Popis subscriptions pro firewally Palo Alto Networks

Licencování Palo Alto Networks je založeno na využití tzv. předplatných (subscriptions). Předplatné je časově omezená licence rozšiřující základní vlastnosti firewallu nové generace.

Typy předplatných jsou následující:

- Threat Prevention
- URL Filtering
- Wildfire
- GlobalProtect
- DNS Security

Předplatné se zpravidla zakupuje na stejně dlouhou dobu jako maintenance k hardwaru. Bližší popis jednotlivých subscription:

Threat Prevention (TP)

Zakoupením předplatného TP je funkce firewallu nové generace rozšířena o pokročilou ochranu na úrovni síťových signatur. Firewall sleduje obsah datových paketů a jakmile zaznamená vzorek provozu, který odpovídá signatuře, může na toto zjištění reagovat jednou z definovaných akcí.

TP umožňuje aktivovat následující funkce firewallu nové generace:

- Antivirus
- Anti-spyware (command-and-control)
- Vulnerability protection (Intrusion Prevention Systém)
- Externí dynamické listy obsahující seznamy škodlivých IP adres a domén užívaných pro komunikaci známým malwarem
- Možnost odesílat spustitelné soubory pro MS Windows ke kontrole do sandboxového prostředí Wildfire

URL Filtering

Předplatné URL filtering umožňuje firewallu kontrolovat URL (Uniform Resource Locator) získané ze síťového provozu oproti cloudové databázi PAN-DB. Na základě této kontroly je možné získat o URL řadu informací, jakými jsou např. risk či kategorie, které lze dále uplatnit při tvorbě bezpečnostních politik. Řazení neznámých URL do kategorií probíhá v reálném čase na úrovni strojového učení a je tak velice rychle možné detekovat nově vzniklé stránky typu Phishing, Command-and-Control apod.

Wildfire

Wildfire je cloudová služba společnosti Palo Alto Networks, určená pro analýzu neznámých vzorků spustitelných souborů. Oproti základní funkcionalitě dostupné v předplatném TP, toto předplatné přidává následující funkce:

- Možnost stáhnout signatury automaticky generované systémem Wildfire okamžitě po jejich zveřejnění (zpravidla do pěti minut po detekci neznámého zero-day útoku)
- Možnost odeslat ke kontrole více typů souborů – kromě běžných spustitelných souborů se jedná i o linky obsažené v emailových zprávách, Android application package (APK), Adobe Flash, Java Archive (JAR), Microsoft Office, Portable document format (PDF), Mac OS X files, Linux (ELF), archivy (RAR and 7-Zip), scripty (JS, VBS, PS1 a Shell scripty)
- Možnost využít Wildfire API
- Možnost využít on-premise řešení Wildfire (nutno pořídit separátní appliance)

GlobalProtect

GlobalProtect je produkt společnosti Palo Alto Networks používaný primárně pro vzdálený přístup (remote-access VPN). Bez nutnosti zakoupit licenci je kdispozici neomezená funkcionalita site-to-site VPN a základní funkcionalita remote-access VPN pro klienty Windows a Mac OSX.

Předplatné GlobalProtect přináší navíc následující funkce:

- Podpora VPN klienta pro systémy Linux, iOS, Android, Chrome OS a Windows 10 UWP
- Podpora pro provedení posture analýzy – tedy kontroly stavu připojovaného koncového bodu, např. verze a aktualizací OS, zapnutí lokálního FW, přítomnost antivirového systému apod.
- Client-less VPN – podpora spuštění portálu pro publikaci webových aplikací bez nutnosti instalace VPN klienta na koncovém bodu

DNS Security

Služba DNS je pro útočníky široce otevřená. Služba DNS Security používá prediktivní analýzu, strojové učení a automatizaci k blokování útoků, které používají službu DNS. Těsná integrace s firewallem nové generace poskytuje automatickou ochranu a eliminuje potřebu nezávislých nástrojů. Služba umožňuje rychle předvídat a předcházet škodlivým doménám, neutralizovat hrozby skryté v tunelování DNS a používat automatizaci pro rychlé vyhledání a uložení infikovaných zařízení.