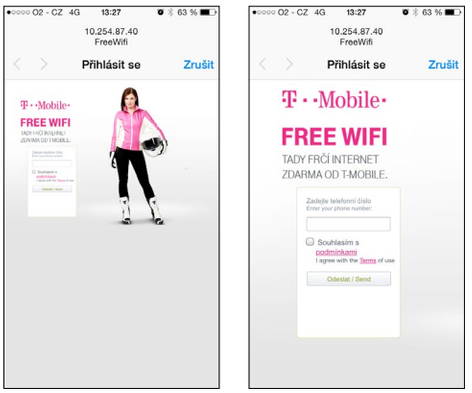
Extreme networks

BYOD řešení řízení přístupu do sítě v síti T-mobile ČR od Extreme Networks

Jednoduchý a bezpečný přístup do sítě a jednotná správa jsou klíče jak ke spokojeným zákazníkům, tak provozovateli.

Mobilita je trendem dnešní doby. Nejsou to jen zaměstnanci, ale také zákazníci T-mobilu, kontraktoři či hosté, kteří vyžadují vysokorychlostní a spolehlivý přístup k síti prostřednictvím Wi-Fi jako alternativy k mobilnímu připojení.

Ve spolupráci s dodavatelem Extreme Networks T-mobile nasadil řešení pro řízení přístupu do sítě v celé své pevné i bezdrátové Wi-Fi síti. Hlavním cílem bylo zajistit co nejjednodušší, a přitom spolehlivé a bezpečné přihlášení pro jednotlivé klienty a následné přidělení příslušných práv podle toho, o jaký typ uživatele se jedná.

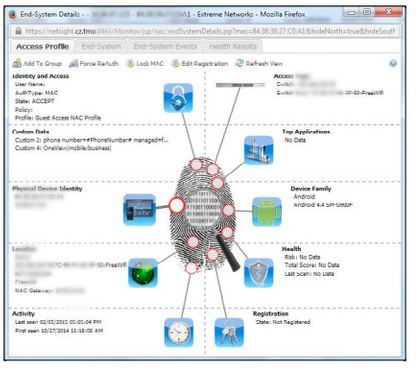


A právě flexibilita a jednoduchost řešení byly jedněmi z hlavních kritérií nasazení. Celkem pochopitelně bylo jako hlavní kritérium identifikace vybráno mobilní telefonní číslo. Uživatel je po připojení k Wi-Fi síti přesměrován automaticky na přístupový portál (viz obrázky), kde jediné, co musí zadat, je mobilní telefonní číslo. Na něj mu posléze přijde SMS s PIN, které je nutné zadat kvůli ověření a akceptovat podmínky připojení. Podle čísla již T-mobile pozná, zdali je uživatel interním či externím zaměstnancem, zákazníkem nebo zákazníkem konkurence. Následně systém přiřadí příslušný přístupový profil (VLAN, ACL, QoS, rate limit atd.). Systém je dále integrován s MDM řešením. V případě, že se jedná o interního zaměstnance s instalovaným MDM klientem pod správou T-mobilu (v tomto případě se jedná o jedno z nejrozšířenějších řešení Mobile Iron), pak není nutné zadávat vůbec nic a zaměstnanec dostane přístup do sítě automaticky podle stavu mobilního zařízení. Toto nasazení je ukázkou životaschopnosti BYOD řešení, neboť v tomto případě si zaměstnanci mohou s sebou nosit vlastní zařízení. Přístup do sítě pak dostanou podle toho, o jaké zařízení se jedná a zdali není připojení potenciálním bezpečnostním rizikem.

Řešení umožňuje, aby na příslušné uživatelské role byly po přihlášení aplikovány síťové profily různé pro zaměstnance a hosty, různé pro notebook, tablet, chytrý telefon, IP telefon, tiskárnu atd. Profily umožňují povolovat, odmítat, prioritizovat, nastavovat rychlostní limity, přesměrovávat a provádět audit síťového provozu. To vše na základě atributů, jako jsou identita uživatele, čas, umístění, typ zařízení, soulad s bezpečnostní politikou, a dalších parametrů souvisejících s okolním prostředím. V existující síti T-mobilu se zachovala původní infrastruktura, a využívá se tak standard RFC 3580 (přiřazení adekvátní VLAN) a dynamických Radius atributů (přiřazení dynamických ACL). V síti LAN se navíc používají dočasní SW agenti pro zjištění bezpečnostního stavu zařízení (tzv. Healthcheck).

Zásadním kritériem pro výběr tohoto řešení byla nutnost zachovat současnou jak pevnou, tak bezdrátovou infrastrukturu, a to se podařilo. Celé řešení je navíc založené kompletně na standardech, nevyžaduje instalaci žádných dalších agentů. Management je provozován na virtualizované platformě, což přináší další úspory a garanci dlouhé životnosti (řešení však dovoluje virtualizovat i jednotlivé autentizační brány). T-mobile navíc není vázán k provozování proprietárního systému a nutnosti zavázat se tak k nákupu dalších komponent od jednoho jediného výrobce.

Automatizované nasazování síťových profilů výrazně snížilo provozní náklady a poskytuje konzistentní přístup k obchodním službám, ať už jsou uživatelé připojeni prostřednictvím zásuvky ve zdi nebo se pohybují volně v rámci sítě T-mobilu. Jednotlivé profily pro řízení přístupu se vytváří v rámci jednotného managementu pro správu sítě Netsight od Extreme Networks a následně jsou distribuovány přímo do sítě, kde jsou posléze uplatňovány právě v bodu vstupu na pevném přepínači nebo v bezdrátovém přístupovém bodu. Pro účely bezpečnosti je řešení integrováno s managementem bezpečnostních informací a událostí (SIEM) pro účely monitoringu v době i po připojení.



Pro viditelnost a kontrolu zařízení v síti je zásadní, že každé zařízení má svůj jedinečný otisk a jednotlivé zjištěné atributy (na obrázku vlevo) nabízejí různé možnosti konfigurace rozdílných práv v rámci přístupu do sítě. Pomocí nich lze následně poskytnout zařízením různý přístup k síti.

Správci zodpovědní za provoz oceňují možnost jednoduchého vyhledávání konkrétního zařízení v síti a viditelnost detailů připojení (viz obrázek). Uživatel obvykle nezná IP nebo MAC adresu svého zařízení. Telefonní číslo či jméno ano, a tak lze okamžitě podle těchto atributů dohledat lokaci a řešit daný problém se zařízením.

Důležitou součástí řešení jsou reporty. Ty je možné aktivovat při připojení nového zařízení nebo změně jeho stavu, registraci hosta, jakékoliv změně v údajích o koncovém zařízení či uživateli a jeho bezpečnostním stavu. Oznámení je realizováno prostřednictvím trapů, zpráv syslog, e-mailu nebo webové služby. Systém má schopnost spuštění programu po oznámení události. Například pokud je integrováno s helpdeskem aplikací, pomocí NAC oznámení lze automaticky mapovat změny v oblasti infrastruktury na konkrétní akce.

Celé řešení je provozováno v redundantním provedení v režimu vysoké dostupnosti s rozložením zátěže (režim active-active).

Hlavním cílem tohoto řešení byl, je a bude spokojený uživatel. Ten oceňuje hlavně jednoduché, rychlé a spolehlivé připojení. Provozovatel T-mobile pak nejvíce oceňuje ekonomické stránky řešení, kterými jsou hlavně viditelnost, kontrola a bezpečnost díky jednotné správě a možnosti zachovat současnou infrastrukturu od jiného výrobce.

Další informace lze vyžádat na adrese: *czech@extremenetworks.com*