Jak zabezpieczyć sieć lokalną?

Jak zabezpieczyć sieć lokalną?

Źródło: Scott Webb, domena publiczna.

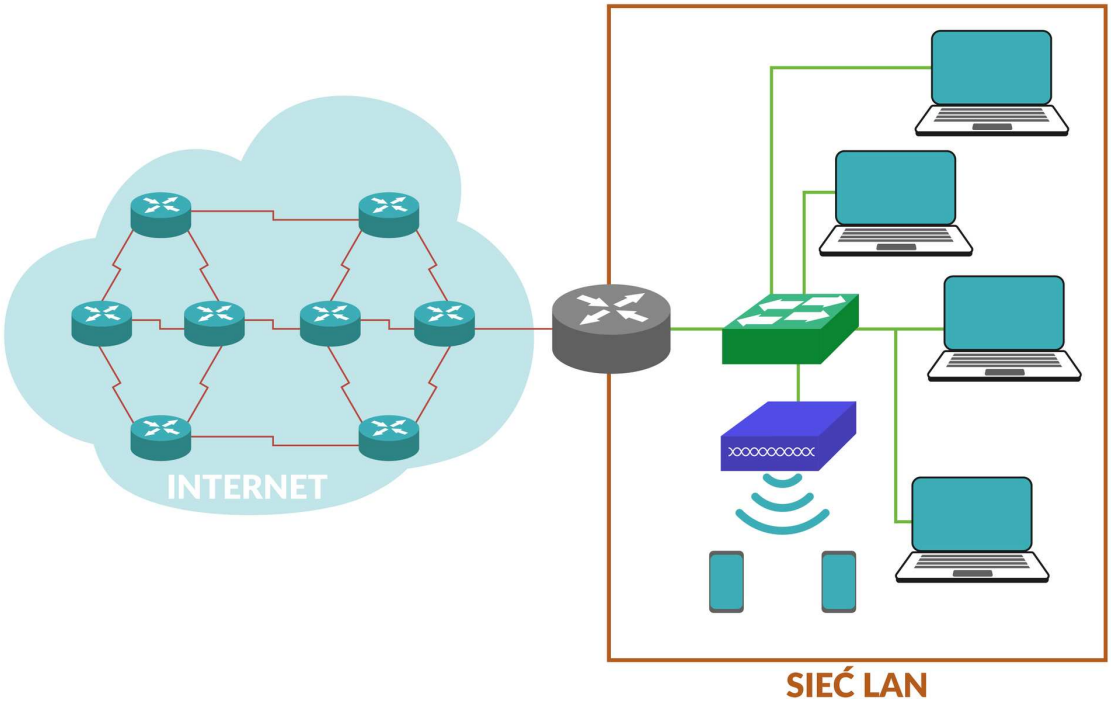
Rozwój technologii informatycznych, a co za tym idzie również sieci komputerowych, oprócz oczywistych korzyści niesie również za sobą zagrożenia. Korzystając na co dzień z zasobów internetu, narażeni jesteśmy na wiele niebezpieczeństw. Część z nich może mieć bardzo przykre konsekwencje zarówno dla nas, gdyż możemy np. utracić cenne dane, jak również dla urządzeń, z jakich korzystamy.

Twoje cele

- Wymienisz zagrożenia, jakie czyhają na użytkowników internetu.
- Wyjaśnisz, jak unikać typowych niebezpiecznych zdarzeń.
- Przeanalizujesz mechanizm działania zapory ogniowej oraz usługi NAT.

Przeczytaj

Większość lokalnych sieci komputerowych ma podobną lub zbliżoną strukturę i topologię:



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Oczywiście wraz ze wzrostem liczby urządzeń pracujących w lokalnej sieci komputerowej zmienić się może struktura takiej sieci. Na jej styku z Internetem zawsze znajduje się jednak ruter sieciowy, który łączy urządzenia sieci lokalnej właśnie z globalną siecią Internet. Ruter stanowiący bramę z i do Internetu jest jednym z podstawowych urządzeń, które mogą zapewnić bezpieczeństwo sieci LAN. Ruterem może być specjalne urządzenie sieciowe, które zostało zaprojektowane i wyprodukowane właśnie do realizacji takich zadań, jak również może to być komputer/serwer z oprogramowaniem, które konfiguruje się w odpowiedni sposób.

