Zscaler představení portfolia

Současná doba vyžaduje zajistit uživatelům nejen přístup k firemním datům, ale také ochránit data proti hrozbám, kterých na internetu číhá stále více.

V roce 2021 došlo k 495 mil. ransomware útoků, což byl roční nárust o 148 %. Firemní data se přitom mohou nacházet jak v datacentru zákazníka nebo externího poskytovatele služeb, tak například ve veřejném či privátním cloudu. Uživatelé dnes potřebují pracovat z jakéhokoliv místa na světě, a tak úkolem IT oddělení je zajistit potřebné podmínky a zabezpečit koncová zařízení a firemní data proti ztrátě nebo ohrožení. Jak? Velmi efektivně to jde s využitím cloudového řešení, se kterým máme velmi dobré zkušenosti.

Kdo je to Zscaler a co dělá?

Zscaler je společnost poskytující služby v oblasti podnikové bezpečnosti cloudu. Společnost Zscaler byla založena v roce 2007 se sídlem v San Jose v Kalifornii. Má registrováno přes 270 patentů a má přes 5000 zaměstnanců. Její produkt Cloud Proxy ZIA se již několik let umisťuje jako Leader v Gartner Magic Quadrantu. Má přes 6700 zákazníků a z toho 30 % z Forbes Global 2000.

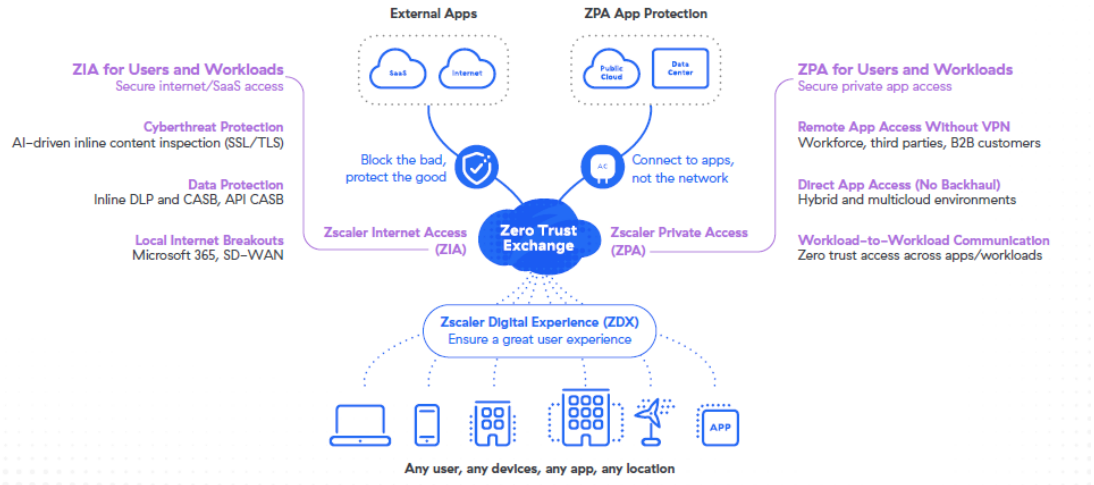
Zscaler má datová centra po celém světě, ve více jak 150 lokalitách. Má přímé propojení mezi svými datacentry a datacentry Microsoft a stará se o detekci provozu do datacenter Microsoftu automaticky, čímž odpadá další zátěž pro IT oddělení. Zscaler urychluje digitální transformaci, aby zákazníci mohli být agilnější, efektivnější, odolnější a bezpečnější. Zscaler nativní cloudová platforma Zero Trust Exchange chrání tisíce zákazníků před kybernetickými útoky a ztrátou dat tím, že bezpečně připojuje uživatele, zařízení a aplikace z jakéhokoliv místa a kdekoliv.

Portfolio Zscaler

Zscaler nabízí kompletní řešení pro Zero Trust přístup k firemním aplikacím (ať už se nacházejí v on-premises datacentrech nebo v cloudu) a k internetu. Přístup Zscaleru k tomuto řešení je i v současné době unikátní, protože není postaven na propojování sítí, ale na propojování uživatelů s aplikacemi.

