

Politechnika Łódzka
Wydział Elektrotechniki, Elektroniki, Informatyki i Automatyki
Katedra Informatyki Stosowanej



PRACA DYPLOMOWA MAGISTERSKA

**Zdalny dostęp do zasobów sieci LAN przedsiębiorstwa oraz
metody uwierzytelniania telepracowników.**

Autor: Michał Strzelecki

Numer albumu: 147308

Opiekun:
dr inż. Łukasz Sturgulewski

Konsultant:
mgr inż. Artur Sierszeń

Łódź, 04.2009

Spis treści:

| | |
|---|----|
| Wstęp..... | 4 |
| Cel i zakres pracy..... | 5 |
| Układ pracy..... | 6 |
| 1 Wprowadzenie do sieci komputerowych..... | 7 |
| 1.1 Sieć Internet – zasada działania | 10 |
| 1.2 Model ISO/OSI oraz TCP/IP | 12 |
| 1.3 Protokół IP | 15 |
| 1.4 Protokoły TCP i UDP | 17 |
| 1.5 Sieci rozległe i metody dostępu | 19 |
| 1.6 Dostęp zdalny do zasobów sieci lokalnych | 26 |
| 2 Zagrożenia przesyłanych danych poprzez sieci publiczne..... | 29 |
| 2.1 Podsłuch danych | 30 |
| 2.2 Podsywanie się..... | 31 |
| 2.3 Łamanie haseł | 31 |
| 2.4 Przejęcie sesji..... | 32 |
| 2.5 Odmowa usługi | 32 |
| 2.6 Błędy w oprogramowaniu..... | 33 |
| 2.7 Złośliwy kod | 33 |
| 3 Procesy bezpieczeństwa | 34 |
| 3.1 Polityka bezpieczeństwa firmy | 34 |
| 3.2 Bezpieczeństwo sieci | 35 |
| 3.2.1 „Koło bezpieczeństwa” | 35 |
| 3.2.2 Bezpieczeństwo urządzeń i hostów sieciowych..... | 36 |
| 4 Zabezpieczenie danych przesyłanych przez sieć publiczną | 38 |
| 4.1 Sieci VPN | 38 |
| 4.1.1 VPN typu „Site-to-Site” | 39 |
| 4.1.2 VPN typu „Remote Access” | 42 |
| 4.2 Warstwa druga modelu ISO/OSI: PPTP, L2F, L2TP | 43 |
| 4.3 Warstwa trzecia ISO/OSI: IP Security (IPsec) | 48 |
| 4.3.1 Funkcje i opcje | 50 |
| 4.3.2 Architektura IPsec | 51 |
| 4.3.3 Protokoły bezpieczeństwa w IPSEC: AH i ESP | 52 |

| | | |
|--------|--|-----|
| 4.3.4 | Tryby pracy tunelowy i transportowy | 57 |
| 4.3.5 | Algorytmy szyfrowania..... | 58 |
| 4.3.6 | Negocjacja parametrów bezpieczeństwa: IKE | 61 |
| 4.3.7 | Fazy IKE | 62 |
| 4.4 | Warstwa czwarta ISO/OSI: Protokoły SSL/TLS | 65 |
| 4.4.1 | Zasada działania SSL | 68 |
| 4.4.2 | Wersje SSL..... | 70 |
| 4.5 | Warstwa siódma ISO/OSI: PGP, S/MIME, SSH..... | 71 |
| 4.5.1 | PGP | 71 |
| 4.5.2 | S/MIME..... | 73 |
| 4.5.3 | SSH | 74 |
| 4.6 | Porównanie metod zabezpieczeń przesyłania danych | 75 |
| 5 | Metody i sposoby uwierzytelniania..... | 79 |
| 5.1 | Nazwa użytkownika i hasło | 82 |
| 5.2 | Jednorazowe hasła | 85 |
| 5.3 | Cechy biometryczne | 88 |
| 5.4 | Klucz współdzielony..... | 90 |
| 5.5 | Certyfikaty cyfrowe i PKI..... | 91 |
| 6 | Model AAA | 94 |
| 6.1 | Protokoły RADIUS i TACACS+..... | 95 |
| 7 | Projekt zdalnego dostępu w firmie | 97 |
| 7.1 | Założenia projektowe..... | 97 |
| 7.2 | Opis projektu..... | 99 |
| 7.2.1 | Aktualny stan sieci WAN..... | 99 |
| 7.2.2 | Aktualny stan sieci LAN..... | 102 |
| 7.2.3 | Wdrożenie koncentratora VPN | 104 |
| 7.2.4 | Adresacja IP w sieci LAN/WAN | 107 |
| 7.2.5 | Adresacja IP dla klientów zdalnego dostępu | 109 |
| 7.2.6 | Konfiguracja koncentratora VPN..... | 111 |
| 7.2.7 | Zarządzanie polisami grup | 113 |
| 7.2.8 | Listy kontroli dostępu (ACL)..... | 121 |
| 7.2.9 | Autoryzacja użytkowników | 135 |
| 7.2.10 | Konfiguracja modelu AAA na koncentradorze VPN..... | 140 |

| | | |
|--------|---|-----|
| 7.2.11 | Profile połączeń | 143 |
| 7.2.12 | Weryfikacja stacji roboczych zdalnych pracowników | 145 |
| 7.2.13 | Proces obsługi połączeń VPN | 149 |
| 7.3 | Testy akceptacyjne..... | 155 |
| 7.3.1 | Połączenie VPN z użyciem IPsec | 156 |
| 7.3.2 | Połączenie VPN z użyciem SSL/TLS | 164 |
| 7.3.3 | Połączenie VPN z użyciem protokołu L2TP/IPsec..... | 168 |
| 7.4 | Testy wydajnościowe..... | 171 |
| 7.5 | Omówienie wyników testów | 174 |
| 8 | Podsumowanie i wnioski..... | 176 |
| 9 | Pliki Konfiguracyjne | 180 |
| 10 | Bibliografia..... | 196 |
| 11 | Słownik pojęć | 197 |

Wstęp

Szybki rozwój dziedziny nowoczesnych technologii sprawił, że dostęp do globalnych zasobów sieci Internet stał się możliwy praktycznie w każdym zakątku ziemi. Już dziś trudno sobie wyobrazić funkcjonowanie oddziałów nowoczesnych przedsiębiorstw, często umiejscowionych w oddalonych od siebie miastach a nawet i różnych kontynentach bez wzajemnej komunikacji. Nie stanowi też już problemu, by zdalne, odległe oddziały firmy połączyć w jedną bezpieczną, wewnętrzną sieć lokalną, jednak konkurencja na rynku oraz rosnące wymagania sprawiają, że często stacjonarne oddziały firm nie są w stanie dotrzeć do odpowiedniej liczby klientów. Tutaj z pomocą przychodzą mobilni pracownicy – tzw. „telepracownicy”.

Niejednokrotnie wyposażeni w przenośny komputer lub palmtop oraz usługę bezprzewodowego dostępu do Internetu np. za pośrednictwem technologii GSM – stanowią mały, lecz mobilny oddział firmy. Zatrudnienie pracowników zdalnych daje dodatkową korzyść biznesową - oszczędność kosztów związanych z wynajmem wciąż kurczącej się powierzchni biurowej (możliwe, że w przyszłości biura dużych firm będą tylko biurami wirtualnymi). Obniżenie kosztów utrzymania biura i pracowników na miejscu – pozwala na podniesienie konkurencyjności usług oferowanych przez przedsiębiorstwo. W przyszłości – ciągła obecność pracowników w biurze nie będzie konieczna – zatem zdalna praca umożliwi także zachowanie ciągłości biznesowej nawet w przypadku sytuacji kryzysowej np. spowodowanej warunkami atmosferycznymi czy też zdarzeniami losowymi. Telepracownicy to także szansa dla osób niepełnosprawnych, na normalną pracę z własnego domu.

Zdalny pracownik w zależności od przyznanego poziomu uprawnień, może posiadać dostęp do firmowej sieci lokalnej tak, jak by znajdował się w macierzystym oddziale. Nie stanowi zatem kłopotu porozumiewanie się z innymi współpracownikami używając wewnętrznej sieci VOIP (ang. *Voice Over IP*), przekazanie obrazu video, czy też pobieranie krytycznych informacji z wewnętrznych baz danych. Wszystko to za sprawą nowoczesnej technologii zdalnego dostępu za pośrednictwem wirtualnych sieci prywatnych VPN (ang. *Virtual Private Network*).

Projektując korporacyjną sieć VPN należy wziąć pod uwagę wiele istotnych czynników, jakimi są między innymi przyszły rozwój – czyli wzrastająca liczba

użytkowników, sposoby dostępu, przepustowość łącz, wydajność urządzeń a także możliwość ich szybkiego zastąpienia w razie awarii (redundancia). Jednakże w miarę rozbudowywania się sieci, udostępnianych użytkownikom kolejnych aplikacji – wzrasta też ilość potencjalnych zagrożeń bezpieczeństwa danych. Niebezpieczeństwo - nie tylko związane z wykryciem coraz to nowych luk w programach, ale także z powodu upowszechnienia się narzędzi do cyber ataków, a także łatwiejszego dostępu do wiedzy technicznej.

Aby zminimalizować ryzyko nie bezpieczeństwa utraty danych, koniecznym jest wdrożenia odpowiednich praktyk tzw. polis bezpieczeństwa, na przykład poprzez dokładną weryfikację osoby próbującej nawiązać połączenie, sprawdzenie jej komputera pod kątem ostatnich aktualizacji oprogramowania czy też przyznanie jej tylko niezbędnych uprawnień do wykonania czynności służbowych.

Bardzo ważnym jest, by znaleźć złoty środek między maksymalnie wysokim poziomem bezpieczeństwa a możliwością pozyskania danych, jakie potrzebuje końcowy użytkownik sieci. Najbezpieczniej było by nie włączać krytycznych komputerów, serwerów z danymi do żadnej sieci – jednak wtedy były by one z punktu widzenia pracowników firmy bezużyteczne. Zatem budowa z góry przemyślanej i bezpiecznej sieci korporacyjnej w tym także i sieci dla zdalnych pracowników jest sprawą pierwszoplanową w dzisiejszych rozwiązań dla administratorów sieci.

Cel i zakres pracy

Celem pracy jest analiza bezpiecznych metod zdalnego dostępu do zasobów sieci LAN przedsiębiorstw oraz związanych z nimi sposobów uwierzytelniania telepracowników.

Wybrane rozwiązania zostaną zaprojektowane, wdrożone i zweryfikowane w przykładowej sieci korporacyjnej firmy mającej 6 oddziałów na całym świecie (w tym dwie lokalizacje centralne) mających dostęp do sieci Internet. Połączenia pomiędzy oddziałami oraz połączenia telepracowników z oddziałem muszą być bezpieczne (szyfrowane). Dodatkowo pracownik zdalny zanim uzyska dostęp do sieci korporacyjnej musi zostać poddany weryfikacji tożsamości (uwierzytelnieniu), co w dalszej kolejności pozwoli na zrewidowanie jego uprawnień do poszczególnych zasobów. W zależności od poziomu uprawnień telepracownik, będzie miał możliwość

uwierzytelniania się za pomocą już posiadanego konta w domenie Active Directory, bądź też za pomocą wskazań jednorazowych haseł generowanych za pomocą elektronicznego Tokenu RSA. [1i]

Wynikiem przeprowadzonych konfiguracji urządzeń i serwerów jest zestaw plików konfiguracyjnych, które zawierają instrukcje dla urządzeń aktywnych, realizujących w/w założenia projektowe.

Układ pracy

Praca niniejsza składa się z 11 rozdziałów. W rozdziale pierwszym zaprezentowano genezę sieci komputerowych, opis technologii używanych do budowy sieci rozległych, Internetu i protokołu IP.

Rozdziały drugi i trzeci poruszają tematy związane z zagrożeniami przesyłania danych poprzez sieć publiczną oraz opis procesów bezpieczeństwa.

W rozdziale czwartym znajdują się szczegółowe informacje o technologiach umożliwiających zabezpieczenie danych podczas tranzytu.

Rozdziały piąty i szósty poświęcone są tematom związanym z metodami i protokołami uwierzytelniania użytkowników.

Rozdział siódmy zawiera opis techniczny i użytkowy zrealizowanego projektu sieci rozległej, przedstawiono w nim budowę i najważniejsze funkcje, opisano sposób instalacji i użytkowania.

Rozdział ósmy jest rozdziałem podsumowującym wykonaną pracę, zawiera wnioski z przeprowadzonego projektu.

W rozdziale dziewiątym załączony został listing pliku konfiguracyjnego urządzenia, na bazie którego powstał projekt.

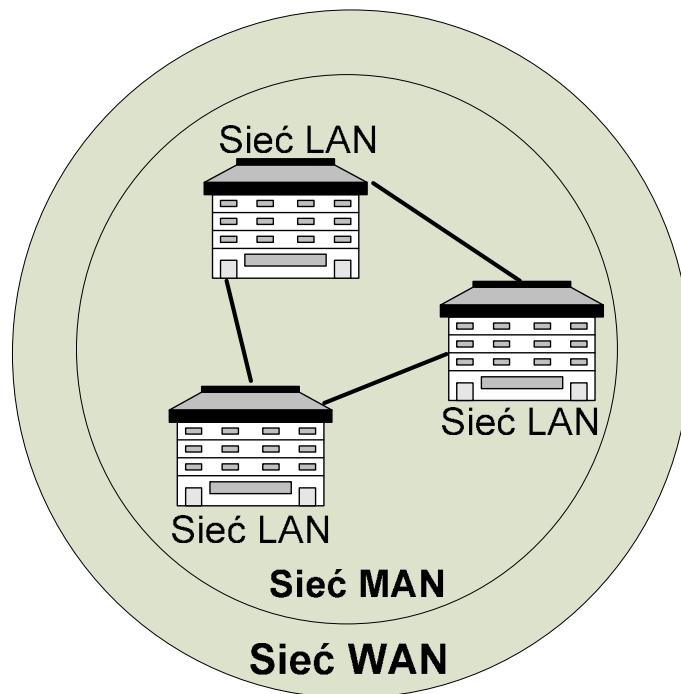
Bibliografia znajduje się w rozdziale dziesiątym.

Słownik pojęć znajduje się w rozdziale jedenastym.

Do pracy dołączony został CD-ROM zawierający pliki konfiguracyjne urządzeń oraz wykonane rysunki.

1 Wprowadzenie do sieci komputerowych

Sieć komputerową (ang. *Computer Network*) tworzyć może grupa komputerów lub innych urządzeń aktywnych i pasywnych połączonych ze sobą fizycznie lub logicznie celem wymiany danych lub współdzielenia zasobów.[1i] Przykładem najmniejszych sieci może być połączenie dwóch komputerów za pomocą kabla UTP lub koncentrycznego, zaś największą jaką powstała i wciąż jest rozwijana jest sieć Internet, którą tworzy prawie 1,5 biliona komputerów. Głównym kryterium podziału sieci komputerowych jest obszar i zakres obowiązywania.



Rysunek 1 Opracowanie własne: Rodzaje sieci komputerowych

Tabela 1 Opracowanie własne: Zastosowanie sieci komputerowych [2i]

| | <i>LAN</i> | <i>MAN</i> | <i>WAN</i> |
|----------------------------|--|----------------------------------|--------------------|
| <i>Obszar geograficzny</i> | 5m-2km | 2km-60km | Bez ograniczeń |
| <i>Główne</i> | ✓ Poczta elektroniczna ✓ Aplikacje bazodanowe | ✓ Połączenie sieci LAN ze sobą w | ✓ Połączenie sieci |

| | | | |
|---------------------|---|----------------|--------------------------|
| Zastosowanie | <ul style="list-style-type: none"> ✓ Strumienie audio-wideo ✓ Współdzielenie plików ✓ Komunikatory ✓ Wewnętrzne aplikacje CRM ✓ Drukowanie/skanowanie ✓ Podpis elektroniczny i szyfrowanie danych | granicy miasta | LAN/MAN |
| | | | bez względu na odległość |
| | | | ✓ Dostęp do Internetu |

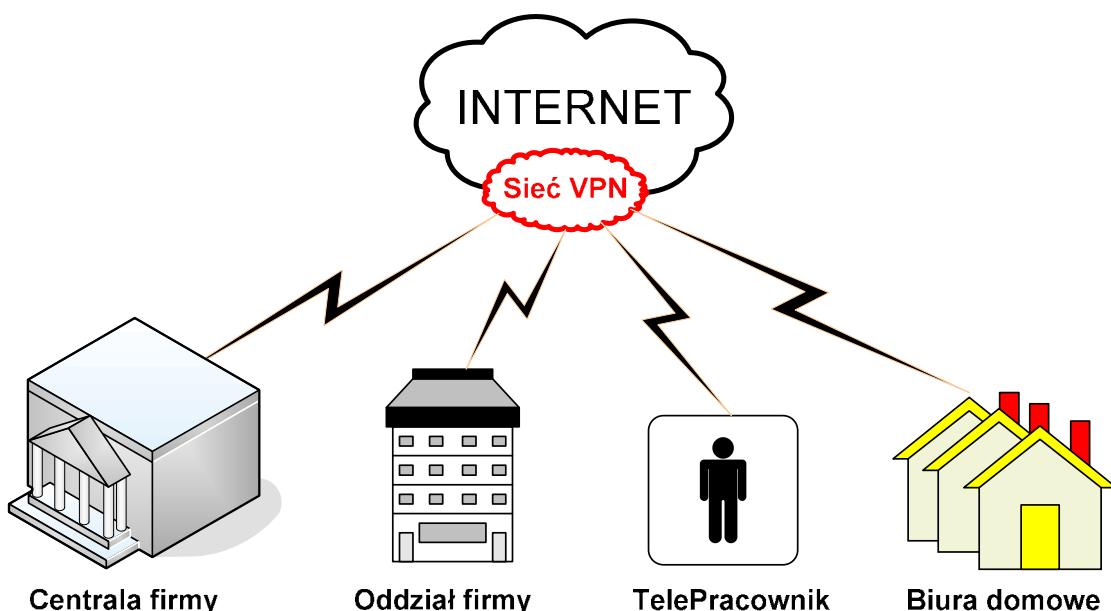
Wyróżniamy **sieci o zasięgu lokalnym - LAN** (ang. *Local Area Network*), które pokrywają obszar zwykle pojedynczego oddziału firmy, małego osiedla, bądź też sieci kampusowych, gdzie liczba użytkowników nie przekracza kilkuset. Sieci lokalne pozwalają na połączenie ze sobą komputerów użytkowników, drukarek, serwerów, skanerów, aktywnych i pasywnych urządzeń sieciowych z dużymi prędkościami (nawet i 10Gbit/s) i bardzo niskim współczynnikiem błędów. Wykorzystując sieci lokalne możliwym jest zatem przesłanie każdego rodzaju danych – od wrażliwego na opóźnienia i utraty pakietów ruchu video i głosowego na żywo, aż po ogromne ilości danych jakie gromadzą serwery zasobowe i bazy danych. Dużą zaletą sieci lokalnych jest też możliwość łatwej administracji, gdyż jej wszystkie punkty dystrybucyjne i media transmisyjne ją tworzące są dostępne do wglądu i ewentualnej naprawy na wypadek usterki. W sieciach LAN, które w całości zarządzane są przez wykwalifikowany i zaufany personel informatyczny, można w znaczący sposób podnieść poziom bezpieczeństwa i ochrony danych stosując odpowiednie praktyki [2i].

Sieć o zasięgu miejskim – MAN (ang. *Metropolitan Area Network*), geograficznie obejmują zwykle obszar jednego miasta, np. połączenie kilku szkół bądź bibliotek znajdujących się w granicach terytorialnych miasta. Sieci MAN łączą ze sobą kilka sieci LAN, lecz nie gwarantują tak dużych prędkości przesyłu jak w sieciach lokalnych. Do przesyłania danych w sieciach MAN wykorzystuje się zwykle linie dzierżawione lub mosty bezprzewodowe (ang. *Bridge*), zapewniające prędkości przesyłu zwykle nie przekraczające 100Mbit/s (wyjątkiem są tutaj miejskie węzły międzyoperatorskie oferujące wymianę ruchu na poziomie 1Gbit/s za pośrednictwem technologii Gigabit-Ethernet). Sieci MAN mogą, ale nie muszą być zarządzane przez personel informatyczny należący do tej samej organizacji, zatem należy wziąć pod uwagę bezpieczeństwo wymiany informacji między sieciami LAN [2i].

Największy zasięg oferują sieci WAN (ang. *Wide Area Network*) – łączące sieci lokalne oraz miejskie ze sobą. Sieci takie nie mają ograniczeń odległości, zatem dwie połączone sieci LAN za pośrednictwem sieci WAN mogą wymieniać się danymi w sposób przezroczysty dla użytkowników nawet kiedy dzieli je kilka tysięcy kilometrów. Połączenia sieci rozległych (WAN) realizowane są przez dostawców usług internetowych (ang. ISP – *Internet Service Provider*) za pomocą różnych technologii:

- ✓ Linie dzierżawione
- ✓ POTS
- ✓ Różne odmiany technologii xDSL
- ✓ ATM
- ✓ Frame Relay
- ✓ X.25
- ✓ Ethernet
- ✓ Dostęp bezprzewodowy

Sieci WAN wykorzystując rozmaite technologie dostępu – mogą zapewnić prędkości transmisji nawet rzędu 40Gbit/s (np. używając technologii SONET OC768) – jednak maksymalne wartości uzależnione są w dużej mierze od odległości. Jako, że sieci WAN w wielu przypadkach wykorzystują logiczną infrastrukturę Internetu, która to zarządzana jest przez różne organizacje – koniecznym jest zadbanie o bezpieczeństwo wymiany informacji, które transmitowane jest przez to potencjalnie niebezpieczne medium [2i].



Rysunek 2 Opracowanie własne: Sieci VPN

Za pomocą sieci VPN (ang. *Virtual Private Network*) możliwym jest zabezpieczenie połączeń w dowolnych sieciach dowolnie oddalonych od siebie i zbudowania logicznej spójnej sieci, zatem możliwym jest połączenie ze sobą dwóch sieci LAN mających własny dostęp do Internetu w sposób przezroczysty dla użytkowników, niezależnie od geograficznej odległości. Sieci VPN umożliwiają także firmom – na bezpieczne dołączenie do swojej lokalnej sieci komputerowej – zdalnych pracowników, wykorzystujących dowolne łącze do Internetu. Jako, że jedynym koniecznym warunkiem do nawiązania komunikacji z oddziałem firmy przez zdalnego pracownika jest, aby posiadał on łącze internetowe, zatem może on przebywać zarówno we własnym domu, jak i w podróży służbowej i nadal być osiągalny i wykonywać swoje obowiązki wobec pracodawcy. Daje to szereg wymiernych korzyści zarówno dla firmy jak i samego zatrudnionego [2i][2][3].

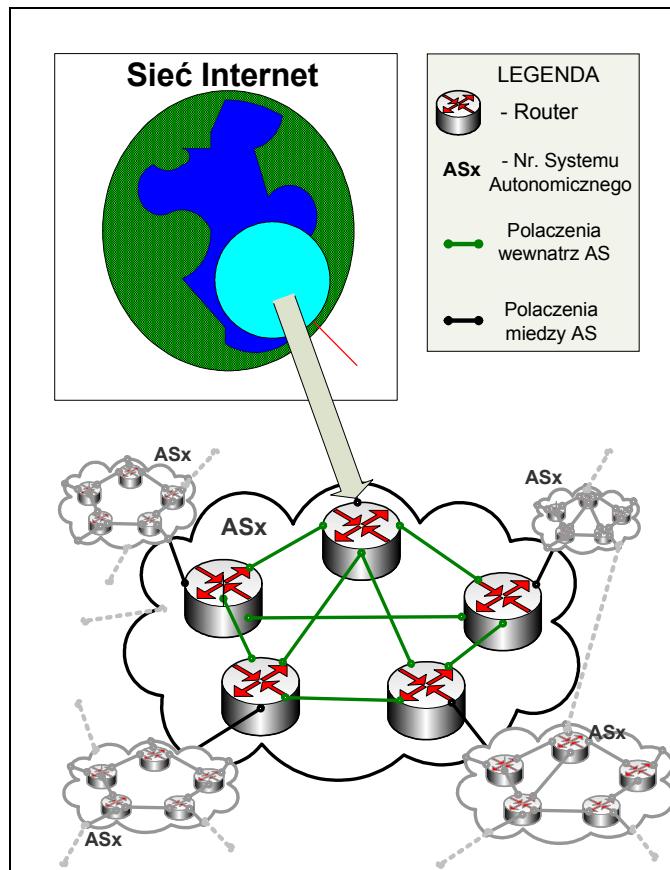
1.1 Sieć Internet – zasada działania

Internet jest siecią komputerową, która powstała w wyniku połączenia mniejszych sieci (LAN, MAN, WAN) w jedną globalną sieć. Głównym założeniem budowy tej ogromnej struktury było, aby każdy host (np. komputer) pracujący w dowolnej części świata mógł nawiązać połączenie z dowolnie oddalonym innym. Zanim informacja zostanie między nimi przekazana – przechodzi wiele urządzeń aktywnych, np. rutery, zapory sieciowe, przełączniki.

Główna rolę (choć nie jedyną) w przekazywaniu informacji pełnią rutery (ang. *routery*). Mogą one przyjmować postać sprzętową np. routery firmy Cisco, 3Com, HP lub też programową – gdzie konfiguracja sprzętowa odgrywa rolę drugoplanową – natomiast najważniejszy jest program realizujący funkcję przekazywania pakietów. Dobrym przykładem routerów programowych mogą być te oparte na bazie systemu Linux (iptables) lub też np. jako cały system operacyjny – produkty firmy Checkpoint.

Zasada działania routera jest następująca: do routera podłączone są przynajmniej dwie podsieci, które można wydzielić w ramach jednej sieci komputerowej. Urządzenie tworzy tzw. tablicę trasowania (routingu), która to zawiera ścieżki do konkretnych obszarów sieci. Na podstawie przynależności (bądź jej braku) podsieci do

odpowiednich interfejsów routera – router podejmuje decyzję o przekazaniu pakietu do odpowiedniego interfejsu sieciowego (portu), bądź też przekazaniu pakietu do sąsiedniego routera.



Rysunek 3: Opracowanie własne: Sieć Internet

Dla przykładu na bazie protokołu routingu dynamicznego BGP (ang. *Border Gateway Protocol*): w każdej niezależnej części sieci Internet (zwanej często numerem AS (ang. *Autonomous System*) umieszczony jest przynajmniej jeden główny (bądź kilka) router zbierający informacje z routerów, które przekazują do niego wszystkie pakiety danych, które nie mogą być dostarczone w ramach podłączonych do ich interfejsów podsieci. Router taki przekazuje je dalej, do następnego (o innym numerze AS) i sprawdza, czy dane adresowane są do jego sieci. Jeśli w swojej tablicy routingu posiada informacje, że żądana sieć jest osiągalna w ramach obsługiwanej przez ten router sieci lokalnej - to przekazuje je do celu, a jeśli nie, to do kolejnego systemu autonomicznego i tak do skutku, aż dane dotrą do adresata (wybór kolejnego routera nie jest przypadkowy – odbywa się na podstawie posiadanych informacji o tzw. prefixach do innych sieci. Jeżeli jedna z dołączonych podsieci ulegnie awarii lub będzie niedostępna z powodu przeciążenia, to pakiety od adresata do odbiorcy mogą trafić inną drogą. Dzięki temu,

że autonomiczne systemy połączone są ze sobą zwykle za pośrednictwem kilku łącz – awaria jednego segmentu sieci Internet nie powoduje zaprzestania działania całej sieci. Inną ważną cechą jest to, że choć poszczególne podsieci różnią się od siebie sposobem komunikacji, rodzajem osprzętu i zastosowaną technologią - mogą się one komunikować ze sobą bez przeszkód dzięki odpowiednim protokołom i standardom.[1i][2][3]

1.2 Model ISO/OSI oraz TCP/IP

W początkowych fazach rozwoju sieci komputerowych ze względu na brak standaryzacji i protokołów mających zapewnić bezproblemowe połączenia między programami, a także sprzętem pochodzących od różnych dostawców - międzynarodowa organizacja standaryzacyjna ISO (ang. *International Standards Organization*) opracowała model referencyjny tzw. systemów otwartych (obsługiwanych w środowiskach wielosystemowych). Omawiany model OSI (ang. *Open System Interconnection*) – jest modelem warstwowym, który dzieli wszystkie procesy jakie zachodzą podczas komunikacji sieciowej na 7 warstw. Każda z warstw ma określone zadanie i jest odwzorowaniem wszystkich zdarzeń jakie zachodzą podczas komunikacji.



Rysunek 4 Opracowanie własne: Model ISO/OSI

Warstwa fizyczna – odpowiada za transmitowanie sygnałów binarnych w sieci. Zatem dotyczy konwersji sygnału elektrycznego na bity i odwrotnie, przesłaniu tego sygnału

przez medium transmisyjne np. kabel miedziany, zmianie amplitudy, regeneracji itd. Przykładem urządzeń i pojęć związkowych z warstwą pierwszą mogą być: przewody miedziane, światłowody, repeatery (regeneratorzy sygnału), huby, złącza, wtyki, gniazda

Warstwa łącza danych – odpowiada za poprawny odbiór strumienia bitów (zer i jedynek), eliminację zakłóceń (ewentualna retransmisja na wypadek błędów), ustalenie prędkości nadawania i odbioru danych. Warstwa ta wprowadza pojęcie adresu fizycznego (MAC), oraz grupy bitów – tzw. ramki.

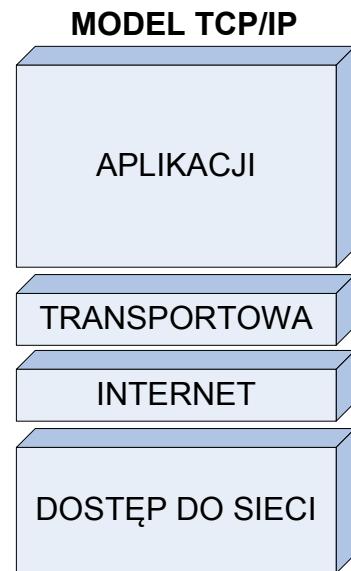
Warstwa sieciowa – zapewnia adresacje sieciową pakietów danych, wybór optymalnej drogi dla pakietów między urządzeniami, które nie są osiągalne lokalnie. Najbardziej znany protokołem realizującym wymienione funkcje jest protokół IP. Warstwa ta steruje działaniem podsieci transportowej

Warstwa transportowa – głównym zadaniem tej warstwy jest obsługa danych przychodzących z warstwy sesji, dzielenie danych na mniejsze jednostki, realizuje funkcję otwarcia i zamknięcia połączenia, wykrywanie błędów komunikacji.

Warstwa sesji – kontrola nad ustanowieniem i zamykaniem sesji między aplikacjami. Definiuje jaką ma być reakcja w przypadku zerwania połączenia (rezygnacja, czy odtworzenie), jakie opcje będą obowiązywały podczas trwania sesji między nadawcą a odbiorcą.

Warstwa prezentacji – nadzór nad formatem danych, sposobem kodowania i dekodowania znaków (oraz wybór algorytmów potrzebnych do tego celu), warstwa ta udostępnia też mechanizmy do kompresji i szyfrowania danych.

Warstwa aplikacji – ma za zadanie dostarczyć określone usługi (rozpoznawane po docelowych portach) – do odpowiednich procesów nasłuchujących w systemie operacyjnym. Np. żądanie na port TCP/80 dostarczyć do procesu realizującego funkcję serwera WWW.[1i][2][3]



Rysunek 5 Opracowanie własne : Model TCP/IP

Model TCP/IP:

Drugim, odmiennym w stosunku do modelu ISO/OSI – jest model TCP/IP. Uproszczona konstrukcja w rzeczywistości realizuje te same funkcje co model ISO/OSI jednak na przestrzeni 4 warstw.

Warstwa Dostępu do sieci – Obejmuje szczegóły związane z technologiami LAN/WAN, łączy ze sobą funkcję warstw fizycznej i łącza danych modelu ISO/OSI

Warstwa Internet – analogicznie do warstwy sieci w modelu ISO/OSI

Warstwa transportowa – realizuje mechanizmy dostarczania danych, niezawodności, kontroli przepływu danych, wykrywania błędów, otwierania i zamknięcia połączenia.

Warstwa aplikacji – zwana warstwą przetwarzania - obejmuje swoim działaniem analogiczne zadania warstw sesji i prezentacji modelu ISO/OSI – prezentacja, kompresja, kodowanie, kontrola sesji.

Podobieństwa i różnice w budowie modelu ISO/OSI a TCP/IP:

| Podobieństwa | Różnice |
|---|--|
| Oba modele mają budowę warstwową Działanie warstwy transportu (TCP/IP) i sieci (ISO/OSI) obejmuje ten sam zakres | Model TCP/IP łączy działanie trzech warstw modelu ISO/OSI (sesji, prezentacji i aplikacji) w jedną – aplikacji |

| | |
|--|--|
| Oba mają warstwę aplikacji, ale zakres działań jest bardzo różny | Model TCP/IP łączy działanie warstw łączących danych i fizyczną w jedną - fizyczną Model TCP/IP jest prostszy, gdyż ma mniej warstw |
|--|--|

Tabela 2 Opracowanie własne: Porównanie modeli ISO/OSI i TCP/IP

Podczas porównania tych dwóch modeli można zauważać, że model TCP/IP jest łatwiejszy i bardziej przejrzysty. Warstwa aplikacji przejmuje dotychczasowe role trzech warstw modelu ISO/OSI czyniąc łatwiejszym tworzenie aplikacji korzystających z sieci (trudno zachować sztywne granice między warstwami modelu ISO/OSI pisząc program, gdyż granice odpowiedzialności modelu zacierają się).[1i][2][3]

1.3 Protokół IP

Podstawowym protokołem w sieci Internet jest protokół IP. Pakietowy sposób przesyłu danych wymaga, aby informacje przesyłaną podzielić na ścisłe określone części – pakiet IP. Każdy z takich pakietów, dzięki protokołowi IP, otrzymuje nagłówek, gdzie znajdują się informacje o adresie nadawcy i odbiorcy, długość pakietu, sumie kontrolnej i inne pola. Z danych tych korzystają między innymi routery, aby właściwie dostarczyć dane do adresata.

| WERSJA | DŁ.NAGŁ. | TYP OBSŁUGI | DŁUGOŚĆ CAŁKOWITA | |
|---------------------|----------|-------------|-------------------|------------------------|
| IDENTYFIKACJA | | | FLAGI | PRZESUNIĘCIE FRAGMENTU |
| TTL | PROTOKÓŁ | | SUMA KONTROLNA | |
| ADRES IP NADAWCY | | | | |
| ADRES IP ODBIORCY | | | | |
| OPCJE IP (jeśli są) | | | UZUPEŁNIENIE | |
| DANE | | | | |
| ... | | | | |

Rysunek 6 Opracowanie własne: Struktura nagłówka IP

Pole Wersja – określa wersję protokołu IP (IPv4 lub IPv6), pole 4 bitowe

Pole Długość nagłówka – (ang. *IP Header Length*) – 4 bitowe pole określające długość nagłówka pakietu IP

Typ obsługi – (ang. *Type Of Service*) 8 bitowe pole określające – poziom pierwszeństwa pakietu w stosunku do innych. Zawiera informację o stopniu ważności pakietu IP, od 0 (normalny stopień ważności) do 7 (sterowanie siecią).

Długość całkowita – 16 bitowe pole określające długość pakietu IP (włącznie z danymi i nagłówkiem). Maksymalny możliwy rozmiar pakietu IP wynosi 2¹⁶-1 czyli 65535 bajtów.

Identyfikacja – 16 bitowe pole, liczba całkowita identyfikująca dany pakiet IP

Flagi – 3 bitowe pole, w którym dwa najmniej znaczące bity kontrolują fragmentację. Jeden bit określa, czy pakiet może być fragmentowany, a drugi bit określa czy pakiet jest ostatnim fragmentem w serii fragmentowanych pakietów.

Przesunięcie fragmentu – 13 bitowe pole służące do składania fragmentowanych pakietów. Pole to wskazuje, do którego miejsca pakietu danych należy ten fragment. Bazując na tym parametrze możliwe jest późniejsze odtworzenie pakietu z części.

TTL - (Time To live) 8 bitowe pole – opisujące tzw. „czas życia pakietu”. Wymaganiem protokołu TCP/IP jest, by podczas przetwarzania nagłówka IP przez każdy router - pole TTL było zmniejszane o 1. W chwili kiedy pole TTL ma wartość 0 – dany pakiet jest niszczony. Ma to na celu zapobieżenie sytuacji krążenia pakietów w sieci w nieskończoność.

Protokół – 8 bitowe pole zawiera numer identyfikacyjny protokołu transportowanego dla którego pakiet jest przeznaczony. Najbardziej protokoły to TCP/UDP/ICMP.

Suma kontrolna – 16 bitowe pole – dotyczy tylko nagłówka IP, nie jest są sprawdzane dane.

Adres źródłowy – pole 32 bitowe – określające adres IP nadawcy

Adres docelowy - pole 32 bitowe – określające adres IP odbiorcy

Opcje – to pole zmiennej długości, nie występuje w każdym pakiecie IP. Pierwotnie pole opcje – było używane do testowania i usuwania błędów. Przykładem użycia może być opcja „tajność” – wykorzystywana do celów wojskowych, czy też „datownik” – do zapisywania czasów wzdłuż ścieżki.

Uzupełnienie – zależne od wybranych opcji, pole to zawiera bity zer, w ilości takiej by długość nagłówka była wielokrotnością 32 bitów (bo długość nagłówka zawiera wartość mierzoną w 32 bitowych jednostkach)

Protokół IP pozwala na komunikację pomiędzy dowolnymi hostami, definiuje sposób ich adresacji, lecz sam w sobie nie posiada żadnych mechanizmów ochronnych, które sprawdzają poprawność nawiązanej transmisji, dlatego koniecznym było użycie protokołów warstw wyższych, które powyższą ogromną wadę eliminującą.[1i][2][3]

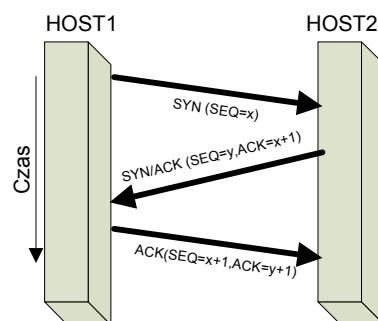
1.4 Protokoły TCP i UDP

Aby uodpornić przesyłaną przez protokół IP informację na wypadek utraty i zapewnić, że wysłane dane trafiły do celu - używany jest nadrzędny w stosunku do protokołu IP - protokół TCP (ang. *Transmission Control Protocol*).

| PORT NADAWCY | | PORT ODBIORCY | |
|---------------------|-----------|-------------------------|--------------|
| NUMER PORZĄDKOWY | | OKNO | |
| NUMER POTWIERDZENIA | | WSKAŹNIK PILNYCH DANYCH | |
| ZAREZ. | BITY KODU | OPCJE IP (jeśli są) | UZUPEŁNIENIE |
| SUMA KONTROLNA | | WSKAŹNIK PILNYCH DANYCH | |
| DANE | | UZUPEŁNIENIE | |
| ... | | ... | |

Rysunek 7 Opracowanie własne: Struktura nagłówka TCP

Ustanawiając połączenie TCP np. klient-serwer – musi być spełniony tzw. warunek „Three Way Handshake” (ang. *potrójny uściszk dłoni*) czyli przejść poprzez synchronizację sesji używając do tego celu pakietów synchronizacyjnych i potwierdzających. Każdy jeden pakiet otrzymuje numer sekwencyjny, który pomaga odbierającemu hostowi zsynchronizować i odbudować strumień pakietów w ich oryginalnie nadanym porządku.



Rysunek 8 Opracowanie własne: „Three Way Handshake”

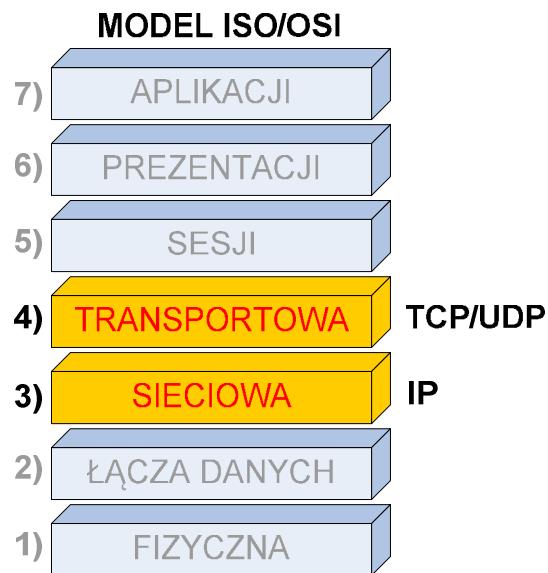
Warto zauważyć, że protokół TCP/IP – nie zawiera żadnych mechanizmów ochrony danych (choćby mechanizmu szyfrowania).

Ze względu na obecność numerów porządkowych i wysyłanych potwierdzeń - protokół TCP nosi często nazwę protokołu „połączniowego”, w przeciwieństwie do „bezpołączniowego” protokołu UDP (ang. *User Datagram Protocol*). Zatem wykorzystując protokół UDP nie ma żadnych gwarancji, że wysłany pakiet dotrze do odbiorcy (bynajmniej nie angażując do tego warstw wyższych modelu ISO/OSI).

| PORT UDP NADAWCY | PORT UDP ODBIORCY |
|------------------------|--------------------|
| DŁUGOŚĆ KOMUNIKATU UDP | SUMA KONTROLNA UDP |
| DANE | |
| ... | |

Rysunek 9 Opracowanie własne: Struktura nagłówka UDP

W nagłówkach pakietów TCP/UDP znajduje się również nr portu, który identyfikuje określoną usługę w sieci. Dzięki numerowi portu docelowego zdalna maszyna (np. serwer) po otrzymaniu pakietu stwierdza, do którego z programów nasłuchujących skierować otrzymane dane i co z nimi zrobić. [1i][2][3]



Rysunek 10 Opracowanie własne: Model ISO/OSI warstwa 3 (IP)
warstwa 4 (protokoły TCP/UDP i inne)

1.5 Sieci rozległe i metody dostępu

Internet jest globalną siecią złożoną z rozległych sieci WAN (ang. *Wide Area Network*), a te są złożone z jeszcze mniejszych struktur jakimi są sieci miejskie: MAN i lokalne: LAN (ang. *Metropolitan i Local Area Networks*). Połączenia między sieciami rozległymi realizowane są zwykle przez dostawców usług internetowych zwanych w skrócie ISP (ang. *Internet Service Provider*). W zależności od potrzeb i wymagań klienta, dostawcy stosują różne technologie dostępu do sieci, wśród których wyróżnić można:

| Nazwa | Metoda tworzenia kanału komunikacyjnego | Właściwości |
|----------------------------|---|---|
| POTS | | -Stała szybkość transmisji -Stała wartość opóźnienia -rezerwacja zasobów |
| ISDN | | |
| Linie dzierżawione | Komutacja obwodów | -gwarantowana przepływność -Dedykowana ścieżka dla ruchu pakietów – stała do czasu zakończenia transferu -cena |
| xDSL | | |
| T1,T3,E1,E3 inne | | |
| ATM | | -prędkość transmisji zależna od medium transmisyjnego i ścieżki pomiędzy kolejnymi urządzeniami tworzącymi połączenie |
| Ethernet | | |
| Bezprzewodowe sieci | | |
| Sieci kablowe | Komutacja pakietów | -opóźnienia mogą się zmieniać |
| FDDI | | |
| FrameRelay | | -możliwość przeciążania łączy |
| (SVC,PVC) | | -zapotrzebowanie na łącze może przekroczyć jego dostępność |
| X.25 | | |

| | | |
|--|--|---|
| | | -niższa cena niż przy technologii z komutacją obwodów |
|--|--|---|

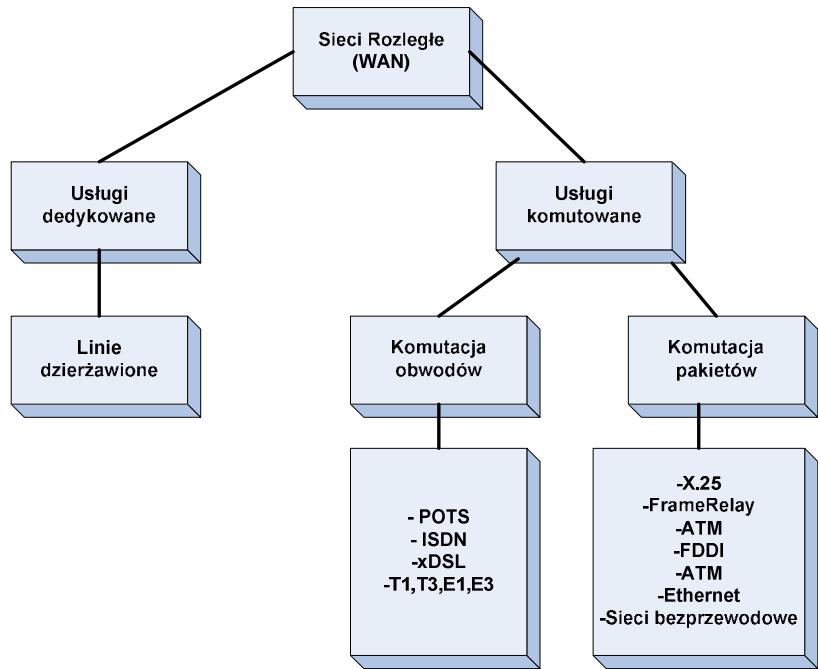
Tabela 3 Opracowanie własne: Metody i technologie dostępu do sieci rozległych [1i][2i][2][3]

Używając metody tworzenia kanału komunikacyjnego poprzez komutację obwodów – używany jest dedykowany kanał komunikacyjny pomiędzy dwoma lokalizacjami, wykorzystując do tego celu jeden lub więcej węzłów przełączających. Dane przesyłane są jako ciągły strumień, zachowując stałą szybkość transmisji danych, przy także stałej wartości opóźnienia, które jest uzależnione od czasu propagacji w danym medium transmisyjnym. Ścieżka, którą przesyłane są dane jest dedykowana i pozostaje do czasu zakończenia transferu. Jako przykłady sieci korzystających z komutacji obwodów zaliczyć można:

Łącza dzierżawione (ang. *Dedicated Line*), POTS (ang. *Plain Old Telephone System*) - analogowa linia telefoniczna, ISDN (ang. *Integrated Services Digital Network*) – sieć cyfrowa z integracją usług, czy sieci Carrier System : Sieci (T) – USA, (E)- Europa, czy popularne łączna xDSL.

Dla przykładu, usługa POTS na czas zestawienia połączenia między dwoma abonentami używa pary miedzianych przewodów w ramach jednej centrali, zaś jeśli potrzeba połączyć użytkowników dalej odległych, stosuje się centrale pośrednie. Na czas połączenia abonenci korzystają na stałe z tej samej ścieżki połączeń poprzez to samo medium transmisyjne.[2i][1i][2][3]

Technika komutowania obwodów zastępowana jest obecnie przez komutację pakietów (przełączanie pakietów) wykorzystująca maksymalnie dostępną infrastrukturę transportową, gdzie dostępne łącze współdzielone jest między użytkowników. Nie jest zestawiane dedykowane połączenie między lokalizacjami - urządzenie klienta nawiązuje połączenie z operatorem ISP. Możliwym jest istnienie wielu ścieżek prowadzących od źródła do celu transmisji, o różnych prędkościach, metrykach i opóźnieniach. Kolejno nadawane pakiety mogą być wysyłane inną drogą, zaś kolejność odbioru wcale nie musi być taka sama jak nadania. Przykładem sieci wykorzystujących technikę przełączania pakietów mogą być: Ethernet, sieci bezprzewodowe, FDDI, X.25, FrameRelay.[1i][2i][2][3]



Rysunek 11 Opracowanie własne: Podział sieci rozległych

Sieci bezprzewodowe

Wśród szeroko dostępnych usług oferowanych przez dostawców Internetu nie sposób nie wspomnieć o technologii dostępu bezprzewodowego. Wykorzystując dobrze już znane standardy 802.11a/b/g możliwym jest udostępnienie szybkiego Internetu praktycznie każdemu użytkownikowi nowoczesnego komputera przenośnego, palmtopa bądź też telefonu wyposażonego w moduł *WIFI*. Z uwagi na wykorzystanie fal elektromagnetycznych rozchodzących się w powietrzu jako medium transmisyjnego – sygnał taki trafia zarówno do osób, do których powinien trafić, ale i do osób trzecich, mogących stanowić zagrożenie dla podłączonych już użytkowników. Sieci bezprzewodowe wymagają zatem lepszego zabezpieczenia przed intruzami próbującymi podłączyć się do sieci niż sieci kablowe. Jako duży plus potraktować można mnogość możliwych zabezpieczeń sieci *WIFI*, począwszy od zabezpieczenia dostępu poprzez kontrolę adresów sprzętowych, użycie IPsec, silnych algorytmów szyfrujących transmisję (3DES, AES), czy też możliwość integracji z serwerami uwierzytelniającymi. Kolejnym czynnikiem jaki należy wziąć po uwagę kiedy planuje się korzystanie z sieci bezprzewodowej – jest stabilność sygnału. Fale elektromagnetyczne rozchodzące się wśród gęstej zabudowy miejskiej i obecności wielu zakłóceń (pochodzące nawet od sprzętu gospodarstwa domowego) często

powodują niestabilność transmisji danych lub jej całkowite zaniki. Klienci korzystający z sieci bezprzewodowych współzielą ze sobą dostępne pasmo, zatem może dojść do sytuacji wysycenia dostępnej przepustowości, kiedy liczba użytkowników wzrasta i tu pojawi się kolejny problem – gwarancji osiągalności zakupionego pasma oraz poziomu usług. Wspomniane wyżej wady dotyczą głównie ogólnie ogólnie dostępnych standardów 802.11 a/b/g, gdzie wykorzystywane do przesyłu danych są niekoncesjonowane pasma częstotliwości 2,4GHz i 5GHz. [1i][2i][2][3]

Sytuacja ma się zdecydowanie lepiej kiedy dostawcy usług bezprzewodowych korzystają z płatnych częstotliwości (3,5-3,7GHz, 10-30GHz) używając nowoczesnych technologii WIMAX, MMDS, LMDS, które pozwalają na bezpieczny(szyfrowany), stabilny przesył danych z dużymi prędkościami, na duże odległości, bez zakłóceń, z praktycznie stałym opóźnieniem i gwarancją jakości usług. Usługi takie dedykowane są jako stały dostęp do Internetu dla firm, bez możliwości przemieszczania się z odbiornikiem sygnału i anteną, co praktycznie uniemożliwia wykorzystanie takich rozwiązań dla mobilnych użytkowników.

Dobrym rozwiązaniem dla często przemieszczających się użytkowników chcących posiadać dostęp do sieci Internet – jest technologia wykorzystująca istniejącą infrastrukturę telefonii komórkowej GSM, dzięki której możliwa jest pakietowa transmisji danych – GPRS (ang. *General Packet Radio Service*) lub jej nowsze odsłony: EDGE (ang. *Enhanced Data Rates for GSM Evolution*), czy w końcu nowego standardu UMTS (ang. *Universal Mobile Telecommunications System*), nazywanego technologią trzeciej generacji . Jako, że sieć GSM, zaprojektowana jest tak, by pokryć swoim zasięgiem maksymalnie duży obszar terenu (dąży się by pokryć obszar całego kraju włącznie z terenami mało zaludnionymi), to i technologa przesyłania pakietowo danych także pokrywa ten zasięg (przynajmniej w teorii). Poważnym problemem użytkowników korzystających z dostępu do Internetu poprzez sieć GSM jest jej prędkość. Chociaż komputery przenośne wyposażone są często w modemy umożliwiające odbiór danych z prędkościami sięgającymi 7,2Mbit/s to faktycznie uzyskiwane transfery nie przekraczają 1-3Mbit/s w dużych miastach, a nieraz spadają do prędkości 20-50kbps na terenach pozamiejskich. Zatem dostęp do Internetu za pośrednictwem sieci GSM ma dość dobre pokrycie w skali całego kraju, jednak bardzo selektywne jeśli chodzi o uzyskiwanie szybszych prędkości pozwalających na swobodną pracę w każdych warunkach.

Brak na rynku tanich technologii pozwalających na bardziej uniwersalny i mobilny dostęp do globalnej sieci niż ten z użyciem GSM, czyni tę technologię bezkonkurencyjną mimo wad jakimi są cena, niestabilna prędkości i często duże opóźnienia propagacji.

Uslugi xDSL

Technologie cyfrowej linii abonenckiej - xDSL (ang. *Digital Subscriber Line*) zapewniają szybki przepływ danych (nawet i do 100Mbps przy odmianie VDSL2). Do realizacji transmisji danych wykorzystuje parę miedzianych przewodów. Typowa asymetryczna odmiana łącza ADSL (ang. *Asymmetric Digital Subscriber Line*) – przeznaczona zwykle do użytku domowego oferuje prędkości sięgające 15Mbit/s, które bardzo zależne są od długości miedzianych przewodów od urządzenia zakańczającego linię DSL – zwanego DSLAM, mieszczącego się w centrali operatora ISP, a modemem użytkownika. Asymetryczność polega na widocznej dysproporcji pomiędzy prędkością z jaką użytkownik może pobierać dane do prędkości z jaką może dane wysyłać. Za pomocą odmiany SDSL i HDLS można transmitować i odbierać dane z taką samą prędkością, gdyż jest to łącze symetryczne (max. transfer do/od abonenta wynosi 4Mbit/s przy odległości do 4 km).

Z pomocą usług xDSL operatorzy oferują stabilne i szybkie połączenie do Internetu z zachowaniem jakości usług (ang. *QOS – Quality Of Service*). Odmiana technologii ADSL – ze względu na asymetryczność – polecana jest użytkownikom domowym (prędkość nawet do 15Mbps), natomiast odmiany symetryczne SHDS, SDSL polecane są dla firm. Operatorzy ISP za pośrednictwem usług xDSL mogą udostępnić pulę publicznych, niezmiennych w czasie adresów IP, które wykorzystać można np. do budowy wirtualnych sieci prywatnych dla małych firm, gdyż prędkości jakich można się spodziewać używając symetrycznych odmian sięgającą 4Mbit/s. Wadą połączeń xDSL – jest brak gwarancji przepływności na określonym poziomie oraz umów SLA (ang. *Service Level Agreement*) [1i][2i].

Sieci operatorów kablowych i osiedlowych

Operatorzy telewizji kablowych CATV (ang. *Community Antenna TeleVision*) oferujących do niedawna tylko i wyłącznie przekaz audio-video, rozszerzyli swoją ofertę o stały dostęp do Internetu. Wykorzystując już istniejącą infrastrukturę kablową, a także modemy, możliwa jest dodatkowa transmisja cyfrowych danych. Uzyskiwane połączenie do Internetu zwykle jest stabilne, szybkie, lecz bez gwarancji możliwej do uzyskania prędkości (nawet i 6Mbit/s do klienta), tanie (jako dodatkowa usługa oprócz telewizji), jednak podobnie jak sieci Ethernet niezbyt bezpieczne, gdyż wykorzystywane medium jest współdzielone między wielu użytkowników, a ruch przesyłany tą drogą jest w większości przypadków nieszyfrowany. Sieci kablowe wykorzystywane są zwykle jako łączna stała dla prywatnych użytkowników, nie do komercyjnych zastosowań ze względu na brak możliwości zagwarantowania poziomu usług, brak umów SLA oraz brak usług dodatkowych jakimi pochwalić się mogą wszyscy zaufani operatorzy ISP, których głównym zadaniem jest dostarczyć sygnał Internetu [1i][2i].

FrameRelay i ATM

Łącza typu FrameRelay znajdują zastosowanie w sieciach rozległych WAN, do łączenia odległych sieci LAN. Możliwa transmisja danych z prędkościami, sięgającymi nawet 45Mbps. Węzły sieci FrameRelay nie dokonują korekcji błędów (w odróżnieniu od protokołu X.25), gdyż protokół z założenia wykorzystuje tylko dobry jakości łączą, gdzie taka korekcja nie jest potrzebna. W celu ustalenia komunikacji protokół FrameRelay tworzy logiczny obwód wirtualny. Wyróżnia się dwa typu takich obwodów:

- SVC (ang. *Switched Virtual Circuits*) – Przełączany obwód wykorzystywane, gdy transmisja danych odbywa się co jakiś czas, obwód jest rozłączany.
- PVC (ang. *Permanent Virtual Circuit*) Permanentny obwód stały – wykorzystywany, gdy transmisja danych między końcami jest stała. Obwód nie jest rozłączny

ATM (ang. *Asynchronous Transfer Mode*) – Dzięki wykorzystaniu protokołu możliwym jest przesyłanie dowolnych danych z dużymi prędkościami dochodzącymi nawet do 40Gbit/s zachowując przy tym stałą wartość opóźnień i poziom jakości usług.

Pakiety przesyłane są w formie mały równych porcji (53 bajty) – gdzie 48 bajtów to dane a kolejne 5 bajtów to nagłówek.

Pomiędzy stronami połączenia zostaje nawiązane logiczne połączenie tzw. kanał VCC (ang. *Virtual Channel Connection*). Kanały mające ten sam numer węzła docelowego tworzą wirtualną ścieżkę VPC (ang. *Virtual Path Connection*).

Użycie ścieżek VPN znacznie upraszcza zarządzanie całą siecią.

Protokół ATM nie zapewnia przepływu i korekcji błędów (w odróżnieniu od protokołu X.25), gdyż protokół z założenia wykorzystuje tylko dobrej jakości łączą, gdzie taka korekcja nie jest potrzebna. Jeśli podczas przesyłania komórek ATM nastąpią błędy – wtedy protokoły warstw wyższych muszą zadbać o retransmisję.

Technologie FrameRelay i ATM dają możliwość połączenia odległych sieci LAN za pomocą sieci WAN. Zapewniają transmisję danych z dużymi prędkościami oraz zachowaniem jakości usług, zarządzanie pasmem, a operatorzy sprzedający takie usługi umowy SLA. Dużą wadą wymienionych technologii jest niska cena [2i].[2][3]

Linie dzierżawione

Wykorzystywane zwykle przez większe firmy, do połączenia ze sobą oddalonych sieci LAN różnych oddziałów. Linie dzierżawi się od usługodawcy (ISP) jeśli oba oddalone końce połączenia są w jego zasięgu, lub też nawiązywana jest współpraca między operatorami, jeśli oddziały firmy znajdują się poza terenem działalności jednego dostawcy. Do realizacji linii dzierżawionych wykorzystywane są różne technologie i typy połączeń: np. miedziany drut i para modemów SDSL, HDSL (prędkość do 8Mbit/s, zasięg do 4km), dzierżawa włókien światłowodowych (prędkość nawet 1Gbit/s, zasięg od kilku do kilkuset kilometrów), technologie bezprzewodowe (WIMAX MMDS LMDS i inne, dające zasięg nawet i 30-40 km, a prędkości do 50Mbps). Możliwa jest także dzierżawa linii dedykowanych w oparciu o usługę MPLS (prędkość możliwa do uzyskania nawet kilkaset Mbit/s), oraz linie FrameRelay (typowa prędkość 2Mbit/s) lub ATM (nawet 40Gbit/s) jednak często połączenie takie nie jest połączeniem fizycznym, a jedynie stałym bądź nie - logicznym kanałem transmisyjnym PVC lub SVC (ang. *Permanent lub Switched Virtual Circuit*).

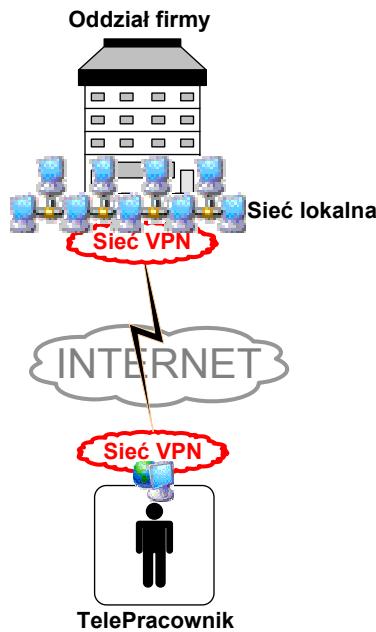
Wszystkie możliwe warianty linii dzierżawionych mają pewne cechy wspólne, do których zaliczyć można: podniesiony poziom bezpieczeństwa (często także przez

szyfrowanie już w warstwie sprzętu samego operatora ISP), gwarancje osiąganej przepływności (zwykle duże przepustowości), opóźnień propagacji, umowy SLA (procentowy poziom dostępności łącza w skali roku, czas reakcji na awarie i inne warunki umowy). Połączenia oddziałów między, którymi istnienie linia dedykowana (dzierżawiona) – są jednak najdroższe ze wszystkich możliwych wariantów połączeń, tym droższe – im większa odległość między końcowymi lokalizacjami i im większa wymagana prędkość transmisji. Wada ta czyni linie dzierżawione praktycznie niedostępnymi dla mniej zasobnych firm[1i].

1.6 Dostęp zdalny do zasobów sieci lokalnych

Idealną sytuacją jest taka, kiedy do dyspozycji korporacji przeznaczona jest dedykowana linia dzierżawiona łącząca oddalone oddziały firmy. Zachowane jest wtedy wysokie bezpieczeństwo przesyłanych danych (o ile obdarzy się zaufaniem dostawcę usług realizującego połączenie dzierżawione), wysoka i stała prędkość transmisji, a także gwarancje w postaci umów SLA na wypadek awarii. Niestety na podobny scenariusz mogą sobie pozwolić tylko nieliczne firmy, a w interesie znakomitej większości jest obecnie ograniczanie największych kosztów (jakimi z pewnością są miesięczne opłaty związane z dzierżawieniem linii).

Implementując wirtualne sieci prywatne – możliwym jest połączenie sieci lokalnych dowolnie oddalonych oddziałów firmy (odległość nie wpływa na finalną cenę połączenia) ze sobą w sposób przezroczysty dla użytkowników, z zachowaniem dużej prędkości transmisji, umów SLA oraz co ważniejsze bardzo dużego poziomu bezpieczeństwa przesyłanych danych. Bezpieczeństwo w tym przypadku jest o tyle istotną sprawą, gdyż dane przesyłane są poprzez sieć Internet, gdzie narażone są na niebezpieczeństwa. Możliwa do uzyskania prędkość transmisji pomiędzy lokalizacjami oraz gwarancja poziomu usług (SLA) i transmisji zależna jest przede wszystkim od dostawcy usług internetowych od jakiego wykupione zostanie łącze do Internetu w jednej i drugiej (zdalnej) lokalizacji.



Rysunek 12 Opracowanie własne: Zdalny dostęp

Sieci VPN stosuje się zwykle do zbudowania logicznego połączenia pomiędzy oddziałami firmy i zasobami ich sieci lokalnych, po to by pracownicy znajdujący się w tych oddziałach mogli bez przeszkód i bezpiecznie wymieniać się danymi. Istnieje jednak wariant połączenia VPN, kiedy to drugą stroną połączenia - nie jest fizyczna lokalizacja (budynek, a w nim aktywne urządzenia sieciowe), lecz zdalny pracownik (jego komputer). Połączenie takie można przyrównać do wybudowanej linii dzierżawionej łączącej lokalną sieć oddziału firmy z komputerem pracownika – czyli miejscem, gdzie aktualnie się znajduje (czy we własnym domu, czy też np. w hotelu w obcym państwie). Pracownik taki naturalnie posiadać musi dostęp do Internetu, używając do tego celu dowolnej dostępnej technologii dostępu. Bezpieczeństwo połączenia zdalnego zapewnione jest przez zestaw odpowiednich protokołów, algorytmów i oprogramowania. Prędkość tak nawiązanej komunikacji z firmowymi zasobami w zasadzie zależy będzie od jakości połączenia do sieci Internet – po stronie pracownika.

Uzyskując zdalnie dostęp do firmowej sieci lokalnej, praktycznie bez żadnej zmiany konfiguracji sieci hosta – telepracownik może bez ograniczeń korzystać ze wszystkich zasobów jakie dostępne są na miejscu w oddziale firmy:

- ✓ Poczta elektroniczna

- ✓ Aplikacje bazodanowe
- ✓ Strumienie audio-wideo (np. telefonia VOIP)
- ✓ Współdzielenie plików
- ✓ Komunikatory sieciowe
- ✓ Wewnętrzne aplikacje CRM
- ✓ Drukowanie/skanowanie
- ✓ Podpis elektroniczny i szyfrowanie danych
- ✓ Zarządzanie usługami, serwerami oraz sprzętem aktywnym

Mając dostęp do wymienionych usług sieciowych, nie będąc na miejscu w biurze, można praktycznie w 100% realizować swoją aktywność zawodową.

