Aspekty bezpieczeństwa w protokole IPv6

Security Aspects in IPv6 Protocol

Magdalena Haręźlak[1], Tomasz Długosz[2], Radosław Wróbel[3]

Streszczenie : Bezpieczeństwo przesyłanych danych w sieciach komputerowych jest współcześnie sprawą priorytetową. W pracy poddano analizie kwestie bezpieczeństwa protokołu IPv6. W tym celu przygotowano sieć i przeprowadzono szereg testów, które wykazały, że przejście z protokołu IPv4 do IPv6 nie wyeliminowało wszystkich niedociągnięć i błędów tkwiących w oprogramowaniu urządzeń.

Słowa kluczowe: bezpieczeństwo sieci, szyfrowanie danych, IPv6, Cisco

Abstract : Security of data transmitted over computer networks is a priority nowadays. In the paper results of analysis security of IPv6 protocol. Series of tests were done that showed that the transition from IPv4 to IPv6 has not eliminated all the shortcomings and errors inherent in software devices.
Keywords: network security, data encryption, IPv6, Cisco

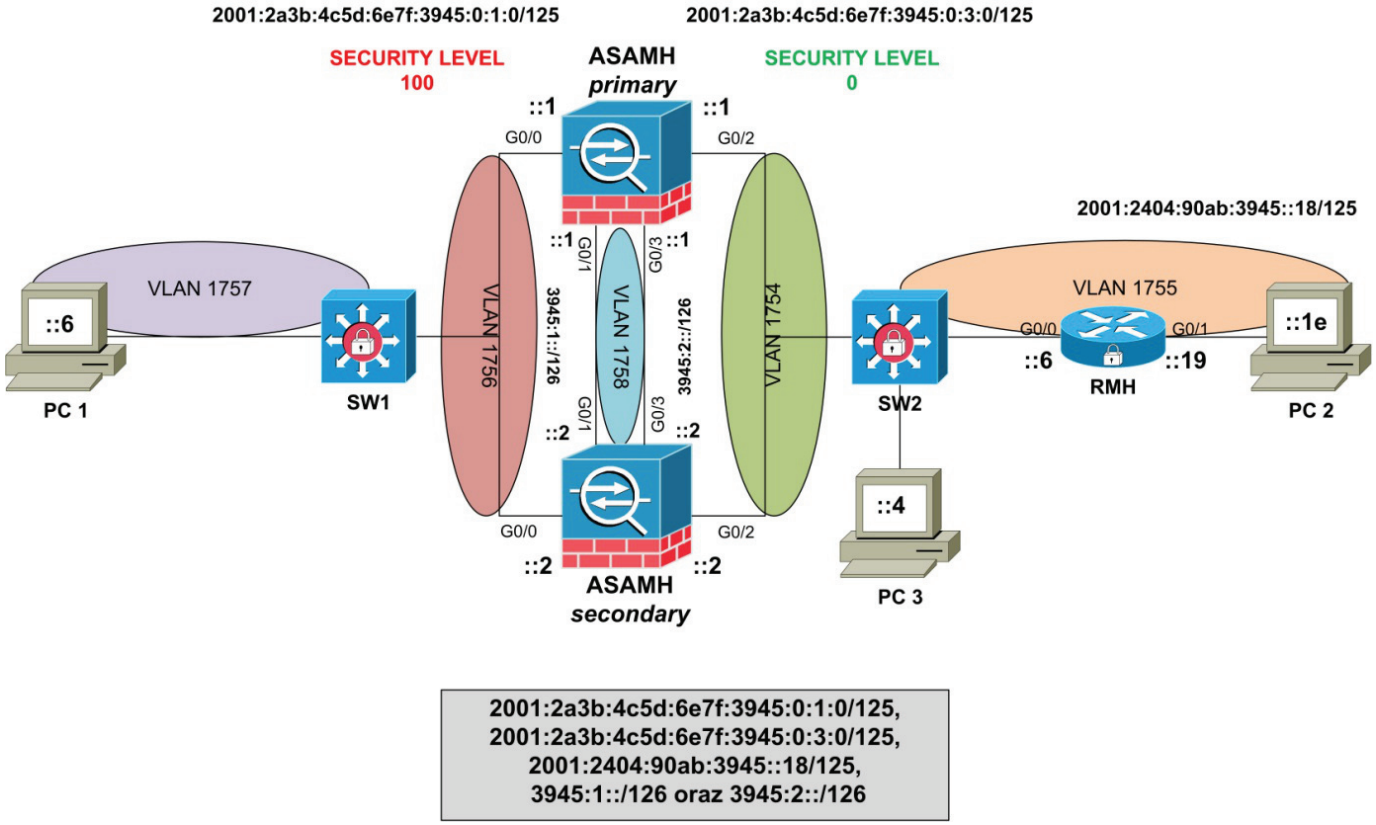
Wstęp

W czerwcu 2016 roku minęła 20 rocznica wprowadzenia dwóch pierwszych standardów RFC 4339 [1] oraz RFC 4472 [2] przedstawiających zalecenia dla dostawców internetowych dotyczące poprawnej konfiguracji **DNS** (ang. Domain Name Service) dla nowej wersji protokołu **IPv6** (ang. Internet Protocol version 6), opisanego w RFC 2460 [3]. Przez ostatnie dwa lata diametralnie wzrosło zainteresowanie owym protokołem, jego implementacją oraz wbudowanymi mechanizmami bezpieczeństwa. Znaczna większość nowych sprzętów komputerowych i sieciowych została przystosowana do konfiguracji IP w wersji 6 wraz z, wprowadzanymi przez lata, kompatybilnymi standardami. Określany jest potocznie mianem protokołu IP następnej generacji (ang. IP Next Generation), który ma rozwiązywać wiele mankamentów jego poprzednika IPv4, takich jak: ograniczona skalowalność i elastyczność, problemy mobilności oraz jakości bezpieczeństwa [4]. Podstawowa wiedza dotycząca architektury i konfiguracji IPv6 stała się dużym atutem w świecie informatycznym.

