T: Sieci wirtualne.

Cel ogólny lekcji: Zapoznanie uczniów z pojęciem VPN (Wirtualna Sieć Prywatna) oraz zasadami działania, możliwościami i zastosowaniami tej technologii. Poznanie najczęściej spotykanych rodzajów VPN oraz zrozumienie, w jaki sposób działają i jakie oferują poziomy bezpieczeństwa.

Cele szczegółowe:

1. Wytłumaczenie, czym jest VPN oraz jakie są różnice między siecią prywatną a siecią VPN.
2. Omówienie korzyści i wad stosowania VPN oraz sytuacji, w których korzystanie z tej technologii jest najbardziej opłacalne.
3. Zaprezentowanie sposobów działania tunelowania VPN oraz podziału sieci VPN w zależności od różnych czynników.
4. Przedstawienie zagrożeń związanych z wykorzystywaniem VPN oraz sposobów zapobiegania blokowaniu połączeń VPN.
5. Wskazanie zastosowań VPN w firmach i organizacjach oraz w codziennym życiu, w tym możliwości telepracy. Uczeń będzie w stanie określić czym jest protokół PPTP oraz jakie ma wady i zalety w stosowaniu w sieciach prywatnych.
6. Uczeń zrozumie, w jaki sposób konfigurować tunel VPN za pomocą protokołu PPTP i jakie dane uwierzytelniające są potrzebne do nawiązania połączenia.
7. Uczeń pozna alternatywne protokoły VPN, takie jak IPSec i OpenVPN, i zrozumie, dlaczego są one bardziej zalecane do stosowania w środowiskach wymagających wysokiego poziomu bezpieczeństwa.
8. Uczeń pozna protokół L2TP i zrozumie, w jaki sposób działa na poziomie łącza danych oraz jakie oferuje funkcjonalności i poziomy bezpieczeństwa.
9. Uczeń zrozumie, jakie konfiguracje są wymagane na urządzeniach sieciowych do poprawnego działania protokołu L2TP oraz jakie ustawienia protokołu IPsec są potrzebne.
10. Wyjaśnienie czym jest protokół SSTP i w jaki sposób działa.
11. Przedstawienie zalet i wad sieci VPN.
12. Omówienie celów tworzenia sieci VPN.
13. Przedstawienie wymagań wdrożenia protokołu SSTP.
14. Zwrócenie uwagi na zagrożenia związane z używaniem sieci VPN oraz sposoby ich minimalizacji.

Wproeadzenie:

VPN (ang. Virtual Private Network, Wirtualna Sieć Prywatna) - tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów.
Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa.

Według podręcznika Administrowanie Windows Server 2008 R2. Training Kit sieci VPN (Virtual Private Network) to rozszerzenie sieci prywatnej obejmujące zaszyfrowane i uwierzytelnione łącza kapsułkowane w sieciach publicznych lub udostępnionych.

A. Ewolucja sieci komputerowych

Początkowo istniały pojedyncze komputery, następnie tworzono małe sieci lokalne LAN, kiedy to rozwiązanie okazało się być niewystarczające zaczęto tworzyć sieci WAN. Koszty takiego rozwiązania są duże i nie wszystkie firmy i użytkownicy prywatni mogą je stosować.
VPN nie wymaga budowy dodatkowej sieci, kupowania specjalistycznych urządzeń czy dzierżawy łącz. Cały ruch i tworzenie takiej sieci odbywają się przy pomocy Internetu, więc jedynym wymaganiem jest dobre połączenie internetowe oraz dwa odpowiednio skonfigurowane komputery.

Określenie „wirtualna” oznacza, że sieć ta istnieje jedynie jako struktura logiczna działająca w rzeczywistości w ramach sieci publicznej, w odróżnieniu od sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łącz. Stacje końcowe mogą korzystać z VPN dokładnie tak, jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne.

Rozwiązania oparte na VPN stosowane są np. w sieciach korporacyjnych firm, których zdalni użytkownicy pracują ze swoich domów na niezabezpieczonych łączach.
Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki

kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie). Rozwiązanie to sprawdza się w firmach, których pracownicy często podróżują lub korzystają z możliwości telepracy.