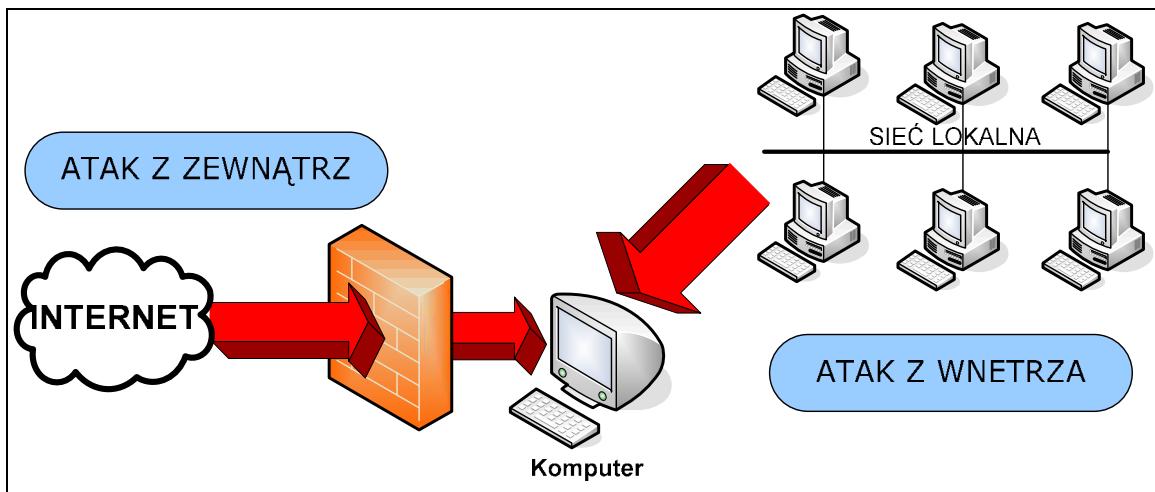
Dostęp zdalny dla pracowników to także szereg innych korzyści dla firmy:

- Zwiększenie wydajności pracy
 - Pracownicy stali i czasowi mogą realizować zadania nawet kiedy są nieobecni przy swoich stanowiskach pracy.
 - Pracownicy często deklarują chęć pracy przez więcej godzin dziennie niż by przebywali w biurze w zamian za możliwość wykonywania obowiązków z domu przy rodzinie.
 - Osoby pracujące na stanowiskach kierowniczych i administracyjnych mogą odpowiadać szybciej w przypadku awarii, a także odpowiadać na mniej krytyczne zgłoszenia, nie odkładając ich do dnia następnego dnia roboczego.
- Obniżenie kosztów
 - W środowiskach biznesowych, w których pracownicy mogą pracować zdalnie na co dzień np. konsulting IT, firma zatrudniająca może pozwolić sobie na zmniejszenie powierzchni biurowej, oszczędzić kosztów wynajmu, ogrzewania, elektryczności.
 - Obniżenie kosztów utrzymania biura pozwala na obniżenie kosztów usług lub towarów oferowanych przez firmę, przez co przedsiębiorstwo takie staje się bardziej konkurencyjne
- Zapewnienie ciągłości biznesowej
 - Pracownicy mogą wykonywać swoje obowiązki nawet w sytuacji kryzysowej np. sytuacji pogodowej

- Możliwość natychmiastowego wykorzystania wszystkich zdalnych pracowników w przypadku sytuacji awaryjnej
- Szansa dla ludzi niepełnosprawnych:
 - Pracownicy niepełnosprawni np. z niedowładem kończyn dolnych, bądź uszkodzeniem np. jednej z rąk mogą być traktowani jako w pełni sprawni w pracy, bez konieczności wychodzenia z domu i borykania się utrudnieniami komunikacyjnymi.
 - Osoby okaleczone, wstydzące się swojego wyglądu mogą na stałe i komfortowo pracować zdalnie .
 - Zdalny dostęp jest szansą na dalszą pracę dla ludzi wieloletnie wykonujących swoje obowiązki, którzy ulegli nagle wypadkowi a chcą kontynuować swoją pracę.
 - Zdalny dostęp z domu jest szansą na rozwój zawodowy i godziwe wynagrodzenie.[1]

2 Zagrożenia przesyłanych danych poprzez sieci publiczne

Ze względu na bardzo dynamiczny rozwój Internetu oraz coraz to częstsze wykorzystywanie do celów komercyjnych stało się jasne, że niezbędne jest położenie większego niż do tej pory nacisku na kwestie bezpieczeństwa. Firmowe dane transmitowane w sieci Internet bez właściwej kontroli i zabezpieczeń, narażone są na różne typy niebezpieczeństw. Zanim zaprojektuje się bezpieczną sieć należy zaznajomić się z możliwymi zagrożeniami jakie mogą czyhać zarówno w publicznie dostępczej sieci Internet (sieć zewnętrzna) jak i od strony sieci wewnętrznej – by móc im przeciwdziałać i chronić ją przed niepowołanymi osobami.



Rysunek 13 Opracowanie własne: Źródła ataku

Najczęściej wykorzystywanym dziś protokołem transmisji danych jest protokół TCP/IP wersja 4 (IPv4), który nie jest wyposażony w żadne mechanizmy utajniające czy też szyfrujące przenoszone dane. Przesyłanie ich w sposób jawnny - daje szanse na przechwycenie wrażliwych danych przez osoby trzecie. Problem szyfrowania danych w warstwie sieciowej i transportowej modelu ISO/OSI możliwy będzie do rozwiązania przy okazji wdrożenia kolejnej odsłony protokołu TCP/IP - wersji 6 (IPv6).

2.1 Podsluch danych

Podłusch danych (ang. *Sniffing*) Przechwycenie i analiza pakietów sieciowych, za pomocą odpowiedniego oprogramowania (tzw. analizatory pakietów), zwykle wykorzystywane jest przez administratorów sieci LAN – do rozwiązywania problemów. Jednak często narzędzie takie wykorzystywane jest przez osoby niepowołane – wtedy może służyć do podsłuchiwanego danych jakie docierają do innych komputerów podpiętych do segmentu sieci opartego głównie o koncentratory (ang. *Hub*) lub przełączniki (ang. *Switch*). Atakujący używa specjalnego trybu pracy karty sieciowej w trybie nasłuchu (ang. *promiscous*), po to by przechwycić cały ruch jaki jest kierowany do hostów z sieci LAN. Następnie za pomocą specjalnych analizatorów sieciowych jest w stanie podejrzeć interesujące go dane. Dobrym przykładem może być próba przechwycenia sesji HTTP użytkownika – kiedy to dane z formularzy (np. login i hasło do poczty) ze strony WWW, przesyłane są zupełnie otwartym tekstem. Kolejnym

dobrych przykładem jest podsłuch komunikatorów internetowych, czy też próba logowania się do serwera TELNET czy FTP.[1i]

2.2 Podsywanie się

Osoba atakująca udaje (podsywa się) pod „legalnego” użytkownika, aby np. ominąć zabezpieczenia dostępu do zdanego systemu informatycznego – które polegają na weryfikacji próbującego podłączyć się adresu IP.

Podsywanie się (ang. *Spoofing*) to zafałszowanie źródłowego adresu IP (bądź też adresu fizycznego), po którym to identyfikowany jest komputer. Serwer przeprowadzający inspekcję źródłowego adresu IP, wysyła na podstawie zapisu w nagłówku TCP/UDP zapytanie zwrotne. Wadą protokołu TCP/IP jest to, że możliwa jest modyfikacja pola „adres źródłowy” (patrz rozdział protokół IP) i w odpowiedzi można wysłać dowolny adres, który będzie przez serwer przyjęty jako wiarygodny - nawet adres IP wskazujący na komputer wewnętrz atakowanej sieci.

Kolejnym etapem ataku poprzez spoofing IP może być tzw. „dns spoofing” czyli udawanie przez komputer atakującego - serwera dns, udzielając pytającemu hostowi błędna odpowiedź na zapytanie o adres IP nazwy domenowej.

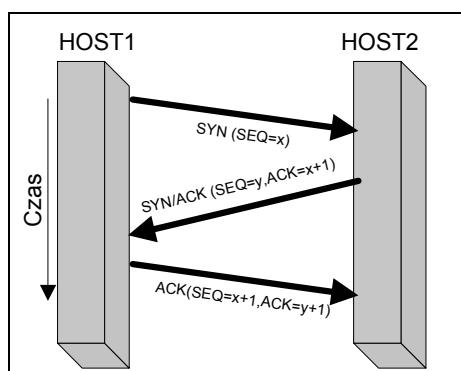
Przykład: host pytając o nazwę onet.pl otrzyma od fikcyjnego serwera dns – adres IP wskazujący na komputer włamywacza zamiast prawdziwego adresu IP:213.180.130.200. [1i]

2.3 Łamanie haseł

Próba odgadnięcia cudzego hasła (ang. *Cracking*) poprzez np. atak słownikowy. Jeśli aplikacja bądź system informatyczny nie jest odpowiednio zabezpieczony, atak słownikowy często ma szansę się powieść - zakłada bowiem, że użytkownik budowę swojego hasła oparł na bazie szeroko dostępnych wyrazów z życia codziennego. W ten sposób wykorzystując zwykle ogólnie ogólnie dostępną aplikację służącą do autoryzacji użytkownika – kolejno podstawiając atakujący eliminuje możliwe wyrazy ze skończonego słownika.[1i]

2.4 Przejęcie sesji

Przejęcie sesji (ang. *Hijacking*) wykorzystuje niedoskonałości omówionego wcześniej protokołu TCP/IP, gdyż możliwym jest przerwanie już nawiązanej sesji TCP pomiędzy dwoma hostami np. klientem a serwerem. Włamywacz podszywając się pod klienta, poprzez spoofing jego adresu IP oraz modyfikacji nagłówka TCP tak by zawierał poprawny numeru SEQ/ACK – serwer traktuje włamywacza tak jak by on był właściwym klientem kontynuującym sesję.



Rysunek 14 Opracowanie własne: „Three Way Handshake”

W ten sposób można doprowadzić do destabilizacji sesji już istniejącej (serwer-host) a kontynuowaniu sesji (serwer-atakujący). Klient próbując kontynuować sesję TCP z już nieaktualnym numerem SEQ/ACK – zostaje przez serwer odrzucony.

Jako, że zwykle uwierzytelnianie klient-serwer (np. WWW) jest potrzeba tylko na początku połączenia, to już ustanowione połączenie (po autentykacji) może zostać „uprowadzone”. Przejęcie sesji może być zrealizowane za pomocą dwóch metod:

Man in the Attack (Tłumaczając dosłownie: „człowiek po środku”) - Atakujący jest cały czas obecny i pośredniczy w wymianie ruchu pomiędzy właściwymi hostami. Mogąc modyfikować dowolnie transmisję

Blind Attack (tłumaczając dosłownie: ślepy atak) - Atakujący próbuje odnaleźć numery sekwencyjne, których oczekuje serwer, tak by nawiązać z nim połączenie). [1i]

2.5 Odmowa usługi

Atak typu odmowa usługi (ang. *Denial Of Service*) – możliwy jest np. poprzez nawiązanie bardzo dużej liczby połączeń do atakowanego serwera, której nie jest on w stanie ich poprawnie obsłużyć doprowadzając do wyczerpania jego zasobów. Często wysyłane pakiety IP mają błędную konstrukcję, bądź też mogą mieć zmodyfikowane pole źródłowego adresu IP doprowadzając do chwili kiedy serwer będzie starał się odpowiedzieć hostowi, który wcale nie nawiązywał połączenia z atakowanym serwerem. [1i]

2.6 Błędy w oprogramowaniu

Skrypty, które wykorzystują luki w programie dzięki czemu możliwym jest przejęcie kontroli nad danym procesem systemu operacyjnego, lub też uzyskanie uprawnień administratora systemu, zwykle wykorzystując do tego celu technikę przepelnienia bufora.[1i]

2.7 Złośliwy kod

To grupa zwykle destruktywnych programów (ang. *Malware*), które mogą w negatywny sposób wpływać na działanie komputera i bezpieczeństwo danych na nim się znajdujących. Do najpopularniejszych programów tego typu zaliczyć można:

Wirusy – fragment kodu programu, zdolny do samoczynnego doklejania własnej struktury do istniejących programów – w ten sposób przenosi się powodując infekcję kolejnych komputerów. Działanie wirusów często nie ogranicza się tylko do samodzielnego rozprzestrzeniania, lecz często niesie ze sobą poważniejsze skutki – jak działania destrukcyjne na danych.

Robaki Internetowe – podobnie jak wirusy posiadają możliwość samoreplikacji i rozprzestrzeniania – jednak za pośrednictwem poczty elektronicznej bądź sieci komputerowych.

Konie trojańskie – zwykle nie posiadają możliwości kopiowania własnego kodu programu ani doklejania go do innych programów, jednak mogą stanowić furtkę dla

włamywacza, który bez problemu uzyska dostęp do danych znajdujących się na komputerze, gdzie uruchomiony jest koń trojański

Spyware – to zwykle programy, które podczas swojego działania - zbierają informacje o użytkowniku komputera, po to by w późniejszym czasie wysłać je bez wiedzy użytkownika do sieci Internet (zwykle do autora oprogramowania *spyware*, bądź organizacji, która takie programy napisała).[1i]

3 Procesy bezpieczeństwa

3.1 Polityka bezpieczeństwa firmy

Każda organizacja, by działać bezpiecznie i efektywnie - potrzebuje ścisłych przepisów regulujących politykę bezpieczeństwa, dzięki czemu we właściwy sposób można chronić zasoby i kapitał firmy. Zabezpieczenia powinny być zastosowane w pierwszej kolejności do ochrony zasobów stanowiących najistotniejszą wartość dla przedsiębiorstwa oraz tych zasobów, dla których istnieje duże zagrożenie i które są na to zagrożenie podatne. W zakresie zabezpieczeń technicznych istotnym dokumentem w tym zakresie jest RFC 2196 o nazwie „Site Security Handbook”.[1d]

Polityka bezpieczeństwa to zestaw reguł jakie powinien znać i przestrzegać każdy pracownik korporacji – bez względu na zajmowane stanowisko.

Decyzja wprowadzenia polityki bezpieczeństwa powinna zostać podjęta przez zarząd firmy, a jej treść zostać sformułowana w porozumieniu wszystkich pracowników, których procedura będzie dotyczyła.

Główną zasadą, którą należy kierować się tworząc dokumenty związane z bezpieczeństwem brzmi: „Zabronione jest wszystko, co nie zostało w sposób jasny wcześniej dozwolone”.

Polityka bezpieczeństwa informatycznego jest potrzebna w każdej firmie, gdyż:

- ✓ Tworzy linię odniesienia do aktualnego poziomu bezpieczeństwa (audyt)
- ✓ Ścisłe definiuje jakie zachowania użytkowników są dozwolone a jakie nie
- ✓ Pomaga definiować role i zakres odpowiedzialności użytkowników
- ✓ Definiuje konsekwencje nadużycia

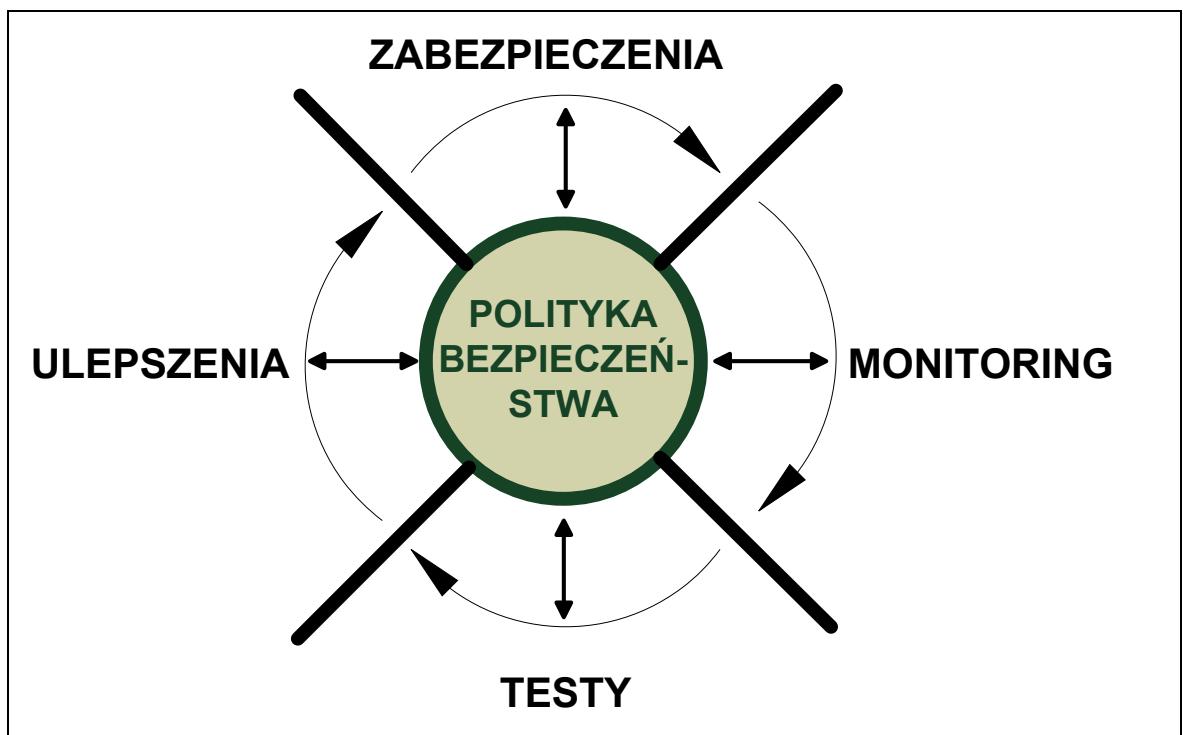
- ✓ Definiuje jak traktować incydenty bezpieczeństwa
- ✓ Definiuje proces zarządzania zmianami
- ✓ Reguluje zasady dostępu do sieci Internet i zasobów zdalnych
- ✓ Reguluje zasady dostępu zdalnego do sieci firmowej
- ✓ Reguluje proces autoryzacji użytkowników
- ✓ Reguluje zasady tworzenia i przechowywania haseł
- ✓ Zasady korzystania sprzętu komputerowego i aplikacji
- ✓ Ustala zasady bezpieczeństwa fizycznego (dostępu do pomieszczeń)
- ✓ Definiuje procedurę DRP (ang. *Disaster Recovery Plan*) – czyli process odbudowy po „katastrofie” [6]

3.2 Bezpieczeństwo sieci

Główym wyzwaniem a zarazem problemem implementacji bezpiecznych sieci informatycznych jest kwestia – jak ułatwić dostęp do systemów informatycznych (by sprostać nowym wymaganiom rynku) a z drugiej strony potrzebą ochrony tych samych systemów przed atakami z zewnątrz jak i wewnętrz sieci. Problem jest o tyle trudny do rozwiązywania, że coraz częściej dostęp do wrażliwych danych formowych musi być możliwy także z sieci Internet, a im większa potrzeba dostępu do publicznej sieci – tym bardziej trudniej chronić korporacyjną sieć i użytkowników przed niepowołanymi osobami, a także konieczne są większe nakłady finansowe, by bezpieczeństwo sieci zapewnić na wymaganym poziomie. [1][6][1d]

3.2.1 „Koło bezpieczeństwa”

Przy rozwiązywaniu powyższego problemu służyć może tzw. koło bezpieczeństwa, czyli cykl nieustannych procesów, które muszą zachodzić w organizacji by utrzymać wymagany poziom bezpieczeństwa.



Rysunek 15 Opracowanie własne : Koło bezpieczeństwa [3][1d]

Krok pierwszy „Zabezpieczenia” – Implementacja zabezpieczeń w postaci: firewalli, systemów identyfikacji i autoryzacji użytkowników, szyfrowanie danych – i inne procesy mające zabezpieczyć przed nieautoryzowanym dostępem do sieci.

Krok drugi „Monitoring” – Ciągłe monitorowanie sieci w poszukiwaniu naruszeń bezpieczeństwa

Krok trzeci „Testy” – Analiza podatności systemów informatycznych, urządzeń, aplikacji na nowe typy zagrożeń i ataków.

Krok czwarty „Ulepszenia” – Na podstawie zebranych informacji i analizy kroków poprzednich, możliwe jest podniesienie poziomu bezpieczeństwa sieci.

„Koło bezpieczeństwa” – jest procesem, który nie skończy się nigdy, gdyż jest ściśle powiązany z rozwojem technologicznym sprzętu i oprogramowania.[6] [3][1d]

3.2.2 Bezpieczeństwo urządzeń i hostów sieciowych

Pod pojęciem bezpieczeństwa sieci kryje się tak naprawdę problem bezpieczeństwa każdego urządzenia jakie tworzy daną sieć, zatem osobno należy rozpatrywać grupę

urządzeń aktywnych a osobno grupę urządzeń końcowych jakimi są komputery i serwery.[1][6][[1d]

Z punktu widzenia bezpieczeństwa sieci, bardzo ważnym elementem jest etap doboru oprogramowania instalowanego na stacjach roboczych oraz serwerach. Począwszy od systemu operacyjnego, programu antywirusowego (mającego chronić przed złośliwym oprogramowaniem) , aż po programową ścianę ogniorę (firewall) – mającą chronić komputer bądź serwer przed atakami z wewnętrz i zewnętrz sieci. Dodatkowym oprogramowaniem podnoszącym poziom bezpieczeństwa - instalowanym na komputerze może być system wykrywania intruzów urządzeń końcowych tzw. HIPS (ang. *Host-Based Intrusion Detection*), który pełni rolę programowej sondy – będącej w stanie wykryć próbę ataku sieciowego i podjąć akcję (w zależności od producenta oprogramowania) informacyjną (do nadzorującego serwera) bądź prewencyjną – tworząc regułę na programowej ścianie ogniorę.

Kolejnym etapem zabezpieczenia stacji roboczych bądź serwerów może być szyfrowanie danych znajdujących się na dysku twardym komputera – co utrudni bądź uniemożliwi odczytanie danych przez osoby trzecie na wypadek kradzieży sprzętu.

Podobnie jak w przypadku urządzeń końcowych (stacje robocze i serwery) tak w przypadku sieci stosuje się systemy detekcji intruzów. Przykładem mogą być sondy IDS/IPS (ang. *Intrusion Detection system, Intrusion Prevention System*) lub też sondy mające postać programu zainstalowanego na systemie operacyjnym np. „Snort”. Działanie sond polega na wykrywaniu anomalii w ruchu sieciowym w stosunku do nauczonego wcześniej wzorca zachowań. W zależności od konfiguracji i możliwości sonda – taka może raportować do serwera nadzorującego o zaistniałej podejrzanej sytuacji, bądź też dać odpowiednią instrukcję dla zapory sieciowej (firewalla), aby podejrzany rodzaj ruchu sieciowego zablokować.

Omawiając temat bezpieczeństwa urządzeń i hostów sieciowych warto wspomnieć o serwerach realizujących funkcje uwierzytelniania, autoryzacji, kontroli dostępu oraz zliczania ruchu – w skrócie AAA (ang. *Authentication, Authorization, Accounting*). Serwer pełniący w/w role – nadzoruje kto (użytkownik, urządzenie) ma prawo dostać się do danego zasobu sieci (bądź urządzenia) oraz na jakich zasadach. Szczegółowo o serwerach pełniących rolę AAA w następnych rozdziałach (patrz „model AAA”).

[1][6][[1d]

4 Zabezpieczenie danych przesyłanych przez sieć publiczną

Aby uniemożliwić bądź też znaczco utrudnić przechwycenie czy zmodyfikowanie transmisji danych wewnątrz sieci przedsiębiorstwa, lub też podczas transmisji w sieć publiczną – wymagany jest dobór odpowiednich metod - czyli protokołów, pozwalających na poufną, szyfrowaną wymianę informacji, sprawdzanie czy dane nie zostały w jakkolwiek sposób zmodyfikowane (sprawdzenie integralności) oraz czy nadawca informacji jest tym za kogo się podaje. Niestety tylko nieliczne protokoły pozwalają na zapewnienie takiej ochrony, dlatego też często stosuje się połączenie właściwości kilku z nich, aby uzyskać wymagany poziom bezpieczeństwa.

Do najczęściej stosowanych protokołów pozwalających na zabezpieczenie (w mniejszym bądź większym stopniu) przesyłanych danych należą: L2TP, PPTP, L2F, IPSec oraz działające w warstwach wyższych modelu referencyjnego ISO/OSI : PGP, SSL/TLS, S/MIME oraz SSH. Protokoły te różnią się od siebie zarówno architekturą jak i możliwością zastosowania. Stosowanie w niektórych protokołach silnych algorytmów kryptograficznych podczas wymiany informacji pozwala na uniknięcie wielu odmian ataków, między innymi: spoofing, DOS, hijacking , sniffing (omówione wcześniej w rozdziale 2 „Zagrożenia przesyłanych danych poprzez sieć publiczną”).

4.1 Sieci VPN

Ochrona danych przesyłanych w sieci Internet sprowadza się przede wszystkim do tworzenia wirtualnych sieci prywatnych (ang. *Virtual Private Network*). Idea funkcjonowania sieci VPN polega na tworzeniu wydzielonych, logicznych kanałów transmisji danych w ramach sieci rozległej (np. Internet) - tak, aby dane przesyłane za pośrednictwem tych kanałów zostały zabezpieczone w zakresie:

- Poufności

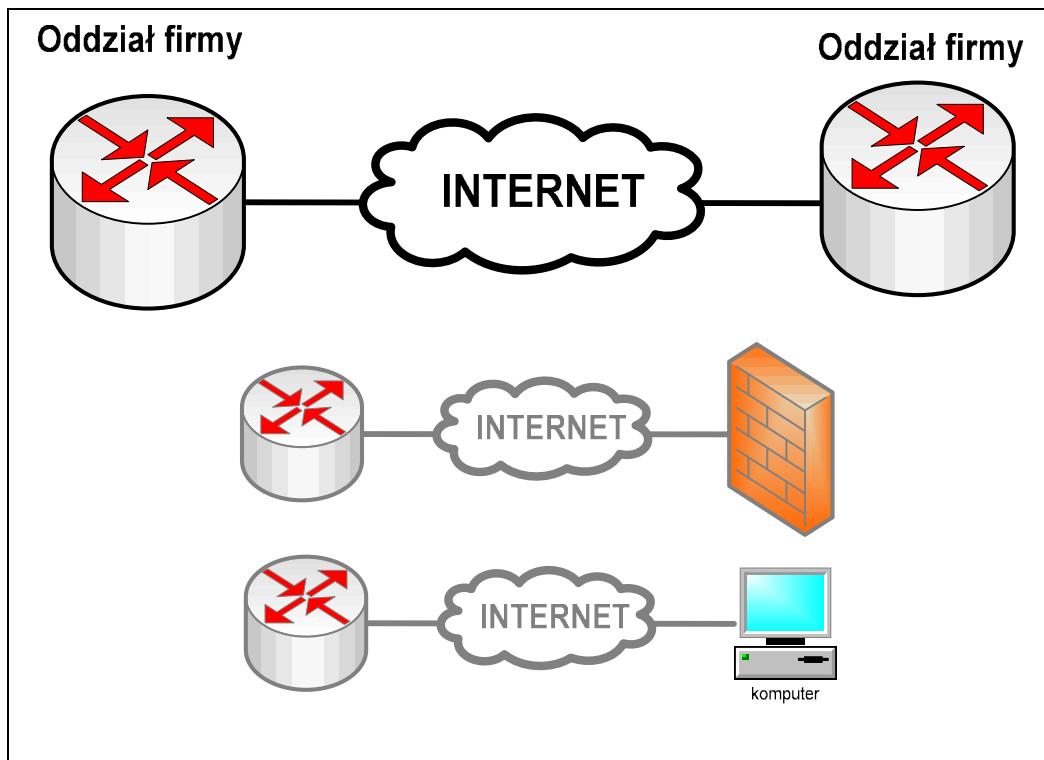
- Autentyczności
- Integralności

Zabezpieczenie danych w sieci VPN realizowane jest za pomocą technik kryptograficznych.

Dzięki połączeniom VPN w sieci Internet, geograficznie oddalone od siebie oddziały firmy mogą mieć ze sobą kontakt, tak jak by dzieliła je jedynie ściana w tym samym budynku, nie płacąc przy tym ogromnych kosztów związanych z dzierżawieniem od usługodawcy (ang. *Internet Service Provider*) linii dedykowanej (cenowo zależnej od prędkości i odległości), a jedynie za dostęp do Internetu o określonych parametrach.[1][6][2i]

4.1.1 VPN typu „*Site-to-Site*”

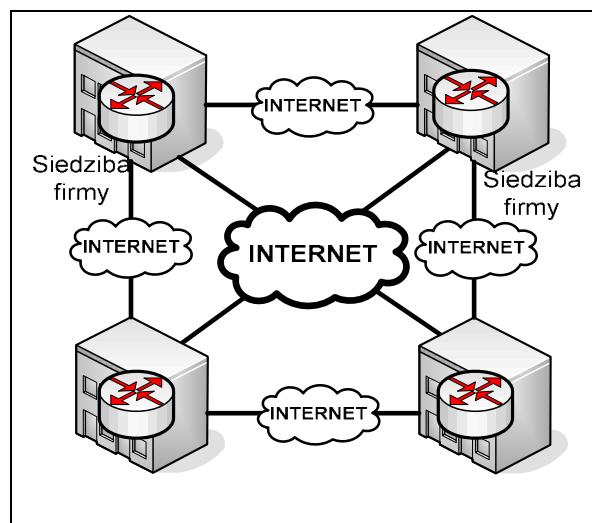
Typ połączeń VPN, gdzie poprzez logiczny kanał transmisji skomunikowane są ze sobą zdalne lokalizacje (oddziały firmy) nosi nazwę: *Site-to-Site* (tłumacząc dosłownie „oddział-do-oddziału”). Istotnym jest by zapamiętać, że logiczne kanały transmisyjne otwierane są i zamkane przez urządzenia brzegowe, do których możemy zaliczyć: routery, ściany ogniowe (firewalle), ale także i komputery końcowych użytkowników.



Rysunek 16 Opracowanie własne: VPN *Site-to-Site*

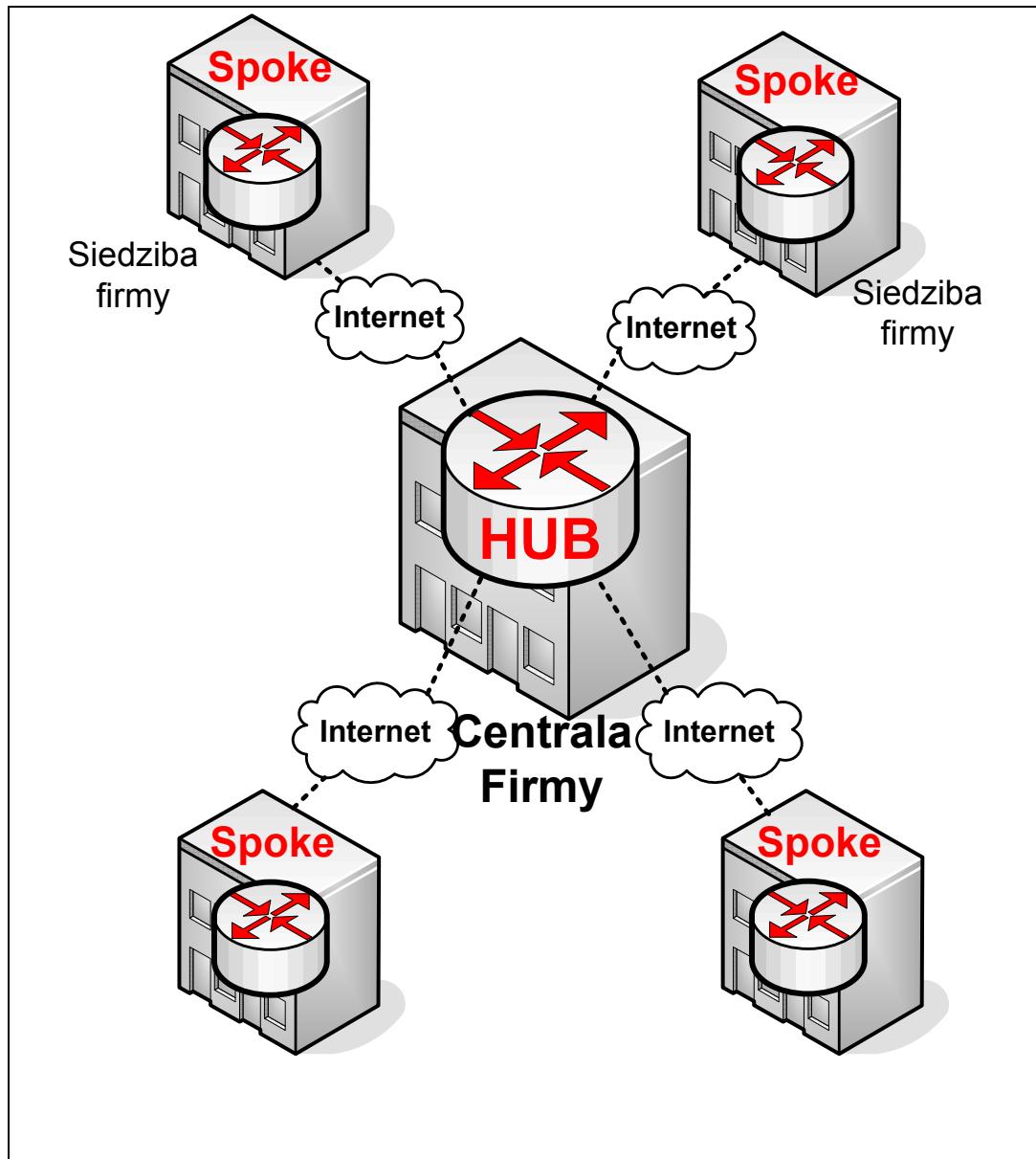
Wśród połączeń VPN typu *Site-to-Site* dokonać można kolejnego podziału, ze względu na topografię połączeń:

- Topologia *Mesh* – czyli połączenie ze sobą tunelami VPN wszystkich urządzeń granicznych (w komunikacji VPN) na raz. Stosowane zwykle tam, gdzie kładziony jest nacisk na maksymalną niezawodność połączeń. Wadą jednak jest dość kłopotliwa administracja przywiększej ilości urządzeń.



Rysunek 17 Opracowanie własne: Topologia "Mesh"

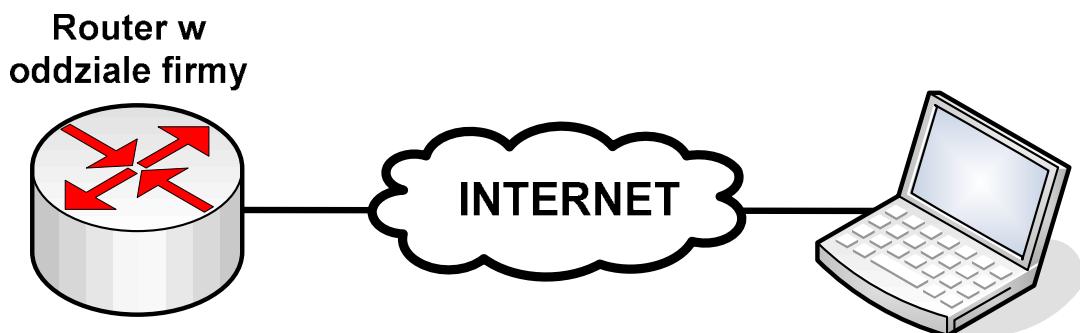
- Topologia *Hub & Spoke* – czyli topologia “gwiazdy” – gdzie wyróżnione są urządzenia centralne (Hub) – pośredniczące w połączeniach VPN między pozostałymi urządzeniami (Spoke) w oddziałach.



Rysunek 18 Opracowanie własne: VPN Topologia Hub & Spoke

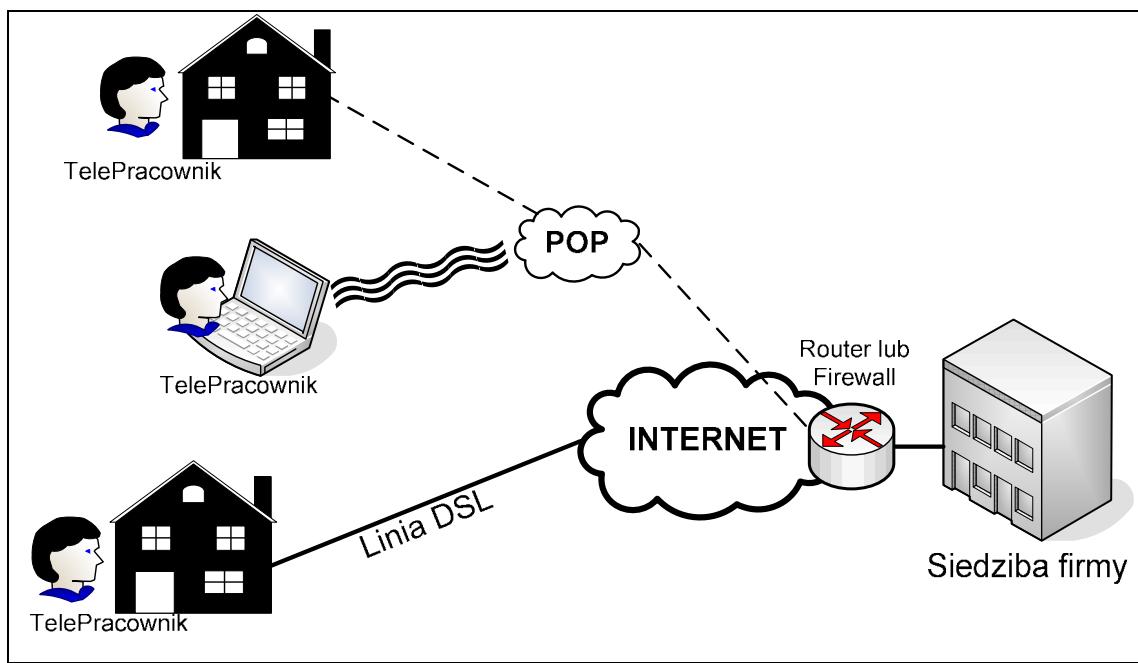
Możliwe jest także połączenie mieszane – wykonane przy użyciu topologii *Mesh* i *Hub & Spoke* na raz – kiedy to wykonanych zostanie więcej niż jeden punkt centralny (Hub) oraz ustanowionych zostanie kilka połączeń VPN z urządzeń granicznych do punktów centralnych. Wykorzystanie obu topologii na raz pozwala na podwyższenie poziomu niezawodności połączeń VPN typu *Site-to-Site*. [1][6][[2i]]

4.1.2 VPN typu „Remote Access”



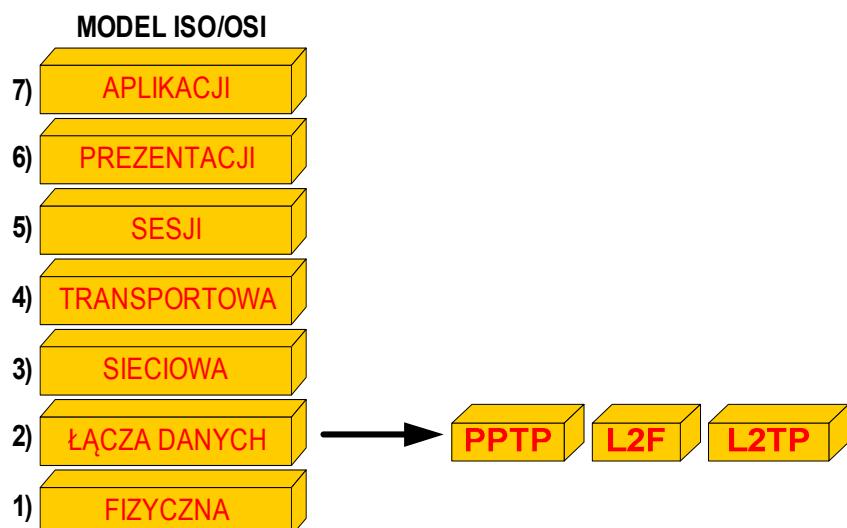
Rysunek 19 Opracowanie własne: VPN client-to-site

Sieci VPN to nie tylko bezpieczne połączenie zdalnych oddziałów firmy, lecz coraz częściej połączenie oddziału z mobilnymi pracownikami – czyli tzw. zdalny dostęp (ang. *Remote Access*). Telepracownik wyposażony w przenośny komputer oraz własne łącze do sieci Internet (np. poprzez sieć GSM, *WIFI*, czy też popularne łącza DSL) – również może nawiązać bezpieczną komunikację z wewnętrznymi zasobami korporacji tworząc logiczny kanał transmisji (VPN) za pomocą zainstalowanego odpowiedniego oprogramowania. Typ połączeń VPN, w którym zdalny pracownik ustanawia logiczny kanał transmisji do oddziału firmy określany jest jako *Client-To-Site* (dosłownie klient-do-oddziału).



Rysunek 20 Opracowanie własne: VPN - Zdalny dostęp

4.2 Warstwa druga modelu ISO/OSI: PPTP, L2F, L2TP



Rysunek 21 Opracowanie własne: Protokoły PPTP,L2F,L2T a Model ISO/OSI

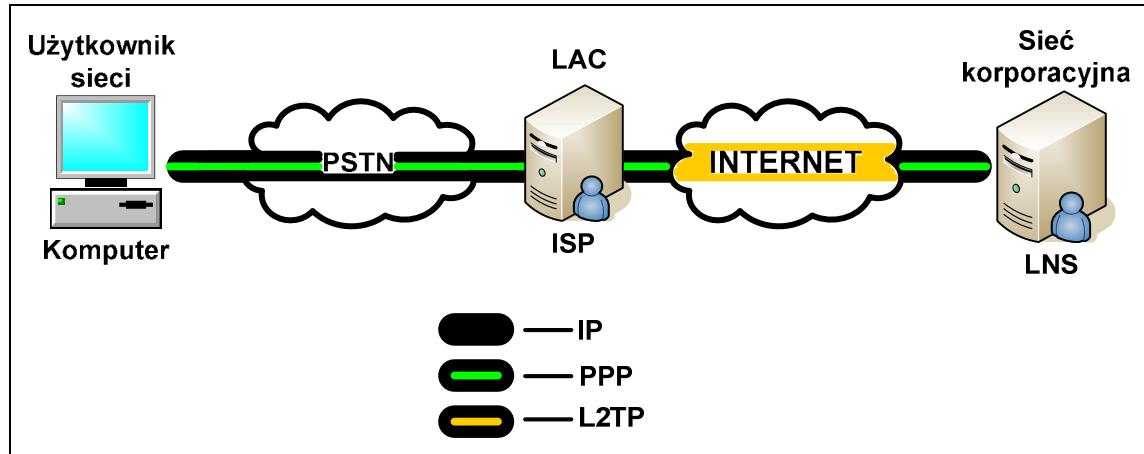
Ponieważ VPN tworzy bezpieczny, wirtualny korytarz czy też tunel komunikacyjny w publicznej sieci Internet - protokoły używane do tworzenia tych połączeń są nazywane tunelowymi. Tunelowanie w wirtualnych sieciach prywatnych stanowi główny składnik usługi wdzwaniowej (ang. *Dial-In*), która najczęściej stosowana jest przez użytkowników zdalnych, do łączenia się poprzez strukturę sieci publicznej do zasobów firmowej sieci. Protokoły pozwalające na utworzenie tunelu w warstwie drugiej modelu ISO/OSI, dają możliwość kapsułkowania (ang. *Encapsulation*) pakietów oraz uwierzytelniania połączeń. Dzięki procesowi enkapsulacji możliwym jest przesyłanie przez tunel nie tylko pakietów IP, ale także IPX/SPX (ang. *Internetwork Packet Exchange*) oraz NETBEUI. Najpopularniejsze protokoły warstwy drugiej modelu ISO/OSI to: PPTP, L2F, L2TP, PLIP/SLIP, PPP.

PPTP (ang. *Point-to-Point Tunnelling Protocol*) jest rozszerzeniem protokołu PPP (ang. *Point-to-Point*), służącym kiedyś do przesyłania pakietów IP poprzez łącza szeregowe. Dziś natomiast dzięki wprowadzeniu wielu ulepszeń i zastosowaniu protokołu uwierzytelniającego EAP (ang. *Extensible Authentication Protocol*) można przesyłać pakiety IP poprzez sieć Internet oraz realizować dodatkowe systemy uwierzytelniania, znane jako typy EAP. Systemy takie to między innymi tokeny sprzętowe generujące jednorazowe hasła, uwierzytelnianie z kluczem publicznym za pomocą kart inteligentnych czy też certyfikatów.[6d]

Protokół PPTP tworzy tunel w sieci publicznej, ale nie oferuje szyfrowania, co jest niewątpliwie jego wadą. Przenosi natomiast niewiele dodatkowych, nadmiarowych informacji, dzięki czemu jest szybszy od innych rozwiązań.

Konkurencyjnym w stosunku do protokołu PPTP firmy Microsoft jest protokół wynaleziony przez firmę Cisco Systems – o nazwie L2F (ang. *Layer Two Forwarding*). Podobnie jak PPTP kapsułkuje dane i inne protokoły wewnątrz pakietu TCP/IP, aby dalej transmitować je przez sieć publiczną, podobnie też protokół L2F nie posiada funkcji szyfrowania danych sam w sobie. Jako cechy odróżniające można wymienić to, że protokół L2F wymaga stosowania routera (który, wspiera funkcjonalność L2F), zaś PPTP korzysta ze specjalnego oprogramowania zarówno po stronie klienta jak i serwera. L2F działa na niższym poziomie i nie wymaga trasowania TCP/IP, którego wymaga PPTP.

Ze względu na to, że oba standardy PPTP i L2F były bardzo podobne do siebie - zostały one połączone przez komisję IETF (ang. *Internet Engineering Task Force*), w wyniku czego powstał protokół o nazwie L2TP (ang. *Layer 2 Tunnelling Protocol*), który łączy standardy obu firm: Microsoft i Cisco Systems.



Rysunek 22 Opracowanie własne: Tunelowanie L2TP

Wykorzystując protokół L2TP, dostawca usług internatowych (ang. *Internet Service Provider*) może zestawić wirtualny tunel pomiędzy zdalnymi klientami a siecią korporacyjną w oddziale firmy. Połączenie *dial-up* zdalnego pracownika jest zakończone na urządzeniu LAC pełniącym rolę koncentratora dostępu L2TP (ang. *L2TP Access Concentrator*). Urządzenie LAC znajduje się w punkcie dostępowym POP (ang. *Point Of Presence*) dostawcy usług, bądź też może to być komputer zdalnego użytkownika. Ostatnim urządzeniem jest serwer LNS (ang. *L2TP Network Server*), zwykle umiejscowiony wewnątrz sieci korporacyjnej, komunikujący się z serwerem LAC za pośrednictwem protokołu L2TP. Użytkownicy zdalni komunikują się z serwerem LAC za pośrednictwem protokołu PPP.

Przykładem klienta L2TP - jest wbudowany w system Windows klient *L2TP over IPSec*, który używa protokołu PPP (protokół UDP port 1701) aby przesłać dane.

Protokoły uwierzytelniające wykorzystujące PPP:

- *PAP* - Podczas uwierzytelniania – *nazwa użytkownika i hasło użytkownika* wysyłane są czystym tekstem
- *CHAP* - W odpowiedzi na prośbę serwera uwierzytelniającego, klient zwraca zaszyfrowaną odpowiedź plus hasło czystym tekstem. Protokół ten jest bezpieczniejszy niż PAP, ale nie szyfruje danych.

- *MS-CHAP, Version 1* - jeśli chodzi o zasadę działania - podobny do protokołu *Chap*, ale bezpieczniejszy gdyż serwer przechowuje i porównuje tylko zaszyfrowane hasła a nie tekst jawnego
- *MS-CHAP, Version 2* - Zawiera rozszerzenia bezpieczeństwa protokołu MS-CHAP, Version 1
- *EAP* - Umożliwia urządzeniom pełniącym rolę NAC np. (ASA) pośredniczyć w procesie uwierzytelniania PPP do zewnętrznego serwera np. RADIUS.

Zasada działania i zestawiania połączenia przy użyciu protokołów PPP i L2TP jest następująca:

- 1) Zdalny użytkownik podłącza się do serwera pełniącego rolę LAC
- 2) Klient oraz serwer LAC rozpoczynają fazę dialogu PPP - negocjacja parametrów (metody uwierzytelniania hasła PAP/CHAP, PPP multilink, kompresja i inne)
- 3) Jeśli podczas negocjacji wybrany został mechanizm autentykacji CHAP, serwer LAC wysyła „wyzwanie” (ang. *Challenge*) do klienta oczekując w odpowiedzi np. na *użytkownik@domena* oraz hasło użytkownika.
- 4) Na podstawie odpowiedzi CHAP (użytkownika/domeny i hasła, serwer LAC sprawdza np. za pośrednictwem np. serwera AAA – RADIUS czy użytkownik o podanym loginie/domenie i haście istnieje oraz czy ma prawo podłączyć się do sieci.
- 5) Urządzenie LAC ustanawia tunel L2TP do LNS.
- 6) Na podstawie uzyskanej odpowiedzi od LAC, LNS sprawdza czy LAC ma prawo do otwarcia tunelu do LNS oraz przeprowadzają wzajemne uwierzytelnianie na podstawie lokalnej bazy lub kontaktują się z serwerem AAA. Następnie tunel zostaje ustanowiony.
- 7) Dla klienta *użytkownik@domena* zostaje ustanowiona jedna sesja z LAC do LNS.
- 8) LAC przekazuje opcje jakie wynegocjowane zostały między LNS a klientem wraz z polami *użytkownik@domena* oraz hasłem od klienta.
- 9) LNS uwierzytelnia klienta za pośrednictwem serwera AAA lub lokalnej bazy.
- 10) LNS wysyła odpowiedź CHAP do klienta.

11) Za pośrednictwem protokołu ICMP (ang. *Control Protocol*) instalowana jest odpowiednia trasa w tablicy routingu, sesja PPP pomiędzy klientem a LNS zostaje ustanowiona. LAC przekazuje ramki PPP (PPP są tunelowane pomiędzy LAC i LNS)

Omawiając współczesne protokoły (PPTP, L2F, L2TP) transmisji w warstwie drugiej *ISO/OSI*, warto wspomnieć o wychodzących obecnie z użycia:

- SLIP (ang. *Serial Line Internet Protocol*),
- PLIP (ang. *Parallel Line Internet Protocol*).

Pierwszy z nich umożliwia transmisję protokołu IP poprzez łącza szeregowe (ang. *Serial*), czyli popularne łącza RS232 lub też modem. System ten pozwalał na transmisję ramek bez kompresji, ani też bez wykrywania błędów. Protokół SLIP pozwala na transmisję pakietów protokołu IP poprzez łącza asynchroniczne i synchroniczne kapsułkując go w swoich ramkach. Wadą SLIP jest brak wsparcia dla protokołów innych niż IP (gdyż, w ramce brak jest pola identyfikującego typ protokołu warstwy sieciowej). Ulepszona odmiana CSLIP (ang. *Compress Serial Line Internet Protocol*) pozwalała przesyłać więcej ramek w jednostce czasu, dzięki wykorzystaniu kompresji. PLIP natomiast używa do komunikacji łącza równoległego tzw. *Centronics* lub *LPT*, które oferuje znacznie większą prędkość transmisji.

Następcą SLIP jest protokół PPP (ang. *Point-to-Point*) gwarantujący niezawodną transmisję na łączach szeregowych. Zapewnia kapsułkowanie pakietów różnych protokołów warstwy sieciowej (IP, IPX, AppleTalk) w ramki nadające się do przesłania poprzez łącza synchroniczne i asynchroniczne, nie nakładając żadnych ograniczeń jeśli chodzi o szerokość pasma transmisji.

Protokół PPP składa się z trzech głównych elementów:

- Funkcja obsługująca kapsułkowanie pakietów IP,
- Protokół kontroli łącza LCP (ang. *Link Control Protocol*), który ma za zadanie nawiązać, skonfigurować, przetestować i zakończyć połączenia w warstwie łącza danych,
- Protokół kontroli sieci NCP (ang. *Network Control Protocol*).

Za pomocą protokołu PPP w wersji rozszerzonej EAP (ang. *Extensible Authentication Protocol*) możliwa jest negocjacja protokołów uwierzytelniających użytkowników,

przesyłanie danych uwierzytelniających (nazwa użytkownika i hasło), jeszcze zanim dany użytkownik zostanie połączony z siecią.[1][6][7]

4.3 Warstwa trzecia ISO/OSI: IP Security (IPsec)

Protokół IP jest obecnie najpopularniejszym protokołem, na bazie którego zbudowana jest sieć Internet. Wynaleziony ponad 20 lat temu na potrzeby militarne Stanów Zjednoczonych, aby zapewnić skutecną komunikację nawet na wypadek ataku jądrowego – służy bez większych modyfikacji po dzień dzisiejszy wszystkim użytkownikom sieci Internet. Protokół ten ma jednak swoje wady, do których zaliczyć można: wyczerpującą się przestrzeń 32-bitowych adresów IP, niemożność obsługiwanego ruchu o wysokich wymaganiach czasowych oraz najważniejsza - brak bezpieczeństwa w warstwie sieciowej. Wszystkie wymienione wady protokołu IP wersji 4 ma wyeliminować jego następcę nowej generacji - IPng (ang. *IP Next Generation*) lub też potocznie IPv6. Protokół IP nowej generacji jest już obecnie implementowany w sieci Internet i istnieje obok IPv4 – jednak z jego zalet korzysta dopiero kilka procent z wszystkich urządzeń tworzących globalną sieć. Proporcja ta zmieni się jednak w ciągu kilku kolejnych lat, gdyż znane są już plany migracji IPv4 do IPv6 w wielu instytucjach rządowych na całym świecie.

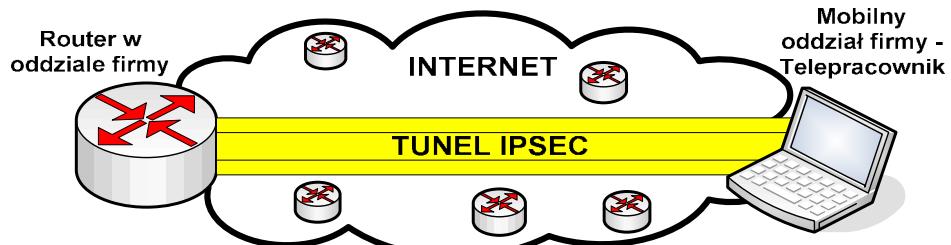
Wraz ze wzrostem gospodarczym oraz rozwojem technologicznym przedsiębiorstw – ogromną rolę zaczął odgrywać handel elektroniczny – nierzadko będący podstawą istnienia wielu firm. Transakcje realizowane tą drogą muszą odbywać się w sposób bezpieczny, tak by nie narazić na straty finansowe bądź też utratę dobrego wizerunku firmy na rynku. Niestety posługując się ogólnie dostępnym protokołem IP (w wersji 4) nie ma możliwości zabezpieczenia danych podczas transakcji w warstwie sieciowej, zatem dane takie podatne są na ataki polegające na podsłuchu (ang. *Sniffing*) czy ingerencji w komunikację (ang. *Spoofing*).

Rozwiązaniem problemu ochrony danych podczas przesyłania przez sieć publiczną jest opracowany w 1995 roku przez organizację IETF (ang. *Internet Protocol Security*) protokół IPsec – rozszerzający działanie protokołu IPv4, a na stałe już obecny w IPv6 (specyfikacja IPsec zawarta jest w dokumencie RFC 2401)

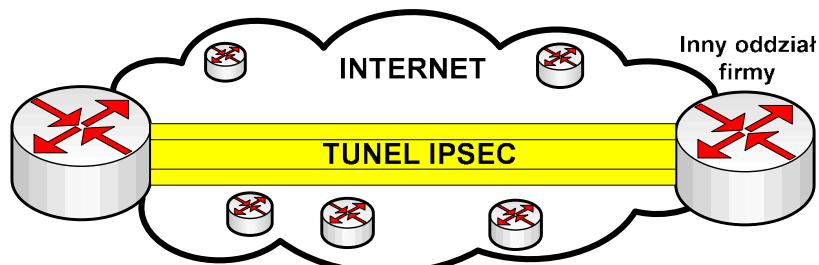
Protokół ten oferuje oparte o otwarte standardy (łatwa współpraca urządzeń pochodzących od różnych producentów) – mechanizmy zapewniające bezpieczną transmisję danych. Może zagwarantować poufność, integralność i autentyczność przesyłanych danych. Integralność (ang. *Data Integrity*) – daje pewność, że dane nie zostały w celowy bądź przypadkowy sposób zmienione. Zapewnienie poufności (ang. *Data Confidentiality*) – poprzez stosowanie technik kryptograficznych, że nawet podczas próby przechwycenia danych – intruz nie będzie w stanie odczytać informacji, czy na końcu autentyczności – czyli gwarancji, że dane otrzymane są z pewnego i znanego nam źródła.

Dzięki mechanizmom kapsułkowania i deenakpsulacji (proces odwrotny) modelu ISO/OSI, protokół IPsec jest w stanie w sposób całkowicie przezroczysty przenosić protokoły warstw wyższych modelu referencyjnego ISO/OSI.

Protokół IPsec używany jest do zabezpieczenia poufnych danych podczas transzu poprzez potencjalnie niebezpieczne medium – np. sieć Internet do tworzenia wirtualnych sieci prywatnych między oddziałami firmy. Lokalizacje tworzące połączenie VPN definiują typ VPN. Lokalizacją może być: klient końcowy (np. PC), małe biuro, duży oddział firmy lub główna siedziba firmy.

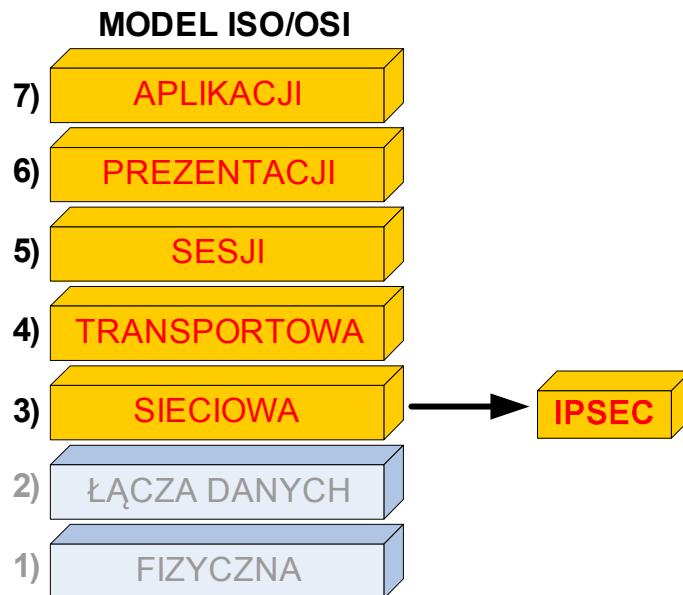


Rysunek 23 Opracowanie własne: Remote Access



Rysunek 24 Opracowanie własne: Site-to-Site VPN

Protokół IPsec może chronić jedynie warstwę IP i wyższe - rozpatrując 7 warstwowy model ISO/OSI. Ochronę warstw niższych można zapewnić stosując omówione wcześniej protokoły zabezpieczające oraz dodatkowo należy zadbać o ile to możliwe o ochronę fizyczną dostępu do pomieszczeń gdzie przechowywane są urządzenia sieciowe (np. switche, huby) plus odpowiednią konfigurację tych urządzeń.[4][5][1i][3i]



Rysunek 25 Opracowanie własne: oznaczone na czerwono
chronione przez IPsec warstwy modelu ISO/OSI

4.3.1 Funkcje i opcje

Podczas transmisji danych protokół IPsec może zapewnić:

Poufność danych (ang. *Data Confidentiality*) – sieci VPN zwykle używają jako medium transmisyjne – publicznej sieci Internet, przez co jak wiemy z rozdziału „zagrożenia przesyłania danych przez sieć publiczną” - dane mogą być podejrzane przez osoby niepowołane. Dzięki użyciu szyfrowania przesyłane dane nie mogą być w prosty sposób odszyfrowane (o ile w ogóle to możliwe), zrozumiałe przez kogokolwiek innego niż druga - zaufana strona połączenia VPN. Użycie szyfrowania wymaga wybrania odpowiedniego algorytmu oraz mechanizmu dystrybucji kluczy szyfrujących. Ochrona poufności danych jest parametrem opcjonalnym IPsec

Integralność danych (ang. *Data Integrity*) – to gwarancja, że dane nie zostały zmodyfikowane podczas transmisji przez sieć IPsec VPN. Integralności danych, nie zapewnia poufności. Do zapewnienia integralności danych używa się algorytmu haszującego (ang. *Hash Algorithm*), by sprawdzić czy dany pakiet został zmodyfikowany podczas tranzystu. Pakiety IP których integralność została naruszona zostają odrzucone.

Autoryzację stron połączenia (ang. *Data Origin Authentication*) – to weryfikacja źródła połączenia VPN (przez każdą ze stron) – by upewnić się, że druga strona połączenia jest tym za kogo się podaje.

Ochronę przed duplikatami (ang. *Anti-Replay*) – Zapewnia, że dane przesyłanie poprzez VPN nie powtórzą się. Dzięki użyciu numerów sekwencyjnych i ruchomego okna (ang. *Sliding Window*) w pakietach, które porównywane są z następnymi co pomaga wykryć te, które są „spóźnione” (te pakiety zostają odrzucone). Ochrona przed duplikatami jest opcjonalna.

Protokół IPsec nie narzuca sposobu uwierzytelniania algorytmów szyfrowania, technik generowania kluczy, czy też mechanizmów SA (ang. *Security Authentication*). [4][5][1i][3i]

4.3.2 Architektura IPsec

Podczas nawiązywania połączenia IPsec między stronami tunelu VPN - każdorazowo ustalany jest zestaw informacji, zawierający między innymi takie pola, jak protokół bezpieczeństwa ESP lub AH, stosowane algorytmy oraz klucze kryptograficzne. Zestaw ten określany jest skrótem SA (ang. *Security Association*). Przekazanie parametrów SA należy rozumieć jako komunikację jednokierunkową, zatem na jeden tunel VPN przypadają dwa różne SA (Jedno SA w jednym kierunku, drugie w przeciwnym).

Najważniejszymi parametrami jakie niesie ze sobą zestaw SA są:

- SPI (ang. *Security Parameters Index*) czyli indeks parametrów bezpieczeństwa. Jest 32-bitową liczbą, która w połączeniu z adresem IP przeznaczenia i protokołem bezpieczeństwa (ESP) w sposób

jednoznaczny identyfikuje SA (ang. *Security Association*) dla danego pakietu

- Destination IP - Docelowy adres IP, jest to adres systemu, z którym nawiązywana jest komunikacja poprzez IPSec.
- SPid (ang. *Security Protocol Identifier*) Identyfikator protokołu bezpieczeństwa, odpowiada za informację, czy używany protokół to ESP czy AH.