Metody zapewniania bezpieczeństwa sieci z wykorzystaniem protokołu IPv6

W związku z powyższym przeprowadzono analizę możliwości osiągnięcia zabezpieczonej sieci, w pełni skonfigurowanej, przy użyciu IP w wersji 6, na urządzeniach firmy Cisco, jednego z kluczowych potentatów w pracy nad standaryzacją i wdrażaniu protokołu internetowego v6 (rys. 1). Wykorzystano dwie zapory sieciowe Cisco ASA5520 (ASAMH) połączone redundantnymi łączami awaryjnymi, w trybie pracy *Active/Standby Failover*, router Cisco 2851 (RMH) oraz dwa przełączniki Cisco Catalyst 6506-E (SW). Do weryfikacji skorzystano z trzech komputerów, z zainstalowanym systemem operacyjnym Windows 7, narzędziem analizy pakietów *WireShark* oraz *Network Shell*, które monitoruje nawiązane połączenia TCP, statystyki, tablice routingu oraz sąsiadów, a także umożliwia naprawę zaistniałych problemów, czy zmianę reguł wbudowanej zapory sieciowej [5].

1. Studentka, Wrocławska Wyższa Szkoła Informatyki Stosowanej, ul. M. Lutra 4, 54-239 Wrocław
2. Wrocławska Wyższa Szkoła Informatyki Stosowanej, e-mail: tdlugosz@horyzont.eu
3 Instytut Konstrukcji i Eksploatacji Maszyn, Politechnika Wrocławska



Rys. 1. Topologia zabezpieczonej, zaprojektowanej sieci IPv6

Zgodnie z założoną topologią, podstawową konfiguracją i manualną adresacją sieci z wykorzystaniem jedynie adresów typu *Global*, odpowiadającą założeniu standardu RFC 4291 [6] o architekturze adresacji dla IPv6, z sukcesem osiągnięto zbieżność oraz przyległość wszystkich sąsiadów.

Nie byłoby to możliwe, gdyby nie dodatkowe usługi zaktualizowanego protokołu **ICMPv6** (ang. Internet Control Message Protocol version 6), czyli zbiór komunikatów protokołu **NDP** (ang. Neighbor Discovery Protocol), zastępujących poprzednie rozwiązania **ARP** (ang. Address Resolution Protocol) [7]. Wymiana wiadomości odpytywania **ND** *(*ang. Neighbor Discovery) *Solicitation* oraz przedstawiania ND *Advertisement*, posiada niewiarygodną wadę i może narazić sieć na ryzyko przechwycenia wszystkich adresów sieciowych oraz fizycznych **MAC** (ang. Media Access Control address). Dzieje się tak, ponieważ każdy wpis definiowanych list kontroli dostępu **ACL** (ang. Access Control List) dla IPv6 zawiera ukryte przepisy pozwalające na dostęp protokołom NDP. Proces ND korzysta z usług warstwy sieciowej, dlatego domyślnie pozwalają na odkrycie, wysłane i odebrane, na interfejsie, pakietu IPv6 [8]. Nie istnieje także możliwość całkowitego wyłączenia wiadomości, ponieważ musi dojść do choć jednej takiej wymiany, aby uzyskać wykrycie relacji oraz przekazać tymczasowy adres docelowy, w celu osiągnięcia przyległości. Jednakże, tutaj pojawia się system **DAD** *(*ang. Duplicate Address Detection) poszukujący dublujące się adresy, gdy w przypadku wykrycia duplikatów system poinformuje administratora, który będzie od razu miał świadomość, iż spowodowane jest to próbą włamania lub błędną konfiguracją [9].

Dodatkowo należy pamiętać o kolejnym mechanizmie ICMPv6 – **SLAAC** (ang. Stateless Address Autoconfiguration), który bazuje na adresach warstwy łącza danych, automatycznie podsumowując adresy w węzły oraz generuje adresy lokalne *Link-local*, na podstawie kombinacji prefiksu i adresu MAC[9]. Dodatkowe adresy można odnaleźć oraz zweryfikować po wprowadzeniu komend dotyczących informacji o interfejsach, czy tablicy routingu, wśród podłączonych bezpośrednio dróg. W powyższej topologii odnaleziono następujące grupowe adresy *Multicast – Link-local* fe80::/10, Global ff00::/8 oraz podgrupy ff02::2, ff02:1. Dlatego zrezygnowano z automatycznej konfiguracji wszystkich adresów oraz **DHCP** (ang. Dynamic Host Configuration Protocol), aby ograniczyć pojawienie się większej ilości podsumowań adresów.

Uznano, iż szczególnym problemem dla bezpieczeństwa IPv6 jest luka, jaką stanowi całość architektury adresacji, gdyż jeden interfejs posiada przypisanych kilka adresów. Adresacja *Link-local*, nie stanowi, aż tak dużego zagrożenia, ponieważ można wykluczyć ją z użytku w celach przesyłu, czy zablokować jego przekazywanie. Aczkolwiek *Multicast* może rozgłaszać te podsumowane węzły i adresy, a sieci oraz interfejsy, będą przez nie dostępne, szczególnie przez adres do monitorowania FE02::1. Stanowią także duże zagrożenie ich wykorzystania, przykładowo do ataków typu **DoS** (ang. Denial of Service), **DDoS** (ang. Distributed DoS) [8]. Blokada odpowiadania na zapytania adresów *Multicast* albo całkowite odrzucenie ich przepuszczania zmniejsza ryzyko, tak jak i zapory sieciowe w połączeniu *Failover* [10].

Każde z urządzeń zostało zabezpieczone oraz spełnia prawidłowo swoją funkcję, wymagania i założenia o zabezpie-

czeniach według instytucji **NIST** (ang. National Institute of Standards and Technology) [11]. W razie awarii aktywnej zapory sieciowej, kolejna znajdująca się w stanie czuwania, będąca w pełnej gotowości na przejęcie pełnienia funkcji aktywnej, zostanie aktywną po osiągnięciu limitu czasowego nieotrzymania pakietu „HELLO" z jednego łącza pomiędzy nimi [10]. Redundancja zarówno urządzeń, jak i połączeń zapewnia zwiększenie zabezpieczenia, ponieważ w razie awarii istnieje zapasowe łącze. Przedstawiona topologia, może spełnić wycinek wewnętrznej sieci lub połączenie dwóch odrębnych np. przedstawionym łączem tunelowym, po przez połączenie internetowe.

Implementacja sieci **VLAN** (ang. Virtual Local Area Network), czyli wykorzystanie fizycznych portów przełączników, wirtualne przydzielenie, aby logicznie przełączać ruch sieciowy pomiędzy urządzeniami, zmniejsza ryzyko ataku *Man-in-the middle*. Mechanizmy generowania statystyk, logów oraz alertów, wspierają szybką reakcję w przypadku wykrycia zagrożeń, czy niechcianego ruchu.

