



**WYŻSZA SZKOŁA
INFORMATYKI i ZARZĄDZANIA**
z siedzibą w Rzeszowie

KOLEGIUM INFORMATYKI STOSOWANEJ

Kierunek: INFORMATYKA
Specjalność: Technologie IoT - Internetu
Rzeczy

Szymon Sutyła
Nr albumu studenta: w66012

Komunikacja człowiek-komputer

***Projektowanie i implementacja sieci przedsiębiorstwa z
wykorzystaniem narzędzia Packet Tracer***

Rzeszów 2024

Spis treści

1.	Analiza istniejących rozwiązań	3
1.1.	Cisco Network Solutions	3
1.2.	Microsoft Azure	4
1.3.	Fortinet	5
1.4.	Elementy wspólne	6
1.5.	Różnice	6
1.6.	Wady i zalety przedstawionych rozwiązań	6

1. Analiza istniejących rozwiązań

Do porównania istniejących rozwiązań wybrałem: Cisco Network Solutions, Microsoft Azure i Fortinet ze względu na ich renomę, szeroką gamę oferowanych produktów i usług oraz znaczącą pozycję na rynku technologii sieciowych i bezpieczeństwa. Każde z tych rozwiązań jest znane z zaawansowanych technologii i kompleksowego podejścia do rozwiązywania problemów sieciowych i zabezpieczeń, co sprawia, że są one idealnymi kandydatami do porównania.

1.1. Cisco Network Solutions

Cisco jest to renomowany dostawca rozwiązań sieciowych, oferujący szeroki zakres produktów. Do kluczowych obszarów, w których specjalizują się Cisco zaliczyć możemy:

- **Routery i przełączniki:** Cisco dostarcza zaawansowane routery i przełączniki LAN i WAN, które umożliwiają efektywne zarządzanie ruchem sieciowym.
- **Bezpieczeństwo:** Cisco oferuje różnorodne produkty z zakresu bezpieczeństwa, takie jak firewalle, VPN, UTM, AAA (autoryzacja, uwierzytelnianie i rachunkowość) oraz NAC (Network Access Control). Te rozwiązania pomagają chronić sieci przed zagrożeniami i atakami.
- **Telefonia IP:** Cisco dostarcza systemy telefonii IP, które pozwalają na przesyłanie głosu w sieciach danych. To ważne dla firm, które chcą zintegrować komunikację głosową z danymi.
- **Sieci bezprzewodowe:** Cisco jest liderem w dziedzinie technologii Wi-Fi i oferuje produkty do budowy wydajnych i bezpiecznych sieci bezprzewodowych.
- **Cisco DNA:** To architektura sieciowa, która umożliwia automatyzację, analizę i zarządzanie siecią. Pozwala na tworzenie bardziej inteligentnych i elastycznych sieci.

Rys. 1. Cisco



Źródło:

https://www.cisco.com/c/pl_pl/index/jcr:content/homepagemaincontentparsys/full_9e22/Full/mosaic_row_wide_narr/mosaic_col_wide_parsys/mosaic_tile_wide_bf6.img.jpg/1707491883682.jpg dostęp 10.05.2024

1.2. Microsoft Azure

Microsoft Azure to platforma chmurowa, która oferuje różnorodne usługi sieciowe i obliczeniowe. Oto kilka kluczowych obszarów, w których Azure się specjalizuje:

- Azure Virtual Network (VNET): To usługa umożliwiająca tworzenie izolowanych, wirtualnych sieci w chmurze. Dzięki VNET możesz łączyć maszyny wirtualne, aplikacje i inne zasoby w jednym bezpiecznym środowisku. To idealne rozwiązanie dla organizacji, które potrzebują elastycznych i skalowalnych sieci.
- Azure Load Balancer: Jest to usługa równoważenia obciążenia, która automatycznie dystrybuje ruch między różnymi serwerami lub maszynami wirtualnymi. Dzięki temu można osiągnąć wyższą dostępność i wydajność aplikacji.
- Azure VPN Gateway: Usługa umożliwiająca bezpieczne połączenie między lokalnymi sieciami a siecią w chmurze. Pozwala na tworzenie wirtualnych sieci prywatnych (VPN) i zapewnia szyfrowaną komunikację.
- Azure App Service: To platforma do hostowania aplikacji internetowych, mobilnych i API. Pozwala na łatwe wdrażanie, skalowanie i zarządzanie aplikacjami w chmurze.



