Atman MACSec

Wstęp

Do niedawna większość przedsiębiorstw koncentrowała swoje polityki bezpieczeństwa głównie na budowaniu zabezpieczeń chroniących przed atakami pochodzącymi z zewnątrz sieci i je neutralizujących. Dzisiejsze dynamicznie zmieniające się środowisko korporacyjne wymaga modyfikacji podejścia do kwestii bezpieczeństwa i uwzględnienia zagrożeń pochodzących z wewnątrz organizacji, jak naruszenia poufności danych i prywatności. W miarę rozszerzania dostępu do sieci na konsultantów, podwykonawców czy gości, zagwarantowanie bezpieczeństwa sieci za zewnętrznymi zaporami ogniowymi stało się priorytetem w różnego typu organizacjach – również instytucjach publicznych.

W tej sytuacji najbardziej odpowiednim rozwiązaniem jest zastosowanie zabezpieczenia opartego na szyfrowaniu end-to-end w całej sieci, jakiego jak usługa Atman MACSec. Gwarantuje ona oczekiwany poziom bezpieczeństwa transmisji, w przeciwieństwie do zabezpieczeń wdrażanych osobno dla poszczególnych aplikacji. Usługa bazuje na MACSec − standardzie IEEE 802, który określa sposób szyfrowania w warstwie drugiej, pozwalający zabezpieczyć łącza za zewnętrznymi zaporami ogniowymi, np. pomiędzy dwoma oddziałami jednego przedsiębiorstwa.

Korzyści

Każdy dłuższy przestój może unieruchomić firmę i zagrozić jej istnieniu. Stąd potrzeba korzystania z usług, które gwarantują bezpieczeństwo danym, aplikacjom i samej sieci. Jedną z takich właśnie usług jest MACSec, który zapobiega uszkodzeniom sieci Ethernet i chroni zainstalowane w niej urządzenia LAN przed różnego rodzaju niebezpieczeństwami.

ATM S.A., ul. Grochowska 21a, 04-186 Warszawa
tel. 22 51 56 100, info@atman.pl

www.atman.pl

Opis techniczny usługi Atman MACSec

Model usługi

Usługa polega na dostarczeniu szyfrowanego end-to-end łącza transmisji danych warstwy drugiej poprzez zapewnienie wymiany kluczy i umożliwienie wzajemnego uwierzytelniania węzłów, które chcą wziąć udział w skojarzeniu łączności MACSec. Realizacja usługi obejmuje instalacje w docelowych lokalizacjach przełączników sieciowych wspierających MACSec, a ochrona obejmuje nie tylko ruch IP, ale szyfrowanie również wszystkich nagłówków protokołów warstwy 2. modelu OSI.

Komponenty rozwiązania

Usługa świadczona jest w oparciu o rozwiązania sprzętowe renomowanych producentów (Cisco, Extreme Networks, Huawei) dobierane wg specyfikacji wymagań klienta.

- Usługa transmisji danych zapewniająca połączenie między lokalizacjami
- Przełączniki wspierające szyfrowanie MACSec, udostępniane klientowi na wyłączność
- Utrzymywanie, konfiguracja urządzeń zgodnie z aktualnymi zaleceniami producenta

Parametry usługi

- Interfejsy 1G lub 10G w zależności od indywidualnych potrzeb klienta
- Urządzenia 24- lub 48-portowe w standardzie, dzięki czemu klient może podłączyć nawet kilkadziesiąt stacji końcowych
- Szyfrowanie end-to-end za pomocą 128- lub 256-bitowych kluczy daje gwarancję najwyższego bezpieczeństwa danych
- Dynamiczna zmiana kluczy szyfrujących odbywa się w interwałach nawet co 1 minutę bez utraty ciągłości transmisji
- W przypadku braku możliwości zestawienia szyfrowanej sesji połączenie jest natychmiast zrywane, dzięki czemu dane nigdy nie będą przesyłane w sposób nieszyfrowany

Zasada działania

Usługa Atman MACSec świadczona jest w oparciu o parę przełączników obsługujących standard 802.1AE. Znajdują się one w lokalizacjach końcowych, do których dostarczana jest usługa. Ich konfiguracja wykorzystuje protokół MKA na interfejsach WAN/uplinkowych. Urządzenia uwierzytelniają się wzajemnie za pomocą klucza PSK, który jest identyczny i wyłączny dla obydwu urządzeń. Po poprawnym uwierzytelnieniu przełączniki przechodzą do negocjacji klucza sesji SAK. Jedno z urządzeń jest jednocześnie serwerem klucza SAK i odpowiada za zmiany klucza sesji po upływie skonfigurowanego czasu życia sesji (np. co 1 godzinę).

Nagłówek MACSecowy „secTag" składa się z 16 bajtów i dokładany jest za „source mac" w ramce ethernetowej. To znacząco poprawia jego wydajność w stosunku do protokołu IPsec, zachowując jednocześnie najwyższe bezpieczeństwo przesyłanych danych. Dla porównania, protokół IPsec dokłada nawet 57 bajtów nagłówka, przez co znacząco wpływa na realną wydajność łącza. Ta niewątpliwa zaleta czyni MACsec protokołem niezwykle szybkim. W przypadku gdy z jakiegoś powodu klucz sesji nie zostanie wynegocjowany, urządzenia bezzwłocznie zaprzestają transmisji danych, dbając o to, aby nie zostały przesłane w sposób jawny.

Wybierając usługę Atman MACSec, klient jest w bardzo komfortowej sytuacji − usługa zdejmuje konieczność posiadania własnego sprzętu sieciowego obsługującego szyfrowanie. Przełączniki dostarczone przez Atman mają wystarczającą liczbę portów, aby podłączyć niezbędne urządzenia końcowe.

Dzięki ogromnej wydajności technologii, MACSec jest w stanie zaszyfrować cały ruch, jaki przychodzi do urządzenia. Jedynym ograniczeniem jest przepustowość portu.