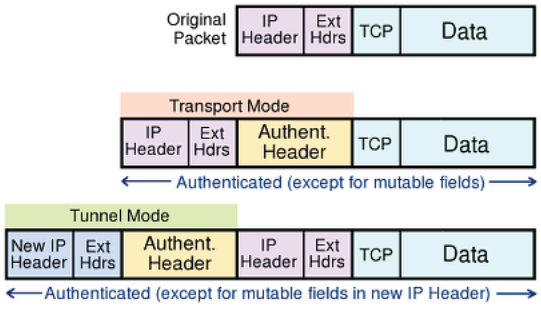
Rozbudowa określona jest standardem RFC 6564 [12], jako nagłówek **EH** (ang. Extension Header), który znajduje się w rozszerzalnym „Następnym nagłówku" stanowi najpotężniejsze narzędzie uwierzytelnienia [13]. Platforma urządzeń Cisco została zaprojektowana tak, aby niezależnie od jej roli, cały proces przetwarzania nagłówków rozszerzeń IP w wersji 6 kompletnie nie wpływało na ich wydajność. Jedynym ograniczeniem platform jest ich zaprojektowanie, które są przystosowane do odczytu tych nagłówków o wielkości 64-bajtów danych, a gdy rozmiar ten zostanie przekroczony, pakiet jest przekierowany ze sprzętowej do oprogramowania **CPU** (ang. Central Processing Unit) *Line-Card*. Należy także zrozumieć, w jaki sposób nagłówki oraz sam pakiet jest odczytywany przez router, iż w jego komponentach najważniejszą rolę odgrywa procesor CPU. Zależnie od użytych protokołów w konfiguracji, istnieje różnica w ich odczytywaniu i kolejności. W przypadku routingu przeskok – przeskok nagłówek EH musi być przetworzony w całości przez wszystkie urządzenia sieciowe, co powoduje, że to rozszerzenie musi być przetworzone, jako pierwsze w kolejności [13].

Mechanizm **IPSec** (ang. Internet Protocol Security) został wbudowany w IPv6, jako obowiązkowy implementacji bezpieczeństwa przy konfigurowania zdalnego dostępu, wirtualnej sieci prywatnej **VPN** (ang. Virtual Private Network) lub najzwyczajniej do zabezpieczenia warstwy sieciowej [14]. Mechanizm ten jest zespołem protokołów i umożliwia systemowi w warstwie IP wyboru wymaganych protokołów bezpieczeństwa **SA** (ang. Security Association), zastosowanych algorytmów oraz rozmieszczenia kluczy kryptograficznych, czyli zapewnia ochronę integralności, uwierzytelnienie nadawcy, szyfrowanie, poufność przesyłanych danych [8]. Zapewnia również ograniczoną poufność przepływu ruchu maskując rozmiar pakietu, utrudniając tym ataki polegające na nasłuchiwaniu, szpiegowaniu. Sprawdza także, czy pakiet nie został wcześniej przetwarzany, ponieważ ma możliwość wykrycia i odrzucenia takiego pakietu przez funkcję *Antireplay* [14]. Negocjacja oraz zarządzanie może odbywać się na bazie nawiązania sesji poprzez algorytm **DH** (ang. Diffie-Hellman), a także na podstawie prywatnych kluczy lub IKE (ang. Internet Key Exchange), czyli standardowy protokół do zarządzania niezabezpieczonymi kluczami internetowymi [15]. Wśród zespołu protokołów IPSec wyróżnia się dwa zasadnicze, odpowiedzialne za rozszerzenia nagłówków, możliwych do wykorzystania w dowolnej ilości:

1. **AH** (ang. Authentication Header) – nagłówek uwierzytelnienia, zapewnia identyfikację źródła na podstawie podpisu i integralność danych przesyłanych między dwoma systemami. Sprawdza, czy komunikat przesłany między routerami, nie uległ modyfikacji. Sam w sobie nie zapewnia on szyfrowania pakietów.
2. **ESP** (ang. Encapsulation Security Payload) – nagłówek zapewnia poufność i uwierzytelnienie, szyfrując pakiet IP, aby dane dotyczące źródła i celu były tajne. Wykorzystywane również, jako zabezpieczenie komunikacji IP pomiędzy dwoma komputerami. Są one ignorowane przez pośrednie urządzenia sieciowe podczas przekazywania ruchu w sieci [13].

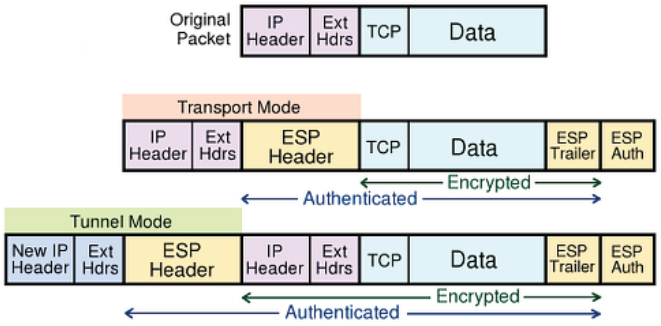
W czasie wspólnej integracji z IPSec zwiększa się jego elastyczność i łatwość konfiguracji. Wymaganiem poprawnej konstrukcji, jak i nawiązania takiego połączenia jest indywidualny dobór parametrów SA między innymi: wybór trybu pracy, rodzaj stosowanych algorytmów kryptograficznych, klucze oraz IP, z którym ma nawiązać przyległość transmisji wykorzystując protokół IPSec. Całość zapisywana jest w bazie **SAD** (ang. Security Association Database) oraz **SPI** (ang. Security Parameters Index), dzięki której pakiety te będą odbierane oraz wiadomo, w jaki sposób pakiety IPSec są zabezpieczone. Jeżeli bazy te są identyczne po jednostronnym zainicjowaniu połączenia, VPN powstanie i będzie sukcesywnie wykorzystywany. Może być on skonfigurowany, w dwóch trybach:

1. Transportowy – odpowiedzialny za ochronę oryginalnej zawartości nagłówków IP, wykorzystywany wewnątrz sieci np. w sieciach lokalnych.



Rys. 2. Wygląd nagłówka IPv6 z zastosowaniem protokołu AH w dwóch trybach IPSec [16]

2. Tunelowy – odpowiedzialny za ochronę nagłówków IP podczas enkapsulacji całości w nowy nagłówek, do użytku w połączeniach między sieciowych, przechodzących przez inną sieć np. Internet.



