Różnice między VLAN a VPN

VLAN (*Virtual Local Area Network*)

- Jedna sieć LAN zostaje podzielona logicznie na kilka sieci LAN (wirtualnych), które nadal korzystają z tego samego fizycznego switcha. Broadcast jest dostarczany tylko do maszyn z danej VLAN, a nie do wszystkich maszyn podłączonych do switcha. Można także stworzyć VLAN z maszyn podpiętych do różnych switchy.

- Można tworzyć VLAN w oparciu o grupy użytkowników (np. grupa księgowych zebrana ze wszystkich LANs), numery portów, numery MAC, protokoły.

- Składniki VLAN połączone są za pomocą przełączników (*switches*), które muszą mieć funkcje obsługi kilku podsieci. Wysyłając pakiet, oznaczają go unikalnym tagiem IEEE *802.1Q*, który odbierany będzie tylko przez określony switch a pomijany przez inne switche.

VPN (*Virtual Private Network*)

- Firmowy LAN można chronić przed dostępem z zewnątrz za pomocą firewalla. Ale co jeśli mobilni pracownicy będą musieli mieć dostęp do tej sieci?

- Stworzenie prywatnej (fizycznej) zabezpieczonej sieci łączącej filie firmy w kilku miastach – jest zbyt drogie. Lepiej wykorzystać do tego celu już istniejący Internet.

VPN (*Virtual Private Network*)

Router VPN zapewnia:

- uwierzytelnianie pakietów (czy rzeczywiście pochodzą od deklarowanego nadawcy),
- kontrolę dostępu użytkowników (login, hasło, ale także definicje zaufanych urządzeń),
- poufność pakietów (zabezpieczenie przed podsłuchaniem),
- integralność danych (zabezpieczenie przed manipulacją danych).

Router VPN zazwyczaj poprzedza firewall (odszyfrowane przez router dane trafiają dopiero do firewalla).

VPN (*Virtual Private Network*)

Router VPN stosuje do tego celu następujące protokoły:

- PPTP (*Point-to-Point Tunneling Protocol*) – polega na pakowaniu protokołu PPP do GRE (*Generic Routing Encapsulation*) i umożliwia proste uwierzytelnianie za pomocą hasła;

- L2TP (*Layer 2 Tunneling Protocol*) – umożliwia szyfrowanie połączenia za pomocą algorytmów IPSec oraz bardziej wyrafinowane uwierzytelnianie haseł (np. za pomocą serwera RADIUS);

- IPSec (*IP Security Protocol*) – umożliwia zaawansowane uwierzytelnianie oraz poufność pakietów; może być używany w trybie transportu (*host-to-host*) lub tunelu (*gateway-to-gateway*).

IPSec

Dwa tryby protokołu:

- **Transportowy** – dane użytkownika i protokół TCP są szyfrowane i pakowanie do jawnego nagłówka ESP (*Encapsulating Security Payload*) oraz IP (jawny). W tym przypadku nie wiemy, o czym jest rozmowa, ale wiemy kto z kim rozmawia;

- **Tunelowy** – szyfrowany jest cały nagłówek TCP/IP oraz dane użytkownika, które są pakowane do nagłówka ESP i nowego nagłówka IPn (*IPnew*).

Uwaga: Protokół ESP nie zawiera informacji o portach docelowych, dlatego w przypadku przepuszczania przez NAT wymagane jest zastosowanie ***NAT Traversal*** (pakowanie ESP do UDP, które rozróżnia porty; transport przebiega między portami UDP 4500 na obu końcówkach).

IPSec

Aby umożliwić połączenie dwóch sieci będących za NAT, należy przekierować porty na interfejsie WAN:

Administracja przez http: **8291**/tcp-udp na **8291**/tcp-udp

IKE: **500**/tcp na **500**/udp

NAT-Traversal: **4500**/udp na **4500**/udp

IPSec Passthrough

Rozwiązanie umożliwiające połączenie dwóch VPN będących za NAT. Nie jest wymagane tutaj przekierowywanie portów, ruch odbywa się automatycznie.

Technologia ta jest alternatywą wobec *NAT Traversal* (funkcje te mogą jednak występować jednocześnie, gdyż na siebie nie wpływają).

IPSec przez DMZ

Zamiast przekierowania portów przez NAT, można komputer z usługą IPSec wystawić na nadrzędnym routerze w DMZ (***D****e****M****ilitarized* ***Z****one*).

Podsumowanie

- **VLAN** – sieć lokalna (LAN) podzielona jest na mniejsze wydzielone części w celu lepszego zarządzania nimi.

- **VPN** - umożliwia połączenie się z LAN będąc poza tą siecią (zazwyczaj poprzez Internet).