Źródło: https://media.licdn.com/dms/image/D4D12AOGUnhgqmwIvzQ/article-cover_image-shrink_720_1280/0/1658421811896?e=2147483647&v=beta&t=mqCHoKMvc-uU5PbGJJ8b-LcnufSTy8aSqUyO2p5F1QE
dostęp 10.05.2024

1.3. Fortinet

Fortinet to globalny lider w dziedzinie bezpieczeństwa sieciowego i rozwiązań cyberbezpieczeństwa. Oferuje szeroki zakres produktów i usług, które pomagają organizacjom chronić swoje sieci przed zagrożeniami. Oto kluczowe rozwiązania oferowane przez Fortinet:

- FortiGate: To seria urządzeń firewall, które łączą w sobie funkcje zapory sieciowej, VPN, wykrywania i eliminacji zagrożeń oraz kontroli treści. FortiGate jest znany ze swojej wydajności, skalowalności i zaawansowanych funkcji bezpieczeństwa.
- FortiAnalyzer: To narzędzie do analizy i raportowania ruchu sieciowego. Pomaga organizacjom monitorować i analizować dane z urządzeń FortiGate, aby zidentyfikować potencjalne zagrożenia.
- FortiManager: Jest to platforma do zarządzania urządzeniami Fortinet. Umożliwia zdalne konfigurowanie, monitorowanie i aktualizowanie urządzeń w sieci.
- FortiAP: To punkty dostępowe WiFi, które można zintegrować z urządzeniami FortiGate. Pozwalają na budowę bezpiecznych i wydajnych sieci bezprzewodowych.
- FortiWeb: To rozwiązanie do ochrony aplikacji internetowych przed atakami, takimi jak SQL injection, cross-site scripting (XSS) i inne.
- FortiSandbox: Jest to środowisko do analizy zachowania plików. Pozwala na wykrywanie zaawansowanych zagrożeń, takich jak złośliwe oprogramowanie i ransomware.

Rys. 3. Fortinet



Źródło: https://sieciowy.com.pl/hpeciai/4832a5f46043f30c243548e5e0270043/pol_pl_Firewall-Fortinet-FortiGate-90G-17307_1.jpg dostęp 10.05.2024

1.4.Elementy wspólne

Do elementów wspólnych wymienionych rozwiązań zaliczyć możemy:

- Bezpieczeństwo: Wszystkie trzy rozwiązania kładą duży nacisk na bezpieczeństwo sieci i oferują produkty do ochrony przed zagrożeniami.
- Sieci bezprzewodowe: Zarówno Cisco, jak i Fortinet oferują rozwiązania do budowy i zarządzania sieciami Wi-Fi.
- Zarządzanie siecią: Cisco DNA i FortiManager umożliwiają zaawansowane zarządzanie sieciami.

1.5.Różnice

Rozwiązania te różnią się od siebie w następujących aspektach:

- Zasięg usług: Microsoft Azure koncentruje się na usługach chmurowych, takich jak wirtualne sieci i równoważenie obciążenia, podczas gdy Cisco i Fortinet oferują bardziej tradycyjne rozwiązania sieciowe i bezpieczeństwa sprzętowego.
- Integracja komunikacji: Cisco wyróżnia się rozwiązaniami do telefonii IP, czego brakuje w ofercie Microsoft Azure i Fortinet.
- Specjalizacja: Fortinet jest silnie skoncentrowany na bezpieczeństwie, oferując szczegółowe narzędzia do analizy zagrożeń i zarządzania urządzeniami bezpieczeństwa, podczas gdy Cisco i Azure oferują bardziej wszechstronne rozwiązania.

1.6.Wady i zalety przedstawionych rozwiązań

1.6.1. Cisco Network Solutions

- Zalety: Wszechstronność, zaawansowane zarządzanie siecią, silne funkcje bezpieczeństwa.

- Wady: Może być kosztowne, skomplikowane do wdrożenia i zarządzania w mniejszych organizacjach

1.6.2. Microsoft Azure

- Zalety: Elastyczność chmury, łatwość skalowania, szeroki zakres usług chmurowych
- Wady: Może być zależne od połączenia internetowego, złożoność zarządzania dużymi infrastrukturami

1.6.3. Fortinet

- Zalety: Silne skupienie na bezpieczeństwie, zaawansowane narzędzia analizy i zarządzania
- Wady: Może być mniej wszechstronne niż rozwiązania oferujące pełne zarządzanie siecią i usługi chmurowe