Ruter może zapewnić bezpieczeństwo sieci lokalnej, którą obsługuje na kilku płaszczyznach, poprzez:

1. usługę NAT (ang. *Network Address Translation*),
2. ustawienia zapory sieciowej (ang. *firewall*),
3. listy kontroli dostępu (ang. *Access Control List* – ACL).

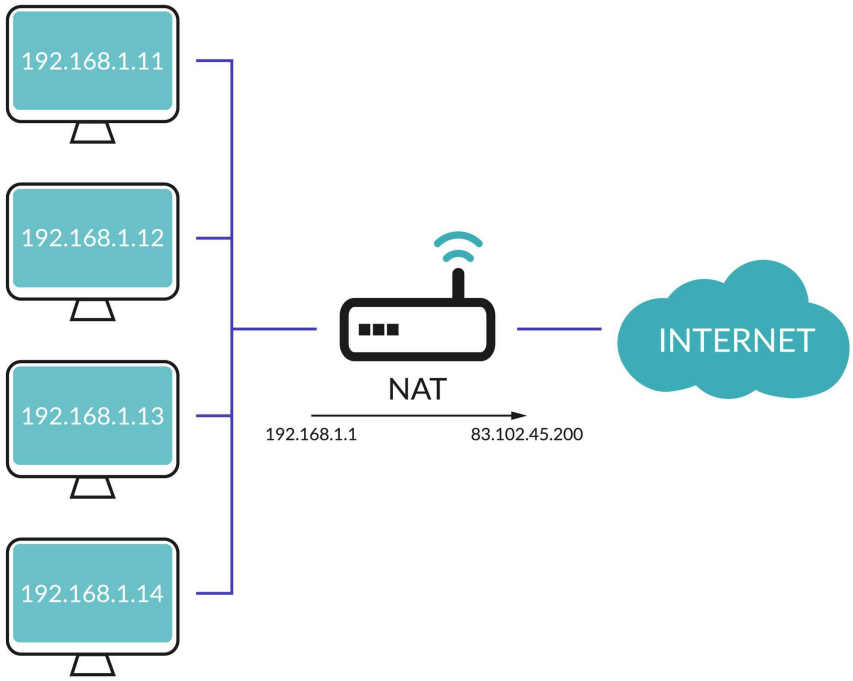
Usługa NAT

Podstawową funkcją usług translacji adresów sieciowych (**NAT** – *Network Address Translation*) jest umożliwienie urządzeniom pracującym w sieci lokalnej dostępu do sieci Internet. Przypomnijmy, że w sieciach komputerowych wykorzystujący adresowanie IPv4

(obecnie większość sieci oparta jest właśnie o ten protokół) wykorzystuje się w komunikacji dwa typy adresów IPv4:

- adresy prywatne,
- adresy publiczne.

Adresy prywatne stosowane są w **sieciach LAN**, natomiast **publiczne** w **sieciach WAN** oraz **internecie**. Najczęściej sieci lokalne posiadają tylko jeden publiczny adres IP, tak więc, aby urządzenia z tych sieci (posiadające przecież adresy IP prywatne) mogły komunikować się z siecią Internet (gdzie stosowane są adresy publiczne), potrzebna jest usługa, która zamieni adres prywatny pochodzący od komputera z sieci lokalnej na adres publiczny widoczny w Internecie, jeśli ten komputer chce np. odwiedzić stronę WWW.



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Usługa NAT działa również na **styku sieci lokalnych**, jeśli struktura tych sieci jest bardzo złożona i wieloelementowa. Podstawowa funkcja usług NAT to jednak **translacja – tłumaczenie – zamiana** adresów IP na takie, które wymagane są w danej sieci.

