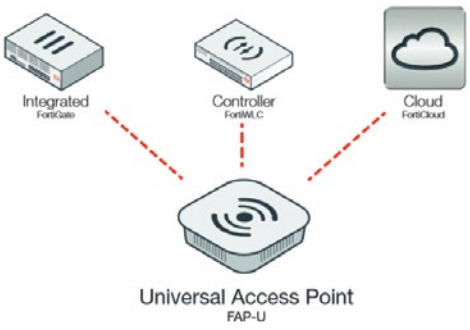
Architektúra a zabezpečenie sietí Wi-Fi

» Na podujatí TechDay´18, ktoré usporiadali spoločnosti Veracomp Slovakia a Fortinet pre svojich partnerov, nás najviac zaujal interaktívny workshop, na ktorom odborníci v skupinách riešili vybudovanie siete Wi-Fi a jej zabezpečenie pre rôzne objekty a scenáre (kancelárske priestory firmy, maloobchodnú prevádzku, konferenčné centrum, školu či nemocnicu) s využitím komponentov Fortinet.

Každý z týchto objektov si vzhľadom na špecifiká vyžaduje iný typ, počet a rozmiestnenie prístupových bodov.

Scenár 1: **Konferenčné centrum**

Napríklad v konferenčnom centre sa na malej ploche pripája veľký počet účastníkov, ale len jednorazovo počas konkrétneho podujatia. Počet zamestnancov, ktorí sa pripájajú pravidelne, je naproti tomu malý. Infraštruktúra teda musí byť navrhnutá tak, aby zvládla predpokladaný počet návštevníkov a pripájanie bolo jednoduché. Pri rozmiestňovaní väčšieho počtu prístupových bodov určených na scenáre s veľkým počtom prihlásených používateľov treba prihliadať na pokrytie celého priestoru tak, aby sa zariadenia navzájom nerušili. Typ a počet prístupových bodov, ako napríklad FortiAP, sa vyberá podľa veľkosti objektu a maximálneho predpokladaného počtu návštevníkov. Bežný scenár zabezpečenia predpokladá security controller a minimálne dve SSID - jedno pre návštevníkov, ktorí budú mať prístup len k internetu, prípadne ak to námet konferencie vyžaduje, tak do sietí na demá a praktické cvičenia, a druhé pre prednášajúcich, aby mali k dispozícii potrebnú kvalitu a rýchlosť pripojenia. Nielen na IT, ale aj na podnikateľských konferenciách sa totiž najčastejšie prezentujú ukážky vyžadujúce pripojenie ku cloudovým službám.



Scenár 2: **Firma**

Iný typický scenár je presťahovanie firmy do nových priestorov, v ktorých treba vytvoriť infraštruktúru bezdrôtovej siete. Na rozdiel od kongresového centra sa predpokladá, že väčšinu budú tvoriť pripojení kmeňoví, prípadne externí zamestnanci a občas sa pripoja návštevníci, napríklad obchodní partneri, spravidla v presne lokalizovanej oblasti, teda na recepcii a v zasadacích miestnostiach. Priorita pri takomto scenári je stabilita a bezpečnosť pripojenia a garantovaná šírka pásma. Tá bude iná pre firmu pracujúcu s bežnými dokumentmi a agendou a iná pre firmy, ktorých zamestnanci intenzívne pracujú s multimédiami. Samozrejme, požiadavky na úroveň zabezpečenia sa budú odvíjať od predmetu podnikania – či treba chrániť citlivé, prípadne osobné údaje a podobne. Dôležitú úlohu pri projekte zabezpečenia a riadenia politiky prístupu k sieti hrá aj typ architektúry, teda či firma využíva interné servery a úložiská, alebo cloudové služby, prípadne hybridnú infraštruktúru. Vo firemnej sieti treba prioritne riešiť spoľahlivú autentifikáciu používateľov. V súčasnej ére BYOD a práce z domu, prípadne odkiaľkoľvek a zo širokej palety zariadení vrátane smartfónov a tabletov už WPA2 pre firemné prostredie nestačí, štandardne sa využíva dvojfaktorová autentifikácia. Preto súčasťou siete musia byť príslušné zariadenia, napríklad FortiAuthenticator.

