Bezpieczeństwo w IPv6

Autor: Mariusz Sepczuk

Opiekun: prof. dr hab. inż. Zbigniew Kotulski

Plan prezentacji

- Wstęp, czyli dlaczego IPv6
- Ataki na protokół i metody zabezpieczeń
  - “nowe” ataki w IPv6
  - ataki podobne do ataków w Ipv4
- IPsec
- Firewalle w środowisku używającym IPv6
- Tunelowanie IPv6

Plan prezentacji

- Wstęp, czyli dlaczego IPv6
- Ataki na protokół i metody zabezpieczeń
  - “nowe” ataki w IPv6
  - ataki podobne do ataków w Ipv4
- IPsec
- Firewalle w środowisku używającym IPv6
- Tunelowanie IPv6

Motywacja

- dotychczasowa 32-bitowa przestrzeń adresowa niedługo się wyczerpie

Zobacz za ile dni kończy się internet

Dotychczas przewidywano, że zapasy adresów IPv4 pozostające do dyspozycji agencji IANA (Internet Assigned Numbers Authority) wystarczą do marca 2011 roku. Tempo, w jakim znikają, można śledzić dzięki rozmaitym widżetom. Jednak zasoby wolnych adresów naprawdę topnieją szybciej, niż oczekiwano: w połowie października IANA miała w zapasie jeszcze 12 wolnych bloków /8, przy czym jeden zarezerwował rejestr odpowiedzialny za Afrykę (AfriNIC).

We wtorek (30 listopada) IANA **przyznała po dwa bloki /8** innym regionalnym administratorom adresów (Regional Internet Registries, RIR). Były nimi organizacje ARIN (obsługująca USA, Kanadę i część Karaibów) oraz RIPE NCC (odpowiedzialna za Europę, Bliski Wschód i centralną część Azji). Krótko mówiąc, **w puli agencji IANA** pozostało jeszcze siedem wolnych bloków adresowych typu /8.

Pięć spośród tych bloków jest już zarezerwowanych dla potrzeb specjalnej procedury wydawania ostatnich adresów: zostaną one rozdysponowane równo – czyli po jednym bloku /8 dla każdego z pięciu rejestrów regionalnych (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC). Stanie się tak wówczas, gdy z siedmiu wolnych jeszcze bloków znikną dwa.

W związku z tym daty podawane na licznikach wolnych adresów IPv4 mogą być już nieaktualne: według klasycznej metody przydzielania bloków /8 pozostały tylko dwa takie zakresy (ponieważ pięć kolejnych dostaną poszczególne RIR-y). Niewykluczone więc, że zasoby IANA wyczerpią się już w styczniu, a nie w marcu 2011 roku. Co prawda regionalne rejestry nie zaczęły przydzielać klientom adresów z ostatnich pięciu bloków, ale i te mogą wyczerpać się szybciej niż przewidywano. Wcześniej – według internetowych liczników – wolne numery IPv4 miały się skończyć na początku grudnia 2011 roku.

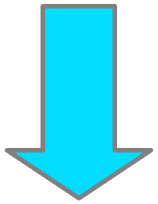
Co mamy w związku z IPv6 ?