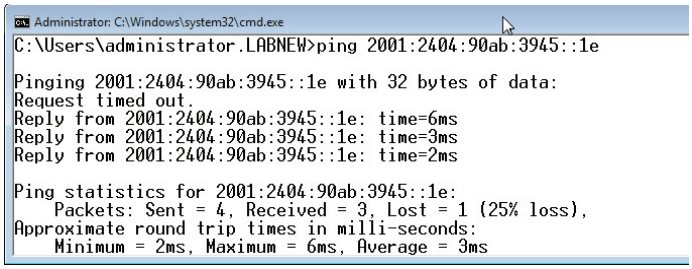
Rys. 3. Wygląd nagłówka IPv6 z zastosowaniem protokołu ESP w dwóch trybach IPSec [16]

Typ VPN, dostępny niezależnie od wersji oprogramowania na **ASA** (ang. Adaptive Security Appliance), to *Site-to-Site* oraz zdalny dostęp w oparciu o **SSL** (ang. Secure Socet Layer). Zastosowano jednak łącze tunelowe typu Site-to-Site. Najważniejszym aspektem, aby rozpocząć konfigurację IPSec, czy VPN, jest upewnienie się, iż istnieje stabilizacja i przyległość wszelkich łącz lokalnych, od początku do końca, według zaleceń (*ang. established end-to-end*) [17]. Pierwsza próba nawiązania komunikacji przy użyciu szyfrowanego łącza, została udaremniona, przez spowodowanie całkowitego rozłączenia połączenia, między ASA, a routerem. Pomogło wykrycie błędu CSCux42019 przez firmę Cisco, iż w obecnie zainstalowanym oprogramowaniu na ASA istnieją luki w zabezpieczeniach z wykorzystaniem IKE, umożliwiających na nawiązanie połączenia osób nieautoryzowanych, zapychając łącze nieznanym ruchem **UDP** (ang. User Datagram Protocol) [18]. Również błędy mogły być powodem różnic w bazie danych SA, powodując problemy przy próbie nawiązania połączenia VPN. Korzystając z przewodnika aktualizacji oprogramowania (*ang. upgrade guide*) zainstalowano nową wersję na obydwie zapory sieciowe ASA rozwiązując problem niespójności SAD [19].

Prywatna wirtualna sieć oparta została na polityce nr 10, zastosowaniu tych samych algorytmów kryptograficznych **ESP** (ang. Encapsulating Security Payload) i **AES** (ang. Advanced Encryption Standard) 128, szyfrów **SHA** (ang. Secure Hash Algorithm) 256 i **HMAC** (ang. keyed-Hash Message Authentication Code), hasła oraz sparowaniu ze sobą zastosowanych parametrów grupą nr 2 Diffiego-Hellmana [17]. Listy kontroli dostępów, dla adresów przynależnych do wyjściowych interfejsów, umożliwiły negocjacje i połączenie. Natomiast wprowadzono wyjątkową translacje adresów (*ang. Exemption NAT*) nie powodując zmiany adresu: adres źródłowy i docelowy jest zmieniany na dokładnie ten sam adres. Z powodu wielu błędów podczas weryfikacji pakietów, spowodowanych brakiem translacji, zdecydowano się na skonfigurowanie wyjątkowego NAT. Po mimo, iż nie powinno się go stosować dla IPv6, ASA posiada pewne ograniczenia oraz przeprowadza inspekcję NAT niezależnie od wersji protokołu. Zaimplementowano także mapę, którą przypisano do przylegających interfejsów. Wiedząc, iż ASA pracująca w trybie routera wykorzystywać będzie odpytywanie i rozgłaszanie informacji o sobie poprzez ND, za pośrednictwem protokołu ICMPv6 zastosowano ich blokadę na interfejsie z poziomem zabezpieczeń, określonym w konfiguracji, jako zero. W takim przypadku to router będzie pełnił docelową funkcję rozsyłania anonsu i weryfikacji, czy jego sąsiedzi nadal nimi są.

Analiza ruchu sieciowego i skuteczności zabezpieczeń

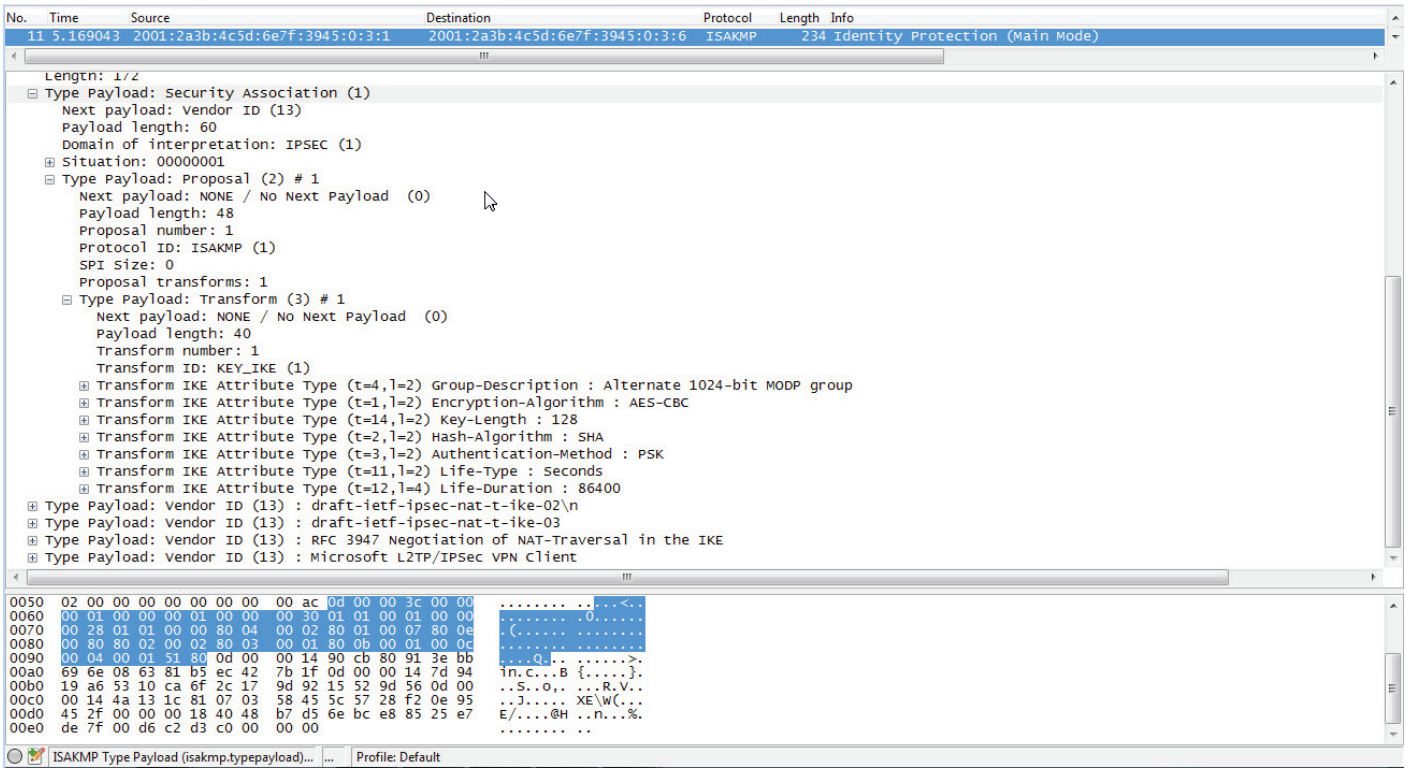
W sieci pokazanej na rys. 1 zaimplementowano konfigurację IPSec, skonfigurowano tunel na interfejsach pomiędzy routerem a ASA, i przeprowadzono pierwszy przesył wiadomości ICMP między PC1 i PC2, aktywując tym samym łącze tunelowe (rys. 4).