Dzięki swojej specyficznej architekturze usługa NAT pozwala również zapewnić pewien stopień bezpieczeństwa sieci, w jakich jest uruchomiona, blokując połączenia przychodzące z Internetu. Po prostu **nie przepuszcza ruchu sieciowego, który „przychodzi" z zewnątrz**, jeśli oczywiście w jej konfiguracji nie zezwolono na wyjątki. Dzięki temu, jeśli jakiś haker zechce z Internetu dostać się do naszej sieci LAN, to nie będzie mógł tego zrobić.

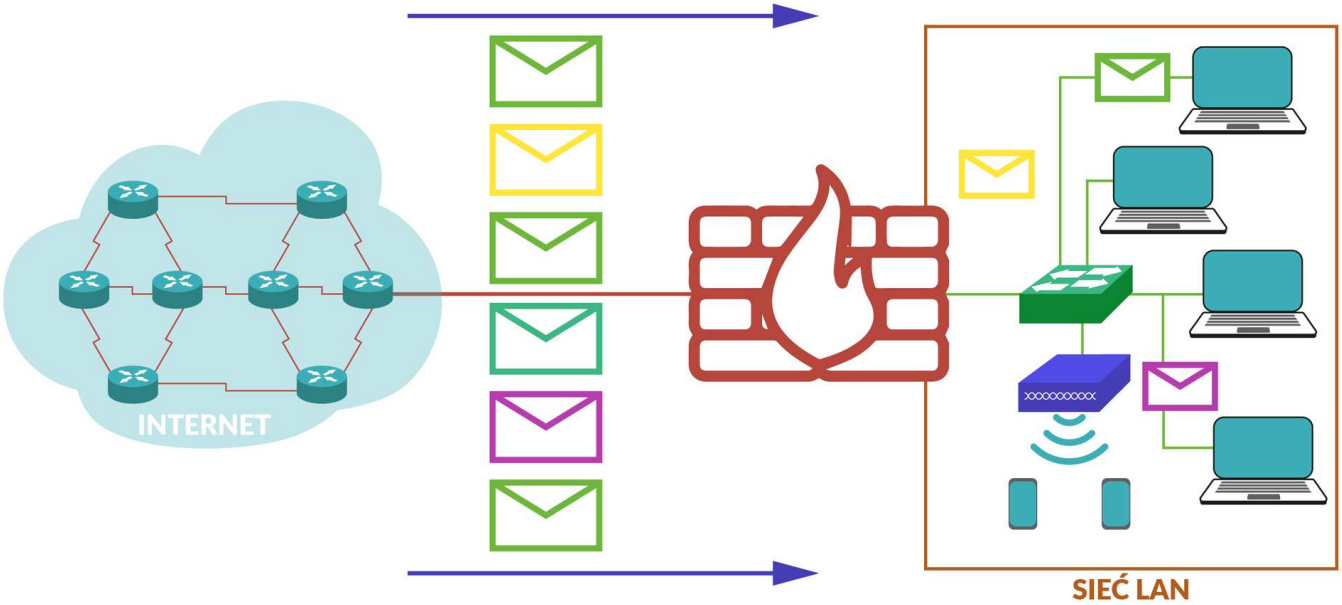
> **Ważne!**
>
> Usługa NAT blokuje cały ruch do sieci LAN pochodzący z Internetu!

Firewall, czyli zapora ogniowa

Kolejnym elementem zabezpieczenia sieci lokalnej jest odpowiednie skonfigurowanie **zapory/ściany ogniowej** (ang.firewall).