- pula adresów

$$2^{128} \quad vs \quad 2^{32}$$

- struktura adresu

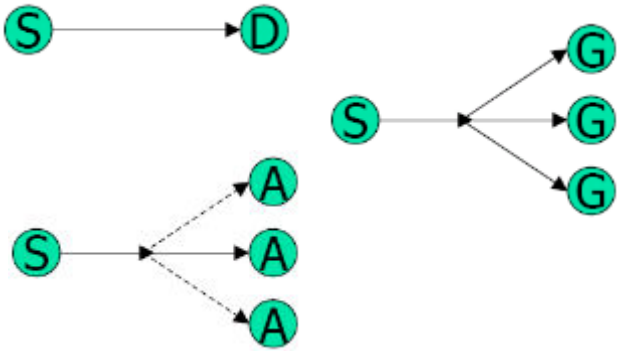
2001:0db8:0000:0000:0000:0000:1428:070b

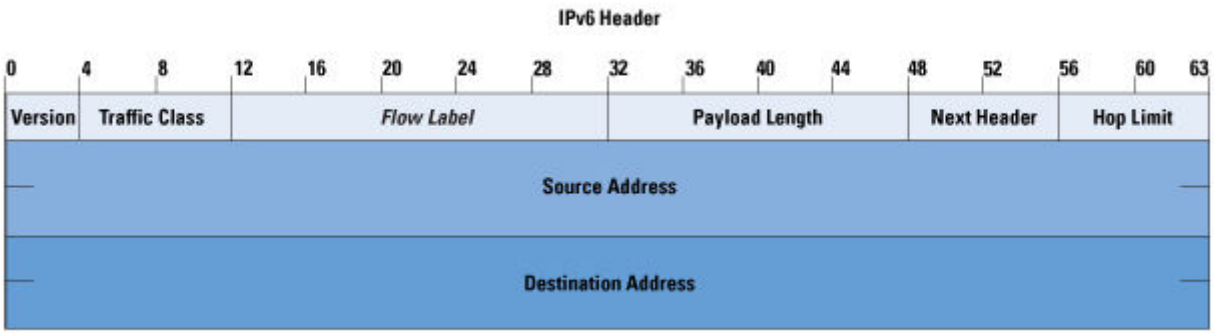


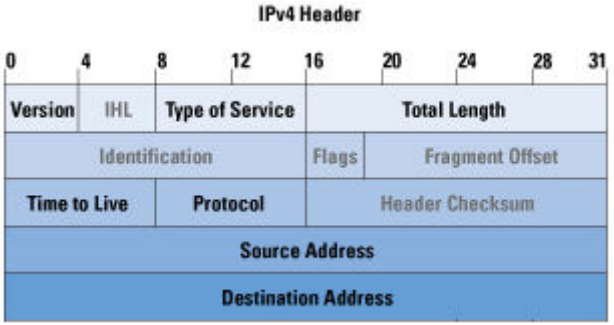
2001:db8::1428:70b

Co mamy w związku z IPv6 ?

- typy adresów
  - unicast address
  - anycast address
  - multicast address
- nowy nagłówek







Plan prezentacji

- Wstęp, czyli dlaczego IPv6
- Ataki na protokół i metody zabezpieczeń
  - “nowe” ataki w IPv6
  - ataki podobne do ataków w Ipv4
- IPsec
- Firewalle w środowisku używającym IPv6
- Tunelowanie IPv6

Ataki na protokół

- rozpoznanie (rekonesans)
- manipulowanie nagłówkiem i fragmentacja
- spoofing warstw 3 i 4
- ARP and DHCP attacks
- smurf attack
- ataki na routing
- wirusy i robaki

Rekonesans

- Pierwsza faza ataku mająca na celu odkrycie słabych punktów potencjalnej ofiary
- Atak w IPv4
  - Ping sweeps
  - Port scans
  - Applocation and vulnerability scans
- Atak w IPv6
  - Ping sweeps lub port scans
  - Opcja wykorzystania adresów multicast

Jak się zabezpieczać?

- Wdrożenie rozszerzeń prywatności
- Filtr do użytku wewnętrznego adresów ipv6 na routerach brzegowych
- Używanie standardowych, ale nie oczywistych adresów dla systemów
- Filtr niepotrzebnych usług na zaporze
- Selektywny filtr ICMP

Manipulacja nagłówkiem i fragmentacja

- Jedna z najłatwiejszych technik nadużycia
- W nowej wersji protokołu dodatkowo:
  - Niedopracowanie oprogramowania (w tym liczne błędy)
- Dlaczego filtrowanie pakietów ipv6 jest trudne?
  - Brak ograniczenia na rozmiar nagłówka
  - Ściśle określona kolejność występowania po sobie rozszerzeń nagłówka
- Fragmentacja: nie wiemy jak zachowa się system ze stosem OSI w przypadku dwóch ramek zawierających ten sam numer sekwencyjny

Jak się zabezpieczać?

