Co siedzi w chmurce?

czyli technologie sieciowe wykorzystywane w systemach CCTV

Cz. 2. Bezpieczeństwo

Tomasz Żuk

Akademia CCTV IP

W pierwszej części tego cyklu (sa 5/2013) opisałem kilka podstawowych sposobów na zwiększenie przepustowości sieci. Tym razem chciałbym poruszyć drugi, nie mniej ważny temat, jakim jest bezpieczeństwo. Ma ono kolosalne znaczenie przy budowie sieci IP, zwłaszcza obsługujących systemy zabezpieczeń, w tym CCTV IP. Rozszyfrowując akronim CCTV (*Closed Circuit Television*, czyli w dosłownym tłumaczeniu telewizja w obwodzie zamkniętym), zauważymy pewien paradoks – systemy zamknięte są oparte na sieci IP, czyli środowisku z definicji otwartym. Zatem chcąc zapewnić odpowiedni poziom bezpieczeństwa, należy najpierw zadbać o „zamkniętość" sieci IP. Można to osiągnąć, stosując dobrej klasy przełączniki oferujące wiele funkcji.

SIECI WIRTUALNE VLAN

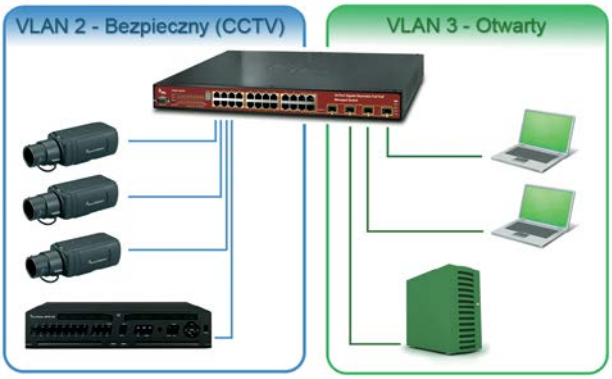
O sieciach wirtualnych VLAN *(Virtual Local Area Network)* pisałem w poprzednim artykule w kontekście ich wykorzystania do zarządzania ruchem, dzielenia infrastruktury sieciowej na odseparowane od siebie domeny rozgłoszeniowe i zwiększania wydajności przełączników. Teraz skupię się na możliwościach wykorzystania VLAN do podniesienia poziomu bezpieczeństwa instalacji CCTV.

Wirtualna sieć VLAN jest logiczną podsiecią utworzoną z wybranych urządzeń (portów/stacji roboczych – w naszym przypadku kamer/rejestratorów/stacji graficznych), które mogą się komunikować jedynie w obrębie danej podsieci, czyli tylko z urządzeniami należącymi do wspólnego VLAN. Mówiąc inaczej, jedynie urządzenia należące do wspólnej podsieci VLAN „widzą się wzajemnie" i mogą wymieniać pomiędzy sobą informacje.

Oczywiście można przesyłać informacje także pomiędzy różnymi sieciami VLAN, ale do tego potrzebny jest router, a więc urządzenie realizujące wymianę ruchu w warstwie trzeciej, do której nie mają dostępu zarządzalne przełączniki sieciowe.

Korzystając z możliwości oferowanych przez VLAN, można utworzyć grupę urządzeń CCTV, do której będą należeć kamery, rejestratory oraz komputery z oprogramowaniem do monitoringu wizyjnego, i dodać je do wspólnego VLAN. W ten sposób pozostałe urządzenia, które nie należą do utworzonej wirtualnej podsieci, nie będą miały dostępu do przesyłanych danych, a więc nie będą mogły w sposób nieuprawniony podsłuchiwać transmisji.

Dodawanie poszczególnych urządzeń do odpowiadających im podsieci VLAN odbywa się na poziomie konfiguracji portu przełączników. Dlatego, aby unikać niebezpieczeństwa podsłuchu, wszystkie porty, które nie są wykorzystywane do podłączenia urządzeń CCTV, należy albo dodać do innego VLAN, albo wyłączyć.



Rys. 1. Sieci wirtualne VLAN

Trzeba oczywiście w tym momencie pamiętać, aby pozostawić port „administracyjny" – a więc taki, który ma dostęp do wskazanego VLAN w celach diagnostycznych – do którego dostęp fizyczny musi być chroniony.

