Ostoja

150 wizualnych map konfiguracji UniFi

Od planu sieci do sprawdzonego wdrożenia



Znajdź ustawienie.

Wykonaj kroki.

Sprawdź wynik.

Gateway • przełączniki • Wi-Fi • VLAN • firewall • VPN

Niezależny przewodnik praktyczny

Jak korzystać z map

1. Wybierz zadanie

Zacznij od spisu modułów. Numer mapy oznacza zadanie, a numer w stopce oznacza stronę.



2. Sprawdź warunki

Zapisz model urządzenia i wersję aplikacji. Potwierdź, że funkcja jest dostępna w Twoim środowisku.



3. Wykonaj kroki

Przeczytaj całą mapę przed zmianą. Modyfikuj jeden element naraz i zapisuj poprzednie wartości.



4. Potwierdź wynik

Sprawdź podany test. Sam zapis ustawienia nie potwierdza poprawnego działania sieci.



5. Zapisz dokumentację

Zanotuj zmianę, wynik i sposób cofnięcia. W razie błędu wróć do ostatniej działającej konfiguracji.



Legenda

- Niebieski: kolejność i połączenia.
- Zielony: poprawny wynik.
- Czerwony: błąd lub blokada.
- Żółty: warunek do sprawdzenia.

Schematy przedstawiają przykłady, nie zrzuty konkretnej wersji interfejsu.

Wersja, zgodność i bezpieczna zmiana



1. Zapisz punkt wyjścia

Model gateway: _____

UniFi OS / firmware: _____

UniFi Network: _____

Data sprawdzenia: _____



2. Sprawdź zgodność

Dostępność funkcji zależy od modelu, wersji i sposobu zarządzania. Nazwy menu mogą zmieniać się między wydaniami.

Firewall oparty na strefach

Wymaga UniFi Gateway, UniFi Network 9.0.108 lub nowszego oraz oprogramowania gateway 4.1 lub nowszego.

3. Przygotuj powrót

Przed zmianą wykonaj kopię konfiguracji. Upewnij się, że znasz lokalny sposób logowania i masz zapisane poprzednie ustawienia.



4. Zmieniaj etapami

Nie zmieniaj jednocześnie adresacji zarządzającej, reguł dostępu i konfiguracji uplinku. Po każdym kroku sprawdź łączność.



5. O tym materiale

Niezależny przewodnik Ostoja. Nie jest oficjalną dokumentacją Ubiquiti. Scenariusze i dane klientów są przykładowe. W razie rozbieżności sprawdź aktualną dokumentację producenta przed zastosowaniem ustawień.

Źródła: [3]

Ostoja | Nawigacja

Spis modułów

01 **Planowanie i dostęp** | str. 5

Mapy 001–015: projekt, adresacja, zasilanie i dostęp administratora.



02 **Kontroler i adopcja** | str. 21

Mapy 016–030: uruchomienie, urządzenia, uprawnienia i kopie.



03 **Internet i gateway** | str. 37

Mapy 031–045: WAN, dostawca, łącze zapasowe i trasy.



04 **Sieci lokalne i usługi** | str. 53

Mapy 046–060: VLAN, DHCP, DNS i adresacja.



05 **Przełączniki i porty** | str. 69

Mapy 061–075: porty, uplinki, PoE i kontrola połączeń.



06 **Wi-Fi** | str. 85

Mapy 076–090: SSID, pasma, kanały i klienci.



07 **Goście i izolacja** | str. 101

Mapy 091–105: dostęp gości, portal i testy izolacji.



08 **Firewall i bezpieczeństwo** | str. 117

Mapy 106–120: strefy, wyjątki i reguły dostępu.



09 **VPN i routing** | str. 133

Mapy 121–135: dostęp zdalny, tunele i kierowanie ruchem.



10 **Utrzymanie i odbiór** | str. 149

Mapy 136–150: diagnostyka, odtwarzanie i dokumentacja.



Źródła i zgodność | str. 165–166



Ostoja • Moduł 1

Planowanie i dostęp



Zanim zmienisz sieć, ustal, co już działa i jak odzyskasz dostęp. Dobrze opisany przewód bywa cenniejszy niż kolejna próba konfiguracji.

1 W tym module rozpoznasz wersje i role urządzeń, narysujesz topologię, zaplanujesz adresy, VLAN-y, PoE oraz rozmieszczenie AP.



2 Pracuj na kopii projektu. Dla każdego urządzenia zapisz model, MAC, miejsce i właściciela; nie zapisuj haseł na mapie.



3 Wynik: zatwierdzony plan bez nakładających się zakresów, sprawdzony dostęp lokalny i konkretna procedura wycofania pierwszej zmiany.



4 Źródła: [11], [10], [6], [1]



Sprawdź wersję UniFi Network

Ostoja • Mapa 001

Najpierw zapisz wersję aplikacji Network i systemu konsoli. Numer firmware AP jest osobną informacją; nie określa układu całego panelu.

GDZIE: Site Manager → Update Manager;
lokalnie Settings → Control Plane → Updates.

Wersja aplikacji Network

Network (vX.Y.Z)

Konsola

Wersja systemu UniFi OS

UniFi OS (vX.Y.Z)

Firmware AP
(to osobna informacja)

AP firmware (vX.Y.Z)

Nie określa układu całego panelu.

1. Wybierz właściwą lokalizację i konsolę; porównaj jej nazwę z dokumentacją klienta.
2. Odczytaj wersję Network oraz UniFi OS, jeżeli host korzysta z UniFi OS.
3. Zapisz datę odczytu i kanał aktualizacji. Nie uruchamiaj aktualizacji podczas samego rozpoznania.

PRZYKŁAD: Wpis: Kraków / Network: ____ / UniFi OS: ____ / data: ____.
Własny serwer może nie mieć UniFi OS.

PUŁAPKA: Nie dobieraj instrukcji tylko po wyglądzie ikon.

SPRAWDŹ / COFNIJ: Ponownie otwórz tę samą instancję.
Zgodność nazwy i obu wersji kończy rozpoznanie; konfiguracja pozostaje bez zmian.

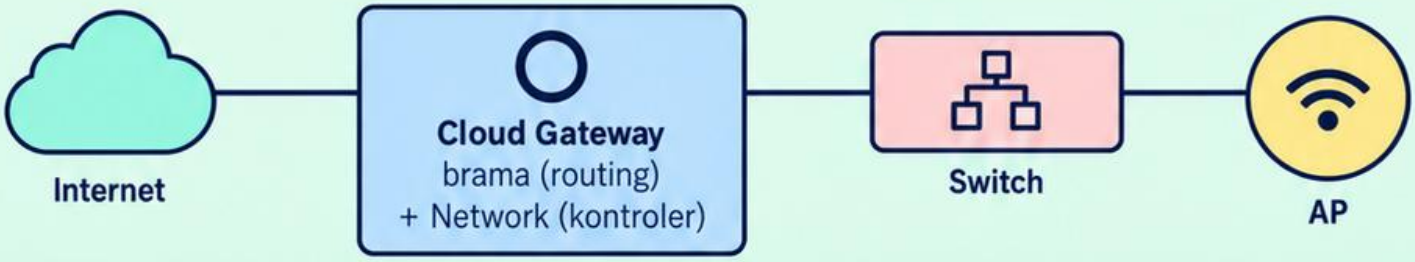
Źródła: [23]

Ostoja • Mapa 002

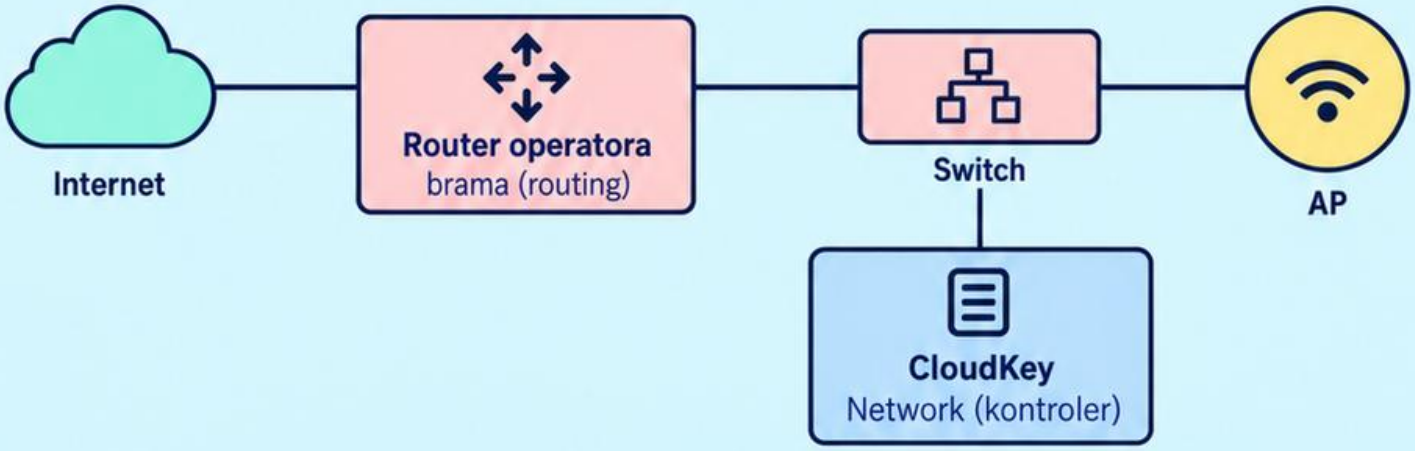
Rozpoznaj bramę i kontroler

Ustal, które urządzenie routuje ruch, a które uruchamia Network.
Cloud Gateway może łączyć te role; CloudKey sam nie zastępuje routera.

Wariant 1: Cloud Gateway – brama i kontroler w jednym urządzeniu



Wariant 2: CloudKey + router operatora – oddzielne role



GDZIE:
Site Manager → wybrana lokalizacja; Network → UniFi Devices.

PRZYKŁAD:
Biuro: CloudKey zarządza AP, a router operatora pozostaje bramą. Dwa urządzenia, dwie odpowiedzialności.

1. Odczytaj model konsoli lub adres własnego serwera Network.
2. Na komputerze sprawdź adres bramy domyślnej i porównaj z urządzeniem w szafie.
3. Zapisz fizyczny port WAN oraz połączenie brama–switch. Oznacz urządzenia spoza UniFi.

PUŁAPKA:
Brak bramy UniFi w panelu nie oznacza braku routera w sieci.

SPRAWDŹ / COFNIJ:
Z komputera otwórz lokalny panel kontrolera. Sprawdź bramę w konfiguracji IP; niczego nie resetuj.

Źródła: [11], [10]

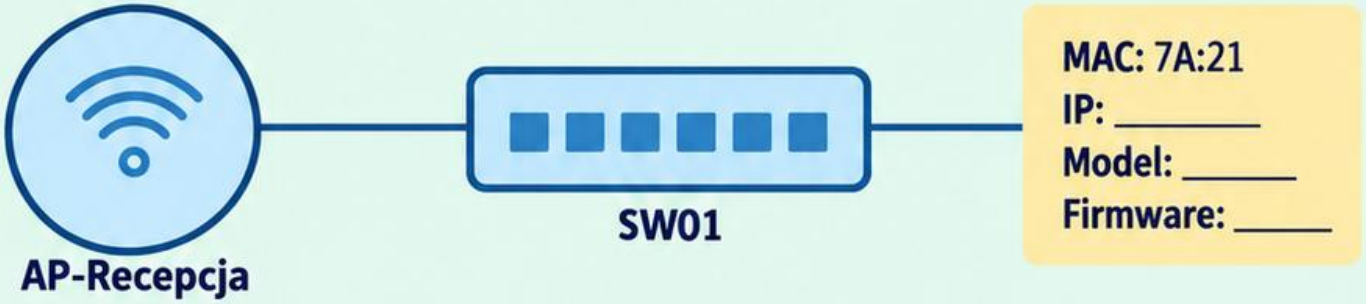
Zinwentaryzuj switche i AP

Ostoja • Mapa 003

Stwórz rejestr sprzętu przed adopcją i zmianami.
Licz urządzenia fizyczne, także te niewidoczne w aplikacji lub zarządzane przez inną instancję.

GDZIE: Network → UniFi Devices; dane techniczne: techspecs.ui.com.

1. **Dla każdego urządzenia zapisz model, MAC, lokalizację, adres IP oraz firmware.**



2. **Porównaj MAC z etykietą;** przy podobnych nazwach nie polegaj na kolejności listy.

3. **Dopisz źródło zasilania, numer portu uplink i właściciela urządzenia.**

PRZYKŁAD:
AP-Recepcja | MAC kończy się 7A:21 | switch SW01/8 | PoE+ | firmware: _____.

PUŁAPKA:
Nazwa AP nie dowodzi, że wskazujesz właściwy egzemplarz.

SPRAWDŹ / COFNIJ:
Porównaj liczbę pozycji ze sprzętem na miejscu.
Niewyjaśnione braki oznacz jako zadanie; nie usuwaj wpisów z panelu.

Źródła: [24], [6]

Ostoja • Mapa 004

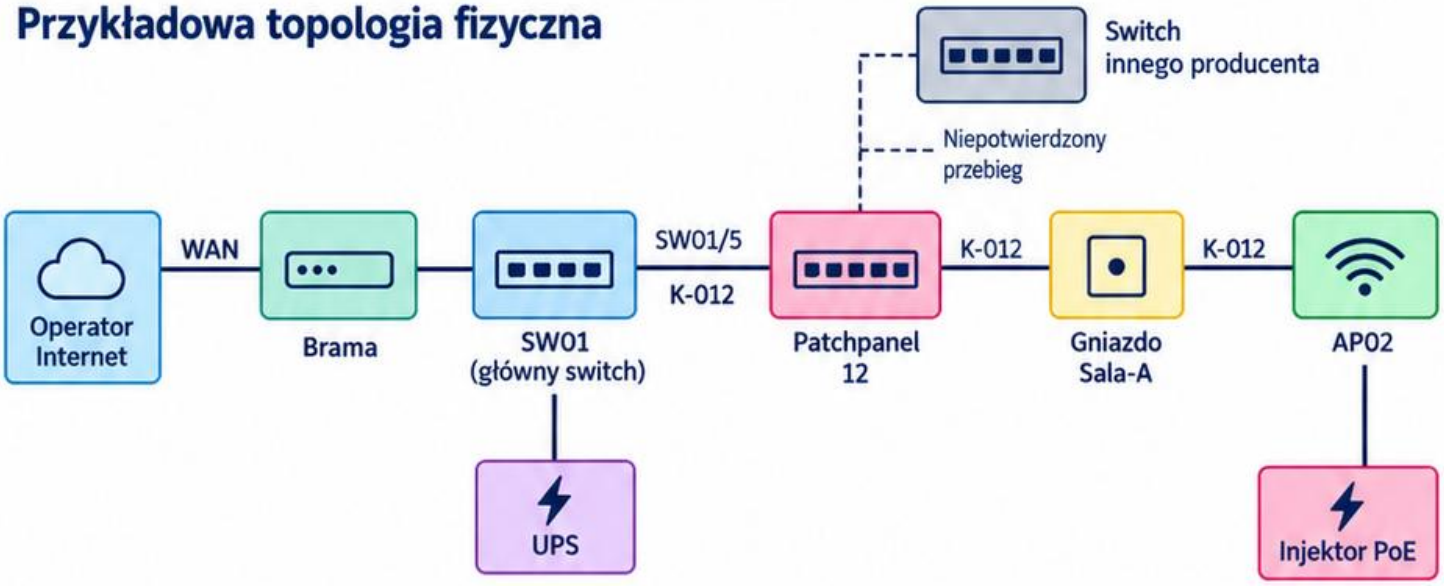
Narysuj topologię fizyczną

Mapa ma pokazywać przewody i źródła zasilania. Widok aplikacji jest punktem startowym, zwłaszcza gdy po drodze stoją switche innych producentów.

GDZIE: Network → Topology; weryfikacja przy szafie i gniazdach.

1. Zacznij od zakończenia łącza operatora, następnie narysuj WAN, bramę i główny switch.
2. Dla każdego uplinku wpisz oba numery portów i rodzaj medium.
3. Dodaj AP, patchpanel, injektory PoE i UPS. Oznacz przebieg niepotwierdzony linią przerywaną.

Przykładowa topologia fizyczna



PRZYKŁAD:
SW01/5 → patchpanel 12 → gniazdo Sala-A → AP02.
Etykieta przewodu: K-012.

PUŁAPKA:
Automatyczna topologia może nie pokazać poprawnie każdego urządzenia pośredniego.

SPRAWDŹ / COFNIJ:
Porównaj etykiety na obu końcach. Weryfikuj pojedyncze połączenie bez odłączania produkcyjnego uplinku.

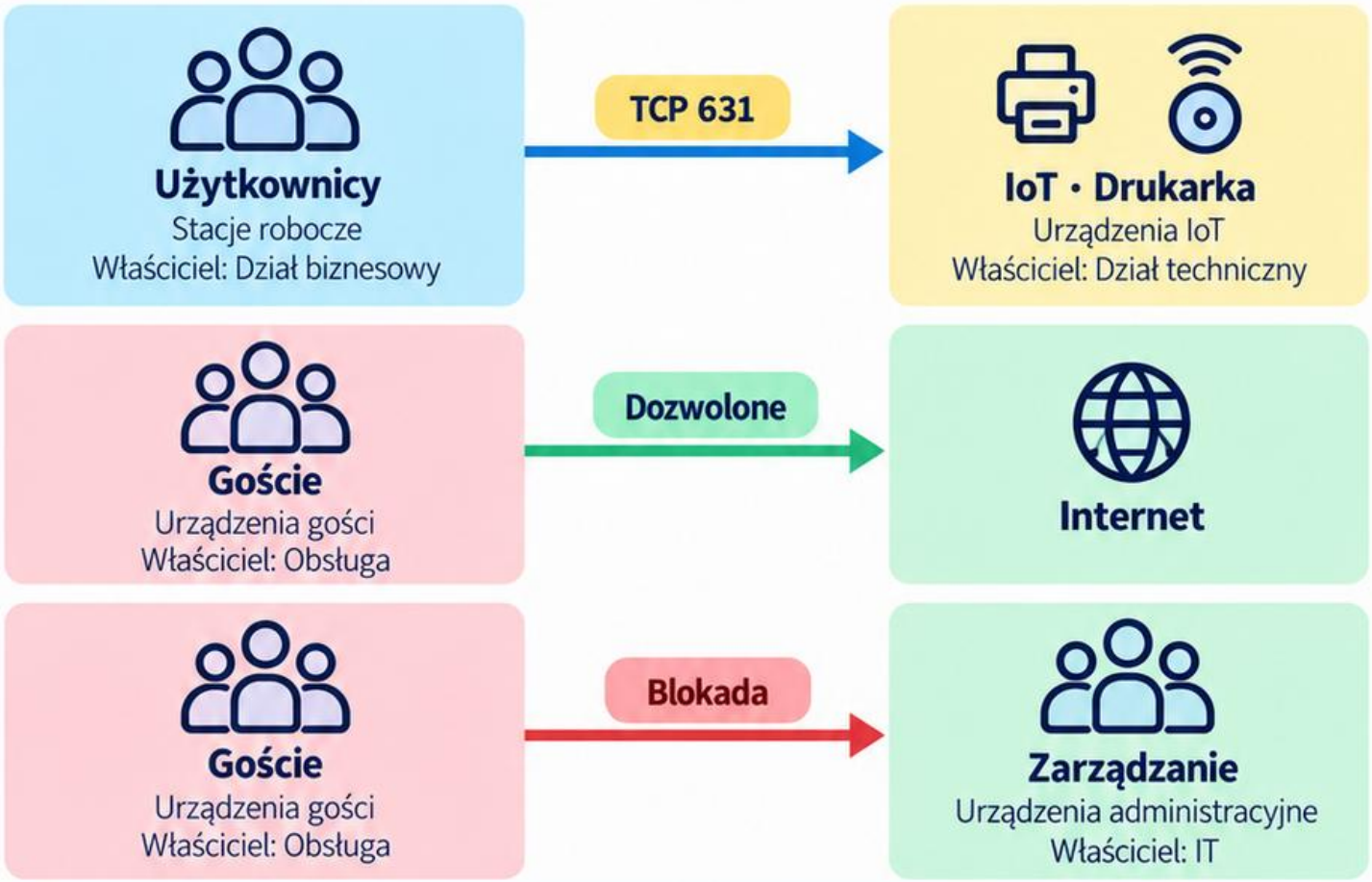
Źródła: [1], [4]

Zaplanuj topologię logiczną

Ostoja • Mapa 005

Rozdziel funkcje: zarządzanie, użytkownicy, goście i IoT. Schemat logiczny pokazuje granice routingu oraz dozwolone usługi, niezależnie od liczby switchy.

GDZIE: Arkusz projektu; istniejące sieci: Settings → Networks.



1. Wypisz grupy urządzeń i właściciela każdej usługi.
2. Dla każdej grupy wybierz VLAN, podsieć, router oraz źródło DHCP i DNS.
3. Narysuj tylko potrzebne połączenia między grupami, z kierunkiem i numerem portu usługi.

PRZYKŁAD: Pracownicy → drukarka: TCP 631; goście → internet; goście → zarządzanie: blokada.

PUŁAPKA: Samo utworzenie VLAN nie tworzy pełnej polityki izolacji.

SPRAWDŹ / COFNIJ: Przejdź po schemacie z właścicielem usług. Każda strzałka ma uzasadnienie; nie wdrażaj nieuzgodnionych połączeń.

Źródła: [1], [20]

Ostoja

Dobierz rozłączne podsieci

Ostoja • Mapa 006

Zarezerwuj odrębny zakres dla każdego segmentu. Sprawdzaj całe prefiksy; różne adresy bram mogą nadal należeć do tej samej podsieci.

GDZIE: Settings → Networks oraz dokumentacja sieci zdalnych i VPN.

1. Wypisz zakresy LAN, WAN prywatnej, VPN i oddziałów.
2. Dla każdej podsieci określ adres sieci, prefiks i przewidywaną liczbę hostów.
3. Porównaj zakresy przed zapisaniem projektu; uwzględnij przyszłe połączenia między biurami.

PRZYKŁAD: VLAN 10: 192.168.10.0/24; VLAN 20: 192.168.20.0/24.
W typowej /24 dostępne są 254 adresy hostów.

VLAN 10
192.168.10.0/24
254 adresy hostów

VLAN 20
192.168.20.0/24
254 adresy hostów

PUŁAPKA: 192.168.10.1/24 i 192.168.10.200/24 należą do tej samej sieci.

192.168.10.1/24 ✕ 192.168.10.200/24

SPRAWDŹ / COFNIJ:
Sprawdź brak przecięcia wszystkich zakresów. Konflikt rozwiąż w projekcie, zanim zmienisz adres bramy produkcyjnej.

Źródła: [1], [25]

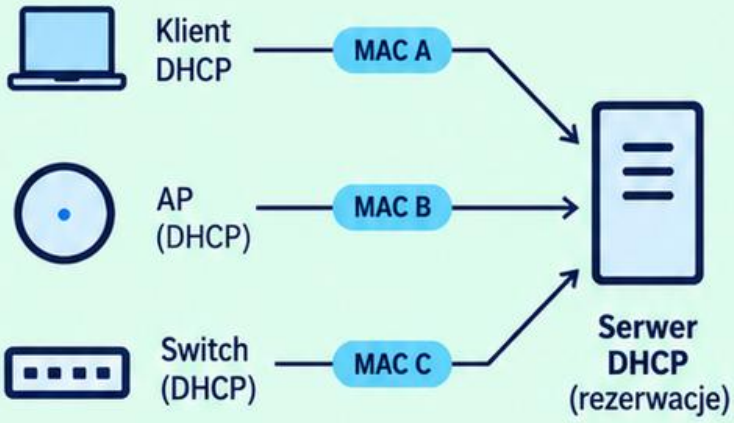
Ostoja • Mapa 007

Zarezerwuj adresy infrastruktury

Dla sprzętu używającego DHCP stosuj rezerwacje powiązane z właściwym MAC. Dla adresów wpisanych ręcznie prowadź osobny rejestr i wyklucz kolizje.