- Zapewnienie odpowiednich zdolności filtrowania fragmentacji IPv6
- Usuwanie wszystkich fragmentów z mniej niż 1280 oktetów (oprócz ostatniego)

Spoofing warstw 3 i 4

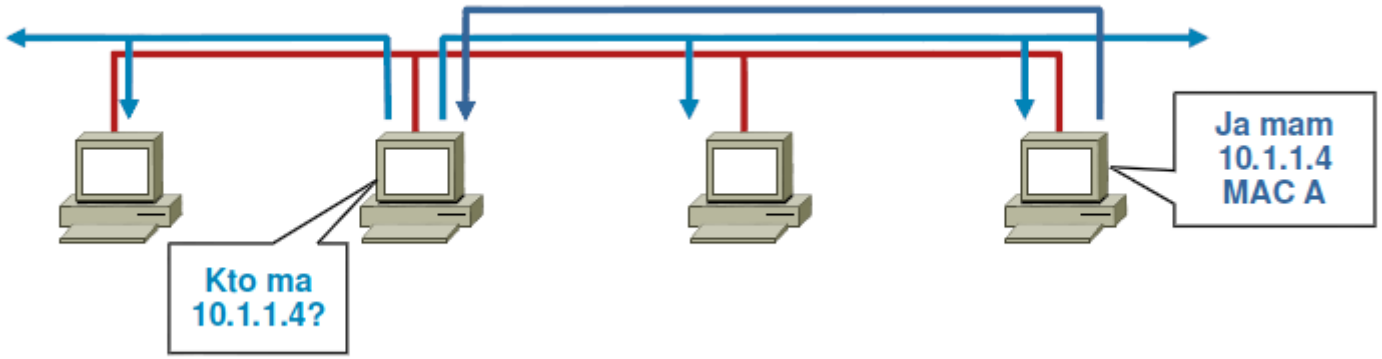
- Jeden z najpoważniejszych ataków
- Fałszowanie podstawowych usług i protokołów sieciowych
- Atak w IPv4
  - Następuje każdego dnia (DoS, spam, robaki I wirusy)
  - RFC 2827 definiuje metody do filtrowania przeciwdziałające spoofingowi warstwy 3
    - Zasadniczo nie wprowadzono w życie (ochrona przed spoofingiem części sieciowej adresu, a nie części hosta)

Spoofing warstw 3 i 4

- Atak w IPv6
  - Zagregowany charakter IPv6 pozwala na zaimplementowanie metod filtrowania z RFC 2827
  - Spoffing warstwy 4 nie został zmieniony w stosunku do IPv4
  - Dużo więcej adresów → więcej adresów do sfałszowania
- Zabezpieczenia
  - RFC 2827
  - Ochrona kryptograficzna