> **Ważne!**
>
> Zapora sieciowa to mechanizm bezpieczeństwa sieci komputerowych pozwalający tworzyć reguły, na podstawie których ruch sieciowy przychodzący do naszej sieci jest blokowany lub akceptowany. Reguły blokujące lub zezwalające na dany ruch mogą być tworzone na podstawie **adresów IP** lub na podstawie **nazw domenowych** (w sieciach komputerowych stosuje się nazwy domenowe, aby ułatwić wyszukiwanie urządzeń i usług po nazwach, a nie po adresach IP). Dzięki temu możemy, np. **zablokować możliwość korzystania z określonych stron czy portali użytkownikom sieci LAN**.

Zasada działania zapory ogniowej jest stosunkowo prosta: kiedy pakiet danych trafi do rutera pełniącego funkcje zapory lub do urządzenia dedykowanego (w dużych sieciach komputerowych stosuje się dedykowane zapory ogniowe będące osobnymi urządzeniami), sprawdzane są parametry takiego pakietu (głównie adresy IP). Na podstawie zdefiniowanych przez administratora reguł urządzenie podejmuje decyzję czy dany pakiet zablokować i odrzucić, czy umożliwić mu dotarcie do sieci i konkretnego urządzenia.



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Proste funkcje zapory ogniowej zaimplementowane są praktycznie na każdym ruterze sieciowym, nawet na prostych urządzeniach, z których korzystamy w domu. Jeśli sieć komputerowa jest stosunkowo duża, ze sporą ilością użytkowników, powinno stosować się dedykowane zapory ogniowe z szerokim wachlarzem możliwości konfiguracyjnych.

W zapory ogniowe wyposażone są również systemy operacyjne urządzeń, z których korzystają użytkownicy sieci lokalnych. Tego typu zapory mogą również blokować ruch sieciowy przychodzący już do konkretnego komputera, ale dodatkowe pozwalają również

na definiowanie, jakie aplikacje na swojej maszynie może uruchamiać użytkownik. Systemy operacyjne z rodziny Microsoft Windows stosują zaporę tego typu.

Listy kontroli dostępu (ACL)

Ostatnim z trzech głównych mechanizmów bezpieczeństwa lokalnych sieci komputerowych są **listy kontroli dostępu** (ang. *Access Control List*). Mechanizmy **ACL** również implementowane są na ruterach sieciowych, a ich głównym zadaniem jest decydowanie o tym, jaki ruch sieciowy jest w sieci LAN akceptowany, a jaki nie. Zasada działania na pierwszy rzut oka jest podobna do zapory ogniowej. Zapora filtruje jednak ruch **przychodzący do sieci lokalnej**, natomiast ACL pozwala na **definiowanie ruchu wewnątrz sieci**, co również ma wpływ na jej bezpieczeństwo. Nawet jeśli do naszej sieci „dostanie" się niepożądany ruch, dzięki regułom ACL możemy ograniczyć jego zasięg, blokując dostęp do poszczególnych elementów sieci LAN.

Listy ACL administrator sieci komputerowej może tworzyć w oparciu o **adresy IP**, **numery portów aplikacji**, a także o konkretne **protokoły sieciowe**.

Reguły ACL zazwyczaj tworzone są w firmowych sieciach LAN, gdzie liczba użytkowników, a co za tym idzie zagrożeń, jest dużo większa niż, np. w naszych domach.

> **Ważne!**
>
> Reguły ACL umożliwiają definiowanie, jaki ruch sieciowy w sieci LAN jest dozwolony, a jaki zakazany. Ma to na celu zwiększenie bezpieczeństwa sieci oraz jej wydajności.

To nie wszystko...

Aby działania związane z bezpieczeństwem, jakie podjął administrator sieci były skuteczne, należy dodatkowo zadbać o bezpieczeństwo **urządzeń końcowych,** jakie w sieci pracują, czyli komputerów, smartfonów czy tabletów. Zabezpieczenie urządzeń końcowych opiera się w znacznej mierze na:

- zapewnieniu, aby oprogramowanie tych urządzeń było **zawsze aktualne i zawierało wszystkie poprawki bezpieczeństwa** wydane przez producenta oprogramowania;
- instalacji na każdym z urządzeń **oprogramowania antywirusowego**, właściwie skonfigurowanego z aktualną bazą wirusów.