Dodatkowymi informacjami zawartymi w SA są:

- Port wejściowy oraz wyjściowy, może on także spełniać funkcję identyfikatora SA.
- Adres IP źródłowy.
- Nazwa, może to być identyfikator użytkownika, jak i nazwa urządzenia.
- Algorytm szyfrujący (ang. *Encryption Algorithm*), dodatkowo może znaleźć się informacja o kluczu publicznym (ang. *Encryption Key*).
- Algorytm uwierzytelniający (ang. *Authentication Algorithm*), dodatkowo może znaleźć się informacja o kluczu publicznym.
- Tryb pracy IPsec (tunelowy bądź też transportowy).
- Długość życia SA.
- Numer sekwencji.
- Maksymalny rozmiar pakietów (ang. MTU).
- Identyfikator związku z SPD (ang. *Security Policy Database*) – wskaźnik pozwalający odszukać połączenie w bazie SAD (ang. *Security Association Database*). Baza ta zawiera informacje na temat SA. Na podstawie informacji z bazy SAD można podjąć decyzję na temat sposobu obsłużenia pakietów IPSEC w zależności od przypisanego SA. SPD jest narzędziem pozwalającym określić czy dany pakiet wysłany bądź odebrany spełnia reguły bezpieczeństwa.
[4][5][1i][3i]

4.3.3 Protokoły bezpieczeństwa w IPSEC: AH i ESP

Trzy protokoły bezpieczeństwa, które używane są przez IPsec to:

Internet Key Exchange (IKE) - Jest podstawą i szkieletem dla procesu negocjacji i wymiany parametrów bezpieczeństwa oraz uwierzytelnienia kluczy szyfrowania (protokół IKE szczegółowo omówiony zostanie w następnych rozdziałach)

Encapsulating Security Payload (ESP) – protokół, który zapewnia poufność danych, integralność, autoryzacje stron połączenia oraz opcjonalnie ochronę anti-reply. Funkcje integralności, niezaprzeczalności realizowane są, podobnie jak w przypadku protokołu AH, dzięki ICV (ang. *Integrity Check Value*). ESP jest jedynym protokołem IPsec, który zapewnia szyfrowanie danych a także wszystkie pozostałe opcjonalne funkcje IPsec, z tego powodu protokół ESP jest częściej stosowany niż protokół AH. [7d][8d]

Nagłówek ESP składa się z następujących pól:

- *Security Parameters Index* – czyli indeks parametrów bezpieczeństwa. Jest dowolną 32-bitową wartością, która w połączeniu z adresem IP przeznaczenia i protokołem bezpieczeństwa (ESP) w sposób jednoznaczny identyfikuje SA (ang. *Security Association*) dla danego pakietu
- *Sequence Number* – czyli numer sekwencyjny – to 32 bitowa wartość – pełni rolę licznika, który inkrementuje o jeden przy wysyłce każdego pakietu. Wypełnienie pola jest obowiązkowe nawet gdy adresat nie włączył zabezpieczenia (ang. *Anit-reply*) przed powtórzeniami pakietów dla danego połączenia (SA). Analiza tego pola leży po stronie adresata
- *Payload data* – jest polem o zmiennej długości zawierającym właściwe dane przenoszone przez protokół IPsec. Pole jest obowiązkowe i jego długość jest całkowitą liczbą bajtów. Jeżeli algorytm (możliwe tylko algorytmy symetryczne) użyty do szyfrowania danych(np. DES 3DES CBC IDEA Blowfish) wymaga danych synchronizacyjnych np. IV (ang. *Initiation Victor*), to dane te mogą być przenoszone bezpośrednio w tym polu. Każdy algorytm, który ich wymaga musi wskazywać ich długość, strukturę oraz położenie.
- *Padding* – czyli dopełnienie w zależności od stosowanego algorytmu szyfrowania - pole to może być wymagane do dopełnienia do jakiejś wielokrotności bajtów, której wymaga dany algorytm np. przed szyfrowaniem danego bloku danych. Pole może mieć długość od 0 do 255 bajtów.
- *Pad Length* – czyli długość dopełnienia określa długość pola Padding i jest obowiązkowe.

- *Next Header* - czyli następny nagłówek, 8 bitowe pole mówiące o rodzaju danych za nagłówkiem AH.
- *Authentication Data* – czyli dane uwierzytelniania, jest polem o zmiennej długości zawierającym wartość ICV sprawdzającą integralność. Obliczenia ICV wykonywane są po dokonaniu zaszyfrowania, tak aby uniknąć niepotrzebnego deszyfrowania w przypadku, gdy dane nie spełniają warunku integralności. Przeciwdziała to atakom typu DOS, gdyż pakiety zmodyfikowane podczas tranzytu mogą zostać szybciej odrzucone. Długość tego pola jest zależna od wyboru metody uwierzytelniania. Pole to jest opcjonalne i wypełnianie tylko wtedy gdy metoda uwierzytelniania ostała wybrana w chwili tworzenia SA.
[7d][8d]

Tabela 4 Opracowanie własne: Nagłówek ESP [7d][8d]

| | | |
|---------------------------------|------------|-------------|
| SPI (Security Parameters Index) | | |
| Sequence Number | | |
| Payload data | | |
| Padding | Pad lenght | Next Header |
| Authentication Data | | |

Authentication Header (AH) – (uwierzytelnianie nagłówka) jest protokołem, który zapewnia integralność danych oraz opcjonalnie ochronę przed duplikatami. Protokół AH zapewnia jedynie, że dane podczas tranzytu nie zostały zmodyfikowane, ale nie ukrywa danych (zatem nie zapewnia poufności danych). Dlatego też protokół AH jest częściej stosowany niż ESP. Nagłówek protokołu AH umieszczony jest zaraz za nagłówkiem pakietu IP. [7d][8d]

Nagłówek AH składa się z następujących pól:

- *Next header* – czyli następny nagłówek, to 8 bitowe pole mówiące o rodzaju danych za nagłówkiem AH. Liczba 4 oznacza dane protokołu IPv4. Liczba 41 protokół IPv6 zaś liczba 6 protokół TCP
- *Payload Length* – czyli długość nagłówka AH. Pole długości 8 bitów – wyrażone wielokrotnością liczby 32 (pomniejszona o 2)

- *Reserved* – czyli zarezerwowane . Pole długości 16 bitów możliwe do użycia w przyszłości. Wartość powinna być ustawiona 0 by uniknąć odrzucenia po drugiej stronie tunelu VPN
- *Security Parameters Index* – czyli indeks parametrów bezpieczeństwa. Jest dowolną 32-bitową wartością, która w połączeniu z adresem IP przeznaczenia i protokołem bezpieczeństwa (ESP) w sposób jednoznaczny identyfikuje bezpieczne połączenie (ang. *Security Association*) dla danego pakietu
- *Sequence Number* – czyli numer sekwencyjny – to 32 bitowa wartość – pełni rolę licznika, który inkrementuje o jeden przy wysyłce każdego pakietu. Wypełnienie pola jest obowiązkowe nawet gdy adresat nie włączył zabezpieczenia (ang. *Anit-reply*) przed powtórzeniami pakietów dla danego połączenia (SA). Analiza tego pola leży po stronie adresata
- *Authntication Data* – czyli dane uwierzytelnienia – jest polem o zmiennej długości, będące wielokrotnością 32 bitów (To pole może zawierać dopełnienie, żeby zapewnić odpowiednią wielokrotność) zawierającym wartość sprawdzającą integralność (ang. *Integrity Check Value*) dla tego pakietu. Pozwala zapewnić integralność transmitowanych danych. Pole to jest obecne, jeśli została wybrana odpowiednia opcja dla danego SA. Przykładem algorytmów stosowanych podczas uwierzytelniania i zapewniania integralności najpopularniejszymi są HMAC-MD5 oraz HMAC-SHA1.[4d] [7d][8d]

Tabela 5 Opracowanie własne: Nagłówek AH

| | | |
|---------------------------------|----------------|----------|
| Next header | Payload length | reserved |
| SPI (Security Parameters Index) | | |
| Sequence Number | | |
| Authentication Data | | |

Zarówno protokół ESP jak i AH używają algorytmu haszującego HMAC (ang. *Hash Based Authentication Code*) – do weryfikacji uwierzytelnienia i integralności danych.

Tabela 6 Opracowanie własne: Algorytmy haszujące

| Algorytm | Wejście | Wyjście | Używane przez IPsec |
|-----------------------------|---------|----------|---------------------|
| Message Digest 5 (MD5) | Zmienne | 128bitów | 128bitów |
| Secure Hash Algorithm(SHA1) | Zmienne | 160bitów | Pierwsze 96 bitów |

MD5 jak i SHA-1 używają tajnego współdzielonego klucza (ang. *Shared Secret Key*) do kalkulacji oraz weryfikacji. Siła szyfrowania HMAC – uzależniona jest od właściwości funkcji haszującej. MD5 i SHA-1 jako wynik operacji haszowania dają zawsze ciąg znaków równej długości (tabela 6) niezależnie od ilości znaków na wejściu – odpowiednio dla MD5 – 128bitow a dla SHA-1 – 160 bitów. Za bezpieczniejszy uważa się algorytm SHA-1, jednak jest on wolniejszy niż MD5.

IPsec używa protokołów IKE, ESP i AH do ustalenia reguł uwierzytelniania, szyfrowania oraz zarządzania kluczami, warto wspomnieć, że protokoły te, również oparte są o otwarte standardy. [4][5][1i][3i] [7d][8d]

Porównanie protokołów AH i ESP

Porównując właściwości protokołów AH i ESP wynika, że protokół ESP jest dużo bardziej uniwersalny i wypełnia wszystkie wstępne założenia protokołu IPsec co do integralności, poufności i autentyczności danych oraz dodatkowo w nowej wersji ESP rozszerzony licznik sekwencyjny (ang. *Extended Sequence Number*). Jeśli nie jest natomiast wymagane szyfrowanie danych – można posłużyć się protokołem AH.

Tabela 7 Opracowanie własne: Porównanie protokołów AH i ESP [7d][8d]

| Protokół i przeznaczenie | AH | ESP (z szyfrowaniem) | ESP (szyfrowanie i uwierzytelnianie) |
|--------------------------|-----|----------------------|--------------------------------------|
| Poufność | NIE | TAK | TAK |
| Integralność | TAK | NIE | TAK |
| Niezaprzecjalność | TAK | NIE | TAK |
| Kontrola dostępu | TAK | TAK | TAK |
| Poufność przesyłu | NIE | TAK | TAK |

Dalszy rozwój protokołu IPsec ma przynieść całkowitą eliminację protokołu AH na rzecz ESP. Zmianie ma też ulec składnik IPsec jakim jest proces wymiany parametrów

bezpieczeństwa IKE. W jego drugiej odsłonie zastosowane zostaną najlepsze cechy z protokołów Photurius, Sigma, JFK, Son of IKE.

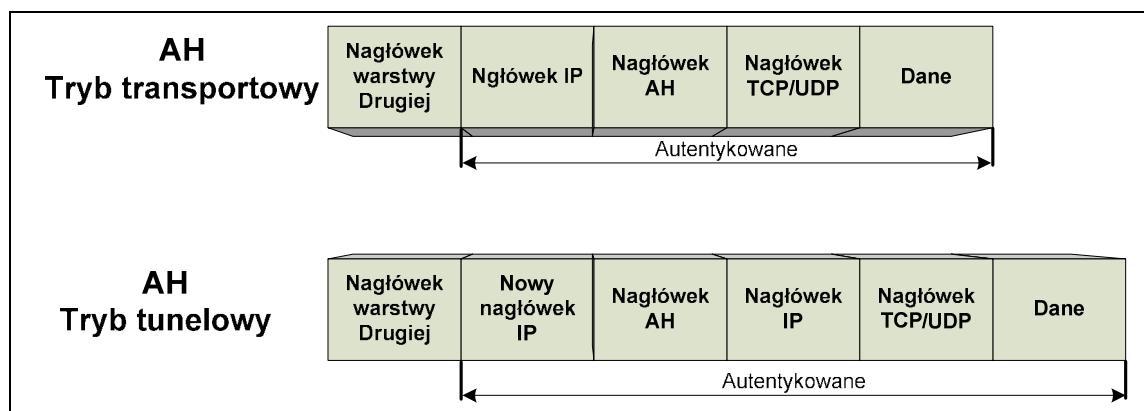
4.3.4 Tryby pracy tunelowy i transportowy

IPsec może pracować w dwóch trybach, zapewniających ochronę pakietu IP.



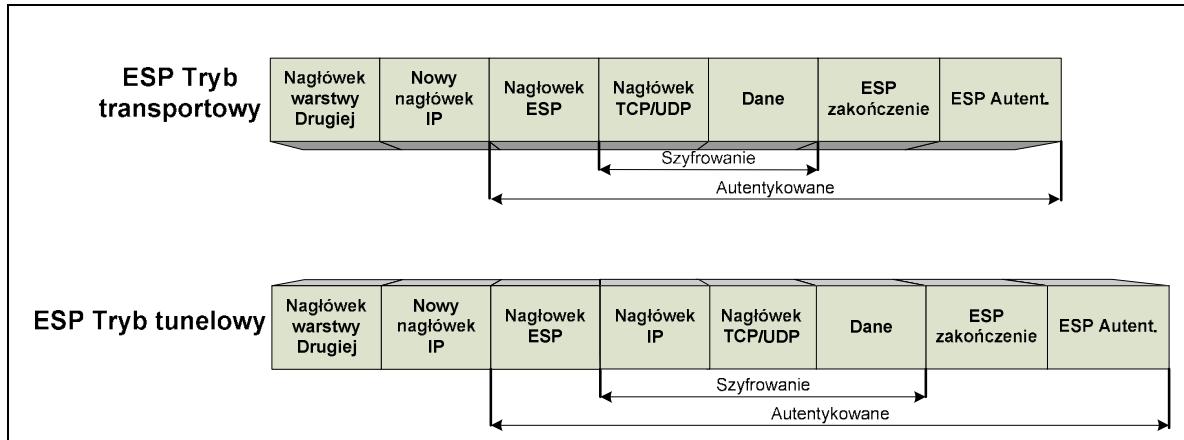
Rysunek 26 Opracowanie na podstawie Cisco CCNP ISCW Oficial str 261

Tryb transportowy – (ang. *Transport Mode*) – kiedy nagłówki IPsec są dołączane do pakietu IP (po nagłówku IP), mówimy o trybie transportowym. Oryginalny nagłówek IP jest widoczny i niechroniony, dane i warstwy od transportowej w górę - tak. Kiedy pakiety IPsec przesyłane są przez sieć Internet (strefa potencjalnie niebezpieczna) – dane zawarte w pakietach są bezpieczne, jedynie ryzyko polega na tym, że osoby trzecie mogą podejrzeć adresy IP hostów wymieniających dane.



Rysunek 27 Opracowanie na podstawie Cisco CCNP ISCW official str. 261

Tryb tunelowy – (ang. *Tunel Mode*) – Zarówno oryginalny nagłówek IP jak i dane są chronione w pakiecie IPsec. Tryb tunelowy tworzy nowy zewnętrzny nagłówek IP, który zawiera adresy IP tuneli końcowych (np. routery, czy też koncentrator VPN). Nie można zatem podejrzeć adresów IP hostów, które komunikują się wewnątrz tunelu VPN.



Rysunek 28 Opracowanie na podstawie Cisco CCNP ISCW official str. 261

W Internecie najczęściej wykorzystywany jest tryb tunelowy, dzięki któremu po przechwyceniu danych – atakujący nie jest nawet w stanie poznać adresów IP, między którymi istnieje komunikacja wewnętrz tunelu. Osoba taka posiada jedynie wiedzę na temat adresów IP urządzeń wymieniających szyfrowany ruch poprzez Tunel VPN. [4][5][1i][3i]

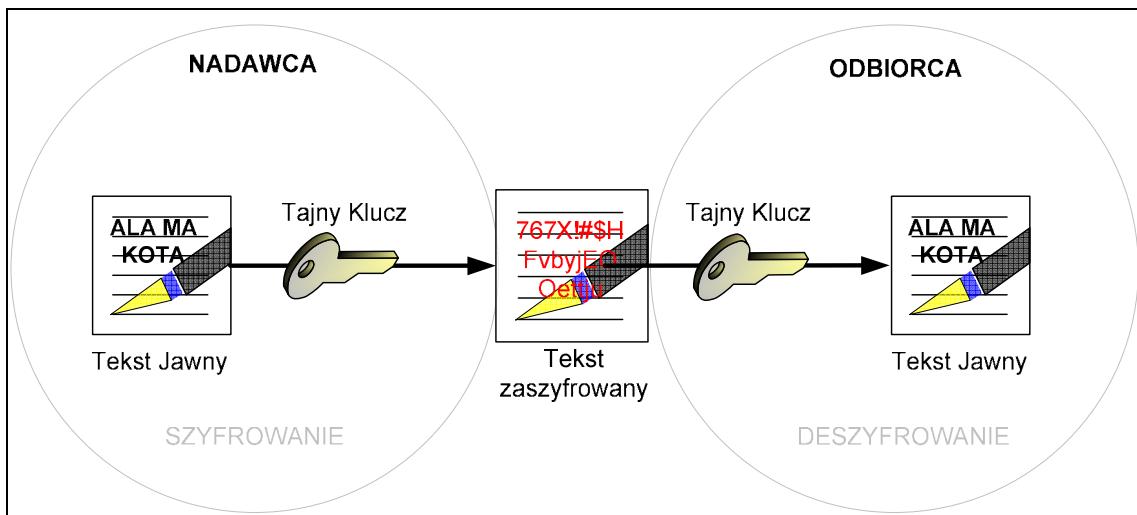
4.3.5 Algorytmy szyfrowania

Szyfrowanie to nic innego jak zamiana tekstu jawnego, który chcemy utajnić w szyfrogram - często treść pozornie nie mająca sensu, będąca nie do odczytania, nawet dla osób, które znają zasadę działania algorytmu szyfrującego.

Idealnie zaszyfrowana informacja – to taka, która jest możliwa do odszyfrowania wtedy i tylko wtedy, gdy znany jest właściwy klucz. Trudność odszyfrowania jest tym większa im bardziej złożony algorytm szyfrowania został użyty oraz im większy rozmiar klucza użytego do szyfrowania.

Istnieją dwa typy algorytmów szyfrowania: symetryczne i asymetryczne.[1i][6]

Symetryczne – zwane często kryptografią ukrytego klucza. Jak nazwa wskazuje jest jeden klucz, który używany jest zarówno do szyfrowania jak i deszyfrowania danych. Każdy kto jest w stanie poznać sekretny klucz – jest w stanie odszyfrować ukrytą informację.



Rysunek 29 Opracowanie własne: Szyfry symetryczne

Sprzętowa implementacja algorytmów symetrycznych jest łatwiejsza niż algorytmów asymetrycznych. Przykładami algorytmów symetrycznych mogą być:

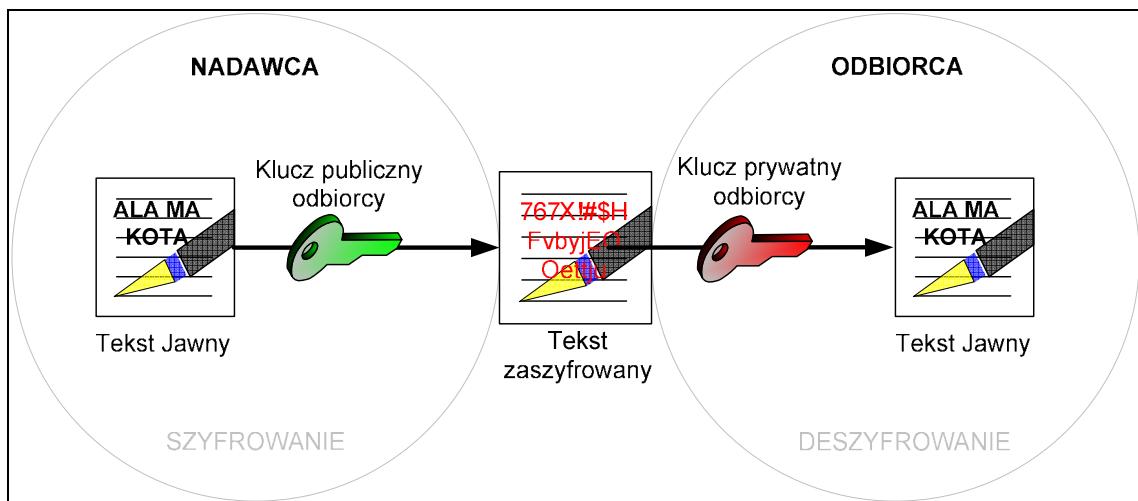
- **DES** (ang. *Data Encryption Standard*) – z kluczem długości 56 bitów, przy dostępnej dziś mocy obliczeniowej komputer - możliwy do złamania w ciągu kilku godzin
- **3DES** (ang. *Triple Data Encryption Standard*) – na szyfrowanej informacji uruchamiane są kolejno trzy różne 56 bitowe algorytmy DES. (w kolejności: szyfrowanie DES, deszyfrowanie DES, szyfrowanie DES) co w wyniku daje szyfrogram. Nie odnotowano dotąd udokumentowanej próby złamania algorytmu 3DES
- **AES** (ang. *Advanced Encryption Standard*) – odmiana algorytmu „Rijandael”. Oba używają tego samego algorytmu szyfrowania i wspierają klucze z zakresu 128 do 256 bit, lecz różni je od siebie inna liczba rund szyfrujących oraz AES używa skoku inkrementującego co 64-bit a Rijandael – wielokrotności 32. Algorytm AES uważa się za najbezpieczniejszy z algorytmów szyfrowania symetrycznego.
- **IDEA** (ang. *International Data Encryption Algorithm*) – długości klucza 128 bitów (jest algorymem opatentowanym)

Asymetryczne – Poważnym problemem szyfrowania symetrycznego jest proces dystrybucji tajnego klucza, potrzebnego do szyfrowania i deszyfrowania - dlatego bezpieczniejszym jest stosowanie algorytmów asymetrycznych. Każda ze stron

realizujących szyfrowane połączenie posiada parę kluczy: publiczny i prywatny, przy czym klucz publiczny jest kluczem ogólnodostępnym (ang. public key) i znany obu stronom połączenia a prywatny jest kluczem tajnym. Między kluczami prywatnym i publicznym istnieje matematyczna zależność. Jeśli nadawca chce wysłać zaszyfrowaną wiadomość do odbiorcy, używa do tego celu klucza publicznego odbiorcy (ogólnie znany), natomiast odbiorca chcąc odczytać szyfrogram – używa swojego klucza prywatnego (tajnego).

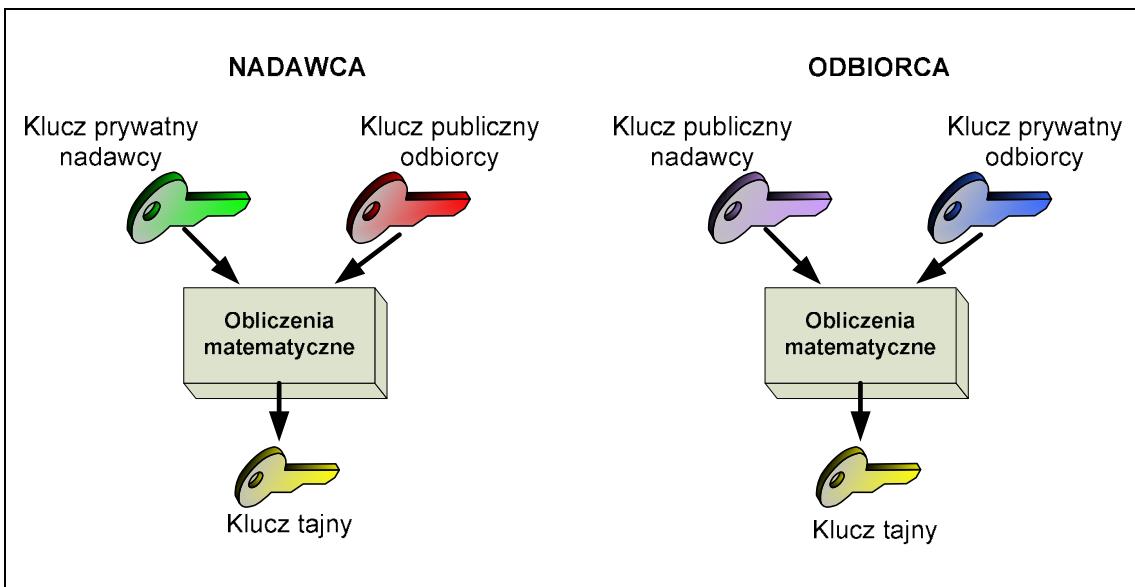
Przykładem algorytmu asymetrycznego jest **RSA** (skrót od nazwisk trzech wynalazców: Ronald Rivest, Adi Shamir, Leonard Adelman). Największą wadą algorytmów asymetrycznych jest ich prędkość działania – testy pokazały, że porównując RSA do DES - algorytm asymetryczny okazał się blisko tysiąc razy wolniejszy.

Dlatego też najczęściej stosuje się hybrydę – jeśli chodzi szyfrowanie – wymiana klucza tajnego, ze względu na bezpieczeństwo odbywa się za pomocą algorytmu asymetrycznego (RSA 512-2048 bit), natomiast dalsza wymiana informacji za pomocą algorytmu symetrycznego (np. 3DES lub AES) – ze względu na szybkość.



Rysunek 30 Opracowanie własne: Szyfry symetryczne

Algorytm Diffiego-Helmana – opracowany przez Whitfielda Diffie i Martina Hellmana. Algorytm nie jest bezpośrednio wykorzystywany do szyfrowania, lecz do ustalenia tajnego klucza służącego do komunikacji. Zasada działania polega na wyznaczeniu tajnego klucza przy pomocy własnego klucza prywatnego oraz klucza publicznego drugiej strony szyfrowanej komunikacji. Odbiorca wiadomości wykonuje taką samą operację do ustalenia klucza tajnego.



Rysunek 31 Opracowanie własne: Algorytm Diffiego-Hellmana

Funkcje haszujące – Podczas przesyłania danych poprzez medium Internet – bardzo ważnym jest by dane nie zostały w jakikolwiek sposób zmodyfikowane – czyli zachowana została ich integralność. Pewność taką może dać użycie jednokierunkowych funkcji skrótu (ang. *Message Digest*) – dzięki czemu niemożliwe jest odtworzenie wiadomości na podstawie jej skrótu. Zasada działania jest następująca: wiadomość jaką chcemy przesłać – jest używana jako argument funkcji haszującej – dając wynik jej działania, zawsze ciąg znaków równej długości. Więcej na temat funkcji skrótu – w rozdziale „Protokoły bezpieczeństwa”.

4.3.6 Negocjacja parametrów bezpieczeństwa: IKE

Bezpieczne połączenie IPsec pomiędzy dwoma lokalizacjami może być wstępnie skonfigurowane na obu partycypujących urządzeniach, jednakże tak pozostawione mogą paść ofiarą ataku typu *brute-force* (słownikowego). Potrzeba ręcznej zmiany kluczy szyfrujących IPsec co każdą godzinę lub co kilka godzin może być problematyczne – dlatego do automatycznej negocjacji parametrów bezpieczeństwa wymyślony został protokół IKE (ang. *Internet Key Exchange*). [2d]

Głównym zadaniem protokołu IKE jest automatyzacja procesu wymiany i aktualizacji kluczy kryptograficznych, czyli pośrednio - przeciwdziałanie atakom na sesje IPsec oraz wzajemne uwierzytelnianie urządzeń tworzących połączenie IPsec. IKE używa dwóch protokołów by ustalić dane uwierzytelniające dla danego tunelu tzw. SA (ang. *Security Association*):

ISAKMP – (ang. *Internet Security Association and Key Management Protocol*) definiuje procedury, ustanowienia, negocjacji, modyfikacji oraz usunięcia SA.

OAKLEY – protokół ten wykorzystuje algorytm Diffie-Hellman'a do wymiany kluczy poprzez tunel IPsec. Działanie kryptograficznego algorytmu Diffie-Hellman'a pozwala przesyłać klucz wspólnodzielony (ang. *Shared Secret*) poprzez medium jakim jest Internet, gdzie przesyłane danych jest zagrożone.

Protokół IKE bazuje na algorytmie Diffiego-Hellmana, dzięki któremu do wyznaczenia tajnego klucza sesji nie jest wymagane przesyłanie tajnych informacji między stronami szyfrowanego połączenia. Bezpieczeństwo IKE zależy od długości liczby *Diffiego-Hellmana* (długość liczby pierwszej, wykorzystanej w algorytmie):

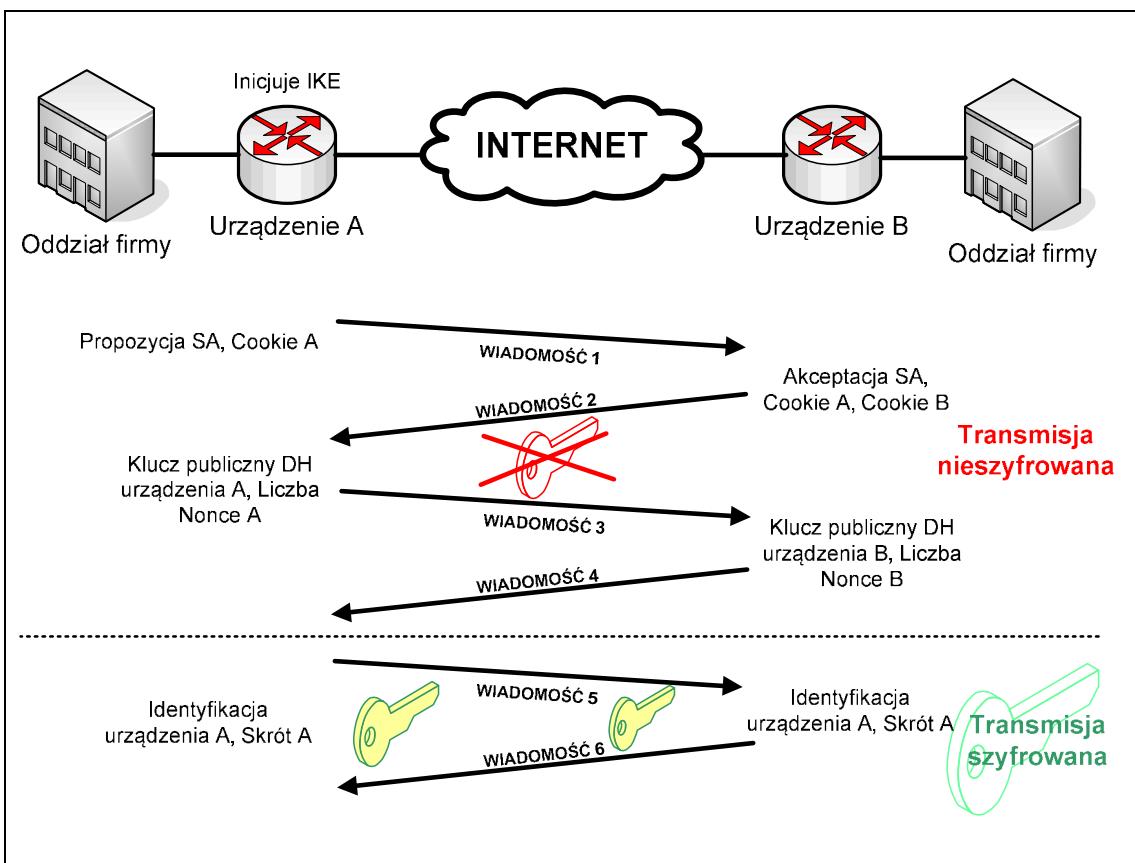
- Diffie-Hellmana Group 1 (768Bitów)
- Diffie-Hellmana Group 2 (1024Bitów)
- Diffie-Hellmana Group 3 (1536Bitów)

4.3.7 Fazy IKE

Negocjacja IKE przebiega trójfazowo (dwie fazy stałe plus jedna opcjonalna). Kiedy zestawiane jest bezpieczne połączenie pomiędzy lokacjami IPsec proces przebiega następująco:

IKE faza 1 – jest fazą główną, przeprowadzaną tylko raz, w której to zachodzi proces ustanowienia dwukierunkowej komunikacji SA, co oznacza, że dane wysłane pomiędzy urządzeniami końcowymi tunelu IPsec używają tego samego klucza. Faza pierwsza zapewnia także uwierzytelnianie urządzeń partycipujących w tworzeniu SA. Faza pierwsza może przebiegać w dwóch trybach: *main mode* oraz *aggressive mode*.

Podczas działania fazy 1, w trybie *main mode* (zwykle stosowany w połączeniach *Site-to-Site*) dochodzi do wymiany sześciu wiadomości, natomiast w szybszym trybie *Aggressive Mode* (zwykle stosowany w połączeniach typu *Remote-Access*) dochodzi do wymiany jedynie trzech.



Rysunek 32 Opracowanie własne: Faza pierwsza IKE, tryb Main Mode

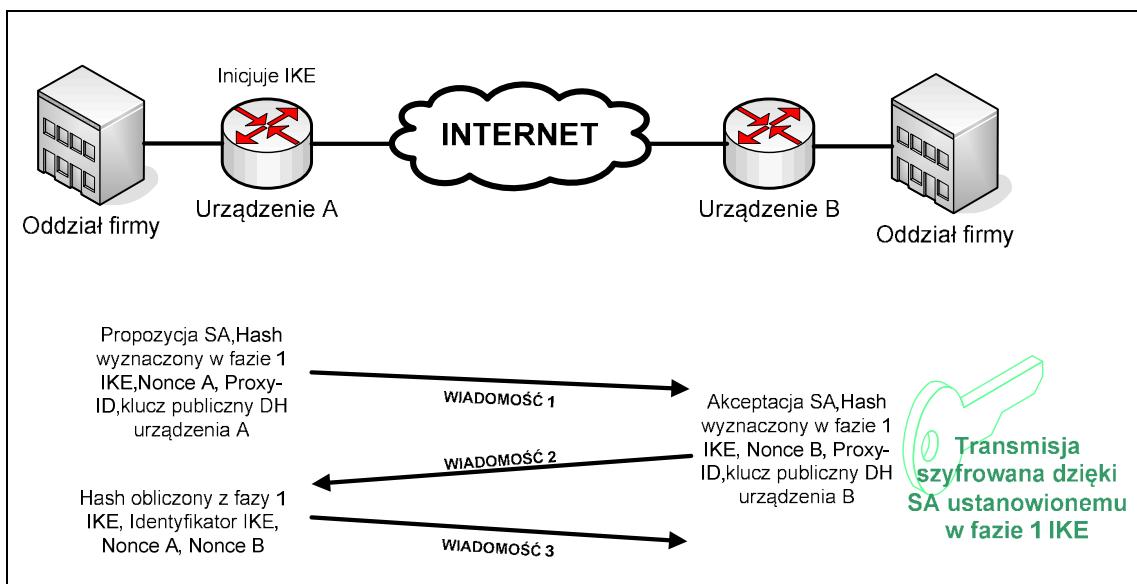
W trybie pracy *Main Mode*, czyli trybie normalnym, dwie pierwsze wiadomości przesłane pomiędzy urządzeniami, mają zadanie wynegocjować informacje SA będące dalej szkieletem bezpiecznej komunikacji do dalszych negocjacji. Mogą to być propozycje zestawów różnych grup DH, algorytmów szyfrowania 3DES, AES, funkcje skrótów MD5, SHA1 itd. Dodatkowo przesyłanymi informacjami w tzw. ciasteczkach (ang. *Cookies*) są adresy IP urządzeń tworzących tunel VPN. Kolejne wiadomości (3 i 4) zawierają klucze publiczne DH. Po wymianie tych komunikatów na podstawie kluczy publicznych – oba urządzenia są w stanie obliczyć używając funkcji skrótu – tajny klucz, który użyty zostanie do zabezpieczenia sesji poprzez jej zaszyfrowanie. Kolejne dwie wiadomości (5 i 6) są już zaszyfrowane i uwierzytelnione za pomocą parametrów wynegocjowanych za pomocą wcześniejszych wiadomości. Za pomocą ostatnich wiadomości dokonuje się sprawdzenia autentyczności końcowych urządzeń tunelu VPN poprzez porównanie tajnych kluczy (ang. *Pre-Shared Key*) bądź też cyfrowych certyfikatów obu urządzeń.

W przyspieszonym trybie pracy *Aggresive Mode* – pierwsza z trzech wiadomości zawiera propozycję SA, a także publiczny klucz *DH*, liczbę losową *Nonce* oraz identyfikator *ISE*. Wiadomość druga jest odpowiedzią na propozycję SA a zarazem akceptacją parametrów SA, dokonuje uwierzytelnienia (na podstawie obliczonego skrótu z klucza publicznego), zawiera klucz publiczny DH, liczbę losową *Nonce* i identyfikator IKE. Ostatnia wiadomość – nadawana jest przez urządzenie inicjujące zestawienie tunelu VPN – dokonanie uwierzytelnienia (na podstawie obliczonego skrótu z klucza publicznego).

W trybie pracy *Aggresive Mode* nie jest zapewniona ochrona poufności danych, gdyż podczas zestawiania połączenia IPsec, pierwsze dwie wiadomości przesyłanie poprzez sieć – podczas negocjacji parametrów bezpieczeństwa – są nieszyfrowanie, zatem istnieje ryzyko podsłuchania danych, a co za tym idzie wyliczenia tajnego klucza *Pre-Shared Secret*, za pomocą specjalnych programów. Z tego powodu należy unikać stosowania trybu *Aggresive Mode* w implementacji bezpiecznych sieci VPN typu *Remote-Access*, o ile jako metody uwierzytelniania nie są stosowane dynamiczne hasła (np. tokeny) lub też certyfikaty cyfrowe.

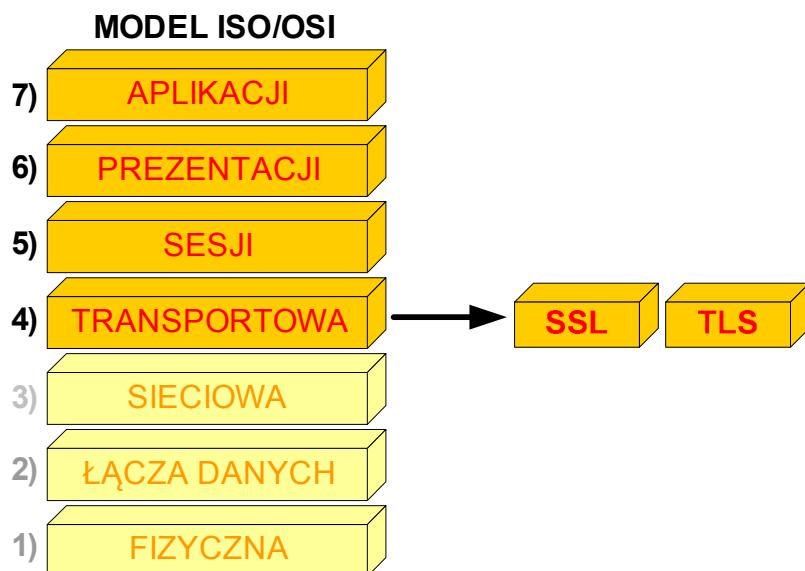
IKE faza 1.5 – to faza opcjonalna. Wprowadza dodatkową warstwę uwierzytelnienia IPsec w fazie 1 – zapewnia autentykację urządzeń, ale nie użytkowników będących za tymi urządzeniami. Rozszerzona autentykacja tzw. Xauth – zmusza także użytkownika do uwierzytelnienia, aby dać mu prawo do używania tunelu IPsec.

IKE faza 2 – (ang. *Quick Mode*) - negocjacja parametrów SA oraz powiązanie materiału kluczowego z fazą 1. Ma za zadanie wyznaczyć SA do szyfrowania i uwierzytelniania danych przesyłanych przez tunel IPsec. Etap ten wymaga przesłania trzech wiadomości. Wiadomości te są już zaszyfrowane dzięki fazie pierwszej IKE. Pierwsza wiadomość służy do wymiany informacji o tworzonym SA i wysłana jest w formie propozycji. Druga wiadomość jest odpowiedzią i zatwierdzeniem. Wśród przesyłanych informacji mogą być zawarte pola Proxy-ID (w zależności od polityki bezpieczeństwa) lub też może nastąpić ponowna wymiana kluczy publicznych DH i obliczenie tajnego klucza (uzależnione od włączonej bądź wyłączonej funkcji PFS (ang. *Perfect Forwarding Secrecy*).[2d]



Rysunek 33 Opracowanie własne: Faza druga IKE

4.4 Warstwa czwarta ISO/OSI: Protokoły SSL/TLS



Rysunek 34 Opracowanie własne: zaznaczone protokoły SSL/TLS na tle modelu ISO/OSI

Protokół SSL (ang. *Secure Socket Layer*) został opracowany przez firmę Netscape Communications Corporation w 1994 roku. Jest protokołem typu klient-serwer pozwalającym na nawiązanie bezpiecznego połączenia z użyciem certyfikatów. Według początkowych założeń miał być protokołem pozwalającym na szyfrowanie

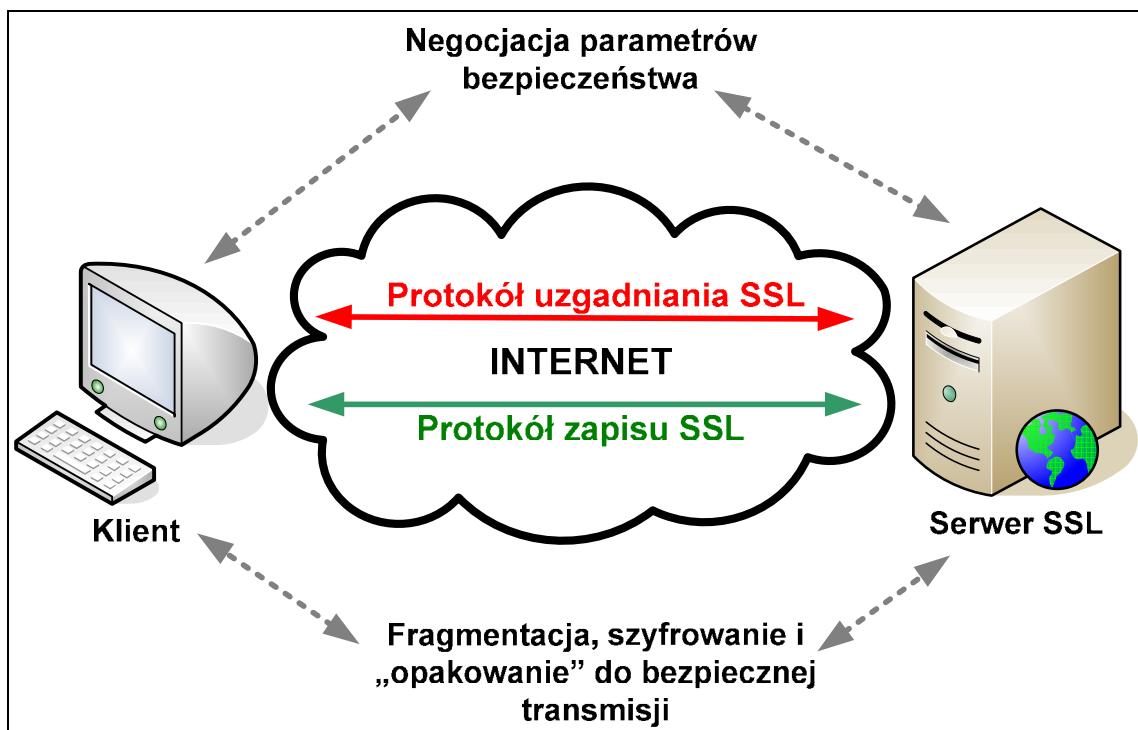
połączeń Internetowych dowolnego typu, lecz w praktyce najczęściej używany jest po dziś dzień dzisiejszy do zabezpieczenia połączeń z serwerami WWW (ang. *Word Wide Web*). Wykorzystuje on zarówno symetryczne i asymetryczne (z kluczem publicznym) algorytmy szyfrowania. Pozwala realizować ochronę integralności danych, autentyczność, jak i wymianę kluczy kryptograficznych. Specyfikacja protokołu SSL jest publicznie dostępna dlatego też jest on wspierany od strony klienta przez wszystkie obecnie używane graficzne przeglądarki internetowe oraz przez większość liczących się na rynku serwerów WWW.

Protokół SSL zapewnia trzy podstawowe komponenty zabezpieczania:

- ✓ Uwierzytelnienie - możliwość weryfikacji serwera lub serwera i klienta,
- ✓ Poufność – szyfrowanie informacji tak, aby treść poufna informacji mogła być zrozumiała tylko dla znających klucz deszyfrujący,
- ✓ Integralność – zabezpieczenie informacji na wypadek celowej bądź przypadkowej modyfikacji podczas transaktu danych.

SSL to protokół warstwy transportowej ISO/OSI, zawierający dwa sub-protokoły:

- uzgodnienia warunków transmisji (ang. *SSL Handshake Protocol*)
 - Autoryzacja serwera wobec klienta,
 - Wybór algorytmów szyfrowania i poziomu bezpieczeństwa,
 - Opcjonalnie (autoryzacja klienta wobec serwera),
 - ustalenie połączenia SSL,
 - uwierzytelnianie.
- zapisów (ang. *SSL Record Protocol*).
 - Podział danych na mniejsze fragmenty
 - zabezpieczenie danych przed ingerencją poprzez „opakowanie” (ang. *Wrapper*)
 - szyfrowanie danych i dołączenia opakowania



Rysunek 35 Opracowanie własne: Protokół SSL/TLS

Zaletą SSL jest fakt, że działa on w oparciu o protokół TCP, a więc można go łatwo zastosować do zabezpieczenia protokołów warstwy aplikacyjnej, które same w sobie szyfrowania nie obsługują (np.: SMTP, HTTP, POP3, IMAP) tworząc nowe bezpieczne protokoły niewrażliwe na prostego typu ataki osób trzecich.

| PODATNE NA ATAK TYPU „SPOOFING” | | CHRONIONE PRZED PODSLUCHEM i MODYFIKACJĄ | |
|------------------------------------|----------|---|----------|
| BEZ SSL | PORT TCP | Z SSL | PORT TCP |
| HTTP | 80 | HTTPS | 443 |
| POP3 | 110 | POP3S | 995 |
| IMAP | 143 | IMAPS | 585 |
| SMTP | 25 | SSMTP | 465 |

Tabela 8 Opracowanie własne: SSL jako zabezpieczenie różnych aplikacji

Jako wadę zaliczyć można fakt, że SSL nie spełnia zasad niezaprzeczalności.[1][5][6]

4.4.1 Zasada działania SSL

Znajdujące się na stronach WWW formularze i tekst w chwili przesyłania danych do/z serwera są przesyłane przez sieć otwartym tekstem, który można stosunkowo łatwo przechwycić (szczególnie w sieci LAN). Jeśli serwer używa protokołu SSL do komunikacji z przeglądarką, wówczas informacja w obie strony (między serwerem WWW a przeglądarką) jest przesyłana przez sieć w sposób zaszyfrowany, co w znacznym stopniu utrudnia *sniffing*.

Realizacja bezpiecznej komunikacji SSL/TLS odbywa się przy pomocy algorytmu RSA (ang. *Rivest - Shamir - Adleman*). Każdy serwer akceptujący "bezpieczne" połączenia posiada swój klucz publiczny, który wysyła klientowi (przeglądarce nawiązującej z nim połączenie). Certyfikat serwera podpisany jest przez zaufany ośrodek jakim może być urząd ds. certyfikatów CA (ang. *Certification Authorities*). Aby certyfikat serwera został zaakceptowany przez przeglądarkę klienta musi znajdować się na wbudowanej w nią liście znanych i zaufanych CA wraz z ich kluczami publicznymi. Urzędy certyfikacyjne prowadzone są przez firmy, które zostały upoważnione przez właściciela algorytmu *RSA Data Security Inc.* (przykładowe CA: *Thawte, Verisign*)

Klient weryfikuje certyfikat serwera za pomocą klucza publicznego udostępnionego przez CA i jego klucza publicznego.

Następnym etapem komunikacji jest uzgodnienie klucza (wymiana). Klient generuje tzw. klucz sesji, czyli losową wartość (ang. *Pre-Master Secret*), która następnie szyfrowana jest za pomocą klucza publicznego (*RSA*) serwera. Następnie serwer odszyfrowuje tą wartość używając swojego klucza prywatnego RSA. Długość klucza używanego do wymiany informacji zależy zarówno od wersji przeglądarki jak i samego serwera WWW.

Dla kluczy asymetrycznych długością sugerowaną jest 1024 bitów. W przykładzie SSL 128bitów - podana w bitach długość określa długość użytego klucza symetrycznego. Może wynosić 40, 56 lub 128 bitów przy czym im dłuższy klucz tym prawdopodobieństwo rozszyfrowania danych mniejsze.

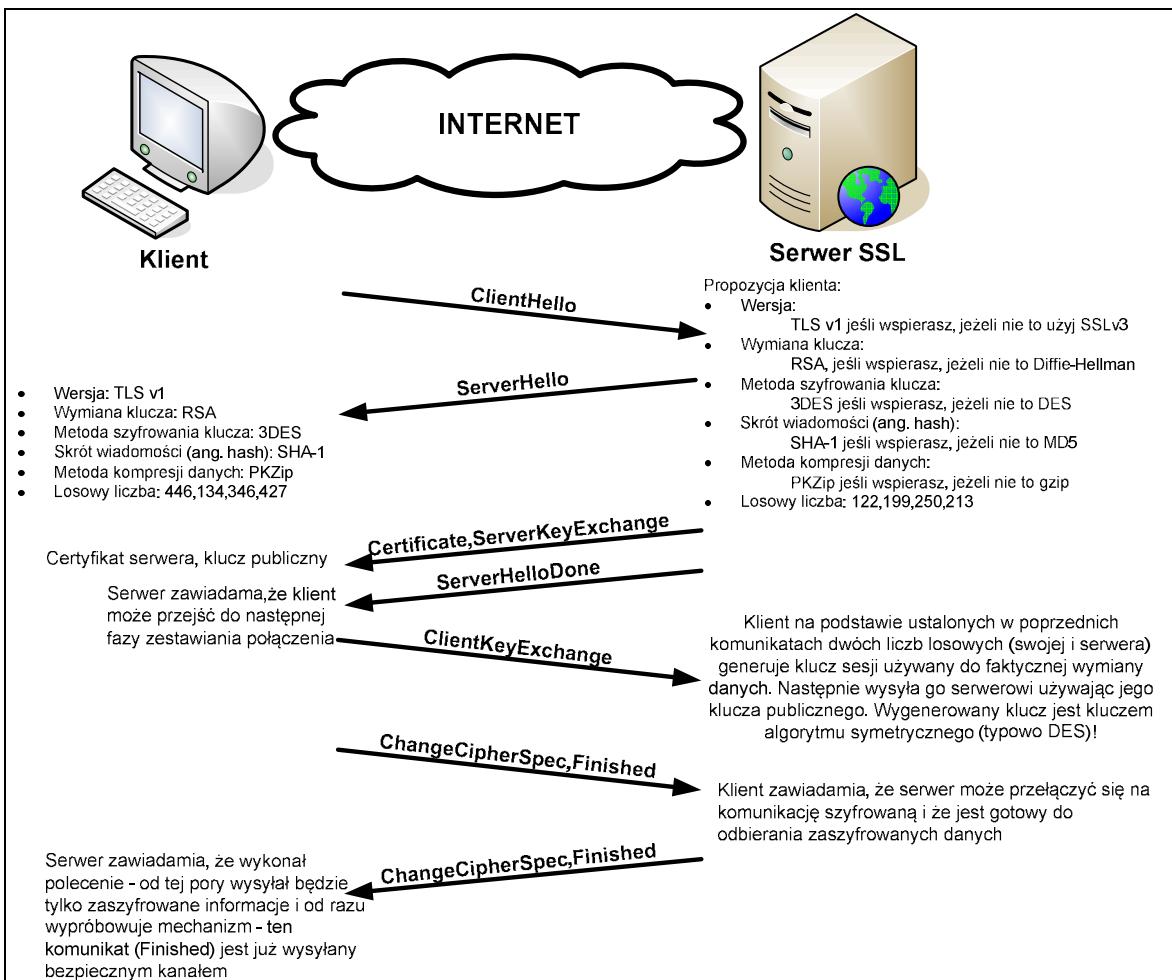
Następnie serwer generuje 3 tajne klucze dla wiadomości przesyłanych od serwera do klienta. Pierwszy klucz służy do odszyfrowania, drugi klucz do sprawdzenia integralności wiadomości (funkcja skrótu *HMAC*), i trzeci klucz jest używany do zainicjalizowania szyfru (IV). Klucze te są używane tylko dla wiadomości przesyłanych

w kierunku serwer-klient. Serwer generuje trzy inne klucze dla wiadomości przesyłanych w kierunku klient-serwer. Klient podobnie jak serwer także musi wygenerować dokładnie takie same klucze.

Następnie serwer kompresuje wiadomość korzystając z uzgodnionej metody kompresji, haszuje (ang. *Hash*) skompresowane wiadomości i klucz *HMAC* tworząc *HMAC*, następnie szyfruje kombinację *HMAC* i spakowanych wiadomości za pomocą klucza DES (od serwera do klienta).

Klient (przeglądarka) otrzymując zaszyfrowaną wiadomość - odwraca cały proces: odszyfrowuje kombinację *HMAC* i spakowanych wiadomości używając jego kopii klucza DES (od serwera do klienta), uwierzytelnia wiadomość w dwóch krokach. Po pierwsze haszuje odszyfrowane spakowane dane z kluczem *HMAC*. Potem porównuje *HMAC* z kroku 1 z *HMAC* uzyskanym z haszowania.

Klient dekompresuje i odzyskuje tekst jawnny. Zasada działania protokołu SSL w uproszczonej zasadzie – zaprezentowana na rysunku poniżej.[1i]



Rysunek 36 Opracowanie własne: SSL Zasada działania

4.4.2 Wersje SSL

Obecnie najczęściej używaną wersją jest trzecia odsłona protokołu SSL (3.1) - uważanego jako standard bezpiecznej transmisji danych w Internecie i rozwijany pod nazwą TLS 1.0 (ang. *Transport Layer Security*).[1i][1]

- SSL 1 – ta wersja miała poważną dziurę, brak procedury weryfikującej uzgodnienie szyfrowania przez co atakujący mógł wymusić używanie przez strony najsłabszego szyfru obsługiwanej przez obie strony (np. 40bitowy), ze złamaniem którego mógł sobie poradzić znacznie łatwiej niż z szyfrem, który strony wybrałyby normalnie.
- SSL 2 – wersja weryfikuje procedurę negocjacyjną.
- SSL 3 – wersja obecnie najczęściej używana.

- TLS 1.0 – rozwinięcie SSL 3 opisane w dokumencie RFC 2246.
- TLS 1.1 – wersja obecnie rozwijana, opisana w dokumencie RFC 4346, zalecana przez IETF jako standard i coraz częściej używana. Wyjaśnia ona pewne niejednoznaczności i dodaje nowe zalecenia wynikające z praktyki użycia – opisano to w RFC 4366, RFC 4680 i RFC 4681.

4.5 Warstwa siódma ISO/OSI: PGP, S/MIME, SSH

4.5.1 PGP

PGP (ang. *Pretty Good Privacy*) – tłumacząc dosłownie: “całkiem dobra prywatność” jest projektem, który zapoczątkowany został w 1991 przez Philipa Zimmermanna i rozwijany przy pomocy społeczności programistów z całego świata.

PGP pozwala:

- ✓ szyfrować i deszyfrować przesyłane wiadomości,
- ✓ podpisywać je cyfrowo,
- ✓ weryfikować autentyczność nadawcy (pod warunkiem że ten także korzysta z PGP),
- ✓ zarządzać kluczami.

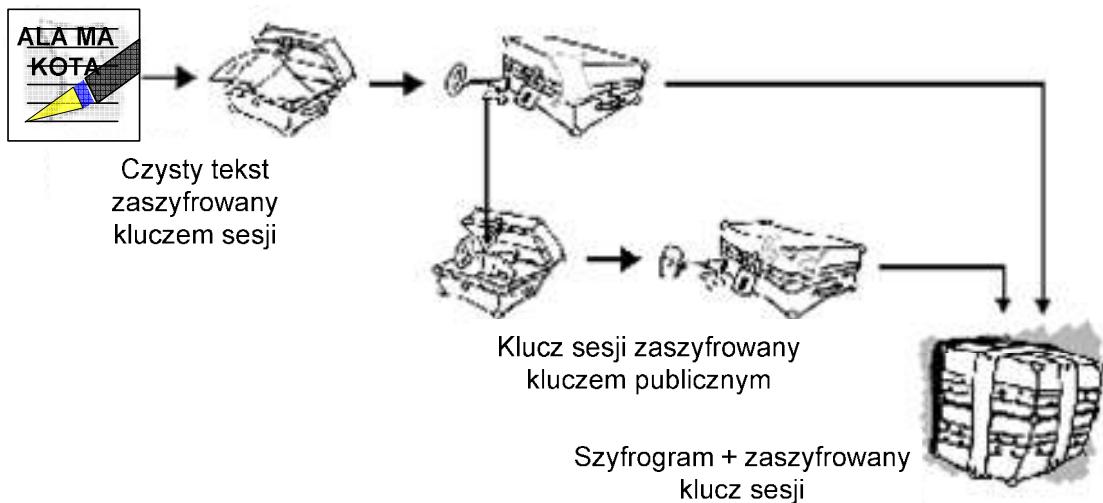
Podpis cyfrowy

Cyfrowy podpis daje odbiorcy wiadomości możliwość weryfikacji, czy otrzymany drogą elektroniczną został wysłany przez „tą” a nie inną osobę, oraz pewność, że nie została ona w żaden sposób zmodyfikowana podczas przesyłania. Podpis cyfrowy ma taką samą ważność w świecie elektronicznego biznesu jak podpis odręczny na kartce papieru, przy czym podpis odręczny jest zdecydowanie łatwiejszy do podrobienia.

Nadawca wiadomości używa PGP do cyfrowego podpisu dla wiadomości stosując do tego celu algorytmu RSA lub DSA. Aby to uczynić z pomocą PGP tworzony jest *Hash* (skrót wiadomości) z czystego tekstu, a następnie tworzy cyfrowy podpis ze skrótu wiadomości oraz prywatnego klucza nadawcy.

Szyfrowanie wiadomości:

Kiedy użytkownik szyfruje czysty tekst za pomocą PGP, w pierwszej kolejności tekst zostaje skompresowany, następnie tworzony jest klucz sesji (ang. *Session Key*), który jest ważny tylko jeden raz (klucz ten jest losową liczbą powstającą na podstawie ruchów myszy czy też przypadkowych przyciśnięć przycisków klawiatury). Klucz sesji użyty zostaje do zaszyfrowania czystego tekstu. Kiedy dane zostają zaszyfrowane, klucz sesji zostaje zaszyfrowany kluczem publicznym odbiorcy wiadomości a następnie wysłany wraz z szyfrogramem (zaszyfrowanymi danymi) do odbiorcy.

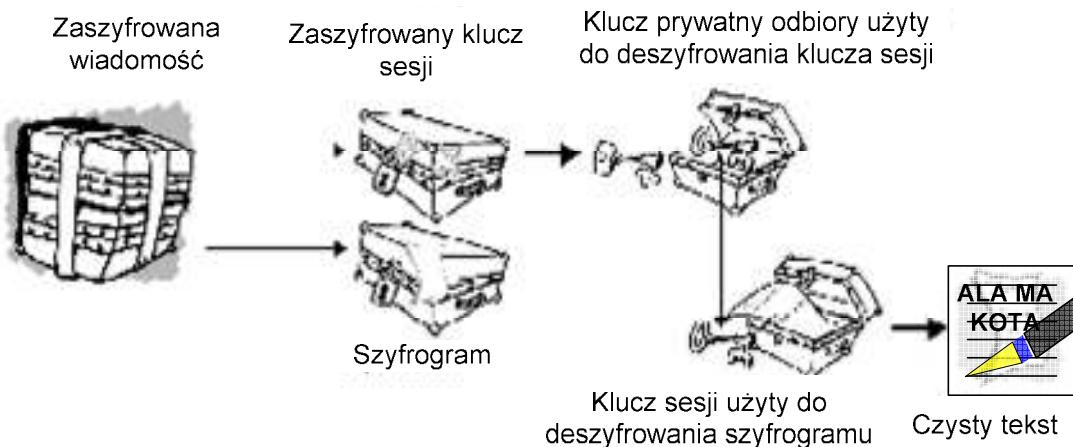


Rysunek 37 Opracowanie własne: PGP szyfrowanie

Deszyfrowanie wiadomości:

Odbiorca używa swojego klucza prywatnego do odtworzenia tymczasowego klucza sesji, którego PGP używa do deszyfrowania szyfrogramu.

Szyfrowanie kluczem publicznym wymusza jak najszerze propagowanie własnego klucza publicznego wśród osób które mają zaszyfrowane wiadomości otrzymywać, tak aby dane mogły być do nas przesłane, co daje rozwiązanie problemu dystrybucji kluczy pomiędzy użytkownikami.



Rysunek 38 Opracowanie własne: PGP deszyfrowanie

Dystrybucja kluczy publicznych może odbywać się w następujący sposób:

- Poprzez ręczną wymianę:
 - Dyskietka
 - CD-ROM
 - Transfer plików
- Za pośrednictwem Serwerów Certyfikatów czy też PKI (ang. *Public Key Infrastructures*) – pełniących rolę bazy danych przechowującej klucze publiczne użytkowników. Serwer certyfikatów w korporacjach daje dodatkową możliwość zarządzania uprawnieniami – tak by np. klucze użytkowników spełniające określone wymagania mogły być przechowywane bądź użyte.

4.5.2 S/MIME

S/MIME (ang. *Secure/Multipurpose Internet Mail Extensions*) to opracowany przez firmę RSA Data Security standard służący do przekazywania zaszyfrowanych wiadomości. Standard S/MIME zapewnia ochronę w zakresie:

- autentyczności wiadomości,
- integralności,
- poufności,
- oraz niepodważalności (podpis cyfrowy).

Podobnie jak PGP pozwala na szyfrowanie poczty elektronicznej, jednak wykorzystuje do tego celu certyfikaty X.509(szyfrowanie kluczem publicznym). Zasada

działania zarówno PGP jak i S/MIME jest taka sama. Każdy użytkownik posiada dwa klucze cyfrowe - prywatny (tajny) i publiczny (udostępniony). Użytkownik A chcąc przesyłać tajne dane do użytkownika B, używa do szyfrowania klucza publicznego użytkownika B. Użytkownik B chcąc odszyfrować dane – używa do tego celu swojego klucza prywatnego. S/MIME, w odróżnieniu od PGP, posługuje się pojęciem certyfikatu, szerszym niż pojęcie zestawu klucz publiczny-klucz prywatny.

Certyfikaty X.509, służące głównie do szyfrowania poczty elektronicznej (na podstawie standardu S/MIME), zawierają w sobie klucz publiczny i prywatny, oprócz tego zawierają dodatkowe informacje o tożsamości właściciela certyfikatu. Certyfikat cyfrowy X.509 nie może być wystawiony samodzielnie – tak jak to mogło mieć miejsce przy PGP. Wystawianiem certyfikatów zajmują się urzędy certyfikacji - CA (ang. *Certificate Authority*), lecz operacja wystawienia certyfikatu jest operacją płatną (dla osoby prywatnej jest to kwota kilkanaście dolarów na rok).[1i][1][6]

4.5.3 SSH

SSH (ang. *Secure Shell*) to standard protokołów komunikacyjnych używanych w sieciach komputerowych TCP/IP, w architekturze klient-serwer. SSH jest następcą protokołu TELNET służącego do terminalowego łączenia się ze zdalnymi komputerami, bądź aktywnymi urządzeniami sieciowymi. SSH różni się od TELNET tym, że transmisja wszelkich danych odbywa się w sposób szyfrowany oraz możliwe jest rozróżnienie użytkowników (na kilka sposobów) nawiązujących zdalne połączenie, a co za tym idzie przyznanie im różnych uprawnień. Za pomocą rodziny protokołów SSH możliwym jest także:

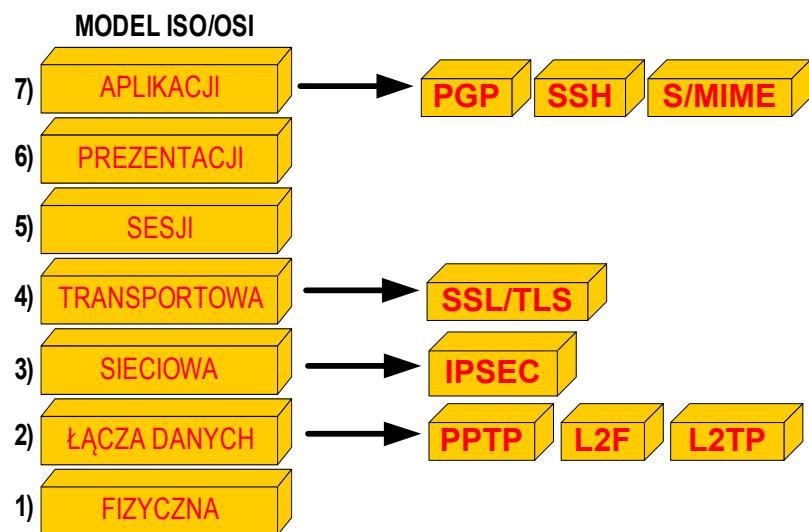
- ✓ przesyłania plików (SCP, SFTP),
- ✓ zdalnej kontroli zasobów,
- ✓ tunelowania,
- ✓ i wielu innych zastosowań.

Obecnie używane są dwie wersje SSH: 1 i 2 przy czym wersja 1 ze względu na podatność na ataki typu *Man-In-The-Middle* nie jest zalecana. Wersja 2 wspiera dowolne sposoby szyfrowania (np. AES, 3DES, DES, Blowfish) i cztery sposoby rozpoznawania użytkownika, podczas gdy pierwsza wersja obsługuje tylko stałą listę

algorytmów szyfrujących i tylko dwa sposoby rozpoznawania użytkownika (klucze RSA/DSA i zwykłe hasło).