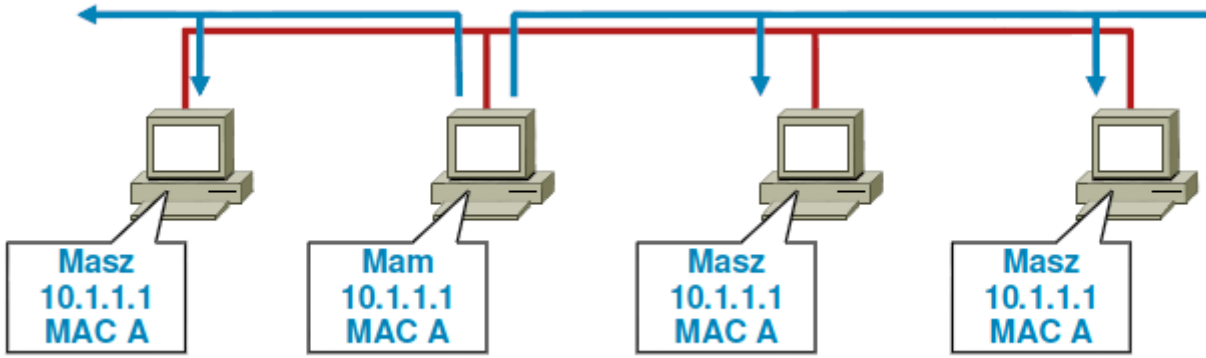
ARP I DHCP attack

- Zanim stacja zacznie komunikację musi znać adres MAC drugiej strony (wysyła zapytanie ARP)
- Wszystkie stacje w podsieci przetwarzają zapytanie i odpowiada tylko ta której ip było w zapytaniu



ARP I DHCP attack

- Zgodnie z ARP RFC, klient może wysłać odpowiedź ARP bez żądania (ARP „grzecznościowy” –Gratuituous ARP). Inne hosty w podsieci mogą zachować tę informację w swoich tablicach ARP
- Każdy może podać się za posiadacza dowolnego IP/MAC
- Ataki ARP pozwalają przekierowywać ruch

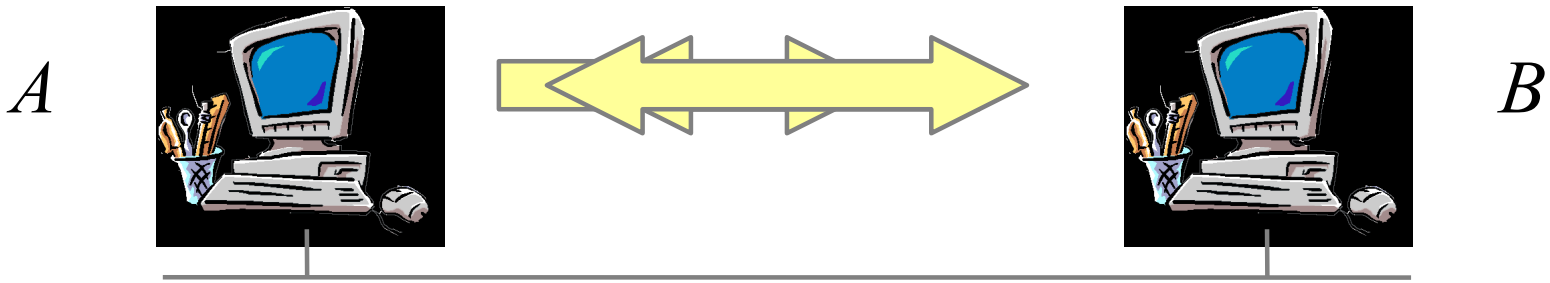


ARP I DHCP attack

- DHCP: przyznawanie dynamicznego ip na żądanie
- Atak w IPv6
  - Brak zabezpieczeń dla IPv6 odpowiedników ARP i DHCP
  - Ataki takie jak w IPv4
    - Fałszywy serwer DHCP
    - Wygłodnienie serwera DHCP

