DPA, ktorý zahŕňa štandardné zmluvné doložky Európskej komisie (tiež známy ako doložky modelu EÚ), takže zákazníci môžu umožniť prenos a spracovanie osobných údajov mimo EHP v súlade s

platnými európskymi predpismi na ochranu súkromia a osobných údajov a miestnymi zákonmi. Len pre informáciu je DPA k dispozícii aj v nemčine a francúzštine.

Ďalšie informácie o DPA a zárukách, ktoré využívame v súvislosti s prenosmi dát z EHP, môžete nájsť v našich často kladených otázkach - FAQ. FAQ sú k dispozícii aj v nemčine. Informácie súvisiace s cloudom EÚ Meraki sú k dispozícii v liste Cloud EÚ a Príručke konfigurácií cloudu EÚ.
Ďalšie informácie súvisiace s cloudom EÚ Meraki sú k dispozícii v liste Cloud EÚ a Príručke konfigurácií cloudu EÚ.

Riešenie dátového centra Cisco Meraki

Služba Cisco Meraki je spolu umiestnená na vrstve 1 v certifikovaných dátových centrách SAS70 typu II / SSAE16. Tieto dátové centrá zabezpečujú najmodernejšiu fyzickú a kybernetickú bezpečnosť a vysoko spoľahlivé riešenia. Všetky služby Cisco Meraki sa replikujú cez niekoľko nezávislých dátových centier, takže zákaznícky orientované služby sa v prípade katastrofického zlyhania dátového centra obnovujú rýchlejšie.

Sledovanie dostupnosti

- Dohoda o 99,99% dostupnosti služieb (to je menej ako jedna hodina ročne)
- 24 hodín x 7 dní v týždni automatická detekcia zlyhania - všetky servery sa testujú každých päť minút z viacerých umiestnení
- Procesy rýchlej eskalácie vo viacerých prevádzkových tímoch
- Nezávislý systém upozornenia na výpadok s 3-násobnou redundanciou

Redundancia

- Celosvetovo distribuované dátové centrá
- Dáta každého zákazníka (konfigurácia siete a metriky týkajúce sa používania) sa replikujú v rámci troch nezávislých dátových centier
- Replikácia dát medzi dátovými centrami v reálnom čase (do 60 sekúnd)
- Archivácia záloh počas noci

Zotavenie po havárii

- Rýchle obnovenie v hot spare (kompletný priestor v alternatívnej lokalite) v prípade zlyhania hardvéru alebo prírodnej katastrofy
- Architektúra správy z externého pásma (out of band) zachováva funkčnosť siete koncových užívateľov aj v prípade, keď sa pripojenie ku coudovým službám Cisco Meraki preruší
- Týždenné trénovanie procesov obnovy pri poruche

Bezpečnosť cloudových služieb

- 24 hodín x 7 dní v týždni automatická detekcia narušenia
- Ochrana cez IP a firewally na báze portov
- Vzdialený prístup obmedzený podľa IP adresy a overený verejným kľúčom (RSA)
- Systémy nie sú prístupné prostredníctvom hesla
- Administrátori sa automaticky upozorňujú na zmeny konfigurácie

Architektúra Out-of-Band

- V cloude je uložená iba konfigurácia siete a štatistiky využívania
- Údaje koncových používateľov cez dátové centrum neprechádzajú
- Všetky citlivé dáta (napr. heslá) sa uchovávajú zašifrované

Fyzická bezpečnosť

- Pre riadenie prístupu k zariadeniu sa využíva systém na kartové kľúče s vysokou bezpečnosťou a biometrické čítačky
- Všetky vstupy, výstupy a skrine sú monitorované kamerovým systémom
- Ochranka sleduje všetkých vchádzajúcich do dátových centier a vychádzajúcich z nich 24 hodín x 7 dní v týždni, čo zaisťuje, že sa dodržiavajú procesy pre vstup