Serwer SSH używany do podłączenia się do urządzeń w trybie terminalowym pracuje zwykle na porcie TCP/22 (chociaż nie jest to reguła).[1i][2][3]

4.6 Porównanie metod zabezpieczeń przesyłania danych



Rysunek 39 Opracowanie własne:
Porównanie metod zabezpieczeń w różnych warstwach modelu ISO/OSI

Najbardziej uniwersalnym protokołem jeśli chodzi o bezpieczeństwo i sposób implementacji we współczesnych bezpiecznych wirtualnych sieciach prywatnych jest IPsec. Zapewnia on najwyższy poziom bezpieczeństwa w warstwie sieciowej, używa najnowszych i najbezpieczniejszych algorytmów szyfrowania (np. 3DES, AES256). Z pomocą IPsec można zrealizować tunele łączące zdalne lokalizacje firmy w sposób przezroczysty (pełny dostęp do zasobów sieci) dla użytkowników, a także zrealizować połączenia typu *Remote-Access*, aby zapewnić łączność telepracownikom z oddziałem. Dodatkowym atutem przemawiającym na korzyść IPsec – jest łatwa integracja z sieciami bezprzewodowymi.

Protokół ten oparty jest o otwarte standardy (łatwa współpraca urządzeń pochodzących od różnych producentów) i mechanizmy zapewniające bezpieczną transmisję danych.

Stosując IPsec można zagwarantować poufność, integralność i autentyczność przesyłanych danych. Daje zatem pewność, że dane nie zostały w celowy bądź przypadkowy sposób zmienione a dzięki zastosowaniu silnych technik kryptograficznych, że nawet podczas próby przechwycenia danych – intruz nie będzie w stanie odczytać informacji. Nie bez znaczenia jest też zapewnienie autentyczności połączenia – czyli gwarancji, że dane otrzymane są z pewnego i znanego źródła, a nie od osoby trzeciej podszywającej się.

Największym konkurentem protokołu IPsec jest SSL/TLS opracowanym przez firmę Netscape w roku 1994. Jest protokołem działającym w warstwie aplikacji i pozwala chronić wiele z nich działających w oparciu o protokół TCP np. POP3, SMTP, HTTP tworząc ich bezpieczne odmiany POP3S, SSMTP, HTTPS. SSL w wersji 3.1 (zwany TLS 1.0) jest obecnie standardem służącym do ochrony danych przesyłanych w Internecie. Swoją popularność zawdzięcza przede wszystkim dzięki temu, że wykorzystuje protokół HTTP, którym posługują się wszystkie obecne na rynku graficzne przeglądarki internetowe. Z pomocą SSL możliwe jest szyfrowanie i uwierzytelnianie (dzięki algorytmom kryptograficznym symetrycznym i asymetrycznym), ale i zapewniona jest integralność (dzięki użyciu funkcji skrótu MD5 czy SHA-1), autentyczność (dzięki wbudowanym w przeglądarki certyfikatom urzędów SA) jak i mechanizm wymiany kluczy kryptograficznych.

Wykorzystując dodatkowe kontrolki ActiveX lub aplikacje Java działające z poziomu przeglądarki internetowej, dzięki SSL można zestawiać dwukierunkowy tunel VPN do korporacyjnej sieci, przesyłając przez niego nie tylko wybiórcze aplikacje działające na protokole TCP, ale cały ruch IP. Stosowanie dodatkowych kontrolek ActiveX daje dodatkową przewagę nad IPsec – możliwość dokładnej weryfikacji komputera pod kątem ostatnich aktualnień systemu operacyjnego, obecności programu antywirusowego czy też przynależności do domeny Active Directory. Protokół IPsec sam w sobie nie posiada podobnych własności i aby osiągnąć podobny cel koniecznym jest instalacja dodatkowych programów weryfikujących, dodatkowo płatnych.

Porównując IPsec z SSL widać łatwo, że rodzaj danych przesyłanych poprzez tunele VPN nie gra roli, co zaś jest ogromną przeszkodą dla SSL (bez stosowania kontrolek ActiveX lub aplikacji Java). Natomiast na korzyść głównego rywala IPsec można zaliczyć możliwość kontroli uprawnień do konkretnych zasobów np. witryny WWW na podstawie np. loginu i hasła. Podczas implementacji SSL można napotkać

problem z przystosowaniem niektórych aplikacji działających w oparciu o protokół HTTP – wtedy koniecznym jest stosowanie kontrolek ActiveX lub aplikacji napisanych w języku Java, lecz jest to kolejny punkt obawy o bezpieczeństwo danych, gdyż aplikacje takie mogą być podatne na ataki złośliwego oprogramowania (*Malware*), podobnie ma się sprawa samej przeglądarki internetowej.

Porównując cechy obu protokołów, należy także rozpatrzyć kwestie ekonomiczne. Biorąc pod uwagę możliwość uzyskania zdalnego dostępu do sieci korporacyjnej (*Remote-Access*) przez telepracownika – należy zwrócić szczególną uwagę na koszty licencji zarówno po stronie koncentratorów VPN jak i po stronie klienta (oprogramowanie służące do nawiązania połączenia VPN) gdyż w przypadku IPsec i SSL VPN będą one inne.

Zarówno SSL VPN jak i IPsec VPN są dobrymi metodami dostępu dla zdalnych pracowników. IPsec VPN stosowany jest zwykle do połączeń VPN typu *Site-to-Site* (między oddziałami firmy) natomiast SSL VPN dla pracowników zdalnych (wykorzystując przeglądarkę internetową) łączących się do oddziału firmy. Nie ma jednak żadnych problemów w odwrotnej implementacji, czy też wykorzystaniu tylko jednej metody dostępu bądź obu na raz.

Tabela 9 Porównanie IPsec i SSL

| IPsec | SSL |
|---|---|
| Bezpieczeństwo danych: Zapewnia poufność, integralność, autentyczność i niezaprzeczalność | |
| Ochrona warstwa sieciowej i wszystkich wyższych | |
| Przeznaczenie: Realizacja bezpiecznego połączenia VPN | Przeznaczenie: Realizacja bezpiecznych transakcji elektronicznych, poczta elektroniczna, aukcje internetowe, połączenia VPN typu <i>Remote-Access</i> |
| Możliwość przeniesienia wszystkich protokołów i zapewnienia przezroczystego, pełnego dostępu do sieci | |
| Konieczna jest przeglądarka Internetowa i stosowna akcja użytkownika, a także dostosowanie aplikacji do działania z SSL | |

| | |
|---|--|
| bez ograniczeń. | oraz dodatkowe kontrolki ActiveX lub aplikacje Java |
| Uprawnienia użytkowników: Możliwość kontroli uprawnienień do konkretnych zasobów, dla adresów IP, dla użytkowników. Potrzeba dodatkowej autoryzacji do konkretnych aplikacji. | Uprawnienia użytkowników: Całkowita kontrola nad uprawnieniami użytkownika do konkretnych witryn a nawet ich części składowych (portale z prawami dostępu dla określonych użytkowników) |
| Przeznaczenie: realizacja połączeń VPN typu <i>Site-to-Site</i> oraz <i>Remote-Access</i> (dla telepracowników) | Przeznaczenie: realizacja połączeń VPN typu <i>Remote-Access</i> (dla telepracowników), ekstranety |
| Bezpieczeństwo komputera klienta: Brak możliwości sprawdzenia komputera pod kątem aktualizacji, oprogramowania antywirusowego, czy też dodatków do systemu operacyjnego, bez instalacji dodatkowego oprogramowania do weryfikacji. | Bezpieczeństwo komputera klienta: Możliwości sprawdzenia komputera zanim zostanie nawiązanie połączenie VPN pod kątem aktualizacji, oprogramowania antywirusowego i dodatków do systemu operacyjnego za pomocą specjalnej kontrolki ActiveX instalowanej z poziomu przeglądarki, a także umieszczenie komputera w specjalnej grupie podwyższonego ryzyka (ze zmniejszonymi uprawnieniami do sieci firmowej) |

Tabela 10 Opracowanie własne: Porównanie IPSec i SSL

Słabszą konkurencją wymienionych wcześniej metod zabezpieczeń komunikacji jest protokół SSH opracowany przez firmę SSH Communications Security. Stosowany najczęściej do zapewnienia bezpiecznej (szyfrowanej) komunikacji z serwerami terminalowymi, aktywnymi urządzeniami sieciowymi, tunelowania oraz do transferowania danych. Obecnie stosowana wersja SSHv2 wspiera dowolne sposoby szyfrowania (np. AES, 3DES, DES, Blowfish) i cztery sposoby rozpoznawania użytkownika. Podczas transmisji zapewnia poufność, uwierzytelnianie i integralność danych.

Różnicą pomiędzy IPsec a SSH jest to, że SSH pracuje w warstwie aplikacji i zabezpieczenie ruchu odbywa się od samego początku a nie jak w przypadku IPsec w

warstwie sieci. Ograniczeniem protokołu SSH w porównaniu do IPsec jest to, że możliwa jest komunikacja szyfrowana tylko dla protokołu TCP, nie zaś jak w przypadku IPsec całego ruchu IP. Na korzyść SSH można natomiast zaliczyć mały narzut danych, podczas przesyłania (SSH znajduje się w 7 warstwie modelu referencyjnego ISO/OSI) i to tam właśnie odbywa się szyfrowanie danych, podczas gdy IPsec szyfrując wszystko od 3 warstwy modelu ISO/OSI w góre. Ze względu a ograniczenia stosowania tylko do protokołu TCP - SSH nie jest na tyle uniwersalnym protokołem, by samodzielnie i całościowo zapewnić bezpieczną komunikację użytkowników pomiędzy oddziałami firm, oraz by mógł zastąpić rozwiązań IPsec czy też SSL.

Protokoły PGP i S/MIME podobnie jak SSH pracują w warstwie aplikacji i podobnie jak SSH mają pewne ograniczenia jeśli chodzi o zakres działania. PGP i S/MIME służą głównie (choć nie jedynie) do zabezpieczenia wiadomości elektronicznych przed niepowołanymi osobami, szyfrowania plików i tworzenia cyfrowych podpisów. Protokoły te zapewniają ochronę integralności wiadomości, uwierzytelnienie i niepodważalność nadania.

Podobnie jak SSH, protokoły PGP i S/MIME są specjalistycznymi protokołami, które powstały w konkretnym celu – zabezpieczenia danych w warstwie aplikacji. Nie są na tyle uniwersalne by można było na ich podstawie zbudować kompletną i bezpieczną sieć dla użytkowników korzystających z różnych aplikacji. Stosowanie kombinacji wyżej wymienionych metod zabezpieczeń sieci – pozwoli podnieść poziom bezpieczeństwa przesyłanych danych.

Z powyższych porównań nie można wyciągnąć prostego wniosku, czy dana metoda zabezpieczeń jest lepsza czy gorsza, można jednak zauważyc, że implementacja danej metody jest ściśle uzależniona od sytuacji i potrzeb stosowania. Projektując bezpieczne sieci należy zadbać o to, by na każdym etapie przesyłania danych zapewnić maksimum bezpieczeństwa, do czego wykorzystać można omówione wcześniej metody.

5 Metody i sposoby uwierzytelniania

Za pomocą protokołów IPsec, SSL i innych omówionych wcześniej możliwym jest zaszyfrowanie danych – dzięki czemu osoby niepowołane nie mogą ich odczytać ani zmodyfikować podczas przesyłania gdyż jest sprawdzana integralność danych, jednakże funkcje te niewiele znaczą gdy nie ma pewności, że urządzenie bądź użytkownik po drugiej stronie komunikacji np. tunelu VPN jest zaufane(y) i jest tym, za które/kogo się podaje. Zatem konieczna jest weryfikacja stron(y) zanim dojdzie do jakiekolwiek wymiany danych. W systemach informatycznych stosuje się trzy rodzaje uwierzytelniania:

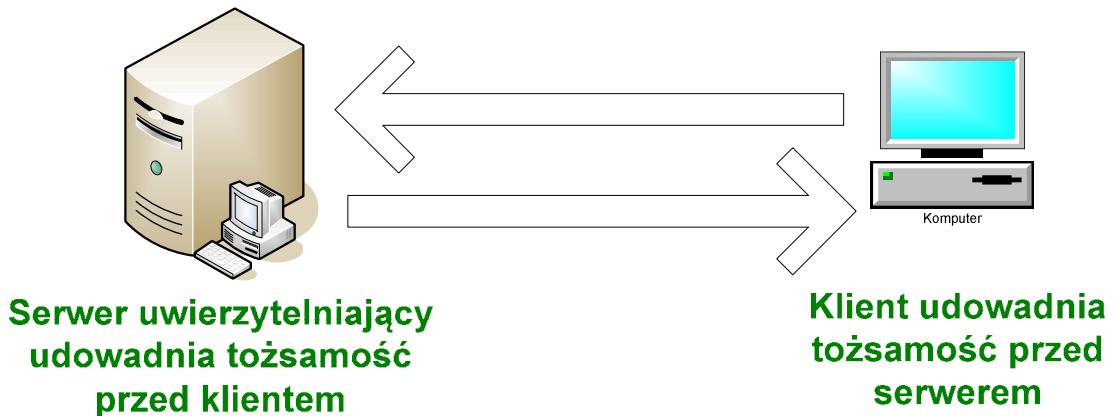
- Uwierzytelnienie jednokierunkowe,
- Uwierzytelnienie dwukierunkowe,
- Uwierzytelnienie z udziałem zaufanej strony trzeciej.

Uwierzytelnienie jednokierunkowe polega na uwierzytelnieniu jednego podmiotu (uwierzytelnianego) np. klienta logującego się aplikacji lub też aktywnego urządzenia sieciowego, wobec drugiego (uwierzytelniającego) – serwera. Udowodnienie tożsamości następuje przez zweryfikowanie danych uwierzytelniających przekazanych przez podmiot uwierzytelniany. Przykładem danych uwierzytelniającymi może być np. identyfikator użytkownika (login) i jego hasło dostępu.



Rysunek 40 Opracowanie własne: Uwierzytelnianie jednokierunkowe

Uwierzytelnianie dwukierunkowe – polega na jednoczesnym lub sekwencyjnym udowodnieniu tożsamości obu podmiotów (klienta i/lub serwera). Jeżeli uwierzytelnianie następuje sekwencyjnie czyli najpierw klient przed serwerem, a później serwer przed klientem, to taki rodzaj uwierzytelnianie nazywamy dwuetapowym. Gdy udowodnienie tożsamości odbywa się jednocześnie to taki sposób uwierzytelnienia stron nazywamy jednoetapowym.

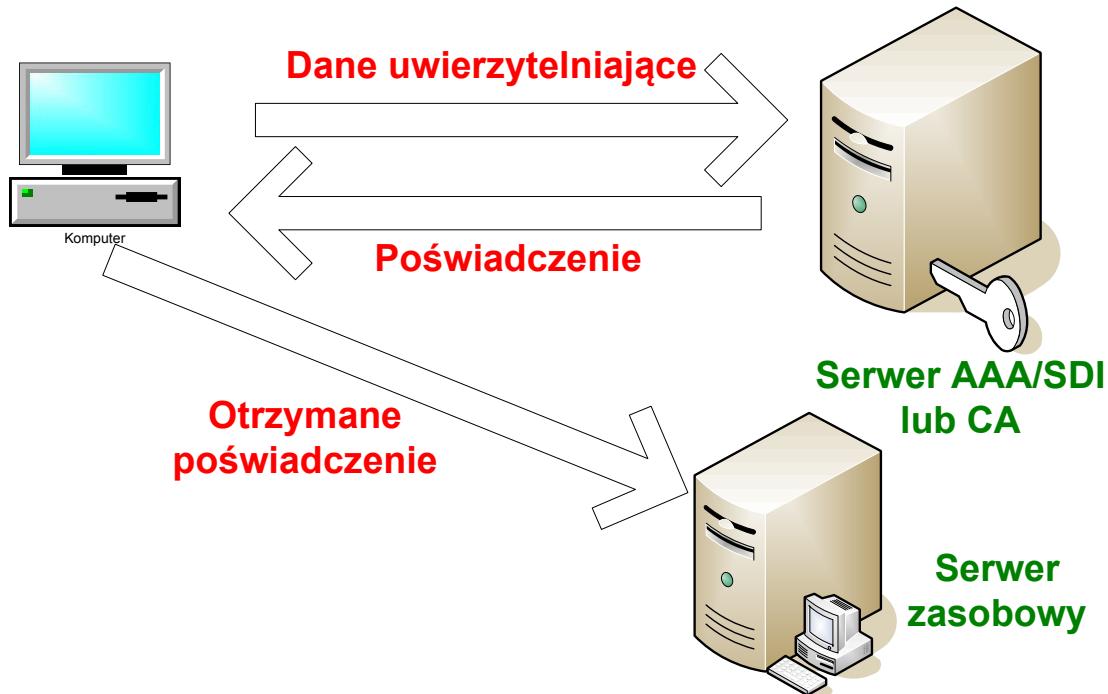


Rysunek 41 Opracowanie własne: Uwierzytelnienie dwukierunkowe

Uwierzytelnianie z udziałem zaufanej trzeciej strony – polega na tym, że w procesie udowodniania tożsamości klienta wobec serwera etapem weryfikacji danych uwierzytelniających zajmuje się zaufana strona trzecia, którą może być serwer AAA znajdujący się w sieci lokalnej lub też zewnętrzny serwer np. urzędu certyfikacji SA bądź też serwer SDI (ang. *Security Dynamics Inc.*) czyli z użyciem tokenów.[1][6][7][1i]

Po pomyślnej weryfikacji klient otrzymuje poświadczenie, które następnie przedstawia serwerowi, do którego chce uzyskać dostęp. Największą zaletą uwierzytelnienia z udziałem strony trzeciej jest możliwość przesunięcia odpowiedzialności weryfikacji na wyspecjalizowane do tego celu urządzenie jakim jest serwer uwierzytelniający, który można poddać szczególnej ochronie zabezpieczeń. Warto zwrócić uwagę, że przypadku użycia serwera uwierzytelniającego do weryfikacji uprawnień przez różne aplikacje – poziom bezpieczeństwa tej operacji jest zawsze taki sam wysoki i nie jest koniczne stosowanie dodatkowych metod zabezpieczeń samych aplikacji.

Pozyskane przez klienta poświadczenie może być wykorzystane wielokrotnie eliminując potrzebę wielokrotnego podawania informacji przez klienta (tzw. SSO ang. *Single Sign-On*)



Rysunek 42 Opracowanie własne: Uwierzytelnianie z użyciem strony trzeciej

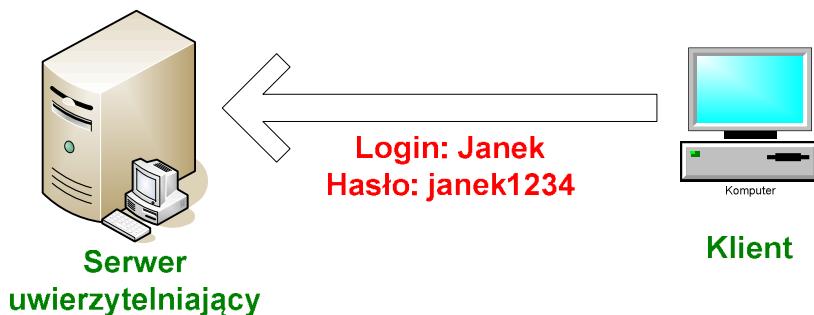
Wyróżnia się pięć różnych grup a zarazem możliwych metod uwierzytelnienia (uwierzytelniania) użytkowników i urządzeń:

- ✓ Nazwa użytkownika i hasło,
- ✓ Jednorazowe hasła,
- ✓ Cechy biometryczne,
- ✓ Klucz współdzielony,
- ✓ Cyfrowe certyfikaty.

5.1 Nazwa użytkownika i hasło

Nazwa użytkownika/hasło (ang. *Username and Password*) – W przypadku wielu współczesnych systemów informatycznych, aplikacji i systemów baz danych, nadal istnieje klasyczny mechanizm udowodnienia tożsamości (uwierzytelnienia) poprzez

podanie właściwej nazwy użytkownika (login) i hasła pasującego do tego konta. Proces weryfikacji inicjowany jest przez klienta, który chce uzyskać dostęp do aplikacji, bądź też systemu informatycznego Serwer pyta o nazwę użytkownika (login), a następnie o hasło i na podstawie pasującej (bądź nie) pary tworzącej dane uwierzytelniające wydaje decyzję o zaakceptowaniu bądź odrzuceniu prośby klienta. Niestety jeszcze w wielu przypadkach przesyłane dane uwierzytelniające (użytkownik i hasło) do starszych aplikacji wędrują tekstem jawnym, czyniąc je podatnym na atak polegający na podsłuchaniu informacji (ang. *Sniffing*). Na szczęście sytuacja ma się inaczej w przypadku logowania do współczesnych systemów operacyjnych np. z rodziny Windows czy Linux gdzie podane dane uwierzytelniające przesyłane są w postaci zaszyfrowanej.



Rysunek 43 Opracowanie własne: Metoda uwierzytelnienia login i hasło

Metoda uwierzytelnienia poprzez podanie loginu i hasła jest prosta w implementacji, ale niezalecana ze względu na jej liczne wady:

| | | |
|---|--|--|
| 1 | Hasła są możliwe do odgadnięcia | Atak typu <i>Brute-Force</i> – przeszukiwanie skończone |
| | | Atak typu <i>Dictionary</i> – z wykorzystaniem odpowiednio dużego słownika wyrazów |
| 2 | Hasła przesyłane w formie niezaszyfrowanej są podatne na atak poprzez podsłuchanie <i>Sniffing</i> | |
| 3 | Czas przez który można polegać na tajności hasła jest skońzoną wartością. Hasła wygasają i wymagają zmian co określony okres czasu. | |
| 4 | Hasła można wykraść o ile są przechowywane są w bazie danych lub pliku w formie niezaszyfrowanej, lub też użyty do szyfrowania algorytm jest możliwy do złamania w skończonym czasie | |
| 5 | Istnieje duże niebezpieczeństwo istnienia zaszytych w aplikacji loginów z domyślnymi | |

| | |
|---|---|
| | hasłami, które powinny być usunięte lub zmienione . |
| 6 | Hasła można pozyskać innymi metodami np. Social Engineering, czyli wyłudzenie haseł od nieświadomych zagrożeń użytkowników. |

Tabela 11 Opracowanie własne: Cechy metody uwierzytelnienia login/hasło

Hasła są podatne na próby odgadnięcia poprzez stosowanie ataków słownikowych (ang. *Dictionary*) lub też poprzez przeszukanie skończone (ang. *Brute-Force*). Atak słownikowy polega na próbie podstawienia w miejsce hasła jakie żąda aplikacji kolejnych pozycji ze słownika, celem znalezienia właściwego. Atak *Brute-Force* polega na podstawianiu w miejsce hasła kolejnych sekwencji znaków alfabetu (dużych i małych), znaków alfanumerycznych i symboli specjalnych tak by odgadnąć potencjalne hasło danego konta.

Mögliwym jest także próba odgadnięcia haseł z posiadanych (wykрадzionych) zaszyfrowanych danych, które powstały poprzez użycie jednokierunkowych funkcji skrótu. Atak na tak zaszyfrowane dane polega na porównaniu wyniku takich samych operacji jednokierunkowych funkcji skrótu na kolejnych hasłach ze słownika z hasłami w postaci zaszyfrowanej aż do chwili odnalezienia wzorca.

Z pomocą metody *Brute-Force* odnalezienie hasła jest bardzo czasochłonne gdyż - wymaga porównania każdej permutacji do odgadywanego hasła, co jest zależne od użytego alfabetu znaków i długości potencjalnego hasła.

Prawdopodobieństwo odgadnięcia hasła można wyrazić wzorem:

$$P = \frac{L * R}{N^k}$$

Gdzie

P- prawdopodobieństwo

L - czas ważności hasła

R - ilość prób na jednostkę czasu

N – alfabet

k –długość haseł

Aby utrudnić odgadnięcie hasła należy zatem:

- ✓ Stosować hasła zawierające możliwe dużo znaków (minimalnie 8), nie składające się ze znanych fraz bądź wyrazów,

- ✓ Przykładem dobrego hasła czyli takiego, które zawiera cyfry, duże i małe litery, znaki specjalne może być (np. Aw#VdV*abP),
- ✓ Wybierać hasło w sposób losowy nie wskazujący na możliwą inkrementację w czasie (np. Janek001, Janek002, Janek003 itd.),
- ✓ Zmieniać często hasło, szczególnie jeśli zajdzie podejrzenie, że hasło mogło zostać poznane przez osoby trzecie.

5.2 Jednorazowe hasła

Jednorazowe hasła (ang. *One Time Password*) - Idea wykorzystania haseł jednorazowych wynika z potrzeby ochrony ich przed przechwyceniem i wykorzystaniem możliwością wykorzystania przez osoby trzecie w przyszłości.

W tym przypadku zapewnienie poufności podczas przesyłania jednorazowego hasła nie gra już pierwszorzędnej roli – tak jak miało to miejsce przy metodzie login/hasło, gdyż przechwycone podczas tranzytu hasło a następnie użyte przez powołaną osobę traci ważność.

Zasada działania haseł jednorazowych, jak nazwa wskazuje, polega na tym, że można je użyć tylko raz. Hasła takie przy kolejnych próbach uwierzytelnienia mają inną postać (długość pozostaje taka sama jednak szyk liter i cyfr jest za każdym razem inny). Zatem przechwycone hasło jednorazowe po użyciu nie jest przydatne, ponieważ przy kolejnej próbie uwierzytelnienia będzie obowiązywać już nowe.

Stosujące jednorazowe hasła należy zadbać o to by procedura tworzenia kolejnych haseł, czyli matematyczny algorytm był odpowiednio skomplikowany, tak by odgadnięcie kolejnych haseł w czasie nie było możliwe lub było bardzo utrudnione.

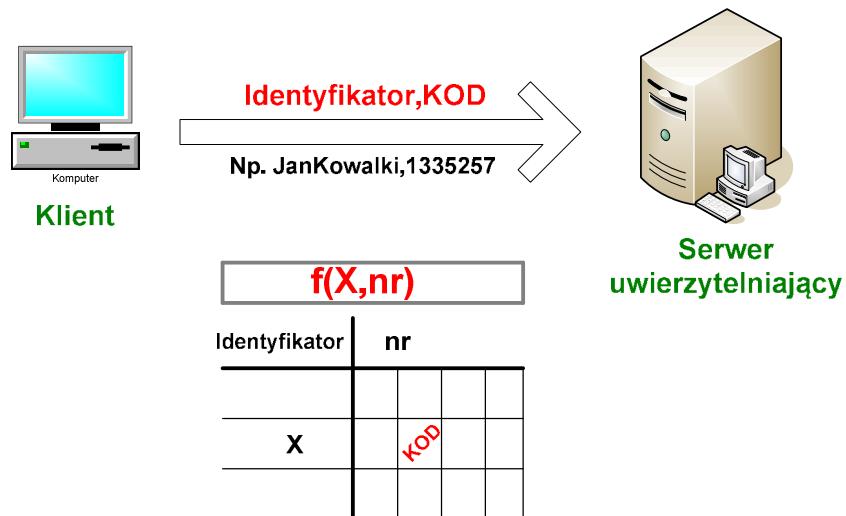
Hasła jednorazowe generowane mogą być na kilka sposobów:

| Metoda generowania hasła OTP | Przykład zastosowania |
|---|---|
| Lista haseł | Ponumerowane zdrapki, listy papierowe, SMSy |
| Synchronizacji czasu | Tokeny sprzętowe i programowe |
| Metoda <i>Challenge-Response</i> (pytanie – | Tokeny sprzętowe i programowe |

| | |
|-----------|--|
| odpowiedź | |
|-----------|--|

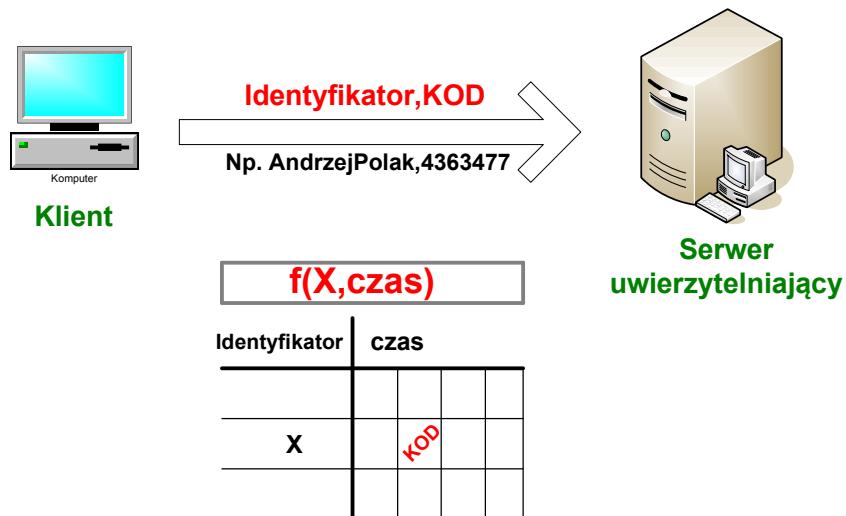
Tabela 12 opracowanie własne: Metody generowania hasel jednorazowych OTP

Listy hasel – to najtańsza i najprostsza metoda weryfikacji użytkowników, często wykorzystywana przez banki. Klient otrzymuje listę zawierającą zakryte, ponumerowane hasła. Taka sama lista znajduje się w bazie danych systemu uwierzytelniającego. Podczas logowania klient podaje swój identyfikator, zaś system weryfikujący prosi o podanie losowego hasła z listy użytkownika z odpowiednim numerem. Po pozytywnej weryfikacji klient wpuszczany jest do systemu informatycznego, a użyte hasło oznaczone jest w bazi danych, tak aby nie prosić użytkownika ponownie o hasło kryjące się pod tym numerem, zatem klient za każdym razem musi się posłużyć innym hasłem, aż do chwili wyczerpania się listy (wtedy otrzymuje od banku nową)



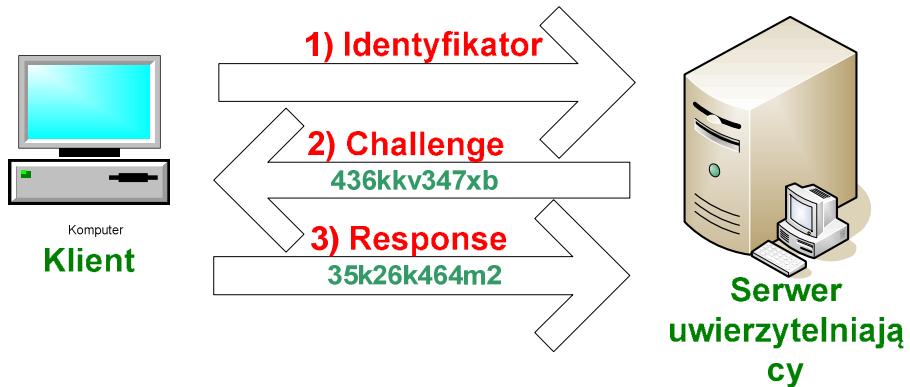
Rysunek 44 Opracowanie własne: Hasła Jednorazowe - Lista hasel

Synchronizacja czasu (ang. *Time Synchronization*) Hasło czyli kod w metodzie z synchronizacją czasu generowane jest za pomocą funkcji pewnego parametru X, którym może być np. numer seryjny tokenu, karty identyfikacyjnej, kod pin oraz drugi parametr funkcji - bieżącego czasu. W chwili kiedy serwer uwierzytelniający otrzyma parę identyfikator i hasło następuje procedura weryfikacji po stronie serwera. Uruchamiana jest taką samą funkcję jaka była uruchomiona po stronie użytkownika i następuje porównanie obu wartości. Jeśli wartości są zgodne – użytkownik jest pozytywnie zweryfikowany.



Rysunek 45 Opracowanie własne: Hasła Jednorazowe - Synchronizacja czasu

Metoda *Challenge-Response* polega na tym, że serwer uwierzytelniający najpierw pyta o identyfikator użytkownika (np. jego login), a następnie przesyła ciąg znaków *challenge* (wyzwanie) do użytkownika. Otrzymany ciąg znaków klient szyfruje kluczem (którym może być np. kod PIN do tokenu, tajne hasło) i odsyła do serwera uwierzytelniającego jako odpowiedz *response*. Serwer znając klucz szyfrujący klienta jest w stanie zweryfikować poprawność danych i na tej podstawie uwierzytelić klienta. Token służący do generowania jednorazowych wskazań w jednostce czasu może przyjmować postać zarówno sprzętową jak i programową, przy czym odmiana sprzętowa jest dużo bardziej bezpieczna ze względu na brak możliwości zdalnego przejęcia, uruchomienia czy skopiowania aplikacji generującej jednorazowe hasła. Sprzętowa odmiana tokenów, posiada wyświetlacz LCD, na którym prezentowane są jednorazowe hasła, a samo włączenie tokenu także chronione jest kodem PIN. Istnieją też odmiany tokenów sprzętowych bez klawiatury, gdzie hasła generowane są w pewnych odstępach czasu bez ingerencji użytkownika.



Rysunek 46 Opracowanie własne: Hasła Jednorazowe - Challenge-Response

5.3 Cechy biometryczne

Cechy biometryczne (ang. *Biometrics Technologies*) . Do tej pory omówione metody uwierzytelnienia wymagały od użytkownika posiadania pewnej wiedzy (w przypadku metody użytkownik/hasło sekretnego hasła) lub też posiadania pewnych przedmiotów (w przypadku generowanych haseł jednorazowych np. tokenu), aby móc udowodnić swoją tożsamość przed serwerem weryfikującym i uzyskać dostęp do pewnych zasobów informacji. Wykorzystując nowoczesną technologię, dzięki analizie budowy ludzkiego ciała – zauważono, że pewne fizyczne cechy mogą posłużyć do jednoznacznej identyfikacji konkretnej osoby. Takie niepowtarzalne fizyczne cechy każdego z nas to cechy biometryczne. Bardzo trudne, bądź niemożliwe do podrobienia jak np. odcisk palca, wzór tęczówki oka, cechy twarzy, analiza głosu, rozkład temperatur twarzy – to jedne z tych cech, które można wykorzystać do weryfikacji użytkownika. Metoda taka pozwala jednoznacznie rozpoznać, a do tego nie wymaga pamiętania haseł czy też noszenia ze sobą żadnych dodatkowych urządzeń.

| Cecha biometryczna | Opis |
|--------------------|---|
| Linie papilarne | Znajdujące się na opuszkach palców małe bruzdy, których przypadkowy układ jest wynikiem marszczenia się skóry w czasie rozwoju płodu. Bruzdy te, a właściwie zbiór ich charakterystycznych punktów – mogą mieć zastosowanie do identyfikacji człowieka. Do odczytania punktów służą czytniki linii papilarnych, które skanują palec po przyłożeniu do powierzchni czujnika. System biometryczny ma za |

| | |
|-------------------------|--|
| | <p>zadanie porównać rozpoznane przez czytnik linie osoby próbującej uzyskać dostęp z bazą danych znanych już linii papilarnych. W przypadku pozytywnej weryfikacji osoby system ma za zadanie podjąć odpowiednią akcję.</p> |
| Tęczówka oka | <p>Tęczówka oka uznawana jest obecnie za element ciała ludzkiego, który jednoznacznie identyfikuje daną osobę. Raz ukształtowana (około 15 tygodnia życia płodu) nie zmienia się do końca życia. Wzór tęczówki oka jest na tyle odmienny u każdego człowieka, że można dzięki niemu rozróżnić bliźniaki jednojajowe.</p> <p>System biometryczny działa na zasadzie porównania wzoru tęczówki oka osoby badanej z wzorami innych, znanych już tęczówek (informacje przechowywane są w bazie danych). Obrazy tęczówki oka wykonywane są w postaci zdjęcia w wysokiej rozdzielcości, gdzie naznaczane są punkty charakterystyczne.</p> |
| Geometria twarzy | <p>Twarz człowieka posiada wiele charakterystycznych cech, które mogą zostać wykorzystane w procesie identyfikacji osoby. Układ oczu, wielkość nosa, kształt kości policzkowych, kształt czaszki, wielkość oczu – to jedne z cech, dzięki którym możliwym jest zapisanie matematycznego wzoru opisującego człowieka. Wzór taki tworzony jest na podstawie zdjęcia z kamery lub aparatu fotograficznego osoby badanej – gdzie pomiar kolejnych cech biometrycznych zamieniany jest na odpowiednie współczynniki wzoru, tworząc w sumie bardzo skomplikowany ciąg. Istotnym jest, aby podczas badania dobierać cechy biometryczne, których odczyt nie będzie zakłócony z zmienionych warunkach ponownego badania (np. inne uczesanie czy kolor włosów)</p> |
| Geometria dloni | <p>Dokonując trójwymiarowego zdjęcia ludzkiej dłoni, wskazać można ogólną ilość indywidualnych cech (ponad 90 różnych). Rejestrowane są między innymi : grubość, długość</p> |

| | |
|----------------------------------|--|
| | palców, obszar jaki tworzy powierzchnia między kostkami. Wynik pomiarów cech dloni zapisywany jest w formie 9 bajtowego wzorca (czyli ponad 1024 kombinacje). Nowoczesne systemy biometryczne uwzględniające geometrię dloni pozwalają uwzględnić czynnik starzenia się skóry i kości z biegiem czasu, dzięki czemu ich skuteczność pozostaje tak samo wysoka. |
| Rozkład temperatur twarzy | Twarz każdego człowieka ma odmienny układ temperatur, który można zarejestrować dzięki kamerze termowizyjnej widzącej w dalekiej podczerwieni. Możliwa jest zatem identyfikować osoby bez jej wiedzy (nawet w całkowitej ciemności). Czynnikiem zmniejszającym dokładność tej metody jest temperatura zewnętrzna, która wpływa znaczaco na odczyt, podobnie jak np. okulary. |

Tabela 13 Opracowanie własne: Cechy biometryczne człowieka [1i]

Biometryczne cechy człowieka to jedna z najlepszych metod jakie mogą służyć do weryfikacji użytkowników, jednak jest to stosunkowo nowy i nadal bardzo drogi sposób. Najtańszymi sensorami cech biometrycznych są obecnie skanery linii papilarnych, często chroniące ważne pomieszczenia firmy, jednak na ich stosowanie do weryfikacji uprawnień na szeroką skalę dla wszystkich użytkowników mogą sobie pozwolić tylko nieliczne firmy.

Sytuacja jednak zmienia się - już dziś można zakupić droższe komputery przenośne wyposażone w czytniki linii papilarnych, jednak dokładność tych sensorów często pozostawia wiele do życzenia, dlatego zaleca się weryfikację dwu fazową (odcisk palca i dodatkowo np. kod pin).

5.4 Klucz współdzielony

Klucz współdzielony – podobnie jak przy metodzie nazwa użytkownika/hasło - klucz współdzielony (ang. *Pre-Shared Key lub Shared Key*) jest ciągiem znaków, którego spodziewają się urządzenia VPN lub inne usługi pełniące podobną rolę zanim pozwolą na jakiekolwiek inne metody uwierzytelnienia (np. login/hasło), zatem podczas

tworzenia połączenia VPN IPsec, koncentrator VPN nie zezwoli na uruchomienie procesu uwierzytelnienia użytkownika zanim nie zostanie podany prawidłowy klucz współdzielony. Połączenia bez prawidłowego klucza *pre-shared key* będą odrzucane, mimo iż użytkownik może znać poprawne dane uwierzytelniające: nazwa użytkownika i hasło. Klucz współdzielony znać powinny wszyscy użytkownicy korzystający z usługi zdalnego dostępu realizowanego poprzez IPsec, co nie jest konieczne korzystając z dostępu VPN SSL.

Klucz współdzielony jest czasem także używany do tworzenia domowych sieci bezprzewodowych oznaczanych jako WPA-PSK lub WPA2-PSK.

5.5 Certyfikaty cyfrowe i PKI

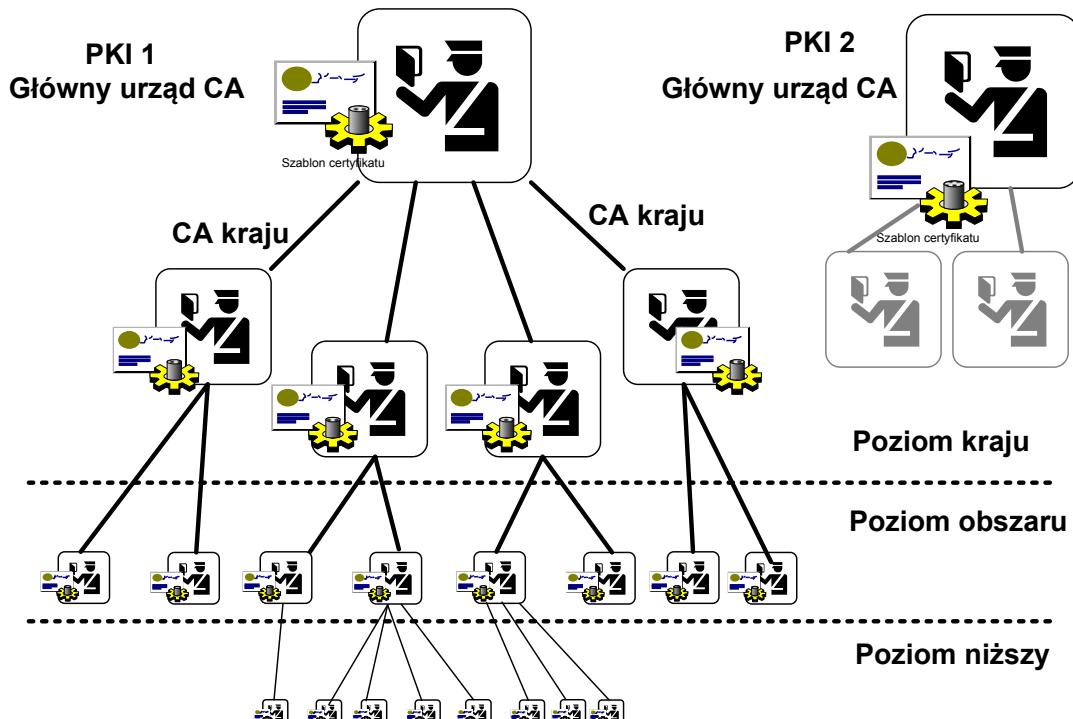
Cyfrowe certyfikaty (ang. *Digital Certificates*) – Certyfikat cyfrowy jest zaświadczeniem wydawany przez Urząd Certyfikacji (ang. *Certification Authority*), który w momencie wydania dokumentu potwierdza podpisem cyfrowym związek pomiędzy użytkownikiem a kluczem, którego używa. Poświadczenie takie wydawane jest na określony czas, np. 1 rok, po czym traci ważność i należy go odnowić.

Certyfikat cyfrowy jest ciągiem danych zapisanych na odpowiednim nośniku - np. specjalny token USB, czy karcie magnetycznej bądź mikroprocesorowej. Najpopularniejszym standardem certyfikatów cyfrowych jest X.509. Certyfikat taki zawiera następujące pola:

- wydawca certyfikatu,
- wersja,
- numer seryjny,
- ważność,
- podmiot dla którego certyfikat został wystawiony,
- klucz publiczny,
- podpis cyfrowy organu wydającego.

Weryfikację podpisu wystawcy można sprawdzić tylko wtedy, gdy jest znany klucz publiczny CA urzędu certyfikacyjnego wystawiającego, zatem weryfikacja to prześledzenie łańcucha zaufania, zakończonego przez główny urząd pełniący rolę CA

będący instytucją zaufania publicznego, która sama dla siebie wystawia certyfikat. Kryptografia klucza publicznego wymaga dobrze funkcjonującej infrastruktury, zwanej Infrastrukturą Klucza Publicznego (PKI). Infrastruktura PKI ta służy do zarządzania cyfrowymi certyfikatami i kluczami szyfrującymi dla osób, urządzeń i systemów informatycznych. Najważniejszych standardy w dziedzinie bezpieczeństwa teleinformatycznego (SSL/TLS, S/MIME, IPSEC) są tak zaprojektowane tak, aby umożliwić współpracę z PKI.



Rysunek 47 Przykładowa hierarchia PKI

Struktura PKI składa się z trzech elementów:

- Urzędów rejestracji – weryfikujący dane użytkownika i rejestrujący go,
- Urzędów certyfikacji – wydaje certyfikat z określoną datą,
- Repozytoriów kluczy, certyfikatów i list nieważnych certyfikatów (CRL) – umożliwienie dostępu do certyfikatów (np. poprzez protokół LDAP) oraz publikacja nieważnych, skompromitowanych certyfikatów, poprzez umieszczenie ich numerów seryjnych na listach CRL.

Funkcje jakie pełni PKI:

| Najważniejsze funkcje PKI | Przeznaczenie |
|---|---|
| Certyfikacja (ang. <i>Key Certification</i>) | Po pozytywnej weryfikacji danych użytkownika, urząd CA wystawia i dostarcza mu certyfikat wraz z kluczem publicznym oraz umieszcza go w publicznym repozytorium kluczy |
| Rejestracja (ang. <i>Key Registration</i>) | Użytkownik końcowy składa do organu rejestracyjnego wniosek o wydanie certyfikatu podając szczegółowe dane wraz z własnoręcznym podpisem- jeśli jest to osoba fizyczna. Jeśli podmiot ubiegający się o certyfikat jest firmą należy podać nazwę własną, nazwę domenową, adres IP. Dane następnie są weryfikowane ze stanem faktycznym przez Organ Rejestracyjny |
| Generowanie kluczy (ang. <i>Key Generation</i>) | Urząd certyfikacyjny generuje parę kluczy : prywatny i publiczny a następnie w sposób poufnny dostarcza je użytkownikowi. Możliwe jest także dostarczenie własnego klucza publicznego do urzędu CA celem podpisania (nie ujawniając klucza prywatnego) |
| Odnawianie kluczy (ang. <i>Key Update</i>) | Odnawianie kluczy może być spowodowane upłynięciem ważności certyfikatu lub jego kompromitacją, czyli ujawnieniem osobom trzecim klucza prywatnego. W przypadku kompromitacji numer seryjny certyfikatu umieszczany jest na liście CRL celem unieważnienia, a następnie rozpoczyna się procedura wystawienia nowego certyfikatu. |

| | |
|---|---|
| Certyfikacja wzajemna (ang. <i>Cross-Certification</i>) | Główne urzędy certyfikujące (ROOT CA) wystawiają sobie wzajemnie certyfikaty, po to by użytkownicy jednej struktury PKI mogli ufać certyfikatom innej struktury PKI. Certyfikacja wzajemna nie zawsze jest dwukierunkowa. |
| Odwołanie certyfikatu (ang. <i>Key Revocation</i>) | Umieszczenie numeru seryjnego certyfikatu na liście CRL, celem jego unieważnienia np. z powodu kompromitacji klucza prywatnego |
| Odzyskanie klucza (ang. <i>Key Recovery</i>) | Dodatkowe zabezpieczenie na wypadek, gdy użytkownik utraci swoje klucze do szyfrowania lub negocjacji |

Tabela 14 Opracowanie własne: Najważniejsze PKI

6 Model AAA

Uwierzytelnianie, autoryzacja, zliczanie ruchu – to przetłumaczony na język polski, skrót tzw. modelu AAA (ang. *Authentication, Authorization and Accounting*). Zdefiniowanie w/w zestawu pozwala administratorowi w prosty i szybki sposób ustawić parametry bezpieczeństwa grup lub pojedynczych użytkowników. Parametry te mają wpływ na możliwość weryfikacji użytkownika, regulację dostępu do chronionych obszarów oraz opcję śledzenia i zliczania ruchu (zapisy te w prosty sposób pokazują, który użytkownik oraz przez jaki czas korzystał z danych zasobów sieci).

Aby dokładnie zdefiniować funkcje i zasadę działania modelu koniecznym jest rozwinięcie i omówienie kolejnych składowych modelu AAA. [1][6][7][1i]

Authentication – czyli uwierzytelnianie - odpowiada w prosty sposób na pytanie „Kim jesteś?”. Weryfikuje czy użytkownik jest za kogo się podaje. Właściwa kombinacja nazwy użytkownika oraz hasła skojarzonego z loginem – gwarantuje poprawne uwierzytelnienie.

Authorization – czyli autoryzacja – odpowiada na pytanie „Czy użytkownik ma prawo do ... ?”. Użytkownik może być uprawniony (lub też nie) – do dostępu do określonych hostów sieciowych, usług, czy też aktywnych urządzeń sieciowych. Dodatkowo autoryzacja pozwala przyznać odpowiedni adres IP, podczas połączenia VPN, czy też dać odpowiedni poziom uprawnień do zasobów.

Accounting – czyli zliczanie – odpowiada na pytanie „Co użytkownik robił na sieci?”. Zalogowana informacja może zawierać np. czas połączenia VPN, ile razy dany użytkownik odwiedzał danego zasobu, ilu użytkowników aktualnie używa danej usługi sieciowej.

Istotnym jest by pamiętać, że proces uwierzytelniania jest konieczny, dopiero po jego pozytywnym zakończeniu – możliwa będzie autoryzacja i zliczanie ruchu. Nie ma wymogu używania autoryzacji czy też zliczania.

6.1 Protokoły RADIUS i TACACS+

Zarówno protokół TACACS+ jak i RADIUS – pełnią podobną funkcję, zapewniając usługi AAA dla zastosowań sieciowych. Jest jednak wiele różnic między nimi.

Protokół RADIUS wynaleziony przez firmę Livingston Enterprises, opisany w dokumencie RFC 2865, był i jest wspierany przez większość urządzeń sieciowych i można śmiało powiedzieć, że jest protokołem uniwersalnym często wybieranym ze względu na mniejsze zapotrzebowanie na moc procesora oraz pamięci operacyjnej serwera, na którym rezyduje.

Komunikacja między urządzeniem sieciowym pełniącym rolę NAS (ang. *Network Access Server*) a serwerem RADIUS odbywa się za pomocą bezpołączeniowego protokołu UDP. Klientem RADIUS jest zwykle urządzenie NAS (np. router, switch etc.) zaś serwerem RADIUS jest proces uruchomiony na systemie operacyjnym UNIX/LINUX bądź Windows z rodziny NT. Klient (urządzenie) przekazuje informacje o użytkowniku do serwera RADIUS i oczekuje na odpowiedź. Serwer RADIUS otrzymuje zapytanie, uwierzytelnia (bądź nie) użytkownika, a następnie zwraca parametry konfiguracji potrzebne klientowi do zapewnienia odpowiednich usług dla

końcowego użytkownika. Serwer RADIUS może pełnić rolę klienta *proxy* (pośrednika) w stosunku do kolejnego serwera RADIUS bądź też innych serwerów uwierzytelniających. Podczas przesyłania danych uwierzytelniających za pomocą protokołu RADIUS – tylko hasło zostaje zaszyfrowane, zaś pole nazwy użytkownika, i usługi *Authorization i Accounting* przesyłane są czystym tekstem, zatem mogą zostać podsłuchane. Mimo to protokół ten uważa się za bezpieczny i częściej niż TACACS+ stosowany, gdyż często w sieciach stosuje się sprzęt wyprodukowany przez różne firmy – a tylko protokół RADIUS zachowuje pełną kompatybilność i wsparcie, TACACS+ – pełne wsparcie tylko dla sprzętu marki Cisco Systems.[1][6][7][1i][3d][5d]

Firma Cisco Systems wynalazła protokół TACACS+ (opisany w dokumencie RFC 1492) ponieważ zaistniała potrzeba wsparcia dla wciąż rosnącej liczby coraz to większych sieci. Architektura protokołu TACACS+ zapewnia w łatwiejszy sposób na rozdzielenie funkcjonalności modelu AAA, np. możliwym jest użycie uwierzytelniania KERBEROS, zaś TACACS+ do autoryzacji i zliczania ruchu (kiedy urządzenie NAS przejdzie pomyślną próbę uwierzytelniania serwera KERBEROS, przystąpi do autoryzacji za pomocą serwera TACACS+). Podczas sesji, jeśli zajdzie potrzeba dodatkowej autoryzacji, serwer żądający dodatkowego potwierdzenia sprawdza wraz z serwerem TACACS+ czy użytkownik ma prawo dostępu np. do wykonania danego polecenia i uprawnienia takie przyznaje lub nie. Dzięki temu możliwa jest lepsza kontrola nad procesami modelu AAA.

Komunikacja między urządzeniem NAS a serwerem TACACS+ przebiega za pośrednictwem połączniowego protokołu TCP. Podczas przesyłania żądania od urządzenia NAS do serwera TACACS+ – cała zawartość pakietu zostaje zaszyfrowana – zatem jest on odporny na prostą metodę podsłuchania sesji TCP.

[1][6][7][1i][3d][5d]

Tabela 15 Opracowanie własne: Porównanie protokołów RADIUS i TACACS+

| RADIUS | TACACS+ |
|--|---|
| Używa protokołu UDP | Używa protokołu TCP |
| Szyfruje tylko hasło w żądaniach uwierzytelnienia | Szyfrowana jest cała zawartość pakietu zawierającego dane uwierzytelniające |
| Połączenie autentykacji i autoryzacji w jednym kroku | Wszystkie kroki modelu AAA są oddzielone |

| | |
|---|---|
| Ogólnodostępny standard | Własność Cisco Systems. |
| Protokół RADIUS nie pozwala na kontrolę jakich poleceń może używać zalogowany na routerze użytkownik. | Protokół TACACS+ zapewnia dwie metody kontroli autoryzacji komend routera : -na podstawie użytkownika -na podstawie przynależności do grupy |

7 Projekt zdalnego dostępu w firmie

7.1 Założenia projektowe

Zarząd firmy mającej 6 oddziałów na całym świecie (w tym dwie lokalizacje centralne) zdecydował się na wdrożenie usługi zdalnego dostępu dla swoich pracowników. Wśród wymagań jakie zostały postanowione administratorom projektującym i implementującym znalazły się następujące punkty:

- ❖ Zapewnić możliwie bezpieczny dostęp do zasobów firmowej sieci lokalnej dla pracowników zdalnych (telepracowników), używającym do tego celu komputera oraz dowolnego łącza do sieci Internet. Pracownik w zależności od poziomu uprawnień powinien mieć ograniczony lub całkowicie otwarty dostęp do wszystkich usług, które mógłby osiągnąć będąc w oddziale firmy.
 - Dostęp ograniczony przeznaczony dla większości pracowników - pozwalać ma na połączenie z wewnętrznymi serwerami poczty, stronami intranetowymi (HTTP/HTTPS), dostęp do wewnętrznego komunikatora sieciowego, dostęp doewnętrznych aplikacji oraz do serwera świadczącego usługi telefonii IP. Dodatkowo w celach diagnostycznych zezwolono jest także ruch ICMP.
 - Dostęp pełny - zezwala na odblokowanie całego ruchu IP od klienta, poprzez koncentrator VPN do głównej ściany ogniowej. Dostęp taki ma zezwalać na bezproblemową pracę administratorów IT np. poprzez klienta SSH czy zdalny pulpit.

- ❖ Aby zapewnić wysoki poziom dostępności usługi zdalnego dostępu dla użytkowników - należy zapewnić dwa niezależne punkty umożliwiające nawiązanie połączenia VPN
 - Punktem głównym gdzie umieszczony jest koncentrator VPN jest lokalizacja centralna Szwecja
 - Punktem zapasowym jest lokalizacja centralna Niemcy
- ❖ Możliwość dostępu zdalnego dla telepracowników za pomocą technologii:
 - ✓ IPsec (Za pomocą klienta Cisco VPN instalowanego na stacji roboczej),
 - ✓ SSL VPN (Automatyczna instalacja po otwarciu strony internetowej),
 - ✓ L2TP/IPsec (za pomocą wbudowanego klienta vpn w systemy Windows XP/2000/Vista).
- ❖ Zapewnić możliwość uwierzytelniania użytkowników za pomocą metod:
 - ✓ Login/hasło z domeny Active Directory,
 - ✓ Z użyciem jednorazowych haseł (OTP) – generowanych przez sprzętowe Tokeny RSA (dla użytkowników spoza domeny Active Directory).
- ❖ Integracja z Active Directory, aby możliwym było przyznanie stosownych uprawnień już na poziomie warstwy IP na podstawie przynależności do grup domenowych
- ❖ Możliwość automatycznej weryfikacji stacji roboczych pracowników używających metody dostępu SSL VPN pod kątem:
 - ✓ Ostatnich aktualizacji systemu operacyjnego,
 - ✓ Obecności oprogramowania antywirusowego,
 - ✓ Członkostwa w domenie Active Directory,
 - ✓ Obecności programowej zapory sieciowej.
- ❖ Zapewnienie możliwe bezpiecznego połączenia dla klientów używających komputerów w potencjalnie niebezpiecznych środowiskach np. w kafejkach internetowych - poprzez automatyczne instalowanie aplikacji Cisco Secure Desktop (rezerwującej pewne wirtualne zasoby komputera, które nie mają bezpośredniego kontaktu z już używanymi przez zalogowanego użytkownika, tworząc programową izolację klienta na czas połączenia VPN)
- ❖ Możliwość integracji z dowolnymi serwerami uwierzytelniającymi np. RADIUS, TACACS+, SDI

- ❖ Zapewnić integrację nowych urządzeń pełniących rolę bram VPN z istniejącą strukturą sieci LAN i WAN przedsiębiorstwa.

7.2 Opis projektu

Opis projektu w pierwszej jego części dotyczy sposobu połączenia poszczególnych urządzeń tworzących sieć rozległą oraz poszczególne sieci LAN przedsiębiorstwa ze sobą. Następnie przedstawiono sposób implementacji urządzeń świadczących usługi zdalnego dostępu (koncentratory VPN) oraz serwerów uwierzytelniających użytkowników w strukturze sieci (RADIUS, SDI).

Druga część projektu poświęcona została konfiguracji programowej urządzeń i serwerów pod kątem realizacji założeń projektowych.

Ostatnim etapem realizacji projektu było przeprowadzenie testów akceptacyjnych oraz wydajnościowych zaproponowanego rozwiązania.

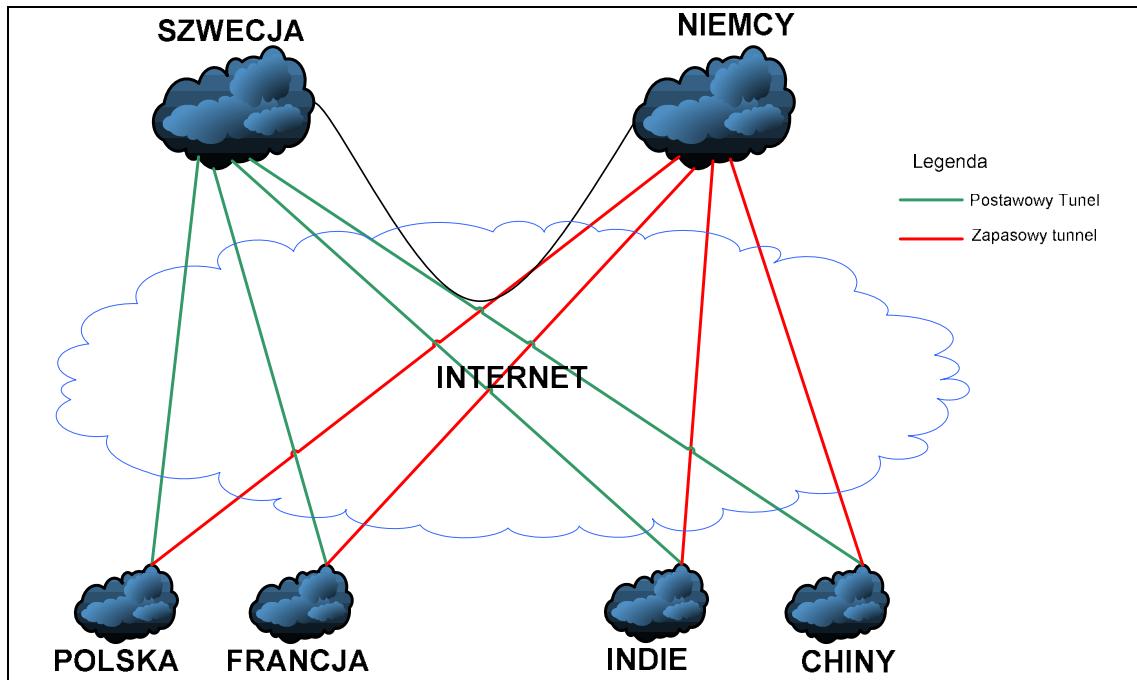
7.2.1 Aktualny stan sieci WAN

Firma posiada 6 oddziałów na świecie. Każda z lokalizacji posiada wykupione własne łącze gwarantujące dostęp do Internetu (tabela 16: zestawienie parametrów łącz Internetowych), za pośrednictwem którego realizowane są połączenia VPN do centralnych biur w Szwecji i Niemczech. Jako punkty styku (HUB Routery) a zarazem zakończenia tuneli połączeń VPN typu *Site-to-Site* wybrano lokalizacje centralne, ze względu na to, iż posiadają najszybszy dostęp do sieci Internet oraz obecność łącz zapasowych.

| Oddział | Prędkość dostępu do Internetu | Łącze zapasowe |
|---------|--|----------------|
| Szwecja | 100Mbit/s (symetryczny upload/download) | TAK |
| Niemcy | 50Mbit/s (symetryczny upload/download) | TAK |
| Polska | 30Mbit/s (symetryczny upload/download) | NIE |
| Francja | 20Mbit/s (symetryczny upload/download) | NIE |
| Indie | 10Mbit/s (symetryczny upload/download) | NIE |
| Chiny | 8Mbit/s (symetryczny upload/download) | NIE |

Tabela 16 Opracowanie własne: Zestawienie parametrów łącz do sieci rozległych

Ideowy schemat połączeń VPN realizowanych poprzez sieć Internet – zobrazowany jest na Rysunku nr 48



Rysunek 48 Logiczny schemat połączeń VPN

W lokalizacjach: Polska, Francja, Indie, Chiny użyty został następujący sprzęt do budowy sieci WAN:

| Typ | Model |
|-----------|--|
| Router: | 2 x Cisco 1812 |
| Switche: | Cisco Catalyst 2960G |
| Firewall: | Nokia IP 350, system operacyjny IPSO 4.2 + CheckPoint NGX R65 |

Tabela 17 Opracowanie własne: Sprzęt użyty do budowy sieci WAN

W lokalizacjach centralnych: Szwecja, Niemcy pełniących rolę HUB routerów – został wykorzystany następujący sprzęt do budowy sieci WAN:

| Typ | Model |
|---------|----------------|
| Router: | 2 x Cisco 2821 |

| | |
|-----------|--|
| Switches: | Cisco Catalyst 2960G |
| Firewall: | Nokia IP 350, system operacyjny IPSO 4.2 + CheckPoint NGX R65 |

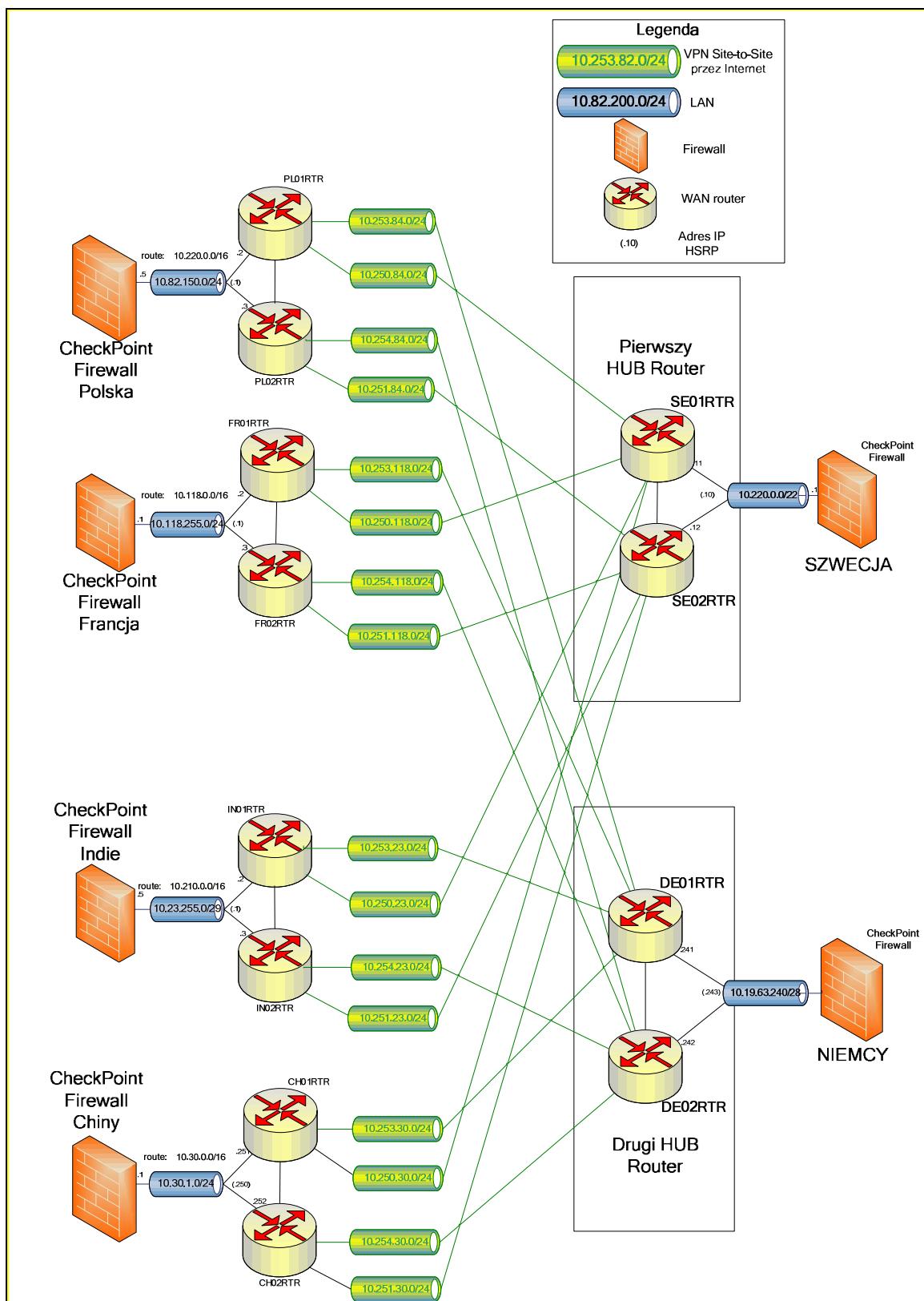
Tabela 18 Opracowanie własne: Sprzęt użyty do budowy sieci WAN w centralach firmy

Aby zapewnić możliwe wysoki poziom dostępności i niezawodności usług sieciowych dla użytkowników – zdecydowano się na użycie w każdej z lokalizacji dwóch routerów pracujących pod kontrolą protokołu HSRP (ang. *Hot Standby Router Protocol*) zapewniającego nieprzerwaną dostępność do odległych sieci LAN nawet w przypadku uszkodzenia jednego z routerów.