Neighbors Discovery

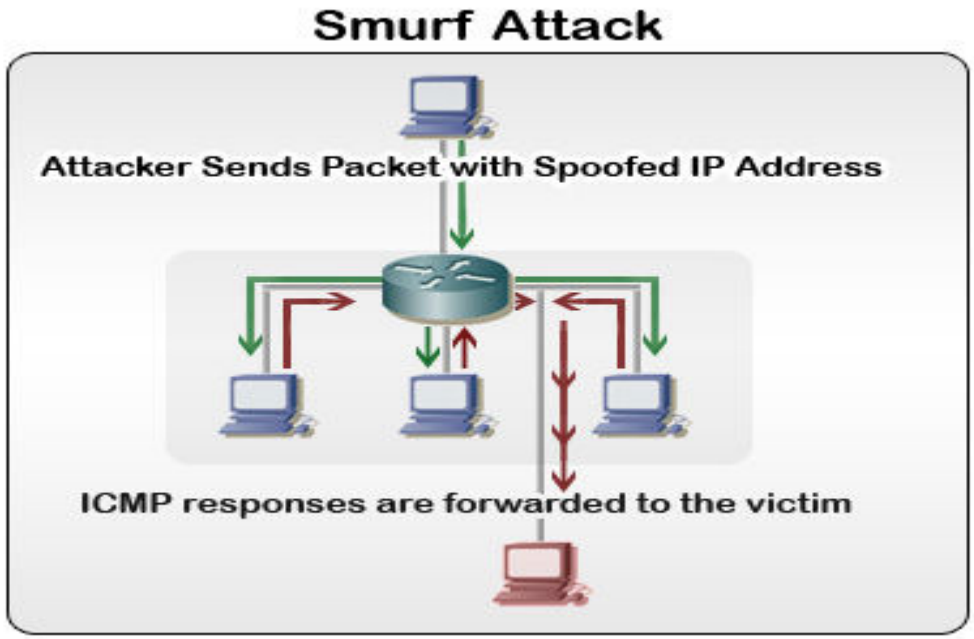
- Komunikacja stacji znajdujących się w jednym segmencie (bez routerów I konfiguracji tras routingu)
- Działanie:
  - A, po włączeniu się do sieci wysyła swój adres jednostkowy łącza lokalnego na adres Solicited- Node Address hosta B z zapytaniem o adres B
  - B wysyła swój adres jednostkowy łącza lokalnego
  - A i B mogą się komunikować



Jak się zabezpieczać?

- DHCP snooping- nie pozwala on na nadawanie adresów IP serwerom DHCP z nie zaufanych portów na switchu
- Używanie statycznych wpisów sąsiada

Smurf attack



- Atakujący fałszuje ping, poprzez zmianę adresu źródła tych zapytań na adres atakowanego serwera
- Pakiety wysyłane są na adres rozgłoszeniowy, po czym odpowiedź przesyłana będzie na sfałszowany adres źródłowy atakowanej ofiary

Smurf attack

- Atak w IPv4
  - Prosta metoda ograniczenia w sieciach IP
    - Wyłączenie broadcastu na routerach: : `no ip directed broadcasts`
- Atak w IPv6
  - Usunięcie adresów broadcast
  - Pakiety ICMPv6 nie powinny być generowane jako odpowiedź na IPv6 multicast destination address lub link-layer multicast address(Jeśli tak jest w routerach końcowych, to atak nie jest problemem)

Jak się zabezpieczać?

- Wprowadzenie filtrowania pakietów z *IPv6 multicast source addresses*

Ataki na routing

- Zakłócenia lub przekierowanie ruchu w sieci
  - Flooding, szybkie ogłaszanie i usuwanie tras, podrabianie tras
- Zależne od wyboru protokołu routingu
- IPv4: uwierzytelnienie w celu zabezpieczenia komunikacji między węzłami
- Protokoły w IPv6
  - Uwierzytelnienie w BGP i IS-IS
  - OSPFv3 i RIPng- brak pola uwierzytelnienia nagłówka

Jak się zabezpieczać?

- Używać tradycyjnych mechanizmów uwierzytelnienia w BGP i IS-IS
- Używać IPsec jako ochrony dla protokołów OSPFv3 I RIPng
- Generalised TTL Security Mechanism
  - GTSM chroni sesje BGP przed atakami z oddalonych sieci/stacji
  - Routery wymieniają się pakietami IP z polem TTL ustawionym na wartość 255(<254 odrzucamy)
  - Urządzenia niepodłączone bezpośrednio pomiędzy routerami nie może wygenerować takiego ruchu

Wirusy i robaki

- Wirusy i robaki pozostają jednym najważniejszych problemów w sieciach IP
- Atak w IPv4
  - uszkodzenie hosta
  - uszkodzenie transportu sieciowego
    - Obciążenie routerów, serwerów pocztowych w całym Internecie
    - SQL slammer
- Ataki w IPv6
  - Utrudnione skanowanie potencjalnej ofiary

Jak się zabezpieczać?