Pripravenosť na katastrofy

- Dátové centrá sú vybavené sofistikovanými hasiacimi zariadeniami s blokovaním, aby sa zabránilo neúmyselnému vypusteniu vody
- Záložné napájanie dieselovými motormi v prípade výpadku napájania
- Systémy napájania typu UPS (neprerušiteľný zdroj napájania) a v prípade úplného výpadku prúdu zabezpečenie riadneho vypnutia
- Každé dátové centrum využíva službu najmenej dvoch nosičov najvyššej úrovne
- Pre zvýšené podlahy, skrine a podporné systémy je k dispozícii seizmické vystuženie
- V prípade katastrofického zlyhania dátového centra sa služba obnoví v inom, geograficky oddelenom dátovom centre

Regulácia z pohľadu životného prostredia

- Predimenzované systémy na vykurovanie, ventiláciu a chladenie poskytujú chladenie aj reguláciu vlhkosti
- Na rozvod vzduchu slúžia podlahové systémy

Pravidelné testovanie vniknutia

- Všetky dátové centrá Cisco Meraki prechádzajú každý deň testovaním vniknutia, ktorý realizuje nezávislá tretia strana

Certifikácia dátových centier

- Dátové centrá Cisco Meraki sú certifikované ako SSAE16 / SAS70, typ II

Cisco Meraki cloud manažment dovoľuje aj nasledovné aplikácie v spolupráci s ďalšími aktívnymi prvkami v sieti:

centrálny IPv4 NAT

filtrovania obsahu a blokovania nevhodného obsahu (podľa kľúčových slov, URL, verejne dostupných blacklistov)

podľa času (vyučovací čas, ostatný čas),

podľa WiFi SSID/LAN

Predstavuje cloud manažment riešenie, ktoré nepotrebuje umiestniť riadiaci systém v žiadnej lokalite obstarávateľa.

Dátová prevádzka používateľov pripojených k wifi prístupovým bodom nie je smerovaná cez riadiaci systém, avšak pre riadiaci systém môže uchovávať štatistické informácie o dátovej prevádzke používateľov.

Komunikácia medzi riadiacim systémom a wifi prístupovým bodom je kryptovaná, na úrovni protokolu AES 256 alebo ekvivalentného.

Rozširovanie siete nevyžaduje inštaláciu riadiaceho systému v žiadnej lokalite zákazníka. Riadiaci systém vie škálovať a obslúžiť 15 000 bezdrôtových prístupových bodov.

Obsluha riadiaceho systému je cez webové rozhranie dostupné cez protokol HTTPS a šifrované AES s 128 bitovým kľúčom

Správcovi je umožnený prístup na riadiaci systém na základe overenia jeho používateľského mena a hesla a podľa jemu pridelenej právomoci (plné práva, práva na čítanie, žiadne práva).

Systém poskytuje zálohovanie riadiaceho systému a prevádzku s dostupnosťou na úrovni 99.9%

V prípade nedostupnosti riadiaceho systému:
už autentifikovaní užívatelia ostávajú pripojení,
dátová komunikácia prebieha bez prerušenia,
používatelia môžu roamovať medzi wifi prístupovými bodmi,
pravidlá pre limity na šírku pásma ostávajú v platnosti a sú naďalej aplikované,
skupinové a bezpečnostné politiky ostávajú v platnosti a sú naďalej aplikované,
RF vlastnosti bezdrôtovej siete (DFS) sú bez prerušenia,
mesh WiFi infraštruktúra pracuje bez prerušenia.

Všetky nové funkcie, ktoré sú kompatibilné s wifi prístupovými bodmi zakúpené na obdobie 1/3/5/7 aklebo 10 rokov sú dostupné zákazníkovi bez cenového navýšenia.

Podpora IPv4 a IPv6.

Podpora WMM/IEEE 802.11e.

Podpora plnotextového vyhľadávania v systéme a vyhľadávania na základe správcom priradenej identifikácie zariadení (napr. číslo inventáru).

Celá prevádzka medzi wifi mesh prístupovými bodmi je kryptovaná na úrovni AES 256.

Integrácia s mapami Google alebo ekvivalentnými a zobrazenie polohy wifi prístupových bodov.