Za wymianę ruchu między lokalizacjami odpowiedzialny jest protokół routingu dynamicznego EIGRP, który w przypadku awarii ścieżki podstawowej wybierze ścieżkę zapasową, tak by finalnie osiągnąć cel.

Połączenia typu *Site-to-Site* VPN realizowane między lokalizacjami centralnymi (Szwecja i Niemcy) a pobocznymi (Polska, Francja, Indie, Chiny) zabezpieczone są za pomocą protokołu IPsec gwarantującego integralność, autentyczność, niezaprzeczalność i poufność przesyłanych danych (przy zastanej konfiguracji). Dodatkowe mechanizmy list kontroli dostępu (ang. *ACL – Access Control List*) oraz ograniczoną tablicę routingu tylko do znanych adresów IP – tworzą bezpieczną strukturę VPN między odległymi oddziałami .

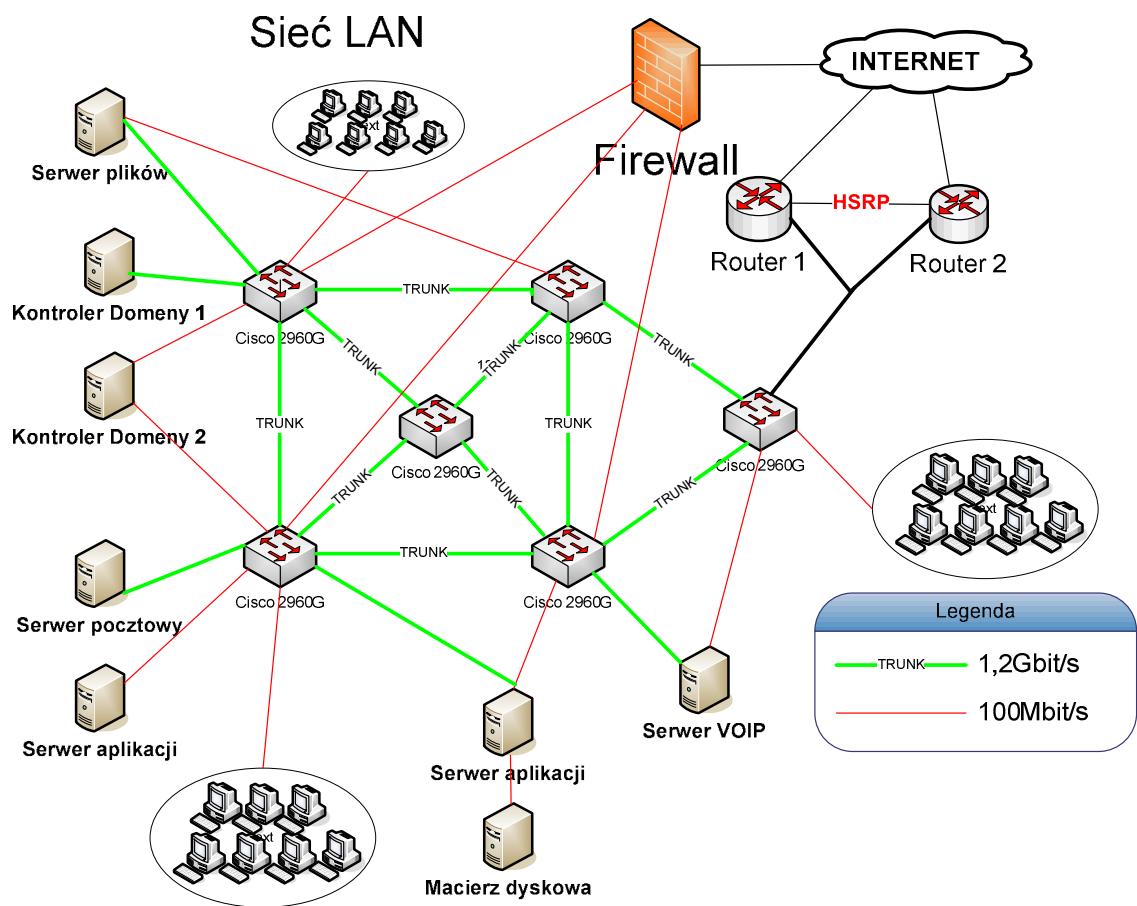
Schemat połączeń logicznych między lokalizacjami centralnymi a pobocznymi znajduje się na rys 49.



Rysunek 49 Opracowanie własne: Schemat połączeń między oddziałami

7.2.2 Aktualny stan sieci LAN

W Sieci lokalnej w każdej z lokalizacji pobocznych pracuje nie mniej niż 100 użytkowników, zaś w centralnych po około 200 osób. Infrastruktura sieci LAN zbudowana jest w całości w oparciu o sprzęt firmy Cisco Systems. Zastosowane przełączniki Cisco model 2960G-48 zapewniają szybkość transmisji do komputerów użytkowników na poziomie 100Mbit/s, zaś w sieci szkieletowej łączącej poszczególne przełączniki oraz główne serwery ze sobą - na poziomie 1 lub 2 Gbit/s (w zależności od ilości połączeń nadmiarowych).



Rysunek 50 Opracowanie własne: Schemat sieci LAN

W sieci lokalnej dla użytkowników udostępnione są następujące serwery usług:

- ✓ Serwery plików
- ✓ Serwery pocztowe (Microsoft Exchange)
- ✓ Kontrolery domeny (*Active Directory*)
- ✓ Serwery Aplikacji
- ✓ Serwery WWW-Proxy

- ✓ Serwer świadczący usługi telefonii IP (*VOIP*)
- ✓ Serwery baz danych

7.2.3 Wdrożenie koncentratora VPN

Do realizacji projektu zdalnego dostępu VPN dla pracowników firmy - wymagany był zakup stosownych urządzeń. Dwa wydajne urządzenia firmy Cisco Systems (model ASA5520) pełniące rolę ściany ogniowej (ang. *Firewall*) i jednocześnie koncentratora VPN umieszczone zostały w centralach firmy w lokalizacjach centralnych: Szwecji i Niemczech. Adaptacyjne urządzenia zabezpieczające w skrócie ASA (ang. *Adaptive Security Appliances*) serii 5520 pozwalają w sposób bezpieczny zrealizować podstawowe założenia projektowe, mówiące o dostępie zdalnym z użyciem technologii IPsec, SSL VPN, oraz L2TP/IPsec, a także w łatwy sposób zintegrować je z serwerami uwierzytelniającymi. Dodatkowe opcje jakimi są ochrona w warstwie aplikacji, filtry antyspamowe, odwiedzanych adresów URL oraz możliwość wdrożenia specjalnej polityki sprawdzenia komputera użytkownika jeszcze przed podłączeniem – są dodatkowymi zaletami przemawiającymi za wyborem właśnie tego modelu. Specyfikacja techniczna modelu Cisco ASA5520 przedstawia się następująco:

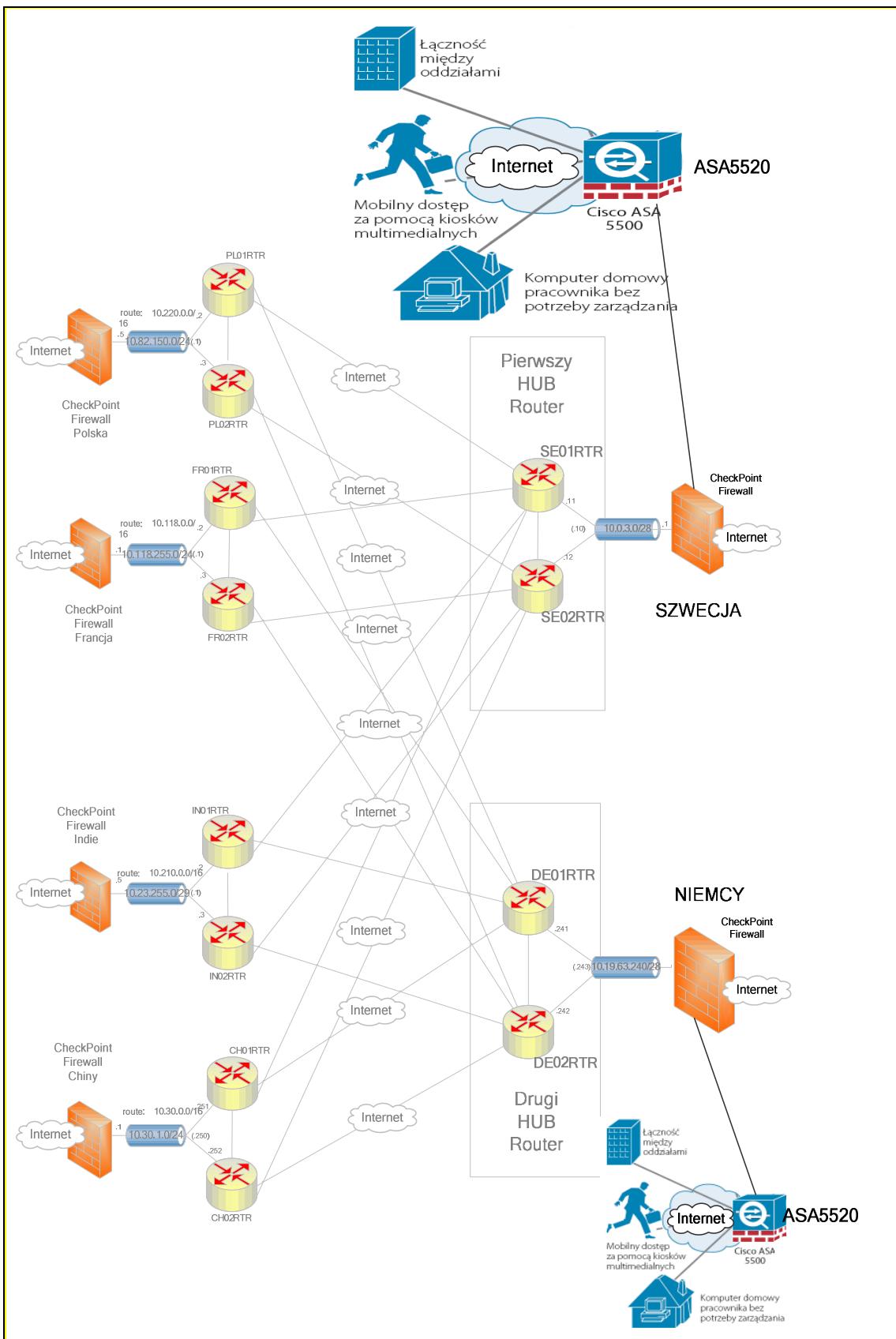
| Model/licencja z serii Cisco ASA 5500 | Cisco ASA 5520 |
|---|--|
| Rynek | korporacje |
| Podsumowanie możliwości | |
| Maksymalna przepustowość zapory (Mb/s) | 450 |
| Maksymalna przepustowość 3DES/AES sieci VPN (Mb/s) | 225 |
| Maksymalna liczba sesji między biurami i zdalnego dostępu VPN | 750 |
| Maksymalna liczba sesji SSL sieci VPN ¹ | 750 |
| Maksymalna liczba połączeń | 280 000 |
| Maksymalna liczba połączeń na sekundę | 9000 |
| Pakiety na sekundę (64 bajty) | 320 000 |
| Podsumowanie techniczne | |
| Pamięć (MB) | 512 |
| Pamięć flash systemu (MB) | 64 |
| Wbudowane porty | 4-10/100/1000, 1-10/100 |
| Maksymalna liczba interfejsów wirtualnych (VLAN) | 150 |
| Gniazdo rozszerzeń SSC/SSM | Tak (SSM) |
| Możliwości SSC/SSM | |
| Obsługiwane urządzenia SSC/SSM | CSC-SSM, AIP-SSM, 4GE-SSM |
| Blokowanie dostępu intruzów | Tak (z AIP-SSM) |
| Współbieżna przepustowość zmniejszania zagrożenia (Mb/s) (zapora + usługi IPS) | 225 (z AIP-SSM-10) 375 (z AIP-SSM-20) |
| Usługi anti-X (ochrona przed wirusami, programami szpiegującymi, spamem i witrynami wyludzającymi informacje, blokowanie plików, filtrowanie adresów URL) | Tak (z CSC-SSM) |
| Maksymalna liczba użytkowników usług ochrony przed wirusami i programami szpiegującymi oraz blokowania plików (tylko CSC-SSM) | 500 (CSC-SSM-10) 1000 (CSC-SSM-20) |
| Funkcje licencji CSC SSM Plus | Ochrona przed spamem i witrynami wyludzającymi informacje, filtrowanie adresów URL |
| Funkcje | |
| Bezpieczeństwo warstwy aplikacji | Tak |
| Transparentna zapora w warstwie 2 | Tak |
| Konteksty zabezpieczeń (dodane/maksymalnie) ² | 2/20 |
| Badanie GTP/GPRS ² | Tak |
| Obsługa wysokiej dostępności ³ | A/A i A/S |
| Łączenie sieci VPN w klastry i równoważenie obciążenia | Tak |

Rysunek 51 Specyfikacja techniczna urządzenia ASA5520.

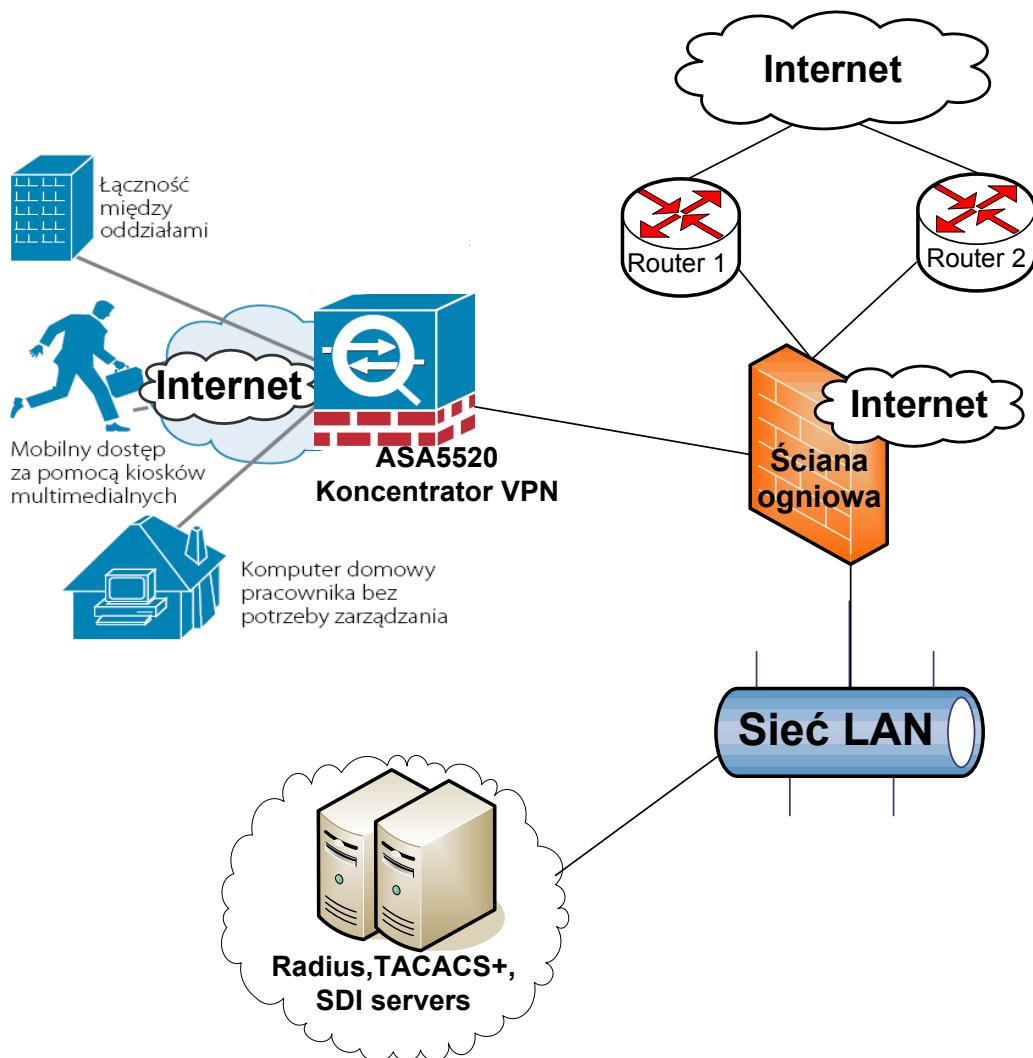
Źródło <http://www.awnet.pl/images/Cisco%20ASA%205500.pdf>

Koncentrator VPN – ASA5520 połączony został jednym interfejsem (GigabitEthernet0/0) do sieci Internet, zaś drugim (GigabitEthernet0/1) do karty sieciowej firewalla firmy Checkpoint, tworząc kaskadowe połączenie dwóch ścian ogniowych od strony użytkowników dostępu zdalnego VPN oraz dając dodatkową barierę dla potencjalnych włamywaczy.

Logiczne umiejscowienie koncentratorów VPN w sieci WAN obrazuje rys. 52



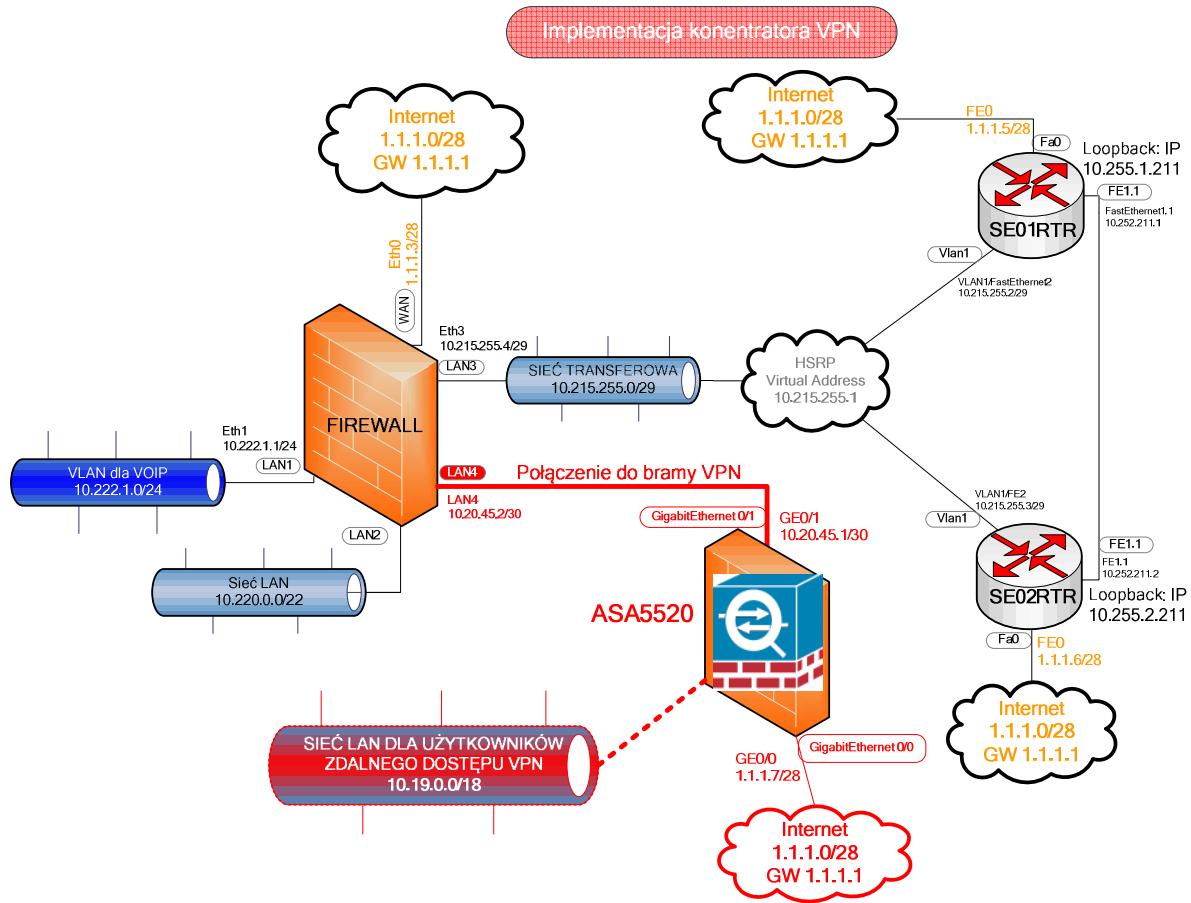
Rysunek 52 Opracowanie własne: Logiczne umiejscowienie koncentratorów VPN w sieci WAN



Rysunek 53 Opracowanie własne: Logiczne umiejscowienie koncentratora VPN w sieci WAN i LAN

7.2.4 Adresacja IP w sieci LAN/WAN

Aby zaadresować wszystkie wewnętrzne urządzenia oraz hosty sieciowe firmy – użyta została adresacja IPv4 z puli adresów prywatnych, klasy A (10.0.0.0/8). W lokalizacji centralnej (w Szwecji), gdzie umiejscowiony został podstawowy koncentrator VPN – schemat adresacji IP przedstawia się następująco:



Rysunek 54 Opracowanie własne: Adresacja IP w sieci LAN/WAN i VPN

Tabela 19 Opracowanie własne: Przeznaczenie poszczególnych podsieci IP

| Podsieci IP: | Zastosowanie: |
|-----------------|---|
| 10.220.0.0/22 | Sieć LAN dla hostów połączonych wewnętrz lokalizacji „Szwecja” |
| 10.19.0.0/18 | Sieć LAN dla użytkowników zdalnego dostępu VPN ze wszystkich 6 lokalizacji na świecie. Podzielona jest na mniejsze podsieci po 62 hosty każda. |
| 10.222.1.0/24 | Sieć LAN przeznaczona dla telefonów IP (telefonia VOIP) |
| 10.215.255.0/29 | Sieć transferowa łącząca interfejs fizyczny firewalla z routerami WAN oraz sieciami LAN z pozostałych lokalizacji. Adres IP |

| | |
|----------------------|--|
| | 10.215.255.1 jest adresem wirtualnym protokołu HSRP. |
| 10.20.45.0/30 | Sieć połączeniowa między urządzeniem ASA5520 a istniejącym firewallem firmy CheckPoint |

Jako publiczne adresy IP dostawca usług internetowych przydzielił pulę: 1.1.1.0/28. Przeznaczenie poszczególnych adresów IP jest następujące:

Tabela 20 Opracowanie własne: Opracowanie własne: Wykorzystanie publicznych adresów IP

| Publiczne adresy IP: | Zastosowanie: |
|----------------------|---|
| 1.1.1.1/28 | Adres IP bramy – dostawcy Internetu |
| 1.1.1.7/28 | Adres IP przydzielony interfejsowi GigabitEthernet0/0 koncentratora VPN. Łączy urządzenie z siecią Internet. |
| 1.1.1.3/28 | Adres IP interfejsu sieciowego łączącego firewall firmy CheckPoint z siecią Internet. |
| 1.1.1.5/28 | Adres IP interfejsu sieciowego FastEthernet0/0 pierwszego WAN routera. |
| 1.1.1.6/28 | Adres IP interfejsu sieciowego FastEthernet0/0 zapasowego WAN routera. |

7.2.5 Adresacja IP dla klientów zdalnego dostępu

Użytkownicy korzystający z usługi zdalnego dostępu w zależności od lokalizacji (kraju) oraz poziomu uprawnień w usłudze globalnego katalogu - Active Directory (ograniczony lub pełny dostęp) otrzymają adresy IP z określonych pul, dzięki czemu na

głównym firewallu, obecnym w każdej z lokalizacji możliwym jest ustalenie stosownych reguł dostępu dla użytkowników zasobów już na poziomie warstwy IP.

Oznaczenie nazwy puli adresów IP skonstruowane jest według następującego wzorca:

KRAJ_GRUPA_DOSTĘPU

Jako KRAJ możliwe pozycje:

- Poland (Polska),
- Sweden (Szewcja),
- India (Indie),
- Germany (Niemcy),
- France (Francja),
- China (Chiny),
- Vistorm (dla klientów korzystających z metody uwierzytelnienia poprzez TokenRSA).

Jako GRUPA_DOSTĘPU możliwe dwie pozycje:

- WEB_Access – Dostęp ograniczony przeznaczony dla większości pracowników - pozwalać ma na połączenie z wewnętrznymi serwerami poczty, stronami intranetowymi (HTTP/HTTPS), dostęp do wewnętrznego komunikatora sieciowego, dostęp do baz danych SQL,ewnętrznych aplikacji oraz do serwera świadczącego usługi telefonii IP. Dodatkowo w celach diagnostycznych zezwolono jest także ruch ICMP.
- FULL_Access – Dostęp zezwala na odblokowanie całego ruchu IP od klienta, poprzez koncentrator VPN do głównej ściany ogniowej. Dostęp taki ma zezwalać na bezproblemową pracę administratorów IT np. poprzez klienta SSH czy zdalny pulpit.

Zgodnie ze schematem nazw grup dostępu - w konfiguracji urządzenia użyto następujących nazw pul oraz powiązane z nimi zakresów adresów IP:

| Nazwa puli IP | Zakres adresów IP | Maska podsieci |
|-------------------|----------------------|-----------------|
| Sweden_WEB_Access | 10.19.0.2-10.19.0.62 | 255.255.255.192 |

| | | |
|---------------------|-------------------------|-----------------|
| Sweden_FULL_Access | 10.19.0.66-10.19.0.126 | 255.255.255.192 |
| Poland_WEB_Access | 10.19.0.130-10.19.0.190 | 255.255.255.192 |
| Poland_FULL_Access | 10.19.0.194-10.19.0.254 | 255.255.255.192 |
| India_WEB_Access | 10.19.1.2-10.19.1.62 | 255.255.255.192 |
| India_FULL_Access | 10.19.1.66-10.19.1.126 | 255.255.255.192 |
| Germany_WEB_Access | 10.19.1.130-10.19.1.190 | 255.255.255.192 |
| Germany_FULL_Access | 10.19.1.194-10.19.1.254 | 255.255.255.192 |
| France_WEB_Access | 10.19.2.2-10.19.2.62 | 255.255.255.192 |
| France_FULL_Access | 10.19.2.66-10.19.2.126 | 255.255.255.192 |
| VISTORM_RSA | 10.19.2.130-10.19.2.190 | 255.255.255.192 |
| China_WEB_Access | 10.19.2.194-10.19.2.222 | 255.255.255.192 |
| China_FULL_Access | 10.19.2.226-10.19.2.253 | 255.255.255.192 |

7.2.6 Konfiguracja koncentratora VPN

Za pomocą kabla konsolowego typu rollover łączącego port konsolowy koncentratora (oznaczony jako CONSOLE) oraz port szeregowy komputera - możliwym jest nawiązanie połączenia terminalowego celem wstępnej konfiguracji urządzenia. Możliwa jest także konfiguracja poprzez protokół SSH lub też za pomocą aplikacji ASDM (ang. *Cisco Adaptive Security Device Manager*) używając protokołu HTTP. Aplikacja ASDM pozwala odczytywać i zmieniać parametry urządzenia szybciej, gdyż odbywa się to w trybie graficznym, jednak nie pozwala na pełną kontrolę nad wynikowymi ustawieniami i plikami konfiguracyjnymi urządzenia.

Konfiguracja interfejsów sieciowych z poziomu linii poleceń

```
interface GigabitEthernet0/0
  nameif Outside
  security-level 0
  ip address 1.1.1.7 255.255.255.240
```

Listing 1 Opracowanie własne: konfiguracja interfejsów sieciowych z poziomu konsoli

- interface GigabitEthernet0/0 – wejście w tryb konfiguracji interfejsu o nazwie „GigabitEthernet” o indeksie 0/0.
- nameif Outside – oznacza interfejs jako łączący z siecią zewnętrzną.
- security-level 0 – poziom bezpieczeństwa może przyjmować wartości od 0 do 100 (gdzie 0 dla niezaufanych, a 100 dla zaufanych sieci)
- ip address 1.1.1.7 255.255.255.240 – ustawia adres ip i maskę interfejsu od strony sieci Internet

```
interface GigabitEthernet0/1
nameif Inside
security-level 100
ip address 10.20.45.1 255.255.255.252
```

Listing 2 Opracowanie własne: konfiguracja interfejsów sieciowych z poziomu konsoli

- interface GigabitEthernet0/1 – wejście w tryb konfiguracji interfejsu o nazwie „GigabitEthernet” o indeksie 0/1,
- nameif Inside – oznacza interfejs jako łączący z siecią zewnętrzną,
- security-level 100 – poziom bezpieczeństwa 100 od strony zaufanych sieci,
- ip address 10.20.45.1 255.255.255.252 ustawia adres ip i maskę interfejsu od strony sieci łączącej koncentrator VPN z główną ścianą ognową. Jest to adres połączeniowy.

Konfiguracja tablicy tras (routingu):

```
route Outside 0.0.0.0 0.0.0.0 1.1.1.1 1
route Inside 10.0.0.0 255.0.0.0 10.20.45.2 1
route Inside 0.0.0.0 0.0.0.0 10.20.45.2 tunneled
```

Listing 3 Opracowanie własne: konfiguracja tablicy routingu z poziomu konsoli

- route Outside 0.0.0.0 0.0.0.0 1.1.1.1 1 – polecenie definiuje domyślną bramę sieciową osiąganą poprzez interfejs oznaczony wcześniej jako Outside poprzez adres IP 1.1.1.1 (brama dostawcy sieci Internet),

- route Inside 10.0.0.0 255.0.0.0 10.20.45.2 1 - wskazuje, że cała sieć 10.0.0.0/8 osiągalna jest przez firewall (Checkpoint) przez adres IP 10.20.45.2 z metryką równą 1,
- route Inside 0.0.0.0 0.0.0.0 10.20.45.2 tunneled – wskazuje domyślną bramę dla połączeń tunelowych. Brama to adres IP 10.20.45.2 (firewall CheckPoint).

Konfiguracja zakresów adresów IP dla klientów zdalnego dostępu:

```
ip local pool Sweden_WEB_Access 10.19.0.2-10.19.0.62 mask
255.255.255.192
ip local pool Sweden_FULL_Access 10.19.0.66-10.19.0.126 mask
255.255.255.192
ip local pool Poland_WEB_Access 10.19.0.130-10.19.0.190 mask
255.255.255.192
ip local pool Poland_FULL_Access 10.19.0.194-10.19.0.254 mask
255.255.255.192
ip local pool India_WEB_Access 10.19.1.2-10.19.1.62 mask
255.255.255.192
ip local pool India_FULL_Access 10.19.1.66-10.19.1.126 mask
255.255.255.192
ip local pool Germany_WEB_Access 10.19.1.130-10.19.1.190 mask
255.255.255.192
ip local pool Germany_FULL_Access 10.19.1.194-10.19.1.254 mask
255.255.255.192
ip local pool France_WEB_Access 10.19.2.2-10.19.2.62 mask
255.255.255.192
ip local pool France_FULL_Access 10.19.2.66-10.19.2.126 mask
255.255.255.192
ip local pool VISTORM_RSA 10.19.2.130-10.19.2.190 mask 255.255.255.192
ip local pool China_WEB_Access 10.19.2.194-10.19.2.222 mask
255.255.255.224
ip local pool China_FULL_Access 10.19.2.226-10.19.2.253 mask
255.255.255.224
```

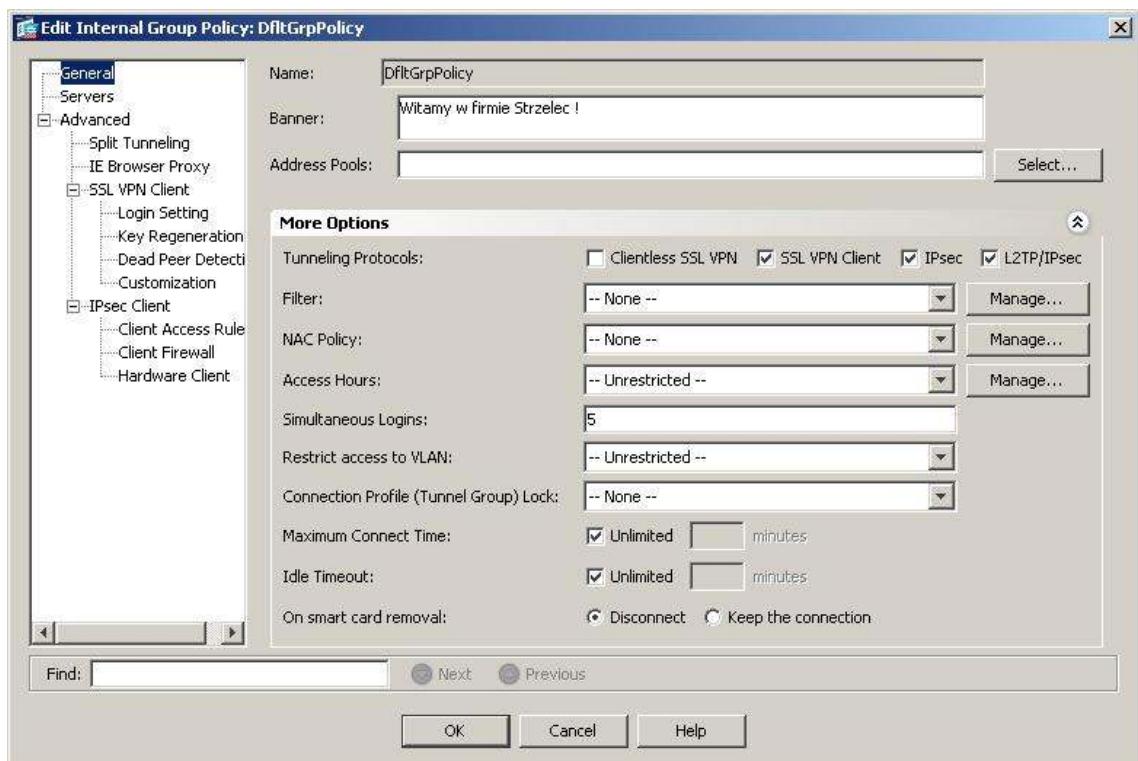
Listing 4 Opracowanie własne: konfiguracja zakresu adresów IP z poziomu linii poleceń

7.2.7 Zarządzanie polisami grup

Tworzenie grup polis VPN (ang. *VPN Group Policies*) daje możliwość indywidualnego traktowania grup użytkowników podczas zestawiania połączenia zdalnego. Polisy grup tworzą zestaw atrybutów i wartości opisujących parametry połączenia VPN. Definiując polisę dla określonej grupy użytkowników zdalnych można im zezwolić np. na używanie wszystkich metod dostępu zdalnego (IPsec, SSL VPN, L2TP/IPsec), bądź tylko wybranych, skonfigurować im inne niż pozostałym użytkownikom serwery DNS, WINS, zastosować dowolne filtrowanie(listy kontroli dostępu) na bazie adresów IP lub

usług, wyłączyć limit jednoczesnych prób uwierzytelnienia, zmienić ustawienia parametrów połączenia sieciowego, ustawienia serwera proxy w przeglądarce internetowej, czy też wymusić tzw. no split tunneling i wiele innych opcji opisanych poniżej.

Konfigurując polisy grup (Rys. 58) na koncentradorze ASA5520 można zdefiniować następujące parametry:



Rysunek 55 Opracowanie własne: Widok okna konfiguracji „VPN Polisy grup” z aplikacji ASDM

Tabela 21 Opracowanie własne: Opis funkcji „VPN Polisy grup”

| Opcja | Znaczenie |
|---------------|--|
| Name | Nazwa grupy polisy VPN |
| Banner | powitalna wiadomość jaką zobaczy użytkownik, który poprawne nawiążę komunikację poprzez tunel VPN. |
| Address Pools | możliwe jest wskazanie zdefiniowanych wcześniej pul adresów IP dla klientów |

| | |
|-------------------------|---|
| | <p>VPN. Nawiązujący komunikację użytkownik - otrzyma jeden z adresów IP będących w zakresie zdefiniowanym. W pozycji Address Pools należy wskazać zbuowaną wcześniej pulę, np.: Poland_WEB_Access</p> |
| Tunneling Protocols | <p>Używając tej opcji można zezwolić użytkownikom zdalnym na połaczenie VPN używając dowolnej wspieranej przez ASA5520 technologii zdalnego dostępu: IPsec,SSL VPN, L2TP</p> |
| Filter | <p>Pozwala zdefiniować listę kontroli dostępu IP (ang. <i>ACL</i>) dla danej grupy użytkowników. Już na tym etapie możliwym jest ograniczenie ruchu IP danym użytkownikom, bądź grupom do danych usług bądź serwerów docelowych. W opcji „Filter” należy wskazać nazwę listy kontroli dostępu (ACL) np. WEB_ACCESS, FULL_ACCESS</p> |
| Access Hours | <p>Pozwala zdefiniować zakres czasu (np. tylko od godziny 8:00 do 16:00) podczas, których możliwym będzie zalogowanie się danej grupy użytkowników. W pozostałym czasie użytkownicy nie będą mogli używać zdalnego dostępu</p> |
| Simultaneous Login | <p>Określa limit jednoczesnych prób logowania danej grupy użytkowników</p> |
| DNS Server, WINS Server | <p>Umożliwia podanie adresów IP serwerów DNS i WINS obowiązującego dla danej grupy użytkowników</p> |
| Split Tunneling | <p>Umożliwia wskazanie podsieci IP (zbudowanego obiektu), osiągalnej</p> |

poprzez tunel VPN. Pozostałe podsieci nie będą osiągalne poprzez tunel VPN, tylko poprzez domyślną bramkę do sieci Internet.

Definicja domyślnej grupy polis VPN o nazwie DfltGrpPolicy z poziomu linii poleceń wygląda następująco:

Tabela 22 Opracowanie własne: Konfiguracja zachowania (polis) grup domyślnych "Group Policy" z poziomu linii poleceń

```
group-policy DfltGrpPolicy attributes
  banner value Welcome to VPN Access (Sweden)
  dns-server value 10.220.1.10 10.10.1.1
  vpn-simultaneous-logins 5
  vpn-idle-timeout none
  vpn-tunnel-protocol IPsec 12tp-ipsec svc
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value Strzelec_Internal
  default-domain value strzelec.local
  split-dns value strzelec.local
  webvpn
```

Gdzie:

- group-policy DfltGrpPolicy attributes – wejście w tryb konfiguracji polis grup o nazwie “DfltGrpPolicy”,
- banner value Welcome to VPN Access (Sweden) – powitalna wiadomość dla użytkowników zdalnych,
- dns-server value 10.220.1.10 10.10.1.1 – definicja serwerów DNS, jakie zostaną skonfigurowane na zdalnych komputerach
- vpn-simultaneous-logins 5 – liczba jednocześnie logowań ustawiona na 5,
- vpn-idle-timeout none – czas bezczynności,
- vpn-tunnel-protocol IPsec 12tp-ipsec svc – definiuje dozwolone metody połączeń zdalnych, dla klientów VPN:

- Clientless SSL VPN - określa użycie VPN poprzez tunel SSL/TLS, który używa przeglądarki internetowej by zestawić połączenie typu *Remote Access* do koncentratora VPN. Tryb Clientless SSL VPN w łatwy sposób dostarcza możliwość prezentacji aplikacji opartych na protokole HTTP/HTTPS, zasobów struktury Windows NT (tzw. Web-enabled), klienty e-mail (oparte o serwisy WWW) , oraz inne aplikacje oparte na protokole TCP,
 - SSL VPN Client - Używa aplikacji Cisco AnyConnect, aby ustanowić połączenie od klienta do koncentratora VPN,
 - IPSec - Uważane za najbezpieczniejszą metodę zabezpieczania połączeń i tuneli VPN (Zarówno tryby *Site-to-Site jak i Client-to-Site (Remote Access)*),
 - L2TP over IPSec - Pozwala zdalnym użytkownikom komputerów PC oraz innych urządzeń mobilnych wyposażonych we wbudowaną aplikację – ustanowić bezpieczne połączenie za pośrednictwem publicznie dostępnych sieci – do koncentratora VPN i sieci firmowych. Użytkownicy wykorzystujący protokół L2TP używają protokołu PPP (protokół UDP port 1701), aby zainicjować tunel do przesyłania danych.
- `split-tunnel-policy tunnelspecified` - wpis definiuje politykę procesu *split-tunneling* (czyli wskazania podsieci IP, które mają być osiągalne poprzez tunel VPN, a pozostałych osiągalnych poprzez sieć Internet). Split tunnel pozwala na zastosowania dwóch bram w tablicy routingu na komputerach klientów. Pierwszej, aby osiągnąć firmową sieć VPN, zaś drugiej dla zwykłego ruchu do sieci Internet. Pozwala to zaoszczędzić pasmo używane przez bramę VPN, gdyż zwykły ruch generowany przez zdalonego pracownika np. przeglądanie stron internetowych puszczy zostanie bezpośrednio poprzez bramkę do dostawcy usług internetowych, zaś ruch przeznaczony do wewnętrznych usług firmowej sieci – poprzez tunel VPN.

Z punktu widzenia bezpieczeństwa sieci opcja `no split-tunnel` jest lepszym wyborem, gdyż cały ruch z komputera użytkownika do sieci Internet (w tym przeglądanie stron, pobieranie aktualizacji oprogramowania, komunikatory internetowe itd.) zostanie przekazany do koncentratora VPN. Dowolny ruch

generowany przez komputer użytkownika poddany zostanie inspekcji przez urządzenie ASA, a następnie w zależności od polityki bezpieczeństwa - zaakceptowany przez firewall w siedzibie firmy, bądź nie. Zapewniona jest także ochrona wszystkich danych przed podsłuchiwaniem informacji (ang. *Sniffing*). Używając opcji no split-tunnel – można zachować taki sam poziom ograniczeń dostępu do sieci Internet dla użytkowników zdalnych jaki panuje w lokalnej sieci w siedzibie firmy, zatem można zabronić używania sieci P2P, komunikatorów internetowych etc, co pozwoli w taki sam sposób chronić komputery zdalne jak i lokalne.

- `split-tunnel-network-list value Strzelec_Internal` – Zdefiniowanie obiektu Strzelec_Internal jako sieci 10.0.0.0/8 pozwoli wskazać całą lokalną sieć firmową, jako możliwą do osiągnięcia poprzez tunel VPN w przypadku stosowania split-tunnel. Każdy inny docelowy adres IP nie zawierający się w firmowej sieci - będzie osiągalny poprzez bramkę dostawcy Internetu,
- `default-domain value strzelec.local`,
- `split-dns value strzelec.local` – Zdefiniowanie parametrów default-domain i split-dns dla domeny strzelec.local pozwoli klientom zdalnym wysyłać wszystkie zapytania DNS o hosty z domeną strzelec.local przez tunel VPN do wewnętrznych serwerów DNS,
- `webvpn` – uruchamia wewnętrzny serwer WWW dla klientów zdalnego dostępu umożliwiając im wykorzystanie technologii SSL VPN do zestawienia połączenia z siecią firmową.

Aby zrealizować kolejne założenie projektowe mówiące o:

- ✓ możliwości przydzielania innych adresów IP dla klientów zdalnych w zależności od tego czy dany klient przynależy do pewnej grupy w Active Directory,
- ✓ możliwości filtrowania ruchu IP i usług już na poziomie koncentratora VPN (grupa ograniczona WEB_ACCESS oraz grupa bez ograniczeń FULL_ACCESS),
- ✓ zezwalania poszczególnym grupom użytkowników na wybór technik dostępu (IPsec, SSL VPN, L2TP/IPsec)

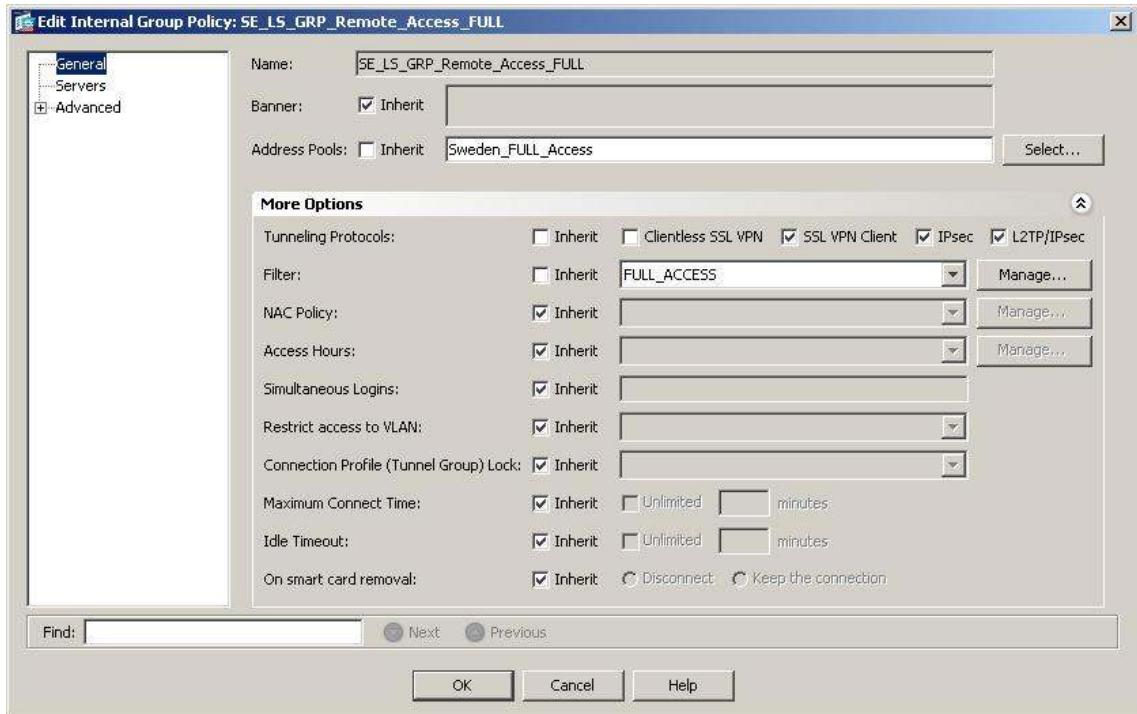
- ✓ możliwości ograniczania dostępu użytkownikom poprzez zastosowania należało zbudować odrębne zestawy group-policy na koncentratorze VPN dla grup użytkowników z każdej lokalizacji:

Tabela 23 Opracowanie własne: Tworzenie grup polis dla poszczególnych grup użytkowników (wiersz poleceń)

```
group-policy SE_LS_GRP_Remote_Access_FULL internal
group-policy SE_LS_GRP_Remote_Access_FULL attributes
dns-server value 10.220.1.10 10.10.1.1
vpn-filter value FULL_ACCESS
vpn-tunnel-protocol IPSec l2tp-ipsec svc
split-tunnel-policy tunnelspecified
split-tunnel-network-list value strzelec_Internal
address-pools value Sweden_FULL_Access
```

- group-policy SE_LS_GRP_Remote_Access_FULL internal
- group-policy SE_LS_GRP_Remote_Access_FULL attributes – definiuje nowy zestaw parametrów połączenia dla grupy o nazwie SE_LS_GRP_Remote_Access_FULL,
- dns-server value 10.220.1.10 10.10.1.1 – wskazuje serwery DNS, które będą używane przez użytkowników zdalnego dostępu,
- vpn-filter value FULL_ACCESS – nakazuje użycia listy kontroli dostępu o nazwie FULL_ACCESS,
- vpn-tunnel-protocol IPSec l2tp-ipsec svc – zezwala na użycie wszystkich dostępnych technologii umożliwiających zestawienie zdalnego połączenia (IPsec, SSL VPN, L2TP/IPsec),
- split-tunnel-policy tunnelspecified,
- „split-tunnel-network-list value strzelec_Internal – uruchomienie split-tunnelingu dla firmowej sieci (obiekt Strzelec_Internal – 10.0.0.0/8),
- address-pools value Sweden_FULL_Access – nakazuje urządzeniu ASA automatycznie przydzielać adresy IP klientom zdalnym zgodnie z wcześniejszą definicją obiektu „Sweden_FULL_Access”.

```
ip local pool Sweden_FULL_Access 10.19.0.66-
10.19.0.126 mask 255.255.255.192
```



Rysunek 56 Opracowanie własne: Definicja polis grup dla poszczególnych grup użytkowników z poziomu aplikacji ASDM

Przykładem grupy polis z ograniczeniami (WEB_ACCESS) jest zdefiniowana dla użytkowników z Indii grupa (IN_LS_GRP_Remote_Access_WEB):

```
group-policy IN_LS_GRP_Remote_Access_WEB internal
group-policy IN_LS_GRP_Remote_Access_WEB attributes
vpn-filter value WEB_ACCESS
split-tunnel-policy excludespecified
split-tunnel-network-list value Local_LAN
address-pools value India_WEB_Access
```

Rysunek 57 Opracowanie własne: Definicja zestawu polis dla grupy z ograniczeniami dostępu

Na użytkowników tej grupy nałożone zostaną ograniczenia zgodnie z definicją poleceń:

- `vpn-filter value WEB_ACCESS` – filtrowanie za pomocą listy kontroli dostępu o nazwie WEB_ACCESS,
- `split-tunnel-policy excludespecified`,

- `split-tunnel-network-list value Local_LAN` – czyli cały ruch z komputera użytkownika do Internetu wysyłany będzie do firmowej sieci lokalnej za wyjątkiem(ang. *excludespecified*) ruchu do sieci LAN użytkownika(ang. *Local_LAN*),
- `address-pools value India_WEB_Access` nakazuje urządzeniu ASA automatycznie przydzielać adresy IP klientom zdalnym zgodnie z wcześniejszą definicją obiektu `India_WEB_Access`
`ip local pool Sweden_FULL_Access 10.19.1.2-10.19.1.62
mask 255.255.255.192.`

Kolejne grupy polis dla poszczególnych lokalizacji tworzone są analogicznie:

Tabela 24 Opracowanie własne: Wzorzec dla pozostałych polis grup

| |
|---|
| Dla grup z ograniczeniami FULL_ACCESS: |
| <pre>group-policy FR_LS_GRP_Remote_Access_FULL internal group-policy FR_LS_GRP_Remote_Access_FULL attributes dns-server value 10.220.1.10 10.10.1.1 vpn-filter value FULL_ACCESS split-tunnel-policy tunnelspecified split-tunnel-network-list value strzelec_Internal address-pools value FR_FULL_Access</pre> |
| Dla grup z ograniczeniami WEB_ACCESS: |
| <pre>group-policy FR_LS_GRP_Remote_Access_WEB internal group-policy FR_LS_GRP_Remote_Access_WEB attributes vpn-filter value WEB_ACCESS split-tunnel-policy excludespecified split-tunnel-network-list value Local_LAN address-pools value France_WEB_Access</pre> |

7.2.8 Listy kontroli dostępu (ACL)

Aby zrealizować założenie projektowe mówiące o możliwości filtrowania ruchu pochodzącego z komputerów klientów już w warstwie IP, koniecznym było zbudowanie

list kontroli dostępu tzw. ACL (ang. *Access Control List*). Lista ACL jest programowym filtrem, w którym parametrami wejściowymi mogą być:

W przypadku list ACL zwykłych:

- Adres IP sieci lub hosta docelowego

W przypadku list rozszerzonych:

- Źródłowy i/lub docelowy adres IP sieci lub hosta,
- Usługa (ang. *Service*) definiowana jako nazwa lub port TCP/UDP (np. dla usługi rozwiązywania nazw hostów na IP oznaczenie: DNS/UDP, lub jednoznacznie 53/UDP)

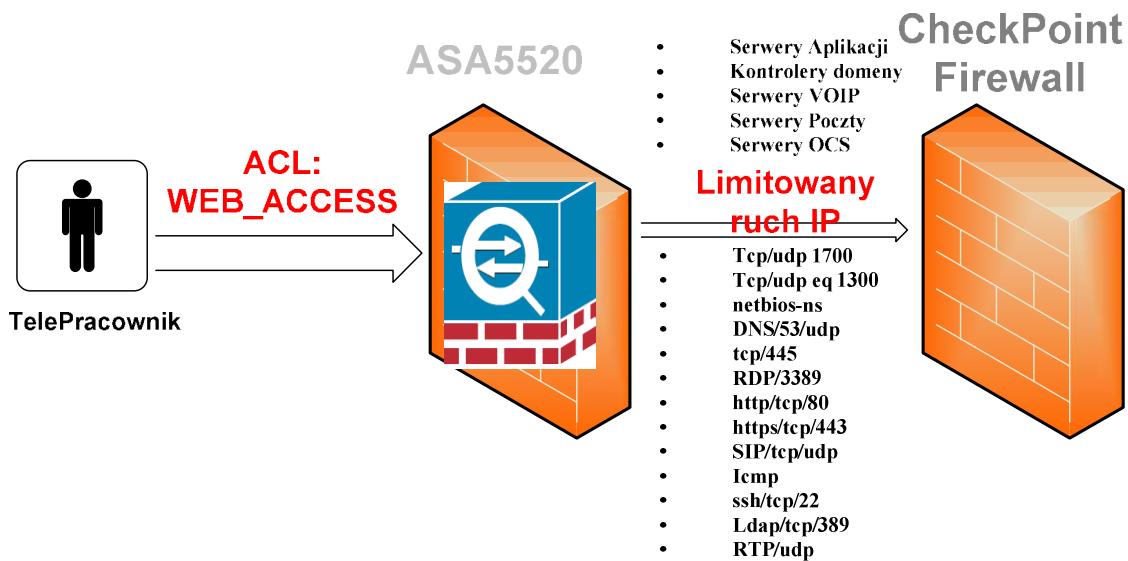
Aby zbudować listy ACL na urządzeniu ASA5520 koniecznym było zgromadzenie informacji na temat adresów IP serwerów, usług i sieci jakie mogą być osiągalne przez zdalnych klientów, a które uruchomione są wewnątrz lokalnej sieci korporacyjnej.

Zbudowano trzy rozszerzone listy kontroli dostępu o nazwach:

- WEB_ACCESS
- FULL_ACCESS
- VISTORM_RSA

Budowa listy dostępu dla użytkowników o ograniczonym dostępie (WEB_ACCESS)

Rozszerzona lista ACL o nazwie WEB_ACCESS powinna zezwolić na limitowany ruch IP od wszystkich klientów zdalnego dostępu, którzy znajdują się w domyślnych grupach domenowych (dla wszystkich użytkowników zdalnych spoza działu IT).



Rysunek 58 Opracowanie własne: Zasada działania ograniczonej listy kontroli dostępu WEB_ACCESS

Ograniczona lista ACL ma zapewnić dostęp klientom zdalnym do wielu usług uruchomionych w lokalnej sieci korporacyjnej :

| Serwer lub usługi | Adres(y) IP i nazwa: | Porty |
|--|--|--|
| Serwery plików i aplikacji | 10.10.2.22 (APP SERVER02) 10.39.32.22 (APP SERVER04) 10.11.2.6 (APP SERVER06) 10.182.46.2 (APP SERVER08) | <ul style="list-style-type: none"> • Tcp/udp 1700 • Tcp/udp eq 1300 • netbios-ns • netbios-dgm • netbios-ssn • DNS/53/udp • tcp/445 • RDP/3389 • HTTP/tcp/80 • HTTPS/tcp/443 • ICMP |
| Serwery pocztowe (Microsoft Exchange) | 10.39.32.1 (EXCH SERVER01) 10.39.32.3 (EXCH SERVER02) 10.10.1.22 (EXCH SERVER03) 10.10.1.21 (EXCH SERVER04) 10.39.32.5 (EXCH SERVER05) 10.39.48.131 (EXCH SERVER06) | <ul style="list-style-type: none"> • netbios-ns • netbios-dgm • netbios-ssn • tcp/445 • DNS/53/udp • RDP/3389 • HTTP/tcp/80 • HTTPS/tcp/443 • ICMP |

| | | |
|--|--|---|
| Kontrolery domeny (Active Directory) | 10.10.2.51 (DCCONTROLLER01) 10.11.2.149 (DCCONTROLLER02) 10.11.2.49 (DCCONTROLLER03) | <ul style="list-style-type: none"> • netbios-ns • netbios-dgm • netbios-ssn • tcp/445 • RDP/3389 • DNS/53/udp • KERBEROS/ • ICMP |
| Telefonia IP (VOIP) | 10.220.1.9 (TRIXBOX_PL) 10.182.6.9 (TRIXBOX_FR) | <ul style="list-style-type: none"> • Sip:5060(TCP/UDP) • Sip:5061(TCP) • SSH/tcp/22 • ICMP • HTTP/tcp/80 • HTTPS/tcp/443 • Porty dla RTP (50001-51000) |
| Serwer OCS/LCS (komunikator sieciowy) | 10.10.2.45 (OCSSERVER01) 10.39.48.135 (OCSSERVER02) | <ul style="list-style-type: none"> • Porty dla RTP (50001-51000) • 5060(TCP/UDP) • 5061(TCP) • 5062(TCP) • 5063(TCP) |

Aby zbudować listę kontroli dostępu ograniczonego należy zdefiniować obiekty (sieci, hosty, usługi), które mają mieć zagwarantowany dostęp do sieci.

```

name 1.1.1.7 Outside_Interface
name 10.220.2.200 SD Server
name 10.10.2.22 APPSERVER02
name 10.10.2.23 APPSERVER03
name 10.39.32.22 APPSERVER04
name 10.11.2.6 APPSERVER06
name 10.182.46.2 APPSERVER08
name 10.39.32.1 EXCHSERVER01
name 10.39.32.3 EXCHSERVER02
name 10.10.1.22 EXCHSERVER03
name 10.10.1.21 EXCHSERVER04

```

```
name 10.39.32.5 EXCHSERVER05
name 10.39.48.131 EXCHSERVER06
name 10.39.42.128 FR_VISTORM_RSA
name 10.10.2.45 OCSSERVER01 description LCS server
name 10.39.48.135 OCSSERVER02 description LCS server
name 10.10.2.51 DCCONTROLLER01
name 10.11.2.149 DCCONTROLLER02
name 10.11.2.49 DCCONTROLLER03
name 10.220.1.9 TRIXBOX_PL description Trixbox Poland
name 10.182.6.9 TRIXBOX_FR description Trixbox FR
```

Listing 5 Opracowanie własne: Definicja obiektów hostów

Powyższy listing definiuje obiekty, którymi są adresy IP oraz nazwy serwerów, które będą osiągalne dla zdalnych pracowników.

name 10.10.2.22 APPSERVER02 – Definiuje obiekt o nazwie APPSERVER02 i o adresie IP 10.10.2.22

Następnie zbudowane obiekty hostów można połączyć w odpowiednio nazwane grupy, np. grupę zawierającą wszystkie serwery MS Exchange, czy też wszystkie kontrolery domeny Active Directory.

```
object-group network Exchange_Servers
    description All strzelec exchange servers
    network-object host EXCHSERVER01
    network-object host EXCHSERVER02
    network-object host EXCHSERVER03
    network-object host EXCHSERVER04
    network-object host EXCHSERVER05
    network-object host EXCHSERVER06

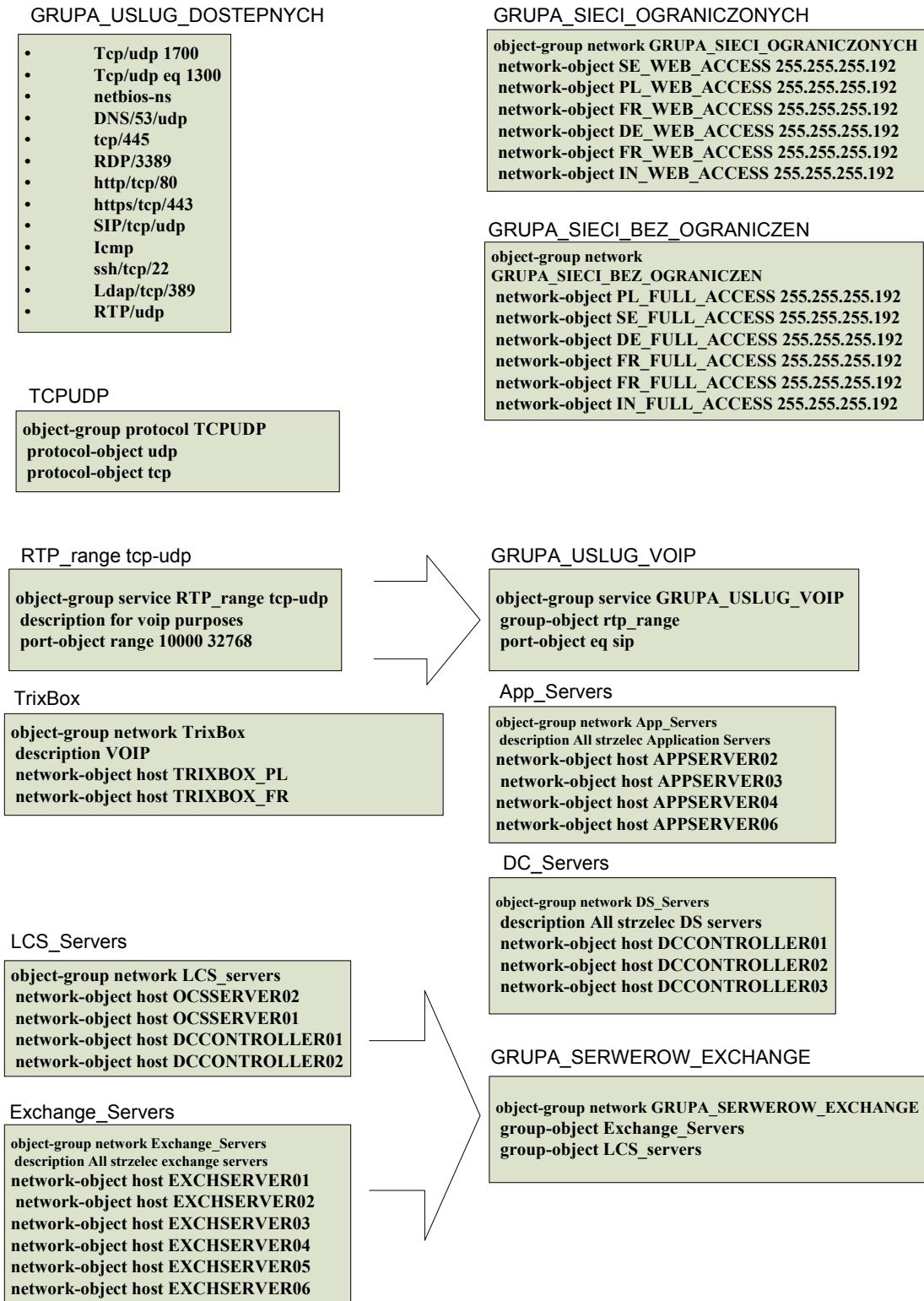
object-group network App_Servers
    description All strzelec Application servers
    network-object host APPSERVER02
    network-object host APPSERVER03
    network-object host APPSERVER04
```

```
network-object host APPSERVER06

object-group network DS_Servers
description All strzelec DS servers
network-object host DCCONTROLLER01
network-object host DCCONTROLLER02
network-object host DCCONTROLLER03
```

Listing 6 Opracowanie własne: Przykład tworzenia grup serwerów jako jeden obiekt

Aby listy dostępu miały przejrzystą formę, warto zamiast posługiwać się szczegółowymi adresami hostów, podsieci IP lub usługami – tworzyć grupy zawierające obiekty, np. zdefiniowany obiekt GRUPA_SIECI_OGRANICZONYCH zawiera w sobie sześć wcześniej zbudowanych obiektów XX_WEB_ACCESS (zawierające odpowiednie pule adresów ip klientów zdalnego dostępu). Następnie definiując kolejne listy dostępu można wielokrotnie posługiwać się jedną nazwą grupy, co sprawia, że osoba czytająca lub poprawiająca pliki konfiguracyjne koncentratora VPN może w łatwy sposób zrozumieć działanie list ACL.