Wszystkie wymienione elementy bezpieczeństwa można nazwać **środkami technicznymi**. Zabezpieczają one sieć w znaczmy stopniu, jednak nie załatwiają kwestii bezpieczeństwa zupełnie. Aby spełniały swoją rolę i funkcję, czyli chroniły nas przed zagrożeniami, nie możemy im przeszkadzać, a czasem możemy im pomóc. Żadne techniczne środki bezpieczeństwa nie uchronią nas przed atakiem i kradzieżą danych, jeśli sami nie

będziemy rozważni i nie będziemy stosować podstawowych zasad bezpieczeństwa podczas korzystania z sieci.

Podczas pracy w sieci pamiętajmy o tym, aby:

- Korzystać z urządzenia **tylko przez jedną osobę**, a jeśli nie jest to możliwe – korzystać z kont użytkowników utworzonych na tym urządzeniu.
- Korzystać tylko ze stron internetowych **szyfrujących komunikację**, jeśli te wymagają podania od nas danych (np. danych logowania). Jeśli dana strona wymaga podania od nas danych, a nie szyfruje komunikacji łatwo możemy paść ofiarą kradzieży tych danych, jeśli ktoś przechwyci komunikację pomiędzy serwerem WWW, a naszą przeglądarką.
- **Nie logować się do poczty**, **konta bankowego** czy **portalu społecznościowego,** jeśli korzystamy z Internetu w **otwartej sieci WiFi** (np. sieci WiFi dla gości).
- **Nie klikać w linki niewiadomego pochodzenia** (np. te, które przyszły do nas pocztą elektroniczną).
- Instalować oprogramowanie pochodzące **tylko ze znanego i pewnego źródła**.
- **Nie podawać swoich danych osobowych** oraz **prywatnych zdjęć i filmów**, osobom których tożsamości nie jesteśmy pewni (np. tym, które poznaliśmy przez Internet).

Słownik

> **ACL**
>
> zbiór reguł i zasad definiujących, jaki ruch sieciowy jest w sieci LAN akceptowany
> **firewall**
>
> inaczej zapora ogniowa; mechanizm implementowany na ruterach sieciowych lub oprogramowaniu, pozwalający blokować ruch sieciowy pochodzący z Internetu do sieci lokalnej
> **NAT**
>
> usługa translacji adresy IPv4

Infografika

Polecenie 1

Zapoznaj się z infografiką. Zweryfikuj, które z zabezpieczeń stosowane są w twojej domowej sieci komputerowej.

Podstawy bezpieczeństwa

Dodatkowe zabezpieczenia

Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Wskaż, które urządzenie sieciowe łączy sieć LAN z internetem.

- ◯ punkt dostępu
- ◯ ACL
- ◯ przełącznik
- ◯ ruter
- ◯ zapora ogniowa

Ćwiczenie 2

Uzupełnij zdanie.

Ruter na kilku płaszczyznach może zapewnić bezpieczeństwo sieci lokalnej, którą obsługuje.

1. Poprzez usługę [ ] (ang. Network Address Translation).
2. Poprzez ustawienia [ ] sieciowej (ang. [ ]).
3. Poprzez listy [ ] dostępu (ang. [ ] – ACL).

Firewall | NAT | maskowania | Access Control List | zapory | kontroli | translacji