Uwaga praktyczna. Konfigurując VLAN do obsługi urządzeń CCTV powinno się skonfigurować VLAN o identyfikatorze innym niż 1, ponieważ jest on powszechnie wykorzystywany jako VLAN fabryczny (ustawiany domyślnie dla wszystkich portów), ma więc pewne szczególne właściwości i funkcje, np. w przełącznikach IFS nie można zmienić ustawień domyślnego VLAN ani go usunąć. Większość przełączników wykorzystuje także VLAN 1 do obsługi protokołu STP *(Spanning Tree Protocol).*

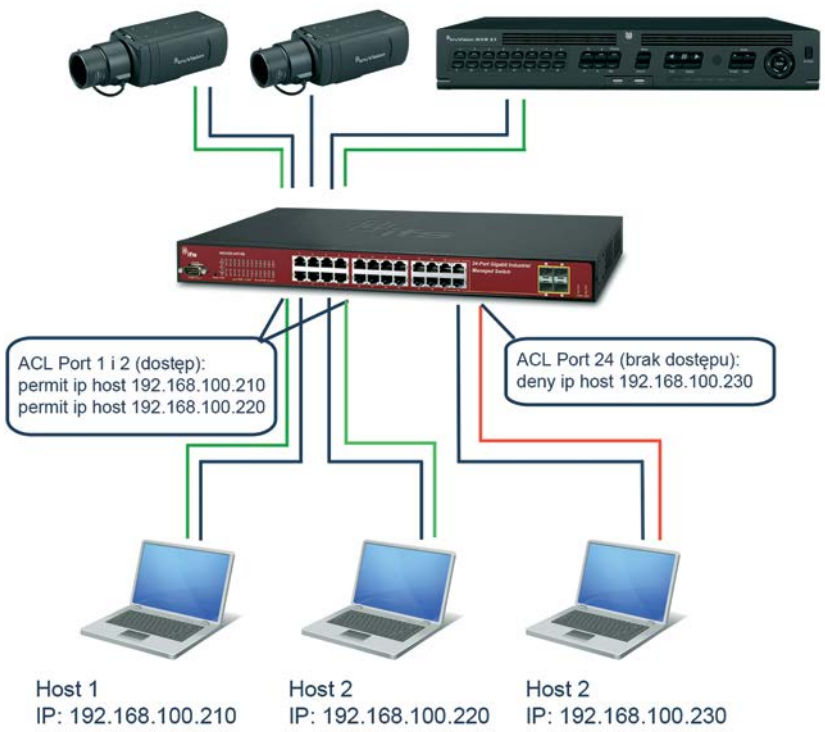
Powszechnie rekomenduje się budowanie niezależnych sieci IP dedykowanych do pracy z systemami CCTV IP, do których nie są podłączane żadne inne urządzenia (komputery, serwery itp.). Założenie to nie wyklucza koncepcji sieci wirtualnych, więcej – wzajemnie się one uzupełniają. Budując bowiem fizyczne sieci dedykowane, również jesteśmy potencjalnie narażeni na próby podłączenia innych, nieautoryzowanych urządzeń.
Korzystając z sieci wirtualnych, nawet jeżeli dojdzie do nieautoryzowanego podłączenia jakiegoś urządzenia do istniejącej infrastruktury, przy poprawnej konfiguracji będzie ono i tak wpięte do innego VLAN. A więc pomimo fizycznego połączenia wciąż nie będzie miało dostępu do urządzeń i danych CCTV.