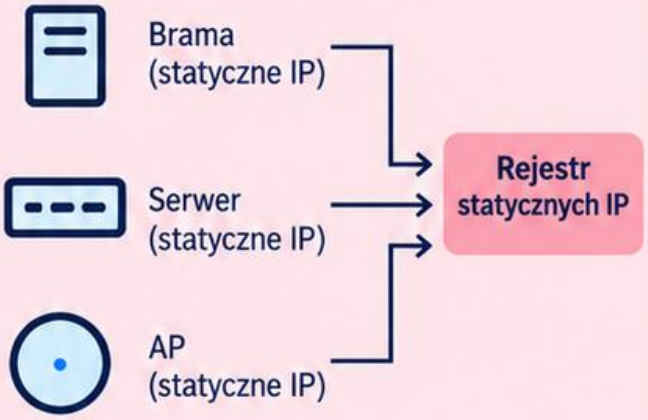
Urządzenia z DHCP

Rezerwacje powiązane z MAC



Urządzenia ze statycznym IP

Osobny rejestr, bez kolizji z DHCP



GDZIE:

Klient DHCP: Client Devices → klient → Settings → Fixed IP Address.

Adoptowana infrastruktura: sprawdź osobno IP Settings w UniFi Devices.

KROKI:

1. Ustal adres bramy, DNS, switchy, AP i serwerów.
2. Zidentyfikuj interfejs urządzenia po MAC; interfejs przewodowy i Wi-Fi mogą mieć inne adresy.
3. Dodaj rezerwację, zastosuj ustawienia i odnów dzierżawę w uzgodnionym oknie.

PRZYKŁAD:

SW01: 192.168.10.11; AP01: 192.168.10.21; rejestr zawiera MAC i sposób przydziału.

Nazwa	Adres IP	MAC	Sposób przydziału
SW01	192.168.10.11	MAC	Rezerwacja DHCP
AP01	192.168.10.21	MAC	Rezerwacja DHCP

PUŁAPKA:

Rezerwacja DHCP nie zmienia adresu urządzenia skonfigurowanego statycznie.

SPRAWDŹ / COFNIJ:

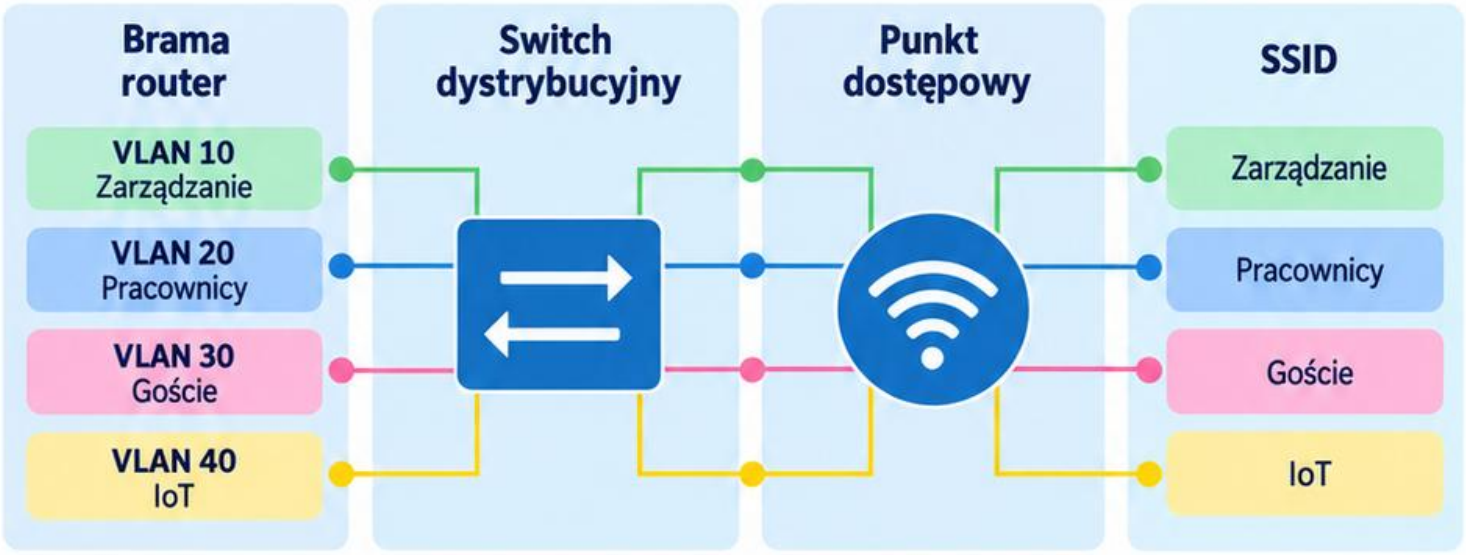
Po odnowieniu sprawdź IP i panel zarządzania. Przy błędzie usuń nową rezerwację i przywróć poprzedni zapis.

Źródła: [26], [12]

Przydziel VLAN-y według funkcji

Identyfikator VLAN oznacza segment warstwy drugiej. Zaplanuj jego znaczenie jednolicie na bramie, switchach i punktach dostępowych.

GDZIE: Settings → Networks; przypisanie realizują porty switcha lub SSID.



1. Przypisz jedną funkcję do każdej planowanej sieci.
2. Nadaj unikalne VLAN ID i podsieci, a następnie wskaż właściwy router.
3. Rozpisz porty dostępowe, uplinki z tagami oraz SSID korzystające z danego VLAN.

PRZYKŁAD: 10 Zarządzanie; 20 Pracownicy; 30 Goście; 40 IoT.
To przykład projektu, nie wymagane numery UniFi.

PUŁAPKA: VLAN w nazwie SSID nie oznacza rzeczywistego przypisania.

SPRAWDŹ / COFNIJ: Porównaj tabelę z konfiguracją wszystkich odcinków. Zmiany zarządzania wykonuj dopiero po przygotowaniu drogi powrotnej.

Źródła: [1], [4], [2]

Policz budżet PoE

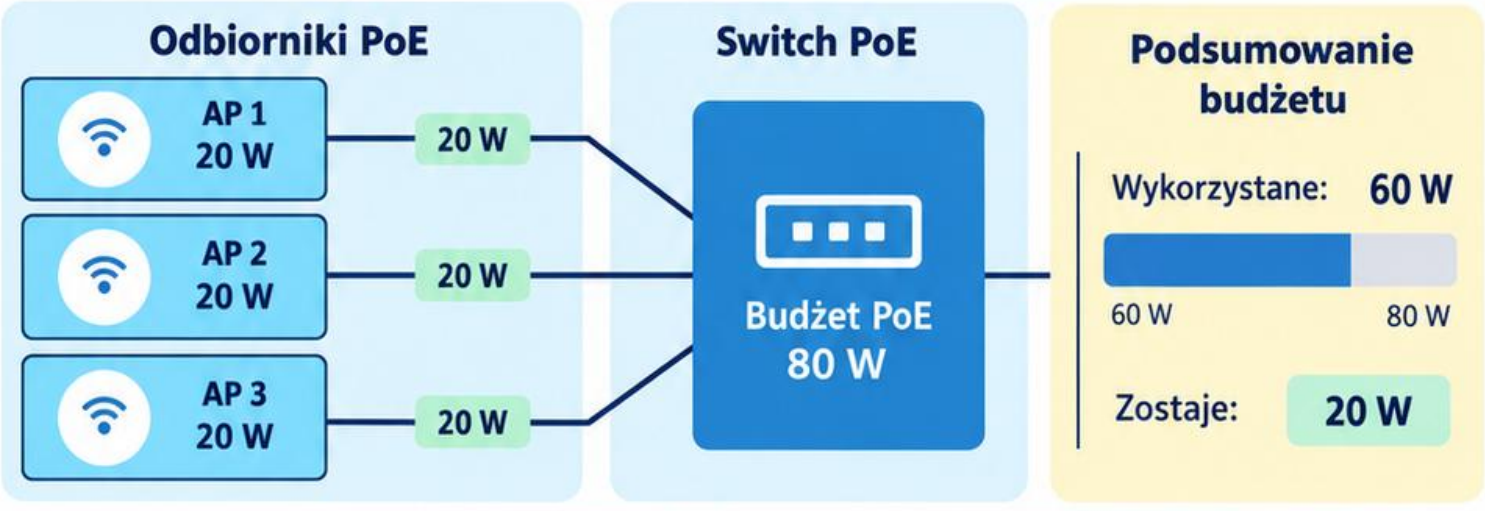
Ostoja • Mapa 009

Sprawdź osobno standard portu, limit portu i łączny budżet switcha. Licz maksymalne zapotrzebowanie urządzeń, nie sam bieżący pobór.

GDZIE: Tech Specs konkretnego modelu;
UniFi Devices → switch → Overview → Power Utilization.

1. Odczytaj wymagania każdego AP i innego odbiornika ze specyfikacji.
2. Zsumuj moce maksymalne i porównaj z budżetem dostępnym przy faktycznie używanym zasilaczu.
3. Sprawdź zgodność standardu na każdym porcie; dopisz zaplanowaną rezerwę projektową.

PRZYKŁAD: 3 x 20 W = 60 W. Przy budżecie 80 W zostaje 20 W; każdy port nadal musi obsługiwać wymagany standard.



PUŁAPKA:
Nie zakładaj zgodności pasywnego 24 V z aktywnym PoE.

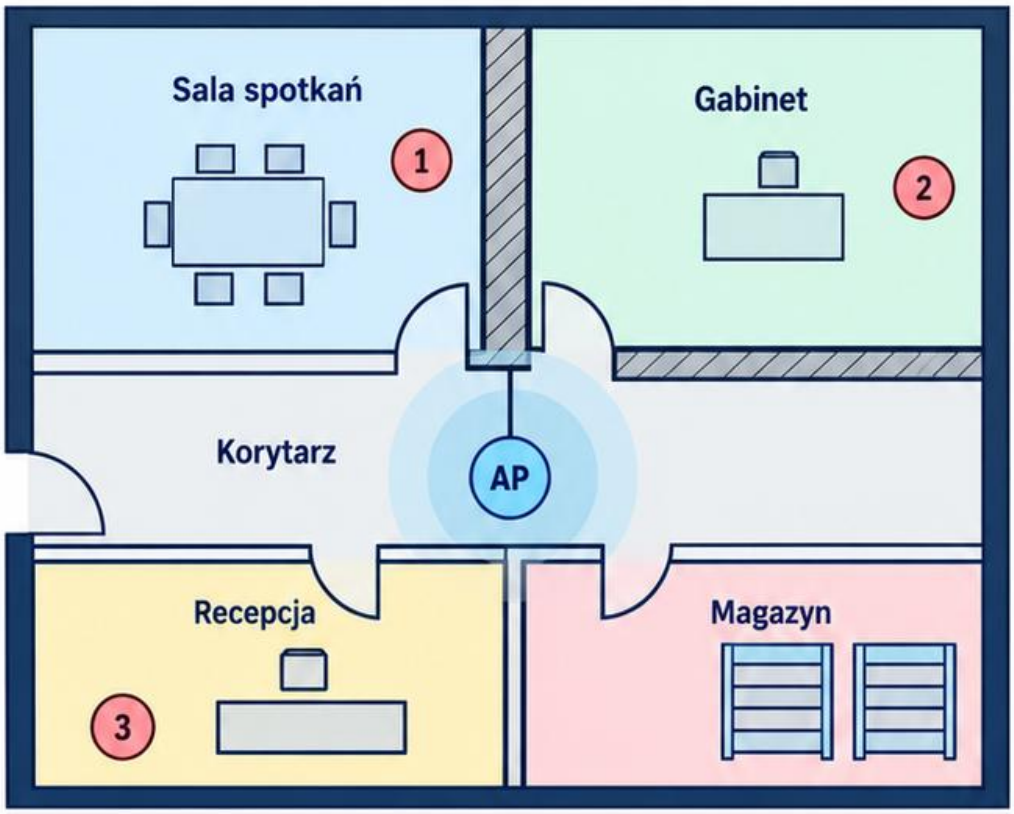
SPRAWDŹ / COFNIJ:
Uruchom odbiorniki razem i obserwuj restartowanie oraz pobór. Przy przeciążeniu odłącz nowy odbiornik lub użyj właściwego zasilania.

Źródła: [6]

Zaplanuj rozmieszczenie AP

Ostoja • Mapa 010

Rozmieszczenie dobieraj do ścian, użytkowników i ruchu, nie do samej powierzchni. Projekt radiowy wymaga późniejszego pomiaru z urządzeniem klienta.



Legenda

- AP — Punkt dostępowy (AP)
- 1 — Punkt pomiarowy klienta (1–3)
- Ściana żelbetowa
- Ściana działowa
- Orientacyjny zasięg AP

1. Nanieś pomieszczenia, materiały ścian i miejsca pracy na rzut.
2. Zaznacz punkty montażu z przewodem i zgodnym zasilaniem; uwzględnij charakterystykę anteny modelu.
3. Sprawdź miejsca krytyczne: sala spotkań, recepcja, magazyn. Zapisz wynik i rodzaj klienta.

GDZIE: UniFi Design Center: design.ui.com; pomiary na miejscu przez WiFiman.

PRZYKŁAD: Gabinet za dwiema żelbetowymi ścianami może wymagać innej lokalizacji AP niż sąsiedni otwarty pokój.

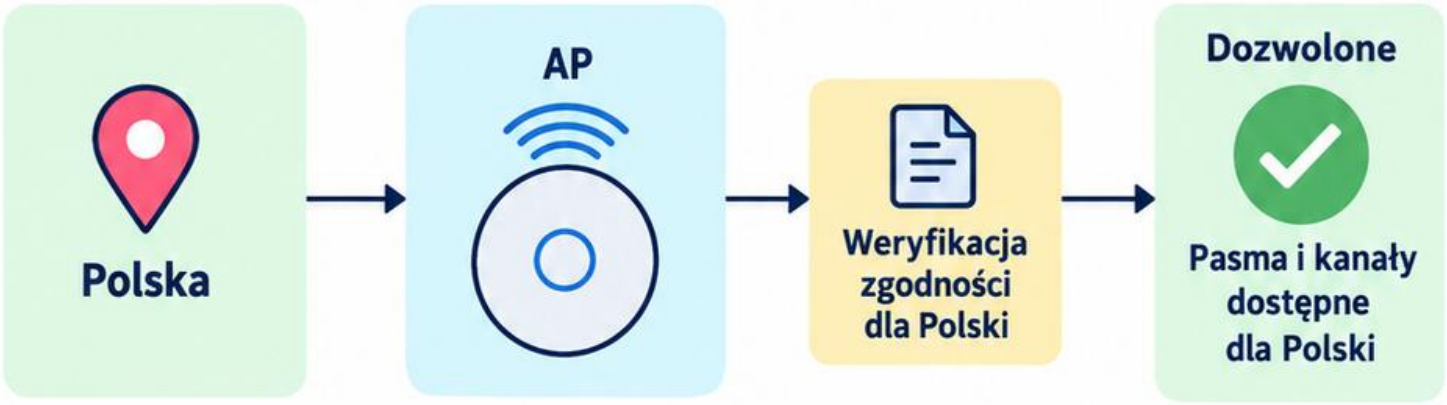
PUŁAPKA: Zwiększenie mocy AP nie wzmacnia nadajnika telefonu.

SPRAWDŹ / COFNIJ: Porównaj pomiary w tych samych punktach przed i po montażu. Zachowaj poprzednie miejsce jako wariant powrotu.

Źródła: [19]

Potwierdź kraj i domenę radiową

Ustawienia muszą odpowiadać rzeczywistemu miejscu instalacji. Dla wdrożenia w Polsce potwierdź kraj *Poland* i zgodność regionalnej wersji urządzenia.



GDZIE:
Konfiguracja lokalizacji i radia właściwej wersji; wymagania modelu w *Tech Specs* oraz *Regions Supporting 6 GHz*.

1. Zapisz aktualny kraj, model AP oraz wersje Network i firmware.
2. Sprawdź w dokumentacji modelu dostępne pasma, kanały i przeznaczenie do wnętrz lub na zewnątrz.
3. Wybieraj wyłącznie opcje udostępnione dla Polski. Po zmianie kraju ponownie sprawdź plan kanałów.

PRZYKŁAD:
Tabela Ubiquiti dla Polski wskazuje obsługę 6 GHz wewnątrz budynków; sam AP musi obsługiwać to pasmo.

PUŁAPKA:
Nie wybieraj innego kraju, aby odblokować dodatkowe kanały.

SPRAWDŹ / COFNIJ:
Porównaj kraj z adresem instalacji i dostępnymi kanałami. Przy niezgodności wstrzymaj wdrożenie radia i skoryguj projekt.

Źródła: [21], [19]

Ostoja

Ostoja • Mapa 012

Uporządkuj konta administratorów

Każdy administrator powinien pracować na własnym koncie. Ustal właściciela systemu, zastępcę i zakres odpowiedzialności przed przekazaniem dostępu.

Właściciel systemu

- pełny dostęp
- zarządzanie kontami
- odpowiedzialność za system

Zastępca administratora

- dostęp do wybranych aplikacji
- określone lokalizacje
- wsparcie w razie nieobecności

Ograniczony technik

- dostęp do jednej lokalizacji
- tylko niezbędne uprawnienia
- zgodnie z umową

Lokalizacja A | **Lokalizacja B** | **Lokalizacja C**

1. Spisz osoby, lokalizacje i rzeczywiście potrzebne uprawnienia.
2. Dodaj administratora przez New Admin i wybierz właściwe aplikacje oraz lokalizacje.
3. Potwierdź przyjęcie zaproszenia i logowanie zastępcy przed usunięciem starego dostępu.

GDZIE: Site Manager → People; lokalnie Network → Admins. W Fabric zarządzanie odbywa się na poziomie Fabric.

PRZYKŁAD: Serwis zewnętrzny: dostęp do jednej lokalizacji; pracownik odbierający wdrożenie: uprawnienia zgodne z umową.

PUŁAPKA: Konto użytkownika usług UniFi nie musi mieć uprawnień administratora.

SPRAWDŹ / COFNIJ: Z drugiej sesji sprawdź widoczność właściwej lokalizacji. Nie odbieraj ostatniego działającego dostępu właściciela.

Źródła: [14]

Skonfiguruj MFA i odzyskiwanie

Ostoja • Mapa 013

Zabezpiecz konto UI oraz zapewnij możliwość logowania po utracie telefonu. MFA konta UI i lokalne dane logowania mają inne zasady działania.

GDZIE: account.ui.com → Security → dodanie metody MFA.

1 Dodaj metodę uwierzytelniania, na przykład aplikację Verify lub generator kodów.



2 Skonfiguruj dodatkową dostępną metodę i zabezpiecz kody odzyskiwania poza telefonem.



3 Otwórz nową sesję i sprawdź logowanie; pozostaw dotychczasową sesję aktywną do zakończenia testu.



PRZYKŁAD:
Rejestr zawiera właściciela, datę testu i miejsce przechowywania kodów; nie zawiera samych kodów ani sekretu TOTP.

PUŁAPKA:
Nie usuwaj jedynej sprawnej metody przed sprawdzeniem nowej.

SPRAWDŹ / COFNIJ:
Zaloguj się przy użyciu metody zapasowej. Ubiquiti nie resetuje MFA po utracie wszystkich metod; przygotowanie ma znaczenie.

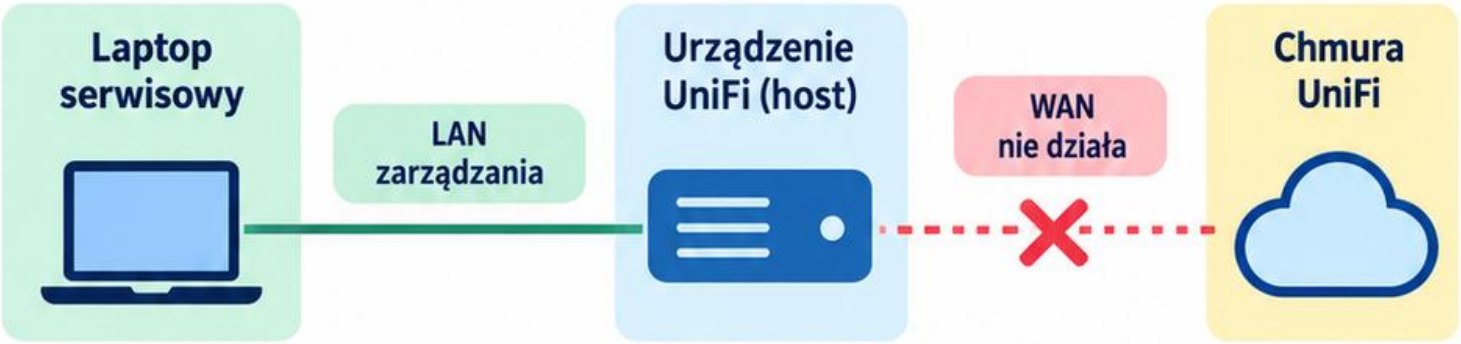
Źródła: [15]

Ostoja

Ostoja • Mapa 014

Przygotuj lokalny dostęp awaryjny

Sprawdź zarządzanie z LAN, zanim zmienisz WAN, VLAN zarządzania lub reguły dostępu. Sama działająca sesja chmurowa nie potwierdza gotowości lokalnej.



1. Zapisz adres hosta, port dostępu i port switcha dla laptopa serwisowego.
2. Podłącz laptop przewodem do dozwolonej sieci zarządzania i otwórz panel po adresie IP.
3. Sprawdź właściwe lokalne dane logowania, jeżeli zostały przygotowane; zabezpiecz je zgodnie z ustaleniami klienta.

GDZIE:
Przeglądarka → adres IP hosta UniFi; Cloud Gateway także przez unifi/.

PRZYKŁAD:
Własny Network Server zwykle używa HTTPS 8443; konsola używa HTTPS 443. Potwierdź faktyczny adres instalacji.

PUŁAPKA:
Nie wpisuj publicznego adresu chmurowego jako jedynej ścieżki awaryjnej.

SPRAWDŹ / COFNIJ:
W uzgodnionym oknie sprawdź lokalny dostęp przy odłączonym WAN. Przywróć kabel i potwierdź działanie usług.