Integrácia CAD alebo ekvivalentnými nástrojmi nákresov podlaží lokalít s podporou formátov ako sú JPEG, GIF, PDF, PNG.

Adaptácia na problémy súvisiace s RF pokrytím:

automatické vykrytie oblastí rádiových dier, manuálne aj automatické nastavovanie vyžarovacieho výkonu jednotlivých wifi prístupových bodov. Automatické nastavenie jekoordinované riadiacim systémom pre dosiahnutie najlepšieho možného výsledku,

manuálne aj automatické prideľovanie neprekrývajúcich sa kanálov na každý wifi prístupový bod. Automatické nastavenie jekoordinované s riadiacim systémom pre dosiahnutie najlepšieho možného výsledku,

podpora prepnutia wifi prístupového bodu do módu merania wifi signálu v reálnom čase pre potreby obhliadky priestorov nepokrytých wifi signálom,

Bezpečnosť a manažment:

bezpečné pripojenie wifi klientov na úrovni IEEE 802.11i spolu s IEEE 802.1x a RADIUS. Šifrovanie na úrovni AES s 128 bitovým kľúčom. Podpora EAP-MSCHAPv2 , EAP-TLS a EAP-TTLS. Integrácia

s externým úložiskom identít používateľov pomocou Windows Active Directory alebo ekvivalentnými alebo LDAP,

podpora MAC autentifikácie pre zariadenia bez IEEE 802.1x klientského softvéru,

aplikovanie rôznych bezpečnostných politík na základe prihlásenia používateľa. (napr. iné oprávnenia má užívateľ v prvej užívateľskej skupine, iné v druhej, tretej, ďalšej skupine a pod.),

podpora webovej autentifikácie pre návštevy pomocou protokolu HTTP aj HTTPS. Webový portál je možné hosťovať priamo v riadiacom systéme alebo na externom serveri,

filtrovanie nevhodného obsahu, vrátane webových stránok s pornografickým obsahom, hier cez internet, atď. Blokovanie aplikácií ako sú napríklad bitTorenty, sociálne médiá, atď.,

vytváranie whitelist a blacklist pre individuálnych používateľov na SSID báze,

limitovanie šírky pásma na úrovni SSID aj na úrovni používateľa. V pravidlách pre limity je možné definovať cieľové IP adresy, porty, doménové mená, rozpoznané aplikácie aj skupiny aplikácií,

podpora aplikačného firewallu. V pravidlách pre firewall je možné definovať cieľové IP adresy, porty, doménové mená, rozpoznané aplikácie aj skupiny aplikácií,

zabudovaná podpora pre wifi IPS služby,

systém podporuje detekciu a remediáciu proti rogue WiFi prístupovým bodom a aj tzv. honeypot rogue wifi prístupovým bodom,

systém podporuje detekciu DoS útokov, ako napr. záplava paketmi,

podpora manažmentu koncových zariadení umožňujúca centrálne spravovať
a kontrolovať koncové zariadenia používané používateľom.

Podpora mobility:

je poskytnutá podpora pre L2 a L3 roaming,

pripájanie zariadení podporujúcich 5GHz aj 2.4GHz pásmo do 5GHz pásma, tzv. band steering.

Lokalizačné služby:

vizualizácia pohybu a hustoty pripojených zariadení v jednotlivých lokalitách podľa času. Zobrazenie tejto informácie na importovanom nákrese podlažia,

Poskytuje API pre integráciu s trasovacími systémami tretích strán.