Tunelowanie VPN jest wykorzystywane do ochrony przed monitorowaniem ruchu sieciowego przez agendy rządowe. Pozwala w sposób bezpieczny komunikować się z krajów z silną cenzurą (np. Chiny, Iran), a także w przypadku transmisji obarczonej ryzykiem prawnym (np. współdzielenie plików). Istnieją techniki blokowania połączeń VPN.

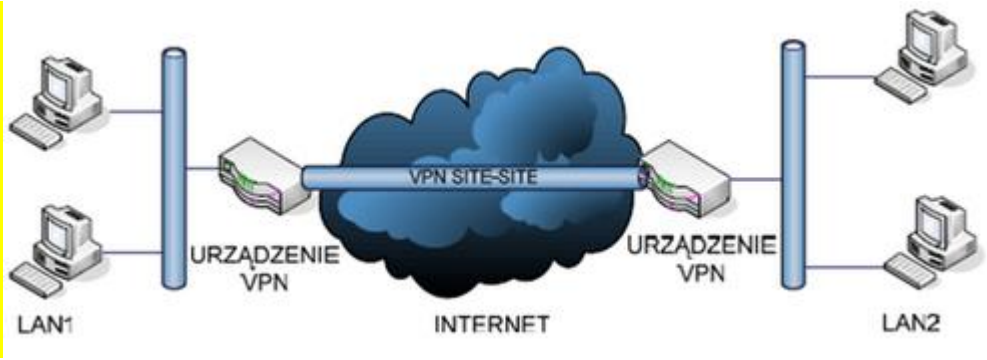
Sieci VPN możemy podzielić w zależności od:

- protokołów użytych w procesie tunelowania ruchu sieciowego,
- punktu końcowego tunelowania, może być nim na przykład sam klient, bądź dostarczyciel Internetu,
- dostępu punkt-punkt lub zdalnego dostępu,
- dostarczanych poziomów bezpieczeństwa,
- wykorzystywanej warstwy modelu OSI łączonej sieci, takiej jak połączenia w warstwie 2, bądź łączności warstwy 3.

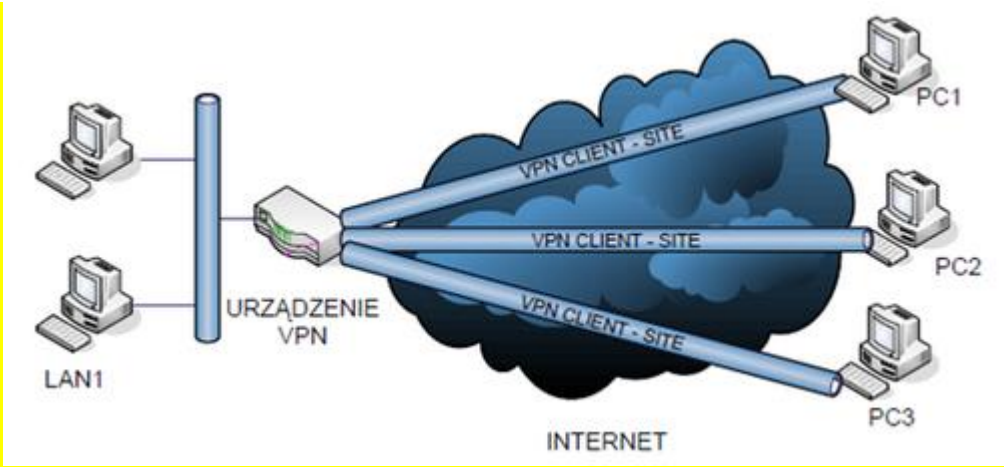
Działanie VPN według podręcznika Administrowanie Windows Server 2008 R2. Training Kit. Komputer kliencki łączy się do sieci publicznej, na przykład do Internetu, i inicjuje połączenie VPN do serwera zdalnego. Ten serwer zdalny zwykle znajduje się w podsieci brzegowej organizacji, z którą komputer kliencki próbuje uzyskać połączenie. Po wykonaniu połączenia tworzony jest zaszyfrowany tunel pomiędzy komputerem klienckim a serwerem VPN. Ten zaszyfrowany tunel przenosi ruch sieci lokalnej pomiędzy komputerem klienckim a siecią zdalną, do której komputer się połączył. Maszyny klienckie łączą się z siecią w ten sam sposób, co podczas ich fizycznej obecności w biurze. Zamiast kabla CAT-5 połączonego ze przełącznikiem w biurze, kabel wirtualny w formie tunelu VPN łączy je z infrastrukturą sieci organizacyjnej.