Źródła: [10], [15]

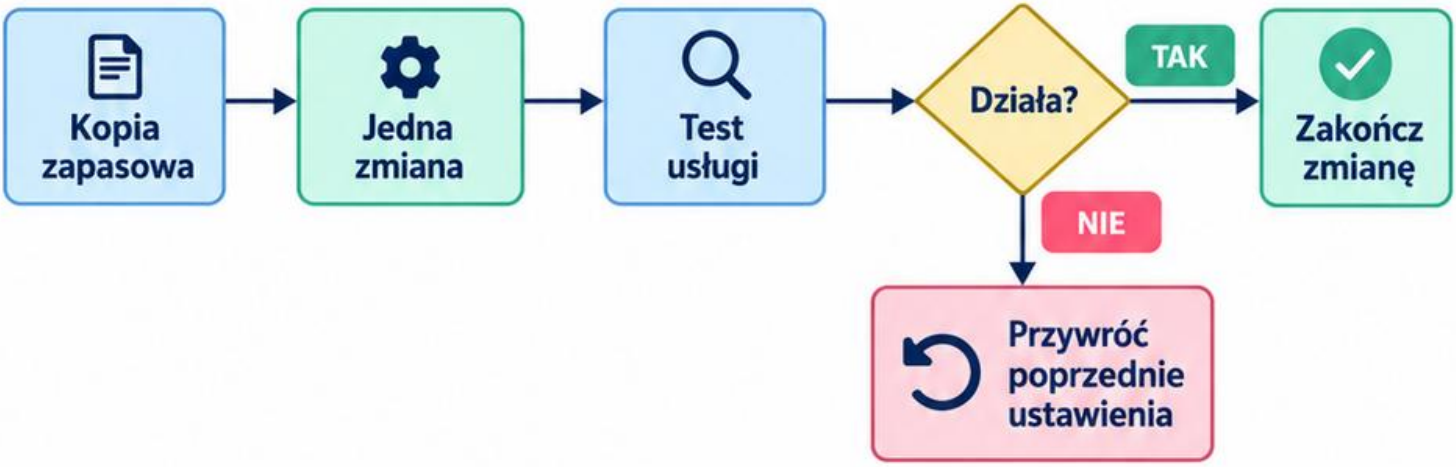
Zapisz plan zmiany i wycofania

Ostoja • Mapa 015

Przed pierwszym zapisem określ moment przerwania prac. Cofnięcie konkretnego parametru bywa szybsze niż odtwarzanie całej konfiguracji.

GDZIE: Karta zmiany oraz panel backupu odpowiedni dla hosta.

1. Zapisz cel, objęte urządzenia, parametry przed zmianą i planowany czas przerwy.
2. Pobierz aktualną kopię oraz sprawdź dostęp lokalny. Wyznacz osobę zatwierdzającą testy.
3. Ustal kolejność: jedna zmiana, test usługi, decyzja. Przypisz termin powrotu i konkretne ustawienia do przywrócenia.



PRZYKŁAD: Jeżeli po zmianie VLAN drukarka pozostaje niedostępna przez 5 minut, wróć do poprzedniego przypisania portu.

PUŁAPKA: Nie zmieniaj jednocześnie adresacji, uplinku i reguł, jeśli nie potrafisz rozdzielić przyczyny awarii.

SPRAWDŹ / COFNIJ: Przeczytaj procedurę drugiej osobie. Musi wskazać plik kopii, port awaryjny oraz warunek przerwania.

Źródła: [8], [10]

Ostoja

Ostoja • Moduł 2

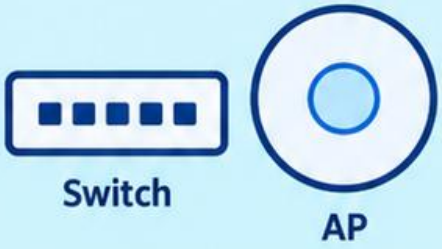
Kontroler i adopcja

Adopcja przypisuje urządzenie do aplikacji, która będzie nim zarządzać. Najpierw potwierdź właściciela, host Network, zasilanie i drogę komunikacji.

Host i konfiguracja początkowa



Dodanie urządzeń



Wariant między podsieciami



Nazwy i uprawnienia

Zaczniesz od wyboru hosta oraz konfiguracji początkowej. Następnie dodasz switch i AP, sprawdzisz wariant między podsieciami oraz uporządkujesz nazwy i uprawnienia.

Migracja i reset

Urządzenie zarządzane przez inną instancję wymaga ustalenia migracji. Reset traktuj jako zaplanowany zabieg, który usuwa konfigurację.

Wynik

Urządzenia Online we właściwej lokalizacji, działający klient testowy, zapisane wersje i kopia umożliwiająca odtworzenie.

Źródła: [24], [27], [11], [8]

Ostoja • Mapa 016

Wybierz sposób hostowania Network

Dobierz host do urządzeń, skali i odpowiedzialności za utrzymanie. Cloud Gateway łączy zarządzanie i routing; CloudKey oraz własny serwer wymagają osobnej bramy.

GDZIE: Dokumentacja *Choosing the Right UniFi Control Plane*; rejestr wymagań instalacji.

1. Spisz modele urządzeń, liczbę lokalizacji i wymagane aplikacje.
2. Wybierz Cloud Gateway, host lokalny albo obsługiwany hosting zgodnie z kompatybilnością urządzeń.
3. Ustal zasilanie, aktualizacje, kopie oraz osobę odpowiedzialną za dostępność hosta.

Jaki sposób hostowania wybrać?

Cloud Gateway

Łączy zarządzanie i routing.

CloudKey (host lokalny)

Wymaga osobnej bramy.

Własny serwer lub obsługiwany hosting

Wymaga osobnej bramy.

PRZYKŁAD: Istniejący router innego producenta może pozostać bramą przy CloudKey; zasady routingu nadal konfiguruje się na routerze.

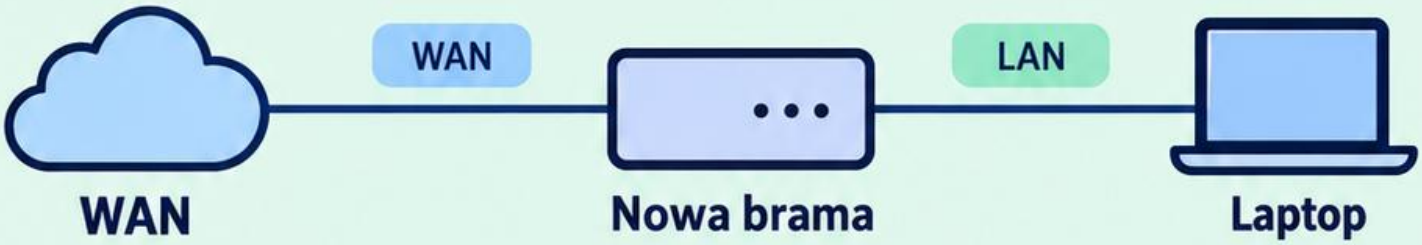
PUŁAPKA: Nie zakładaj, że każda brama UniFi może być adoptowana do dowolnego zewnętrznego hosta.

SPRAWDŹ / COFNIJ: Sprawdź zgodność konkretnego modelu z wybranym hostem przed zakupem. Zapisz alternatywę i koszt utrzymania.

Źródła: [11], [9]

Przejdź konfigurację początkową

Uruchom nową instalację w kontrolowanym środowisku. Nie podłączaj portu LAN nowej bramy do czynnej sieci z własnym DHCP bez projektu.



GDZIE: Aplikacja UniFi lub przeglądarka pod lokalnym adresem konsoli.

1. Połącz **WAN** zgodnie z wymaganiami operatora, a laptop do LAN konsoli.
2. Uruchom kreator przez adres konsoli lub aplikację; potwierdź model i lokalizację.
3. Ustaw własne dane administratora, nazwę instalacji i wymagane parametry internetu; zapisz wynik konfiguracji.

PRZYKŁAD: Dla Bluetooth podczas konfiguracji mobilnej pozostań blisko konsoli; instrukcja Ubiquiti podaje odległość do 3 metrów.

PUŁAPKA: Drugi serwer DHCP w tym samym segmencie może przydzielać klientom błędne ustawienia.

SPRAWDŹ / COFNIJ: Sprawdź adres laptopa, bramę, DNS i ponowne logowanie. W razie błędu odłącz nowy LAN od sieci produkcyjnej.

Źródła: [9]

Ostoja • Mapa 018

Otwórz panel lokalny

Dostęp lokalny wymaga połączenia z siecią, z której host jest osiągalny. Adres konsoli może różnić się od adresu bramy domyślnej.

GDZIE: Przeglądarka → lokalny IP hosta;
WiFiman → Discovery pomaga ustalić adres.

1. **Odczytaj IP hosta** z dokumentacji, ekranu konsoli lub Discovery.



IP hosta
192.168.10.5

2. Wpisz adres w przeglądarce; dla własnego Network Server uwzględnij faktyczny port, zwykle 8443.



3. Sprawdź tożsamość urządzenia i zaloguj się przygotowanym kontem. Otwórz właściwą aplikację Network.



- Zgodny adres
- Zgodne urządzenie
- Ważny certyfikat

↓

Otwórz aplikację Network

PRZYKŁAD:
CloudKey 192.168.10.5 oraz brama 192.168.10.1 to dwa różne punkty dostępu.



CloudKey
192.168.10.5



Brama
192.168.10.1

PUŁAPKA:
Nie potwierdzaj ostrzeżenia certyfikatu bez porównania adresu i urządzenia z dokumentacją.





SPRAWDŹ / COFNIJ:
W nowej sesji sprawdź nazwę lokalizacji i listę sprzętu. Brak dostępu diagnozuj od adresacji i trasy.



Źródła: [10]

Rozpoznaj urządzenia oczekujące

Ostoja • Mapa 019

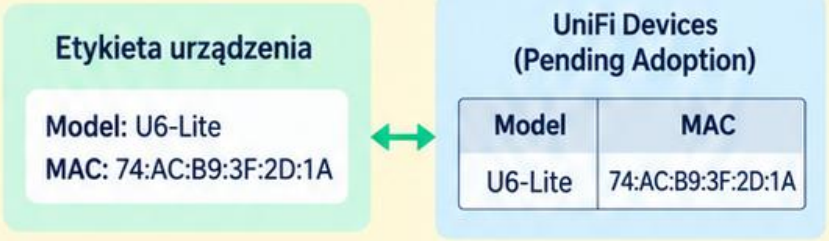
Przed adopcją potwierdź, że urządzenie należy do tego wdrożenia. Odkrycie po MAC jest pewniejsze niż nazwa domyślna podobnych egzemplarzy.

GDZIE: Network → UniFi Devices; stan Pending Adoption.

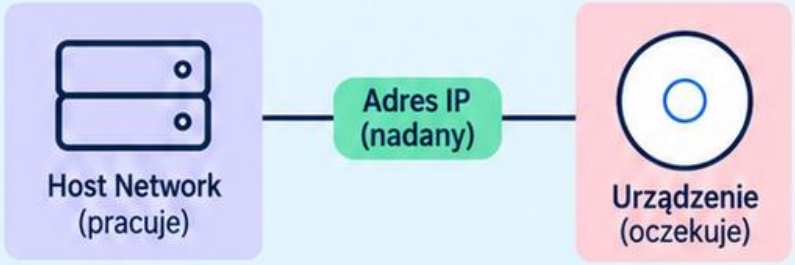
1. Połącz urządzenie z właściwym VLAN i zgodnym zasilaniem.



2. Porównaj MAC oraz model w panelu z etykietą i rejestrem.



3. Sprawdź, czy host Network pracuje, a urządzenie otrzymało poprawny adres; dopiero potem wybierz adopcję.



PRZYKŁAD: Na stole uruchom jeden nowy AP; dopisz końcówkę MAC do jego planowanej nazwy.

PUŁAPKA: Nie resetuj urządzenia widocznego jako zarządzane przez inną instancję bez zgody właściciela.

SPRAWDŹ / COFNIJ: Zapisz początkowy status, IP i MAC. Brak Pending Adoption kieruje do diagnostyki łączności, nie do masowych resetów.

Źródła: [24]

Ostoja

Adoptuj switch w tej samej sieci

Zacznij od jednego połączenia uplink i poprawnego zasilania. Po adopcji konfiguracja switcha może zostać dostosowana przez aplikację Network.

GDZIE:
Network → UniFi Devices → właściwy switch → Adopt.

1. Przygotuj kopię konfiguracji hosta i zanotuj port łączący switch z siecią.

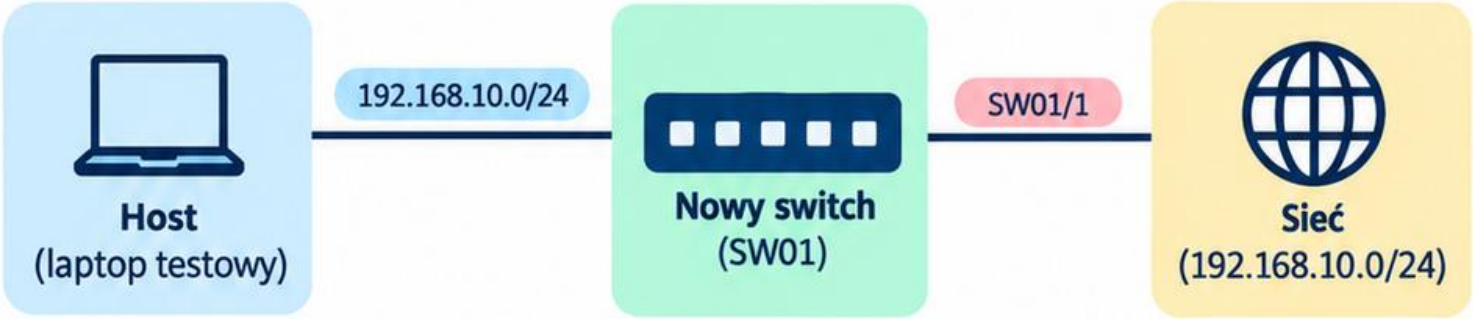


2. Podłącz switch do tej samej sieci/VLAN co host; potwierdź jego MAC i adres DHCP.



3. Wybierz Adopt i poczekaj na zakończenie provisioningu bez odłączania zasilania.





PRZYKŁAD: Host i nowy switch znajdują się w sieci 192.168.10.0/24; uplink oznacz jako SW01/1.

PUŁAPKA: Nie dodawaj drugiego przewodu między switchami bez planu STP lub agregacji.

SPRAWDŹ / COFNIJ: Sprawdź status Online i ruch przez jeden port testowy. Przy problemie zachowaj uplink i zdiagnozuj adresację.

Źródła: [24]

Adoptuj punkt dostępowy

Najpierw potwierdź przewodowy uplink i standard PoE konkretnego modelu. Adopcja AP i nadawanie docelowego SSID to dwa oddzielne etapy.

1 PoE i uplink danych

Podłącz AP do zgodnego portu lub injektora PoE z działającą transmisją danych.

2 Adopcja AP

Sprawdź MAC, IP i VLAN zarządzania; przy pierwszej adopcji użyj tej samej sieci co host.

3 Aktywacja SSID

Wybierz Adopt, zaczekaj na Online i dopiero potem przypisz planowane Wi-Fi.



GDZIE:
Network → UniFi Devices → AP → Adopt; aplikacja mobilna także umożliwia adopcję.

PRZYKŁAD:
AP testowy stoi obok switcha; krótki sprawny przewód pozwala wykluczyć instalację budynkową.

PUŁAPKA:
Samo świecenie diody nie dowodzi prawidłowego uplinku danych.

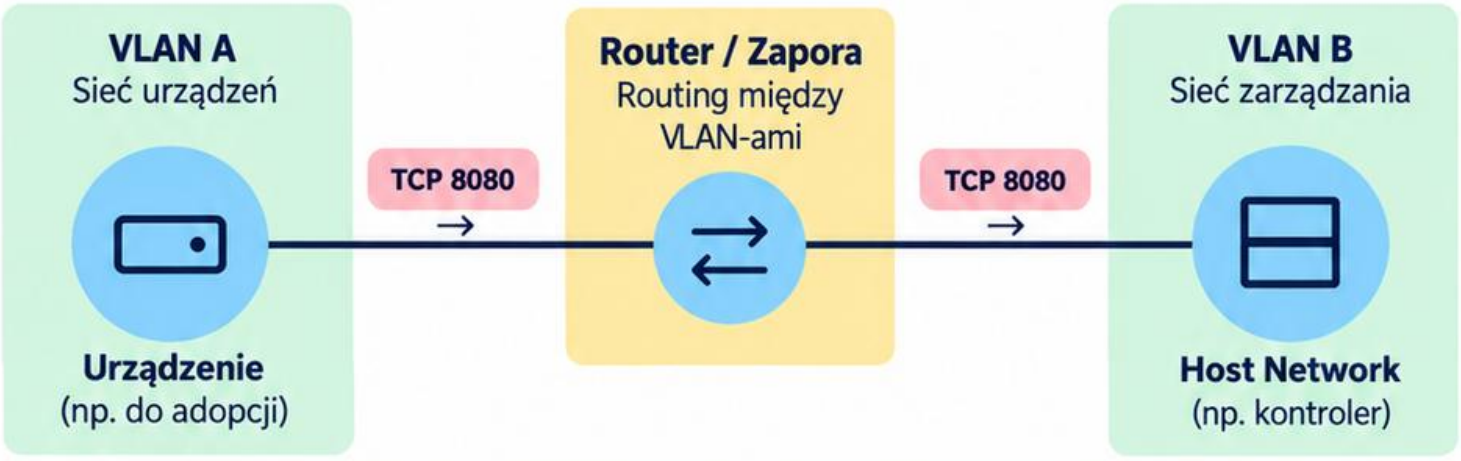
SPRAWDŹ / COFNIJ:
Sprawdź panel AP i klienta testowego. Jeśli AP znika, sprawdź *PoE* oraz DHCP przed zmianą ustawień radia.

Źródła: [24], [6]

Ostoja • Mapa 022

Sprawdź warunki adopcji między sieciami

Urządzenie musi dotrzeć do właściwego hosta Network. Wykrywanie lokalnym broadcastem nie zastępuje routingu między podsieciami.



1. Zapisz adresy urządzenia i hosta, bramy oraz trasę w obie strony.
2. Sprawdź dostęp TCP 8080 pomiędzy urządzeniem a hostem i rozwiązywanie używanej nazwy DNS.
3. Wybierz udokumentowaną metodę Layer 3; polecenie set-inform stosuj dopiero po potwierdzeniu adresu hosta i dostępu SSH.

GDZIE: Dokumentacja Remote Adoption (Layer 3); konfiguracja routera i zapory między VLAN-ami.

PRZYKŁAD: Inform wskazuje host Network, na przykład http://192.168.10.5:8080/inform; nie dowolny router.

PUŁAPKA: Nie otwieraj całego interfejsu administracyjnego do internetu w celu adopcji.

SPRAWDŹ / COFNIJ: Obserwuj pojawienie się urządzenia i provisioning. Cofnij wyłącznie tymczasowe reguły, które nie są już potrzebne.

Źródła: [27], [24]

Znajdź poprzedni kontroler urządzenia

Ostoja • Mapa 023

Stan zarządzania przez inną instancję oznacza potrzebę ustalenia właściciela. Reset usuwa konfigurację i może przerwać działające usługi.



1. Zapisz MAC, IP i dokładny komunikat widoczny w panelu.
2. Sprawdź, czy poprzednia konsola nadal działa i czy właściciel ma do niej dostęp.
3. Wybierz migrację z kopią lub procedurę przekazania; reset zaplanuj dopiero jako świadomy ostatni krok.

GDZIE:
Network → UniFi Devices; dokumentacja właściciela i rejestr poprzedniego hosta.

PRZYKŁAD:
Przejęte biuro może mieć stary CloudKey w szafie, mimo że nowy administrator loguje się do innej konsoli.

PUŁAPKA:
Nie traktuj komunikatu Managed by Another Console jako zgody na wymazanie urządzenia.

SPRAWDŹ / COFNIJ:
Po migracji potwierdź zarządzanie z jednej docelowej instancji. Zachowaj wcześniejszą kopię i plan odtworzenia.

Źródła: [24], [8]

Nadaj nazwy urządzeniom i portom

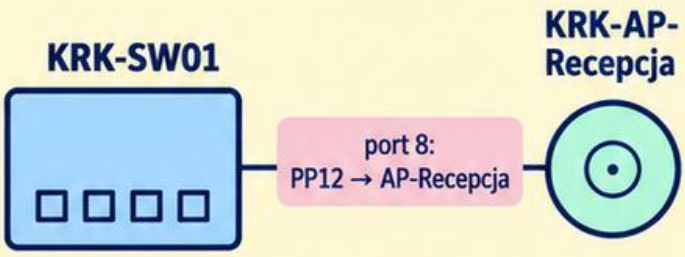
Nazwy powinny wskazywać miejsce i rolę, a opis portu oba końce połączenia. Ułatwia to diagnozę bez zgadywania na podstawie adresu IP.

1 Przyjmij krótki schemat: lokalizacja, typ i numer urządzenia.

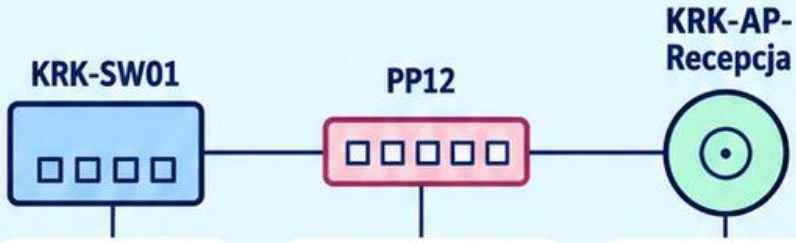
LOKALIZACJA-TYP-NR

- **Lokalizacja** np. KRK
- **Typ urządzenia** np. SW, AP
- **Numer** np. 01

2 Zmień nazwę po porównaniu MAC z inwentarzem. Opisz uplink oraz porty krytycznych odbiorników.



3 Dodaj te same oznaczenia do przewodów, patchpanelu i mapy fizycznej.



4 Przykład

KRK-SW01; KRK-AP-Recepcja; port 8: PP12 → AP-Recepcja.

Pułapka

Nie wpisuj haseł, danych osobowych ani kluczy VPN do nazw lub opisów.

Sprawdź / Cofnij

Wybierz losowy port i odtwórz jego przebieg z dokumentacji. Przy niezgodności popraw opis przed kolejną zmianą.

GDZIE: Network → UniFi Devices → urządzenie; porty w widoku switcha.

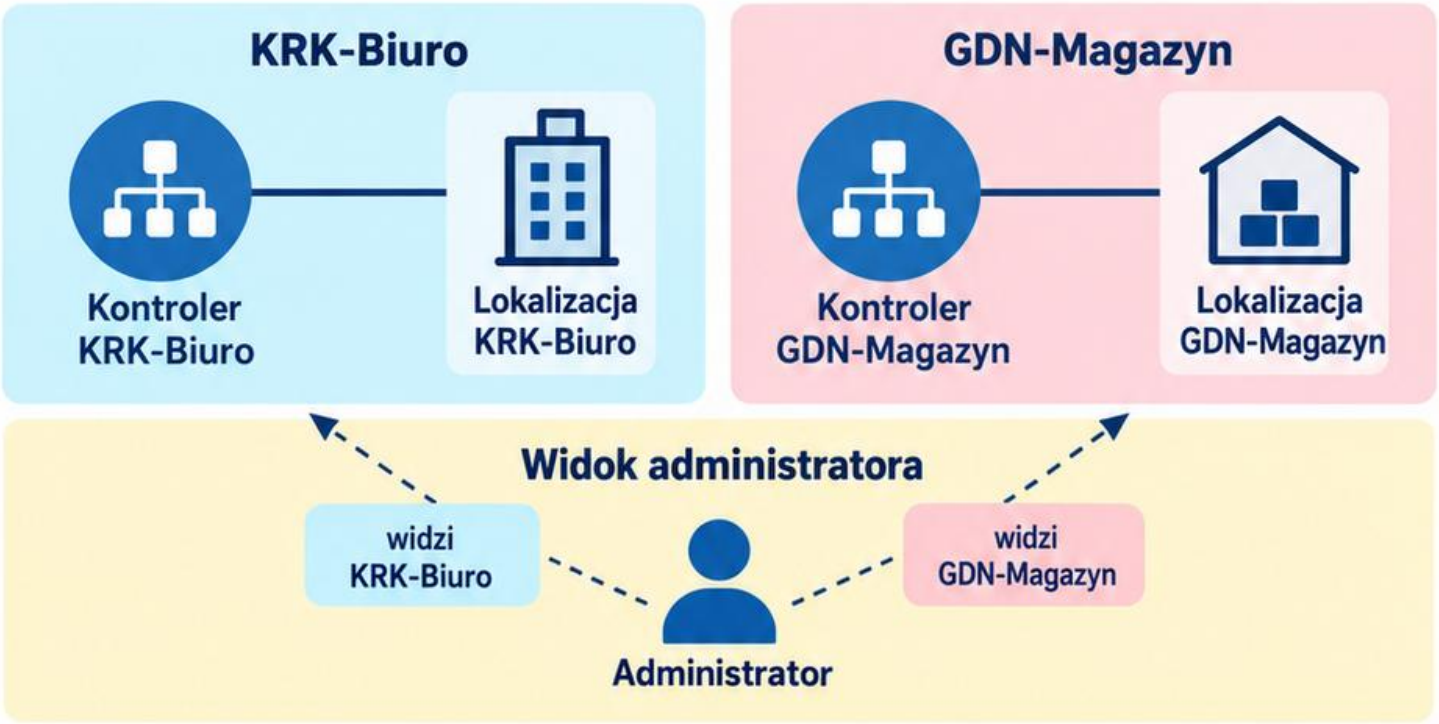
Źródła: [4], [24]

Uporządkuj lokalizacje

Ostoja • Mapa 025

Jedna lokalizacja powinna odpowiadać czytelnemu obszarowi zarządzania. Wspólna nazwa w Site Manager nie scala podsieci ani konfiguracji urządzeń.