Monitoring a štatistiky:

logovanie a ukladanie eventov automaticky,

podpora nástrojov pre zrýchlené a zjednodušené riešenie problémov

v bezdrôtovej sieti - zabudovaný spektrálny analyzátor pre vizualizáciu rádiového spektra, odchytávanie paketov medzi wifi prístupovým bodom a pripojeným koncovým zariadením s možnosťou exportu v pcap formáte,

riadiaci systém dovoľuje umožniť uchovávanie udalostí, ich vyhľadávanie, tvorbu reportov, export udalostí cez Syslog, SNMP alebo XML, uchovávanie štatistík podľa jednotlivých aplikácií, pridávanie nových aplikačných signatúr bez nutnosti softvérového update a heuristickú identifikáciu dynamických aplikácií (napr. skype),

riadiaci systém dovoľuje umožniť proaktívne notifikovať správcu systému o zmenách (detekcia výpadku a rogue wifi prístupového bodu) cez email, Syslog alebo SNMPv3,

Riadiaci systém dovoľuje trasovať všetky konfiguračné zmeny, ktoré správca v riadiacom systéme vykoná,

historický report dovoľuje obsahovať údaje za posledný 1 mesiac a dovoľuje obsahovať tieto informácie – celkový počet prenesených dát, top 10 SSID podľa prenesených dát a počtu pripojených klientov, top 10 wifi prístupových bodov podľa prenesených dát a počtu pripojených klientov, top 10 používateľov podľa prenesených dát, top 10 aplikácií podľa prenesených dát, top 10 operačných systémov podľa prenesených dát a počtu pripojených klientov. Historický report je možné poslať napr. emailom jednorazovo alebo periodicky,

štatistiky podľa jednotlivých aplikácií umožňujú obsahovať globálny náhľad pre každé SSID a lokálny náhľad podľa každej aplikácie. Štatistiky podľa aplikácií ako aj podľa konkrétneho používateľa umožňujú obsahovať tieto informácie: názov aplikácie, kategóriu aplikácie, prenosový protokol, číslo portu, počet prenesených dát (rozdelený na upstream a downstream), zoznam klientov používajúcich danú aplikáciu, cieľové domény, IP adresy a operačný systém. Riadiaci systém dovoľuje udržať históriu týchto štatistík po dobu 1 mesiaca a umožniť export vo formáte CSV alebo XML.

Riešenie umožňuje nastaviť, že riadiaca prevádzka z WiFi prístupových bodov, používateľské štatistiky a lokalizačné dáta nikdy neopustia územie Európskej únie.

Ovládacia plocha out-of-band

Out-of-band ovládacia plocha Meraki oddeľuje údaje sieťovej správy od užívateľských dát. Správa údajov (napríklad konfigurácie, štatistiky, monitorovanie, atď) prichádza zo zariadení Meraki (bezdrôtové prístupové body, prepínače a bezpečnostné zariadenia) do Meraki cloudu cez zabezpečené internetové pripojenie. Užívateľské dáta (webový prehliadač, interné aplikácie, atď.) neprichádzajú do cloudu, namiesto toho plynú priamo na miesto určenia v sieti LAN, alebo cez WAN.

Výhody ovládacej plochy out of band Škálovateľnosť
• Neobmedzená priepustnosť: žiadne prekážky centrálneho správcu

• Pridávanie zariadení alebo lokalít bez MPLS tunelov

• Pridávanie kapacity bez stohovacieho obmedzenia

Spoľahlivosť
• Redundantné cloudové služby poskytujú vysokú dostupnosť

• Sieť funguje aj v prípade, že riadenie prevádzky je prerušené

Bezpečnosť
• Cez dátové centrá Meraki neprechádza žiadna sieťová prevádzka užívateľa

• Plne kompatibilné s HIPAA / PCI

Sieťová prevádzka užívateľa	Sieťová prevádzka užívateľa
Správa údajov	Správa údajov

Čo sa stane, ak sieť stratí pripojenie ku Meraki cloudu?
Vďaka Meraki out of band architektúre nebude väčšina koncových užívateľov ovplyvnená prípadným komunikačným výpadkom prístupových bodov či ističov alebo ak bezpečnostné zariadenia nebudú môcť nadviazať spojenie s cloudovými službami Meraki (napr. kvôli dočasnej poruche WAN):

• Užívatelia budú môcť využívať lokálnu sieť (tlačiarne, zdieľanie súborov atď.)