Aby bolo pripojenie k firemnej IT infraštruktúre pre správcov na jednej strane a zamestnancov na druhej strane jednoducho použiteľné, treba využiť overovanie na báze protokolu 802.1X a už spomínaný FortiAuthenticator. To umožní zamestnancom pripájať sa nielen z firemných zariadení, ale aj zo súkromných zariadení, ktoré si prinesú do práce, pričom je vynútené dodržiavanie zásad bezpečnosti a firemných politík vrátane nevyhnutnosti inštalácie aktualizácií a opravných balíčkov aj na súkromné zariadenia, ktoré nie sú v správe firmy.

Scenár 3: **Škola**

Internetové pripojenie v školách má špecifické požiadavky na limitovanie prístupu k internetovým stránkam, ktorých obsah nie je pre žiakov vhodný. V mnohých školách je pripájanie zariadení žiakov limitované aj časovým rozvrhom. Tieto špecifické funkcie je potrebné jednoducho nastavovať. Cez vyučovacie hodiny je zablokované a žiaci sa môžu pripájať k internetu iba cez prestávky. K ďalším špecifikám škôl patria limitované možnosti, čo sa týka rozpočtu nielen na zriadenie, ale aj na správu. Podobne ako v kongresovom centre aj v objekte školy treba nadimenzovať dostatočný počet prístupových bodov. Výhodou je síce väčší, ale limitovaný počet používateľov, ktorí sa pripájajú každý deň. Kľúčový prvok je centrálny kontrolér, napríklad Fortinet Wireless Controller, ktorý riadi politiky prístupu do siete. Do popredia vystupuje aj požiadavka autentifikácie, napr. cez FortiAuthenticator.

Scenár 4: **Hotel a penzión**

Veľmi variabilná je architektúra pripojenia Wi-Fi v ubytovacích zariadeniach – hoteloch a penziónoch. Úroveň zabezpečenia závisí od požiadaviek prevádzkovateľa. Predpokladá sa, že ubytovaní hostia budú navštevovať rôzne stránky podľa ich osobných preferencií, sťahovať a inštalovať aplikácie z rôznych (aj neoverených) zdrojov, ľudia na služobných cestách sa budú pripájať k sieťam VPN, mnohí budú využívať internetbanking a nie je vylúčené, že niektorí hostia využijú anonymné pripojenie aj na menej seriózne, ba až nekalé aktivity. Existuje viac filozofií konfigurácie a zabezpečenia pripojenia, počnúc prístupovými bodmi bez centrálnej správy. Prevádzkovateľ zariadenia s takouto sieťou Wi-Fi si však neuvedomuje potenciálne riziká.

Napríklad ak niekto odošle výhražný e-mail a podobne, nebude sa dať identifikovať, kto bol vtedy pripojený a túto aktivitu urobil. Zodpovední prevádzkovatelia ubytovacích zariadení budú síce preferovať, aby pripojenie do siete bolo zákaznícky prívetivé, no zároveň aj dostatočne zabezpečené, aby sa pripojenie nedalo zneužiť. Aplikujú sa pravidlá na overenie používateľov. Najviac sa osvedčilo poskytnúť hosťovi pri príchode jednorazové prístupové parametre na celý čas jeho pobytu. Používateľ je takto jednoznačne identifikovaný a sú na neho aplikované nastavené politiky, čo na danej sieti môže robiť, aké protokoly môže používať. Kľúčový prvok takejto siete je centrálny kontrolér Fortinet Wireless Controller.

Podobné odporúčania ako pre hotel platia aj pre rodinné penzióny. Na pokrytie 8 – 10 izieb na dvoch poschodiach stačia v priemere štyri prístupové body s integrovanými bezpečnostnými funkciami a firewall kontrolujúci prístup k internetovým stránkam a službám. Na tento scenár je ideálna správa sieťovej infraštruktúry z cloudu. Správa z cloudu, napríklad cez FortiCloud, poskytuje prakticky rovnaké možnosti ako in house riešenia, samozrejme, zákazník musí dôverovať tretej strane, ktorá cloudovú službu správy siete poskytuje.

Výhodné je, že zákazník ušetrí investičné prostriedky, pretože nemusí nakupovať technológie a starať sa o ich fungovanie. Za poskytovanie služby platí na mesačnej báze podľa toho, ako dlho ju potrebuje. Výhodné je aj jednoduché škálovanie. Možnosťou predovšetkým pre menšie firmy s predmetom podnikania mimo IT je aj outsourcovanie správy sieťovej infraštruktúry, no táto možnosť sa u nás zatiaľ veľmi nevyužíva.

» ĽUBOSLAV **LACKO**