- Program antywirusowy
- Firewall
- Aktualizacja bazy wirusów i regularne skanowanie dysków
- Niezbędne dalsze badania dotyczące rozwoju wirusów i robaków

Plan prezentacji

- Wstęp, czyli dlaczego IPv6
- Ataki na protokół i metody zabezpieczeń
  - “nowe” ataki w IPv6
  - ataki podobne do ataków w Ipv4
- IPsec
- Firewalle w środowisku używającym IPv6
- Tunelowanie IPv6

Ataki podobne do ataków w Ipv4

- Sniffing, czyli przechwytywanie danych podczas transmisji w sieci
- Ataki na warstwę aplikacji, czyli ataki na aplikacje webowe
- Rogue devices, czyli wprowadzanie fałszywych urządzeń do sieci
- Man in the middle, czyli podsłuch i modyfikacja przesyłanych wiadomości
- Flooding, czyli wysyłanie tej samej wiadomości w bardzo krótkim odstępie czasu

Plan prezentacji

- Wstęp, czyli dlaczego IPv6
- Ataki na protokół i metody zabezpieczeń
  - “nowe” ataki w IPv6
  - ataki podobne do ataków w Ipv4
- IPsec
- Firewalle w środowisku używającym IPv6
- Tunelowanie IPv6

IPsec

- Zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami
- Co oferuje?
  - Kontrola dostępu
  - Integralność danych (bezpołączeniowa)
  - Autentyczność pochodzenia danych
  - Odrzucanie powtarzających się pakietów
  - Poufność (szyfrowanie)
  - Ograniczona poufność przepływu danych

IPsec

- Jakie zalety?
  - Implementowalny w firewallach/routerach, zapewnia silne bezpieczeństwo
  - Ruch nie może ominąć firewalla z zaimplemntowanym Ipsec
  - Położony poniżej warstwy transportowej, przejrzysty dla warstwy aplikacji
  - Przejrzysty dla użytkowników końcowych
  - Zapewnia bezpieczeństwo dla użytkowników indywidualnych gdy to konieczne

IPsec

- Ograniczenia?
  - Nie prowadzi analizy ruchu
  - Nie gwarantuje niezaprzeczalności
  - Nie chroni przed odmową usługi

Plan prezentacji

- Wstęp, czyli dlaczego IPv6
- Ataki na protokół i metody zabezpieczeń
  - “nowe” ataki w IPv6
  - ataki podobne do ataków w Ipv4
- IPsec
- Firewalle w środowisku używającym IPv6
- Tunelowanie IPv6

Firewall

- Zapory ogniowe stanowią jeden z najważniejszych mechanizmów bezpieczeństwa sieci
- Filtrują wychodzący i wchodzący ruch sieciowy
- Każdy pakiet jest badany i sprawdzany z regułami ustawionymi na zaporze
- Reguły filtrowania muszą być zdefiniowane dla obu wersji protokołu

Firewall

- Architektura IPv6 I zapory (Wymagania)
  - NAT nie jest potrzebny
  - Słabe strony filtrowania pakietów nie mogą być ukryte przez NAT
  - Wsparcie dla transformacji i współistnienia IPv4/IPv6