• V prípade, že je k dispozícii WAN, užívatelia budú mať prístup k internetu

• Sieťové pravidlá (pravidlá pre firewall, QoS, atď) sa budú aj naďalej uplatňovať

• Používatelia sa môžu identifikovať prostredníctvom 802.1X/RADIUS a môžu sa bezdrôtovo presúvať medzi prístupovými bodmi

• Užívatelia môžu iniciovať a obnovovať DHCP leasy

• Vytvorené VPN tunely budú aj ďalej funkčné

• Lokálne konfiguračné nástroje budú k dispozícii (napríklad IP konfigurácie zariadení

Pri nemožnosti nadviazať spojenie s Meraki cloudom bude správa, monitoring a hostingové služby dočasne nedostupné:
• Konfiguračné a diagnostické nástroje nebudú k dispozícii

• Štatistiky využitia budú uložené lokálne, kým nedôjde k opätovnému pripojeniu a následne budú uložené do cloudu

• Úvodné stránky a súvisiace funkcie nebudú k dispozícii

Dizajn Datacentra Meraki

Správa cloudových služieb je súbežná s certifikovanými dátovými centrami tier-1, SAS70 typ II. Tieto dátové centrá sú navrhnuté z pohľadu fyzickej i kybernetickej bezpečnosti ako najmodernejšie a najspoľahlivejšie centrá svojho druhu. Všetky služby Meraki sa replikujú cez viacero nezávislých dátových centier, aby zákaznícky orientované služby boli chránené v prípade katastrofálneho zlyhania príslušného dátového centra.

Redundancia

- Päť geograficky rozptýlených dátových centier
- Všetky dáta zákazníka (sieťové konfigurácie a metrika používania) sa replikujú cez tri nezávislé dátové centrá
- Real-time replikácia dát medzi dátovými centrami (do 60 sekúnd)
- Nočné zálohovanie pre účely archivácie

Monitoring dostupnosti

- 24 x 7 automatická detekcia porúch - všetky servery sú testované každých päť minút z viacerých miest
- Rýchle postupy eskalácie cez viaceré operačné tímy
- Nezávislé výstražný systém pri výpadku s 3-násobnou redundanciou

Obnovenie po výpadku

- Rýchle obnovenie do hot spare v prípade zlyhania hardvéru alebo prírodnej katastrofy
- Out of band architektúra zachováva sieťovú funkcionalitu koncového užívateľa aj v prípade prerušenia pripojenia ku cloudovým službám Meraki
- Testovanie postupov v prípade zlyhania na týždennej báze

Zabezpečenie cloudových služieb

- 24 x 7 automatická detekcia narušenia
- Chránené prostredníctvom IP a na port nastavených firewallov
- Prístup obmedzený IP adresou a overený verejným kľúčom (RSA)
- Systémy nie sú prístupné prostredníctvom zadania hesla
- Správcovia sú automaticky upozornení na zmeny konfigurácie

Fyzická bezpečnosť

- Vstup do zariadenia je kontrolovaný kartovými kľúčmi s vysokou úrovňou bezpečnosti a biometrickými čítačkami
- Všetky vstupy, východy a skrine sú monitorované kamerovým systémom
- Bezpečnostný personál monitoruje všetky vstupy do a z dátového centra 24 x 7, čo zabezpečuje dodržiavanie procedúr pre vstup.

Out-of-Band architektúra

- V cloude sú uložené iba konfigurácie a užívateľské štatistiky
- Údaje koncových užívateľov cez dátové centrum neprechádzajú.
- Všetky citlivé údaje (napr. heslá) sú uložené v šifrovanej podobe

Pripravenosť na katastrofy

- Dátové centrá sú vybavené sofistikovanými hasiacimi systémami s blokovacími mechanizmami na zabránenie náhodného spustenia vody
- Dieselové generátory poskytnú v prípade výpadku energie záložné napájanie
- UPS systémy poskytujú záložné napájanie a zabezpečia riadne vypnutie v prípade opätovného nabehnutia napájania
- Každé dátové centrum má k dispozícii služby aspoň dvoch špičkových dopravcov
- Seizmické ukotvenie pre zvýšené podlahy, skrine a podporné systémy