GDZIE: Site Manager → lista lokalizacji; dla Fabric zakres administracji ustala się centralnie.



1. **Zapisz konsolę**, adres instalacji, właściciela i osobę kontaktową dla każdej lokalizacji.
2. Nadaj jednoznaczne nazwy z miastem lub kodem oddziału.
3. Przypisz administratorów do właściwego zakresu; porównaj wybraną lokalizację przed każdą zmianą.

PRZYKŁAD: KRK-Biuro i GDN-Magazyn pozostają oddzielnymi wdrożeniami, nawet jeśli ten sam administrator widzi obie pozycje.

PUŁAPKA: Nie przenoś urządzeń między instancjami samą zmianą nazwy lokalizacji.

SPRAWDŹ / COFNIJ: Zaloguj się jako administrator danego oddziału i potwierdź widoczny zakres. Cofnij błędne uprawnienia, zachowując dostęp właściciela.

Źródła: [11], [14]

Ostoja

Przydziel uprawnienia administratorom

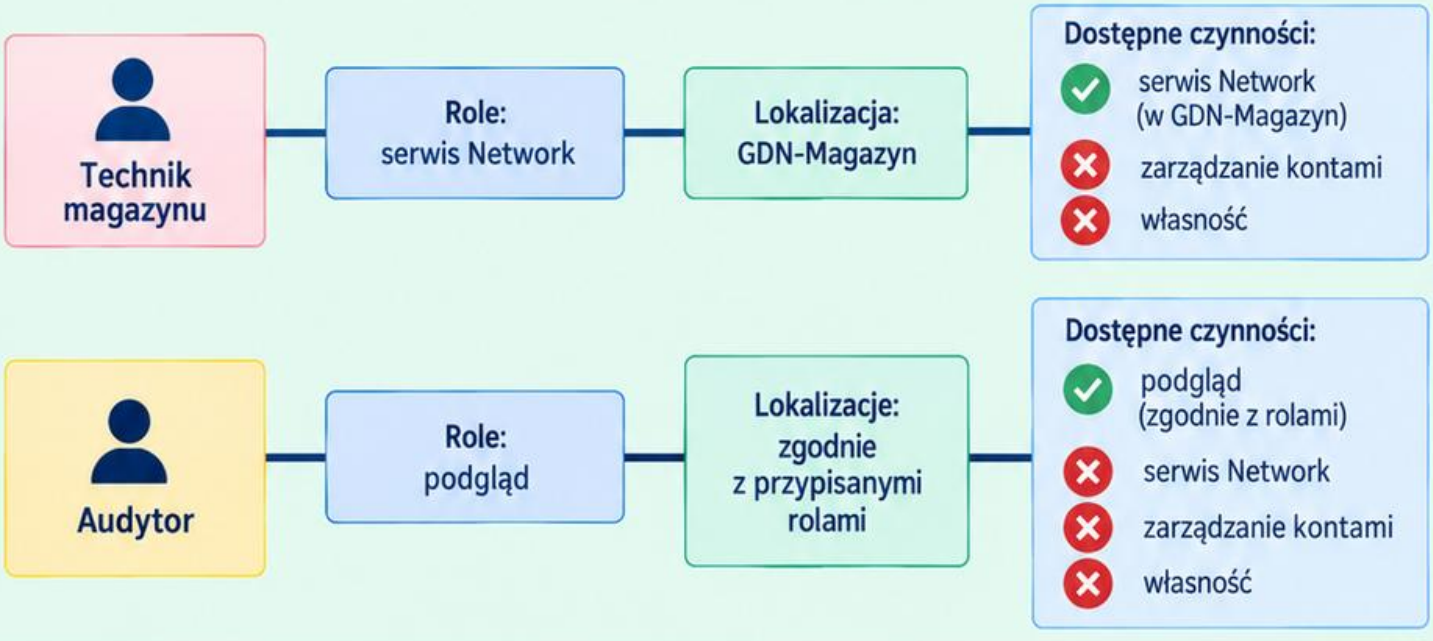
Ostoja • Mapa 026

Dobieraj uprawnienia do obowiązków i lokalizacji.
Osoba obserwująca stan sieci nie musi móc zmieniać konfiguracji.

GDZIE: Site Manager → People → New Admin;
Fabric: People → Roles.

1. **Wypisz zadania:** podgląd, serwis Network, zarządzanie kontami i własność.
2. **Wybierz lokalizacje** oraz uprawnienia aplikacji; w Fabric sprawdź sumę przypisanych ról.
3. **Przetestuj konto** w osobnej sesji: potrzebna funkcja działa, a czynność poza zakresem pozostaje niedostępna.

PRZYKŁAD: Technik magazynu otrzymuje dostęp tylko do GDN-Magazyn; audytor otrzymuje podgląd zgodny z dostępnymi rolami.



PUŁAPKA:
W Fabric wiele ról może rozszerzać efektywne uprawnienia.

SPRAWDŹ / COFNIJ:
Zapisz wynik testu i osobę zatwierdzającą. Przy nadmiarowym dostępie popraw przypisanie, nie usuwając ostatniego administratora.

Źródła: [14]

Ostoja • Mapa 027

Sprawdź wersje firmware

Spisz faktyczne wersje każdego modelu przed wyborem aktualizacji. Wersja dostępna do instalacji nie musi oznaczać wersji już działającej.

GDZIE: Network → UniFi Devices → urządzenie; aktualizacje w aplikacji i Site Manager → Update Manager.

1 **Zapisz model, obecną wersję firmware oraz stan urządzenia.**

- Urządzenie (model)
- Obecna wersja firmware
- Stan urządzenia

2 **Porównaj propozycję aktualizacji z oficjalnymi release notes dla tego modelu.**

- Propozycja aktualizacji
- Oficjalne release notes (dla tego modelu)

3 **Sprawdź wymagania minimalne Network, znane ograniczenia i wpływ restartu na klientów lub PoE.**

- Wymagania minimalne Network
- Znane ograniczenia
- Wpływ restartu na klientów
- Wpływ restartu na PoE

PRZYKŁAD: AP01: obecna _____; docelowa _____; Network wymagany _____; spodziewana przerwa _____.

PUŁAPKA: Nie stosuj pliku firmware przeznaczonego dla innego modelu ani instrukcji z innej generacji.

SPRAWDŹ / COFNIJ: Zestaw listę urządzeń z inwentarzem. Sam odczyt nie wymaga restartu; nie naciskaj Update podczas dokumentowania.

Źródła: [23]

Zaplanuj aktualizację etapami

Ostoja • Mapa 028

Najpierw wybierz małą grupę pilotażową oraz kryteria sukcesu. Aktualizacja switcha zasilającego AP może przerwać wiele usług jednocześnie.

GDZIE: Site Manager → Update Manager; lokalnie Settings → Control Plane → Updates.

1 Przygotowanie i kopia

Pobierz kopię i przeczytaj wymagania wersji; sprawdź drogę dostępu lokalnego.

2 Plan i kolejność

Ustal kolejność zależności według release notes i okno serwisowe.

3 Pilot i testy

Zaktualizuj jeden reprezentatywny element, sprawdź adopcję, DHCP, DNS i usługę użytkownika; dopiero potem rozszerz zakres.

4 Pozostałe elementy

Po pozytywnych testach zaktualizuj pozostałe urządzenia zgodnie z planem.

STOP
Przy niepowodzeniu zatrzymaj kolejne etapy.

PRZYKŁAD:
Pilot: AP w sali testowej. Akceptacja: ponowne Online i poprawna praca dwóch różnych klientów.

PUŁAPKA:
Nie traktuj obniżenia firmware jako zawsze dostępnej lub bezpiecznej metody cofnięcia.

SPRAWDŹ / COFNIJ:
Przy niepowodzeniu zatrzymaj kolejne etapy. Zachowaj logi i użyj procedury odzyskiwania zgodnej z modelem.

Źródła: [23], [8]

Zrób kopię przed zmianą

Ostoja • Mapa 029

Rozróżniaj kopię całej konsoli i kopię aplikacji Network. Plik musi pasować do planowanej ścieżki odtworzenia, a nie tylko istnieć na dysku.

GDZIE: W aktualnej konsoli Settings → Control Plane → Backups.
Dla własnego Network Server sprawdź wariant Network-only zgodny z hostem.



1. Zapisz model hosta, wersję Network i zakres danych kopii.
2. Utwórz aktualną kopię oraz pobierz ją do zabezpieczonego miejsca poza urządzeniem.
3. Sprawdź nazwę, rozmiar, datę i możliwość odczytu pliku; ustal dostęp do konta potrzebnego przy odtworzeniu.

PRZYKŁAD: KRK-Network-2026-10-21-przed-VLAN; rejestr zawiera lokalizację pliku i odpowiedzialną osobę.

PUŁAPKA: Nie pozostawiaj jedynej kopii na konsoli, którą zamierzasz wymienić lub resetować.

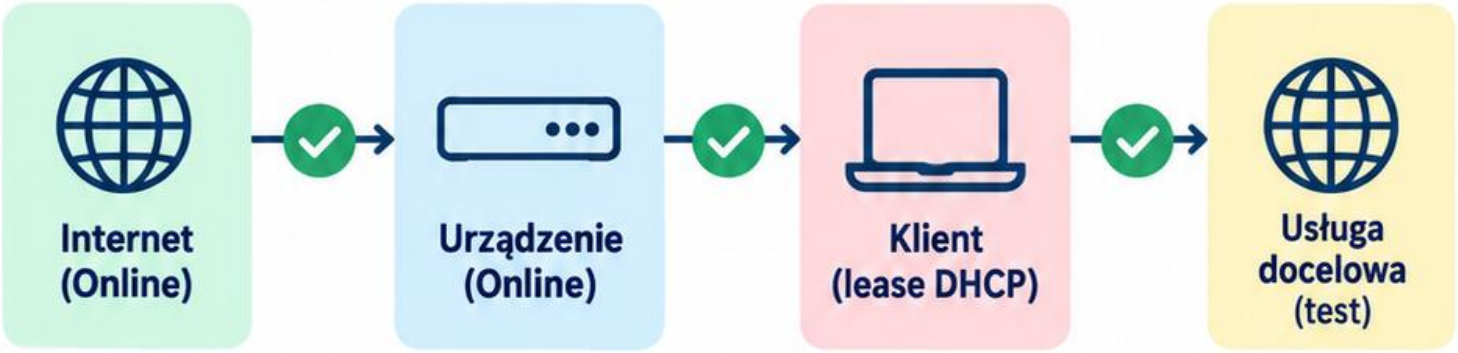
SPRAWDŹ / COFNIJ: Test odtworzenia wykonaj w odseparowanym środowisku. Nie uruchamiaj drugiej aktywnej instancji zarządzającej tymi samymi urządzeniami.

Źródła: [8]

Ostoja • Mapa 030

Potwierdź zakończenie adopcji

Stan Online jest konieczny, ale nie kończy odbioru. Urządzenie musi obsługiwać ruch zgodnie z przypisaną rolą i pozostawać zarządzalne.



GDZIE:
Network → UniFi Devices → urządzenie; Client Devices dla klienta testowego.

1. Potwierdź MAC, nazwę, IP, firmware i właściwą lokalizację.

2. Sprawdź uplink oraz docelowy VLAN zarządzania bez zmiany działającej drogi awaryjnej.

3. Podłącz klienta: sprawdź DHCP, DNS i usługę docelową; obserwuj, czy urządzenie nie wraca do adopcji.

PRZYKŁAD:
AP: klient łączy się z właściwym **SSID** i otrzymuje adres z planowanego VLAN.

PUŁAPKA:
Zielona ikona nie dowodzi poprawnej segmentacji ani działania DNS.

SPRAWDŹ / COFNIJ:
Zapisz wynik i czas obserwacji. Jeśli test nie przechodzi, wróć do poprzedniego przypisania portu lub SSID.

Źródła: [24], [12], [18]

Ostoja • Moduł 3

Internet i gateway



Stabilny WAN zaczyna się od danych operatora.

Metoda przydziału, VLAN, uwierzytelnianie, publiczny adres i iPv6 muszą odpowiadać konkretnej usłudze.

Przejdziesz od rozpoznania łącza do DHCP, adresu statycznego i PPPoE.

Następnie sprawdzisz NAT, DNS, drugi WAN, failover, IPv6 oraz routing.

Każdy zapis wykonuj z przygotowanym dostępem lokalnym.

Zachowaj parametry poprzedniego routera i nie zmieniaj jednocześnie kilku niewyjaśnionych ustawień.

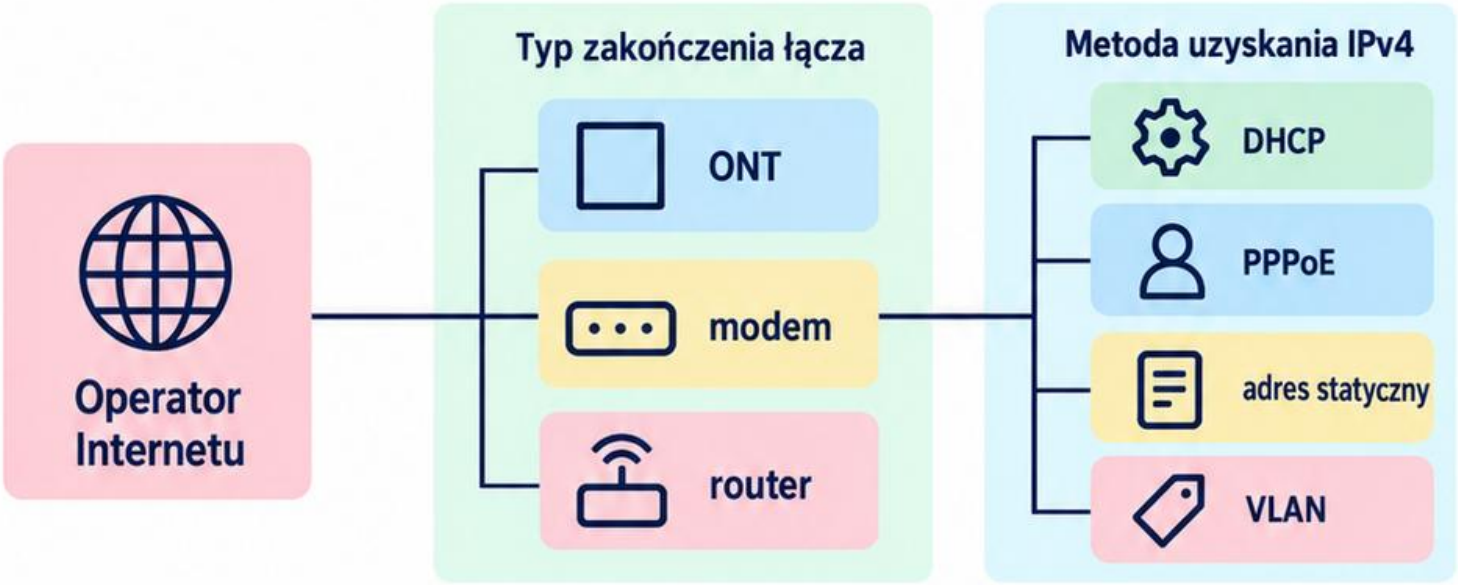
Wynik:

powtarzalny test internetu, udokumentowane ograniczenia dostępu przychodzącego i sprawdzony powrót po awarii łącza.

Źródła: [16], [17], [13], [18]

Ustał sposób przekazania łącza

Przed wymianą routera zbierz parametry usługi. Gniazdo Ethernet nie przesądza, czy operator używa DHCP, PPPoE, adresu statycznego lub tagowania VLAN.



1. Zapisz typ zakończenia łącza: ONT, modem albo router; ustal jego tryb pracy.
2. Poproś operatora o metodę IPv4, VLAN, dane PPPoE, MTU i warunki IPv6, jeżeli są wymagane.
3. Potwierdź wiązanie z MAC, rodzaj adresu publicznego i sposób przywrócenia poprzedniego routera.

GDZIE: Dokumentacja operatora; Settings → Internet → właściwe połączenie WAN.

PRZYKŁAD: Karta WAN: operator _____; port _____; metoda _____; VLAN _____; dane dostępowe w sejfie _____.

PUŁAPKA: Nie kopiuj numeru VLAN z instrukcji innego klienta tego samego operatora.

SPRAWDŹ / COFNIJ: Porównaj dane z działającym urządzeniem. Zachowaj jego konfigurację i przewody do czasu odbioru nowej bramy.

Źródła: [9], [16], [13]

Uruchom WAN przez DHCP

Ostoja • Mapa 032

Użyj DHCP, gdy operator przydziela ustawienia automatycznie.
Osobno potwierdź ewentualny VLAN i warunek rejestracji adresu MAC.

GDZIE: Settings → Internet → wybrany WAN → konfiguracja IPv4.

1. Zapisz poprzednią konfigurację i sprawdź, który fizyczny port pełni rolę WAN.



2. Wybierz **DHCP** dla IPv4, zachowując tylko parametry dodatkowe potwierdzone przez operatora.



3. Zastosuj ustawienia i odczytaj przydzielone IP, bramę oraz DNS. Porównaj podsieć WAN z LAN.



Wymiana komunikatów DHCP w sieci WAN



Otrzymane ustawienia z DHCP

Adres IP (WAN)	Brama domyślna (WAN)	Serwery DNS
IP 192.168.1.20	192.168.1.1	192.168.1.1 8.8.8.8

PRZYKŁAD: WAN otrzymuje 192.168.1.20, a LAN używa 192.168.10.0/24: zakresy są różne, ale WAN może być za routerem.

PUŁAPKA: Brak adresu nie jest powodem do losowego wpisywania statycznego IP.

SPRAWDŹ / COFNIJ: Sprawdź DNS i stronę HTTPS z klienta. Przy braku dzierżawy skontaktuj się z operatorem lub przywróć wcześniejsze połączenie.

Źródła: [9], [16]

Ostoja • Mapa 033

Wprowadź statyczne IPv4 na WAN

Adres statyczny wymaga kompletu danych operatora. Adres publiczny, maska i brama są osobnymi polami; nie wyprowadzaj ich z domysłów.

GDZIE: Settings → Internet → wybrany WAN → konfiguracja IPv4 → Static IP.

Dane od operatora

- Adres publiczny IPv4 (przydzielony IP)
- Prefiks lub maska
- Brama IPv4
- DNS

Konfiguracja WAN

WAN

- IP (Static IP)
- Prefiks lub maska
- Brama IPv4
- DNS

1. Przepisz przydzielony IP, prefiks lub maskę, bramę i DNS do karty zmiany.
2. Ustaw Static IP na właściwym porcie WAN; dodaj VLAN tylko wtedy, gdy operator go wymaga.
3. Zastosuj konfigurację lokalnie i sprawdź status łącza oraz poprawność wpisanych parametrów.

PRZYKŁAD: Formularz: IP ____ / prefiks ____ / brama ____ / DNS ____.
Dane przykładowe nie mogą zastąpić danych operatora.

PUŁAPKA: Adres sieci albo broadcast nie jest zwykłym adresem hosta; nietypowe przekazania wymagają potwierdzenia u operatora.

SPRAWDŹ / COFNIJ: Przetestuj ruch IP, DNS i HTTPS. Jeżeli brak łączności, przywróć zapisane parametry zamiast zmieniać kilka pól naraz.

Źródła: [16], [28], [18]

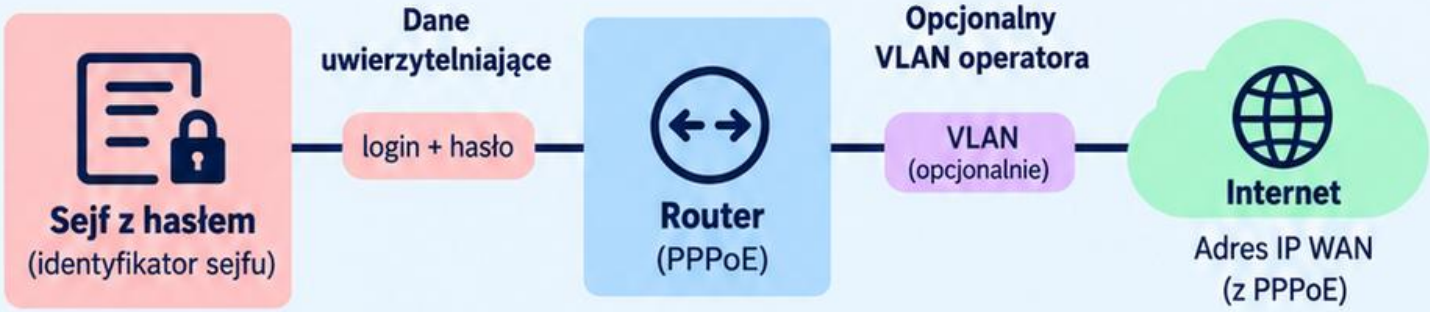
Ostoja • Mapa 034

Skonfiguruj PPPoE

PPPoE wymaga danych uwierzytelniania usługi internetowej. Hasło do panelu klienta operatora może być inne niż hasło sesji PPPoE.

GDZIE: Settings → Internet → właściwy WAN → konfiguracja IPv4 → PPPoE.

1. **Zabezpiecz** dotychczasowe ustawienia i ustal login, hasło oraz dodatkowe wymagania operatora.
2. **Wybierz PPPoE**, wpisz dane bez spacji i sprawdź ewentualny **VLAN**.
3. **Zastosuj** ustawienia, obserwuj zestawienie sesji i otrzymany adres; nie zmieniaj od razu MTU.



PRZYKŁAD: Karta zawiera identyfikator sejfu z hasłem, nie jawne hasło. Dopisz czas ostatniej udanej sesji.

PUŁAPKA: Nie uruchamiaj równoległej sesji na starym routerze, jeśli operator dopuszcza tylko jedną.