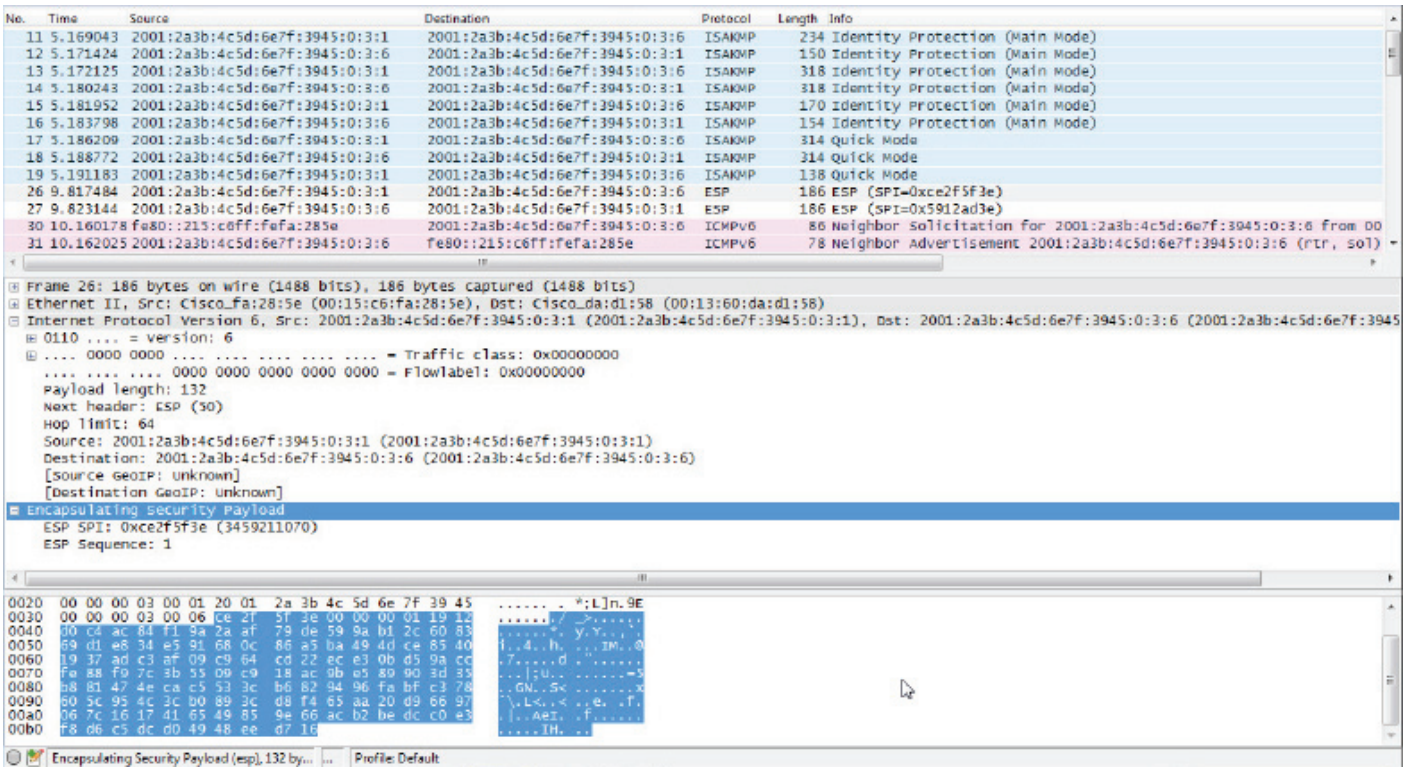
Rys. 4. Pierwszy przesył ICMP przez VPN na PC1 do PC2

Analiza przechwyconych pakietów ruchu IPv6 na ASA jest bardzo utrudniona, co jest spowodowane wciąż nierozwiązanym problemem odnalezionego błędu CSCtn09836. Alternatywą jest zastosowanie *access-list* odpowiedniej dla ruchu tej wersji, IP, którą można wykorzystać, jako przechwycenie ruchu przechodzącego dzięki skonfigurowanej liście kontroli dostępu [20], co też zostało zrobione.

Pierwszym pakietem nawiązania tunelu jest ISAKMP (ang. Internet Security Association and Key Management Protocol), który zawiera całość polityki zabezpieczeń, jaką wprowadzono zarówno do konfiguracji zapory, jak i routera (rys. 5). Spowodowało to nie dostarczenie pierwszego pakietu *request* i opóźnienia w dostarczeniu.