Řešení lze nabídnout buď v kompletní podobě, nebo rozdělené po jednotlivých produktech (respektive po částech řešení), což jsou:

- Zscaler Private Access (ZPA) - Zero trust přístup
- Zscaler Internet Access (ZIA) - Cloud proxy
- Zscaler Digital Experience (ZDX) - End to end monitoring uživatelů a aplikací
- Zscaler Cloud Control - Řízení přístupu ke cloudovým službám



Zero Trust Network Access (ZTNA)

ZTNA je moderní koncept přístupu k firemní síti s nulovou důvěrou. To je přesný opak VPN přístupu, kde uživatel má po přístupu do sítě neomezený přístup.

Veškerá komunikace je zabezpečená

ZTNA ve výchozím stavu žádný přístup nedovoluje. Ke konkrétním zdrojům musí být udělen jedinečný přístup. To znamená, že uživatelé pracující v prostředí ZTNA nemají přístupy do aplikací a služeb uvnitř prostředí bez explicitně udělených práv pro přístup k nim. ZTNA je důležitý pro organizace, jejichž velká část pracovních sil přistupuje k interním zdrojům z domácností/hotelů po celém světě a různých zařízení.

Každý přístup je jedinečný

Udělení či neudělení důvěry zařízení či identitě v předchozí relaci nemá žádný vliv pro následující relace. Anomální chování uživatele nebo změna bezpečnostního stavu přistupujícího zařízení jsou pokaždé vyhodnocovány a rozhodují o udělení přístupu a o jeho rozsahu.

Parametry jsou například identita uživatele, lokalita, či čas přístupu aj. U zařízení je to bezpečnostní stav zařízení (Compliance). Následně se tyto hodnoty vyhodnocují a dle nastavení aktuálních podmínek uživatele a zařízení se poskytne úplný přístup, omezený přístup, nebo dokonce dojde k odepření přístupu.

Řešení pro rizikový přístup

Na základě informací od uživatele a zařízení je možné si vyžádat vyšší úroveň autentizace, například více-faktorovou autentizaci (MFA) anebo aplikovat omezení úrovně udělovaného přístupu.

Klíčové vlastnosti ZTNA:

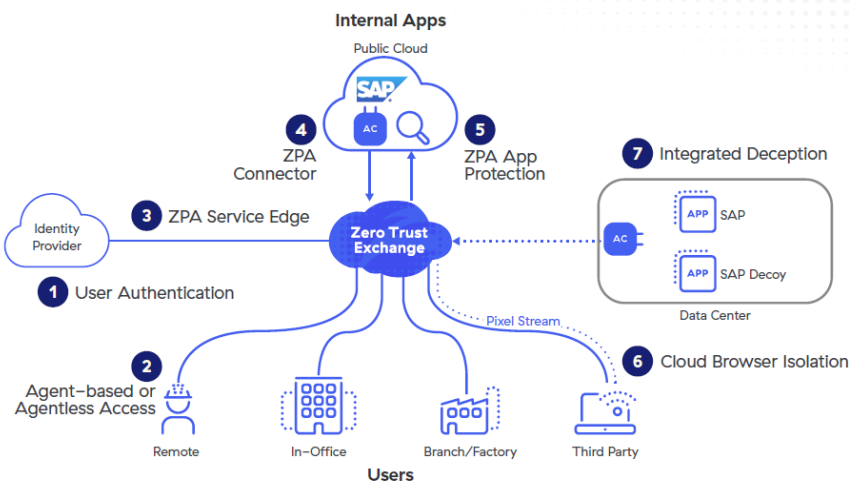
- Konstantní monitoring a validace přístupů
- Přidělení omezeného rozsahu a jen nejnutnějších zdrojů
- Kontrola přistupujícího zařízení
- Mikro-Segmentace
- Jen omezené možnosti pohybu uživatele v prostředí
- Více-faktorové ověřování

Monitoring a stav bezpečnosti

Každý požadavek v ZTNA na zdroj by měl vyvolat posouzení bezpečnostního stavu. To zahrnuje nepřetržité monitorování stavu podnikových aktiv, ať už ve vlastnictví organizace nebo např. BYOD, pokud mají přístup k interním zdrojům. Například kontrola, že přistupující zařízení neobsahuje žádné kritické zranitelnosti či že nechybějí důležité opravy zabezpečení.