LISTY DOSTĘPOWE ACL

Kolejnym mechanizmem, który chętnie wykorzystują administratorzy sieci do zapewnienia odpowiedniego poziomu bezpieczeństwa poprzez filtrowanie ruchu, są listy dostępowe ACL *(Access Control List)*. Ogólna zasada ich działania polega na utworzeniu grupy reguł opisujących sposób obsługi ruchu pochodzącego od pojedynczego użytkownika czy grupy użytkowników i przypisania tych reguł do poszczególnych portów w przełączniku.
Każdy pakiet przychodzący do interfejsu przełącznika jest sprawdzany pod kątem zgodności z poszczególnymi regułami, począwszy od pierwszej, skończywszy na ostatniej. Pierwsza reguła, która będzie spełniona, zostanie wykonana. Oznacza to, że odebrany pakiet zostanie zgodnie z zapisem reguły przesłany dalej *(permit)* lub odrzucony *(deny)*, a dalsze sprawdzanie listy zostanie przerwane.
Implementacja list dostępowych może przyjmować skomplikowane formy, szczególnie w sytuacji gdy są one priorytetyzowane pod kątem obsługi różnego rodzaju ruchu sieciowego. W ogólności listy dostępowe służą do zarządzania ruchem przychodzącym do przełącznika i z zasady działania przypominają zaporę ogniową *(firewall)*.
Każda z list ACL w zależności od producenta może zawierać od kilkudziesięciu do nawet kilkuset reguł *(ACE – Access Control Entry)*, niektóre przełączniki mają ograniczenia dotyczące ogólnej liczby reguł dostępnych w urządzeniu.
Każda z zapisanych na liście ACL reguł może odnosić się do wielu szczegółów przesyłanego pakietu. Najczęściej do tworzenia reguł filtrowania ruchu wykorzystuje się następujące elementy:

- numer IP (numer hosta, zakres numerów hostów, numer całej podsieci itd.),
- typ przesyłanej ramki (ARP, Ethernet, IPv4 itd.),
- rodzaj transmisji (multicast, broadcast, unicast),
- adres sprzętowy MAC,
- numer VLAN,
- rodzaj protokołu (ICMP, UDP, TCP itp.).

Rys. 2. Listy dostępowe ACL



Listy ACL (typu podstawowego i rozszerzonego) są wykorzystywane nie tylko w przypadku przełączników. Są także stosowane do tworzenia reguł filtrujących ruch sieciowy w innych urządzeniach sieciowych, np. routerach firmy Cisco.

UWIERZYTELNIANIE

W przełącznikach zarządzalnych stosuje się wiele metod mających na celu uwierzytelnienie użytkowników lub urządzeń (sprawdzenie, z kim lub czym przełącznik ma do czynienia), zanim umożliwi się im nawiązanie komunikacji z innymi użytkownikami lub hostami. Powszechnym rozwiązaniem jest stosowanie protokołu 802.1x, który zapewnia bezpieczne i scentralizowane uwierzytelnianie użytkowników i urządzeń.
Zasada działania protokołu 802.1x polega na wymianie informacji uwierzytelniających pomiędzy urządzeniem, które zostało podłączone do przełącznika zwanego suplikantem *(supplicant)* a dedykowanym zewnętrznym serwerem uwierzytelniającym *(authentication server)*. Funkcję serwera uwierzytelniającego może pełnić np. serwer RADIUS *(Remote Authentication Dial In User Service)*. Po podłączeniu do portu przełącznika nowego urządzenia przełącznik blokuje wszelki ruch do tego urządzenia, oprócz ruchu umożliwiającego uwierzytelnienie. Dopiero po poprawnym potwierdzeniu tożsamości urządzenia przez serwer uwierzytelniający następuje zezwolenie na dostęp do zasobów.

Istnieje wiele implementacji wykorzystujących protokół 802.1x, które są stosowane w zarządzalnych przełącznikach sieciowych. Są to między innymi:

- Uwierzytelnianie oparte na portach *(Port-Based Authentication)* – w tym trybie przełącznik, z punktu widzenia komuni-

kacji, jest praktycznie przeźroczysty dla uwierzytelniających się urządzeń. Jego rolą jest jedynie odbieranie od urządzenia żądającego uwierzytelnienia specjalnych pakietów EAPOL *(Extensible Authentication Protocol over LAN),* uzupełnienie ich o dodatkowe informacje (takie jak numer portu, na którym jest podłączone urządzenie, czy adres IP przełącznika) i przesyłanie ich dalej do serwera uwierzytelniającego w formie pakietów RADIUS. Po otrzymaniu odpowiedzi od serwera przełącznik zmienia format ramki z RADIUS na EAPOL i odsyła do urządzenia, a w przypadku pozytywnego uwierzytelnienia umożliwia dostęp. Przełącznik nie musi nawet wiedzieć, z jakiej metody uwierzytelniania korzystają obie strony.