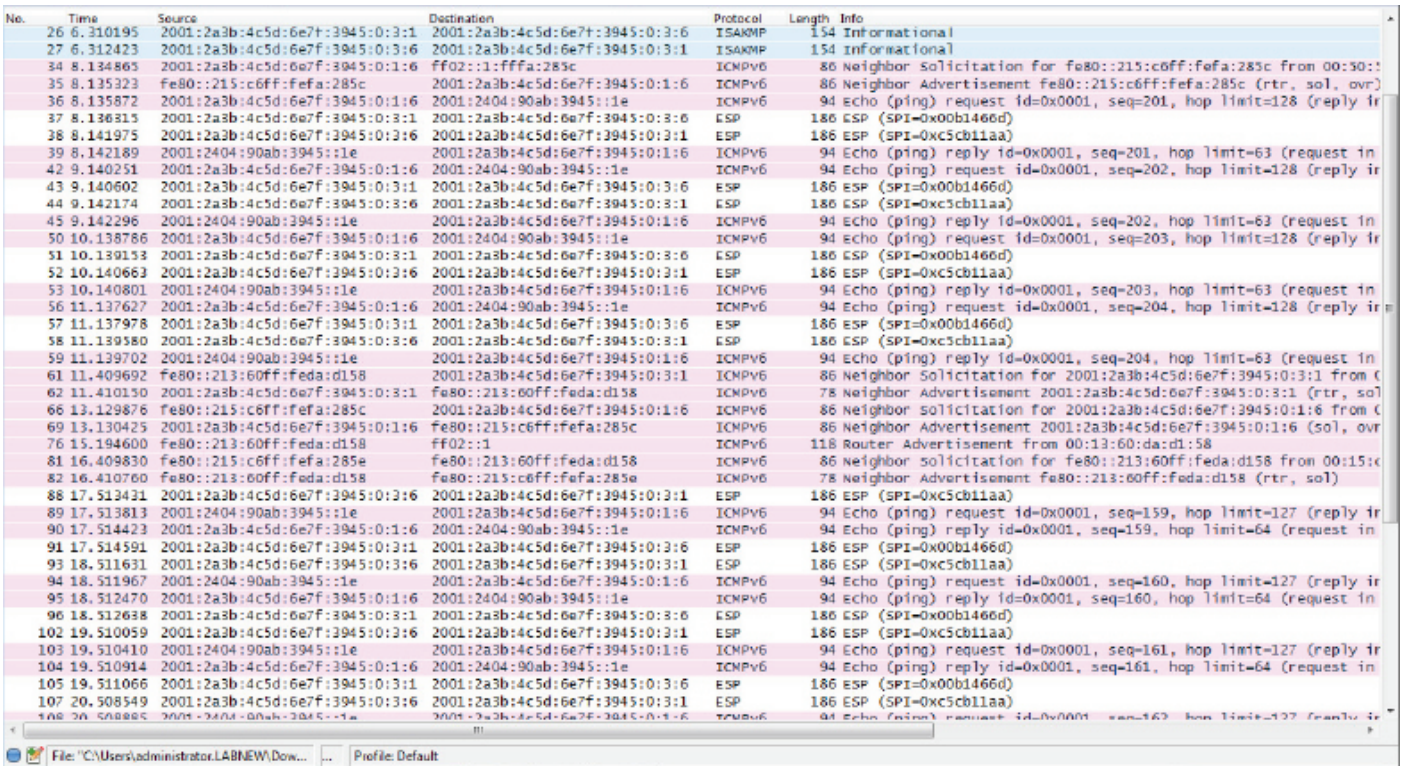


Rys. 5. Pierwsze nawiązanie ISAKMP

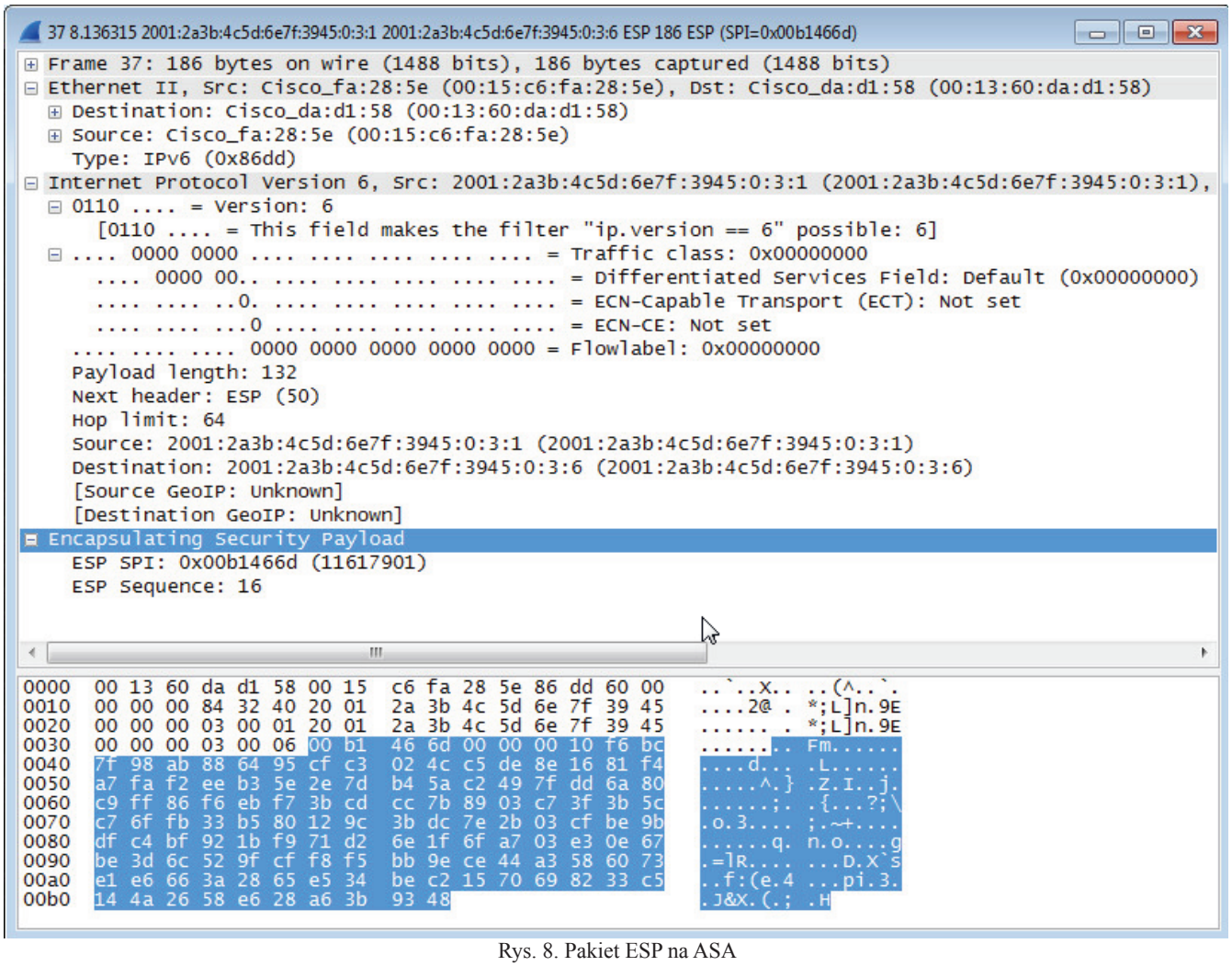


Rys. 6. Pierwszy pakiet ESP o numerze sekwencyjnym 1

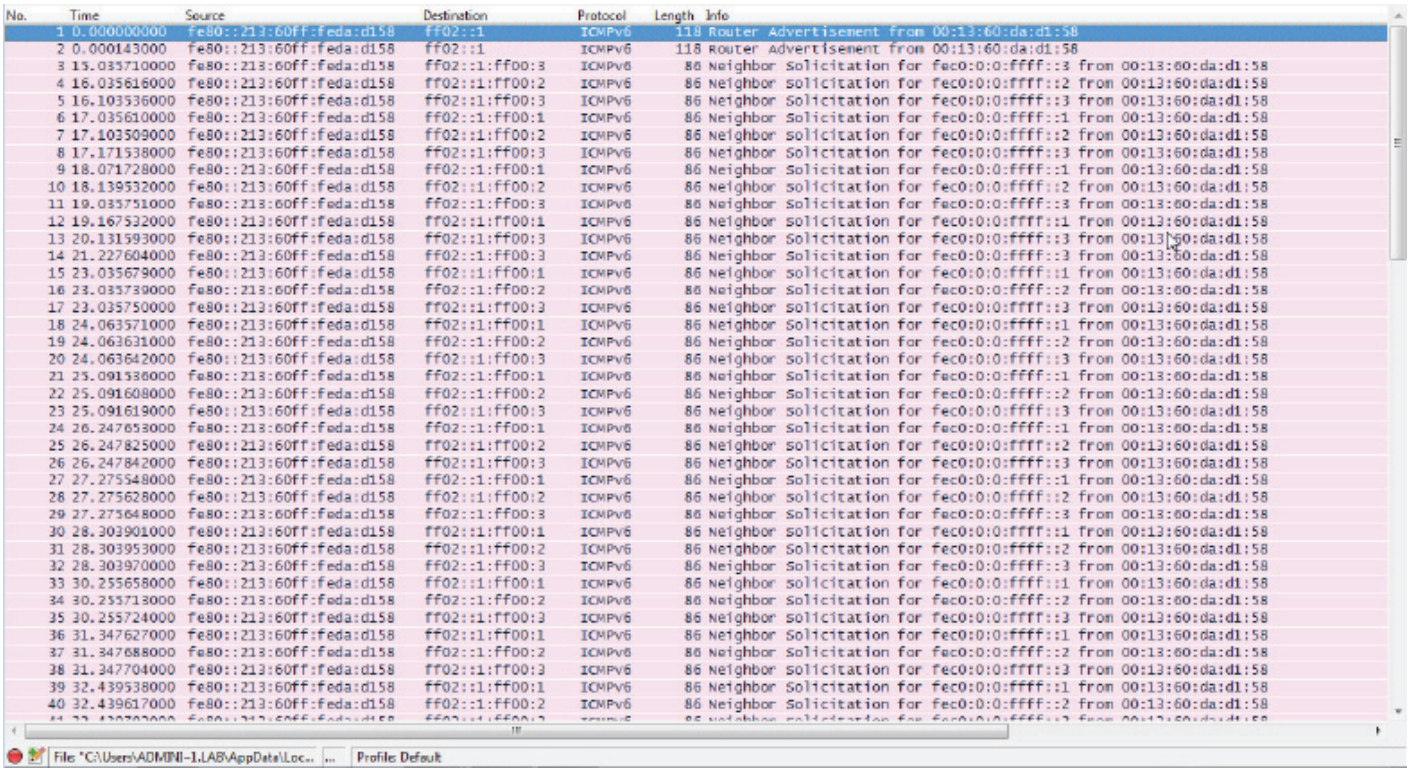
Kolejnym pakietem jest ESP, widoczny na rysunkach
rys. 6 – rys. 9.



Rys. 7. Przejście ping z PC1 do PC2 i odwrotnie na ASA



Rys. 8. Pakiet ESP na ASA



Rys. 9. Perspektywa ping PC1-PC2 na PC3

Pakiet, po mimo poddaniu zmiany w ESP, dotarł nienaruszony do PC2 o tej samej wartości.

Wszelkie dane przesyłane pomiędzy routerem a ASA były zaszyfrowane, zabezpieczone przed niepożądanym odczytem, nawet w razie przechwycenia. Nie posiada to znaczącego wpływu na prędkość przesyłu, jedynie pierwszy pakiet może zostać przesłany z niewielkim opóźnieniem, przez wzgląd na wymogi spełnienia wielu warunków oraz weryfikacji, aby został dopuszczony do celu.

Dzięki architekturze ASA, użytkownicy hostów nie są w stanie sprawdzić prawdziwej trasy, ponieważ interfejs przeciwległy na zaporze sieciowej jest nieosiągalny do przeprowadzenia analizy „*traceroute*", czy „*ping*", sądzą, iż ich następnym przeskokiem jest bezpośrednio router.

Wprowadzenie lokalnej bazy autoryzowanych użytkowników oraz ich ograniczony dostęp, poprzez listy kontroli i politykę zabezpieczeń, skutecznie udaremniają próbę nawiązania połączenia nieznanym użytkownikom, nieposiadającym poświadczenia umożliwiających