Zscaler Private Access (ZPA)

Služba Zscaler Private Access (ZPA) umožňuje organizacím poskytovat přístup k interním aplikacím a službám, a zároveň zajistit bezpečnost jejich sítí. ZPA je moderní nákladově efektivnější a bezpečnější alternativa k VPN, a i její nasazení je jednodušší. Na rozdíl od sítí VPN, které pro přístup k podnikovým aplikacím vyžadují, aby se uživatelé připojovali do firemních sítí, tak ZPA umožňuje poskytnout uživatelům na základě zásad zabezpečený přístup pouze k interním aplikacím, které potřebují ke své práci. ZPA umožní přístup k aplikacím a nevyžaduje přístup k síti.



ZPA navíc odděluje aplikace od fyzické sítě, takže můžete zajistit bezproblémové připojení k soukromým interním aplikacím a aktivům, ať už jsou v cloudu, datovém centru nebo obojím. Také se dynamicky přizpůsobuje změnám sítě, takže můžete přesouvat své prostředky, aniž byste ovlivnili přístup uživatelů.

Zscaler Private Access je Cloudové řešení, a tak není potřeba kupovat drahé boxy do datacentra, o které je pak nutné se starat, upgradovat je, fixovat, a po pěti letech (případně dříve) je nakupovat znovu. Lze tak ušetřit nejen na pořizovací ceně, ale i na provozních nákladech a na případných výpadcích HW v datacentru.

Proč je VPN zastaralé řešení

VPN jsou již dlouho zavedenou metodou pro vzdálený přístup k podnikovým sítím, ale některé mají vážné problémy, zejména pokud jde o bezpečnost, používají zastaralé a neúčinné způsoby, jak přistupují k bezpečnosti.

Klienti připojeni VPN, mají často široký přístup ke všem zdrojům v síti. To do značné míry vystavuje zbytek podnikové sítě hrozbám, které využívají koncový bod jako vektor útoku.

Pokud je povolen split-tunel, uživatel může surfovat po internetu, aniž by musel použít podnikové firewally, a přitom je ale stále připojeni k firemní síti. Riziko úniku dat, ransomware útoky nebo napadení malwarem v podnikové síti, se exponenciálně zvyšuje, pokud je uživatel vlastním správcem OS např. u BYOD zařízeni. VPN na zařízeních v osobním vlastnictví mohou být už před navázáním VPN kompromitována.

VPN se používají k připojení k podnikové síti přes šifrovaný tunel při práci z hotspotů v hotelech, v kavárnách, popř. z domovů. Tento tunel zabraňuje kyberzločincům v slídění na relaci, ale také zabraňuje bezpečnostním kontrolám v kontrole provozu. Protože většina takových hotspotů je převážně připojena k nezabezpečeným sítím, jsou pro kyberzločince zneužitelným cílem pomocí taktik sociálního inženýrství a malwaru.

Aplikace a data jsou nyní rozšířeny napříč podnikovými datovými centry, multi-cloudovými prostředími, distribuovanými pobočkami a domácími kancelářemi. Většina řešení VPN nebyla navržena tak, aby zvládaly tuto úroveň složitosti. VPN připojení backhauluje veškerý provoz v rámci podnikové sítě pro kontrolu, která je náročná na šířku pásma a způsobuje latence.

Zscaler Internet Access (ZIA) - Cloudová proxy

Zscaler Internet Access (ZIA) nebo také cloudová proxy je řešení pro ochranu firemního uživatele, ať pracuje odkudkoliv, kontrola a filtrování přístupu probíhá přímo v cloudu. Tato technologie zároveň umí zabezpečit a ochránit přístup ke cloudovým podnikovým službám jako je Microsoft 365, Dynamics 365, Salesforce, atd. Datová centra Zscaler jsou propojena přímou linkou s datovými centry Microsoftu, kde běží Microsoft 365, takže je zajištěna vysoká rychlost přístupu k těmto službám.