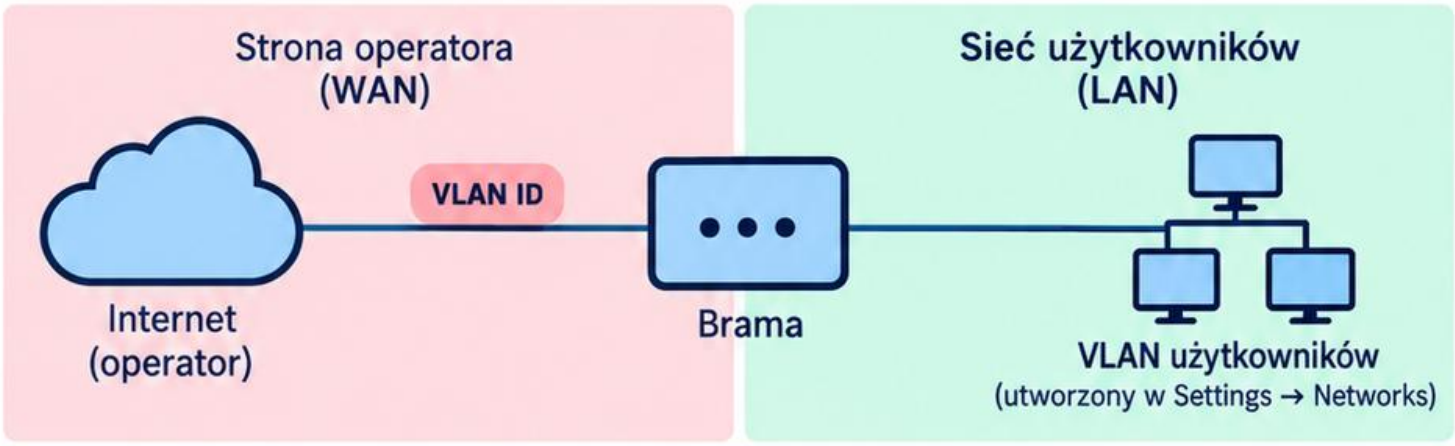
SPRAWDŹ / COFNIJ: Z klienta otwórz kilka stron HTTPS. Przy błędzie uwierzytelniania potwierdź dane u operatora; zachowaj lokalny dostęp.

Źródła: [9], [16], [28]

Ostoja • Mapa 035

Ustaw VLAN wymagany przez operatora

VLAN na WAN opisuje sposób przekazania internetu. Nie jest tym samym co VLAN użytkowników tworzony w Settings → Networks.



GDZIE: Settings → Internet → wybrany WAN; opcje dodatkowe połączenia.

1. **Potwierdź VLAN ID** i ewentualny priorytet bezpośrednio w dokumentacji swojej usługi.
2. **Sprawdź,** czy tag dodaje brama, ONT czy urządzenie pośrednie; wyznacz jeden właściwy punkt tagowania.
3. **Wprowadź** uzgodniony VLAN dla WAN oraz zachowaj prawidłową metodę DHCP, Static IP albo PPPoE.

PRZYKŁAD: Jeżeli ONT przekazuje wymagany VLAN jako ruch nietagowany, dodatkowe tagowanie na bramie może zerwać usługę.

PUŁAPKA: Nie twórz sieci LAN o numerze VLAN operatora w celu naprawy WAN.

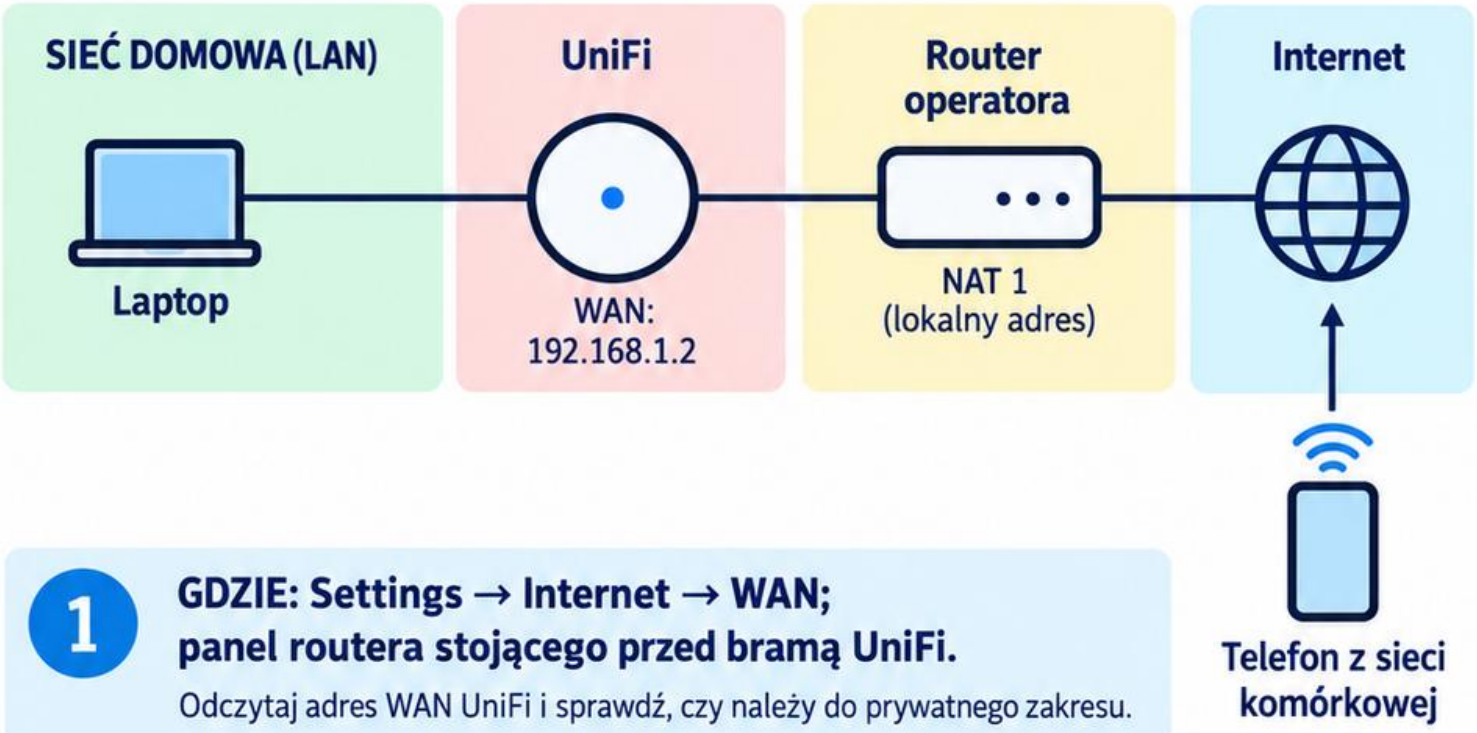
SPRAWDŹ / COFNIJ: Sprawdź adres lub sesję WAN i ruch klienta. Przy utracie usługi cofnij wyłącznie nowy tag według zapisanej konfiguracji.

Źródła: [16], [1]

Sprawdź podwójny NAT

Ostoja • Mapa 036

Podwójny NAT występuje, gdy ruch przechodzi przez dwie translacje. Dostęp do stron może działać mimo utrudnień z usługami przychodzącymi.



1. **GDZIE: Settings → Internet → WAN; panel routera stojącego przed bramą UniFi.**
   Odczytaj adres WAN UniFi i sprawdź, czy należy do prywatnego zakresu.

2. **Ustal urządzenie przed UniFi oraz jego adres WAN; porównaj z adresem widocznym w zewnętrznej usłudze.**

3. **Z operatorem oceń tryb bridge lub przekazanie publicznego adresu; zapisz wpływ na telefon i telewizję.**

PRZYKŁAD:
Laptop → UniFi z WAN 192.168.1.2 → router operatora → internet: lokalny router może wykonywać pierwszy NAT.

PUŁAPKA:
DMZ na routerze operatora zwykle nie usuwa samej translacji.

SPRAWDŹ / COFNIJ:
Po zmianie sprawdź internet i potrzebne usługi przychodzące z sieci komórkowej. Przy awarii wróć do poprzedniego trybu.

Źródła: [17]

Rozpoznaj CGNAT

Ostoja • Mapa 037

CGNAT oznacza translację po stronie operatora. Samo przekierowanie portu na UniFi nie zapewni wtedy publicznego dostępu do usługi.



1. **Zapisz adres WAN i adres widoczny poza siecią.**

2. Sprawdź zakres 100.64.0.0–100.127.255.255 oraz prywatne zakresy; potraktuj różnicę adresów jako wskazówkę, nie pełny dowód.

3. **Poproś operatora o potwierdzenie CGNAT i możliwości publicznego IPv4 lub odpowiedniego rozwiązania IPv6.**

GDZIE:
Settings → **Internet** → **WAN**; potwierdzenie rodzaju usługi u operatora.

PRZYKŁAD:
WAN 100.72.10.8 należy do 100.**64.0.0/10**. Nie jest publicznym adresem IPv4 Twojej bramy.

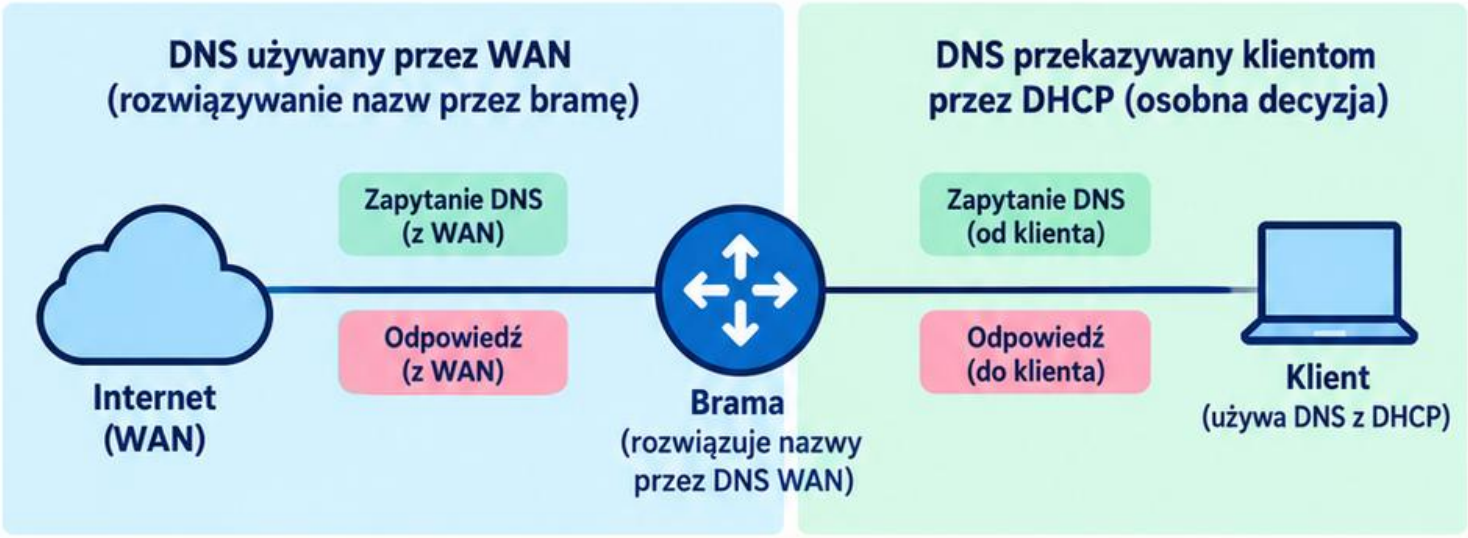
PUŁAPKA:
DDNS nadaje nazwę adresowi, lecz nie usuwa NAT operatora.

SPRAWDŹ / COFNIJ:
Zapisz odpowiedź operatora i wybraną metodę dostępu.
Nie publikuj kluczy VPN ani panelu zarządzania podczas testów.

Źródła: [17], [13]

Ustaw DNS używany przez WAN

Resolver WAN obsługuje zapytania bramy. DNS przekazywany klientom przez DHCP jest osobną decyzją i może wskazywać serwer firmowy.



GDZIE:

Settings → Internet → właściwe połączenie → DNS Server.

1. Zapisz bieżące serwery oraz powód planowanej zmiany.
2. Wprowadź zatwierdzone resolvery osiągalne z WAN; uwzględnij politykę organizacji i domeny potrzebne do działania UniFi.
3. Zastosuj ustawienia i porównaj odpowiedzi na zapytania o kilka nazw publicznych.

PRZYKŁAD: Test: ui.com oraz domena usługi używanej w firmie. Wynik ma wskazywać adres, a nie timeout.

PUŁAPKA: Nie dodawaj publicznego DNS jako przypadkowego zamiennika serwera Active Directory dla klientów domenowych.

SPRAWDŹ / COFNIJ: Sprawdź aktualizacje i logowanie zdalne. Gdy rozwiązywanie nazw przestaje działać, przywróć poprzedni resolver.

Źródła: [18]

Ostoja

Ostoja • Mapa 039

Zweryfikuj łączność bramy

Oddziel warstwę fizyczną, przydział adresu, routing i DNS. Ikona internetu nie wyjaśnia sama, który z tych etapów zawiódł.

GDZIE: Settings → Internet → WAN; testy z przewodowego klienta w kontrolowanej sieci.

1. LINK



Połączenie aktywne i poprawny port WAN.

2. ADRES



IP, brama i metoda połączenia.

3. ROUTING I DNS



Ruch do celu po IP oraz zapytanie DNS o nazwę.

4. HTTPS



Rzeczywista usługa działa z klienta.

1. **Sprawdź link oraz poprawny port WAN, następnie IP, bramę i metodę połączenia.**
2. **Porównaj ruch do zatwierdzonego celu po adresie IP z zapytaniem DNS o nazwę.**
3. **Uruchom stronę HTTPS z klienta i potwierdź, że problem nie dotyczy tylko jednej aplikacji.**

PRZYKŁAD: Adres IP osiągalny, lecz zapytania DNS kończą się timeoutem: badaj resolver i reguły, zanim wymienisz kabel.

PUŁAPKA: Brak odpowiedzi ping może wynikać z filtrowania ICMP; użyj także testu rzeczywistej usługi.

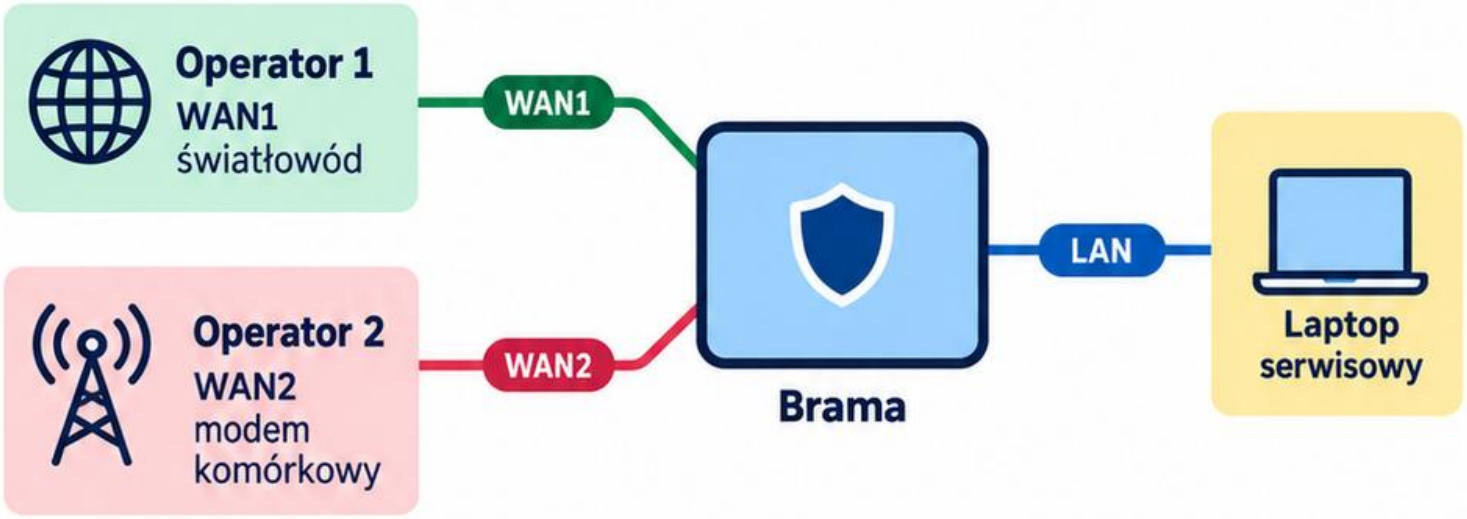
SPRAWDŹ / COFNIJ: Zapisz czas, klienta i wyniki każdego etapu. Cofaj ostatnią zmianę, jeśli wcześniej te same testy przechodziły.

Źródła: [16], [18]

Ostoja

Dodaj zgodne drugie łącze WAN

Sprawdź możliwości sprzętu przed przepięciem przewodów. Port używany przez laptop serwisowy lub uplink LAN nie może przypadkowo stać się WAN.



1. Potwierdź model, dostępny port WAN i parametry drugiego operatora.
2. Podłącz drugie łącze oraz skonfiguruj jego metodę IP; zachowaj działający port LAN.
3. Jeśli zmieniasz role portów, najpierw zapewnij aktywne połączenie na docelowym porcie i zapisz poprzednie przypisania.

GDZIE: Settings → Internet; role fizycznych portów zależą od modelu bramy.

PRZYKŁAD: WAN1: światłowód; WAN2: modem komórkowy. Sprawdź limit danych i NAT drugiego operatora.

PUŁAPKA: Nie zakładaj identycznej liczby portów i możliwości Multi-WAN we wszystkich bramach.

SPRAWDŹ / COFNIJ: Zweryfikuj osobno adres i dostępność WAN2. Przy niepowodzeniu przywróć rolę portu i poprzednie okablowanie.

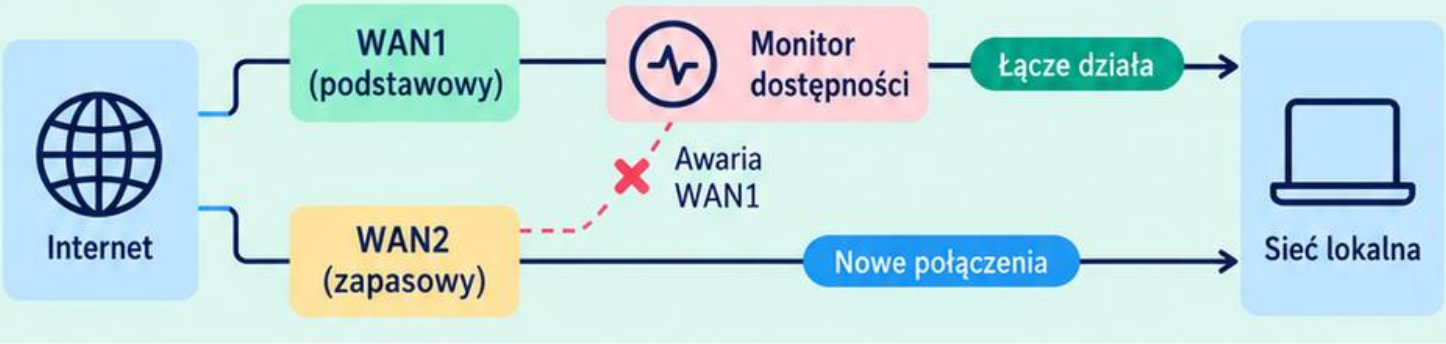
Źródła: [16]

Ostoja • Mapa 041

Ustal tryb failover

Failover kieruje ruch przez łącze zapasowe po wykryciu awarii podstawowego. Wybierz kolejność łączy zgodnie z kosztem i wymaganiami usług.

GDZIE: Settings → Internet → konfiguracja połączeń i monitorowania WAN.



1. Oznacz WAN podstawowy i zapasowy; wybierz **Failover** zamiast równoważenia, jeśli taki jest cel projektu.

2. Sprawdź sposób badania dostępności: domyślny **Auto** lub świadomie dobrane cele SLA w obsługiwanej wersji.

3. Zapisz warunek przełączenia oraz ograniczenia aplikacji wymagających stałego adresu źródłowego.

PRZYKŁAD: Po awarii światłowodu nowe połączenia korzystają z modemu LTE; aktywna rozmowa może wymagać ponownego zestawienia.

PUŁAPKA: Sprawny link Ethernet nie dowodzi, że operator zapewnia dostęp do internetu.

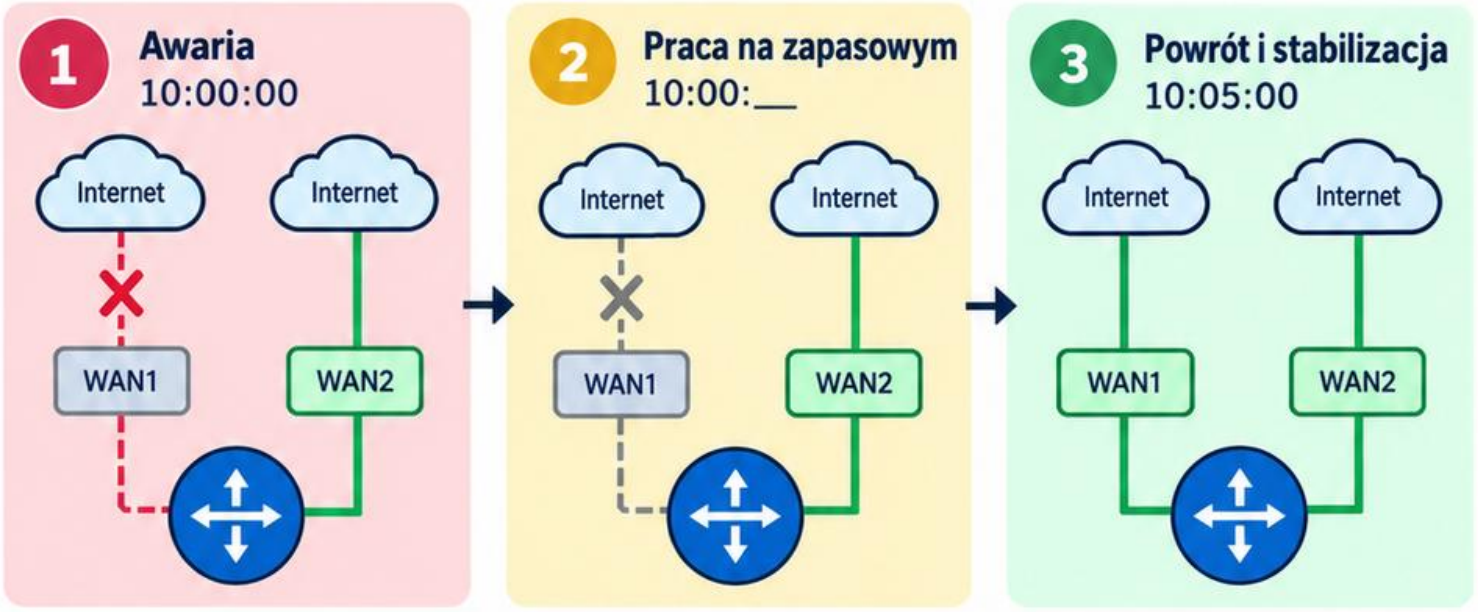
SPRAWDŹ / COFNIJ: W oknie serwisowym odłącz WAN1 i uruchom nową sesję HTTPS. Cofnij test, ponownie podłączając właściwy przewód.

Źródła: [16]

Przetestuj powrót WAN

Zbadaj awarię, przełączenie oraz powrót jako trzy osobne momenty. Nie obiecuj ciągłości każdej sesji przy zmianie publicznego adresu.

GDZIE: Settings → Internet; karta testu awarii i powrotu.



1. Zapisz stan początkowy, aktywny WAN i działanie krytycznych usług.
2. Przerwij podstawowe łącze w uzgodniony sposób; zmierz czas wykrycia i sprawdź nowe połączenie.
3. Przywróć WAN1, poczekaj na ustabilizowanie monitoringu i ponownie wykonaj te same testy.

PRZYKŁAD:
Protokół: awaria 10:00:00; nowa sesja działa 10:00:__;
WAN1 przywrócony 10:05:00; wynik ____.

PUŁAPKA:
Nie testuj przez przypadkowe odłączenie uplinku LAN albo zasilania całej szafy.