Rysunek 59 Opracowanie własne: Zestawienie wszystkich grup obiektów zbudowanych na koncentratorze VPN

object-group network GRUPA_SIECI_OGRANICZONYCH

```
network-object SE_WEB_ACCESS 255.255.255.192
network-object PL_WEB_ACCESS 255.255.255.192
network-object FR_WEB_ACCESS 255.255.255.192
network-object DE_WEB_ACCESS 255.255.255.192
network-object FR_WEB_ACCESS 255.255.255.192
network-object IN_WEB_ACCESS 255.255.255.192
network-object CN_WEB_ACCESS 255.255.255.192
```

Listing 7 Opracowanie własne: Tworzenie grupy obiektów

Podobnie jak tworzenie grup hostów, podsieci IP – można tworzyć i nazywać grupy usług sieciowych (portów i protokołów):

```
object-group service GRUPA_USLUG_DOZWOLONYCH
    service-object ICMP
    service-object tcp-udp eq domain
    service-object tcp eq www
    service-object tcp eq HTTPS
    service-object tcp eq 445
    service-object tcp eq 3389
    service-object tcp eq 5061
    service-object tcp eq netbios-ssn
    service-object udp eq netbios-dgm
    service-object udp eq netbios-ns
    service-object tcp eq sip
    service-object udp eq 5061
    service-object udp eq sip
    service-object tcp-udp eq 1030
    service-object tcp-udp eq 1700
    service-object tcp eq 5062
    service-object udp eq 5062
    service-object udp range 50001 51000
    service-object tcp-udp eq 5063
```

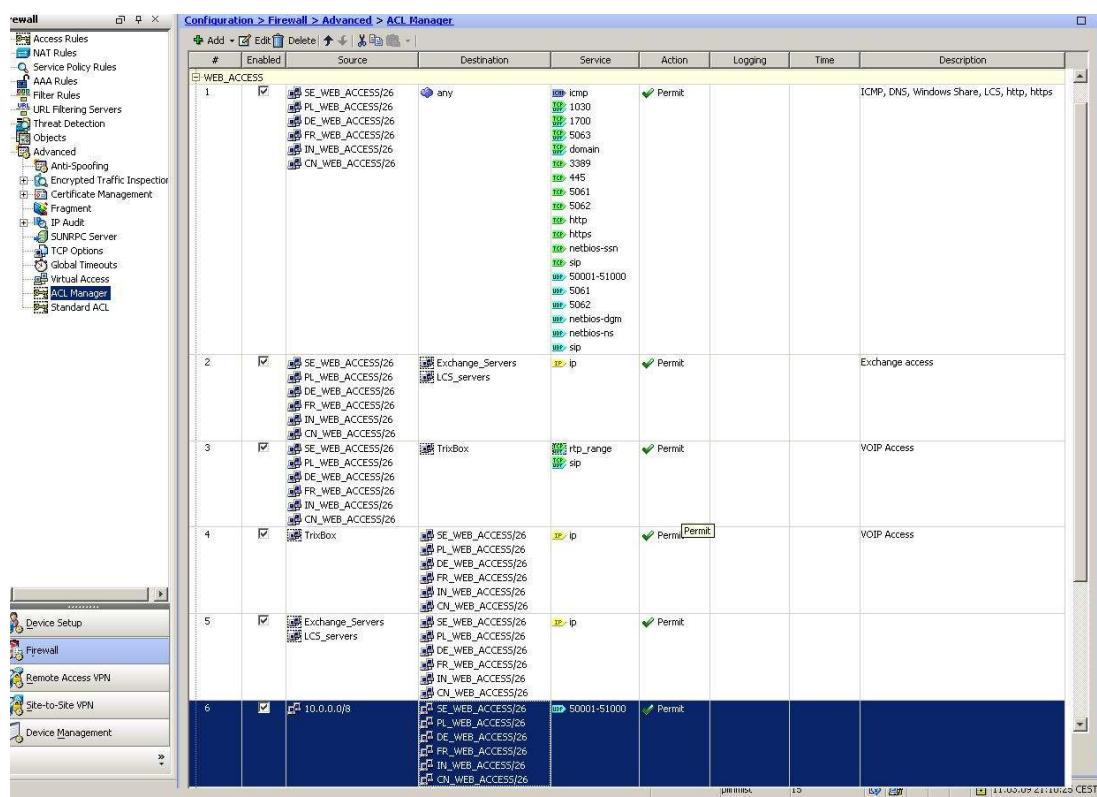
Listing 8 Opracowanie własne: Tworzenie grupy usług sieciowych

Definicja grupy usług sieciowych to nic innego jak wskazanie jakie porty (TCP lub UDP) lub jaki ich zakres ma być brany pod uwagę.

`service-object udp range 50001 51000` – Definiuje zakres portów UDP od 50001 do 50000.

`service-object tcp eq www` – Jak widać można zamiast numeru portu wskazać nazwę usługi WWW

Mając zdefiniowane wszystkie obiekty (sieci, hosty, usługi) można przystąpić do tworzenia właściwych list ACL. Z poziomu aplikacji ASDM można to zrobić analogicznie jak na rys. nr 64



Rysunek 60 Opracowanie własne: Lista WEB_ACCESS zbudowana przy pomocy ASDM

Analogicznie zbudowana lista ACL z poziomu linii poleceń:

```
access-list WEB_ACCESS remark ICMP, DNS, Windows Share,
LCS, HTTP, HTTPS
access-list WEB_ACCESS extended permit object-group
GRUPA_USLUG_DOZWOLONYCH object-group
```

```

GRUPA_SIECI_OGRANICZONYCH any
access-list WEB_ACCESS remark Exchange access
access-list WEB_ACCESS extended permit ip object-group
GRUPA_SIECI_OGRANICZONYCH object-group
GRUPA_SERWEROW_EXCHANGE
access-list WEB_ACCESS remark Application server access
access-list WEB_ACCESS extended permit ip object-group
GRUPA_SIECI_OGRANICZONYCH object-group APP_Servers
access-list WEB_ACCESS remark Application DS access
access-list WEB_ACCESS extended permit ip object-group
GRUPA_SIECI_OGRANICZONYCH object-group DS_Servers
access-list WEB_ACCESS extended permit object-group TCPUDP
object-group GRUPA_SIECI_OGRANICZONYCH object-group TrixBox
object-group GRUPA_USLUG_VOIP
access-list WEB_ACCESS remark VOIP Access
access-list WEB_ACCESS extended permit ip object-group
TrixBox object-group GRUPA_SIECI_OGRANICZONYCH
access-list WEB_ACCESS extended permit ip object-group
GRUPA_SERWEROW_EXCHANGE object-group
GRUPA_SIECI_OGRANICZONYCH
access-list WEB_ACCESS extended permit ip object-group
APP_Servers object-group GRUPA_SIECI_OGRANICZONYCH
access-list WEB_ACCESS extended permit ip object-group
DS_Servers object-group GRUPA_SIECI_OGRANICZONYCH
access-list WEB_ACCESS extended permit udp 10.0.0.0
255.0.0.0 object-group GRUPA_SIECI_OGRANICZONYCH range
50001 51000

```

Wzorcem do zastosowania polecenia „access-list” w wersji rozszerzonej jest:

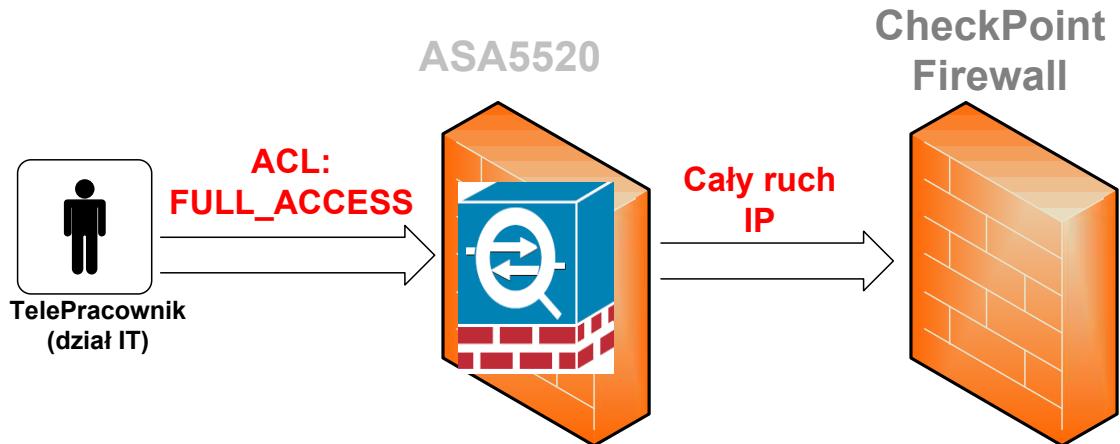
```

access-list NAZWA_LIST extended permit/deny ip/tcp/udp
ŹRÓDŁOWA_SIEC DOCELOWA_SIEĆ USŁUGI

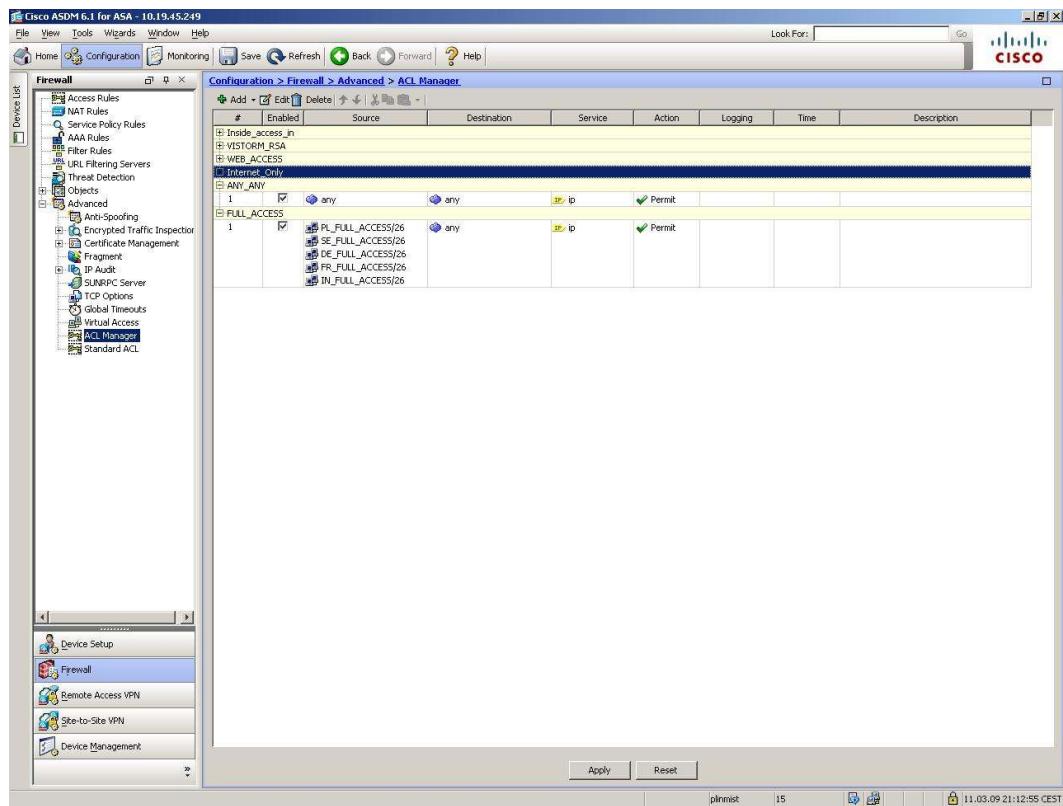
```

**Budowa listy dostępu dla użytkowników o nieograniczonym dostępie
(FULL_ACCESS)**

Druga lista ACL o nazwie FULL_ACCESS ma zapewnić przepływ całego ruchu IP bez żadnych restrykcji od wszystkich klientów zdalnego dostępu, którzy znajdą się w odpowiednich grupach domenowych (tylko dla wykwalifikowanego personelu IT).



Rysunek 61 Opracowanie własne: Zasada działania kontroli list dostępu o nazwie FULL_ACCESS



Rysunek 62 Opracowanie własne: Budowa listy ACL "Full_Access" z poziomu aplikacji ASDM

Lista ACL o nazwie „FULL_ACCESS” ma za zadanie przepuścić CAŁY ruch IP pochodzący z pul adresów IP o nazwach:

```
Sweden_FULL_Access 10.19.0.66-10.19.0.126 mask  
255.255.255.192  
Poland_FULL_Access 10.19.0.194-10.19.0.254 mask  
255.255.255.192  
India_FULL_Access 10.19.1.66-10.19.1.126 mask  
255.255.255.192  
Germany_FULL_Access 10.19.1.194-10.19.1.254 mask  
255.255.255.192  
France_FULL_Access 10.19.2.66-10.19.2.126 mask  
255.255.255.192  
China_FULL_Access 10.19.2.226-10.19.2.253 mask  
255.255.255.224
```

Analogicznie zbudowana lista kontroli dostępu z poziomu linii poleceń wygląda następująco:

```
object-group network GRUPA_SIECI_BEZ_OGRANICZEN  
    network-object PL_FULL_ACCESS 255.255.255.192  
    network-object SE_FULL_ACCESS 255.255.255.192  
    network-object DE_FULL_ACCESS 255.255.255.192  
    network-object CN_FULL_ACCESS 255.255.255.192  
    network-object FR_FULL_ACCESS 255.255.255.192  
    network-object IN_FULL_ACCESS 255.255.255.192
```

Listing 9 Opracowanie własne: Budowa grupy obiektów z poziomu linii poleceń

object-group network GRUPA_SIECI_BEZ_OGRANICZEN – tworzy grupę obiektów o nazwie GRUPA_SIECI_BEZ_OGRANICZEN, której członkami są zdefiniowane wcześniej obiekty sieciowe XX_FULL_ACCESS (zawierające odpowiednie pule adresów ip klientów zdalnego dostępu).

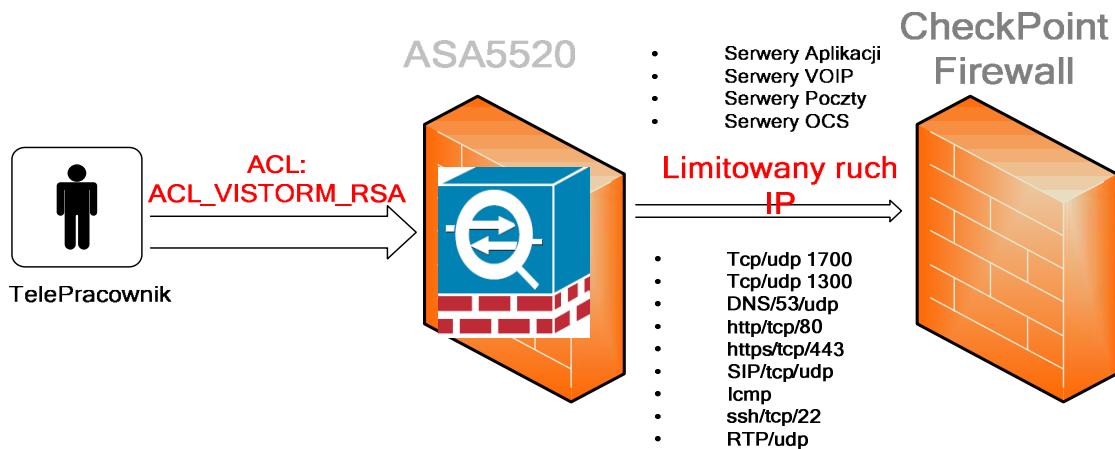
Mając tak zdefiniowaną grupę obiektów i pul adresów IP można przystąpić do budowy rozszerzonej listy dostępu:

```
access-list FULL_ACCESS extended permit ip object-group  
GRUPA_SIECI_BEZ_OGRANICZEN any
```

Listing 10 Opracowanie własne: Budowa rozszerzonej listy dostępu FULL_ACCESS

Tak wykonane polecenie zostanie zinterpretowane przez urządzenie ASA jako rozkaz do zbudowania rozszerzonej listy dostępu o nazwie FULL_ACCESS, która zezwala na cały ruch ip pochodzący ze źródła, którym jest obiekt GRUPA_SIECI_BEZ_OGRANICZEN, a którego celem jest dowolna sieć IP lub host.

Budowa listy kontroli dostępu ACL_VISTORM_RSA dla użytkowników korzystających z metody uwierzytelnienia opartej o jednorazowe hasła.



Rysunek 63 Opracowanie własne: Zasada działania ograniczonej listy kontroli dostępu ACL_VISTORM_RSA

Lista dostępu ACL_VISTORM_RSA jest podobnie zbudowana do listy WEB_ACCESS i korzysta w dużej mierze z tych samych obiektów , jednakże do różnic zaliczyć można ograniczony dostęp do serwerów świadczących usługi kontrolery domeny AD oraz ograniczone usługi (porty).

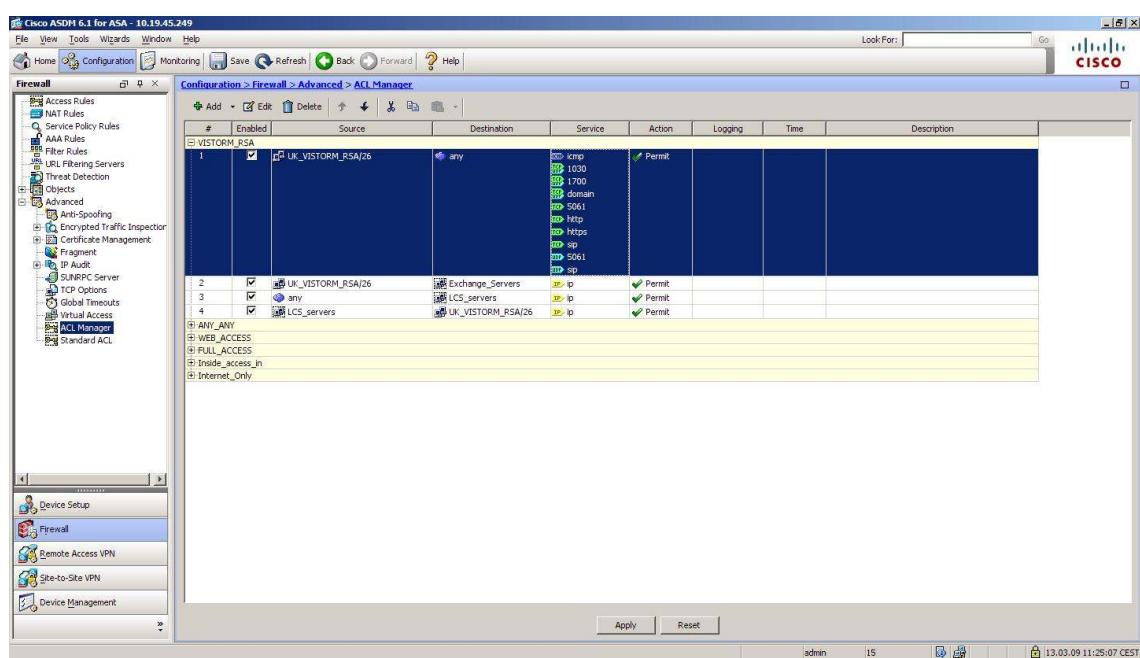
```
object-group service GRUPA_USLUG_DOZWOLONYCH_RSA
    service-object ICMP
    service-object tcp-udp eq domain
    service-object tcp eq www
    service-object tcp eq HTTPS
    service-object tcp eq 5061
    service-object tcp eq sip
    service-object udp eq 5061
```

```

service-object udp eq sip
service-object tcp-udp eq 1030
service-object tcp-udp eq 1700
service-object tcp eq 5062
service-object udp eq 5062
service-object udp range 50001 51000
service-object tcp-udp eq 5063

```

Rysunek 64 Opracowanie własne: Definicja grupy usług dla użytkowników korzystających z uwierzytelnienia poprzez podanie jednorazowych hasel



Rysunek 65 Opracowanie własne: Widok okna ASDM, gdzie zbudowana jest lista kontroli dostępu ACL_VISTORM_RSA

Używając wiersza poleceń koncentratora VPN zbudowana została lista kontroli dostępu w analogiczny jak przy liście ACL: WEB_ACCESS sposób:

```

access-list ACL_VISTORM_RSA extended permit object-group GRUPA_USLUG_DOZWOLONYCH_RSA object-group VISTORM_RSA any
access-list ACL_VISTORM_RSA extended permit ip object-group VISTORM_RSA object-group GRUPA_SERWEROW_EXCHANGE
access-list ACL_VISTORM_RSA extended permit ip object-group VISTORM_RSA object-group APP_Servers
access-list ACL_VISTORM_RSA extended permit object-group

```

```
TCPUDP object-group VISTORM_RSA object-group TrixBox
object-group GRUPA_USLUG_VOIP
access-list ACL_VISTORM_RSA extended permit ip object-group
TrixBox object-group VISTORM_RSA
access-list ACL_VISTORM_RSA extended permit ip object-group
GRUPA_SERWEROW_EXCHANGE object-group VISTORM_RSA
access-list ACL_VISTORM_RSA extended permit ip object-group
APP_Servers object-group VISTORM_RSA
access-list ACL_VISTORM_RSA extended permit udp 10.0.0.0
255.0.0.0 object-group VISTORM_RSA range 50001 51000
```

Listing 11 Opracowanie własne: Lista ACL: ACL_VISTORM_RSA

7.2.9 Autoryzacja użytkowników

Zgodnie z wymaganiami projektowymi należy zapewnić możliwość uwierzytelniania użytkowników za pomocą metod:

- ✓ Nazwa użytkownika/hasło z domeny Active Directory
- ✓ Z użyciem jednorazowych haseł (*OTP*) – generowanych przez sprzętowe Tokeny RSA (dla użytkowników spoza domeny Active Directory)

Aby zapewnić realizację punktu pierwszego zdecydowano się na użycie znajdujących się wewnętrz sieci korporacyjnej serwerów IAS (ang. *Internet Authentication Service*), czyli serwerów RADIUS zainstalowanych na systemach operacyjnych Windows 2003. Możliwość autentykacji poprzez RSA SecurID (sprzętowe tokeny generujące jednorazowe hasła) zapewnia zewnętrzny serwer świadczący usługi SDI (ang. *Security Dynamics Incorporated*).

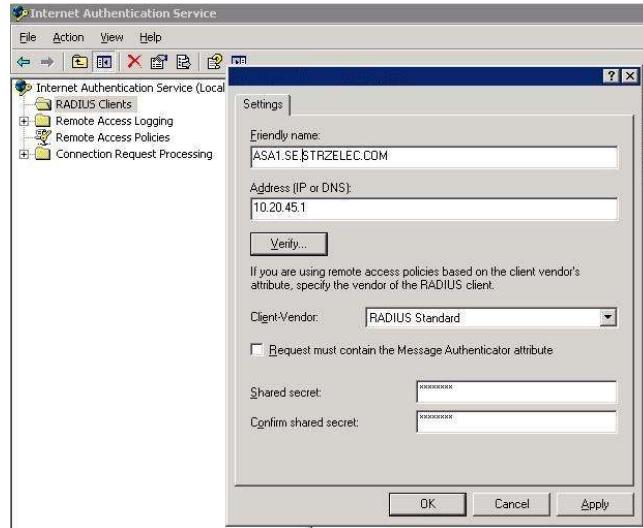
Konfiguracja Serwera IAS (RADIUS)

Z uruchomionej konsoli IAS należy wybrać pozycję New RADIUS Client a następnie wypełnić pola:

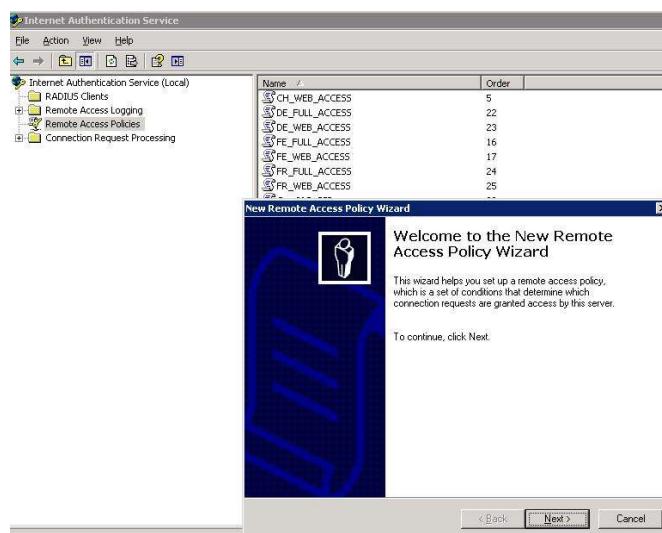
friendly name: wpisem asa1.se.teleca.com – czyli dokładnie taka nazwa jaką posiada koncentrator VPN

Address IP or DNS – należy wskazać adres IP koncentratora VPN należący do Interfejsu sieciowego łączącego go z siecią korporacyjną (10.20.45.1)

W pole tekstowe Shared secret – należy podać frazę, za pomocą której serwer IAS oraz koncentrator VPN będą mogły wzajemnie się uwierzytelnić.

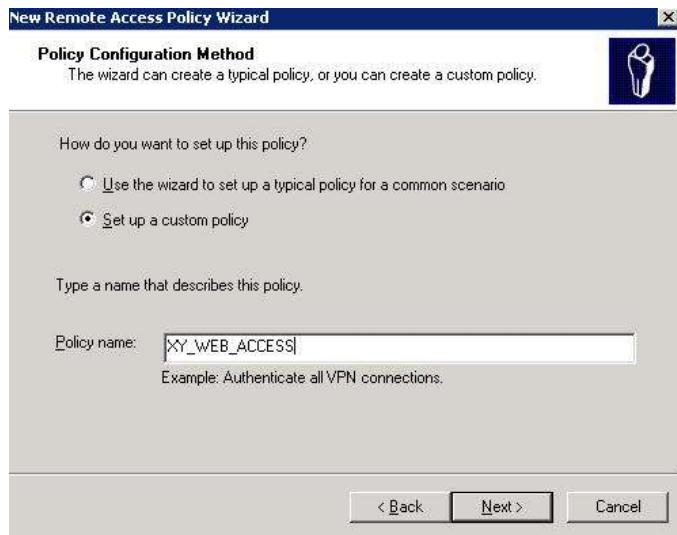


Rysunek 66 Opracowanie własne: Konfiguracja nowego klienta serwera RADIUS
Następnie należy dodać nową polisę (zestaw konfiguracji) zdalnego dostępu.



Rysunek 67 Opracowanie własne: Konfiguracja nowej polisy zdalnego dostępu

Nazwę polisy Policy name należy konstruować według wzorca XY_TYPDOSTEPU_ACCESS,
gdzie XY – dwie pierwsze litery państwa (np. PL, SE, DE, FR, IN,CN)
TYPDOSTEPU – to WEB (dla ruchu z ograniczeniami) lub FULL (ruch bez ograniczeń).



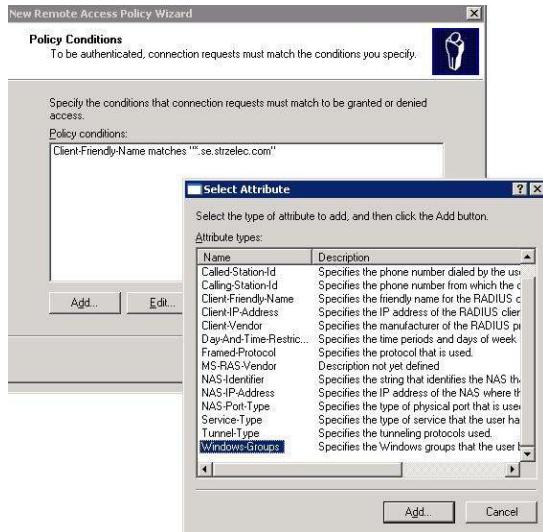
Rysunek 68 Opracowanie własne: Konfiguracja nowej polisy zdalnego dostępu c.d.

Zatem finalnie powstać powinny polisy o nazwach:

Tabela 25 Opracowanie własne: Konstrukcja nazwy polis zdalnego dostępu

| Klienci z dostępem ograniczonym | Klienci z dostępem bez ograniczeń |
|---------------------------------|-----------------------------------|
| PL_WEB_ACCESS | PL_FULL_ACCESS |
| SE_WEB_ACCESS | SE_FULL_ACCESS |
| DE_WEB_ACCESS | DE_FULL_ACCESS |
| IN_WEB_ACCESS | IN_FULL_ACCESS |
| CN_WEB_ACCESS | CN_FULL_ACCESS |
| FR_WEB_ACCESS | FR_FULL_ACCESS |

W dalszym etapie konfiguracji nowej polisy należy skonstruować (z dostępnych opcji) warunki jakie będzie musiał spełnić zdalny klient, aby dana polisa zagwarantowała mu dostęp. Należy pamiętać, że dodawanie kolejnych warunków oznacza, że klienta zdalny będzie musiał je wszystkie na raz spełnić.



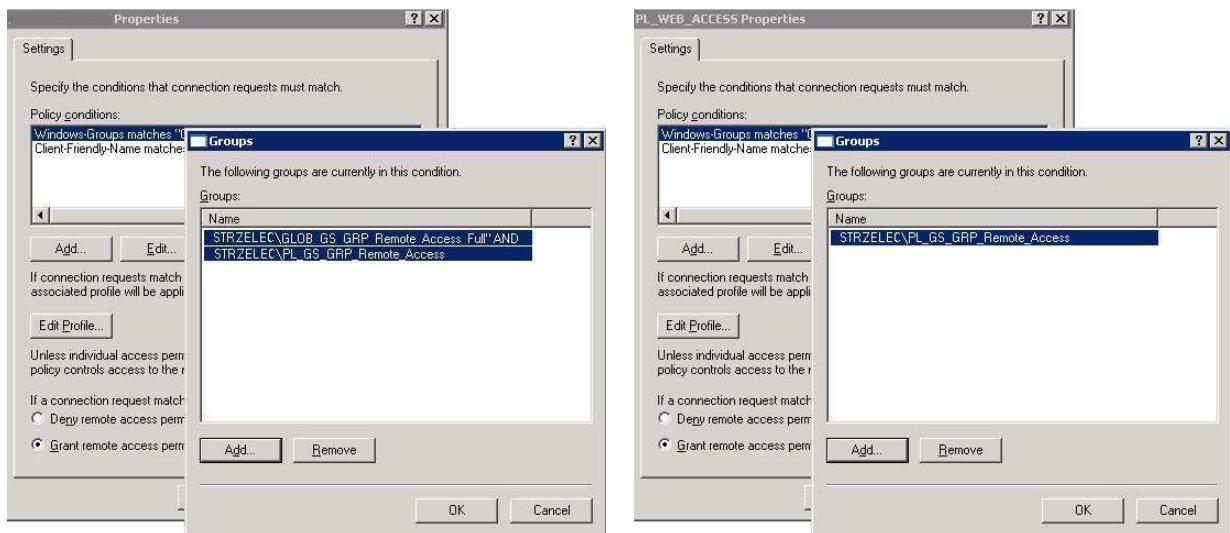
Rysunek 69 Opracowanie własne: Konstruowanie warunków dostępu dla klientów zdalnych

Z listy należy wybrać dwa warunki:

Client-Friendly-name definiującą nazwę klienta RADIUS (w tym przypadku jest to nazwa koncentratora VPN. Wypełniając to pole można posłużyć się znakami wieloznacznymi np. *.se.strzelec.com

Windows Groups" definiującą grupy domenowe (domeny Active Directory STRZELEC), których zdalny użytkownik musi być członkiem.

W zależności od tego czy aktualnie konfigurowana jest polisa dostępu zdalnego dla użytkowników z ograniczeniami (XY_WEB_ACCESS), czy też grupa użytkowników bez ograniczeń (XY_FULL_ACCESS), należy dodać inne grupy domenowe.



Dla polis typu XY_FULL_ACCESS należy dodać dwie grupy domenowe:
 STRZELEC\GLOB_GS_GRP_Remote_ACCESS FULL
 STRZELEC\XY_GS_GRP_Remote_ACCESS

Dla polis typu XY_WEB_ACCESS należy dodać dwie tylko jedną grupę domenową:
 STRZELEC\GLOB_GS_GRP_Remote_ACCESS FULL
 STRZELEC\XY_GS_GRP_Remote_ACCESS

Rysunek 70 Opracowanie własne: Konstruowanie warunków dostępu dla klientów zdalnych

Kiedy żądane warunki zostaną zdefiniowane, należy zaznaczyć opcję Grant Remote Access permission, a następnie przejść do edycji profilu (Edit Profile). W zakładce Authentication należy zaznaczyć jedynie opcję:

Microsoft Encrypted Authentication version 2 (MS-CHAPv2), gdyż protokół ten jest udoskonaloną wersją MS-CHAP I pozwala na przesyłanie hasła użytkownika w formie zaszyfrowanej.

W zakładce Advanced należy wskazać atrybuty jakie serwer RADIUS ma przesyłać do koncentratora VPN w przypadku pozytywnej weryfikacji osoby. Na podstawie tych parametrów, koncentrator VPN przyzna użytkownikom adresy z odpowiedniej puli dla ich kraju oraz zastosuje odpowiednie listy kontroli dostępu. Atrybutami jakie powinien zwrócić serwer RADIUS są:

Class – jest to pole, w którym należy umieścić dokładną nazwę grupy polis opracowanych wcześniej na urządzeniu ASA (patrz rozdział „zarządzanie polisami grup”). Nazwa ta powinna być poprzedzona symbolem OU=

Np.: dla polisy zdalnego dostępu PL_WEB_ACCESS (dla użytkowników z kraju Polska)

Należy w polu Class wskazać:

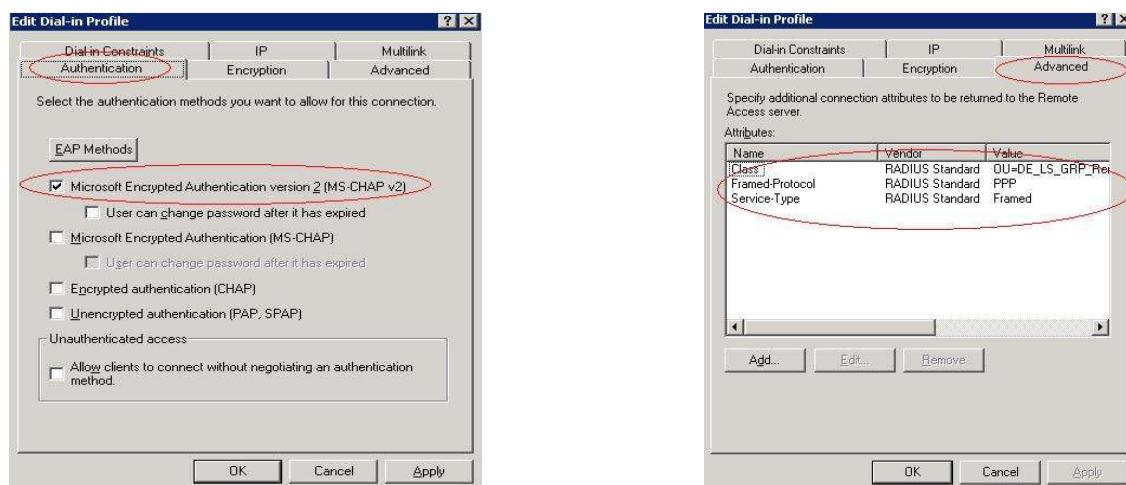
OU=PL_LS_GRP_Remote_Access_WEB

FramedProtocol – wskazuje używany protokół warstwy łączącej danych (tutaj PPP)

Service Type – tutaj Framed

Dla każdej z polis zdalnego dostępu pole Class powinno zawierać inną wartość zależną od definicji nazwy grupy polis na koncentratorze VPN.

Tabela 26 Opracowanie własne: Zaawansowana konfiguracja polis zdalnego dostępu serwera RADIUS



Finalnie na serwerze RADIUS powinno powstać lista 12 polis dla zdalnego dostępu, przy czym kolejność w jakiej występują ma znaczenie, gdyż lista jest sprawdzana od góry do dołu do pierwszego dopasowania. Zatem na samej górze listy należy umieścić polisy, których warunki najtrudniej spełnić zdalnym użytkownikom (XY_FULL_ACCESS), zaś polisy, które mają mniej warunków (XY_WEB_ACCESS) poniżej.

7.2.10 Konfiguracja modelu AAA na koncentratorze VPN

Aby zweryfikować użytkowników, próbujących podłączyć się do firmowej sieci korporacyjnej na urządzeniu ASA, należy zdefiniować grupę urządzeń AAA (AAA Server Groups). Grupa ta w zależności od konfiguracji może wykorzystywać następujące protokoły służące pośrednio do uwierzytelnienia użytkowników:

- **Radius,**
- **SDI (SecurID – z użyciem jednorazowych haseł),**
- Tacacs+,
- NT Domain,
- Kerberos,
- Ldap.

Aby zrealizować cele projektowe - zdefiniowane zostały dwie grupy modelu AAA.

Pierwsza grupa o nazwie AD-STRZELEC wykorzystująca serwery IAS (RADIUS), natomiast grupa druga o nazwie TEST_SDI, serwer SDI (ang. *SecurID*).

Konfiguracja grupy dotyczącej serwerów RADIUS i SDI wygląda następująco:

```
aaa-server AD-STRZELEC protocol radius
  accounting-mode simultaneous
  reactivation-mode timed
  max-failed-attempts 3
aaa-server AD-STRZELEC (Inside) host 10.9.25.251
  timeout 2
  key qweRty13214
aaa-server AD-STRZELEC (Inside) host 10.1.2.17
  timeout 2
  key rbrel13Vae2evevb
aaa-server Test_SDI (Outside) host 194.125.246.1
```

Listing 12 Opracowanie własne: Konfiguracja modelu AAA na koncentratorze VPN

aaa-server AD-STRZELEC protocol radius – określa nową grupę serwerów AAA i wskazuje protokół radius
 accounting-mode simultaneous – ustawia tryb accounting dla danej grupy, tak by dane wysyłane były jednocześnie do wszystkich serwerów w tej grupie.
 reactivation-mode timed – określa sposób reaktywacji serwerów Radius, oznaczonych wcześniej jako uszkodzone (ang. *failed*) na 30 sekund.
 max-failed-attempts 3 – określa ilość prób jaka będzie podjęta zanim serwer radius zostanie uznany jako nieosiągalny.

aaa-server AD-STRZELEC (Inside) host 10.9.25.251 do grupy AD-STRZELEC dodany zostaje serwer radius o adresie IP 10.9.25.251 osiągalny poprzez interfejs sieciowy Inside

time out 2 – określa czas, po którym serwer RADIUS oznaczony zostaje jako nieosiągalny

key qweRty13214 – to sekretny klucz użyty przy konfiguracji serwera IAS (Radius). Klucz musi być zgodny, aby możliwa była jakakolwiek komunikacja. Rozróżniane są duże i małe litery.

aaa-server AD-STRZELEC (Inside) host 10.1.2.17 do grupy AD-STRZELEC dodany zostaje serwer RADIUS o adresie IP 10.1.2.17 osiągalny poprzez interfejs sieciowy Inside

time out 2 – określa czas, po którym serwer RADIUS oznaczony zostaje jako nieosiągalny

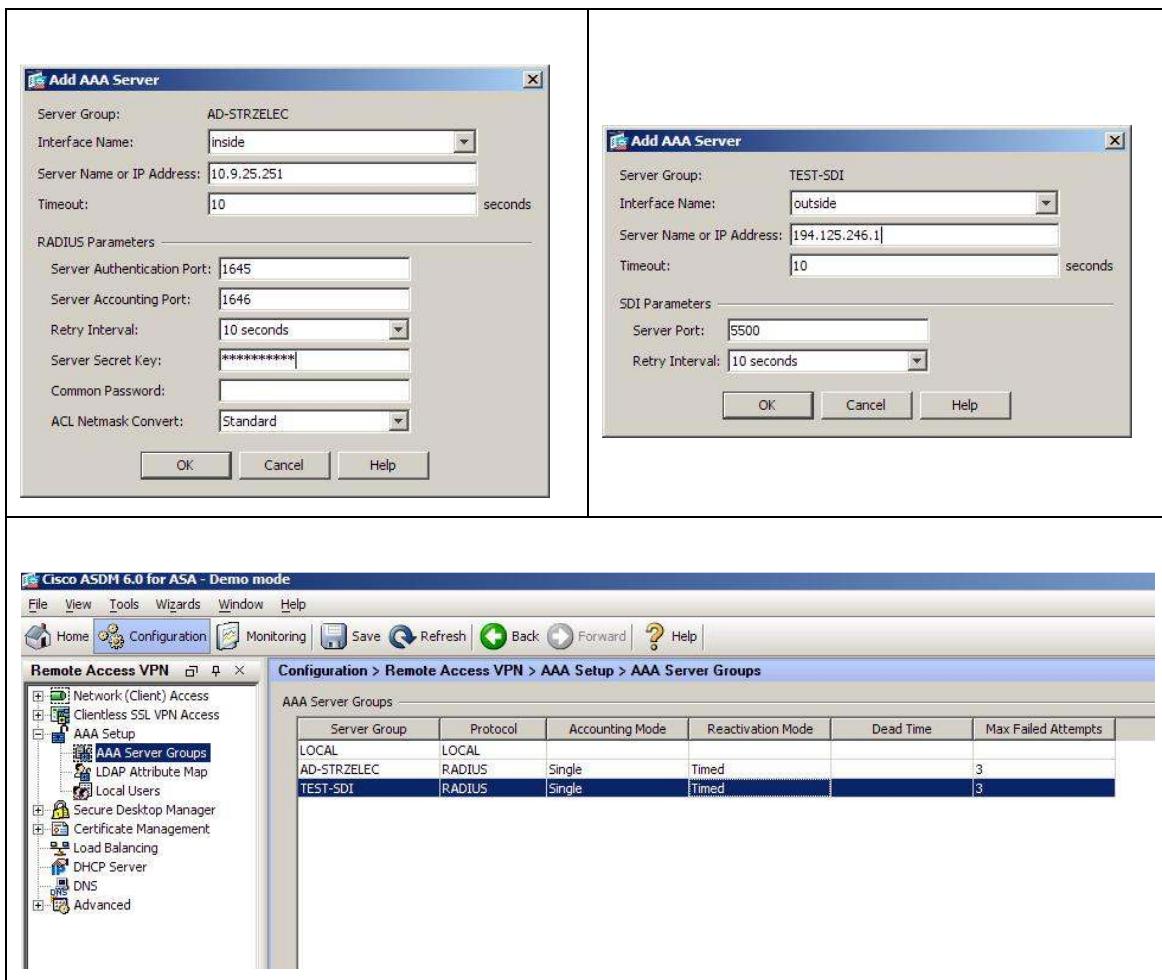
key rbre13Vae2evevb – to sekretny klucz użyty przy konfiguracji serwera IAS (Radius). Klucz musi być zgodny, aby możliwa była jakakolwiek komunikacja. Rozróżniane są duże i małe litery.

aaa-server Test_SDI (Outside) host 194.125.246.1 – określa nową grupę serwerów AAA, wskazuje protokół SDI oraz serwer uwierzytelniający na IP: 194.125.246.1 (zewnętrzna firma: Vistorm, od której wykupiona została usługa SecurID)

Konfiguracja modelu AAA z poziomu aplikacji ASDM w menu:

Configuration > RemoteAccessVPN > AAA/Local Users > AAA Server Groups

| Konfiguracja dla Radius: | Konfiguracja dla SDI (SecurID): |
|--|--|
| A screenshot of the 'Add AAA Server Group' dialog for the Radius protocol. The 'Server Group' field contains 'AD-STRZELEC'. The 'Protocol' dropdown is set to 'RADIUS'. Under 'Accounting Mode', the 'Single' radio button is selected. Under 'Reactivation Mode', the 'Timed' radio button is selected. A 'Dead Timer' input field shows '10' with a 'minutes' unit. A 'Max Failed Attempts' input field shows '3'. At the bottom are 'OK', 'Cancel', and 'Help' buttons. | A screenshot of the 'Add AAA Server Group' dialog for the SecurID protocol. The 'Server Group' field contains 'TEST-SDI'. The 'Protocol' dropdown is set to 'RADIUS'. Under 'Accounting Mode', the 'Single' radio button is selected. Under 'Reactivation Mode', the 'Timed' radio button is selected. A 'Dead Timer' input field shows '10' with a 'minutes' unit. A 'Max Failed Attempts' input field shows '3'. At the bottom are 'OK', 'Cancel', and 'Help' buttons. |



Rysunek 71 Opracowanie własne: Konfiguracja modelu AAA z poziomu aplikacji ASDM

Mając tak przygotowane zestawy grup (AD-STRZELEC, TEST-SDI) dla różnych metod uwierzytelnienia, należy przystąpić do tworzenia profili połączeń.

7.2.11 Profile połączeń

Aby umożliwić telepracownikom korzystanie z metod uwierzytelniania poprzez podanie nazwy użytkownika i hasła z domeny *Active Directory* lub z użyciem jednorazowych haseł generowanych poprzez sprzętowe tokeny RSA, należy zbudować stosowne profile połączeń (ang. *Connection Profiles*). Oprócz domyślnie istniejących na urządzeniu ASA profili:

- DefaultRAGroup
- DefaultWEBVPNGroup

należało zbudować dwa dodatkowe:

- `ipsec_all` (alias `Active_Directory`)

Profil ten definiuje obsługę połączeń VPN kiedy wybraną metodą uwierzytelnienia jest ta poprzez podanie nazwy użytkownika i hasła. Wskazaną grupą serwerów uwierzytelniających (AAA) jest grupa `AD-STRZELEC`.

- `vistorm_rsa` (alias `Token_RSA`)

Profil ten definiuje obsługę połączeń VPN kiedy wybraną metodą uwierzytelnienia jest ta poprzez podanie wskazań sprzętowego tokenu RSA. Wskazaną grupą serwerów uwierzytelniających (AAA) jest grupa `TEST-SDI`.

```
tunnel-group DefaultRAGroup general-attributes
  authentication-server-group AD-strzelec
  password-management
tunnel-group DefaultRAGroup webvpn-attributes
tunnel-group DefaultRAGroup ipsec-attributes
  pre-shared-key Str3l3cki
tunnel-group DefaultRAGroup ppp-attributes
  authentication ms-chap-v2
tunnel-group DefaultWEBVPNGroup general-attributes
  authentication-server-group AD-strzelec
tunnel-group DefaultWEBVPNGroup webvpn-attributes
  customization strzelecCustomization
tunnel-group DefaultWEBVPNGroup ipsec-attributes
  pre-shared-key test
tunnel-group DefaultWEBVPNGroup ppp-attributes
  authentication ms-chap-v2
tunnel-group ipsec_all type remote-access
tunnel-group ipsec_all general-attributes
  authentication-server-group AD-strzelec
tunnel-group ipsec_all webvpn-attributes
  group-alias Active_Directory enable
tunnel-group ipsec_all ipsec-attributes
  pre-shared-key Str3l3cki
tunnel-group vistorm_rsa type remote-access
```

```
tunnel-group vistorm_rsa general-attributes  
authentication-server-group Test_SDI  
default-group-policy vistorm_RSA  
tunnel-group vistorm_rsa webvpn-attributes  
group-alias Token_RSA enable  
tunnel-group vistorm_rsa ipsec-attributes  
pre-shared-key Str3l3cki
```

Listing 13 Opracowanie własne: Tworzenie profili połączeń

tunnel-group DefaultRAroup general-attributes – Definiuje profil połączeń o nazwie DefaultRAroup oraz skojarzone z tym profilem parametry połączenia.

Jako parametr połączenia tunnel-group mogą zostać użyte:

general-attributes – definicja domyślnych połączeń VPN

webvpn-attributes – dla definicji połączeń SSL VPN

ipsec-attributes – dla definicji połączeń VPN IPsec

ppp-attributes – zmiana parametrów i protokołów uwierzytelniania użytkowników np. authentication ms-chap-v2

authentication-server-group AD-strzelec – wskazuje na grupę serwerów uwierzytelniających (AAA) o nazwie AD-strzelec

authentication-server-group Test_SDI – wskazuje na grupę serwerów uwierzytelniających (AAA) o nazwie TEST-SDI.

pre-shared-key Str3l3cki – definiuje sekretną frazę, która później zostanie użyta do konfiguracji oprogramowania na komputerze zdalnego pracownika.

default-group-policy vistorm_RSA – wskazuje domyślną grupę polis na vistorm_RSA.

group-alias Token_RSA enable – definiuje nazwę profilu jaką zobaczą zdalni pracownicy próbujący nawiązać połaczenie VPN. Telepracownicy będą mogli wybrać spośród dwóch opcji: Token_RSA i Active_Directory.

7.2.12 Weryfikacja stacji roboczych zdalnych pracowników

Aby spełnić wymaganie projektowe mówiące o możliwości automatycznej weryfikacji stacji roboczych pracowników zdalnych jeszcze przez podłączeniem do sieci korporacyjnej stosuje się *Cisco Secure Desktop Manager (CSDM)*. Aplikacja ta instaluje się automatycznie z poziomu przeglądarki internetowej (w formie kontrolki ActiveX) w chwili nawiązania połączenia SSL VPN. Odpowiednio konfigurując polisy *SCDM* (ang. *Prelogin Policy*) można sprawdzić bądź zmodyfikować następujące ustawienia stacji roboczej zdalnego pracownika:

- Sprawdzić obecność dowolnego oprogramowania (np. antywirus, firewall, antispyware) i wymusić odpowiednie ich stosowanie,
- Zweryfikować zainstalowany system operacyjny i sprawdzić go pod kątem ostatnich poprawek bezpieczeństwa,
- Sprawdzić/zmodyfikować dowolne klucze rejestru systemu Windows,
- Sprawdzić obecność dowolnych plików na dysku twardy, włącznie ze sprawdzeniem sumy kontrolnej pliku,
- Sprawdzić obecność cyfrowych certyfikatów.

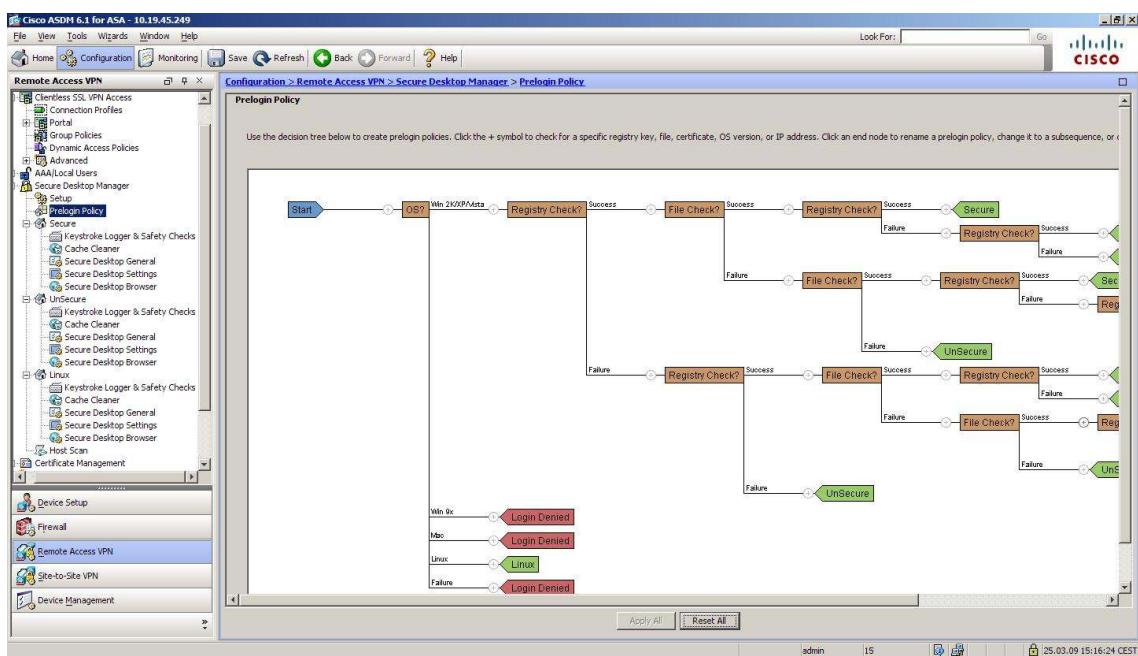
Na podstawie kolejnych kroków sprawdzających polis *CSDM* można odpowiednio traktować połączenia od stacji roboczej zdalnego pracownika. W zależności od tego czy spełnia wszystkie wymagania bezpieczeństwa lub nie, stacji roboczej przyporządkowana jest stosowna etykieta np. *Secure* lub *UnSecure*.

Jeśli stacja robocza otrzyma etykietę *UnSecure* oznacza, że komputer, z którego korzysta użytkownik (np. w kafejce internetowej) nie spełnia wszystkich wymogów polityki bezpieczeństwa, wymusza się stosowanie aplikacji *Cisco Secure Desktop (CSD)*. Aplikacja ta na czas połączenia VPN ma za zadanie wyizolować użytkownikowi systemu operacyjnego nowe wirtualne zasoby (włącznie z nowym pulpitem), które nie mają kontaktu z aktualnie używanymi. Ma to na celu odseparowanie aplikacji już uruchomionych na stacji roboczej od tych, które zostaną uruchomione po nawiązaniu połączenia VPN z firmową siecią lokalną. Aplikacja *CSD* pozwala dodatkowo na:

- Ograniczenie ruchu VPN od zdalnego pracownika tylko dla przeglądarki internetowej,
- Wyłączyć dostęp do dysków lub folderów sieciowych,
- Wyłączyć dostęp do portów USB i/lub urządzeń przenośnych,
- Wyłączyć możliwość modyfikacji rejestru systemu Windows,

- Wyłączyć dostęp do wiersza poleceń,
- Wyłączyć możliwość drukowania,
- Zezwolić na działanie klientów pocztowych (np. Outlook).

Jeśli stacja robocza otrzyma etykietę **Secure** oznacza, że komputer, z którego korzysta użytkownik spełnia wszystkie wymogi polityki bezpieczeństwa, zatem nie ma konieczności stosowania aplikacji CSD dodatkowo zabezpieczającej stację roboczą i połączenie VPN do firmowej sieci lokalnej.



Rysunek 72 Opracowanie własne: aplikacja CSDM, tworzenie polis bezpieczeństwa dla stacji roboczych

Proces sprawdzenia stacji roboczej przebiega następująco:

- 1) W pierwszej kolejności sprawdzany jest system operacyjny zdalnej stacji roboczej. Jeśli rozpoznany został system Windows 2K/XP/Vista/Linux – sprawdzany jest następny etap, jeśli jest inny niż wymienione połączenie VPN jest odrzucone.
- 2) Następny etap to sprawdzenie czy komputer posiada ostatnie poprawki bezpieczeństwa zawierające tzw. *Service Pack 2 lub 3*. Weryfikacja odbywa się poprzez przeszukanie gałęzi rejestru systemu Windows `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SoftwareDistribution\DownloadStatus`.

tVersion\CSDDVersion w poszukiwaniu frazy „Service Pack 2” lub „Service Pack 3”. Jeśli fraza ta zostanie znaleziona, sprawdzony jest następny etap, jeśli nie komputer opatrzony zostaje etykietą UnSecure.

- 3) Kolejnym krokiem jest sprawdzenie czy komputer posiada zainstalowany program antywirusowy firmy McAfee lub F-Secure, poprzez przeszukanie ścieżki „C:\Program Files\McAfee\Common Framework” w poszukiwaniu pliku FrmInst.exe lub „C:\Program Files\F-Secure\common\” w poszukiwaniu pliku ILAUNCHR.EXE. Oprócz obecności plików sprawdzana jest też ich suma kontrolna Checksum In Hex podawana jako liczba heksadecymalna. Jeśli proces weryfikacji programu antywirusowego przebiega pomyślnie, sprawdzany jest następny etap, jeśli nie komputer opatrzony zostaje etykietą UnSecure.
- 4) W kolejnym etapie gałąź rejestru systemu Windows stacji roboczej HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Domain przeszukiwana jest w poszukiwaniu frazy strzelec.local. Jeśli fraza zostanie znaleziona, oznacza to, że komputer jest członkiem domeny Active Directory o nazwie strzelec.local i sprawdzany jest kolejny etap, jeśli nie, opatrzony zostaje etykietą UnSecure i zastosowana zostanie polisa zwiększąca bezpieczeństwo.

Kiedy proces weryfikacji stacji roboczej klienta zostaje zakończony, w zależności od otrzymanej etykiety Secure/UnSecure (polisa SDM), uruchamiana jest aplikacja *Secure Desktop* lub nie.

Po uruchomieniu aplikacji *Secure Desktop* wprowadzane są także dodatkowe zmiany w systemie operacyjnym:

- Wyłączenie możliwości modyfikacji rejestru systemu Windows,
- Wyłączenie dostępu do dysków i folderów sieciowych,
- Wyłączenie dostępu do urządzeń przenośnych,
- Umożliwienie przełączania pomiędzy pulpitem wirtualnym zbudowanym przez CSD a lokalnym,
- Wprowadzony jest tzw. czas bezczynności, ustawiony na 15 minut (ang. *Inactivity Timeout*). Po przekroczeniu w/w czasu, jeśli telepracownik, nie korzysta z połączenia VPN, tunel zostaje automatycznie rozłączony,

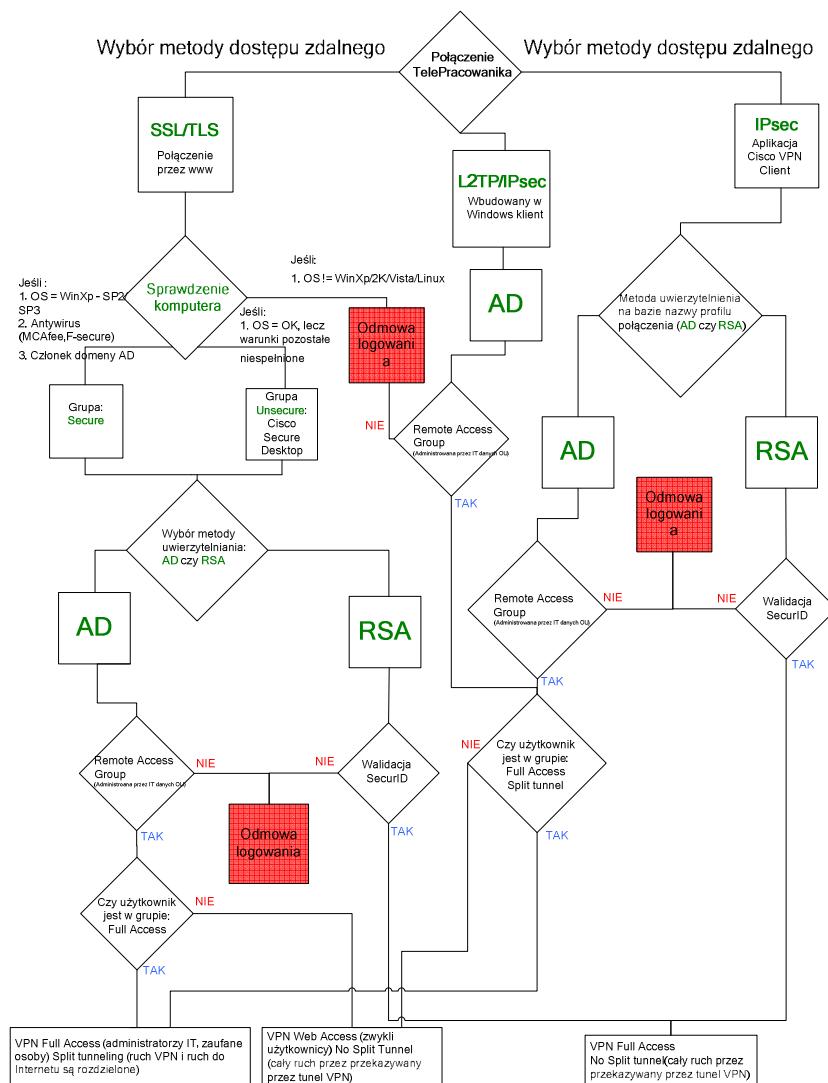
- przypadku rozłączenia połączenia VPN aplikacja *SCD* zostaje automatycznie odinstalowana.

Konfiguracja *Secure Desktop Manager* odbywa się w trybie graficznym z poziomu aplikacji ASDM możliwa jest z menu:

Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy.

7.2.13 Proces obsługi połączeń VPN

Proces nawiązywania połączenia VPN pracownika zdalnego do firmowej sieci lokalnej przebiega zgodnie z drzewem decyzyjnym (rys. 73).



Rysunek 73 Opracowanie własne: Proces obsługi połączeń VPN od użytkowników zdalnych

Zgodnie z wymaganiami projektowymi użytkownicy dostępu zdalnego mają możliwość nawiązania połączenia zdalnego do firmowej sieci lokalnej używając trzech metod dostępu:

- 1 SSL/TLS VPN (poprzez stronę WWW)
 - 2 IPsec (klient Cisco VPN Client)
 - 3 L2TP/IPsec (klient VPN wbudowany w system Windows)
-
- 1.1 Wybrana została metoda SSL/TLS, czyli ustanawianie bezpiecznego połączenia poprzez klienta VPN ładowanego jako kontrolka *ActiveX* z poziomu przeglądarki internetowej.
 - 1.2 Za pomocą aplikacji *Cisco Secure Desktop* (ładowanej automatycznie poprzez kontrolkę ActiveX w przeglądarce) stacja robocza zostaje zweryfikowana pod kątem obecnego systemu operacyjnego, poprawek *Service Pack 2/3*, programu antywirusowego oraz przynależności do domeny AD. Jeśli nie spełnia chociaż jednego z w/w wymagań wymuszone jest stosowanie dodatkowych zabezpieczeń (poprzez CSD). Jeśli wszystkie wymagania zostały spełnione CSD nie jest wymuszane.
 - 1.3 Kolejnym etapem jest wybór metody uwierzytelniania. Użytkownik z poziomu strony internetowej z listy rozwijalnej ma do wyboru dwa profile:
 - Active_Directory
 - Token_RSA



The screenshot shows a login interface. At the top is a dark blue header bar with the word "Login" in white. Below it is a light gray content area. In the center, the text "Please enter your username and password." is displayed. There are three input fields: "USERNAME" with an empty text box, "PASSWORD" with an empty text box, and "GROUP" with a dropdown menu showing "Active_Directory". At the bottom is a large, rounded rectangular button labeled "Login".