bycie autoryzowanym. Stwierdzono, iż wszystko opiera się o podstawowe zabezpieczenia między innymi spójność, integralność i poufność. Gdyby wykorzystane hasło trafiłoby w niepowołane ręce, całość zabezpieczeń byłaby bez znaczenia. Narażone są wówczas zarówno dane znajdujące się na urządzeniu, konfiguracja urządzeń, czy VPN. Pomimo zastosowania szyfrowania haseł, należy pamiętać, że nie wolno udostępniać ich osobom trzecim, ani przechowywać w miejscu ogólnodostępnym. Stosownym rozwiązaniem jest także stosowanie wielu długich i trudnych, również różnych od siebie, przypisanych do wykorzystywanych technologii i hierarchii użytkowników.

W przypadku pakietów IP w wersji 6, odmienionych przez protokół IPSec, bardziej rozważnym rozwiązaniem między odległymi urządzeniami sieciowymi jest tryb tunelowy, ponieważ otrzymujemy wygenerowany dodatkowy, nowy nagłówek, znajdujący się na początku całego szyku. Stanowi to solidne zabezpieczenie przed uzyskaniem informacji chronionych w pakiecie IP takich jak adres fizyczny MAC, adres *Link-local*. Natomiast, w sieci lokalnej dla połączenia host-host lub komputer - komputer najlepszy jest tryb transportowy, ponieważ ułatwia to oszacowanie urządzeniom sieciowym, na podstawie niezmienionego nagłówka IP, jego docelowe przeznaczenie, dodając jedynie szyfrowanie. Jednakże istnieje pewne ryzyko, iż cały ruch sieciowy jest widoczny, widać źródło i cel pakietów.