B. Topologie sieci VPN:

- Site-Site - kanał VPN zestawiany między dwoma, odległymi fizycznie, sieciami LAN. Urządzeniem VPN może być serwer firmowy lub odpowiednio skonfigurowany router z obsługą sieci VPN.



- Client-Site - kanał VPN zestawiany między komputerem PC zdalnego użytkownika, a odległą siecią LAN.



a) Protokoły uwierzytelniające używane przez serwer Windows Server 2008 do uwierzytelniania przychodzących połączeń VPN. Lista uporządkowana jest w kolejności od najlepiej do najgorzej zabezpieczonych:

- Protokół EAP-TLS (Extensible Authentication Protocol-Transport Level Security jest wdrażany, jeśli klienci sieci VPN mogą uwierzytelniać się przy pomocy kart inteligentnych lub certyfikatów cyfrowych. Protokół EAP-TLS nie jest obsługiwany przez pojedyncze serwery i może być wdrożony tylko wtedy, gdy serwer będący hostem usługi roli Remote Access Service należy do domeny Active Directory.

- Protokół MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol) zapewnia wzajemne uwierzytelnienie i pozwala na szyfrowanie danych uwierzytelniających i danych połączenia. Protokół MS-CHAPv2 jest domyślnie włączony w systemie Windows Server 2008.

- Protokół CHAP (Challenge Handshake Authentication Protocol) jest to starsza metoda uwierzytelniania szyfrująca dane uwierzytelniające za pomocą hasha MD5. Protokół CHAP nie

obsługuje szyfrowania danych i jest najczęściej używany w celu zapewnienia kompatybilności ze starszymi klientami innych producentów (nie firmy Micmsoft).

- Protokół EAP-MD5 CHAP (Extensible Authentication Protocol-Message Digest 5 Challenge Handshake Authentication Protocol) wersja protokołu CHAP dopasowana do struktury protokołu EAP. Ten protokół uwierzytelniający obsługuje szyfrowanie danych uwierzytelniania za pomocą hasha MD5 i zwykle jest używany w celu zapewnienia kompatybilności ze starszymi klientami innych producentów.

- Protokół SPAP (Shiva Password Authentication Protocol) słabo zaszyfrowany protokół uwierzytelniania nieobsługujący szyfrowania danych połączenia.

- Protokół PAP (Password Authentication Protocol) dane uwierzytelniające nie są szyfrowane, lecz przesyłane przez sieć w formie tekstu otwartego. Protokół PAP nie obsługuje szyfrowania w celu ochrony danych.

Proces uwierzytelniania zawsze próbuje negocjować wykorzystanie jak najbezpieczniejszego protokołu uwierzytelniającego. Domyślnym protokołem uwierzytelniającym używanym dla klientów VPN łączących się z systemem Windows Server 2008 VPN jest protokół MS-CHAPv2.

b) Protokoły uwierzytelniające używane przez serwer Windows Server 2019 do uwierzytelniania przychodzących połączeń VPN to:

- MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2) - protokół uwierzytelniający, który działa w oparciu o hasła. Klient wysyła serwerowi swoje dane uwierzytelniające, a serwer sprawdza poprawność tych danych i zwraca klientowi odpowiedź.

- EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) - protokół uwierzytelniający, który wykorzystuje certyfikaty cyfrowe. Klient i serwer wymieniają się certyfikatami, a następnie klient wysyła swój certyfikat do serwera w celu uwierzytelnienia.

