Wniosek ucznia:

1. **Konfiguracja filtrowania ruchu przychodzącego:**

- Otwórz Zaporę systemu Windows z zaawansowanymi zabezpieczeniami.
- Przejdź do sekcji "Reguły ruchu przychodzącego".
- Utwórz nową niestandardową regułę.
- Wybierz, czy ma dotyczyć określonego programu, portu lub istniejącej reguły.
- Określ program, port i protokół.
- Zdefiniuj adres IP lub zakres adresów dla dozwolonej komunikacji.
- Ustal, czy reguła ma zezwalać czy odrzucać ruch.
- Wybierz profile zapory, do których ma być stosowana reguła.
- Nadaj nazwę i opcjonalny opis regule.
- Zakończ proces i sprawdź, czy reguła jest aktywna.

Wniosek: Tworzenie reguł zapory umożliwia kontrolowanie ruchu przychodzącego, co jest kluczowe podczas instalacji nowych aplikacji lub konfiguracji serwera.

2. **Konfiguracja filtrowania ruchu wychodzącego:**

- Skonfiguruj zaporę, aby domyślnie blokowała wychodzące żądania.
- Przetestuj to, próbując odwiedzić witrynę WWW za pomocą Internet Explorer.
- Utwórz regułę zezwalającą na żądania od Internet Explorer.
- Zweryfikuj, czy nowa reguła działa poprawnie.
- Przywróć komputer do pierwotnego stanu, wyłączając filtrowanie wychodzące.

Wnioski:

- Filtrowanie wychodzące może zwiększyć bezpieczeństwo, uniemożliwiając domyślnie wszystkim programom wychodzącym.
- Tworzenie reguł zezwolenia na konkretne programy umożliwia kontrolę nad tym, które aplikacje mogą nawiązywać połączenia wychodzące.

3. **Podsumowanie:**

- Konfiguracja Zaawansowanych zabezpieczeń Zaporą systemu Windows umożliwia bardziej szczegółową kontrolę nad ruchem sieciowym.

- Wiedza na temat konfiguracji filtrów przychodzących i wychodzących jest kluczowa dla utrzymania bezpieczeństwa i optymalnej wydajności serwera.
- Odmowa zazwyczaj powinna być przed zezwoleniem w kolejności reguł.

Zadania były skomplikowane, ale przyswajając procedury konfiguracji firewalla w Windows Server 2019, zdobyliśmy umiejętności zarządzania ruchem sieciowym, co jest istotne w utrzymaniu bezpieczeństwa systemów informatycznych.