Cloudová proxy umožňuje předefinovat starý přístup, který stavěl na bezpečnosti perimetru firmy, na přístup nový, kdy se chrání koncové zařízení, ať se nachází kdekoliv. Toto řešení umožňuje postupně opustit starý koncept využívání VPN a nahradit jej novým, který pracuje s uživatelovou stanicí jako s novým perimetrem. Přitom zachovává veškeré potřebné kontroly, které má moderní proxy poskytovat, např. filtrování URL a obsahu, kategorizace URL, inspekce SSL, cloudový firewall, antivirus, ochrana proti zero-day útokům pomocí sandboxingu, DLP, řízení propustnosti, autentizace uživatelů pomocí ADFS, Azure Active Directory atd.

Podle zveřejňovaných výsledků průzkumu Magic Quadrant od společnosti Gartner je Zscaler dlouhodobým leaderem v oblasti cloudových proxy (resp. Secure Web Gateway - SWG).

Ochrana uživatelů, ať jsou připojeni odkudkoliv - mobilita uživatelů se zrychleným a zjednodušeným přístupem ke cloudovým stále přibývajících služeb třetích stran, je primární výhodou této cloudové proxy. Výhodou je také to, že Zscaler pokrývá svými datovými centry celý svět, a to včetně Číny a jeho datová centra zvládnou stovky tisíc souběžných uživatelů s miliony souběžných relací.

Snadné škálování - díky tomu, že jde o cloudovou službu, odpadají problémy se škálováním, které běžně nastávají při použití hardwarových řešení (např. nákup HW boxů, jejich správa, upgrade, výměny atd.). Snadným škálováním odpadají i náročné odhady požadovaného výkonu při nákupech hardwarové infrastruktury. Uživatelé cloudové proxy vždy dostanou potřebný výkon, bez ohledu na jejich měnící se počet a na to, kolik je aktivováno bezpečnostních ochran. IT má k dispozici aktuální přehled o klientech a možnosti, jak kontrolovat provoz ve více komunikačních vrstvách jako jsou Firewall, Antivirus, SandBox, DLP atd.

Propojení s datovými centry Microsoft - cloudové služby Microsoftu (například Microsoft 365, Dynamics 365, Azure, atd.) dnes používá velké množství firem a jejich počet raketově roste. IT oddělení tedy musí mimo jiné řešit, jak bezpečně a rychle připojit svoji síť a své uživatele k Microsoft cloudu. Cloudová proxy je proto ideálním řešením, neboť Zscaler má přímé propojení mezi svými datacentry a datacentry Microsoft.