- PEAP-MS-CHAP v2 (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2) - protokół uwierzytelniający, który działa w oparciu o hasła i jest zabezpieczony protokołem TLS. Klient wysyła swój login i hasło wraz z żądaniem uwierzytelnienia, a serwer sprawdza poprawność danych i zwraca klientowi odpowiedź.

C. Najczęściej spotykane rodzaje VPN:

1. Point to Point Tunneling Protocol (w skrócie PPTP) to protokół komunikacyjny umożliwiający tworzenie wirtualnych sieci prywatnych wykorzystujących technologię tunelowania. Polega na zdalnym dołączaniu się do stacji roboczych lub sieci (głównie opartych na systemie operacyjnym Windows) za pośrednictwem Internetu i tworzeniu wirtualnego połączenia z lokalną siecią.
Ma zapewnić jednocześnie zachowanie bezpieczeństwa przy zdalnym przesyłaniu danych.
Inicjalizacja połączenia wykonywana jest na port 1723.

PPTP działa na warstwie 2 protokołu TCP/IP i jest obsługiwany przez większość systemów operacyjnych, w tym Windows, macOS i Linux.

Protokół PPTP używa szyfrowania danych za pomocą protokołu Microsoft Point-to-Point Encryption (MPPE), który jest uważany za stosunkowo niskiego poziomu bezpieczeństwa. Z tego powodu PPTP nie jest już zalecany do stosowania w środowiskach, gdzie wymagane jest wysokie zabezpieczenie. Protokół PPTP, w implementacji firmy Microsoft, był wielokrotnie łamany i jego stosowanie nie gwarantuje odpowiedniego poziomu bezpieczeństwa przesyłanych danych.

W celu skonfigurowania tunelu VPN za pomocą protokołu PPTP, użytkownik musi znać adres IP lub nazwę domenową serwera VPN oraz dane uwierzytelniające (nazwę użytkownika i hasło). Po nawiązaniu połączenia, użytkownik będzie mógł korzystać z sieci prywatnej, jakby był bezpośrednio połączony z nią kablem.

Najbardziej rozpowszechniona i jednocześnie zawierająca najwięcej podatności na błędy implementacja protokołu PPTP została opracowana przez firmę Microsoft. Protokół PPTP stanowi standardowe wyposażenie systemu operacyjnego Windows od wersji 98 i NT.

W celu zapewnienia kompatybilności z popularnymi systemami Windows konfiguracja serwera PPTP możliwa jest również w innych systemach operacyjnych. Przykładem może być PoPToP przeznaczony do systemów Linux, OpenBSD oraz FreeBSD. Zaleca się jednak stosowanie innych rozwiązań opartych na otwartym oprogramowaniu.

Alternatywnymi protokołami VPN, które oferują wyższy poziom bezpieczeństwa, są na przykład IPSec i OpenVPN.

2. Layer Two Tunneling Protocol, L2TP (dekapsułkowanie danych tunelowanych za pomocą protokołu IPsec) - protokół umożliwiający tunelowanie ruchu IP, IPX oraz NetBEUI i przekazywanie go poprzez dowolne medium transmisyjne, przez publiczne lub prywatne sieci, które są podzielone na segmenty lub podsieci, obsługujące dostarczanie datagramów w połączeniu punkt-punkt, np. IP, X.25, Frame Relay czy ATM (używany w MS Windows).

Użytkownik może korzystać z różnych usług, np. dostępu do Internetu, bezpiecznej transmisji plików czy zdalnego dostępu do innych systemów.

Protokół L2TP/IPsec zapewnia uwierzytelnianie pierwotne danych dla każdego pakietu, integralność danych, ochronę przed odtwarzaniem (replay) oraz tajność danych.

L2TP działa na warstwie drugiej modelu OSI, czyli na poziomie łącza danych. Protokół umożliwia połączenie dwóch urządzeń za pomocą tunelu, który jest zabezpieczony protokołem IPsec (ang. Internet Protocol Security).

L2TP działa na zasadzie klient-serwer, gdzie klient jest urządzeniem, które inicjuje połączenie z serwerem, który jest odpowiedzialny za przekierowanie ruchu. Protokół L2TP jest często wykorzystywany w systemach operacyjnych Windows, ale jest również dostępny w innych systemach.