Podsumowanie

Po mimo ciągłego wsparcia producentów i naprawiania odnalezionych błędów dla wersji 4, nie udało się ominąć ich w oprogramowaniu wspierającego nowy protokół wersji 6. Natomiast, istnieje wiele przesłanek, iż będzie możliwość zmiany i zwiększenia bezpieczeństwa omijając wady w nowszej wersji.

Uznano, iż większość problemów związanych z bezpieczeństwem zostałoby rozwiązanych, poprzez wprowadzenie techniki kryptografii asymetrycznej, opartej na matematycznej krzywej eliptycznej **ECC** (ang. Elliptic Curve Cryptography). Standard szyfrowania opisany jest jako skuteczną, wydajniejszą, nowszą alternatywą dla standardowej kryptografii. Oferuje bezpieczeństwo tego samego poziomu, ale na mniejszych zasobach [15]. Również ciekawym aspektem było by wprowadzenie najnowszej wersji **TLS** (ang. Transport Layer Security) 1.3, która umożliwiałaby lepsze wykorzystanie z kryptografii opartej na

krzywej eliptycznej ECC, stabilizację zabezpieczenia między dwoma sieciami, wymianę parametrów kryptograficznych bez widocznych danych. Niestety nie udało się jeszcze tego wprowadzić i nadal jest w fazie projektowej, opisywane w dokumencie [21]. Planowana jest ta zmiana, przez wzgląd na wiele luk w powszechnie używanym SSL 3.0, z którego obecnie się rezygnuje i zaleca wyłączać, ponieważ naraża się swoją sieć, klientów, serwery na przesył informacji o użytych zabezpieczeniach [21].

Nieodłączny nagłówek rozszerzalny EH protokołu IPv6 można uznać za potężne narzędzie, które można dostosować do przyszłych wymagań i potrzeb protokołów sieciowych, między innymi do wprowadzenia powyższego projektu, w celu usprawnienia i zabezpieczenia podstawowych funkcji oraz usług. Wykorzystując zabezpieczony nagłówek ESH (ang. Encapsulating Security Header) i informacje w nim zawarte, będą zaszyfrowane i niedostępne dla pośredniczących urządzeń sieciowych oraz może on służyć, jako dodatkowe informacje dla datagramów wyższych warstw. Są one istotne jedynie dla źródła i przeznaczenia pakietu.

Współdzielenie adresu *Anycast*, służącego do identyfikacji wielu interfejsów lub wielu węzłów w zdefiniowanej lokalizacji, jest dobry do ustanowienia podczas wykorzystania takiej samej usługi. Za przykład można przedstawić lepszą, alternatywną metodę uwierzytelnienia AAA (ang. *Authentication*, *Authorization*, *Accounting*) poprzez serwery bezpieczeństwa TACACS+, RADIUS, CiscoSecure ACS (ang. Cisco Secure Access Control Server) lub Kreberos – serwer firmy zewnętrznej [4]. W momencie awarii, kolejny najbliższy serwer zapewni tą usługę poprzez ten sam adres.

Literatura

[1] Dokument RFC 4339: *IPv6 Host Configuration of DNS Server Information Approaches, http://www.rfc-base.org/txt/rfc-4339.txt*, 2006.

[2] Dokument RFC 4472: *Operational Considerations and Issues with IPv6 DNS, http://www.rfc-base.org/txt/rfc-4472.txt*, 2006.

[3] Dokument RFC 2460: *Internet Protocol, Version 6 (IPv6) Specification, http://www.rfc-base.org/txt/rfc-2460.txt*, 1998.

[4] Desmeules R., przekład z j. ang. Zdrojewski K.: *IPv6: Sieci oparte na protokole IP w wersji 6. Implementacja, projektowanie, konfiguracja, wdrożenia*. Wyd. PWN, Warszawa 2006.

[5] Windows: *Netsh Technical Reference, https://technet.microsoft.com/en-us/library/cc725935(v=ws.10).aspx*, 21.01.2016.

[6] Dokument RFC 4291: *IP Version 6 Addressing Architecture, http://www.rfc-base.org/txt/rfc-4291.txt*, 2006.

[7] Dokument RFC 4861: *Neighbor Discovery for IP version6(IPv6),http://www.rfc-base.org/txt/rfc-4861.txt*, 2007.

[8] Cisco System, Inc.: Cisco IOS IPv6 *Configuration Guide*, 2009.

[9] Dokument RFC 4862: *IPv6 Stateless Address Autoconfiguration, http://www.rfc-base.org/txt/rfc-4862.txt*, 2007.

[10] Frahim J., Santos O., Ossipov A.: Cisco ASA All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition. Wyd. Cisco Press, 2014..

[11] National Institute of Standards and Technology: *Guidelines for the Secure Deployment of IPv6. Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf,* 2010

[12] Dokument RFC 6564: *A Uniform Format for IPv6 Extension Headers, http://www.rfc-base.org/txt/rfc-6564.txt*, 2012.

[13] White Paper: *IPv6 Extension Headers Review and Considerations, http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.pdf*, 2006.

[14] Benjamin H., przekład z j. ang. Dąbkowska-Kowalik M.: *CCIE Security Oficjalny podręcznik przygotowujący do egzaminu.* Wyd. MIKOM, Warszawa 2004.

[15] Cisco Security Intelligence Operations: *Next Generation Encryption, http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html,* 2014.

[16] IPv6 Now Pty Ltd: *IPv6 Packet Security, http://www.ipv6now.com.au/primers/IPv6PacketSecurity.php*, 29.12.2015.

[17] CLI Book 3: *Cisco ASA Series VPN CLI Configuration Guide Software Version 9.1, http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config.pdf,* wyd. Cisco Systems, 31.03.2014.

[18] Cisco Security Advisory: *Cisco ASA IKEv1 and IKEv2 Buffer Overflow Vulnerability CSCux42019, https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike,* 10.02.2016.

[19] Cisco Systems: ASA/PIX: *How to Use the CLI to Upgrade the Software Image on a Failover Pair, http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/111867-asa-failover-upgrade.html#actstand,* wyd. Cisco Systems, 16.03.2010.

[20] Cisco Systems: *Configure the ASA to Pass IPv6 Traffic, http://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/119012-configure-asa-00.html*, 29.01.2015.

[21] Projekt dokumentu RFC: *The Transport Layer Security (TLS) Protocol Version 1.3 draft-ietf-tls-tls13-11, https://tools.ietf.org/html/draft-ietf-tls-tls13-11#page-6*, 2015.