Rysunek 74 Opracowanie własne: Wybór metody uwierzytelniania dla dostępu poprzez VPN SSL/TLS

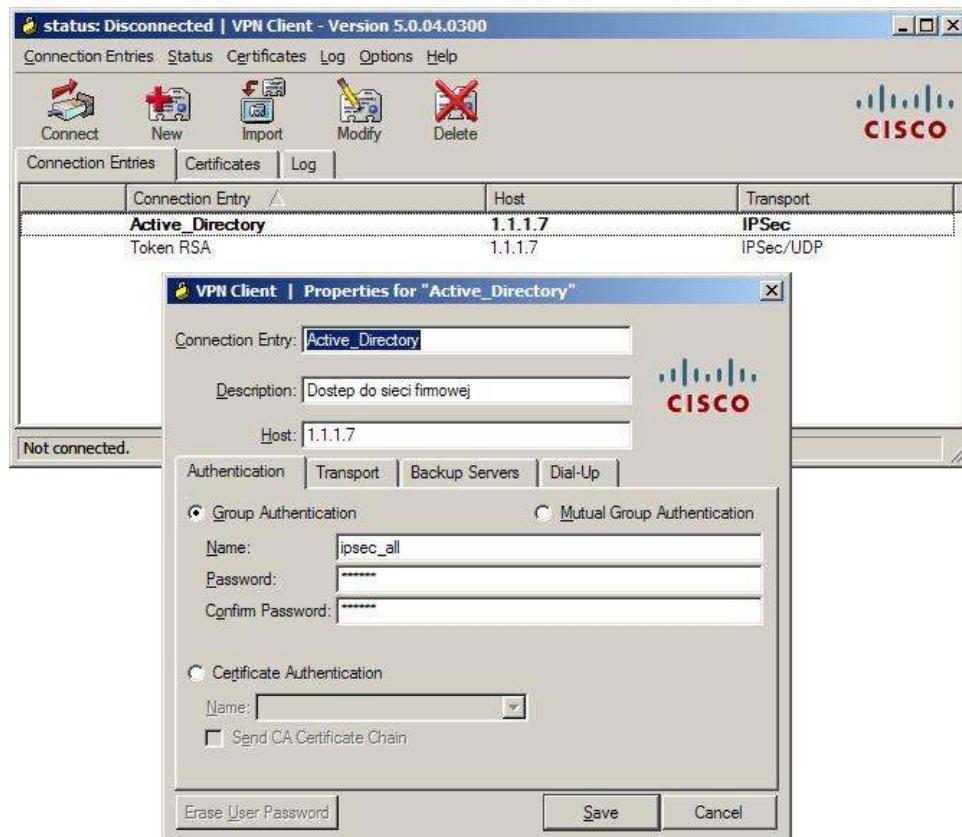
- 1.4 Jeśli wybrany został profil Active_Directory oraz uzupełnione zostały pola USERNAME (nazwa użytkownika) i PASSWORD (hasło użytkownika), następuje weryfikacja ich poprawności. Zapytanie (dane użytkownika) wysyłane są z urządzenia ASA do serwera RADIUS, umieszczonego wewnętrz firmowej sieci lokalnej. Serwer RADIUS weryfikuje czy dany użytkownik ma prawo nawiązać połączenie VPN, czyli czy przynależy do stosownej grupy w domenie.
- 1.5 Jeśli użytkownik nie przynależy do grupy AD:
- STRZELEC\XY_GS_GRP_Remote_ACCESS
- użytkownik nie uzyska dostępu do firmowej sieci lokalnej.
- Jeśli należy to dodatkowo sprawdzana jest przynależność do grupy:
- STRZELEC\GLOB_GS_GRP_Remote_ACCESS FULL
- Obecność użytkownika tylko w pierwszej grupie zagwarantuje mu dostęp ograniczony listą dostępu (ACL) WEB_ACCESS oraz *no split-tunneling* (ze względów bezpieczeństwa cały ruch od stacji roboczej przechodzi przez tunel VPN i tam jest filtrowany). Obecność w obu grupach na raz zapewni nieograniczony dostęp do firmowej sieci lokalnej (ACL: FULL_ACCESS) oraz *split-tunneling* (ruch do sieci VPN i do Internetu są rozdzielone).
- 1.6 Jeśli wybrany został profil Token_RSA (rys.75) oraz uzupełnione zostały pola USERNAME (nazwa użytkownika) i PASSCODE (hasło użytkownika + aktualne wskazanie Tokenu), następuje weryfikacja ich poprawności. Zapytanie (dane od użytkownika i wskazanie tokenu) wysyłane są z urządzenia ASA do serwera SDI stojącego w firmie zewnętrznej (Vistorm). Serwer SDI sprawdza poprawność aktualnej kombinacji nazwy użytkownika oraz pola PASSCODE zawierającej hasło użytkownika i aktualne wskazanie Tokenu o danym numerze seryjnym. Jeśli podane informacje są zgodne z przechowywanymi na serwerze SDI (aktualne pole PASSCODE wyliczone przez serwer na podstawie numeru seryjnego Tokenu zdalnego użytkownika) serwer SDI zwraca informacje do urządzenia ASA o pozytywnej weryfikacji.

Użytkownik otrzymuje adres IP z puli o nazwie VISTORM_RSA, zastosowana jest lista kontroli dostępu ACL_VISTORM_RSA oraz wymuszony zostaje no split tunneling.



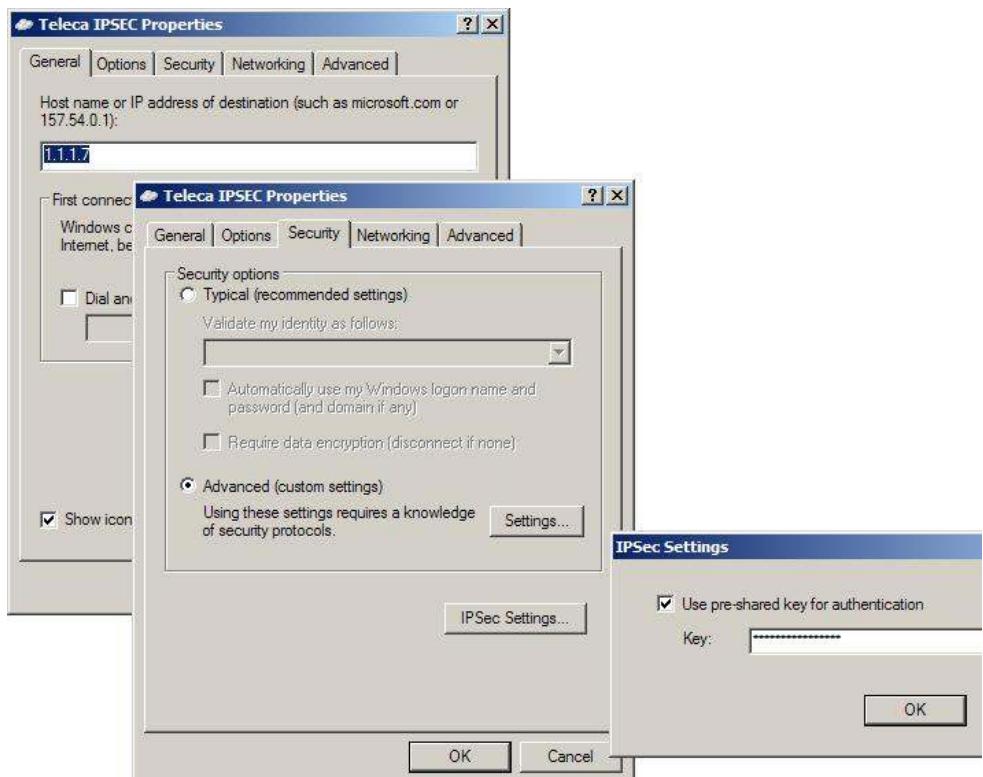
Rysunek 75 Opracowanie własne: Uwierzytelnianie TokenRSA

- 2.1 Wybrana została metoda IPsec, czyli ustanowienia bezpiecznego połączenia poprzez aplikację Cisco VPN Client (rys.75)



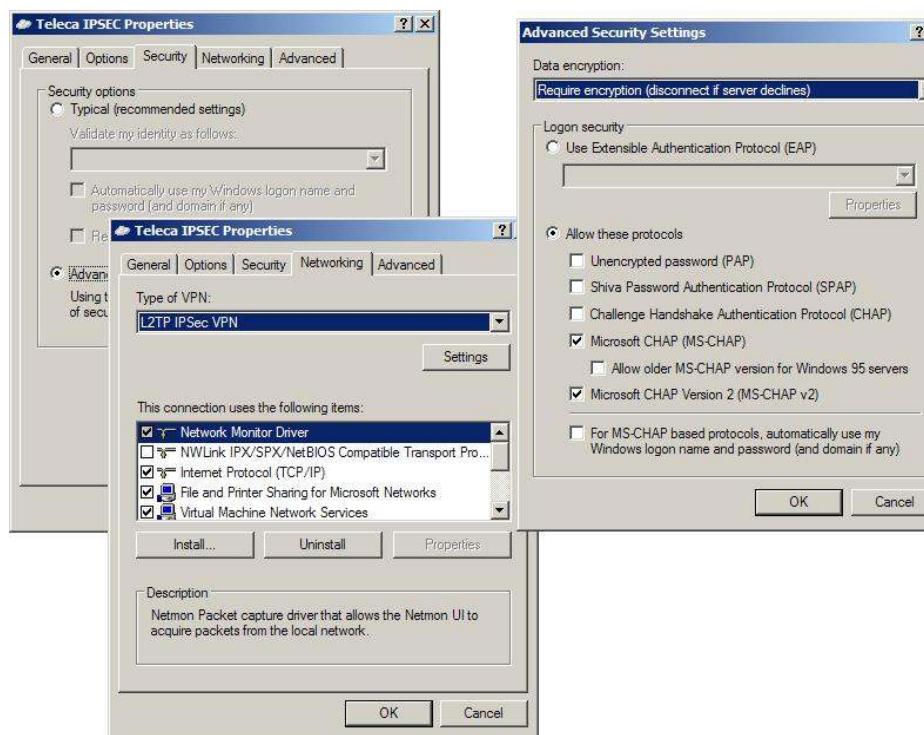
Rysunek 76 Opracowanie własne: Aplikacji Cisco VPN Client

- 2.2 Użytkownik może wybrać odpowiednio skonfigurowany jeden z dwóch profili połączeń dla metod uwierzytelnienia Active_Directory lub Token_RSA, przy czym w odróżnieniu od metody SSL/TLS, w konfiguracji aplikacji Cisco VPN Client koniecznym jest podanie tajnego klucza, hasła (*Pre-Shared Key*, lub *Password*) skonfigurowanego wcześniej w urządzeniu ASA podczas tworzenia profili połączeń IPsec. W zależności od wybranego profilu podjęte zostają analogiczne działania przez serwer RADIUS/SDI oraz urządzenie ASA jakie miały miejsce w punktach od 1.3 do 1.6 aktualnego rozdziału.
- 3.1 Wybrana została metoda L2TP/IPsec, czyli ustanowienia bezpiecznego połączenia VPN poprzez aplikację wbudowaną w systemy Windows (rys.77). Metoda ta dotyczy tylko pracowników firmy posiadających uprawnienia w domenie AD.



Rysunek 77 Opracowanie własne: Klient L2TP/IPsec

Podobnie jak przy konfiguracji klienta IPsec koniecznym jest podanie sekretnej frazy, takiej samej jaka została użyta w konfiguracji profilu połączenia L2TP w urządzeniu ASA.



Rysunek 78 Opracowanie własne: Klient L2TP/IPsec protokoły uwierzytelniające

Dodatkowo w konfiguracji należy wybrać protokoły uwierzytelniania użytkownika MS-CHAP i MS-CHAP v2.



Rysunek 79 Opracowanie własne: Połączenie przez klienta L2TP

3.2 Proces łączenia polega na uruchomieniu wcześniej skonfigurowanego połączenia L2TP, podaniu nazwy użytkownika i hasła, po czym następuje weryfikacja ich poprawności. Zapytanie (dane użytkownika) wysyłane są od użytkownika do urządzenia *ASA* a następnie od ASA do serwera RADIUS, umieszczonego wewnątrz firmowej sieci lokalnej. Serwer RADIUS weryfikuje czy dany użytkownik ma prawo nawiązać połączenie VPN, czyli czy przynależy do stosownej grupy w domenie.

Jeśli użytkownik nie przynależy do grupy AD:

STRZELEC\XY_GS_GRP_Remote_ACCESS

użytkownik nie uzyska dostępu do firmowej sieci lokalnej.

Jeśli należy to dodatkowo sprawdzana jest przynależność do grupy:

STRZELEC\GLOB_GS_GRP_Remote_ACCESS FULL

Obecność użytkownika tylko w pierwszej grupie zagwarantuje mu dostęp ograniczony listą dostępu (ACL) WEB_ACCESS oraz *no split-tunneling* (ze względów bezpieczeństwa cały ruch od stacji roboczej przechodzi przez tunel VPN i tam jest filtrowany). Obecność w obu grupach na raz zapewni nieograniczony dostęp do firmowej sieci lokalnej (ACL: FULL_ACCESS) oraz *split-tunneling* (ruch do sieci VPN i do Internetu są rozdzielone).

Stacja robocza otrzyma adres IP z puli zależnej od grupy AD, do której należy użytkownik.

7.3 Testy akceptacyjne

Aby zweryfikować poprawność konfiguracji urządzeń ASA, serwerów uwierzytelniających i ich implementacji w istniejącej sieci, wykonano test polegający na próbie nawiązania połączenia VPN trzema dostępymi metodami:

- ✓ IPsec (Za pomocą klienta Cisco VPN instalowanego na stacji roboczej),
- ✓ SSL VPN (Automatyczna instalacja klienta VPN po otwarciu strony internetowej),
- ✓ L2TP/IPsec (za pomocą wbudowanego klienta vpn w systemy Windows XP/2000/Vista).

Koniecznymi warunkami powodzenia testów są:

- a) Pozytywne uwierzytelnienie za pomocą metod:
 - nazwa użytkownika i hasło,
 - z użyciem jednorazowych haseł generowanych przez TokenRSA.
- b) Otrzymanie adresu IP ze stosownej puli (w zależności od przynależności do grupy Active Directory lub w przypadku metody OTP, puli odrębnej)
- c) Możliwości nawiązania połączenia do wybranych serwerów wewnętrz sieci lokalnej za pomocą komend systemowych (*ping* i *telnet*)

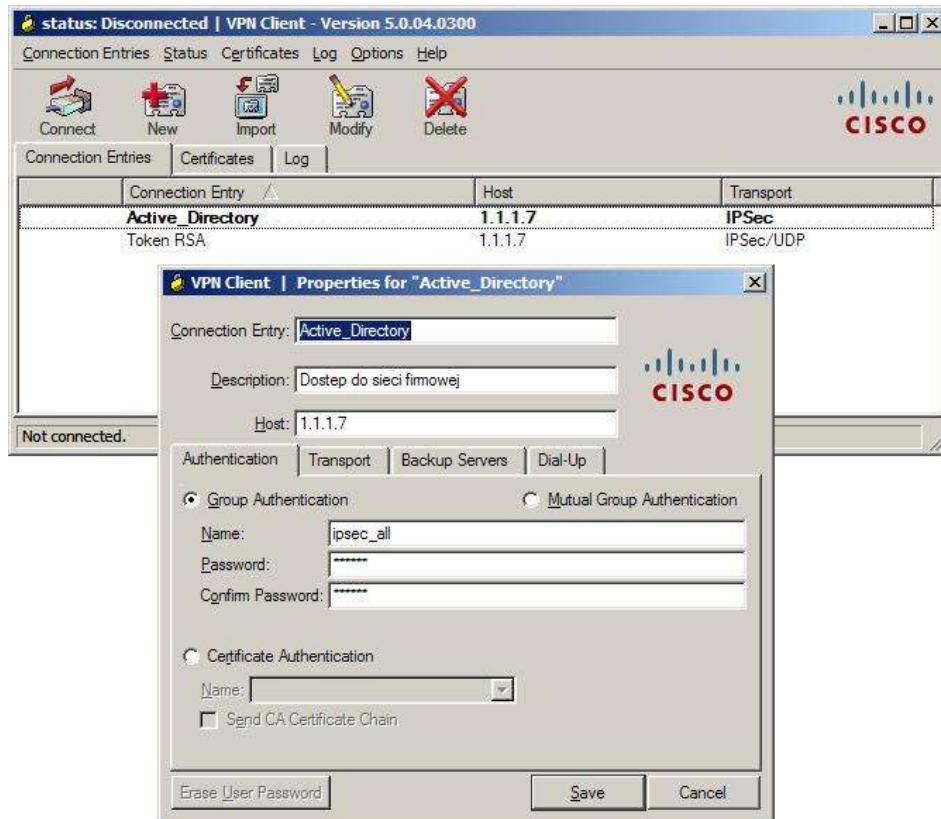
7.3.1 Połączenie VPN z użyciem IPsec

Jako pierwszy test wykonano próbę połączenia VPN poprzez aplikację Cisco VPN Client (IPsec). Konfiguracja programu (rozdział 7.3.1) wymagała zbudowania dwóch profili połączeń VPN (rys.80) :

- 1) Dla metody uwierzytelnienia poprzez podanie nazwy użytkownika i hasła (nazwa profilu połączenia Active_Directory)
- 2) Dla metody uwierzytelniania poprzez podanie jednorazowych haseł (nazwa profilu połączenia Token RSA)

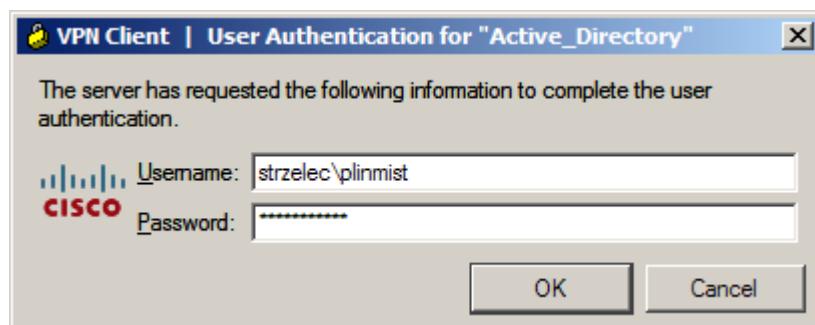
W przypadku obu profili połączeń jako grupa uwierzytelniania (ang. *Group Authentication*) została wybrana opcja: Group Authentication. Nazwa grupy dla profilu Active_Directory powinna być zgodna z konfiguracją urządzenia ASA: `ipsec_all`, zaś nazwą grupy dla profilu połączenia Token RSA powinna być `vistorm_rsa`.

W polu Host podany został publiczny adres IP interfejsu łączącego urządzenie ASA z siecią Internet.



Rysunek 80 Opracowanie własne: konfiguracja aplikacji Cisco VPN Client

Mając skonfigurowany profil połączenia Active_Directory, można rozpocząć inicjację połączenia (przycisk Connect) VPN do firmowej sieci lokalnej (Rys 80). Na rys. 81 widać okno aplikacji Cisco VPN Client, gdzie podano nazwę użytkownika oraz hasło z domeny Active Directory.



Rysunek 81 Opracowanie własne: Uwierzytelnienia użytkownika przy użyciu aplikacji Cisco VPN Client

Użytkownik plinmistr jest członkiem grupy domenowej:

STRZELEC\PL_GS_GRP_Remote_ACCESS (dla grupy użytkowników z Polski w ograniczonym dostępu, lista kontroli dostępu WEB_ACCESS), po podłączeniu do

firmowej sieci lokalnej otrzyma adres IP z puli: Poland_WEB_Access (zakres IP 10.19.0.130-10.19.0.190).

| Nazwa puli IP | Zakres adresów IP | Maska podsieci |
|--------------------|-------------------------|-----------------|
| Poland_WEB_Access | 10.19.0.130-10.19.0.190 | 255.255.255.192 |
| Poland_FULL_Access | 10.19.0.194-10.19.0.254 | 255.255.255.192 |

Konfiguracja karty sieciowej, po ustanowieniu połączenia VPN przedstawiona jest na (rys. 82)

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter <9691BE98-A8F3-4EB7-B53E-0D27886CAA89>:
      Media State . . . . . : Media disconnected

Ethernet adapter <C573B78A-F56C-4AB6-B957-7341253DPC02>:
      Media State . . . . . : Media disconnected

Ethernet adapter Local Area Connection:
      Connection-specific DNS Suffix . : global
      IP Address . . . . . : 10.220.3.17
      Subnet Mask . . . . . : 255.255.252.0
      Default Gateway . . . . . :

Ethernet adapter Local Area Connection 7:
      Connection-specific DNS Suffix . : strzelec.local
      IP Address . . . . . : 10.19.0.189
      Subnet Mask . . . . . : 255.255.255.192
      Default Gateway . . . . . : 10.19.0.189

C:\>
```

Rysunek 82 Opracowanie własne: Konfiguracja stosu TCP/IP po nawiązaniu połączenia VPN (WEB_ACCESS)

Dla połączeń od tego użytkownika zastosowana została lista kontroli dostępu o nazwie WEB_ACCESS (dostęp ograniczony), oraz no split tunneling, czyli cały ruch sieciowy (nawet do Internetu) od tej stacji roboczej przekazywany będzie do urządzenia ASA i tam poddawany inspekcji. Tablica routingu przedstawiona jest na rysunku 83. Pozycja Default Gateway prezentuje domyślną bramę sieciową, która jest adresem IP tunelu VPN.

```

C:\> C:\WINNT\system32\cmd.exe
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface       Metric
          0.0.0.0          0.0.0.0        10.19.0.189   10.19.0.189    1
        10.19.0.128    255.255.255.192  10.19.0.189   10.19.0.189    20
        10.19.0.189    255.255.255.255     127.0.0.1    127.0.0.1     20
        10.220.0.0      255.255.252.0    10.220.3.17   10.220.3.17    20
        10.220.1.10     255.255.255.255  10.220.3.17   10.220.3.17    1
        10.220.3.17     255.255.255.255     127.0.0.1    127.0.0.1     20
        10.255.255.255  255.255.255.255  10.19.0.189   10.19.0.189    20
        10.255.255.255  255.255.255.255  10.220.3.17   10.220.3.17    20
        127.0.0.0        255.0.0.0        127.0.0.1    127.0.0.1     1
        1.1.1.7         255.255.255.255  10.220.1.1    10.220.3.17    1
        224.0.0.0        240.0.0.0        10.19.0.189   10.19.0.189    20
        224.0.0.0        240.0.0.0        10.220.3.17   10.220.3.17    20
      255.255.255.255  255.255.255.255  10.19.0.189   10.19.0.189    1
      255.255.255.255  255.255.255.255  10.220.3.17   10.220.3.17    5
      255.255.255.255  255.255.255.255  10.220.3.17   10.220.3.17    1
      255.255.255.255  255.255.255.255  10.220.3.17   10.220.3.17    4
Default Gateway: 10.19.0.189
=====
Persistent Routes:
  None
C:\>

```

Rysunek 83 Opracowanie własne: Konfiguracja tablicy routingu po nawiązaniu połączenia VPN
(no Split tunneling, ACL: WEB_ACCESS)

Użytkownik plimnist2 jest członkiem grup domenowych:

STRZELEC\PL_GS_GRP_Remote_ACCESS

STRZELEC\GLOB_GS_GRP_Remote_ACCESS FULL

(dla grupy użytkowników z Polski z pełnym dostępem, lista kontroli dostępu FULL_ACCESS), po podłączeniu do firmowej sieci lokalnej otrzyma adres IP z puli: Poland_FULL_Access (zakres IP 10.19.0.194-10.19.0.254).

| Nazwa puli IP | Zakres adresów IP | Maska podsieci |
|--------------------|-------------------------|-----------------|
| Poland_WEB_Access | 10.19.0.130-10.19.0.190 | 255.255.255.192 |
| Poland_FULL_Access | 10.19.0.194-10.19.0.254 | 255.255.255.192 |

Konfiguracja karty sieciowej, po ustanowieniu połączenia VPN przedstawiona jest na (rys. 84)

```

C:\>ipconfig

Windows IP Configuration

Ethernet adapter <9691BE98-ABF3-4EB7-B53E-0D27886CA89>:
    Media State . . . . . : Media disconnected

Ethernet adapter <C573B78A-F56C-4A86-8957-7341253DFC02>:
    Media State . . . . . : Media disconnected

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . . . : global
    IP Address . . . . . : 10.220.3.17
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . : 10.220.1.1

Ethernet adapter Local Area Connection 7:
    Connection-specific DNS Suffix . . . . . : strzelec.local
    IP Address . . . . . : 10.19.0.253
    Subnet Mask . . . . . : 255.255.255.192
    Default Gateway . . . . . :

```

Rysunek 84 Opracowanie własne: Konfiguracja stosu TCP/IP po nawiązaniu połączenia VPN (FULL_ACCESS)

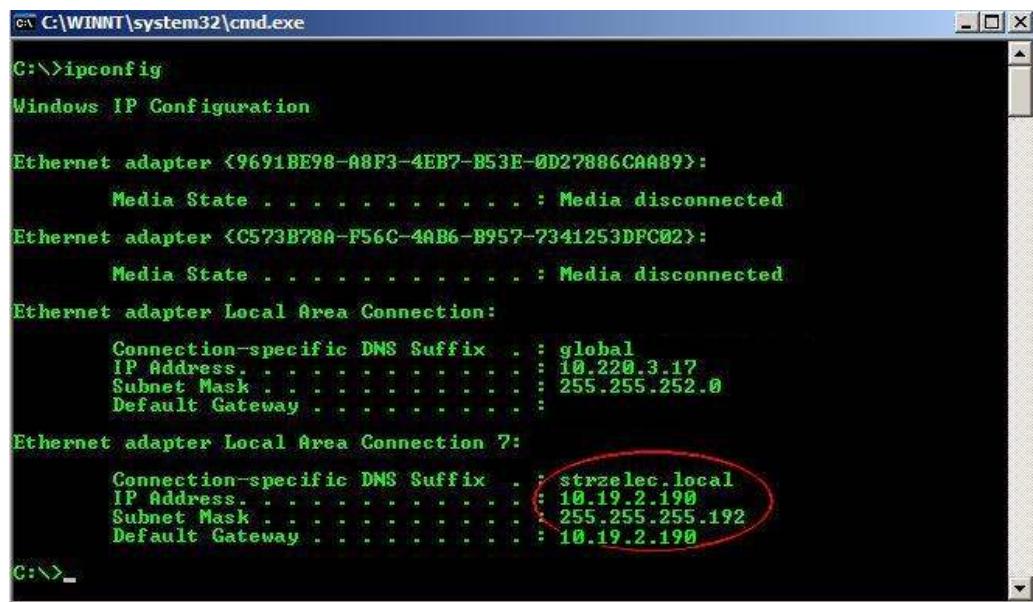
Dla połączeń od tego użytkownika zastosowana została lista kontroli dostępu o nazwie FULL_ACCESS (dostęp bez ograniczeń), oraz split tunneling, czyli ruch sieciowy do Internetu wysyłany jest przez bramę domyślną, zaś ruch do sieci 10.0.0.0/8 od tej stacji roboczej przekazywany będzie do urządzenia ASA i tam poddawany inspekcji. Tablica routingu przedstawiona jest na rysunku 85. Pozycja Default Gateway prezentuje domyślną bramę sieciową, która jest adresem IP dostawcy Internetu.

| Network | Destination | Netmask | Gateway | Interface | Metric |
|-------------------------|-------------------|-------------|-------------|-----------|--------|
| 0.0.0.0 | 0.0.0.0 | 10.220.1.1 | 10.220.3.17 | 20 | |
| 10.19.0.0 | 255.0.0.0 | 10.19.0.253 | 10.19.0.253 | 1 | |
| 10.19.0.192 | 255.255.255.192 | 10.19.0.253 | 10.19.0.253 | 20 | |
| 10.19.0.253 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 20 | |
| 10.220.0.0 | 255.255.252.0 | 10.220.3.17 | 10.220.3.17 | 20 | |
| 10.220.1.10 | 255.255.255.255 | 10.220.3.17 | 10.220.3.17 | 1 | |
| 10.220.3.17 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 20 | |
| 10.255.255.255 | 255.255.255.255 | 10.19.0.253 | 10.19.0.253 | 20 | |
| 10.255.255.255 | 255.255.255.255 | 10.220.3.17 | 10.220.3.17 | 20 | |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 | |
| 1.1.1.7 | 255.255.255.255 | 10.220.1.1 | 10.220.3.17 | 1 | |
| 224.0.0.0 | 240.0.0.0 | 10.19.0.253 | 10.19.0.253 | 20 | |
| 224.0.0.0 | 240.0.0.0 | 10.220.3.17 | 10.220.3.17 | 20 | |
| 255.255.255.255 | 255.255.255.255 | 10.19.0.253 | | 4 | |
| 255.255.255.255 | 255.255.255.255 | 10.19.0.253 | | 5 | |
| 255.255.255.255 | 255.255.255.255 | 10.19.0.253 | 10.19.0.253 | 1 | |
| 255.255.255.255 | 255.255.255.255 | 10.220.3.17 | 10.220.3.17 | 1 | |
| Default Gateway: | 10.220.1.1 | | | | |

Rysunek 85 Opracowanie własne: Konfiguracja tablicy routingu po nawiązaniu połączenia VPN (split tunneling, ACL: FULL_ACCESS)

Użytkownik tel1strzeleckim korzystający z usługi TokenRSA, po pozytywnym uwierzytelnieniu i uzyskaniu połączenia otrzymał adres IP z puli: Vistorm_RSA (zakres IP 10.19.2.130-10.19.0.190).

| Nazwa puli IP | Zakres adresów IP | Maska podsieci |
|---------------|-------------------------|-----------------|
| VISTORM_RSA | 10.19.2.130-10.19.2.190 | 255.255.255.192 |



```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter <9691BE98-A8F3-4EB7-B53E-0D27886CAA89>:
    Media State . . . . . : Media disconnected

Ethernet adapter <C573B78A-F56C-4AB6-B957-7341253DFC02>:
    Media State . . . . . : Media disconnected

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . . . : global
    IP Address . . . . . : 10.220.3.17
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . :

Ethernet adapter Local Area Connection 7:
    Connection-specific DNS Suffix . . . . . : strzelec.local
    IP Address . . . . . : 10.19.2.190
    Subnet Mask . . . . . : 255.255.255.192
    Default Gateway . . . . . : 10.19.2.190

C:\>
```

Rysunek 86 Opracowanie własne: Konfiguracja stosu TCP/IP po nawiązaniu połączenia VPN (VISTORM_RSA)

Dla połączeń od użytkownika tel1strzeleckim zastosowana została lista kontroli dostępu o nazwie FULL_ACCESS (dostęp bez ograniczeń), oraz no split tunneling, czyli cały ruch sieciowy (nawet do Internetu) od tej stacji roboczej przekazywany będzie do urządzenia ASA i tam poddawany inspekcji. W Tablicy routingu (rys. 87) przedstawiona jest pozycja Default Gateway, prezentująca domyślną bramę sieciową, która jest adresem IP tunelu VPN.

```

C:\> C:\WINNT\system32\cmd.exe
=====
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface       Metric
          0.0.0.0          0.0.0.0        10.19.2.190    10.19.2.190      1
        10.19.2.128    255.255.255.192   10.19.2.190    10.19.2.190     20
        10.19.2.190    255.255.255.255   127.0.0.1     127.0.0.1      20
        10.220.0.0      255.255.252.0    10.220.3.17   10.220.3.17     20
        10.220.1.10     255.255.255.255   10.220.3.17   10.220.3.17      1
        10.220.3.17     255.255.255.255   127.0.0.1     127.0.0.1      20
      10.255.255.255    255.255.255.255   10.19.2.190    10.19.2.190      20
      10.255.255.255    255.255.255.255   10.220.3.17   10.220.3.17     20
        127.0.0.0        255.0.0.0        127.0.0.1     127.0.0.1      1
        1.1.1.7         255.255.255.255   10.220.1.1     10.220.3.17      1
      224.0.0.0         240.0.0.0        10.19.2.190    10.19.2.190      20
      224.0.0.0         240.0.0.0        10.220.3.17   10.220.3.17     20
    255.255.255.255    255.255.255.255   10.19.2.190    10.19.2.190      1
    255.255.255.255    255.255.255.255   10.220.3.17   10.220.3.17      5
    255.255.255.255    255.255.255.255   10.220.3.17   10.220.3.17      1
    255.255.255.255    255.255.255.255   10.220.3.17   10.220.3.17     4
Default Gateway: 10.19.2.190
=====
Persistent Routes:
  None
C:\>

```

Rysunek 87 Opracowanie własne: Konfiguracja tablicy routingu po nawiązaniu połączenia VPN
(no split tunneling, ACL: FULL_ACCESS)

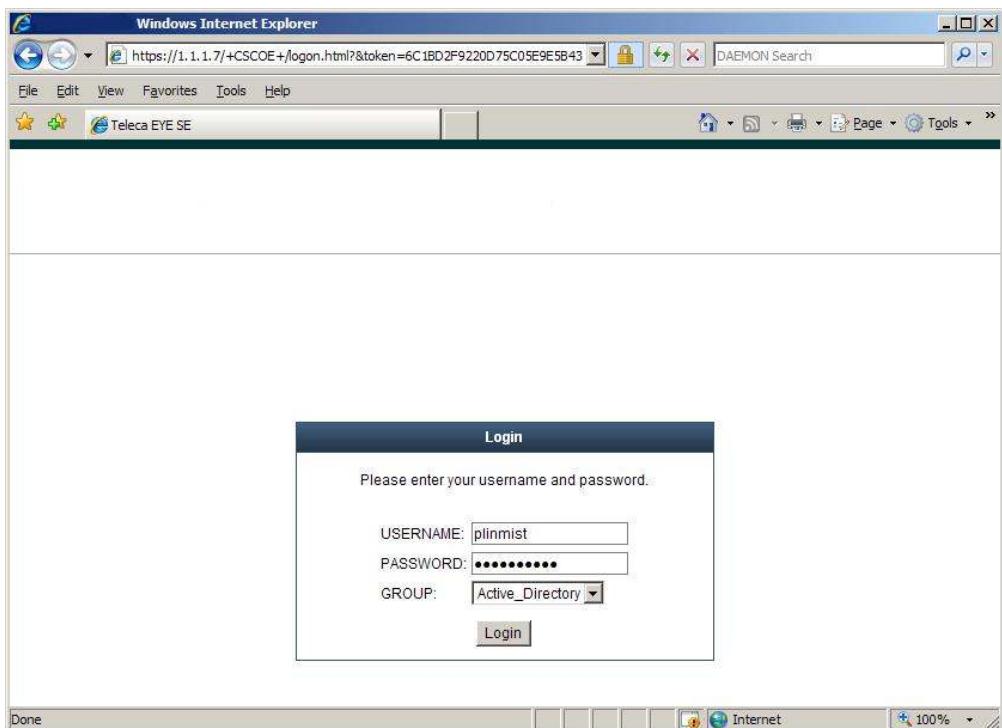
| Lp. | Metoda dostępu IPsec (Cisco VPN Client, ACL: WEB_ACCESS, FULL_ACCESS, VISTORM_RSA) | Status |
|-----|--|-----------|
| 1 | <p>Weryfikacja osiągalności serwerów wewnętrz sieci poprzez polecenie ping z komputera pracownika zdalnego</p> <p>icmp (echo-request):</p> <ul style="list-style-type: none"> • Serwery Aplikacji • Kontrolery domeny • Serwery VOIP • Serwery Poczty • Serwery OCS • Wszystkie pozostałe serwery z sieci lokalnej były osiągalne tylko dla ACL: FULL_ACCESS | Pozytywny |
| 2 | <p>Weryfikacja osiągalności usług sieciowych wewnętrz sieci z użyciem polecenia telnet (na określony) numer portu TCP z komputera pracownika zdalnego dla usług:</p> <ul style="list-style-type: none"> • http/tcp/80 • https/tcp/443 • tcp/445 • RDP/tcp/3389 • ssh/tcp/22 | Pozytywny |

| | | |
|---|---|-----------|
| | <ul style="list-style-type: none"> • ldap/tcp/389 • Wszystkie pozostałe porty osiągalne tylko dla ACL: FULL_ACCESS | |
| 3 | <p>Weryfikacja poprawności konfiguracji IKE poprzez polecenie show crypto isakmp SA na urządzeniu ASA:</p> <pre>ASA1# sh crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 83.88.196.164 Type: user Role :responder Rekey: no State :AM_ACTIVE</pre> | Pozytywny |
| 4 | <p>Weryfikacja poprawności konfiguracji protokołu IPsec poprzez polecenie sh crypto ipsec sa summary lub sh crypto ipsec sa na urządzeniu ASA:</p> <pre>ASA1# sh crypto ipsec sa summary Current IPsec SA's:1 Peak IPsec SA's: IPSec :1 Peak Concurrent SA:4 IPSec over UDP:0 Peak Concurrent L2L:0 IPSec over NAT-T:2 Peak Concurrent RA:-1 IPSec over TCP :0 IPSec VPN LB :0 Total :3 ASA1# sh crypto ipsec sa</pre> | Pozytywny |

| | | |
|--|--|--|
| | <pre>Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: Outside_Interface local ident (addr/mask/prot/port): (Outside_Interface/255.255.255.255/17/1701) remote ident (addr/mask/prot/port): (194.63.135.6/255.255.255.255/17/0) current_peer: 194.63.135.6, username: global\plinmist dynamic allocated peer ip: 10.19.0.194 #pkts encaps: 937, #pkts encrypt: 937, #pkts digest: 937 #pkts decaps: 560, #pkts decrypt: 560, #pkts verify: 560 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 952, #pkts comp failed: 0, #pkts decomp failed: 0 #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 14 local crypto endpt.: Outside_Interface/4500, remote crypto endpt.: 194.63.135.6/4500 path mtu 1500, ipsec overhead 66, media mtu 1500 current outbound spi: 2F494F5D inbound esp sas: spi: 0x50FF3E87 (1358904967) transform: esp-3des esp-sha-hmac no compression in use settings =(RA, Transport, NAT-T-Encaps,) slot: 0, conn_id: 3674112, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (kB/sec): (237244/3492) IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0xFFFFFFFF 0xFFFFFFFF outbound esp sas: spi: 0x2F494F5D (793333597) transform: esp-3des esp-sha-hmac no compression in use settings =(RA, Transport, NAT-T-Encaps,) slot: 0, conn_id: 3674112, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (kB/sec): (237161/3486) IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0x00000000 0x00000001</pre> | |
|--|--|--|

7.3.2 Połączenie VPN z użyciem SSL/TLS

Jako drugi zestaw testów wykonano próbę połączenia VPN do korporacyjnej sieci lokalnej za pośrednictwem automatycznie ładowanej aplikacji Cisco Any Connect z poziomu przeglądarki internetowej. Zestawienie połączenia VPN nie wymaga żadnych konfiguracji na stacji roboczej, jedynie otwarcia strony WWW oraz wybrania odpowiedniej metody uwierzytelniania (rys. 88)

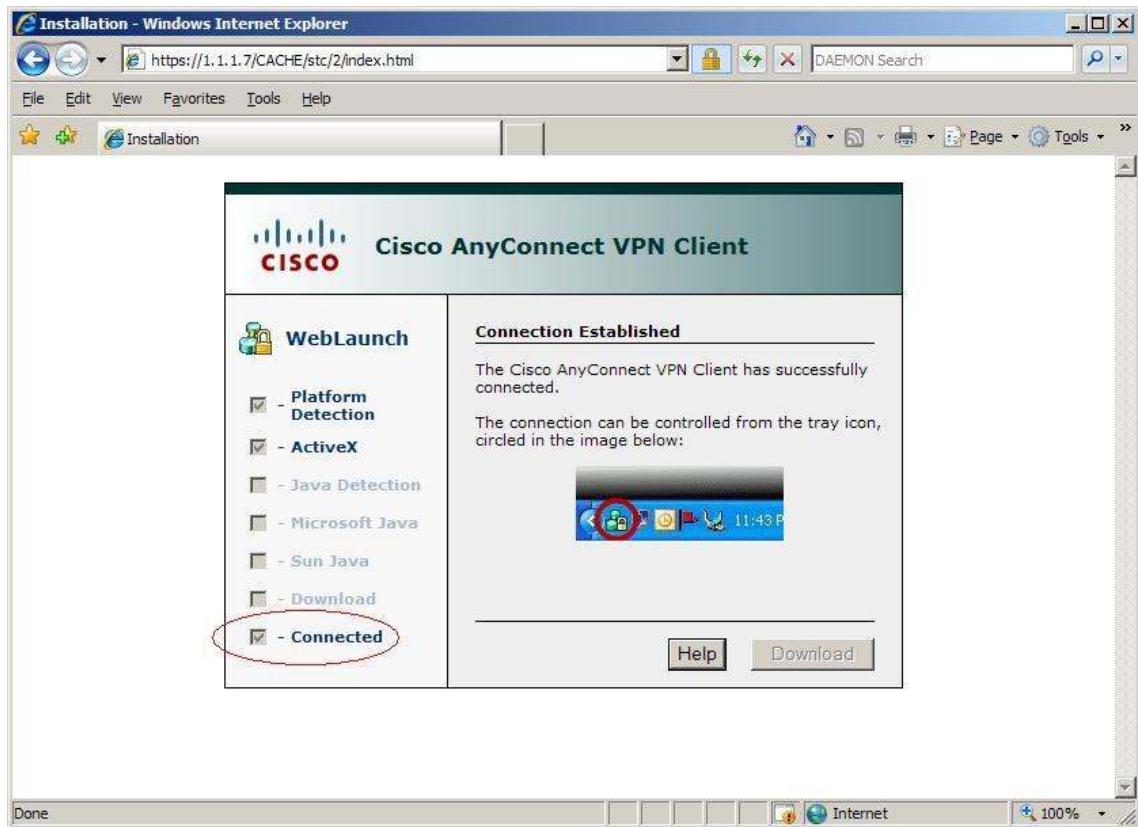


Rysunek 88 Opracowanie własne: metoda dostępu SSL/TLS

- 1) Dla metody uwierzytelnienia poprzez podanie nazwy użytkownika i hasła (należy z rozwijalne listy nazwanej jako Group należy wybrać Active_Directory)
- 2) Dla metody uwierzytelniania poprzez podanie jednorazowych haseł (z listy Group należy wybrać Token_RSA)

W zależności od tego czy stacja robocza spełnia wymagania bezpieczeństwa, czy też nie, załadowana zostanie aplikacja CSD (rozdział 7.2.13: Proces obsługi połączeń VPN).

Ustanowione połączenie VPN sygnalizowane jest na stronie WWW samoistnym zaznaczeniem pozycji Connected (Rys. 89)



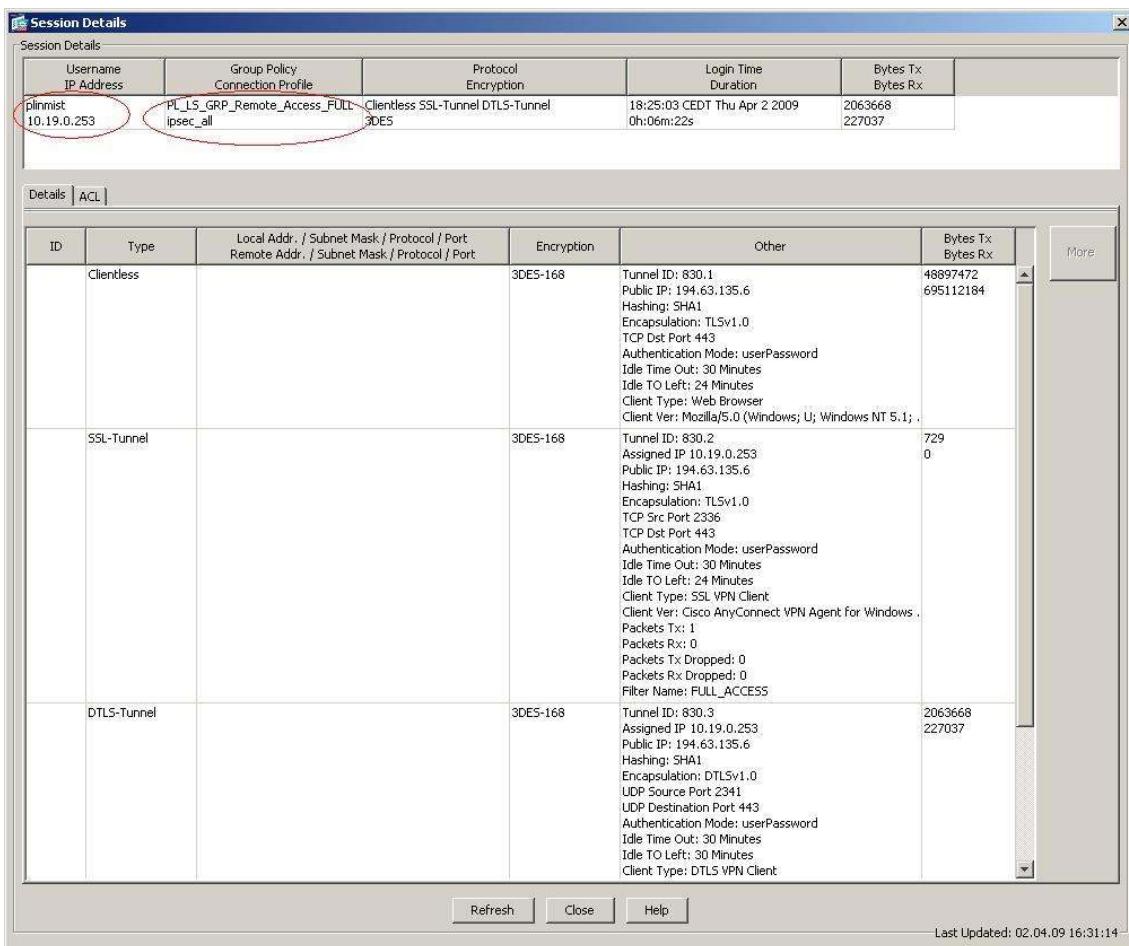
Rysunek 89 Opracowanie własne: metoda dostępu SSL/TLS (połączenie ustanowione)

Przeprowadzono analogiczne jak dla metody połączenia IPsec (7.3.1) próby połączeń dla użytkowników:

- plinmist (Group:Active_Directory)
- plinmist2 (Group:Active_Directory)
- tellstrzeleckim (Group:Token_RSA)

Automatyczna konfiguracja interfejsów sieciowych oraz tablic routingu, przebiegła w analogiczny sposób jak dla metody dostępu IPsec(7.3.1).

Z poziomu aplikacji ASDM (Monitoring > VPN > VPN Statistics > Sessions) można na bieżąco śledzić wszystkie parametry połączenia VPN. Na rys.90 pokazane są parametry połączenia SSL VPN użytkownika plinmist, profil połączenia ASA, przynależność do grupy, aktualny adres IP, typ metody uwierzytelnienia, algorytmy szyfrowania itd.



Rysunek 90 Opracowanie własne: Aplikacji ASDM Session Manager - śledzenie połączeń VPN

| Lp. | Metoda dostępu SSL\TLS (Cisco Any Connect, ACL: WEB_ACCESS, FULL_ACCESS, VISTORM_RSA) | Status |
|-----|--|-----------|
| 1 | <p>Weryfikacja osiągalności serwerów wewnętrz sieci poprzez polecenie ping z komputera pracownika zdalnego icmp (echo-request):</p> <ul style="list-style-type: none"> • Serwery Aplikacji • Kontrolery domeny • Serwery VOIP • Serwery Poczty • Serwery OCS • Wszystkie pozostałe serwery z sieci lokalnej były osiągalne tylko dla ACL: FULL_ACCESS, VISTORM_RSA | Pozytywny |
| 2 | Weryfikacja osiągalności usług sieciowych wewnętrz sieci z użyciem polecenia telnet (na określony) numer portu TCP z | Pozytywny |

| | | |
|---|---|-----------|
| | komputera pracownika zdalnego dla usług: <ul style="list-style-type: none"> • http/tcp/80 • https/tcp/443 • tcp/445 • RDP/tcp/3389 • ssh/tcp/22 • ldap/tcp/389 • Wszystkie pozostałe porty osiągalne były tylko dla ACL: FULL_ACCESS, VISTORM_RSA | |
| 3 | Weryfikacja poprawności zestawienia tunelu VPN poprzez okno Aplikacji ASD: Session Manager | Pozytywny |

7.3.3 Połączenie VPN z użyciem protokołu L2TP/IPsec

Zgodnie z wymaganiami projektowymi, metoda dostępu z użyciem protokołu L2TP/IPsec dostępna jest tylko dla użytkowników posiadających konto w domenie Active Directory. Konfigurację wbudowanego w systemy Windows klienta IPsec przeprowadzono analogicznie jak w rozdziale 7.2.13.

W okno logowania (Rys.91) wprowadzono kolejno nazwy i hasła użytkowników:

- plinmist (Użytkownik jest członkiem grupy domenowej STRZELEC\PL_GS_GRP_Remote_ACCESS z ograniczonym dostępem, lista kontroli dostępu WEB_ACCESS), po podłączeniu do firmowej sieci lokalnej otrzyma adres IP z puli: Poland_WEB_Access (zakres IP 10.19.0.130-10.19.0.190).
- plinmist2 (Użytkownik jest członkiem grup domenowych STRZELEC\PL_GS_GRP_Remote_ACCESS STRZELEC\GLOB_GS_GRP_Remote_ACCESS FULL (dla grupy użytkowników z Polski z pełnym dostępem, lista kontroli dostępu FULL_ACCESS), po podłączeniu do firmowej sieci lokalnej otrzyma adres IP z puli: Poland_FULL_Access (zakres IP 10.19.0.194-10.19.0.254)).



Rysunek 91 Opracowanie własne: Połączenie VPN przez klient L2TP/IPsec

Automatyczna konfiguracja interfejsów sieciowych oraz tablic routingu, przebiegła w analogiczny sposób jak dla metody dostępu IPsec(7.3.1).

| Lp. | Metoda dostępu L2TP/Ipsec (ACL: WEB_ACCESS, FULL_ACCESS) | Status |
|-----|---|-----------|
| 1 | Weryfikacja osiągalności serwerów wewnętrz sieci poprzez polecenie ping z komputera pracownika zdalnego icmp (echo-request): <ul style="list-style-type: none"> • Serwery Aplikacji • Kontrolery domeny • Serwery VOIP • Serwery Poczty • Serwery OCS • Wszystkie pozostałe serwery z sieci lokalnej były osiągalne tylko dla ACL: FULL_ACCESS | Pozytywny |
| 2 | Weryfikacja osiągalności usług sieciowych wewnętrz sieci z | Pozytywny |

| | | |
|---|---|-----------|
| | <p>użyciem polecenia telnet (na określony) numer portu TCP z komputera pracownika zdalnego dla usług:</p> <ul style="list-style-type: none"> • http/tcp/80 • https/tcp/443 • tcp/445 • RDP/tcp/3389 • ssh/tcp/22 • ldap/tcp/389 • Wszystkie pozostałe porty osiągalne były tylko dla ACL: FULL_ACCESS | |
| 3 | Weryfikacja poprawności zestawienia tunelu VPN poprzez okno Aplikacji ASD: Session Manager | Pozytywny |
| 4 | <p>Weryfikacja poprawności konfiguracji IKE poprzez polecenie show crypto isakmp SA na urządzeniu ASA:</p> <pre>ASA1# sh crypto isakmp sa Active SA: 2 Rekey SA: 0 (A tunnel will report 1 Active and 2 Rekey SA during rekey) Total IKE SA: 2 1 IKE Peer: 77.112.195.145 Type: user Role :responder Rekey: no State :AM_ACTIVE</pre> | Pozytywny |
| 5 | <p>Weryfikacja poprawności konfiguracji protokołu IPsec poprzez polecenie sh crypto ipsec sa summary lub sh crypto ipsec sa na urządzeniu ASA:</p> <pre>ASA1# sh crypto ipsec sa summary Current IPsec SA's:1 Peak IPsec SA's: IPSec :1 Peak Concurrent SA:4 IPSec over UDP:0 Peak Concurrent L2L:0 IPSec over NAT-T:2 Peak Concurrent RA:-1 IPSec over TCP :0 IPSec VPN LB :0 Total :3</pre> | Pozytywny |

| | | |
|--|---|--|
| | <pre> ASA1# sh crypto ipsec sa ASA1# sh crypto ipsec sa interface: Outside Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: Outside_Interface local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (10.19.0.195/255.255.255.255/0/0) current_peer: 77.112.195.145, username: strzelec\plinmistr dynamic allocated peer ip: 10.19.40.195 #pkts encaps: 13486, #pkts encrypt: 13492, #pkts digest: 13492 #pkts decaps: 13399, #pkts decrypt: 13395, #pkts verify: 13395 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 13486, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 6, #pre-frag failures: 0, #fragments created: 12 #PMTUUs sent: 0, #PMTUUs rcvd: 0, #decapsulated frgs needing reassembly: 12 #send errors: 0, #recv errors: 4 local crypto endpt.: Outside_Interface, remote crypto endpt.: 77.112.195.145 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 20E189DD inbound esp sas: spi: 0x4A4F3465 (1246704741) transform: esp-3des esp-sha-hmac no compression in use settings =(RA, Tunnel,) slot: 0, conn_id: 3624960, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 21291 IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0xBFFFFFFF 0xFFFFFDFF outbound esp sas: spi: 0x20E189DD (551651805) transform: esp-3des esp-sha-hmac no compression in use settings =(RA, Tunnel,) slot: 0, conn_id: 3624960, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 21290 IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0x00000000 0x00000001 </pre> | |
|--|---|--|

7.4 Testy wydajnościowe

Do wykonania pomiarów posłużył komputer klasy PC z dostępnymi trzema łączami do sieci Internet o następujących parametrach nominalnych:

Tabela 27 Opracowanie własne: Parametry testowych łącz do sieci Internet

| Lp | Typ/Technologia | Max.prędkość pobierania | Max.prędkość wysyłania |
|----|-----------------|-------------------------|------------------------|
| 1 | WIFI (2,4GHz) | 1024kbit/s | 600kbit/s |
| 2 | ADSL | 2048kbit/s | 512kbit/s |
| 3 | ETHERNET | 6000kbit/s | 6000kbit/s |

Aby określić realną, maksymalną prędkość pobierania i wysyłania danych przez dostępne technologie, wykonane zostały wcześniejsze testy łącz, oraz pomiar średniego czasu błędzenia pakietów.

Jako test przyjęto średni transfer danych z/do serwera ISP danego łącza, umiejscowionego w jego sieci szkieletowej oraz serwera <ftp://icm.edu.pl> (serwer posiadający łączę do sieci Internet o prędkości ponad 1Gbit/s). Ten sam pomiar

wykonywany był 5 razy przy pomocy programu BWMeter ver2.7, oraz polecenia systemowego PING (pakiety 32 bajtowe, powtórzone 100 razy). Wyniki przedstawione są w tabeli 28. Wartość procentowa prezentuje realną osiągniętą szybkość łączą uzyskaną w teście w stosunku do nominalnej (deklarowanej przez ISP).

Tabela 28 Opracowanie własne: Parametry zmierzone testowych łącz do sieci Internet

| Lp | Typ/Technologia | Max.uzyskana prędkość pobierania | Max.uzyskana prędkość wysyłania | Czas błędzenia pakietów (min) | Czas błędzenia pakietów (max) |
|----|-----------------|----------------------------------|---------------------------------|-------------------------------|-------------------------------|
| 1 | WIFI (2,4GHz) | 782kbit/s(76%) | 280kbit/s(47%) | 20ms | 80ms |
| 2 | ADSL | 1928kbit/s(94%) | 491kbit/s(96%) | 6ms | 25ms |
| 3 | ETHERNET | 5402kbit/s(90%) | 5609kbit/s(93%) | 4ms | 20ms |

Mając tak przygotowane stanowisko testowe, rozpoczęto pomiar pobierania i wysyłania danych z serwera WWW znajdującego się w siedzibie firmy w oddziale Szwecja (w tej samej sieci, gdzie koncentrator VPN) . Serwer ten jest dostępny jest także w publicznej sieci Internet, dlatego też można zbadać maksymalną prędkość transferu danych zanim zostaną one zabezpieczone i przesłane przez Tunel VPN (między siedzibą firmy a komputerem telepracownika). Wartość procentowa określa stosunek maksymalnej realnej prędkości łączącej do osiągniętej w teście pobierania danych z serwera firmowego poprzez sieć Internet. Wyniki w tabeli 29.

Tabela 29 Opracowanie własne: Szybkość pobierania/wysyłania danych z serwera WWW w siedzibie firmy

| Lp | Typ/Technologia | Max.uzyskana prędkość pobierania | Max.uzyskana prędkość wysyłania | Czas błędzenia pakietów (min) | Czas błędzenia pakietów (max) |
|----|-----------------|----------------------------------|---------------------------------|-------------------------------|-------------------------------|
| 1 | WIFI (2,4GHz) | 621kbit/s(79%) | 230kbit/s(82%) | 16ms | 47ms |
| 2 | ADSL | 1621kbit/s(84%) | 446kbit/s(91%) | 15ms | 18ms |
| 3 | ETHERNET | 4309kbit/s(80%) | 4001kbit/s(71%) | 6ms | 22ms |

Na testowym komputerze skonfigurowano trzy metody dostępu zdalnego:

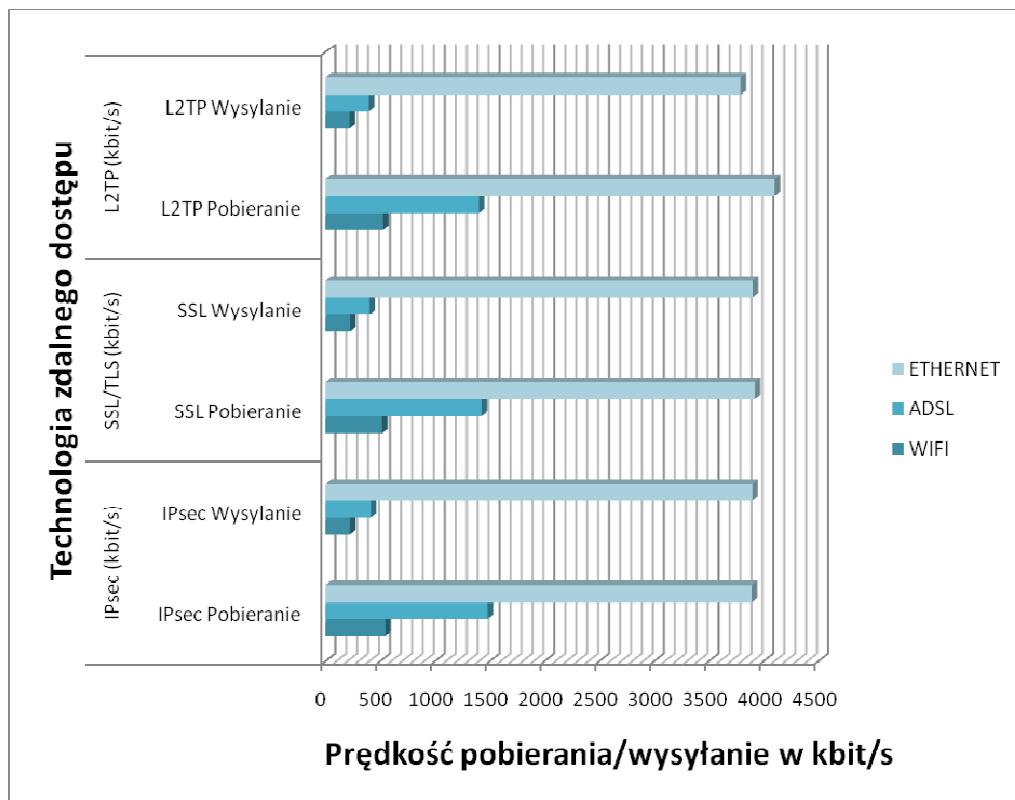
- IPsec

- SSL\TLS
- L2TP\IPsec

Dla każdej z metod wykonano próby zestawienia połączenia VPN ze zdalną siecią korporacyjną (urządzenie ASA5520 zainstalowana jest na symetrycznym łączu do sieci Internet o prędkości 100Mbit/s), a następnie testy prędkości pobierania danych z wewnętrznych serwerów zasobowych, WWW i FTP. Wartość procentowa obrazuje spadek wydajności pobierania i wysyłania danych za pośrednictwem bezpiecznego połączenia VPN w stosunku do wartości zmierzanej podczas poprzedniego testu.

Tabela 30 Opracowanie własne: Szybkość pobierania/wysyłania danych za pośrednictwem połączeń VPN

| Lp | Łącze | IPsec (DL/UL kbit/s) | | SSL/TLS (DL/UL kbit/s) | | L2TP (DL/UL kbit/s) | | RTT (ms) |
|----|----------|-------------------------|----------|---------------------------|----------|------------------------|----------|-------------|
| 1 | WIFI | 546(12%) | 223(3%) | 517(17%) | 225(2%) | 526(15%) | 220(2%) | 22 |
| 2 | ADSL | 1480(9%) | 414(7%) | 1426(12%) | 402(10%) | 1401(14%) | 396(11%) | 20 |
| 3 | ETHERNET | 3892(10%) | 3897(1%) | 3921(9%) | 3900(3%) | 4102(5%) | 3790(5%) | 20 |



Rysunek 92 Opracowanie własne: Wykres porównujący metody dostępu zdalnego na tle osiąganej prędkości pobierania i wysyłania danych (prędkość wyrażona w kbit/s)

7.5 Omówienie wyników testów

W pierwszym etapie testów zweryfikowano możliwości i sposób użycia wszystkich zastosowanych w projekcie technologii zdalnego dostępu do nawiązania bezpiecznego połączenia VPN.

Skonfigurowana aplikacja Cisco VPN Client umożliwiająca nawiązanie połączenia IPsec, nie sprawiła żadnych kłopotów podczas zestawiania tunelu VPN i uwierzytelniania telepracownika. Użytkownik za każdym razem otrzymywał adres IP z właściwej puli, zależnej od metody uwierzytelnienia oraz przynależności do grupy domenowej. Mechanizm Split tunneling, także funkcjonował prawidłowo, modyfikując tablicę routingu na stacji roboczej.

Zestawienie połączenia VPN za pomocą protokołów SSL\TLS okazało się prostsze, gdyż nie wymagało żadnych konfiguracji na stacji roboczej, a jedynie otwarcia stosownego adresu URL w przeglądarce internetowej. Rolą telepracownika próbującego

nawiązać połączenie VPN jest jedynie poprawne wprowadzenie danych uwierzytelniających (użytkownik/hasło, lub login/wskazanie tokenu RSA) oraz wybrania metody uwierzytelniania. Podobnie jak w przypadku aplikacji Cisco VPN Client, nie było żadnych kłopotów z automatyczną konfiguracją interfejsu sieciowego stacji roboczej oraz tablicy routingu.

Mechanizm sprawdzający czy stacja robocza spełnia założone wymogi bezpieczeństwa funkcjonował bez zarzutu. System operacyjny nie spełniający kryteriów, za każdym razem ładował aplikację Cisco Secure Desktop, tworzącą dodatkową barierę ochronną w postaci odseparowanych od systemu operacyjnego zasobów programowych.

Połączenie VPN realizowane za pomocą protokołu L2TP/IPsec, również nie sprawiło kłopotów konfiguracji i eksploatacji. Wbudowany w systemy Windows klient L2TP, w szybki sposób umożliwił nawiązanie tunelowanego połączenia IPsec. Automatyczna konfiguracja interfejsu sieciowego oraz tablicy routingu za każdym razem i dla każdego testowego użytkownika przebiegła w planowany sposób. Zgodnie z wymaganiami projektu, dostęp L2TP dostępny jest tylko dla pracowników mających konta w domenie oraz przynależą do odpowiednich grup.

Listy kontroli dostępu dla każdej z wymienionych metod dostępu i uwierzytelnienia użytkownika funkcjonowały zgodnie z wymaganiami, umożliwiając pełny dostęp do sieci tylko użytkownikom, którzy mają stosowne uprawnienia w domenie lub też używają Tokenów RSA. Pozostali członkowie domeny *Active Directory* (którzy przynależą tylko do jednej grupy) – dostęp ograniczony do określonych serwerów i usług.

Drugą fazą testów było przeprowadzenie pomiarów szybkości pobierania/wysłania danych oraz czasu błądzenia pakietów za pośrednictwem dostępnych trzech technologii zdalnego dostępu.

Przeprowadzenie wstępnych pomiarów wydajności poszczególnych łącz internetowych miało na celu ocenić maksymalną, użyteczną prędkość pobierania/wysyłania danych w stosunku do nominalnej, deklarowanej przez dostawców usług. Średnia wydajności łącz w stosunku do nominalnej różniła się o maksimum 25 % przy pobieraniu a nawet o 40% przy wysłaniu danych. Kolejnym testem był pomiar prędkości pobierania/wysyłania danych poprzez sieć Internet z serwera WWW znajdującego się w oddziale firmy wyposażonym w łączę internetowe, którego prędkość (100Mbit/s) zdecydowanie przekracza maksymalną możliwą do uzyskania na łączach internetowych stanowiska

testowego. Uzyskane wyniki zostały porównane z poprzednim testem (realna do osiągnięcia prędkość pobierania/wysyłania danych w sieci Internet). Średnia prędkość uzyskana podczas transferowania plików z/do serwera WWW w siedzibie firmy różniła się o maksimum 10-15% w stosunku do maksymalnej osiągniętej na danym łączu (w poprzednim teście).

Najważniejszy test polegał jednak na zmierzeniu prędkości pobierania/wysyłania danych za pośrednictwem zdalnego dostępu, i różnych technologii VPN. Największy spadek wydajności jaki zanotowano wynosił 15% (dla L2TP) w stosunku do prędkości transferowania tych samych danych poprzez sieć publiczną bez ochrony danych. Średni spadek wydajności był jednak niezależny od technologii zdalnego dostępu i wynosi ok 10%.

Czas błądzenia pakietów nie przekraczał wartości 25ms, dzięki czemu testowane połączenie VPN może służyć do przesyłania głosu lub wideo w czasie rzeczywistym.

8 Podsumowanie i wnioski

W pracy omówione zostały zagadnienia dotyczące zdalnego dostępu do sieci korporacyjnej poprzez sieci publiczne (Internet). Poznając genezę sieci lokalnych, rozległych i najważniejszego obecnie protokołu komunikacyjnego (IP), można zrozumieć największe zagrożenia, na jakie narażone są dane podczas przesyłania przez Internet. Niełatwo jednak przeciwdziałać wciąż rosnącej fali przestępstw elektronicznych. Omówione w niniejszej pracy technologie i procesy służące ochronie danych już od najniższych warstw, pozwalają na podniesienie poziomu bezpieczeństwa do maksimum, co jest szczególnie istotne dla firm, które korzystają z zalet sieci publicznych. Chociaż w pracy opisane zostały protokoły różnych warstw, to najważniejsze z nich służą do budowy wirtualnych sieci prywatnych. Umożliwiają one zbudowanie bezpiecznych, logicznych połączeń zarówno pomiędzy odległymi oddziałami firm, ale przede wszystkim na bezpieczną komunikację z telepracownikami, będącymi mobilnymi oddziałami firmy.

Omówione w pracy metody i technologie zdalnego dostępu: IPsec, SSL/TLS VPN oraz L2TP/IPsec pozwalają osiągnąć ten sam cel – zapewnić poufną, integralną i

niepodważalną transmisję danych poprzez sieć Internet. Technologie te różnią się od siebie zarówno budową, implementacją jak i sposobem późniejszej eksploatacji.

Protokół IPsec dominujący od wielu lat standard, zdobył swoją popularność dzięki uniwersalności zastosowań. Rozwija możliwości protokołu IPv4 o funkcjonalności, które są już w nowej odsłonie niezbyt jeszcze popularnego IPv6. Zapewnia bardzo wiele możliwości konfiguracyjnych i oferuje wysoki standard bezpieczeństwa. Zrozumienie architektury IPsec nastręcza trudności nawet doświadczonym administratorom, dlatego też w pracy zamieszczony jest jego szczegółowy opis oraz przykład późniejszej implementacji w projekcie sieci.

Protokół L2TP (z użyciem IPsec) jest protokołem hybrydowym powstały na bazie właściwości technologii firmy Microsoft (PPTP) i Cisco Systems (L2F). Pozwala ustanowić bezpieczny tunel komunikacyjny w sieci Internet, już w warstwie drugiej modelu referencyjnego ISO/OSI. Jako, że sam w sobie protokół nie zapewnia funkcji szyfrowania danych, to możliwym jest umieszczenie pakietów IPsec wewnętrz takiego połączenia. Przykładem praktycznym zastosowania i wdrożenia protokołu L2TP jest część projektowa niniejszej pracy dyplomowej.

Protokół SSL/TLS (klient-serwer) pozwala na nawiązanie bezpiecznego połączenia z użyciem certyfikatów. Stosowany głównie do zabezpieczenia komunikacji między klientem (użytkownikiem) a serwerem WWW. Jako największy konkurent protokołu IPsec pozwala także na nawiązanie dwukierunkowej komunikacji klient-serwer, za pośrednictwem automatycznie ładowanych aplikacji z poziomu zwykłej przeglądarki internetowej. Nie wymaga przy tym żadnych konfiguracji stacji roboczej, dlatego też jest coraz częściej stosowany przez administratorów sieci. W części projektowej implementacja metody dostępu VPN poprzez SSL/TLS została szerzej opisana.

Spośród omówionych, protokół SSL/TLS jest moim zdaniem najbardziej uniwersalnym i przyszłościowym rozwiązaniem jeśli chodzi o usługę zdalnego dostępu do firmowych sieci lokalnych. Do nawiązania bezpiecznego połączenia wymaga jedynie dowolnej przeglądarki internetowej obsługującej technologię Java lub ActiveX. Nie wymaga żadnej konfiguracji aplikacji na stacji roboczej, przekazywania użytkownikowi sekretnej frazy koniecznej do konfiguracji połączeń IPsec czy L2TP, ani używania konkretnego systemu operacyjnego. Jako dodatkowo wbudowana opcja automatycznej weryfikacji stacji roboczej użytkownika, pozwala na samoczynne zabezpieczanie systemów operacyjnych komputerów nie spełniających założeń

firmowej polityki bezpieczeństwa. Nie występują także problemy z aktualizacją aplikacji ustanawiającej połaczenie VPN, gdyż za każdym razem kiedy użytkownik nawiązuje komunikacje za pośrednictwem przeglądarki internetowej, aplikacja ta pobierana jest i instalowana na nowo z pamięci koncentratora VPN.

Użycie pozostałych technologii umożliwiających realizację zdalnego dostępu do sieci firmowej, niestety wymaga pewnej początkowej interakcji użytkownika z działem informatyki, gdyż proces instalacji i konfiguracji wymaga znajomości aplikacji VPN oraz parametrów programu. Późniejsza eksploatacja tak skonfigurowanych połączeń nie wymaga zmian, do czasu istotnej modyfikacji konfiguracji koncentratora VPN przez administratorów sieci.

W części praktycznej niniejszej pracy magisterskiej wykonano projekt zdalnego dostępu VPN do sieci korporacyjnej. System ten umożliwia w sposób łatwy i niezależny od miejsca pobytu nawiązanie bezpiecznego połączenia z zasobami firmowej sieci lokalnej. Użytkownik może skorzystać z dowolnej z omówionych w części teoretycznej metod dostępu zdalnego: IPsec, SSL/TLS VPN, L2TP/IPsec pod warunkiem posiadania komputera oraz dowolnego łączka internetowego.

Integracja systemu zabezpieczeń z serwerami RADIUS i SDI, których szczegółowy opis także zawarty jest w pracy, pozwala na weryfikację osoby próbującej uzyskać połaczenie do sieci oraz poziomu jej uprawnień. Możliwym jest uwierzytelnianie telepracowników na podstawie nazwy użytkownika i hasła z domeny Active Directory lub też na podstawie jednorazowych haseł generowanych przez sprzętowe tokeny RSA. Dużo bezpieczniejszym niż pamiętanie loginu i hasła z domeny (które można podpatrzeć, lub podluchać odpowiednimi narzędziami), jest rozwiązywanie kwestii uwierzytelniania z użyciem generatorów haseł jednorazowych (tokenów). Użytkownik nie jest narażony na próby podsłuchu informacji, gdyż przechwycone podczas próby logowania dane uwierzytelniające, raz użyte stają się bezwartościowe. Nawet kradzież Tokenu nie umożliwia w prosty sposób podszcycia się pod jego właściciela, gdyż jednorazowe hasło każdorazowo musi być poprzedzone podaniem kodu pin, który zna tylko właściciel. Rozwiązywanie z użyciem technologii TokenRSA, ma jedną poważną wadę - nie jest tanie.

Jako przyszłość metod uwierzytelniania użytkowników – uważam weryfikację cech biometrycznych ludzi. Nie jest to metoda tania, ani powszechna, ale z pewnością najbezpieczniejsza z wymienionych, przy założeniu weryfikacji np. dwóch różnych

cech ludzkich jednocześnie. Z uwagi na brak dostępu do w/w systemów uwierzytelniających, w pracy został zawarty tylko ich teoretyczny opis. Implementacja dodatkowych możliwości uwierzytelniania w projekcie mogła by stanowić doskonałe rozwinięcie niniejszej pracy magisterskiej.

Po wykonaniu testów wydajnościowych i kontrolnych można zauważyc, nieznaczne zmniejszenie prędkości przesyłania danych za pośrednictwem systemu zdalnego dostępu. Niezależnie od użytej do nawiązania połączenia technologii zdalnego dostępu, należy spodziewać się spadku ok 15% (zależne głównie od użytego algorytmu szyfrowania) w stosunku do prędkości, jaką można by osiągnąć przesyłając dane połączeniem niezabezpieczonym. Obniżenie wydajności spowodowane jest obciążeniem procesora, pamięci i systemu operacyjnego poprzez zaawansowane operacje kryptograficzne, zarówno po stronie komputera telepracownika, jak i samego koncentratora VPN. Prawdopodobnie nowsze wersje oprogramowania VPN na stacjach użytkowników oraz systemu operacyjnego, zostaną w przyszłości bardziej zoptymalizowane, co zaowocuje zmniejszeniem spadku wydajności do kilku procent. Testy wykazały również, że wykorzystując dostępne typowe w domach łącza internetowe, np. za pośrednictwem technologii Ethernet, ADSL, czy dostępu bezprzewodowego, możliwa jest praca zdalna nawet z użyciem technologii VOIP czy Video w czasie rzeczywistym, dzięki niskim i stałym wartościom opóźnień propagacji pakietów.

Niniejsza praca zatytułowana „Zdalny dostęp do zasobów sieci LAN przedsiębiorstwa oraz metody uwierzytelniania telepracowników” stanowi zbiór wiedzy o bezpieczeństwie zarówno sieci lokalnych, ale i publicznych, tworzących sieć Internet. Pozwala zrozumieć protokoły nimi rządzące, a także bezpieczeństwa, jakie mogą grozić nieświadomym użytkownikom.

W pracy opisane zostały wszystkie znane mi protokoły i technologie, które można użyć, aby zapewnić poufną komunikację zdalnym pracownikom z dowolnie oddalonym oddziałem firmy. Omówione techniki weryfikacji tożsamości (uwierzytelniania), pozwalają na skuteczne ograniczenie dostępu do zasobów sieci lokalnej, tylko dla pracowników mających wymagane uprawnienia.

W pracy przedstawione są kolejne etapy implementacji realnego projektu w istniejącej sieci w oparciu o najnowsze protokoły bezpieczeństwa.

9 Pliki Konfiguracyjne

W tym rozdziale zamieszczony jest listing głównego pliku konfiguracyjnego urządzenia ASA5520, na bazie którego powstał projekt zdalnego dostępu. Pozostałe pliki konfiguracyjne, ze względu na duży rozmiar, brak możliwości czytelnego podglądu lub formę zapisu dołączone są na płycie CD-ROM.

Tabela 31 Opracowanie własne: Główny plik konfiguracyjny urządzenia ASA5520