- V prípade katastrofálneho výpadku dátového centra sa služby presunú do iného geograficky oddeleného dátového centra

Kontrola životného prostredia

- Klimatizačné systémy poskytujúce chladenie a kontrolu vlhkosti sú naprojektované s dostatočnou výkonovou rezervou
- Podlahové systémy sú určené pre distribúciu vzduchu

Certifikácia

- Dátové centrá Meraki sú certifikované centrá typu SAS70 II
- Certifikovaná úroveň PCI 1

Dohoda o úrovni poskytovaných služieb

- Správa cloudu Meraki je istená na úrovni 99,99% SLA prevádzkyschopnosti. Podrobnosti nájdete na www.meraki.com/trust.

Bezpečnostné nástroje pre správcov

Okrem out-of-band architektúry a náročných podmienok dátových centier poskytuje Meraki celý rad nástrojov pre správcov s cieľom maximalizovať bezpečnosť ich sieťového nasadenia. Tieto nástroje poskytujú optimálnu ochranu, prehľad a kontrolu nad sieťou Meraki.

Dvojstupňová autentifikácia

Dvojstupňová autentifikácia pridáva ďalšiu vrstvu zabezpečenia siete organizácie požadovaním prístupu k telefónu správcu, okrem jeho užívateľského mena a hesla pri prihlasovaní sa do cloudových služieb Meraki. Dvojstupňová autentifikácia Meraki využíva bezpečnú, pohodlnú a nákladovo efektívnu technológiu SMS: po zadaní mena a hesla, správca obdrží jednorazové heslo cez SMS, ktoré je potrebné zadať pred dokončením autentifikácie. V prípade, že hacker uhádne alebo sa dostane k heslu správcu, keďže nebude mať prístup k telefónu správcu. Meraki ponúka dvojstupňovú autentifikáciu pre všetkých podnikových užívateľov bez dodatočných nákladov

Zásady v oblasti hesiel

Bezpečnostná politika Meraki v oblasti účtov pomáha ochrániť prístup k ovládaciemu panelu Meraki Tieto nástroje umožňujú správcom:

- Vynútiť si periodické zmeny hesla (napr. každých 90 dní)
- Vyžadujú minimálnu dĺžku hesla a jeho zložitosť
- Uzamknúť prístup užívateľa po opakovaných neúspešných pokusoch o prihlásenie
- Zakázať opätovné použitie hesla
- Obmedziť login podľa IP adresy

Správa v závislosti na rolách

Správa v závislosti na rolách umožňuje dohľadu vybrať správcov pre špecifické podskupiny organizácie, a určiť, či majú mať iba prístup k čítaniu správ a nástrojom na riešenie problémov, spravovať prístup hostí, alebo môžu vykonávať zmeny konfigurácie siete. Toto minimalizuje pravdepodobnosť náhodnej alebo zámernej nesprávnej konfigurácie a obmedziť chyby na izolované častí siete.

Upozornenia na zmeny konfigurácie

Systém Meraki môže automaticky odoslať čitateľný e-mail a textovú správu pri vykonaní konfiguračnej zmeny a umožniť tak celej IT organizácii držať krok s novými politikami. Upozornenia na zmeny sú dôležité najmä vo veľkých alebo distribuovaných IT organizáciách.

Audity prihlásení a konfigurácie

Merak zapisuje čas, IP a približné umiestnenie (mesto, štát) prihlásených správcov. Vyhľadateľný zmenový log konfigurácie naznačuje kým boli vykonané zmeny konfigurácie a v ktorej časti organizácie zmena nastala.

SSL certifikáty
Účty Meraki sú prístupné iba cez https, čo zaručuje, že celá komunikácia medzi prehliadačom správcu a cloudovými službami Meraki je šifrovaná.

Časový limit pre nečinnosť
30 sekúnd pred odhlásením sa používateľom zobrazí upozornenie, ktoré umožňuje predĺžiť ich session. Keď tento čas vyprší, používatelia sa umožňujú opätovne prihlásiť.