SPRAWDŹ / COFNIJ:
Sprawdź DNS, VPN i usługę firmową po powrocie. Jeżeli występują kolejne przełączenia, zbadaj cele i progi monitoringu.

Źródła: [16]

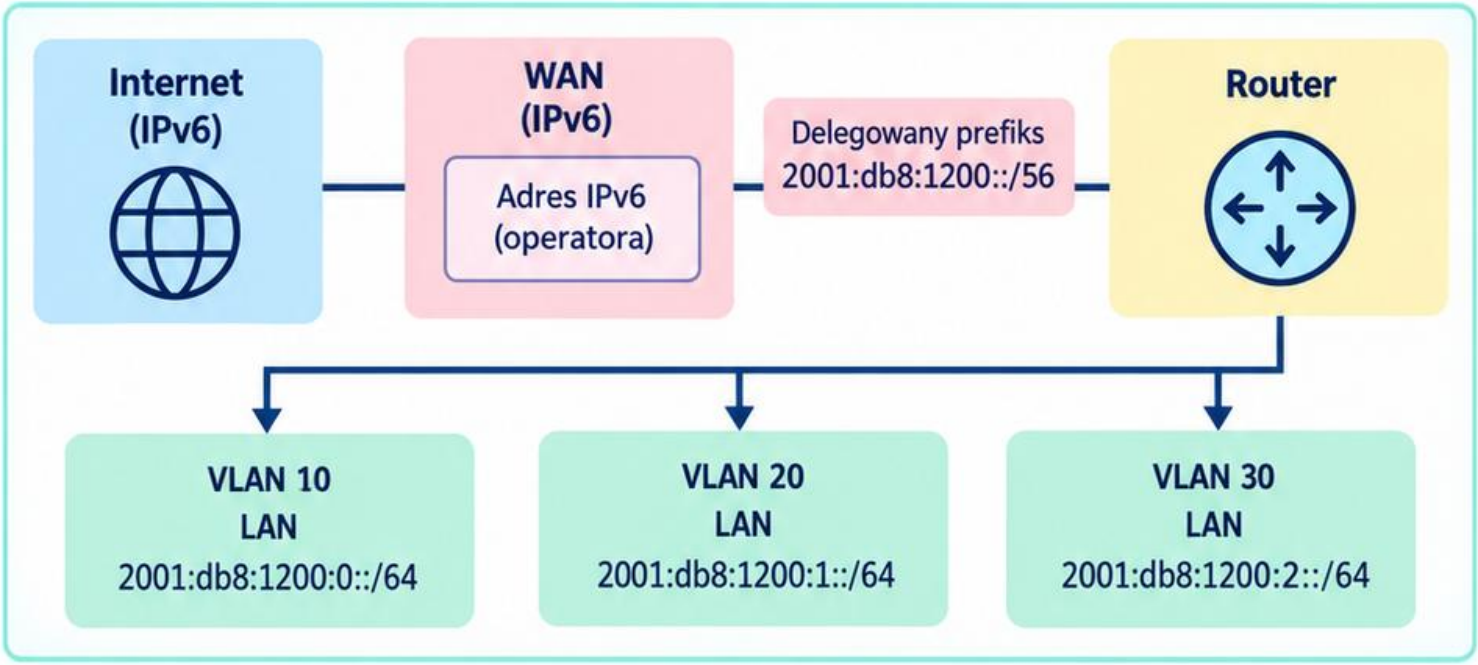
Sprawdź IPv6 operatora

Ostoja · Mapa 043

Zbierz metodę przydziału oraz delegowany prefiks przed włączeniem IPv6 na VLAN-ach. Adres na interfejsie WAN i prefiks dla LAN to różne dane.

GDZIE: Settings → Internet → WAN → IPv6 Configuration.

1. Zapytaj operatora o SLAAC, DHCPv6 lub adresację statyczną oraz wielkość delegacji.
2. Wybierz udokumentowaną metodę WAN i sprawdź przydzielony adres oraz prefiks.
3. **Potwierdź, ile oddzielnych /64** można wydzielić dla planowanych sieci; zapisz zachowanie po odnowieniu łącza.



PRZYKŁAD: Delegacja /56 pozwala wydzielić 256 podsieci /64.
Przykładowy prefiks dokumentacyjny: 2001:db8:1200::/56.

PUŁAPKA: Sam adres link-local fe80:: nie potwierdza dostępu IPv6 do internetu.

SPRAWDŹ / COFNIJ: Sprawdź ruch IPv6 i polityki zapory.
Przy problemie wróć do poprzedniej konfiguracji IPv6, zachowując działający IPv4.

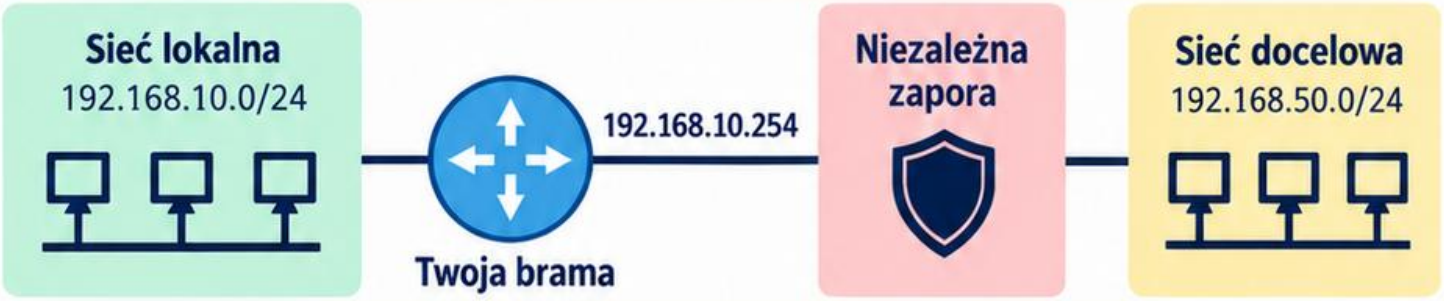
Źródła: [13]

Zaplanuj i dodaj trasę statyczną

Ostoja • Mapa 044

Trasa wskazuje docelową sieć i osiągalny następny skok. Przed zapisaniem sprawdź również trasę powrotną i polityki między segmentami.

GDZIE: Ustawienia routingu bramy; wybierz funkcję Static Route właściwą dla odczytanej wersji.



1. Wypisz prefiks docelowy oraz adres next-hop w sieci bezpośrednio osiągalnej z bramy.
2. Sprawdź, czy cel nie pokrywa się z lokalnym LAN, WAN ani VPN; przygotuj wpis po stronie powrotnej.
3. Dodaj wyłącznie uzgodnioną trasę i zapisz jej nazwę; nie zmieniaj domyślnej trasy przy okazji.

PRZYKŁAD: Cel 192.168.50.0/24 przez router 192.168.10.254 w lokalnym segmencie 192.168.10.0/24.

PUŁAPKA: Trasa nie jest regułą zezwalającą w zaporze i nie naprawia brakującej drogi powrotnej.

SPRAWDŹ / COFNIJ: Testuj między hostami po obu stronach. Przy złej ścieżce wyłącz nowy wpis i porównaj wynik z punktem wyjścia.

Źródła: [25]

Sprawdź MTU przed zmianą

Nie zmniejszaj MTU profilaktycznie. Najpierw ustal, czy problem dotyczy wielkości pakietów, konkretnego tunelu, DNS czy samej aplikacji.

GDZIE: Parametry operatora; opcje bramy w UniFi Devices → brama → Settings.

1. Zapisz obecne MTU i rodzaj WAN; zapytaj operatora o wymagania, zwłaszcza dla PPPoE.
2. Na kontrolowanym kliencie porównaj małe i większe pakiety z zakazem fragmentacji, jeśli narzędzie to obsługuje.
3. Porównaj test z rzeczywistą usługą HTTPS; zmieniaj jeden parametr dopiero po zebraniu powtarzalnego wyniku.

Z czego składa się pakiet (przykład IPv4 / ICMP)



Dodatkowa enkapsulacja zmienia rachunek

Pakiet 1500 bajtów + Dodatkowa enkapsulacja (np. tunel) = Większy pakiet niż 1500 bajtów

PRZYKŁAD

Dla IPv4 ping z ładunkiem 1472 bajtów daje zwykle pakiet 1500 bajtów; dodatkowa enkapsulacja zmienia rachunek.

PUŁAPKA

Brak odpowiedzi ICMP nie wystarcza do rozpoznania błędu MTU. MSS clamping dotyczy TCP, nie wszystkich pakietów.

SPRAWDŹ / COFNIJ

Zapisz wyniki przed i po. Bez poprawy przywróć poprzednią wartość; nie zwiększaj MTU ponad możliwości całej ścieżki.

Źródła: [28], [25]

Moduł 4

Sieci lokalne i usługi

Najpierw adresacja. Potem VLAN-y. Na końcu testy.

Jedna infrastruktura, trzy role



Firma | VLAN 10 | 192.168.10.0/24



Goście | VLAN 20 | 192.168.20.0/24



IoT | VLAN 30 | 192.168.30.0/24



1 Zaplanuj

Unikalna podsieć i brama dla każdej sieci.

2 Skonfiguruj

VLAN, DHCP i przypisanie klientów.

3 Zweryfikuj

Adres IP, DNS i dostęp zgodny z polityką.

Sam VLAN nie określa zasad dostępu między sieciami.

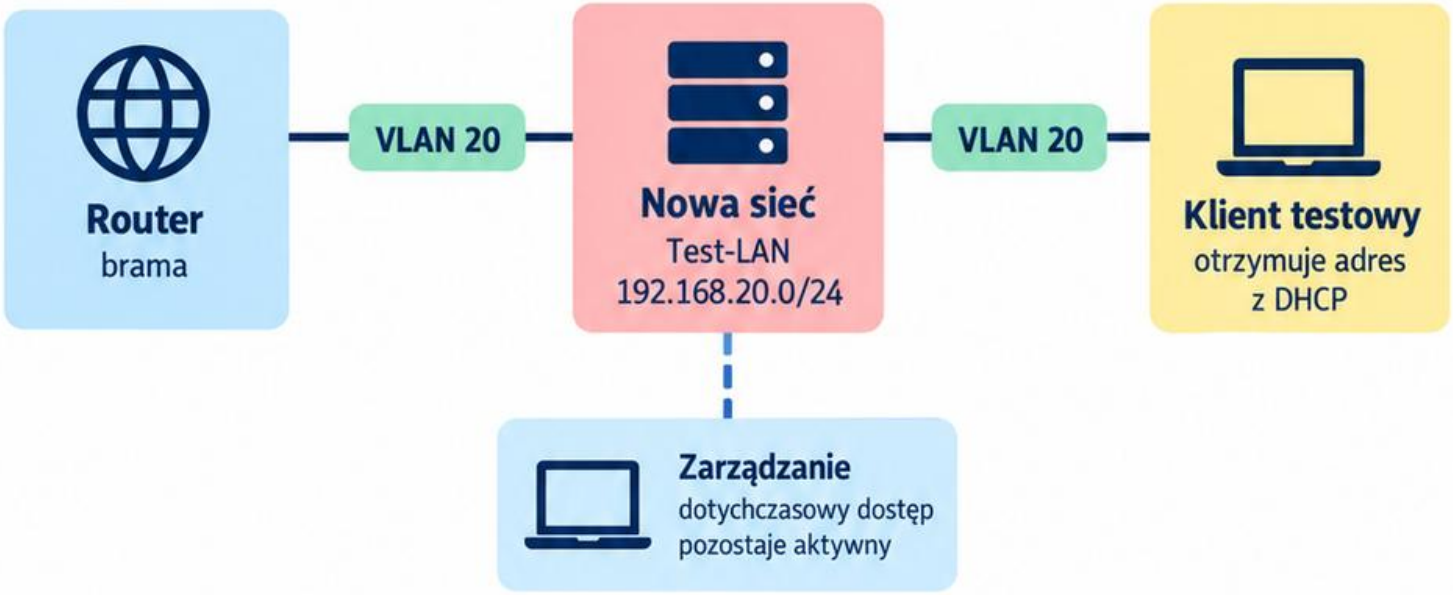
Schemat przykładowy

Utwórz sieć lokalną

Ostoja • Mapa 046

Nowa sieć wymaga routera, rozłącznej podsieci i sposobu podłączenia klientów. Sam zapis sieci nie przenosi do niej urządzeń.

GDZIE: Settings → Networks → utworzenie nowej sieci wirtualnej.



1. Utwórz kopię, nazwij sieć i wskaż właściwą bramę lub router.
2. Ustaw VLAN ID, adresację i DHCP zgodnie z projektem; sprawdź brak nakładania zakresów.
3. Zapisz i przypisz jeden port testowy lub testowe SSID, zachowując dotychczasowy dostęp do zarządzania.

PRZYKŁAD: Test-LAN | VLAN 20 | 192.168.20.0/24 | brama 192.168.20.1.

PUŁAPKA: Nie zmieniaj od razu sieci, przez którą działa jedyna sesja administracyjna.

SPRAWDŹ / COFNIJ: Klient testowy ma otrzymać właściwy adres, DNS i bramę. Przy błędzie przywróć poprzednią sieć na porcie testowym.

Źródła: [1], [12]

Ostoja • Mapa 047

Ustaw adres bramy i maskę

Prefiks określa granice sieci, a adres bramy musi pasować do tego zakresu. Zmiana tych pól może przerwać działające sesje.

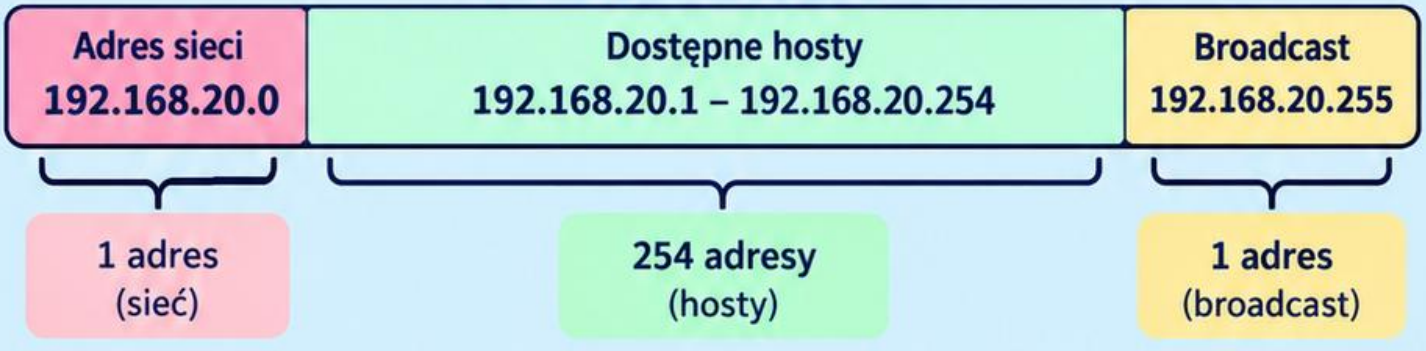
GDZIE: Settings → Networks → wybrana sieć → adresacja podsieci.

1. Oblicz adres sieci, dostępne hosty i broadcast dla IPv4.
2. Wybierz nieużywany adres bramy oraz zgodny zakres DHCP; sprawdź urządzenia ze statycznymi adresami.
3. Wprowadzaj zmianę z lokalnym dostępem i zapisaną poprzednią konfiguracją; po zapisie odnów adres klienta testowego.

PRZYKŁAD: 192.168.20.1/24: sieć .0, hosty .1–.254, broadcast .255. Maska to 255.255.255.0.

IPv4: 192.168.20.1/24

Zakres adresów w podsieci



PUŁAPKA: Nie przypisuj klientowi adresu bramy i nie zakładaj, że każda podsieć ma 254 hosty.

SPRAWDŹ / COFNIJ: Sprawdź bramę oraz panel Network z nowej adresacji. W razie utraty usług odtwórz poprzedni prefiks i adres bramy.

Źródła: [1], [12]

Ostoja • Mapa 048

Wyznacz pulę DHCP

Pula musi mieścić się w podsieci i zapewniać miejsce dla równoczesnych klientów. Zostaw uporządkowany rejestr adresów statycznych i rezerwacji.

GDZIE: Settings → Networks → sieć → ustawienia DHCP.

1. Policz przewidywanych klientów oraz urządzenia zmieniające adres MAC.
2. Wybierz początek i koniec puli bez adresu bramy, sieci i broadcastu.
3. Sprawdź, czy w segmencie działa jeden uzgodniony serwer DHCP; zastosuj ustawienia i odnów dzierżawę klienta.

PODSIEĆ I PULA DHCP – PRZYKŁAD

Podsieć	Pula DHCP	Wykluczone z puli
192.168.20.0/24 (256 adresów)	192.168.20.100 – 192.168.20.220 121 adresów (włącznie)	• adres sieci • adres bramy • adres broadcastu

PRZYKŁAD: W 192.168.20.0/24 pula .100–.220 obejmuje 121 adresów. Adresy statyczne udokumentuj osobno.

PUŁAPKA: Szeroki zakres DHCP nie naprawia kilku serwerów odpowiadających w jednym VLAN.

SPRAWDŹ / COFNIJ: Sprawdź adres, maskę, bramę i DNS klienta. Gdy pula jest błędna, przywróć wcześniejszy zakres przed dalszymi testami.

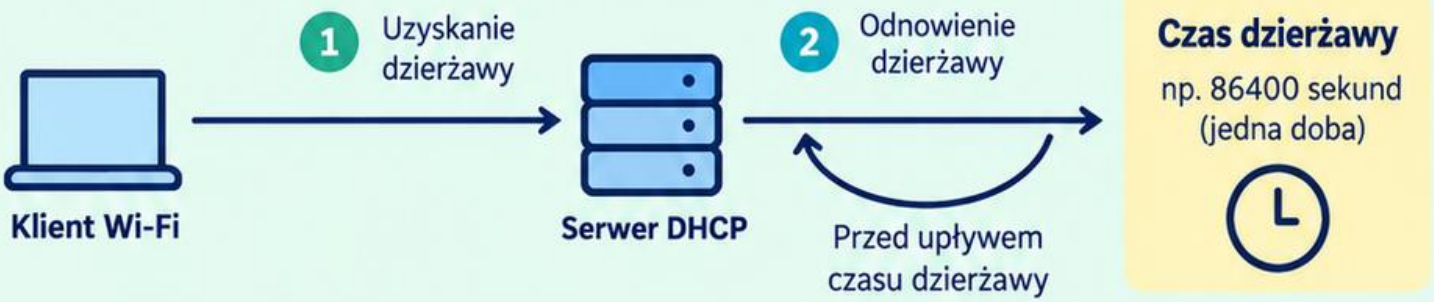
Źródła: [12]

Dobierz czas dzierżawy DHCP

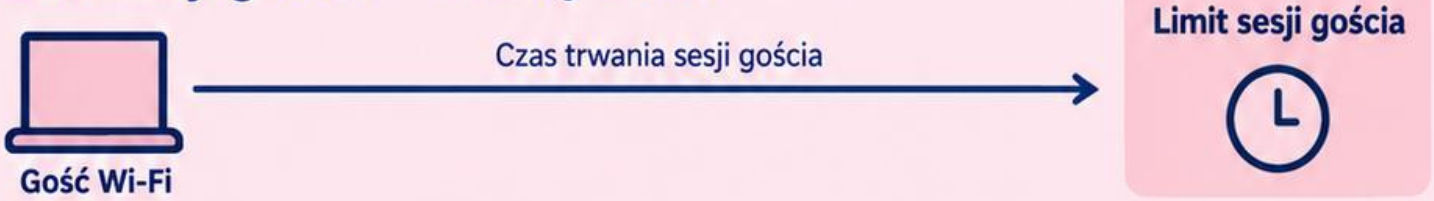
Ostoja • Mapa 049

Czas dzierżawy dobieraj do rotacji klientów i pojemności puli. Krótsza dzierżawa zwiększa częstotliwość odnowień, lecz nie rozłącza automatycznie użytkownika Wi-Fi.

Dzierżawa DHCP – cykl odnowień



Limit sesji gościa – osobny timer



GDZIE: Settings → Networks → sieć → zaawansowane ustawienia DHCP.

1. Zapisz obecny czas, liczbę aktywnych dzierżaw i wielkość puli.
2. Dla stabilnej sieci zacznij od ustawienia domyślnego; zmieniaj je przy konkretnym problemie z rotacją adresów.
3. Po zmianie obserwuj odnawianie i wykorzystanie puli w okresie typowego obciążenia.

PRZYKŁAD: Domyślna wartość wskazana przez Ubiquiti to 86400 sekund, czyli jedna doba.

PUŁAPKA: Nie myl czasu dzierżawy z limitem sesji gościa lub harmonogramem SSID.

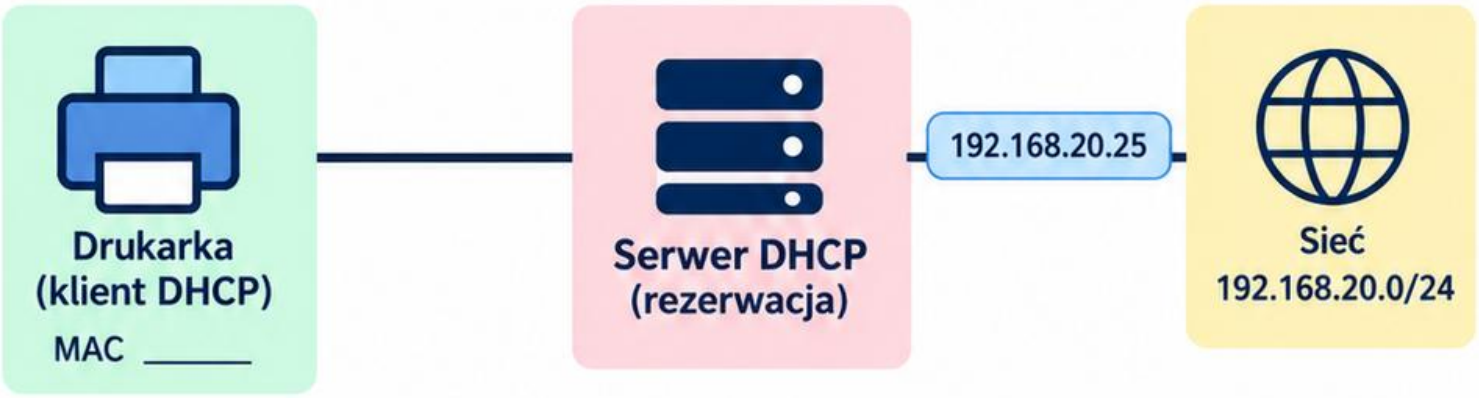
SPRAWDŹ / COFNIJ: Klient ma odnawiać adres bez utraty usługi. Jeśli zmiana nie rozwiązuje problemu, przywróć zapisany czas i zbadaj pojemność puli.

Źródła: [12]

Dodaj rezerwację DHCP

Ostoja • Mapa 050

Rezerwacja zapewnia powtarzalny adres urządzeniu używającemu DHCP. Powiąż ją z właściwym interfejsem i siecią, a nie tylko nazwą klienta.



1. Porównaj MAC urządzenia z inwentarzem; zwróć uwagę na prywatny MAC telefonu.

2. Włącz **Fixed IP Address** i wpisz wolny adres należący do właściwej podsieci.

3. Zastosuj, następnie odnów dzierżawę lub uruchom urządzenie ponownie w uzgodnionym czasie.

GDZIE:
Client Devices → klient → Settings → Fixed IP Address.

PRZYKŁAD:
Drukarka przewodowa: MAC _____ → 192.168.20.25.
Wpisz także port switcha i osobę odpowiedzialną.