Do poprawnego działania protokołu L2TP wymagane są odpowiednie konfiguracje na urządzeniach sieciowych oraz poprawne ustawienia protokołu IPsec. Dlatego też, L2TP jest rozwiązaniem stosowanym głównie przez profesjonalistów i osoby z doświadczeniem w dziedzinie sieci komputerowych.

Połączenia L2TP/lPsec używają dwupoziomowego uwierzytelniania. Uwierzytelnianie na poziomie komputera wykonywane jest za pomocą certyfikatów cyfrowych wydanych przez urząd CA zaufany przez klienta oraz serwer VPN lub za pomocą wdrożenia wstępnie udostępnionych kluczy.

Protokoły uwierzytelniające PPP wykorzystujemy do uwierzytelniania na poziomie użytkownika. Protokół L2TP/lPsec obsługuje wszystkie protokoły uwierzytelniające VPN dostępne dla systemu Windows Server.

3. IPsec (ang. Internet Protocol Security, IP Security) - zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami.

VPN oparta na IPsec składa się z dwóch kanałów komunikacyjnych pomiędzy połączonymi komputerami: kanał wymiany kluczy, za pośrednictwem, którego przekazywane są dane związane

z uwierzytelnianiem i szyfrowaniem (klucze), kanału (jednego lub więcej), który niesie pakiety transmitowane poprzez sieć prywatną. Kanał wymiany kluczy jest standardowym protokołem UDP (port 500). Kanały przesyłu danych oparte są na protokole ESP (protokół numer 50).

Protokół ESP odpowiada za szyfrowanie i uwierzytelnianie przesyłanych danych. W przypadku VPN opartych na IPsec, protokół ESP zapewnia poufność i integralność danych, co oznacza, że przesyłane pakiety są szyfrowane i nie mogą zostać odczytane przez osoby trzecie. Ponadto, protokół ESP może również uwierzytelniać dane, aby zapobiec ich fałszowaniu lub modyfikowaniu w trakcie przesyłania.

Ważne jest, aby zauważyć, że VPN oparta na IPsec działa na warstwie sieciowej, działa ona na poziomie protokołów IP. Aplikacje i usługi działające na urządzeniu są przez całkowicie niezależne i nie muszą być modyfikowane ani konfigurowane w żaden sposób, aby korzystać z VPN.

Podsumowując, VPN oparta na IPsec jest narzędziem do zabezpieczania połączeń sieciowych, zapewniając poufność, integralność i uwierzytelnianie danych przesyłanych przez Internet.
Z powodu swojej niezależności od aplikacji i usług, jest to także wygodne narzędzie, które można z łatwością skonfigurować i korzystać z niego bez wprowadzania zmian w innych elementach systemu.

4. Secure Socket Tunneling Protocol (SSTP) mechanizmem zdalnego dostępu, został udostępniony wraz z Windows Server 2008. Użycie w połączeniu portu 443 pozwala zdalnym użytkownikom uzyskiwać w bezpieczny sposób, dostęp do odległych punktów poprzez internet, nie obawiając się problemów związanych z blokowaniem portów poprzez zapory oraz innych problemów, które pojawiają się z L2TP/IPsec i PPTP.

Protokół SSTP kapsułkuje ruch Point-to-Point Protocol (PPP) przez kanał Secure Sockets Layer (SSL) protokołu Secure Hypenext Transfer Protocol (HTTPS). SSTP podczepia ruch PPP pod HTTPS. Dlatego ruch SSTP przechodzi przez port 443 protokołu TCP, który prawie na pewno będzie otwarty na każdej zaporze pomiędzy Internetem a serwerem sieci Web zwróconym do sieci publicznej, znajdującym się w osłoniętej podsieci organizacyjnej.

Protokół PPP od SSTP umożliwia wdrożenie zaawansowanych metod uwierzytelniania, takich jak protokół EAP-TLS, najczęściej używany z kartami inteligentnymi.
Komponent SSL protokołu SSTP zapewnia tunel VPN z szyfrowaniem, poprawiona negocjacje kluczy i sprawdzanie integralności. Dane przekazywane tym sposobem są zakodowane i możemy dowiedzieć się o próbach naruszenia zawartości tunelu pomiędzy punktami źródła i przeznaczenia.

