Sieci wirtualne i ich bezpieczeństwo

Opiekun: prof. dr hab. inż. Zbigniew Kotulski

Opracował: Krzysztof Zalewski

Plan prezentacji

- Wstęp
- VPN a sieć wirtualna
- Podstawowe składniki
- Role biznesowe w architekturze 4WARD
- Bodźce do wdrażania sieci wirtualnych
- Ataki

Rozwój wirtualizacji

- Uwaga ze strony przemysłu i nauki
- Możliwość budowy i rozwoju architektur sieciowych bez narzuconych technologii
- Ewolucja do Internetu Przyszłości
- Łatwość badań i rozwoju na działającym już systemie

Od usług VPN do VN

- VPN przybliża do dostarczania rozdzielnych sieci wirtualnych na wspólnej infrastrukturze fizycznej

- Po co VN skoro VPN działa tak dobrze?

Niedogodności VPN

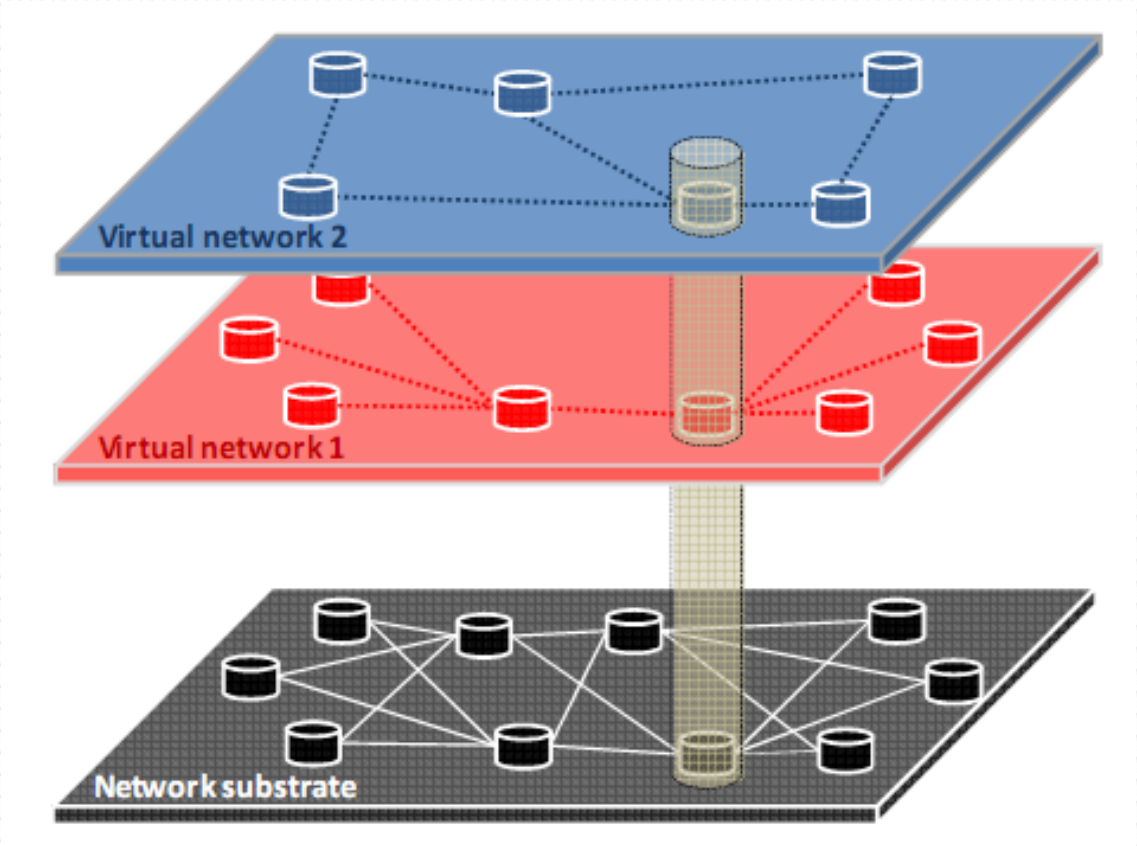
- Jedna technologia i stos protokołów
- Brak możliwości realnej izolacji zasobów sieciowych
- Dostawca infrastruktury i dostawca usługi VPN musza być w rzeczywistości tym samym podmiotem