PUŁAPKA:
Ręcznie ustawiony statyczny IP nie zostanie nadpisany samą rezerwacją serwera.

SPRAWDŹ / COFNIJ:
Po odnowieniu sprawdź rzeczywisty adres i wydruk testowy. Przy kolizji usuń rezerwację i przywróć poprzedni stan.

Źródła: [26], [12]

Przekaż klientom właściwy DNS

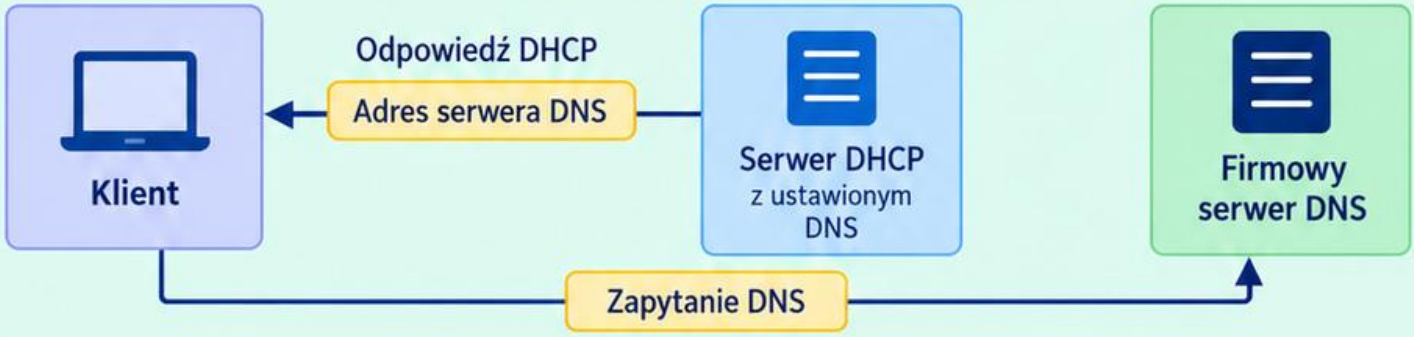
Ostoja • Mapa 051

Klienci mogą potrzebować firmowego resolvera do nazw wewnętrznych. Zmiana DNS WAN nie gwarantuje odpowiedniej konfiguracji klientów.

GDZIE: Settings → Networks → sieć → DNS Server; w części wersji DHCP Service Management.

1. Ustal, czy sieć używa domeny firmowej, lokalnych nazw lub filtrowania DNS.
2. Wprowadź zatwierdzony adres serwera DNS w ustawieniach właściwej sieci.
3. Odnów dzierżawę klienta i sprawdź serwer faktycznie widoczny w jego konfiguracji IP.

Jak klient otrzymuje firmowy DNS



Testy rozwiązywania nazw



PRZYKŁAD:
Klient domenowy korzysta z firmowego DNS; test obejmuje nazwę wewnętrznego serwera oraz ui.com.

PUŁAPKA:
Drugi publiczny DNS może powodować nieprzewidywalne rozwiązywanie nazw firmowych.

SPRAWDŹ / COFNIJ: Sprawdź nazwy lokalne i publiczne z każdego objętego VLAN. W razie błędu przywróć poprzednie DNS i odnów dzierżawę.

Źródła: [18], [26]

Znajdź konflikt adresów

Ostoja • Mapa 052

Podejrzewaj konflikt przy zmiennym MAC dla jednego IPv4, losowej utracie sesji lub komunikacie systemu. Najpierw ustal obie strony.

GDZIE: Client Devices oraz rejestr DHCP i adresów statycznych.



Client Devices



Rejestr DHCP i adresów statycznych



Tablica ARP na kliencie

1. Zapisz problematyczny IP, MAC, port i czas objawu.
2. Porównaj dzierżawy, rezerwacje oraz ręczne ustawienia urządzeń; sprawdź tablicę ARP na kliencie.
3. Odłącz lub przeadresuj **wyłącznie** potwierdzone urządzenie konfliktowe w uzgodnionym oknie.

PRZYKŁAD: Drukarka ma ręcznie .120, a ten sam adres znajduje się w puli DHCP .100–.220.



Drukarka (ręczny IP) .120

IP .120



Pula DHCP .100–.220

PUŁAPKA: Brak odpowiedzi ping nie oznacza, że adres jest wolny; host może blokować ICMP.

SPRAWDŹ / COFNIJ: Po korekcie odnów dzierżawę i sprawdź stałość IP–MAC oraz usługę. Zachowaj poprzednie ustawienia do wycofania.

Źródła: [12]

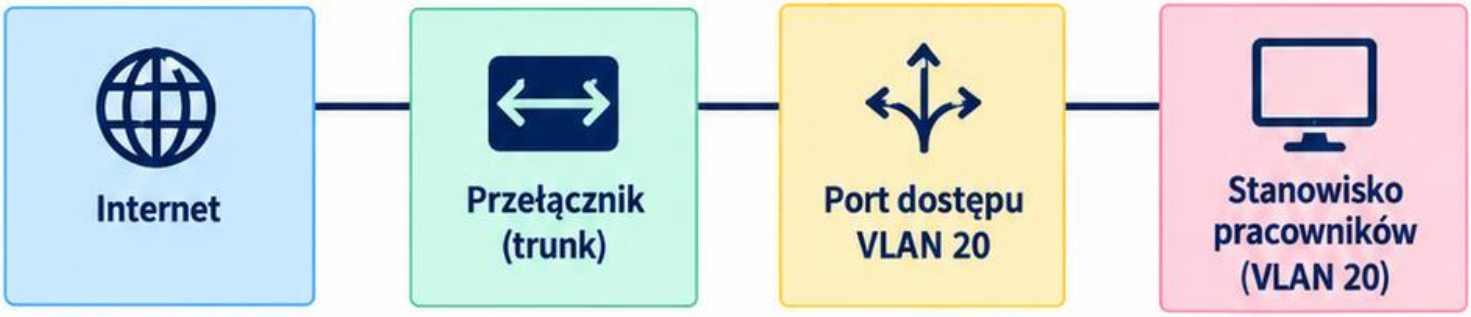
Utwórz VLAN pracowników

Ostoja • Mapa 053

Segment pracowników powinien otrzymać własną podsieć i udokumentowany dostęp do usług. Zmieniaj najpierw jedno stanowisko pilotażowe.

GDZIE: Settings → Networks → nowa sieć; przypisanie przez port lub SSID.

1. Utwórz sieć Pracownicy, wpisz unikalny VLAN ID, bramę i DHCP.
2. Zapewnij przenoszenie VLAN na wymaganych uplinkach i przypisz port testowy lub SSID.
3. Dodaj tylko potrzebne reguły dostępu do drukarki, serwerów i internetu zgodnie z macierzą.



PRZYKŁAD:
VLAN 20 | 192.168.20.0/24; stanowisko testowe otrzymuje .100–.220 i docelowy DNS.

PUŁAPKA:
Samo powstanie sieci nie przypisuje klientów ani nie ogranicza ruchu między VLAN-ami.

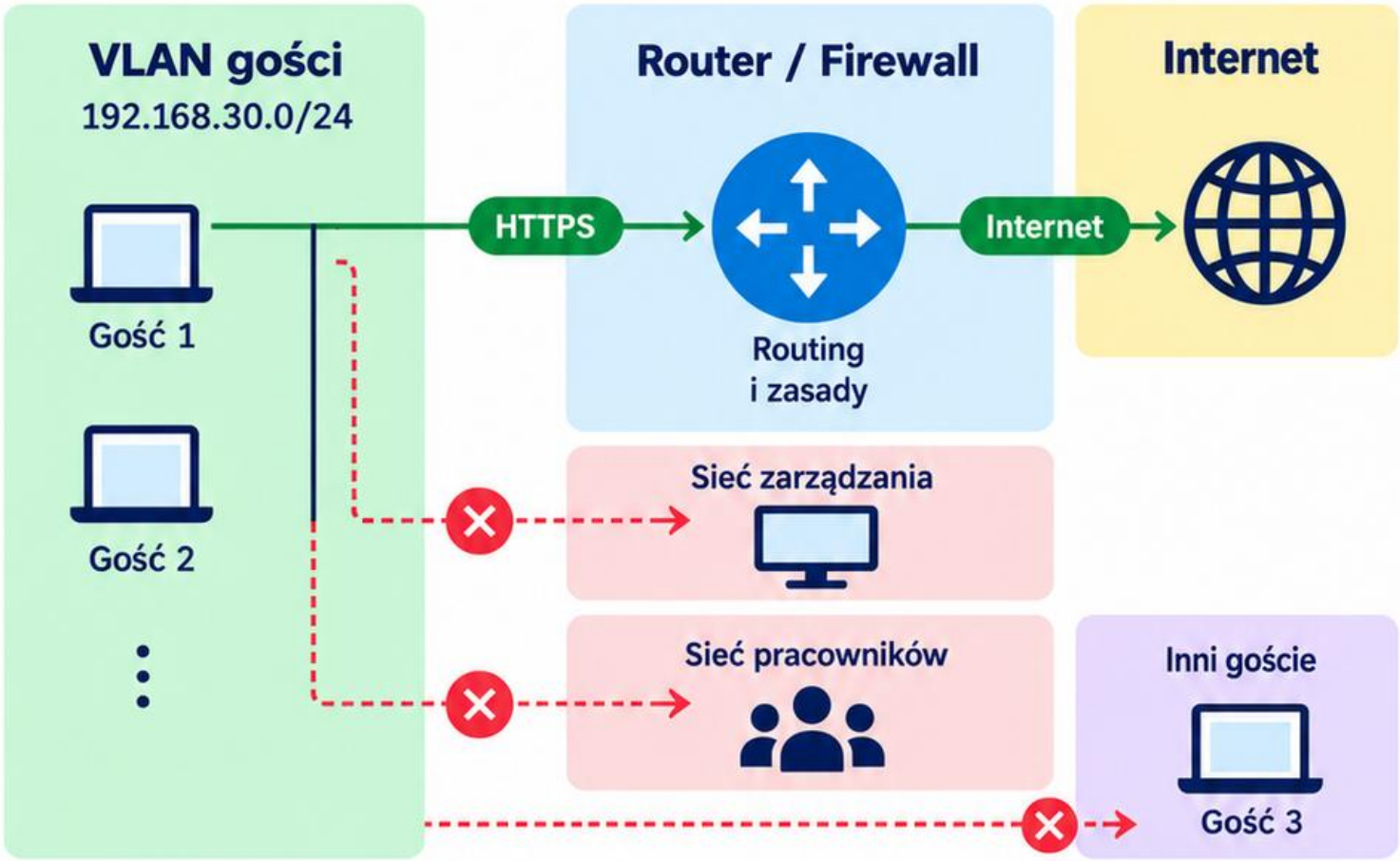
SPRAWDŹ / COFNIJ:
Sprawdź logowanie użytkownika, DNS i wydruk. Przy błędzie przywróć stare przypisanie stanowiska przed migracją pozostałych.

Źródła: [1], [3]

Utwórz VLAN gości

Ostoja • Mapa 054

Goście potrzebują internetu i usług niezbędnych do połączenia. Dostęp do zarządzania, pracowników i urządzeń innych gości oceniaj osobnymi testami.



1. Utwórz odrębną sieć z własnym DHCP i DNS.
2. Przypisz ją do SSID gości i potrzebnych portów; potwierdź VLAN na uplinkach.
3. Skonfiguruj izolację sieci i klientów według możliwości sprzętu oraz wymagań projektu.
4. **GDZIE:** Settings → Networks → nowa sieć; Settings → WiFi dla SSID gości.

PRZYKŁAD: VLAN 30 | 192.168.30.0/24; testowy gość otwiera HTTPS, ale nie panel zarządzania.

PUŁAPKA: Izolacja klientów tego samego AP nie zastępuje wszystkich zasad między sieciami i portami.

SPRAWDŹ / COFNIJ: Sprawdź internet, blokadę LAN i komunikację dwóch gości. Cofnij nowe SSID lub przypisanie, jeśli DHCP przestaje działać.

Źródła: [1], [2], [20]

Utwórz VLAN IoT

Ostoja • Mapa 055

Zbierz wymagania urządzeń IoT przed włączeniem blokad. Czujnik, drukarka i odbiornik multimediów mogą wymagać różnych usług lokalnych.

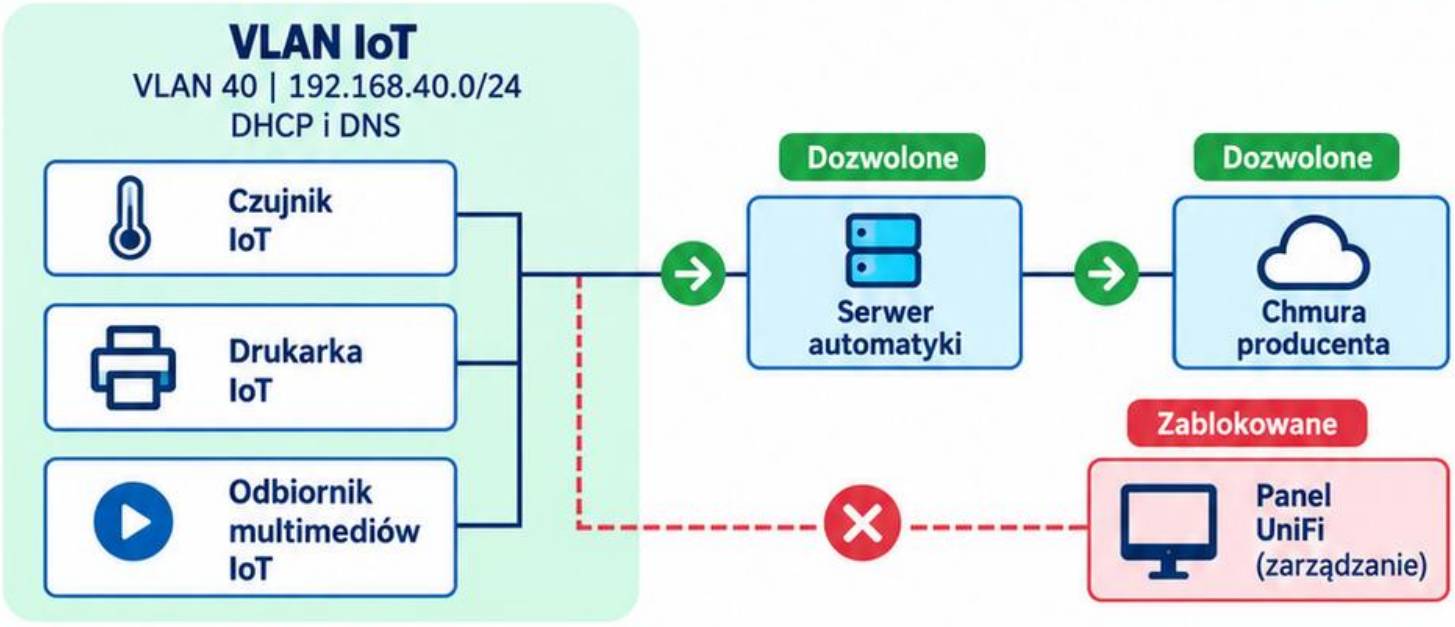
GDZIE: Settings → Networks; przypisanie przez dedykowany port lub SSID.

1. Utwórz sieć IoT z własną adresacją, DHCP i DNS.
2. Przenieś jeden egzemplarz testowy; zapisz jego komunikację z chmurą i potrzebnymi systemami lokalnymi.
3. Ogranicz dostęp do innych segmentów, dodając wyłącznie uzasadnione wyjątki i ewentualne przekazywanie mDNS.

PRZYKŁAD: VLAN 40 | 192.168.40.0/24; sterownik kontaktuje się z wyznaczonym serwerem automatyki, bez dostępu do panelu UniFi.

PUŁAPKA: Blokada całego ruchu przed rozpoznaniem zależności może unieruchomić urządzenie.

SPRAWDŹ / COFNIJ: Sprawdź sterowanie i aktualizację, a następnie wykonaj test zakazanego dostępu. Cofnij ostatnią regułę przy utracie wymaganej funkcji.



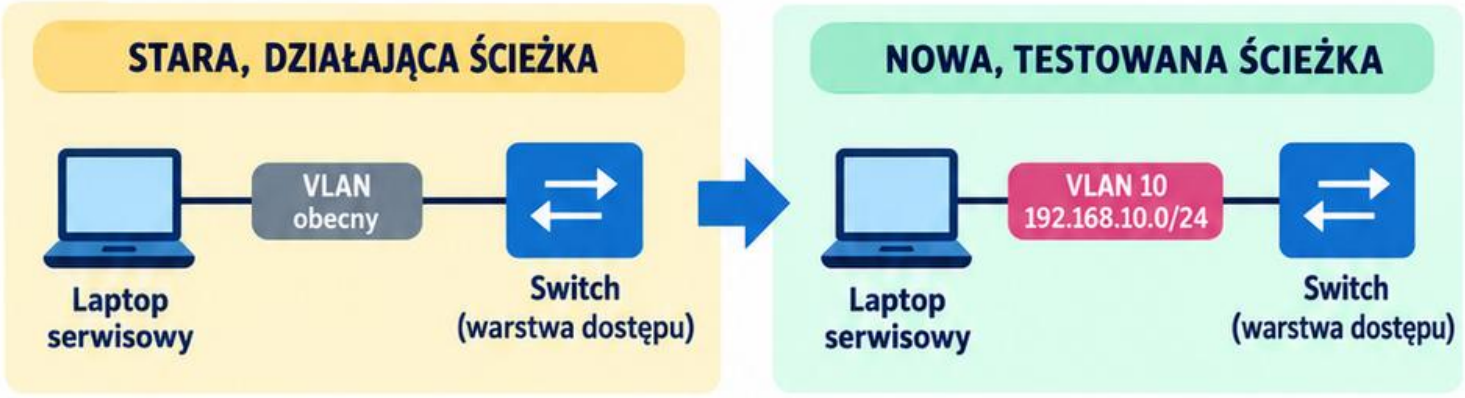
Źródła: [1], [20], [29]

Wydziel VLAN zarządzania

Ostoja • Mapa 056

To zmiana o wysokim ryzyku odcięcia administratora.
Przygotuj nową drogę, zanim przeniesiesz host i urządzenia infrastruktury.

GDZIE: Settings → Networks oraz ustawienia portów i zarządzania konkretnych urządzeń.



1. **Zrób kopię:** zapisz stare IP, port awaryjny oraz sposób lokalnego powrotu.
2. **Utwórz docelową sieć** i zapewnij właściwe tagowanie na całej trasie uplinków.
3. **Przenieś** jedno urządzenie testowe, potwierdź komunikację z Network, następnie przenoś kolejne pojedynczo.

PRZYKŁAD: VLAN 10 | 192.168.10.0/24; laptop serwisowy ma przygotowany port z dostępem do nowej sieci.

PUŁAPKA: Nie zmieniaj jednocześnie VLAN zarządzania na wszystkich switchach i AP.

SPRAWDŹ / COFNIJ: Każdy etap kończy się Online i nowym logowaniem. Przy braku dostępu przywróć poprzedni VLAN na ostatnio zmienionym urządzeniu.

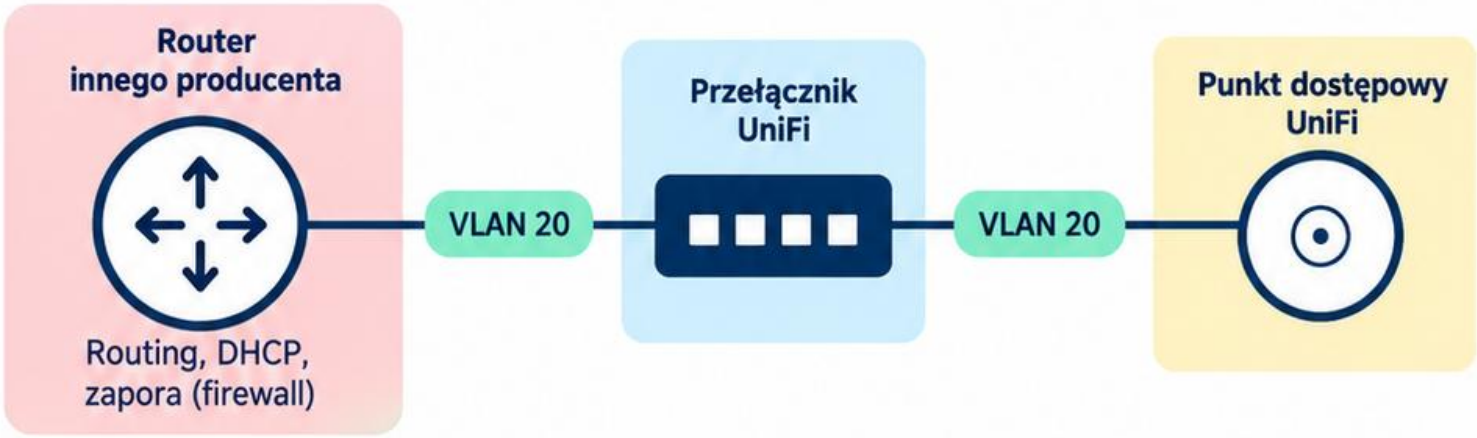
Źródła: [1], [10], [27]

Ostoja

Połącz sieć z bramą innego producenta

Ostoja • Mapa 057

Routing, DHCP i zapora pozostają odpowiedzialnością wybranego routera. Utworzenie sieci w UniFi nie konfiguruje automatycznie bramy spoza UniFi.



GDZIE: Najpierw panel zewnętrznego routera; następnie Settings → Networks → Router → Third-party Gateway.

1. Na zewnętrznym routerze utwórz VLAN, podsieć i uzgodnioną usługę DHCP.
2. W Network utwórz odpowiadającą sieć, wybierz Third-party Gateway i wpisz identyczny VLAN ID.
3. Sprawdź tagowanie portu router–switch oraz dalszych uplinków i przypisz port testowy.

PRZYKŁAD: VLAN 20 jest skonfigurowany na obu końcach; bramę 192.168.20.1 i pulę DHCP zapewnia router zewnętrzny.

PUŁAPKA: Nie zakładaj, że reguły Network sterują zaporą routera innego producenta.

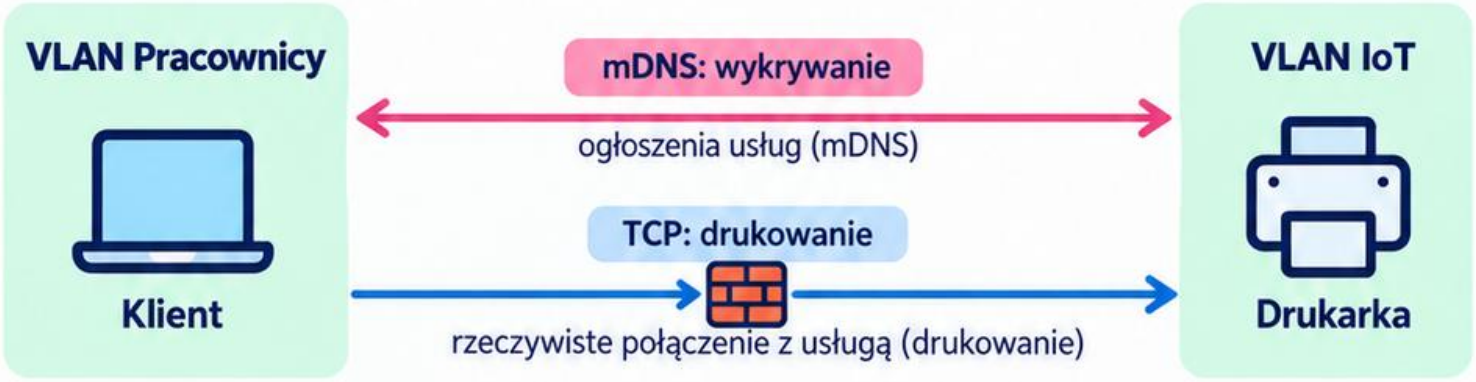
SPRAWDŹ / COFNIJ: Klient musi otrzymać właściwe parametry i działać zgodnie z polityką routera. Cofnij przypisanie portu przy braku usługi.