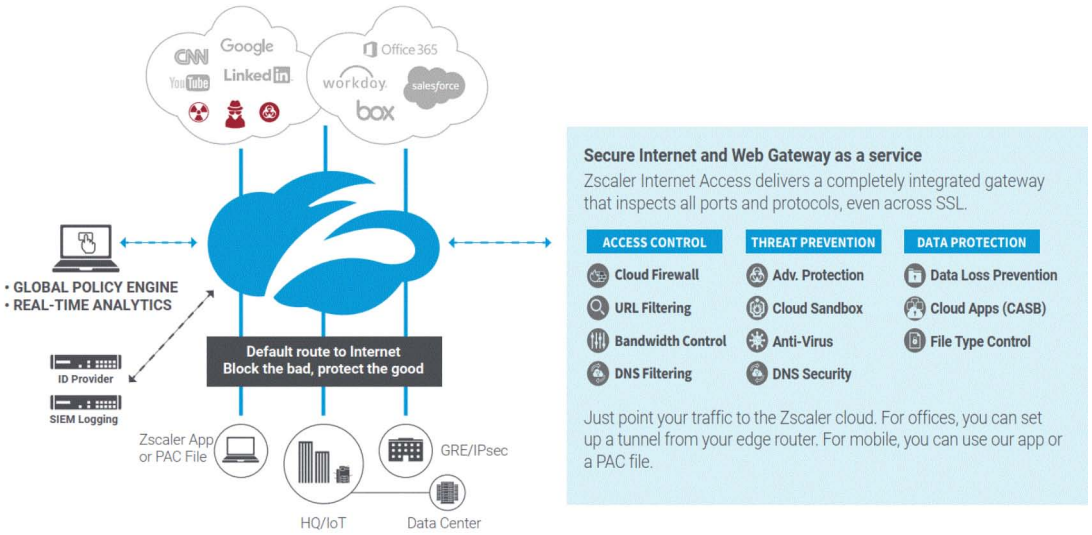
Snížení nákladů za firemní MPSL propojů a provoz z uživatelských zařízení lze nasměrovat do internetu již v místě vzniku požadavku, což může být třeba vzdálená pobočka firmy. Tím lze ušetřit náklady spojené s provozem podnikových MPLS linek, které často znamenají podstatné průběžné náklady. Přes MPLS linky pak jde jen o nezbytně nutný provoz, například připojení k firemnímu CRM, ERP a podobně, ale nikoliv běžný internetový provoz. Ten lze odbočit na nákladově efektivnější internetové připojení a tím výrazně ušetřit na poplatcích za MPLS linky.

Architektura Zscaler Internet Access

Architektura řešení je velmi efektivní tak, jak naznačuje přiložené schéma. Ve své podstatě stačí pouze přesměrovat internet provoz na zařízení uživatele (PC, NB, mobil, tablet) do datacentra Zscaleru.

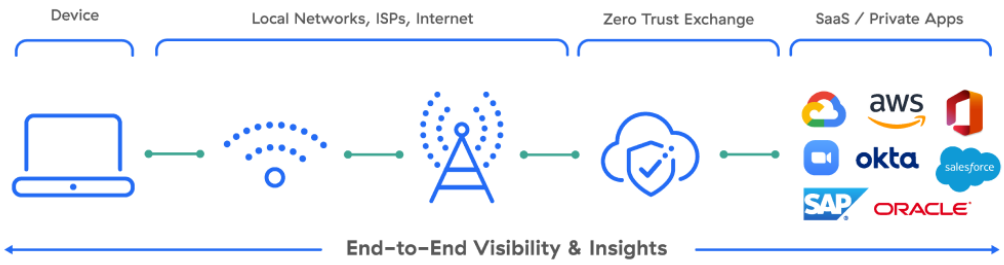
Přesměrování se provádí pomocí úpravy přímo v konfiguraci prohlížeče nebo pomocí instalované aplikace Zscaler Client Connector (nebo také zAPP), která kromě přesměrování provozu zajišťuje, že zásady zabezpečení a přístupu vaší organizace jsou vynuceny všude tam, kde uživatelé mohou přistupovat k internetu. V závislosti na počtu aktivních uživatelů, lze použít různé scénáře jejich připojení. Nejvíce výhod přináší kombinace nasazení klientské aplikace Zscaler Client Connector, která zajistí mobilním uživatelům spojení k nejbližšímu ZENu a napojení centrály či větších poboček na Zscaler ZENy pomocí GRE nebo IPSEC tunelů realizovaných z hraničních routerů.

Autentizace uživatelů je založena na použití standardu SAML 2.0. To otevírá možnosti použití širokého spektra poskytovatelů identity (IdP). Z on-premise řešení je podporováno Microsoft ADFS, z cloudových poskytovatelů Azure Active Directory, Okta, Gemalto, Onelogin. Ale v zásadě lze použít jakékoliv řešení založené na SAML 2.0. Licencování je založeno na počtu aktivních uživatelů a vybrané edici řešení. K dispozici jsou tři edice (Professional Edition, Business Edition a Transformation Edition), ke kterým lze ještě přikupovat další specifické funkcionality.