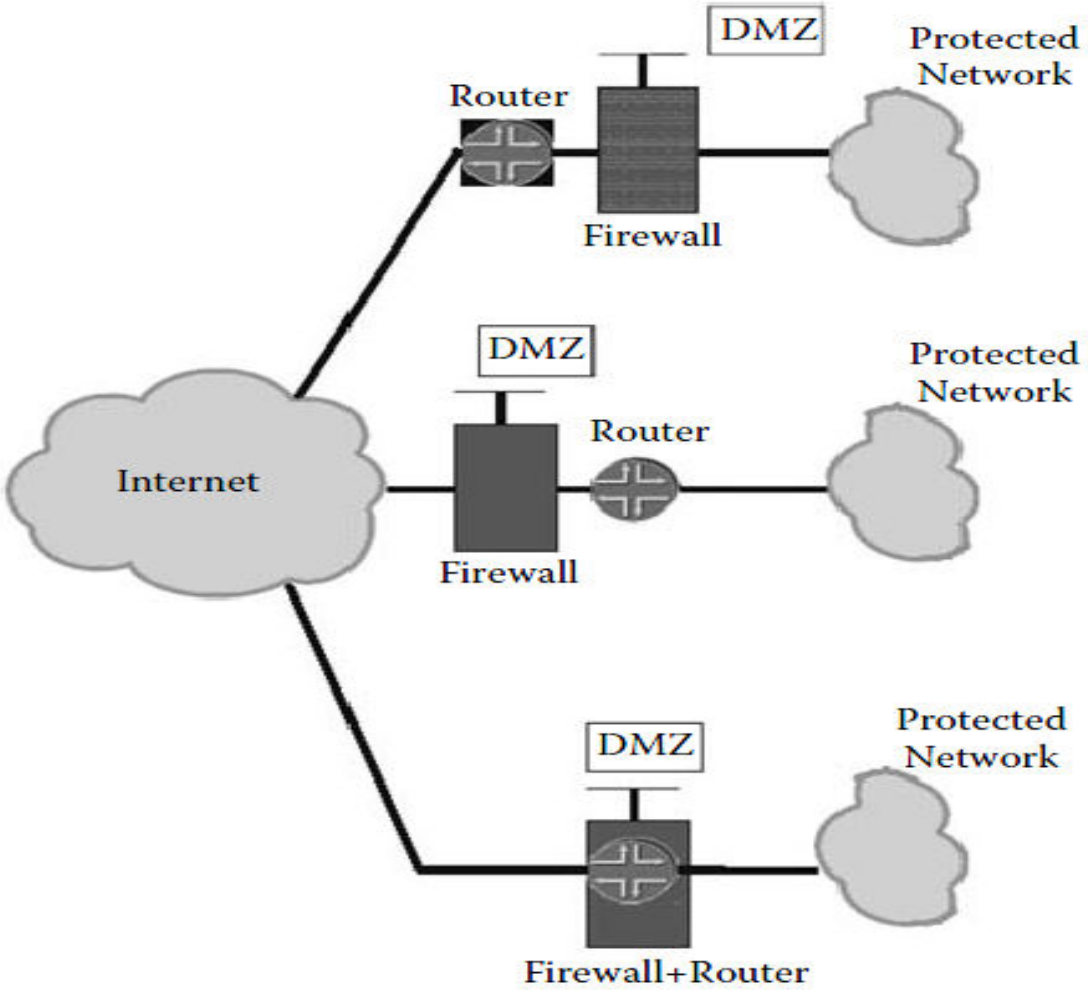
Firewall

- Cechy firewalla w sieci z ipv6

(adapted from ICANN's Survey of IPv6 Support in Commercial Firewalls, October 2007)	
Security Service or Feature	*Description*
Network Address Translation and Tunneling	
– IP masquerading	The product should be able to map IP addresses assigned to endpoints on internal networks to a single IP address on the external (public) interface (and thus prevent the disclosure of the internal network addressing and topology information).
– 4to6	The product should be able to encapsulate (tunnel) IPv4 packets in IPv6 packets. This is useful when it is necessary to bridge two or more IPv4-only hosts or networks that do not use IPv6 and the only available transport between those hosts or networks is IPv6.
– 6to4	The product should be able to encapsulate (tunnel) IPv6 packets in IPv4 packets. This is useful when it is necessary to bridge two or more IPv6-only hosts or networks that do not use IPv4 and the only available transport between those hosts or networks is IPv4.
– Flow monitoring	The product should be able to monitor flows of traffic, detect and respond to known-to-be malicious or suspicious/anomalous traffic patterns.
– Log IPv6 traffic	The product should be able to record security events when the transport is IPv6.
– IPsec	The product should be able to support IP Security when the transport is IPv6.
– DHCPv6	The product should be able to support dynamic address assignment when the transport and addressing scheme is IPv6.
– RADIUS (Remote Authentication Dial in Use Service)	The product should be able to support authentication, accounting, and auditing (AAA) features in conjunction with a RADIUS-capable server when the transport is IPv6.