Podczas planowania wdrożenia protokołu SSTP musimy rozważyć:

a. Wymagania sprzętowe serwera SSTP - protokół SSTP jest wymagający pod względem zasobów serwera, więc trzeba upewnić się, że serwer ma odpowiednią moc obliczeniową, pamięć RAM i przepustowość łącza.
b. Certyfikaty SSL - do ustanowienia bezpiecznego połączenia SSL/TLS konieczne jest posiadanie certyfikatu SSL, co wymaga zainstalowania i skonfigurowania odpowiedniego certyfikatu na serwerze.
c. Konfiguracja zapory sieciowej - konieczne jest otwarcie odpowiednich portów na zaporze sieciowej, aby połączenia SSTP mogły być nawiązywane z zewnątrz.
d. Konfiguracja serwera SSTP - należy skonfigurować serwer SSTP, w tym ustawić parametry sieciowe, wybrać opcje uwierzytelniania, skonfigurować adresy IP klientów VPN i inne opcje.
e. Uwierzytelnienie użytkowników - konieczne jest skonfigurowanie uwierzytelniania użytkowników, w tym wybór metody uwierzytelniania, skonfigurowanie kont użytkowników i grup, a także zapewnienie odpowiednich uprawnień dostępu.
f. Konfiguracja klientów SSTP - konieczne jest skonfigurowanie klientów SSTP, w tym dodanie profili połączeń SSTP, wybór parametrów połączenia, a także skonfigurowanie certyfikatów i uwierzytelnienia.

5. OpenVPN - pakiet oprogramowania, który implementuje techniki tworzenia bezpiecznych połączeń punkt-punkt (VPN) lub strona-strona w sieciach routowanych lub mostkowanych.
Umożliwia on tworzenie zaszyfrowanych połączeń między hostami przez sieć publiczną Internet (tunel) - używa do tego celu biblioteki OpenSSL oraz protokołów SSLv3/TLSv1. W przeciwieństwie do innych rozwiązań VPN nie bazuje na protokole IPsec jako medium. Pakiet ten dostępny jest na platformach Solaris, Linux, OpenBSD, FreeBSD, NetBSD, QNX, Mac OS X oraz Windows 2000/XP/Vista/7/10.
Cały pakiet składa się z jednego kodu binarnego dla klienta i serwera, opcjonalnego pliku konfigurującego oraz z jednego lub więcej plików kluczy w zależności od metody uwierzytelnienia.

Został napisany przez Jamesa Yonana, jest publikowany na licencji GNU GPL.

OpenVPN używa bibliotek OpenSSL do szyfrowania danych i kanałów kontrolnych. Może korzystać z HMAC by stworzyć dodatkową warstwę zabezpieczenia połączenia. Pakiet jest w stanie również wykorzystać możliwości sprzętowe, by polepszyć stopień i jakość szyfrowania.

HMAC (keyed-Hash Message Authentication Code) - kod MAC z wmieszanym kluczem tajnym zapewniający zarówno ochronę integralności jak i autentyczności danych.

Standardowy kod MAC zapewnia ochronę integralności, ale może podlegać sfałszowaniu, jeśli nie jest zabezpieczony dodatkowym mechanizmem chroniącym jego autentyczność (np. podpisem cyfrowym). Dla ochrony integralności i autentyczności w rozwiązaniach wymagających wysokiej wydajności stworzono zmodyfikowany algorytm MAC, w którym podczas każdej operacji dodawany jest tajny klucz.

W Windows Server 2019 konfiguracja OpenVPN jest stosunkowo prosta i można ją przeprowadzić w kilku krokach:

1. Pobierz OpenVPN i zainstaluj go na serwerze.
2. Skonfiguruj sieć prywatną serwera. Upewnij się, że serwer ma stałe IP w sieci.
3. Wygeneruj klucze OpenVPN. Możesz to zrobić za pomocą wbudowanych narzędzi OpenVPN lub za pomocą zewnętrznych narzędzi, takich jak EasyRSA.
4. Skonfiguruj plik konfiguracyjny OpenVPN. W pliku konfiguracyjnym określ, jakie klucze OpenVPN należy użyć, jakie adresy IP są dostępne dla połączeń VPN i jakie opcje powinny być włączone lub wyłączone.
5. Skonfiguruj reguły zapory ogniowej. Upewnij się, że serwer jest skonfigurowany tak, aby umożliwić połączenia VPN.