Zscaler Digital Experience (ZDX)

Zscaler Digital Experience pomáhá IT týmům monitorovat digitální události z perspektivy koncového uživatele k optimalizaci výkonu a rychlé nápravě přestupků problémy s aplikací, sítí a zařízením.



Zákazník získá viditelnost napříč zařízeními, sítěmi a aplikacemi - dokonce i těmi, které nemá pod kontrolou. Zjistí problémy dříve, než si uživatelé začnou stěžovat, a rychle tak určí hlavní příčinu. Zjednoduší si způsob monitorování pomocí jediného komplexního zobrazení.

Požadavky na monitorování se změnily díky cloudu a mobilní světu

Rychlé přijetí cloudových a mobilních zařízení v rámci organizací a přechod k práci odkudkoli přinesly nové výzvy i v oblasti monitorování pro IT týmy. Aplikace se přesouvají z center do cloudu. K nim je potřeba hybridní přístup vzdálených uživatelů, tedy IT týmy již nekontrolují infrastrukturu, z které se uživatelé přihlašují. Problémy s výkonem koncového uživatele vyplývající z dostupnosti SaaS nebo cloudových aplikací, domácí problémy s Wi-Fi, výpadky síťové cesty nebo sítě přetížení nelze tedy tak snadno izolovat a diagnostikovat.

Většina dnešních podniků má více bodů a monitorovací nástroje zakoupené a spravované různými IT týmy. Tyto nástroje vytvářejí informační sílu a nesdílejí mezi sebou žádný kontext, vedoucí k roztříštěné viditelnosti uživatelské zkušenosti a prodloužené době odstraňování problémů. Nástroje pro monitorování bodů optimalizované pro datová centra zanechávají mezery ve viditelnosti detekce, řešení problémů a diagnostiky problémů s výkonem na internetu koncového uživatele.

Digitální monitorování zkušeností hybridní pracovní síly vyžaduje moderní a dynamický přístup. IT týmy potřebují neustále monitorovat a měřit digitální provoz každého uživatele, bez ohledu na jejich umístění. Tradiční monitorovací nástroje využívají k monitorování přístup zaměřený na datová centra a shromažďování metrik z pevných webů častěji než přímo z uživatelského zařízení. Tento přístup neposkytuje jednotný pohled na výkon na základně uživatelského zařízení, síťové cesty nebo aplikace.

Pro jaké zákazníky je to vhodné?

Řešení je vhodné pro zákazníky ze všech oblastí trhu. Primárně lze cílit na zákazníky, kteří mají potřebu snadného připojení svých zaměstnanců k firemním datům a k internetu, ať se jejich koncové zařízení nachází kdekoliv. Velkou výhodou celého řešení je to, že není nutné propojovat sítě, takže dalším vhodným zákazníkem jsou firmy, které často provádějí akvizice a potřebují rychle propojit koupené firmy mezi sebou, respektive umožnit zaměstnancům přístup k aplikacím napříč firmami. Další vhodnou oblastí jsou zákazníci, kteří se vydali na cestu do cloudu a potřebují tedy připojit svoje zaměstnance k aplikacím, které se mohou nacházet jak v lokálním datacentru, tak i v cloudu. A v neposlední řadě jsou to firmy s větší sítí poboček, které s výhodou využijí možnost propojení s nižšími nároky na MPLS linky.

Proč Aricoma?

Firma Aricoma je partnerem firmy Zscaler od roku 2017. Pro implementace a podporu produktu má vyškolený tým odborníků s odpovídajícími certifikacemi a zkušenostmi z implementací i z provozu řešení Zscaler. V neposlední řadě má Aricoma dlouholeté zkušenosti s implementací bezpečnostních řešení pro svoje zákazníky a je spolehlivým partnerem pro velké, střední i malé firmy a také pro organizace v rámci veřejné správy.

Reference

V České Republice se Aricoma podílela na nasazení, rozvoji a správě řešení u firem Škoda-Auto, Liberty Steel a Czech Trade. Po světě (včetně Evropy) má Zscaler nepřeberné množství referencí a v Západní Evropě je defacto standardem pro řešení webové proxy pro velké zákazníky.