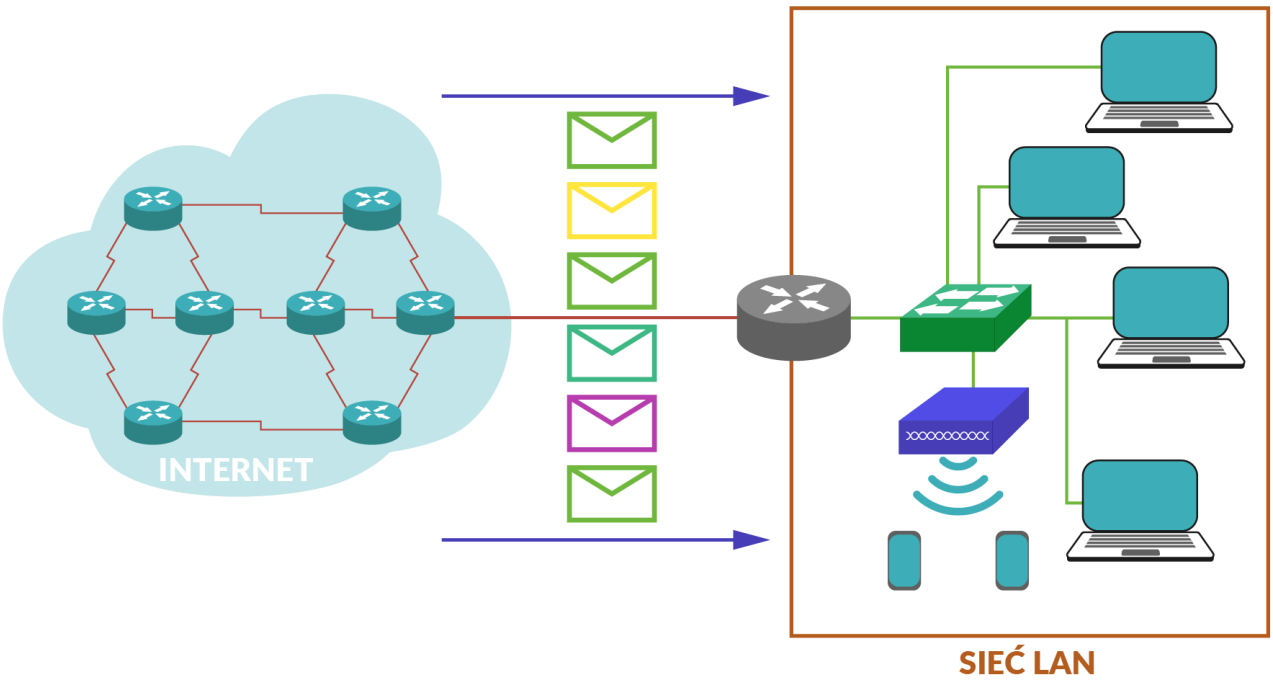
Ćwiczenie 3

Wskaż, które ze stwierdzeń dotyczących usługi NAT jest prawdziwe.

- [ ] tłumaczy tylko adresy publiczne na prywatne
- [ ] tłumaczy również adresy prywatne na prywatne, jeśli struktura sieci tego wymaga
- [ ] uruchamiana jest tylko w dużych sieciach komputerowych
- [ ] tłumaczy adresy publiczne na prywatne
- [ ] jest implementowane na ruterach sieciowych

Ćwiczenie 4

Wskaż, jaką funkcję należy uruchomić na ruterze sieciowym, aby ten zaakceptował lub odrzucił ruch sieciowy:



- ○ ACL
- ○ zapory ogniowej
- ○ NAT

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Ćwiczenie 5

Uzupełnij zdanie:

[ ] sieciowa filtruje [ ] [ ] do sieci [ ], natomiast [ ] pozwala na [ ] ruchu [ ] sieci [ ].

przychodzący | WAN | firewall | zewnątrz | LAN | lokalnej | ACL | ruch | wewnątrz | definiowanie | Zapora | wychodzący

Ćwiczenie 6

Wskaż, na podstawie jakich parametrów mogą być tworzone listy ACL.

- [ ] adresów MAC
- [ ] obciążenia łącza
- [ ] protokołów sieciowych
- [ ] numerów portów aplikacji
- [ ] ustawień zapory sieciowej
- [ ] adresów IP

Ćwiczenie 7

Dokończ zdanie.

Funkcją zapory sieciowej nie jest...