Po przeprowadzeniu tych kroków serwer powinien być gotowy do obsługi połączeń VPN. Klienci OpenVPN muszą zainstalować odpowiednie oprogramowanie na swoich komputerach i skonfigurować połączenie VPN z wykorzystaniem pliku konfiguracyjnego serwera.

OpenVPN oferuje wiele funkcji zabezpieczeń, takich jak szyfrowanie danych i uwierzytelnienie użytkowników. Można również skonfigurować serwer OpenVPN, aby działał w trybie serwera mostkowego, co pozwala na połączenie dwóch lub więcej sieci lokalnych przez połączenie VPN.

OpenVPN oferuje kilka metod uwierzytelnienia użytkowników: poprzez klucze, certyfikaty lub nazwę użytkownika i hasło (opcja z nazwą użytkownika i hasłem może być stosowana, w przypadku klienta bez certyfikatu).

D. Rodzaje VPN w Windows Server 2019 to:

1. VPN Site-to-Site - umożliwia połączenie między dwoma oddzielonymi fizycznie sieciami.

2. VPN Point-to-Site - umożliwia zdalny dostęp do sieci za pośrednictwem VPN. Klient łączy się z siecią za pomocą specjalnego oprogramowania VPN i certyfikatu cyfrowego.

3. VPN ExpressRoute - umożliwia łączenie prywatnej sieci z chmurą publiczną, np. z usługą Azure. Dzięki temu można korzystać z zasobów w chmurze, jakby były one częścią prywatnej sieci.

4. VPN Remote Access - umożliwia zdalny dostęp do sieci firmowej z dowolnego miejsca na świecie. Użytkownik łączy się z siecią za pomocą specjalnego oprogramowania VPN i uwierzytelniania użytkownika lub certyfikatu cyfrowego.

5. VPN Device Tunnel - umożliwia urządzeniom (np. tabletom, smartfonom) łączenie się z siecią VPN za pomocą wbudowanego klienta VPN, bez konieczności instalacji dodatkowego oprogramowania.

6. VPN Always On - zapewnia ciągłe połączenie z siecią VPN, nawet po restarcie komputera lub awarii połączenia internetowego. Jest to szczególnie przydatne dla użytkowników pracujących zdalnie, którzy wymagają stałego dostępu do sieci firmowej.

7. VPN Multi-Site - umożliwia połączenie wielu oddzielonych fizycznie sieci za pomocą jednego połączenia VPN. Dzięki temu można zintegrować oddziały firmy znajdujące się w różnych lokalizacjach.

8. VPN Client to Site - umożliwia połączenie klienta z siecią prywatną za pośrednictwem VPN. Klient korzysta z specjalnego oprogramowania VPN i certyfikatu cyfrowego, aby uzyskać dostęp do sieci prywatnej.

9. VPN Load Balancing - umożliwia równoważenie obciążenia połączeń VPN między różnymi serwerami VPN. Dzięki temu można zwiększyć wydajność i niezawodność połączeń VPN.

10. VPN Server to Server - umożliwia bezpieczne połączenie między dwoma serwerami w różnych lokalizacjach za pomocą VPN. Dzięki temu można synchronizować dane i zasoby między serwerami.

11. VPN Gateway to Gateway - umożliwia połączenie dwóch bram VPN w celu umożliwienia komunikacji między oddzielonymi sieciami. Dzięki temu można zintegrować oddziały firmy znajdujące się w różnych lokalizacjach.

12. VPN User to User - umożliwia bezpieczne połączenie między dwoma użytkownikami za pomocą VPN. Dzięki temu można umożliwić bezpieczną wymianę danych między użytkownikami pracującymi zdalnie.