Firewall

- Typowe umiejscowienie firewalli w sieciach ipv6



Firewall

	IP Filter 4.1	*PF 3.6*	*IP6fw*	*Iptables*	*Cisco ACL*	*Cisco PIX 7.0*	*Juniper firewall*	*Juniper Net Screen*	*Windows XP SP2*
Portability	Excellent	Good	Average	Weak	Weak	Weak	Weak	Weak	Weak
ICMPV6 support	Good	Good	Good	Good	Good	Good	Good	Good	Good
Neighbor Discovery	Excellent	Excellent	Good	Excellent	Excellent	Excellent	Good	Excellent	Weak
RS/RA support	Excellent	Excellent	Good	Excellent	Excellent	Excellent	Excellent	Excellent	Good
Extension header support	Good	Good	Good	Excellent	Good	Good	Good	Good	Weak
Fragmentation support	Weak	Complete block	Weak	Good	Weak	Average	Weak	Average	Weak
Stateful firewall	Yes	Yes	No	Csak USAGI	Reflexive firewall	Yes	ASP necessary	Yes	No
FTP proxy	No	Next version	No	No	since 12.3 (11)T	Yes	No	No	No
Other	QOS support	QoS support, checking packet validity	Predefined rules in *BSD	EUI-64 check,	Time based ACL		No TCP flag support today, HW based	IPsec VPN, routing support	Graphical and central configuration

Plan prezentacji

- Wstęp, czyli dlaczego IPv6
- Ataki na protokół i metody zabezpieczeń
  - “nowe” ataki w iPv6
  - ataki podobne do ataków w Ipv4
- IPsec
- Firewalle w środowisku używającym IPv6
- Tunelowanie IPv6

Tunelowanie IPv6

- Przejście z IPv4 na IPv6 nie będzie szybkie (przez pewien czas współistnienie obu protokołów)
- Mechanizmy tunelowania
  - Teredo
  - 6to4
  - inne

Teredo

- Teredo jest systemem tunelowania, przeznaczonym głównie do tworzenia tuneli dla hostów znajdujących się za NAT, czyli nie posiadających globalnego adresu IPv4
- W systemie Teredo tworzone są tunele automatyczne pomiędzy klientem a serwerem Teredo
- Każdy z klientów systemu posiada adres IPv6 zaczynający się od prefiksu 2001:0000::/32.
- W systemie Teredo używa się kapsułkowania datagramów IPv6 wewnątrz pakietów UDP, które są przesyłane przez sieć IPv4.

6to4

- Mechanizm automatycznych tuneli 6to4 pozwala podłączyć się do sieci IPv6 każdemu kto dysponuje choćby jednym publicznym adresem Ipv4
- Mechanizm 6to4 polega na enkapsulacji (tunelowaniu) pakietów IPv6 w pakiety Ipv4
- Pakiety wysyłane są do komputera stanowiącego bramę pomiędzy siecią opartą o IPv4 a "prawdziwą" siecią IPv6

Bezpieczeństwo tunnelowania

- 6to4 może stwarzać pewne problemy na polu bezpieczeństwa
- Większość z do tej pory rozpoznanych stanowią ataki typu DoS wykorzystujące możliwość łatwego podszywania się pod przekaźnik 6to4
- Ruch tunelowany przez Teredo nie jest należycie kontrolowany w firewallach
- Rozwiązania przystosowane do ruchu IPv4 będą kontrolować warstwę IPv4, ale nie rozpoznają pakietu IPv6 w nim zanurzonego

Pytania???