- ( ) definiowanie ruchu pomiędzy siecią LAN i siecią Internet.
- ( ) translacja adresów sieciowych.
- ( ) blokowanie poszczególnych grup adresów IP.
- ( ) blokowanie stron internetowych.

Ćwiczenie 8

Wskaż, które z elementy stanowią techniczne środki bezpieczeństwa sieci LAN i urządzeń w nich pracujących.

- [ ] korzystanie tylko z szyfrowanych stron WWW
- [ ] ACL
- [ ] NAT
- [ ] oprogramowanie antywirusowe
- [ ] unikanie wchodzenia w linki przesłane pocztą elektroniczną

Dla nauczyciela

Autor: Damian Stelmach
Przedmiot: Informatyka

Temat: Jak zabezpieczyć sieć lokalną?

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres rozszerzony

Podstawa programowa:

Cele kształcenia – wymagania ogólne

> III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, w tym: znajomość zasad działania urządzeń cyfrowych i sieci komputerowych oraz wykonywania obliczeń i programów.

Treści nauczania – wymagania szczegółowe

> III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi.
>
> > Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:
> >
> > > 3) opisuje warstwowy model sieci komputerowej oraz model sieci internet, opisuje podstawowe funkcje urządzeń i protokoły stosowane w przepływie informacji i w zarządzaniu siecią;
> > >
> > > 5) wyjaśnia, od czego zależy sprawne funkcjonowanie sieci komputerowej oraz szybki dostęp do jej usług i zasobów (parametry osprzętu sieciowego, szerokość pasma, zabezpieczenia typu ściana ogniowa i programy antywirusowe, możliwości serwera).

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Wymienisz zagrożenia, jakie czyhają na użytkowników internetu.
- Wyjaśnisz, jak unikać typowych niebezpiecznych zdarzeń.

- Przeanalizujesz mechanizm działania zapory ogniowej oraz usługi NAT.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimedium i ćwiczeń interaktywnych;
- metody aktywizujące.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda;
- telefony z dostępem do internetu.

Przebieg lekcji

Przed lekcją:

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Jak zabezpieczyć sieć lokalną?". Nauczyciel prosi uczniów o zapoznanie się z treściami w sekcji „Przeczytaj".

Faza wstępna:

1. Nauczyciel wyświetla uczniom temat, wskazuje cele zajęć oraz ustala z uczestnikami zajęć kryteria sukcesu.
2. Prowadzący prosi uczniów, aby zgłaszali swoje propozycje pytań do tematu. Jedna osoba może zapisywać je na tablicy. Gdy uczniowie wyczerpią swoje pomysły, a pozostały jakieś ważne kwestie do poruszenia, nauczyciel je dopowiada.

Faza realizacyjna:

1. **Praca z tekstem.** Uczniowie przystępują do cichego czytania tekstu e-materiału. Indywidualnie zapoznają się z treścią w sekcji „Przeczytaj".

2. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Infografika". Uczniowie wspólnie zapoznają się z treścią zawartego w niej multimedium. Zapisują ewentualne problemy i pytania. Po czym następuje dyskusja, w trakcie której nauczyciel wyjaśnia niezrozumiałe treści.
3. **Ćwiczenie umiejętności.** Uczniowie wykonują ćwiczenia nr 1-5 z sekcji „Sprawdź się". Nauczyciel sprawdza poprawność wykonanych zadań, omawiając je wraz z uczniami.

Faza podsumowująca:

1. Nauczyciel wyświetla na tablicy temat lekcji i cele zawarte w sekcji „Wprowadzenie". W kontekście ich realizacji podsumowuje przebieg zajęć, a także wskazuje mocne i słabe strony pracy uczniów.

Praca domowa:

1. Uczniowie wykonują ćwiczenia 6-8 z sekcji „Sprawdź się".

Wskazówki metodyczne:

- Treści w sekcji „Przeczytaj" można wykorzystać jako podsumowanie i utrwalenie wiedzy uczniów.