13. VPN Dynamic Routing - umożliwia automatyczne uaktualnianie tablicy routingu w celu umożliwienia bezpiecznej i efektywnej komunikacji między różnymi sieciami VPN.

14. VPN Split Tunneling - umożliwia równoczesne korzystanie z sieci VPN i internetu publicznego. Dzięki temu można zmniejszyć obciążenie sieci VPN i zwiększyć wydajność połączenia.

15. VPN Transparent Tunneling - umożliwia bezpieczne połączenie między dwoma sieciami VPN z użyciem protokołów innych niż VPN, takich jak protokoły TCP/IP, UDP lub ICMP.

16. VPN Secure Socket Tunneling Protocol (SSTP) - umożliwia bezpieczne połączenie między klientem a serwerem VPN z użyciem protokołu SSL/TLS. SSTP zapewnia wysoki poziom bezpieczeństwa i jest stosowany do połączeń VPN z systemami Windows.

17. VPN Internet Key Exchange version 2 (IKEv2) - umożliwia bezpieczne połączenie między klientem a serwerem VPN z użyciem protokołu IKEv2. IKEv2 jest szybki, bezpieczny i odporny na ataki typu man-in-the-middle.

18. VPN Point-to-Point Tunneling Protocol (PPTP) - umożliwia szybkie i łatwe tworzenie połączeń VPN między klientem a serwerem VPN. PPTP jest stosowany głównie do połączeń VPN z systemami Windows i jest uważany za mniej bezpieczny niż protokoły SSTP i IKEv2.

19. VPN Layer 2 Tunneling Protocol (L2TP) - umożliwia bezpieczne połączenie między klientem a serwerem VPN z użyciem protokołów L2TP i IPSec. L2TP jest stosowany głównie do połączeń VPN z systemami Windows i jest uważany za bezpieczniejszy niż protokół PPTP.

Cele tworzenia sieci VPN:

- potrzeba błyskawicznego i bezpiecznego dostępu do informacji,
- wysokie koszty łącz dzierżawionych oraz budowy własnej sieci WAN,
- mobilność pracowników,
- globalizacja przedsiębiorstw.

Zalety oraz wady rozwiązania

Zaletami VPN są:

- niskie koszty, jeden z głównych powodów stosowania takiego rodzaju sieci.

- możliwość zalogowania czy wejścia do sieci firmowej praktycznie z każdego miejsca na świecie co dla pracownika oddalonego o wiele kilometrów jest tak naprawdę bezcenne, ponieważ może on bez większych problemów pracować tak jak byłby w siedzibie swojej firmy i siedział przy swoim biurku.

- firma może łączyć swoje oddziały tak, aby istniały jako jedna wspólna sieć LAN. Użytkownicy prywatni są w stanie połączyć się ze swoim komputerem domowym będąc w każdym możliwym miejscu na świecie.

Wadami VPN jest:

- podatność na włamania, używa się globalnego medium transmisyjnego jakim jest internet, więc teoretycznie przy pomocy odpowiednich narzędzi i umiejętności, ktoś jest w stanie "podłączyć" się pod dany tunel VPN i wykraść ważne dla firmy informacje.

- zagrożeniem są sami pracownicy, którzy nie przeszkoleni mogą udostępnić swoje dane do logowania w sieci firmowej.

Najczęściej spotykane sposoby szyfrowania protokołów VPN:

- szyfry symetryczne: DES, 3DES, AES, RC2, RC4, itp.,
- szyfry asymetryczne: RSA, DSA, ElGamal, itp.,
- algorytm Diffiego - Hellmana,
- funkcje skrótu: SHA-1, SHA-256, RIPEMD-160, MD5,
- podpisy cyfrowe: RSA, DSA,
- certyfikaty cyfrowe: X.509.

Najczęściej spotykane programy:

- OpenVPN (darmowy),
- Hamachi (darmowo/płatny) - zobacz videocast pokazujący możliwości programu "Hamachi",
- RealVNC (płatny),
- TightVNC (darmowy),
- kvpnc (darmowy na LINUX-a),
- Windows VPN Client (darmowy z kupnem systemu).