Network Virtualization

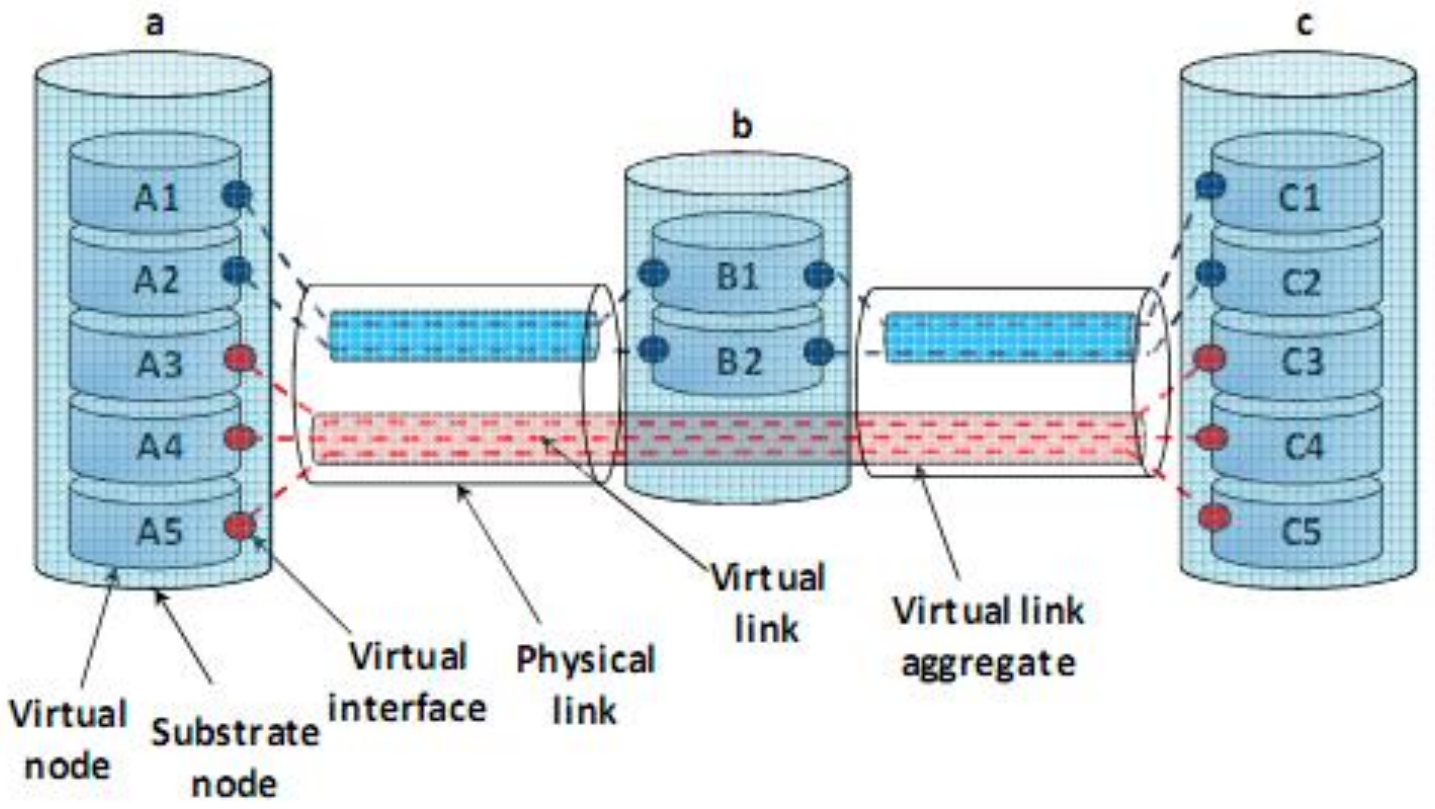
- Niezależne konfiguracje sieci wirtualnych (różne technologie i architektury)
- Zdolność do radzenia sobie z wieloma dostawcami i ukrywanie infrastruktury sieciowej
- Realna izolacja sieci wirtualnych dzielących tą samą infrastrukturę

Podstawowe składniki

- Łącza wirtualne
- Węzły wirtualne



Podstawowe składniki



Role biznesowe

- **Dostawca infrastruktury (InP)**
  - Zasoby fizyczne i ich podział
- **Dostawca sieci wirtualnej (VNP)**
  - Łączenie części od InP dla VNO
  - Kontener do budowy sieci
- **Operator sieci wirtualnej (VNO)**
  - Implementacja stosu protokołów i architektury
  - Administracja jak zwykłą siecią

Bodźce do wdrażania wirtualnych sieci

- VN jako ulepszenie i rozszerzenie VPN
- Sieć postrzegana przez VNO jako własność
- Różne oczekiwania finansowe od różnych udziałowców
- Podział sieci operatora na część biznesową i prywatna
- Podział kosztów budowy sieci szkieletowej proporcjonalny do późniejszych możliwości jej eksploatacji
- Zapewnienie QoS

Ataki

- Ataki na sieć wirtualną są takie same jak na standardową, stosowaną aktualnie technologię

- Ataki na węzeł podstawowy
- Ataki na węzeł wirtualny

Ataki

- Rodzaj atakowanego węzła nie ma znaczenia w sensie technicznym, z punktu widzenia atakującego. Jednak w przypadku ataku na węzeł podstawowy atakowane są wszystkie sieci używające tego węzła, zaś w przypadku węzła wirtualnego tylko pojedyncza sieć.

Rodzaje ataków

- Atak na węzeł podstawowy
- DoS

  Odcięcie innych użytkowników
  Uszkodzenie konfiguracji

- Atak na węzeł wirtualny

Ataki z wewnątrz sieci

- Różne techniki – różne rodzaje ataków
- Ataki na protokoły routingu
- MAC flooding
  Przepełnianie tablicy Content Addressable Memory

Ataki z wewnątrz sieci

- ARP spoofing

  Podszywanie się pod jednego z użytkowników sieci poprzez wysyłanie wiadomości ARP Reply

- Modyfikacja nagłówków czy etykiet

Cel pracy

- Zbadanie działania zaproponowanej w projekcie 4WARD architektury

- Zbadanie odporności na standardowe rodzaje ataków oraz wpływ na cały system udanego ataku na jedna z sieci wirtualnych
- W miarę możliwości na sprzęcie