```
: Saved
: Written by admin at 22:08:24.682 CEST Tue Mar 3 2009
!
ASA Version 8.0(4)
!
hostname ASA1
domain-name strzelec.com
enable password rgdrXSFhefhg5hTR encrypted
passwd ssffsj5uxvI.2KYOU encrypted
name 1.1.1.7 Outside_Interface
name 10.220.2.200 Servicedesk description Servicedesk server
name 10.39.40.192 PL_FULL_ACCESS
name 10.39.40.128 PL_WEB_ACCESS
name 10.39.40.64 SE_FULL_ACCESS
name 10.39.40.0 SE_WEB_ACCESS
name 10.39.41.128 DE_WEB_ACCESS
name 10.39.41.192 DE_FULL_ACCESS
name 10.10.2.22 APPSERVER02
name 10.10.2.23 APPSERVER03
name 10.39.32.22 APPSERVER04
name 10.11.2.6 APPSERVER06
name 10.182.46.2 APPSERVER08
name 10.39.32.1 EXCHSERVER01
name 10.39.32.3 EXCHSERVER02
name 10.10.1.22 EXCHSERVER03
name 10.10.1.21 EXCHSERVER04
name 10.39.32.5 EXCHSERVER05
name 10.39.48.131 EXCHSERVER06
name 10.10.2.45 OCSSERVER01 description LCS server
name 10.39.48.135 OCSSERVER02 description LCS server
name 10.10.2.51 DCCONTROLLER01
name 10.11.2.149 DCCONTROLLER02
name 10.11.2.49 DCCONTROLLER03
name 10.220.1.9 TRIXBOX_PL description Trixbox Poland
name 10.182.6.9 TRIXBOX_FR description Trixbox FR
!
interface GigabitEthernet0/0
  nameif Outside
  security-level 0
  ip address 1.1.1.7 255.255.255.240
!
```

```

interface GigabitEthernet0/1
    nameif Inside
    security-level 100
    ip address 10.20.45.1 255.255.255.252
!
interface GigabitEthernet0/2
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/3
    shutdown
    no nameif
    no security-level
    no ip address
!
interface Management0/0
    nameif management
    security-level 100
    ip address 192.168.1.1 255.255.255.0
    management-only
!
boot system disk0:/asa804-k8.bin
ftp mode passive
clock timezone CEST 1
clock summer-time CEDT recurring last Sun Mar 2:00 last Sun Oct 3:00
dns server-group DefaultDNS
domain-name strzelec.local
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object-group service L2TP udp
port-object eq 1701
object-group network GRUPA_SIECI_OGRANICZONYCH
network-object SE_WEB_ACCESS 255.255.255.192
network-object PL_WEB_ACCESS 255.255.255.192
network-object FR_WEB_ACCESS 255.255.255.192
network-object DE_WEB_ACCESS 255.255.255.192
network-object FR_WEB_ACCESS 255.255.255.192
network-object IN_WEB_ACCESS 255.255.255.192
object-group network GRUPA_SIECI_BEZ_OGRANICZEN
network-object PL_FULL_ACCESS 255.255.255.192
network-object SE_FULL_ACCESS 255.255.255.192
network-object DE_FULL_ACCESS 255.255.255.192
network-object FR_FULL_ACCESS 255.255.255.192
network-object FR_FULL_ACCESS 255.255.255.192
network-object IN_FULL_ACCESS 255.255.255.192
object-group service GRUPA_USLUG_DOZWOLONYCH
service-object icmp
service-object tcp-udp eq domain
service-object tcp eq www
service-object tcp eq https
service-object tcp eq 445
service-object tcp eq 3389
service-object tcp eq 5061
service-object tcp eq netbios-ssn
service-object udp eq netbios-dgm
service-object udp eq netbios-ns

```

```

service-object tcp eq sip
service-object udp eq 5061
service-object udp eq sip
service-object tcp-udp eq 1030
service-object tcp-udp eq 1700
service-object tcp eq 5062
service-object udp eq 5062
service-object udp range 50001 51000
service-object tcp-udp eq 5063
object-group service GRUPA_USLUG_DOZWOLONYCH_RSA
service-object icmp
service-object tcp-udp eq domain
service-object tcp eq www
service-object tcp eq https
service-object tcp eq 445
service-object tcp eq 5061
service-object tcp eq sip
service-object udp eq 5061
service-object udp eq sip
service-object tcp-udp eq 1030
service-object tcp-udp eq 1700
service-object tcp eq 5062
service-object udp eq 5062
service-object udp range 50001 51000
service-object tcp-udp eq 5063
object-group service Exchange_grp
description Strzelec
service-object tcp-udp range 135 139
object-group network Exchange_Servers
description All strzelec exchange servers
network-object host EXCHSERVER01
network-object host EXCHSERVER02
network-object host EXCHSERVER03
network-object host EXCHSERVER04
network-object host EXCHSERVER05
network-object host EXCHSERVER06
object-group network App_Servers
description All strzelec Application servers
network-object host APPSERVER02
network-object host APPSERVER03
network-object host APPSERVER04
network-object host APPSERVER06
object-group network DS_Servers
description All strzelec DS servers
network-object host DCCONTROLLER01
network-object host DCCONTROLLER02
network-object host DCCONTROLLER03
object-group service GRUPA_USLUG_DOSTEPNYCH
service-object icmp
service-object tcp-udp eq domain
service-object tcp eq 445
service-object tcp eq www
service-object tcp eq https
service-object tcp eq 3389
service-object tcp eq 5061
service-object tcp eq netbios-ssn
service-object tcp eq sip
service-object udp eq 5061

```

```

service-object udp eq netbios-dgm
service-object udp eq netbios-ns
service-object udp eq sip
service-object tcp-udp eq 1030
service-object tcp-udp eq 1700
object-group network LCS_servers
network-object host OCSERVER02
network-object host OCSERVER01
network-object host DCCONTROLLER01
network-object host DCCONTROLLER02
object-group service UDP udp
port-object eq 5061
object-group network GRUPA_SERWEROW_EXCHANGE
group-object Exchange_Servers
group-object LCS_servers
object-group network TrixBox
description VOIP
network-object host TRIXBOX_PL
network-object host TRIXBOX_FR
object-group protocol TCPUDP
protocol-object udp
protocol-object tcp
object-group service rtp_range tcp-udp
port-object range 10000 32768
object-group service GRUPA_USLUG_VOIP
group-object rtp_range
port-object eq sip
access-list strzelec_Internal standard permit 10.0.0.0 255.0.0.0
access-list Net_10.19.0.0/18 standard permit 10.19.0.0 255.255.192.0
access-list DefaultRAGroup_splitTunnelAcl standard permit any
access-list Internet_Only extended deny ip any 10.0.0.0 255.0.0.0
access-list ANY_ANY extended permit ip any any
access-list Inside_access_in extended permit ip any any
access-list WEB_ACCESS remark ICMP, DNS, Windows Share, LCS, http, https
access-list WEB_ACCESS extended permit object-group GRUPA_USLUG_DOZWOLONYCH object-group
GRUPA_SIECI_OGRANICZONYCH any
access-list WEB_ACCESS remark Exchange access
access-list WEB_ACCESS extended permit ip object-group GRUPA_SIECI_OGRANICZONYCH object-group
GRUPA_SERWEROW_EXCHANGE
access-list WEB_ACCESS remark Application server access
access-list WEB_ACCESS extended permit ip object-group GRUPA_SIECI_OGRANICZONYCH object-group
APP_Servers
access-list WEB_ACCESS remark Application DS access
access-list WEB_ACCESS extended permit ip object-group GRUPA_SIECI_OGRANICZONYCH object-group
DC_Servers
access-list WEB_ACCESS extended permit object-group TCPUDP object-group GRUPA_SIECI_OGRANICZONYCH
object-group TrixBox object-group GRUPA_USLUG_VOIP
access-list WEB_ACCESS remark VOIP Access
access-list WEB_ACCESS extended permit ip object-group TrixBox object-group
GRUPA_SIECI_OGRANICZONYCH
access-list WEB_ACCESS extended permit ip object-group GRUPA_SERWEROW_EXCHANGE object-group
GRUPA_SIECI_OGRANICZONYCH
access-list WEB_ACCESS extended permit ip object-group APP_Servers object-group
GRUPA_SIECI_OGRANICZONYCH
access-list WEB_ACCESS extended permit ip object-group DC_Servers object-group
GRUPA_SIECI_OGRANICZONYCH
access-list WEB_ACCESS extended permit udp 10.0.0.0 255.0.0.0 object-group GRUPA_SIECI_OGRANICZONYCH
range 50001 51000

```

```

access-list FULL_ACCESS extended permit ip object-group GRUPA_SIECI_BEZ_OGRANICZEN any
access-list ACL_VISTORM_RSA extended permit object-group GRUPA_USLUG_DOZWOLONYCH_RSA object-group
VISTORM_RSA any
access-list ACL_VISTORM_RSA extended permit ip object-group VISTORM_RSA object-group APP_Servers
access-list ACL_VISTORM_RSA extended permit object-group TCPUDP object-group VISTORM_RSA object-
group TrixBox object-group GRUPA_USLUG_VOIP
access-list ACL_VISTORM_RSA extended permit ip object-group TrixBox object-group VISTORM_RSA
access-list ACL_VISTORM_RSA extended permit ip object-group GRUPA_SERWEROW_EXCHANGE object-group
VISTORM_RSA
access-list ACL_VISTORM_RSA extended permit ip object-group APP_Servers object-group VISTORM_RSA
access-list ACL_VISTORM_RSA extended permit udp 10.0.0.0 255.0.0.0 object-group VISTORM_RSA range
50001 51000

access-list Local_LAN standard permit host 0.0.0.0
pager lines 24
logging enable
logging trap debugging
logging asdm debugging
logging host Inside 10.220.2.42
mtu Outside 1500
mtu Inside 1500
mtu management 1500
ip local pool Sweden_WEB_Access 10.19.0.2-10.19.0.62 mask 255.255.255.192
ip local pool Sweden_FULL_Access 10.19.0.66-10.19.0.126 mask 255.255.255.192
ip local pool Poland_WEB_Access 10.19.0.130-10.19.0.190 mask 255.255.255.192
ip local pool Poland_FULL_Access 10.19.0.194-10.19.0.254 mask 255.255.255.192
ip local pool India_WEB_Access 10.19.1.2-10.19.1.62 mask 255.255.255.192
ip local pool India_FULL_Access 10.19.1.66-10.19.1.126 mask 255.255.255.192
ip local pool Germany_WEB_Access 10.19.1.130-10.19.1.190 mask 255.255.255.192
ip local pool Germany_FULL_Access 10.19.1.194-10.19.1.254 mask 255.255.255.192
ip local pool France_WEB_Access 10.19.2.2-10.19.2.62 mask 255.255.255.192
ip local pool France_FULL_Access 10.19.2.66-10.19.2.126 mask 255.255.255.192
ip local pool VISTORM_RSA 10.19.2.130-10.19.2.190 mask 255.255.255.192
ip local pool China_WEB_Access 10.19.2.194-10.19.2.222 mask 255.255.255.224
ip local pool China_FULL_Access 10.19.2.226-10.19.2.253 mask 255.255.255.224
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-613.bin
asdm location Outside_Interface 255.255.255.255 Inside
asdm location Servicedesk 255.255.255.255 Inside
asdm location SE_WEB_ACCESS 255.255.255.192 Inside
asdm location SE_FULL_ACCESS 255.255.255.192 Inside
asdm location PL_WEB_ACCESS 255.255.255.192 Inside
asdm location PL_FULL_ACCESS 255.255.255.192 Inside
asdm location DE_WEB_ACCESS 255.255.255.192 Inside
asdm location DE_FULL_ACCESS 255.255.255.192 Inside
asdm location FR_WEB_ACCESS 255.255.255.192 Inside
asdm location FR_FULL_ACCESS 255.255.255.192 Inside
asdm location IN_WEB_ACCESS 255.255.255.192 Inside
asdm location IN_FULL_ACCESS 255.255.255.192 Inside
asdm location EXCHSERVER01 255.255.255.255 Inside
asdm location EXCHSERVER02 255.255.255.255 Inside
asdm location APPSERVER02 255.255.255.255 Inside
asdm location APPSERVER06 255.255.255.255 Inside
asdm location EXCHSERVER04 255.255.255.255 Inside
asdm location EXCHSERVER03 255.255.255.255 Inside

```

```

asdm location EXCHSERVER05 255.255.255.255 Inside
asdm location EXCHSERVER06 255.255.255.255 Inside
asdm location VIStORM_RSA 255.255.255.192 Inside
asdm location CN_WEB_ACCESS 255.255.255.192 Inside
asdm location DCCONTROLLER01 255.255.255.255 Inside
asdm location DCCONTROLLER02 255.255.255.255 Inside
asdm location DCCONTROLLER03 255.255.255.255 Inside
asdm location TRIXBOX_FR 255.255.255.255 Inside
asdm location TRIXBOX_PL 255.255.255.255 Inside
no asdm history enable
arp timeout 14400
access-group Inside_access_in in interface Inside
route Outside 0.0.0.0 0.0.0.0 1.1.1.1 1
route Inside 10.0.0.0 255.0.0.0 10.20.45.2 1
route Inside 0.0.0.0 0.0.0.0 10.20.45.2 tunneled
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
aaa-server AD-STRZELEC protocol radius
  accounting-mode simultaneous
  reactivation-mode timed
  max-failed-attempts 3
aaa-server AD-STRZELEC (Inside) host 10.9.25.251
  timeout 2
  key qweRty13214
aaa-server AD-STRZELEC (Inside) host 10.1.2.17
  timeout 2
  key rbrel13Vae2evevb
aaa-server Test_SDI protocol sdi
  reactivation-mode timed
aaa-server Test_SDI (Outside) host 194.125.246.1
aaa-server Radius-TOC protocol radius
  accounting-mode simultaneous
  reactivation-mode timed
aaa-server Radius-TOC (Inside) host 10.220.2.42
  retry-interval 5
  timeout 5
  key 457645vree513v!
  radius-common-pw 12g1ddfbal$
nac-policy DfltGrpPolicy-nac-framework-create nac-framework
  reval-period 36000
  sq-period 300
aaa authentication http console LOCAL
aaa authentication serial console LOCAL
aaa authentication ssh console LOCAL
aaa authentication telnet console LOCAL
aaa authentication enable console LOCAL
aaa authorization command LOCAL
aaa authorization exec authentication-server
http server enable 2000
http 217.153.148.192 255.255.255.224 Outside
http 10.220.0.0 255.255.0.0 Inside
http 10.82.4.0 255.255.254.0 Inside
http 81.210.64.192 255.255.255.240 Outside
http 217.153.251.3 255.255.255.255 Outside

```

```

http 10.220.6.0 255.255.255.0 Inside
http 10.21.128.0 255.255.255.192 Inside
http PL_WEB_ACCESS 255.255.255.128 Outside
http redirect Outside 80
snmp-server host Inside 10.20.3.248 community evfpgp234eeg version 2c
snmp-server host Inside 10.220.1.37 community evfpgp234eeg version 2c
snmp-server host Inside 10.220.2.42 community evfpgp234eeg version 2c
snmp-server host Inside 10.20.2.30 community qwsx1@234 version 2c
no snmp-server location
no snmp-server contact
snmp-server community evfpgp234eeg
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set TRANS_ESP_3DES_SHA esp-3des esp-sha-hmac
crypto ipsec transform-set TRANS_ESP_3DES_SHA mode transport
crypto ipsec transform-set TRANS_ESP_DES_SHA esp-des esp-sha-hmac
crypto ipsec transform-set TRANS_ESP_DES_SHA mode transport
crypto ipsec transform-set TRANS_ESP_DES_MD5 esp-des esp-md5-hmac
crypto ipsec transform-set TRANS_ESP_DES_MD5 mode transport
crypto ipsec transform-set TRANS_ESP_AES-128_MD5 esp-aes esp-md5-hmac
crypto ipsec transform-set TRANS_ESP_AES-128_MD5 mode transport
crypto ipsec transform-set TRANS_ESP_AES-128_SHA esp-aes esp-sha-hmac
crypto ipsec transform-set TRANS_ESP_AES-128_SHA mode transport
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec transform-set TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set TRANS_ESP_3DES_MD5 mode transport
crypto ipsec transform-set TRANS_ESP_AES256_MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set TRANS_ESP_AES256_MD5 mode transport
crypto ipsec transform-set TRANS_ESP_AES256_SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set TRANS_ESP_AES256_SHA mode transport
crypto ipsec transform-set TRANS_ESP_AES192_MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set TRANS_ESP_AES192_MD5 mode transport
crypto ipsec transform-set TRANS_ESP_AES192_SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set TRANS_ESP_AES192_SHA mode transport
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map Outside_dyn_map 10 set transform-set TRANS_ESP_3DES_MD5 TRANS_ESP_DES_MD5
TRANS_ESP_3DES_SHA TRANS_ESP_DES_SHA ESP-AES-128-SHA

ESP-AES-128-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5
crypto dynamic-map Outside_dyn_map 10 set security-association lifetime seconds 28800
crypto dynamic-map Outside_dyn_map 10 set security-association lifetime kilobytes 4608000
crypto dynamic-map Outside_dyn_map 20 set pfs
crypto dynamic-map Outside_dyn_map 20 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 20 set security-association lifetime seconds 28800
crypto dynamic-map Outside_dyn_map 20 set security-association lifetime kilobytes 4608000
crypto dynamic-map Outside_dyn_map 40 set pfs
crypto dynamic-map Outside_dyn_map 40 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 40 set security-association lifetime seconds 28800
crypto dynamic-map Outside_dyn_map 40 set security-association lifetime kilobytes 4608000

```

```

crypto dynamic-map management_dyn_map 20 set pfs
crypto dynamic-map management_dyn_map 20 set transform-set ESP-AES-128-SHA
crypto dynamic-map management_dyn_map 20 set security-association lifetime seconds 28800
crypto dynamic-map management_dyn_map 20 set security-association lifetime kilobytes 4608000
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set TRANS_ESP_3DES_SHA
TRANS_ESP_3DES_MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-3DES-SHA

ESP-3DES-MD5 ESP-AES-128-SHA
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set security-association lifetime seconds 28800
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set security-association lifetime kilobytes 4608000
crypto map Inside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map Inside_map interface Inside
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map Outside_map interface Outside
crypto ca trustpoint VPN-SE-strzelec-Com
enrollment terminal
fqdn none
subject-name CN=ASA1.strzelec.com,OU=IT,O=strzelec Sweden
AB,C=SE,St=Skane,L=Malmoe,EA=helpdesk_tms@strzelec.com
keypair VerisignKeystrzelecSweden
crl configure
crypto ca trustpoint Root-CA
enrollment terminal
keypair VerisignKeystrzelecSweden
crl configure
crypto ca trustpoint Verisign
keypair Verisign
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint0
enrollment terminal
fqdn ASA1.strzelec.com
subject-name CN=ASA1.strzelec.com,OU=IT,O=strzelec AB,C=DE,St=Bavaria,L=Nuremberg
keypair my.verisign.key
no client-types
crl configure
crypto ca certificate chain VPN-SE-strzelec-Com
certificate ca 70bae41d10defegh92934b638ca7b03ccbaf
3082023c 308201a5 021070ba e41d10d9 2934b638 ca7b03cc babf300d 06092a86
4886f70d 01010205 00305f31 0b300906 03550406 13025553 31173015 06035504
676e2e63 6f6d2f53 56525365 63757265 32303035 2d616961 2e636572 306e0608
2b060105 0507010c 04623060 a15ea05c 305a3058 30561609 696d6167 652f6769
66302130 1f300706 052b0e03 021a0414 4b6bb928 96060cbb d052389b 29ac4b07
8b210518 30261624 68747470 9f3ffab7 6f676f2e 76657269 7369676e 2e636f6d
040a130e 56657269 5369676e 2c20496e 632e3137 30350603 55040b13 2e436c61
73732033 20507562 6c696320 5072696d 61727920 43657274 69666963 6174696f
6e204175 74686f72 69747930 819f300d 06092a86 4886f70d 01010105 0003818d
00308189 02818100 c95c599e f21b8a01 14b410df 0440dbe3 57af6a45 408f840c
0bd133d9 d911cfec 02581f25 f72aa844 05aaec03 1f787f9e 93b99a00 aa237dd6
ac85a263 45c77227 ccf44cc6 7571d239 ef4f42f0 75df0a90 c68e206f 980ff8ac
235f7029 36a4c986 e7b19a20 cb53a585 e73dbe7d 9afe2445 75df0a90 ed0fa271
644c652e 816845a7 02030100 01300d06 092a8648 86f70d01 01020500 03818100
bb4c122b cf2c2600 4f1413dd a6fbfc0a 11848cf3 281c6792 2f7cb6c5 fadff0e8
95bc1d8f 75df0a90 cc73d8a4 c053f04e d626c076 01578192 5e21f1d1 b1ffe7d0
2158cd69 17e3441c 9c194439 895cdc9c 000f568d 0299eda2 90454ce4 bb10a43d
f032030e f1cef8e8 c9518ce6 629fe69f c07db772 9cc9363a 6b9f4ea8 ff640d64
quit

```

```

crypto ca certificate chain Root-CA
certificate ca 75337d9ab0e1233bae2d7de4469162d4
    3082049c 30820405 a0030201 02021075 337d9ab0 e1233bae 2d7de446 9162d430
    0d06092a 864886f7 0d010105 0500305f 310b3009 06035504 06130255 53311730
    676e2e63 6f6d2f53 56525365 63757265 32303035 2d616961 2e636572 306e0608
    2b060105 0507010c 04623060 a15ea05c 305a3058 30561609 696d6167 652f6769
    66302130 1f300706 052b0e03 021a0414 4b6bb928 96060ccb d052389b 29ac4b07
    8b210518 30261624 68747470 9f3ffab7 6f676f2e 76657269 7369676e 2e636f6d
    17301506 0355040a 130e5665 72695369 676e2c20 496e632e 311f301d 06035504
    0b131656 65726953 69676e20 54727573 74204e65 74776f72 6b313b30 39060355
    040b1332 5465726d 73206f66 20757365 20617420 68747470 733a2f2f 7777772e
    76657269 7369676e 2e636f6d 2f727061 20286329 3035312a 30280603 55040313
    21566572 69536967 6e20436c 61737320 33205365 63757265 20536572 76657220
    43413082 0122300d 06092a86 4886f70d 01010105 00038201 0f003082 010a0282
    01010095 c321128e 40c50d01 5f765e66 94d9732c 581922b8 c9fc7a39 902a7772
    7c1d3ef7 d855e3af 42cb8730 02dc5bac 70e6b844 b42b35eb 93d21705 7ecb46d6
    5c53a032 519d7464 58f90c9a 00ea5e44 496472f4 cd10e285 0af934ee b38866a9
    a5a45ad0 0e987f58 0d2b52bb 75df0a90 fab2487c 8ddb2d5f 0175a28d 063b8bb4
    6107c9be 2299f81b d1b55766 044d35f4 917196b5 9908259b 97c83af3 20b1dd9e
    980c4a63 b7a6cebo 01cef893 6af30c6e 9fb1e984 7b819841 e681dc3d 2ce7b46b
    e39efc08 16d7b3d5 b9661299 7c6d71c8 4dbecc70f e3fb37ad d5758721 6b86d044
    145a5479 75df0a90 c9b931cd 896158e1 d9760505 adf7b902 afa7fd47 91a22234
    5a31d102 03010001 a3820181 3082017d 30120603 551d1301 01ff0408 30060101
    ff020100 30440603 551d2004 3d303b30 39060b60 86480186 f8450107 1703302a
    676e2e63 6f6d2f53 56525365 63757265 32303035 2d616961 2e636572 306e0608
    2b060105 0507010c 04623060 a15ea05c 305a3058 30561609 696d6167 652f6769
    66302130 1f300706 052b0e03 021a0414 4b6bb928 96060ccb d052389b 29ac4b07
    8b210518 30261624 68747470 9f3ffab7 6f676f2e 76657269 7369676e 2e636f6d
    30290603 551d1104 223020a4 1e301c31 1a301806 03550403 1311436c 61737333
    43413230 34382d31 2d343530 1d060355 1d0e0416 04146fec afa0dd8a a4eff52a
    10672d3f 5582bcd7 ef253081 80060355 1d230479 3077a163 a461305f 310b3009
    06035504 06130255 53311730 15060355 040a130e 56657269 5369676e 2c20496e
    632e3137 30350603 55040b13 2e436c61 73732033 75df0a90 6c696320 5072696d
    61727920 43657274 69666963 6174696f 6e204175 74686f72 69747982 1070bae4
    1d10d929 34b638ca 7b03ccba bf300d06 092a8648 86f70d01 01050500 03818100
    c37e0846 5d9136cf 67dc7a7 afaf822 c38b0474 d3b160bc e6feb744 12815b31
    73146356 c6722ed1 1a03435c 380a504a 4dcddab6 19a8f499 0daf3f7 d8f17528
    65f66afe 9bf4bd52 d93fcfda 16cba59e 2e8e6652 783d26fa fe943688 4a955e2a
    4c19ef6e fa823f2d 03efd628 b33718cf 42b23421 6447d320 6b3a4cdc e603900c
quit
crypto ca certificate chain Verisign
certificate 49a36aaacd6b66bd26778f90bd875399f
    3082052c 30820414 a0030201 02021049 a36aacd6 b66bd267 78f90bd8 75df0a90
    0d06092a 864886f7 0d010105 05003081 b0310b30 09060355 04061302 55533117
    30150603 55040a13 0e566572 69536967 6e2c2049 75df0a90 1f301d06 0355040b
    13165665 72695369 676e2054 72757374 204e6574 776f726b 313b3039 06035504
    0b133254 65726d73 206f6620 75736520 61742068 74747073 3a2f2f77 77772e76
    65726973 69676e2e 75df0a90 72706120 28632930 35312a30 28060355 04031321
    676e2e63 6f6d2f53 56525365 63757265 32303035 2d616961 2e636572 306e0608
    2b060105 0507010c 04623060 a15ea05c 305a3058 30561609 696d6167 652f6769
    66302130 1f300706 052b0e03 021a0414 4b6bb928 96060ccb d052389b 29ac4b07
    8b210518 30261624 68747470 9f3ffab7 6f676f2e 76657269 7369676e 2e636f6d
    65636120 4142310b 30090603 55040b14 02495431 33303106 0355040b 142a5465
    726d7320 6f662075 73652061 74207777 772e7665 72697369 676e2e63 6f6d2f72
    70612028 63293030 311a3018 06035504 03141176 706e2e73 652e7465 6c656361
    2e636f6d 30819f30 0d06092a 864886f7 0d010101 75df0a90 8d003081 89028181
    00d6cb28 150e0e7f 75df0a90 86a357f3 b4a2b262 b46a6201 67e41d14 1c013683
    f4e151f8 75df0a90 f515f3e9 26275d5c b75bd5d1 7d55fcf3 8f4a1435 553e48ea

```

```

b35ac568 0f8e6b77 3a75c22c 261e5b9e 3c749fcf bac0a20d c14c3e49 2063eeeb
e8620521 471f27bf 044b7c0f edcb24bc 2386e8fa ac257aa6 48e8172b 53c6f5f2
eb020301 0001a382 01d23082 01ce3009 0603551d 13040230 00300b06 03551d0f
04040302 05a03044 0603551d 1f043d30 3b3039a0 37a03586 33687474 703a2f2f
53565253 65637572 652d6372 6c2e7665 72697369 676e2e63 6f6d2f53 56525365
63757265 32303035 2e63726c 30440603 551d2004 3d303b30 39060b60 86480186
f8450107 1703302a 30280608 2b060105 05070201 161c6874 7470733a 2f2f7777
772e7665 72697369 676e2e63 6f6d2f72 7061301d 0603551d 25041630 1406082b
06010505 07030106 082b0601 05050703 02301f06 03551d23 04183016 80146fec
afa0dd8a a4eff52a 10672d3f 5582bcd7 ef253079 06082b06 01050507 0101046d
676e2e63 6f6d2f53 56525365 63757265 32303035 2d616961 2e636572 306e0608
2b060105 0507010c 04623060 a15ea05c 305a3058 30561609 696d6167 652f6769
66302130 1f300706 052b0e03 021a0414 4b6bb928 96060cbb d052389b 29ac4b07
8b210518 30261624 68747470 9f3ffab7 6f676f2e 76657269 7369676e 2e636f6d
5b305930 57305516 09696d61 67652f67 69663021 301f3007 06052b0e 03021a04
148fe5d3 1a86ac8d 8e6bc3cf 806ad448 182c7b19 2e302516 23687474 703a2f2f
6c6f676f 2e766572 69736967 6e2e636f 6d2f7673 6c6f676f 2e676966 300d0609
2a864886 f70d0101 05050003 82010100 468848ac bcbf4c9c e6abc794 b48ce243
e2913c6d d5ae9f8d ed4e09f0 9edf0ddc ff6579af d0dc8410 8ad1be76 5bf8148d
2cb7aa5e a5b9907c aa56717e 979fd58b 2b4c5b41 75df0a90 3403b708 ff5ff816
9f3ffab7 044ae6f2 9f3ffab7 7c5f6e8c 8c98d8b5 63ef44db 5fdea346 b9214cc0
a3c0ce06 1e890c56 e179fd76 6876f6c 7e20fd53 db0f9a35 5b70da99 08d83c37
cad800c3 2892e4e5 2918de5a c89361d8 721299a9 31333995 c912bf68 384fdd34
c8827210 0246ec61 6108e431 3b633945 7f2cbe9c 858daabf 6345f7c7 96302bf5
a3f7a40c eaef8800 73ccb20c 2f78f878 4dcf22c5 d436859e 92deadd3 96b83584
c582a899 e5fcc8eb 4624655d 4a086ae0

quit
certificate ca 75337d9ab0e1233bae2d7de4469162d4
3082049c 30820405 a0030201 02021075 337d9ab0 e1233bae 2d7de446 9162d430
0d06092a 864886f7 0d010105 0500305f 310b3009 06035504 06130255 53311730
15060355 040a130e 56657269 5369676e 2c20496e 632e3137 30350603 55040b13
2e436c61 73732033 20507562 6c696320 5072696d 61727920 43657274 69666963
6174696f 6e204175 74686f72 69747930 9f3ffab7 35303131 39303030 3030305a
170d3135 30313138 32333539 35395a30 81b0310b 30090603 55040613 02555331
17301506 0355040a 130e5665 72695369 676e2c20 496e632e 311f301d 06035504
0b131656 65726953 69676e20 54727573 74204e65 74776f72 6b313b30 39060355
040b1332 5465726d 73206f66 20757365 20617420 68747470 733a2f2f 7777772e
76657269 7369676e 2e636f6d 2f727061 20286329 3035312a 30280603 55040313
21566572 69536967 6e20436c 61737320 33205365 63757265 20536572 76657220
43413082 0122300d 06092a86 4886f70d 01010105 00038201 0f003082 010a0282
01010095 c321128e 40c50d01 5f765e66 94d9732c 581922b8 c9fc7a39 902a7772
676e2e63 6f6d2f53 56525365 63757265 32303035 2d616961 2e636572 306e0608
2b060105 0507010c 04623060 a15ea05c 305a3058 30561609 696d6167 652f6769
66302130 1f300706 052b0e03 021a0414 4b6bb928 96060cbb d052389b 29ac4b07
8b210518 30261624 68747470 9f3ffab7 6f676f2e 76657269 7369676e 2e636f6d
980c4a63 b7a6ceb0 01cef893 6af30c6e 9fb1e984 7b819841 e681dc3d 2ce7b46b
e39efc08 16d7b3d5 b9661299 7c6d71c8 4dbec70f e3fb37ad d5758721 6b86d044
145a5479 39966956 c9b931cd 896158e1 d9760505 adf7b902 afa7fd47 91a22234
5a31d102 03010001 a3820181 3082017d 30120603 551d1301 01ff0408 30060101
ff020100 30440603 551d2004 3d303b30 39060b60 86480186 f8450107 1703302a
30280608 2b060105 05070201 161c6874 7470733a 2f2f7777 772e7665 72697369
676e2e63 6f6d2f72 70613031 0603551d 1f042a30 283026a0 24a02286 20687474
703a2f2f 63726c2e 76657269 7369676e 2e636f6d 2f706361 332e6372 6c300e06
03551d0f 0101ff04 04030201 06301106 09608648 0186f842 01010404 03020106
9f3ffab7 551d1104 223020a4 1e301c31 1a301806 03550403 1311436c 61737333
43413230 34382d31 2d343530 1d060355 1d0e0416 04146fec 9f3ffab7 a4eff52a
10672d3f 5582bcd7 ef253081 80060355 1d230479 3077a163 a461305f 310b3009
06035504 06130255 53311730 15060355 040a130e 56657269 5369676e 2c20496e

```

```

632e3137 30350603 55040b13 2e436c61 73732033 20507562 6c696320 5072696d
61727920 43657274 69666963 6174696f 6e204175 74686f72 69747982 1070bae4
1d10d929 34b638ca 7b03ccba bf300d06 092a8648 86f70d01 01050500 03818100
c37e0846 5d9136cf 67dc7a7 afafb822 c38b0474 d3b160bc e6feb744 12815b31
73146356 c6722ed1 1a03435c 380a504a 4dcddab6 19a8f499 0daf3f7 d8f17528
65f66afe 9bf4bd52 d93fcfda 16cba59e 2e8e6652 783d26fa fe943688 4a955e2a
4c19ef6e fa823f2d 03efd628 b33718cf 9f3ffab7 6447d320 6b3a4cdc e603900c
quit
crypto ca certificate chain ASDM_TrustPoint0
certificate 0a0ed5b299520c5473642611ad13a125
308204fc 308203e4 a0030201 0202100a 0ed5b299 520c5473 642611ad 13a12530
9f3ffab7 864886f7 0d010105 05003081 b0310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574 776f726b 313b3039 06035504
0b133254 65726d73 206f6620 75736520 61742068 74747073 9f3ffab7 77772e76
65726973 69676e2e 636f6d2f 72706120 28632930 35312a30 28060355 04031321
56657269 5369676e 20436c61 73732033 20536563 75726520 53657276 65722043
676e2e63 6f6d2f53 56525365 63757265 32303035 2d616961 2e636572 306e0608
2b060105 0507010c 04623060 a15ea05c 305a3058 30561609 696d6167 652f6769
66302130 1f300706 052b0e03 021a0414 4b6bb928 96060cbb d052389b 29ac4b07
8b210518 30261624 68747470 9f3ffab7 6f676f2e 76657269 7369676e 2e636f6d
9f3ffab7 652e6465 2e74656c 6563612e 636f6d30 819f300d 06092a86 4886f70d
01010105 0003818d 00308189 02818100 ae93a0a8 e68d35c5 52cb9183 142c11f4
c83181bf 6c475f93 c873536d 9f3ffab7 41b41215 7b458e59 ffa91a68 d1409b8c
bc72777d 8a1931c8 99d9c749 e6cb0408 f04f0930 d218181c 83754062 836141fb
e1a907f1 b94e2216 cae09e19 418f1349 4ad564d2 ab60f92d d12925a4 b3ca5725
b6ac5c77 971f2d64 8cb11762 237aab6f 02030100 01a38201 d3308201 cf300906
03551d13 04023000 300b0603 551d0f04 04030205 a0304406 03551d1f 043d303b
3039a037 a0358633 68747470 3a2f2f53 56525365 63757265 2d63726c 2e766572
69736967 6e2e636f 6d2f5356 52536563 75726532 3030352e 63726c30 44060355
1d20043d 303b3039 060b6086 480186f8 45010717 03302a30 2806082b 06010505
07020116 1c687474 70733a2f 2f777777 2e766572 69736967 6e2e636f 6d2f7270
61301d06 03551d25 04163014 06082b06 01050507 03010608 2b060105 05070302
301f0603 551d2304 18301680 146fecaf a0dd8aa4 eff52a10 672d3f55 82bcd7ef
25307906 082b0601 05050701 01046d30 6b302406 082b0601 05050730 01861868
7474703a 2f2f6f63 73702e76 65726973 69676e2e 636f6d30 4306082b 06010505
07300286 37687474 703a2f2f 53565253 65637572 652d6169 612e7665 72697369
676e2e63 6f6d2f53 56525365 63757265 32303035 2d616961 2e636572 306e0608
2b060105 0507010c 04623060 a15ea05c 305a3058 30561609 696d6167 652f6769
66302130 1f300706 052b0e03 021a0414 4b6bb928 96060cbb d052389b 29ac4b07
8b210518 30261624 68747470 9f3ffab7 6f676f2e 76657269 7369676e 2e636f6d
2f76736c 6f676f31 2e676966 300d0609 2a864886 f70d0101 05050003 82010100
86f65f54 41d6ed31 1cd8e0b0 bcfc2657 ede99e2f 1db3bf91 1d57801b 68509acf
c59f6b97 179cf37c de73ed71 ae39c1c3 3c95eff1 7814c966 37fcf49a 35175733
bf471ca5 a8fb0192 b09dc6f 74d76ffe e4e15ef0 c6babfed 8cf5f1f6 4e8dc4e5
cf68e5a2 f50eb677 e16514a6 1df1cf5f 13c362c6 66f3ed39 723e8a6c a3584d82
13a95b4c dc9160e6 ef7740ff 521e2387 80361c09 35aaecaf 498e1e8b 00c521bc
99871f1d e5abb9eb 25b3b852 657f3140 e8e6b1cb 6b53d4ff 9f3ffab7 e32f3949
38bd141c 3ece8b72 2538e52d f8bc3343 7f331c6b 775dfa5 7c220b6b 43cd5b15
1e6b347c 3e3c2b96 01dcbf24 223b8638 60eccf3e f5c869f6 adf5e1b8 e0
c60f50
quit
crypto isakmp enable Outside
crypto isakmp policy 10
authentication pre-share
encryption aes-256
hash sha
group 5

```

```

lifetime 86400
crypto isakmp policy 20
authentication pre-share
encryption aes-256
hash md5
group 5
lifetime 86400
crypto isakmp policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
crypto isakmp policy 40
authentication pre-share
encryption aes-256
hash md5
group 2
lifetime 86400
crypto isakmp policy 50
authentication pre-share
encryption aes-192
hash sha
group 5
lifetime 86400
crypto isakmp policy 60
authentication pre-share
encryption aes-192
hash md5
group 5
lifetime 86400
crypto isakmp policy 70
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400
crypto isakmp policy 100
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
crypto isakmp policy 110
authentication pre-share
encryption 3des
hash md5
group 2
lifetime 86400
crypto isakmp ipsec-over-tcp port 10000
no vpn-addr-assign aaa
no vpn-addr-assign dhcp
telnet timeout 5
ssh 217.153.251.3 255.255.255.255 Outside
ssh 217.153.148.192 255.255.255.224 Outside
ssh 81.210.64.192 255.255.255.240 Outside
ssh 10.82.4.0 255.255.254.0 Inside
ssh 10.220.0.0 255.255.0.0 Inside

```

```

ssh PL_WEB_ACCESS 255.255.255.128 Inside
ssh 10.21.128.0 255.255.255.192 Inside
ssh timeout 5
ssh version 2
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
vpn load-balancing
    interface lbppublic Outside
    interface lbprivate Inside
threat-detection basic-threat
threat-detection statistics
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate 200
ntp server 192.108.114.23 source Outside prefer
ntp server 62.119.40.98 source Outside prefer
tftp-server Inside 10.19.32.48 strzelecSEVPN2.cfg
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 rc4-md5
ssl trust-point ASDM_TrustPoint0 Outside
webvpn
    enable Outside
    enable Inside
    csd image disk0:/securedesktop-asa-3.2.1.103-k9.pkg
    csd enable
    svc image disk0:/anyconnect-win-2.1.0148-k9.pkg 2 regex "Windows NT"
    svc image disk0:/anyconnect-linux-2.1.0148-k9.pkg 3 regex "Linux"
    svc image disk0:/anyconnect-macosx-powerpc-2.1.0148-k9.pkg 4 regex "PPC Mac OS X"
    svc image disk0:/anyconnect-macosx-i386-2.1.0148-k9.pkg 5 regex "Intel Mac OS X"
    svc enable
    tunnel-group-list enable
group-policy DfltGrpPolicy attributes
    banner value Welcome to strzelec VPN Access (Sweden)
dns-server value 10.220.1.10 10.10.1.1
vpn-simultaneous-logins 5
vpn-idle-timeout none
vpn-tunnel-protocol IPSec 12tp-ipsec svc
split-tunnel-policy tunnelspecified
split-tunnel-network-list value strzelec_Internal
default-domain value strzelec.local
split-dns value strzelec.local
intercept-dhcp enable
webvpn
    svc keepalive none
    svc dpd-interval client none
    svc dpd-interval gateway none
    svc ask none default webvpn
group-policy SE_LS_GRP_Remote_Access_FULL internal
group-policy SE_LS_GRP_Remote_Access_FULL attributes
dns-server value 10.220.1.10 10.10.1.1
vpn-filter value FULL_ACCESS
vpn-tunnel-protocol IPSec 12tp-ipsec svc
split-tunnel-policy tunnelspecified
split-tunnel-network-list value strzelec_Internal
address-pools value Sweden_FULL_Access
group-policy SE_LS_GRP_Remote_Access_WEB internal
group-policy SE_LS_GRP_Remote_Access_WEB attributes
dns-server value 10.220.1.10 10.10.1.1
vpn-filter value FULL_ACCESS

```

```

vpn-tunnel-protocol IPSec l2tp-ipsec svc
split-tunnel-policy excludespecified
split-tunnel-network-list value Local_LAN
address-pools value Sweden_FULL_Access
group-policy DE_LS_GRP_Remote_Access_FULL internal
group-policy DE_LS_GRP_Remote_Access_FULL attributes
dns-server value 10.220.1.10 10.10.1.1
vpn-filter value FULL_ACCESS
split-tunnel-policy tunnelspecified
split-tunnel-network-list value strzelec_Internal
address-pools value Germany_FULL_Access
group-policy DE_LS_GRP_Remote_Access_WEB internal
group-policy DE_LS_GRP_Remote_Access_WEB attributes
dns-server value 10.220.1.10
vpn-filter value WEB_ACCESS
split-tunnel-policy excludespecified
split-tunnel-network-list value Local_LAN
address-pools value Germany_WEB_Access
group-policy IN_LS_GRP_Remote_Access_FULL internal
group-policy IN_LS_GRP_Remote_Access_FULL attributes
vpn-filter value FULL_ACCESS
split-tunnel-policy tunnelspecified
split-tunnel-network-list value strzelec_Internal
address-pools value India_FULL_Access
group-policy IN_LS_GRP_Remote_Access_WEB internal
group-policy IN_LS_GRP_Remote_Access_WEB attributes
vpn-filter value WEB_ACCESS
split-tunnel-policy excludespecified
split-tunnel-network-list value Local_LAN
address-pools value India_WEB_Access
group-policy PL_LS_GRP_Remote_Access_FULL internal
group-policy PL_LS_GRP_Remote_Access_FULL attributes
vpn-filter value FULL_ACCESS
vpn-tunnel-protocol IPSec l2tp-ipsec svc
split-tunnel-policy tunnelspecified
split-tunnel-network-list value strzelec_Internal
address-pools value Poland_FULL_Access
group-policy PL_LS_GRP_Remote_Access_WEB internal
group-policy PL_LS_GRP_Remote_Access_WEB attributes
vpn-filter value WEB_ACCESS
vpn-tunnel-protocol IPSec l2tp-ipsec svc
split-tunnel-policy excludespecified
split-tunnel-network-list value Local_LAN
address-pools value Poland_WEB_Access
group-policy FR_LS_GRP_Remote_Access_FULL internal
group-policy FR_LS_GRP_Remote_Access_FULL attributes
dns-server value 10.220.1.10 10.10.1.1
vpn-filter value FULL_ACCESS
split-tunnel-policy tunnelspecified
split-tunnel-network-list value strzelec_Internal
address-pools value FR_FULL_Access
group-policy FR_LS_GRP_Remote_Access_WEB internal
group-policy FR_LS_GRP_Remote_Access_WEB attributes
vpn-filter value WEB_ACCESS
split-tunnel-policy excludespecified
split-tunnel-network-list value Local_LAN
address-pools value France_WEB_Access
group-policy CN_LS_GRP_Remote_Access_WEB internal

```

```

group-policy CN_LS_GRP_Remote_Access_WEB attributes
  dns-server value 10.220.1.10
  split-tunnel-policy excludespecified
  split-tunnel-network-list value Local_LAN
  address-pools value China_WEB_Access
group-policy vistorm_RSA internal
group-policy vistorm_RSA attributes
  banner value Welcome to strzelec VPN access
  dns-server value 10.220.1.10
  vpn-filter value VISTORM_RSA
  vpn-tunnel-protocol IPSec l2tp-ipsec svc
  split-tunnel-policy tunnelall
  address-pools value VISTORM_RSA
username admin password 35gWgH1HLbEZoNy encrypted privilege 15
username strzelcu password QKNW93431v0soNl0 encrypted privilege 15
tunnel-group DefaultL2LGroup ipsec-attributes
  pre-shared-key L2strzelecTP
tunnel-group DefaultRAGroup general-attributes
  authentication-server-group AD-strzelec
  password-management
tunnel-group DefaultRAGroup webvpn-attributes
  group-alias TOKEN disable
tunnel-group DefaultRAGroup ipsec-attributes
  pre-shared-key Str3l3cki
tunnel-group DefaultRAGroup ppp-attributes
  authentication ms-chap-v2
tunnel-group DefaultWEBVPNGroup general-attributes
  authentication-server-group AD-strzelec
tunnel-group DefaultWEBVPNGroup webvpn-attributes
  customization strzelecCustomization
tunnel-group DefaultWEBVPNGroup ipsec-attributes
  pre-shared-key test
tunnel-group DefaultWEBVPNGroup ppp-attributes
  authentication ms-chap-v2
tunnel-group ipsec_all type remote-access
tunnel-group ipsec_all general-attributes
  authentication-server-group AD-strzelec
tunnel-group ipsec_all webvpn-attributes
  group-alias Active_Directory enable
tunnel-group ipsec_all ipsec-attributes
  pre-shared-key Str3l3cki
tunnel-group vistorm_rsa type remote-access
tunnel-group vistorm_rsa general-attributes
  authentication-server-group Test_SDI
  default-group-policy vistorm_RSA
tunnel-group vistorm_rsa webvpn-attributes
  group-alias Token_RSA enable
  group-alias Token_Vistorm disable
  group-alias Vistorm_RSA disable
tunnel-group vistorm_rsa ipsec-attributes
  pre-shared-key Str3l3cki
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters

```

```

message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
!
service-policy global_policy global
privilege cmd level 3 mode exec command perfmon
privilege cmd level 3 mode exec command ping
privilege cmd level 3 mode exec command who
privilege cmd level 3 mode exec command logging
privilege cmd level 3 mode exec command failover
privilege show level 5 mode exec command import
privilege show level 5 mode exec command running-config
privilege show level 3 mode exec command reload
privilege show level 3 mode exec command mode
privilege show level 3 mode exec command firewall
privilege show level 3 mode exec command interface
privilege show level 3 mode exec command clock
privilege show level 3 mode exec command dns-hosts
privilege show level 3 mode exec command access-list
privilege show level 3 mode exec command logging
privilege show level 3 mode exec command vlan
privilege show level 3 mode exec command ip
privilege show level 3 mode exec command failover
privilege show level 3 mode exec command asdm
privilege show level 3 mode exec command arp
privilege show level 3 mode exec command route
privilege show level 3 mode exec command ospf
privilege show level 3 mode exec command aaa-server
privilege show level 3 mode exec command aaa
privilege show level 3 mode exec command eigrp
privilege show level 3 mode exec command crypto
privilege show level 3 mode exec command vpn-sessiondb
privilege show level 3 mode exec command ssh
privilege show level 3 mode exec command dhcpd
privilege show level 3 mode exec command vpn
privilege show level 3 mode exec command blocks
privilege show level 3 mode exec command wccp
privilege show level 3 mode exec command webvpn
privilege show level 3 mode exec command uauth
privilege show level 3 mode exec command compression
privilege show level 3 mode configure command interface
privilege show level 3 mode configure command clock
privilege show level 3 mode configure command access-list
privilege show level 3 mode configure command logging

```

```
privilege show level 3 mode configure command ip
privilege show level 3 mode configure command failover
privilege show level 5 mode configure command asdm
privilege show level 3 mode configure command arp
privilege show level 3 mode configure command route
privilege show level 3 mode configure command aaa-server
privilege show level 3 mode configure command aaa
privilege show level 3 mode configure command crypto
privilege show level 3 mode configure command ssh
privilege show level 3 mode configure command dhcpcd
privilege show level 5 mode configure command privilege
privilege clear level 3 mode exec command dns-hosts
privilege clear level 3 mode exec command logging
privilege clear level 3 mode exec command arp
privilege clear level 3 mode exec command aaa-server
privilege clear level 3 mode exec command crypto
privilege cmd level 3 mode configure command failover
privilege clear level 3 mode configure command logging
privilege clear level 3 mode configure command arp
privilege clear level 3 mode configure command crypto
privilege clear level 3 mode configure command aaa-server
prompt hostname context
Cryptochecksum:cdf095343b9662f16cb6850e36416b4c9898
: end
```

10 Bibliografia

Książki

- [1] Joseph Steinberg, Timothy Speed, “SSL VPN” - Understanding, Evaluating, And Planning Secure, Web-Based Remote Access,. First Edition 2005
- [2] Amato Vito, Wayne Lewis, „Akademia sieci Cisco, pierwszy rok nauki”, wydanie rozszerzone, tłumaczenie Jakubowska Aleksandra, wydawnictwo Mikom 2002
- [3] P. Bardziński, R.Meryk, K.Zdrojewski, K.Turczyński „Akademia sieci Cisco, CCNA semestry 3 & 4”, wydanie III, wydawnictwo Mikom 2004
- [4] James Henry Carmouche, „IPsec Virtual Private Network Fundamentals”, Cisco Press 2006
- [5] Vijay Bollapragada, Mohamed Khalid, Scott Wainner, “IPsec VPN Design”, Cisco Press 2005
- [6] Gert De Laet, Gert Schauwers, "Network Security Fundamentals" Cisco Press 2004
- [7] Mark Lewis, ”Comparing, Designing, and Deploying VPNs” , Cisco Press 2006

Adresy internetowe

- [1i] <http://pl.wikipedia.org/wiki/>
- [2i] [http://cisco.netacad.net \(Kurs Cisco CCNA/CCNP\)](http://cisco.netacad.net)
- [3i] <http://www.ipsec.com>

Dokumenty techniczne

- [1d] RFC 2196, "Site Security Handbook" <http://www.ietf.org/rfc/rfc2196.txt>
- [2d] RFC 2409 „IKE” <http://www.ietf.org/rfc/rfc2409.txt>
- [3d] RFC 1492, "TACACS" <HTTP://www.ietf.org/rfc/rfc1492.txt>
- [4d] RFC 1321, "MD5" <HTTP://www.ietf.org/rfc/rfc1321.txt>
- [5d] RFC 2138, „RADIUS” <HTTP://www.ietf.org/rfc/rfc2138.txt>
- [6d] RFC 2284, "PPP Extensible Authentication Protocol (EAP)"
- [7d] RFC 2402, "AH" <http://www.ietf.org/rfc/rfc2402.txt>
- [8d] RFC 2406, "ESP" <http://www.ietf.org/rfc/rfc2406.txt>
- [9d] RFC 2401, „Security Architecture for the Internet Protocol"
<http://www.ietf.org/rfc/rfc2401.txt>

11 Słownik pojęć

ATM (ang. *Asynchronous Transfer Mode*) – technologia komunikacyjna, dzięki której można przesyłać dane. Jest to standard, który obecnie może być stosowany w sieciach lokalnych, miejskich, nawet rozległych. Informacja w tym standardzie przesyłana jest w postaci komórek o długości 53 bajtów (48 bajtów dane + 5 bajtów nagłówka).

BGP (ang. *Border Gateway Protocol*) – protokół trasowania międzydomenowego w sieciach opartych na protokole TCP/IP. Wykorzystuje algorytm wektora odległości. Routery BGP przechowują graf całej sieci, ale wymieniają między sobą tylko zmiany w tablicach.

Certyfikat X.509 - jest podstawą infrastruktury PKI, definiuje formaty danych oraz procedury związane z dystrybucją kluczy publicznych za pomocą certyfikatów podpisanych cyfrowo przez CA.

CHAP/ PAP /EAP (ang. *Challenge Handshake Authentication Protocol*) – Protokoły uwierzytelniające wykorzystujące protokół PPP:

PAP - Podczas uwierzytelniania – *nazwa użytkownika i hasło użytkownika* wysyłane są czystym tekstem

CHAP - W odpowiedzi na prośbę serwera uwierzytelniającego, klient zwraca zaszyfrowaną odpowiedź plus hasło czystym tekstem. Protokół ten jest bezpieczniejszy niż PAP, ale nie szyfruje danych.

EAP - Umożliwia urządzeniom pełniącym rolę NAC np. (ASA) pośredniczyć w procesie uwierzytelniania PPP do zewnętrznego serwera np. RADIUS.

DHCP (ang. *Dynamic Host Configuration Protocol*) to protokół komunikacyjny umożliwiający komputerom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski sieci.

Diffie-Hellman (Key Exchange) protokół kodowania z kluczem publicznym pozwalającym dwóm stronom na ustanowienie wspólnego tajnego klucza sesji w niezabezpieczonym kanale komunikacyjnym. Algorytm DH jest używany w IKE do określenia kluczy dla danej sesji. Jest też elementem wymiany kluczy Oakley.

DSL (ang. *Digital Subscriber Line*) technologia szerokopasmowego dostępu do Internetu. Standardowa prędkość pobierania danych od 128 kbit/s do 50Mbit/s, w zależności od zastosowanej technologii DSL. Dla odmiany technologii ADSL prędkość wysyłania danych (ang. *Upstream*) jest niższa od prędkości ich odbierania, natomiast symetryczna w przypadku technologii SDSL, HDSL.

Frame Relay - to sieć z komutacją pakietów, używana do łączenia odległych sieci lokalnych (LAN) oraz dostępu do Internetu. Informacja jest dzielona na ramki o zmiennej długości, które przenoszą dane między sieciami LAN, co pozwala na przekazywanie informacji między urządzeniami końcowymi sieci rozległych (WAN).

GPRS (ang. *General Packet Radio Service*) - jest technologią stosowaną w sieciach GSM do pakietowego przesyłania danych.

Haker (ang. *Hacker*) jest to pojęcie określające osobę o bardzo dużych, praktycznych umiejętnościach informatycznych, która swoją wiedzę nie zawsze wykorzystuje w słuszych celach, często nie zgodnie z prawem. Słowo Hacker jest terminem nieformalnym.

ISDN (ang. *Integrated Services Digital Network*) - Technologia sieci telekomunikacyjnych wykorzystująca infrastrukturę sieci PSTN do bezpośredniego udostępnienia usług cyfrowych. Połączenia ISDN zalicza się do grupy połączeń komutowanych.