Rys. 3. Uwierzytelnienie urządzenia za pomocą dodatkowego serwera (np. RADIUS)

- Uwierzytelnianie oparte na adresach MAC *(MAC-Based Authentication)* – w tym trybie, który właściwie nie jest standardem, a jedynie pewnego rodzaju dobrą praktyką zaadaptowaną i wdrożoną przez komercyjnych producentów, rolę suplikanta (urządzenia żądającego uwierzytelnienia) pełni przełącznik, który wysyła te żądania w imieniu urządzeń podłączanych do jego portów. Po podłączeniu urządzenia do portu przełącznika przechwytuje on pierwszą odebraną ramkę i odczytuje z niej adres MAC nadawcy. Ten adres wykorzystuje następnie jako login i hasło podczas autoryzacji z serwerem RADIUS. Po otrzymaniu odpowiedzi z serwera potwierdzającej uwierzytelnienie urządzenia przełącznik dodaje stosowny wpis do statycznej tablicy MAC, nadając urządzeniu uprawnienia.
- Uwierzytelnienie dostępu użytkowników *(User Authentication)* – kolejna metoda uwierzytelniania oparta na protokole 802.1x dotycząca uwierzytelnienia osób-administratorów przełączników. Możliwe jest uwierzytelnianie użytkowników, którzy logują się do przełącznika przy użyciu konsoli telnet lub klienta WWW za pomocą dedykowanego serwera RADIUS lub TACACS+ *(Terminal Access Controller Access Control System Plus).* W opisywanym przypadku serwer uwierzytelniający zawiera kompletną bazę danych użytkowników i ich haseł z przypisanymi do nich odpowiednimi poziomami dostępu. Dostęp użytkownika do panelu administracyjnego przełącznika jest możliwy jedynie wtedy, kiedy przejdzie on poprawną procedurę uwierzytelnienia.

PORT SECURITY

Port security jest rozwiązaniem stosowanym powszechnie przez wielu producentów do zabezpieczania dostępu do przełączników sieciowych poprzez utworzenie list „bezpiecznych" adresów MAC urządzeń, które mogą być podłączone do danego portu przełącznika. Przełącznik działa w taki sposób, że po odebraniu pakietu jest sprawdzany adres MAC nadawcy *(Source Address).* Jeżeli nie ma go na liście adresów bezpiecznych, nie jest dalej przesyłany.

Jednym z istotnych parametrów listy adresów MAC, który może być ustawiany przez administratorów, jest jej wielkość, czyli liczba adresów, które zawiera. W skrajnym przypadku można ograniczyć jej wielkość do jednego adresu MAC, w efekcie do danego portu może być podłączone tylko jedno bezpieczne urządzenie.

Jeżeli do portu z uruchomioną usługą *port security* zostanie podłączone nowe urządzenie, którego adres MAC nie jest umieszczony na liście adresów autoryzowanych, lub zostanie przekroczona maksymalna liczba adresów, następuje zdarzenie naruszenia bezpieczeństwa. Interfejs (port) może być skonfigurowany w taki sposób, aby w odpowiedzi na takie naruszenie podjąć jedną z następujących akcji:

- port przechodzi do trybu ograniczonego *(restricted)* polegającego na ograniczeniu przesyłania pakietów oraz wysłaniu do odpowiedniego serwera nadzorującego informacji o naruszeniu bezpieczeństwa za pomocą komendy SNMP *(Simple Network Management Protocol)*
- port zostaje natychmiast wyłączony *(error-disabled state)* i zostaje wysłane powiadomienie do serwera SNMP. W zależności od ustawienia port zostaje ponownie włączony po założonym czasie lub pozostaje wyłączony do czasu, aż włączy go ręcznie administrator.

UWAGI KOŃCOWE

Przełączniki sieciowe wywodzą się wprost ze świata IT, gdzie z definicji przykłada się dużą wagę do problemów bezpieczeństwa oraz zabezpieczenia urządzeń i systemów przed nieautoryzowaną ingerencją. Szczęśliwie dla instalatorów systemów CCTV IP przy okazji stosowania przełączników sieciowych mają oni dostęp do wielu funkcji i rozwiązań pozwalających na uzyskanie wysokiego poziomu bezpieczeństwa.

Ich konfiguracja może w pewnych aspektach być nieco czasochłonna czy skomplikowana, ale nagrodą jest spokój instalatora i użytkownika końcowego, którzy są pewni, że system jest bezpieczny i stabilny. □