Źródła: [1]

Rozpisz wykrywanie mDNS

Ostoja • Mapa 058

mDNS pomaga odkrywać usługi między wybranymi sieciami. Samo wykrycie drukarki nie oznacza, że zapora zezwala na późniejsze drukowanie.



GDZIE: Settings → Networks; opcje mDNS wymagają zgodnej bramy UniFi.

1. Wskaż sieć klienta, sieć usługi oraz potrzebny typ usługi.
2. Wybierz możliwie wąski zakres przekazywania; w wersjach z Custom określ VLAN-y i wymagane usługi.
3. Sprawdź osobno pojawienie się urządzenia na liście oraz rzeczywiste połączenie z jego portem usługi.

PRZYKŁAD: Pracownicy odkrywają drukarkę w IoT; goście nie otrzymują jej ogłoszeń. Wyjątek zapory pozwala tylko na potrzebne drukowanie.

PUŁAPKA: Nie włączaj wszystkich usług między wszystkimi VLAN-ami bez uzasadnienia.

SPRAWDŹ / COFNIJ: Przetestuj odkrywanie i wydruk; sprawdź także brak widoczności u gościa. Przy nadmiernym udostępnianiu cofnij zakres mDNS.

Źródła: [29], [4]

Zaplanuj IPv6 w każdej sieci

Ostoja • Mapa 059

Każdy segment potrzebuje własnego prefiksu i spójnej polityki bezpieczeństwa. Najpierw potwierdź działający WAN oraz delegację operatora.

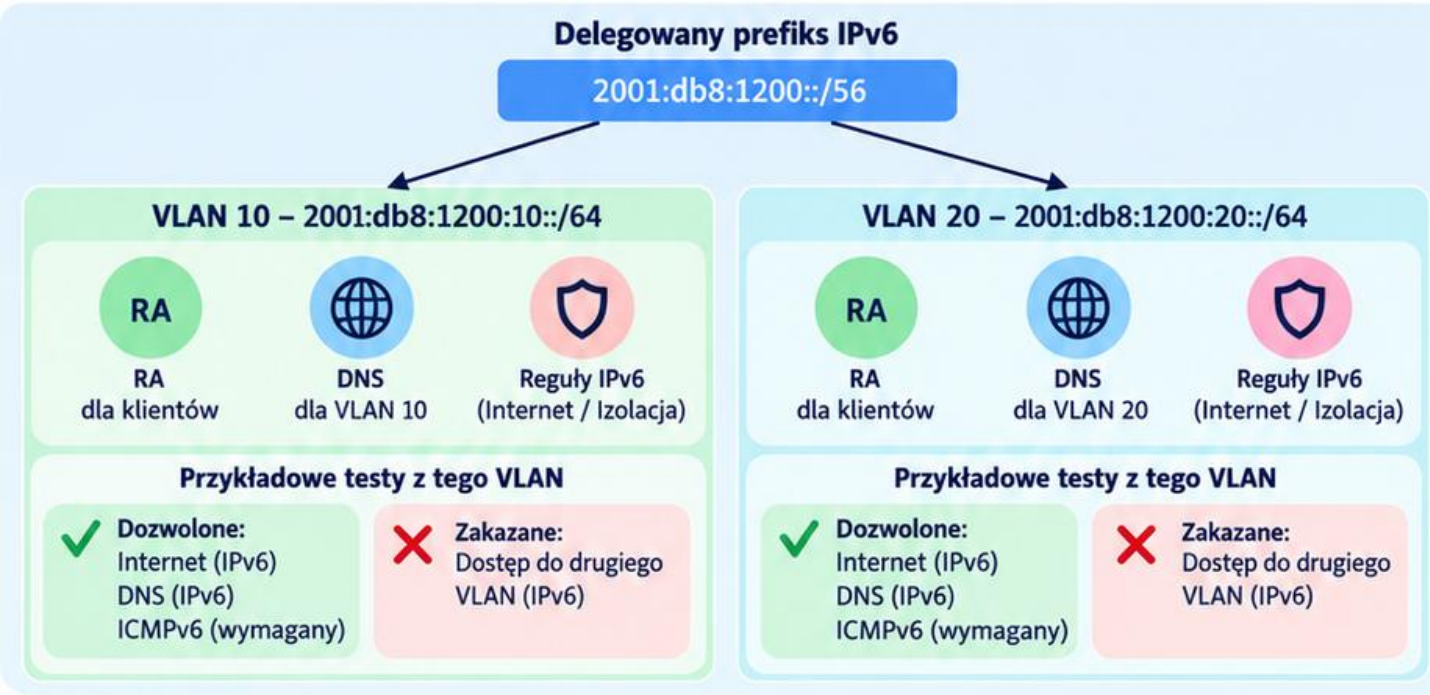
GDZIE: Settings → Internet → WAN → IPv6 Configuration; następnie Settings → Networks → wybrana sieć.

1. Przydziel różne /64 z delegowanego prefiksu do planowanych VLAN-ów.
2. Dobierz automatyczny przydział i RA do klientów; SLAAC jest istotny między innymi dla urządzeń Android.
3. Sprawdź DNS i reguły IPv6 dla internetu oraz izolacji. Zachowaj ICMPv6 wymagany do działania sieci.

PRZYKŁAD: Prefiksy dokumentacyjne: 2001:db8:1200:10::/64 i 2001:db8:1200:20::/64; nie używaj ich jako adresów produkcyjnych.

PUŁAPKA: Blokada tylko IPv4 nie dowodzi izolacji klientów korzystających także z IPv6.

SPRAWDŹ / COFNIJ: Sprawdź adres globalny, trasę domyślną i testy dozwolone oraz zakazane. Cofnij konfigurację objętego VLAN, jeśli testy zawodzą.



Źródła: [13], [3]

Odbierz usługi w każdym VLAN

Ostoja • Mapa 060

Wykonuj tę samą serię testów z każdego segmentu. Sukces w *sieci* administratora nie potwierdza działania gości, IoT ani pracowników.

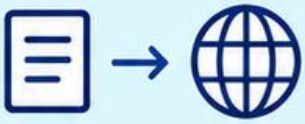
GDZIE: Client Devices i karta testów; konfiguracja sieci w Settings → Networks.

1



Podłącz klienta przewodowego lub Wi-Fi i zapisz IP, prefiks, bramę, DNS oraz VLAN.

2



Sprawdź dzierżawę, nazwy publiczne i lokalne oraz rzeczywistą usługę przewidzianą dla grupy.

3



Wykonaj próbę połączenia, która ma być zablokowana; powtórz dla IPv6, jeżeli jest używane.

Karta testów każdego VLAN-u

Wpisz wynik zgodny z przyjętą polityką.

VLAN / klient	DHCP / DNS	Usługa dozwolona	Próba zabroniona	IPv6, jeśli używane
Administratorzy	☐ _____	☐ _____	☐ _____	☐ _____
Pracownicy	☐ _____	☐ _____	☐ _____	☐ _____
Goście	☐ _____	☐ _____	☐ _____	☐ _____
IoT	☐ _____	☐ _____	☐ _____	☐ _____

PRZYKŁAD: VLAN 30: HTTPS działa, panel UniFi niedostępny, drugi gość niedostępny według przyjętej polityki.

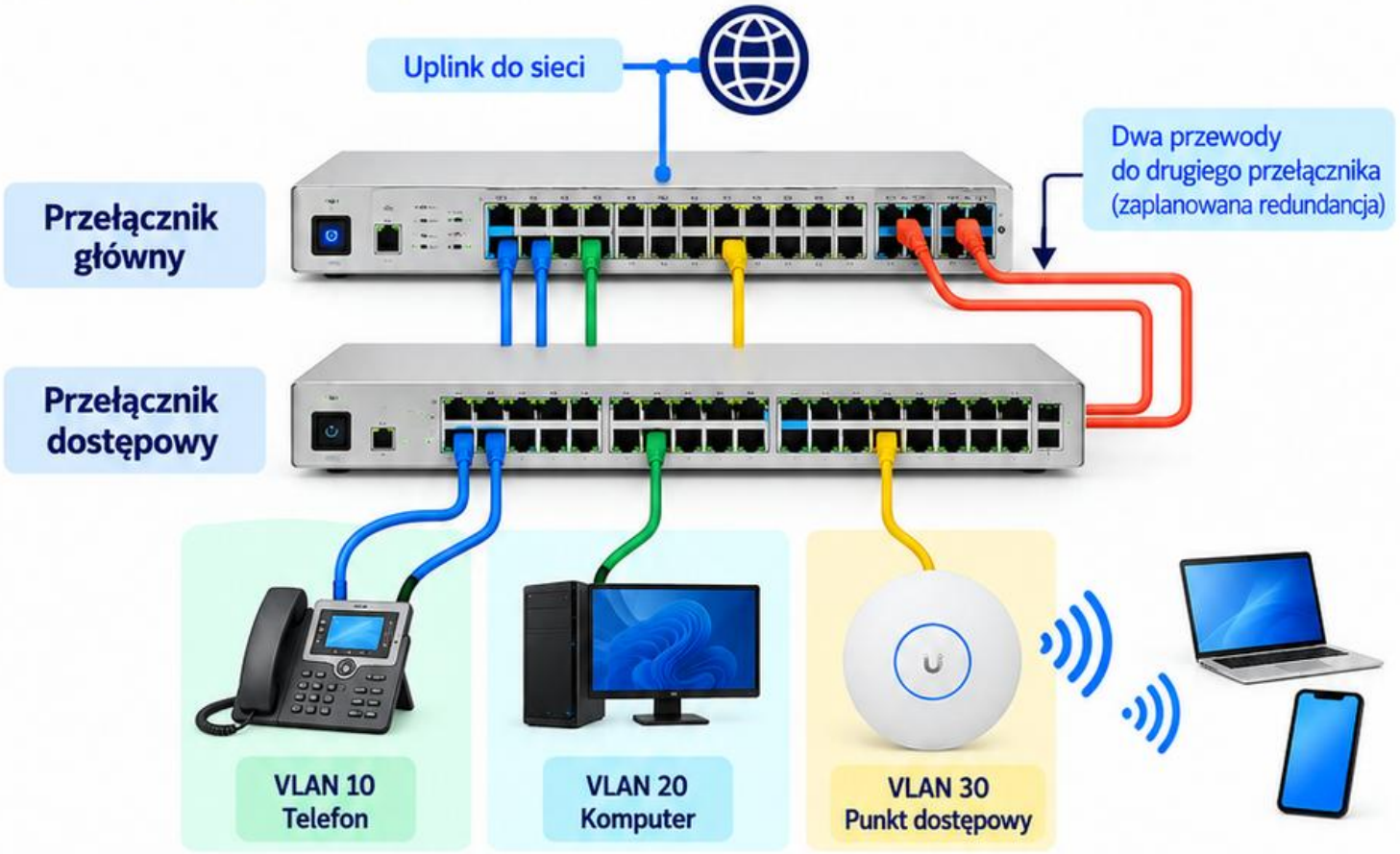
PUŁAPKA: Brak odpowiedzi ping nie potwierdza blokady wszystkich usług; testuj konkretny port lub aplikację.

SPRAWDŹ / COFNIJ: Zapisz wyniki, klienta i czas. Przy błędzie zatrzymaj migrację oraz cofnij ostatnie przypisanie lub regułę.

Źródła: [1], [12], [18], [20], [13]

Przełączniki i porty

Port decyduje, dokąd trafi ramka i czy urządzenie otrzyma zasilanie. Zacznij od opisania przewodów, zanim zmienisz ustawienia.



1. Zrozum topologię

W tym module rozdzielisz ruch nietagowany od tagowanego, sprawdzisz PoE i zbudujesz przewidywalną topologię przełączników.

2. Wykonaj analizę

Kolejność pracy: rozpoznaj uplink, przygotuj port odbiornika, prześledź VLAN, a dopiero później wprowadzaj dodatkowe połączenia.

3. Zastosuj w praktyce

Przykład: biuro w Łodzi ma telefon, komputer i punkt dostępowy. Każdy wymaga innego zestawu dozwolonych sieci.

4. Zadbaj o redundancję

Dwa przewody między przełącznikami wymagają zaplanowanego mechanizmu redundancji. Przypadkowy pierścień może zatrzymać całą sieć.

5. Zmieniając port zarządzający

Przed zmianą portu zarządzającego zapewnij dostęp lokalny. Zapisz poprzednią konfigurację i wskaż osobę mogącą przepiąć przewód.

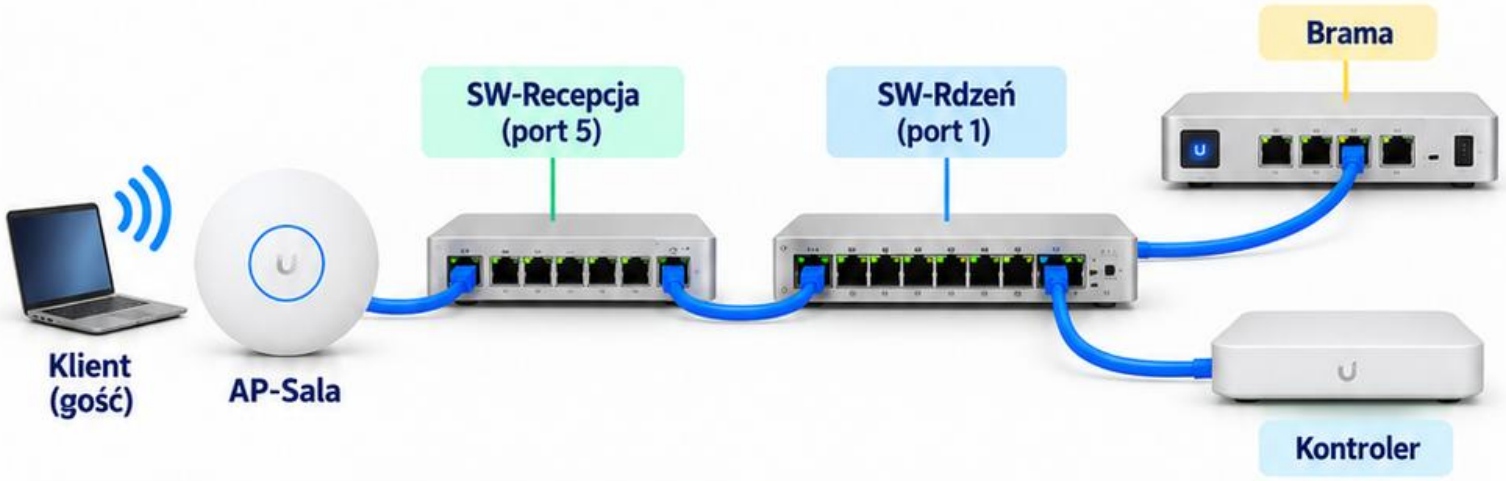
6. Sprawdź wynik

Za poprawny wynik uznaj działanie właściwej usługi, właściwy adres klienta i brak nieoczekiwanych blokad portów.

Źródła: [4], [5], [6]

Ostoja · Mapa 061 · Rozpoznaj uplinki

Cel: ustalić fizyczną drogę do bramy i kontrolera.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1. Porównaj numer portu z opisem przewodu.

Sprawdź urządzenie po drugiej stronie i aktualny stan łącza.



2. Oznacz uplink po obu stronach.

Zapisz sieć zarządzającą oraz VLAN-y wymagane przez urządzenia dalej w topologii.



3. Przykład.

SW-Recepcja prowadzi do SW-Rdzeń, a nie bezpośrednio do bramy. Oba odcinki muszą przenosić VLAN gości.



4. Potwierdź drogę kontrolowanym testem klienta.

Nie wyłączaj uplinku tylko po to, by sprawdzić, który opis był prawdziwy.



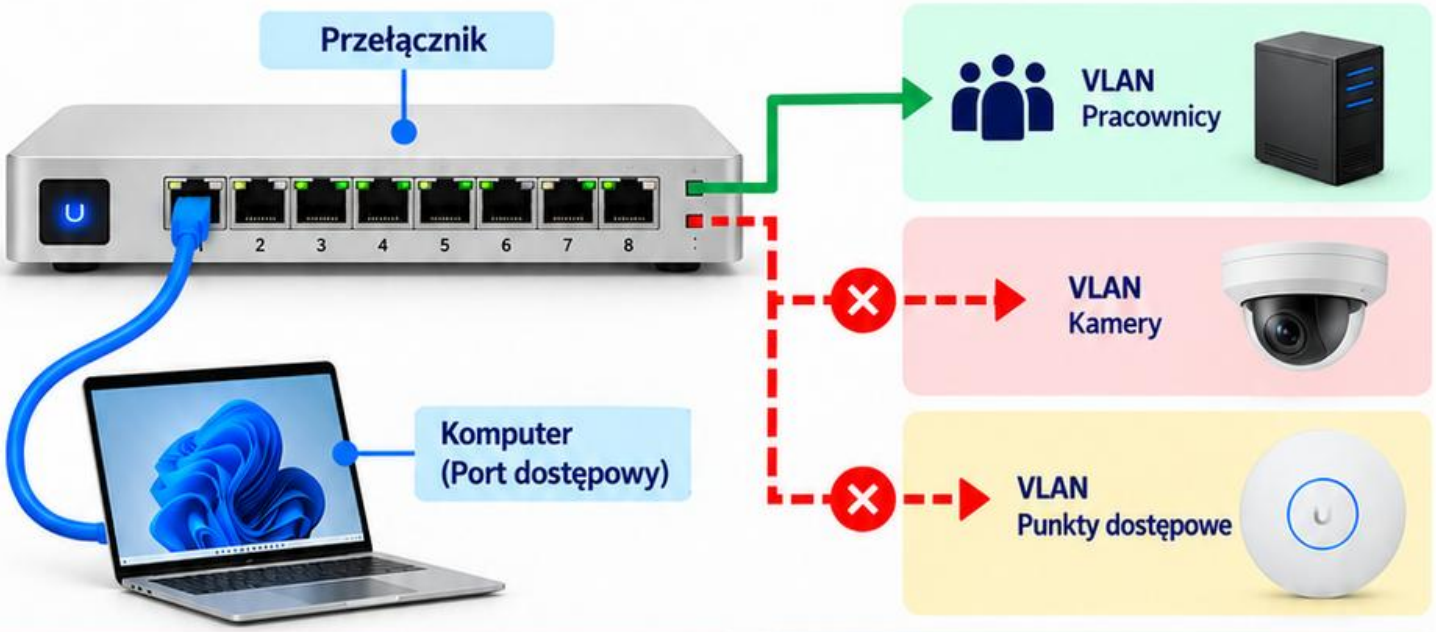


Nie wyłączaj uplinku
tylko po to, by sprawdzić, który opis był prawdziwy.

Źródła: [4]

Ostoja · Mapa 062 · Skonfiguruj port dostępowy

Cel: przyłączyć zwykły komputer do jednej sieci.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1. Wybierz port komputera

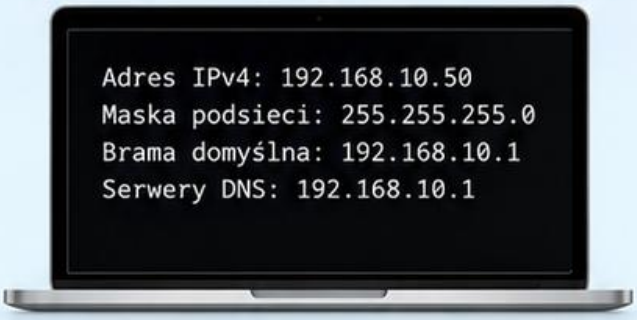
Wybierz port komputera. Ustaw **Native VLAN** na sieć użytkowników. Dla zwykłego odbiornika bez tagowania ogranicz Tagged VLAN Management.

Port Manager – port 1

Port	1
Native VLAN	Pracownicy (VLAN 10)
Tagged VLAN Management	Wyłączone

2. Zastosuj i sprawdź adres

Zastosuj zmianę tylko do wybranego portu. Odnów dzierżawę DHCP klienta i porównaj adres, maskę, bramę oraz DNS.



3. Sprawdź działanie sieci

Sprawdź dozwoloną aplikację i próbę dostępu do zabronionej sieci. Port dostępowy sam nie tworzy polityki firewalla.



4. Przykład

Przykład: komputer księgowości trafia do sieci Pracownicy; nie potrzebuje tagowanych VLAN-ów kamer ani punktów dostępowych.



Źródła: [4]

Ustal natywny VLAN

Cel: jednoznacznie przypisać ruch bez znacznika VLAN.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1. Sprawdź oczekiwania urządzenia końcowego.

Native VLAN klasyfikuje ramki przychodzące bez tagu; nie jest listą wszystkich dostępnych sieci.



2. Porównaj konfigurację obu końców połączenia między przełącznikami.

Zmieniaj ją w oknie serwisowym, zachowując drogę zarządzania.



3. Przykład.

AP zarządza się bez tagowania, a SSID gości używa tagowanego VLAN-u. Te funkcje muszą pozostać rozdzielone.



4. Po zmianie sprawdź dostępność AP i adres klienta każdego SSID.

Błąd natywnego VLAN-u może odciąć zarządzanie mimo aktywnego łącza.



Błędny natywny VLAN może odciąć zarządzanie.



Prawidłowa konfiguracja zapewnia rozdzielenie ruchu i dostępność.

Źródła: [4]

Prześlij ruch VLAN przez uplink

Cel: klient w VLAN 20 otrzymuje adres z właściwej podsieci.
Przykład: Goście, VLAN 20, 192.168.20.0/24



1. Przygotuj sieć

Utwórz VLAN 20, bramę 192.168.20.1/24 i zakres DHCP.



2. Sprawdź uplink

Na obu końcach łącza dopuść tagowany VLAN 20. Zachowaj zgodną sieć natywną.



3. Sprawdź port AP

Dopuść VLAN 20 do AP. Nie zmieniaj pochopnie sieci zarządzającej.



4. Powiąż Wi-Fi

Przypisz SSID Goście do sieci VLAN 20.



5. Przetestuj

Połącz klienta. Sprawdź adres 192.168.20.x, bramę i DNS.



Brak VLAN-u na jednym porcie przerywa całą ścieżkę.
Przed zmianą zapisz konfigurację portów i zapewnij dostęp lokalny.



Schemat przykładowy | Źródła: [1], [2]

Ogranicz VLAN-y na porcie AP

Cel: przekazać punktowi dostępowemu tylko potrzebne sieci.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1. Zapisz potrzebne sieci

Zapisz sieć zarządzającą AP i sieci przypisane do jego SSID. Odróżnij tagowany ruch klientów od ruchu zarządzającego.

Cel	VLAN
Zarządzanie AP	99
SSID Pracownicy	10
SSID Goście	20

2. Skonfiguruj port przełącznika

W Tagged VLAN Management wybierz wymagane VLAN-y. Zachowaj zgodny Native VLAN; nie usuwaj sieci używanej do zarządzania.

Schemat

Native VLAN 99 • Zarządzanie

Tagowane VLAN-y

- [x] VLAN 10 • Pracownicy
- [x] VLAN 20 • Goście
- [ ] VLAN 30 • Kamery

3. Przykład

Przykład: AP w recepcji nadaje Pracownicy i Goście. VLAN kamer nie jest mu potrzebny, jeśli nie obsługuje żadnej takiej usługi.



4. Przetestuj

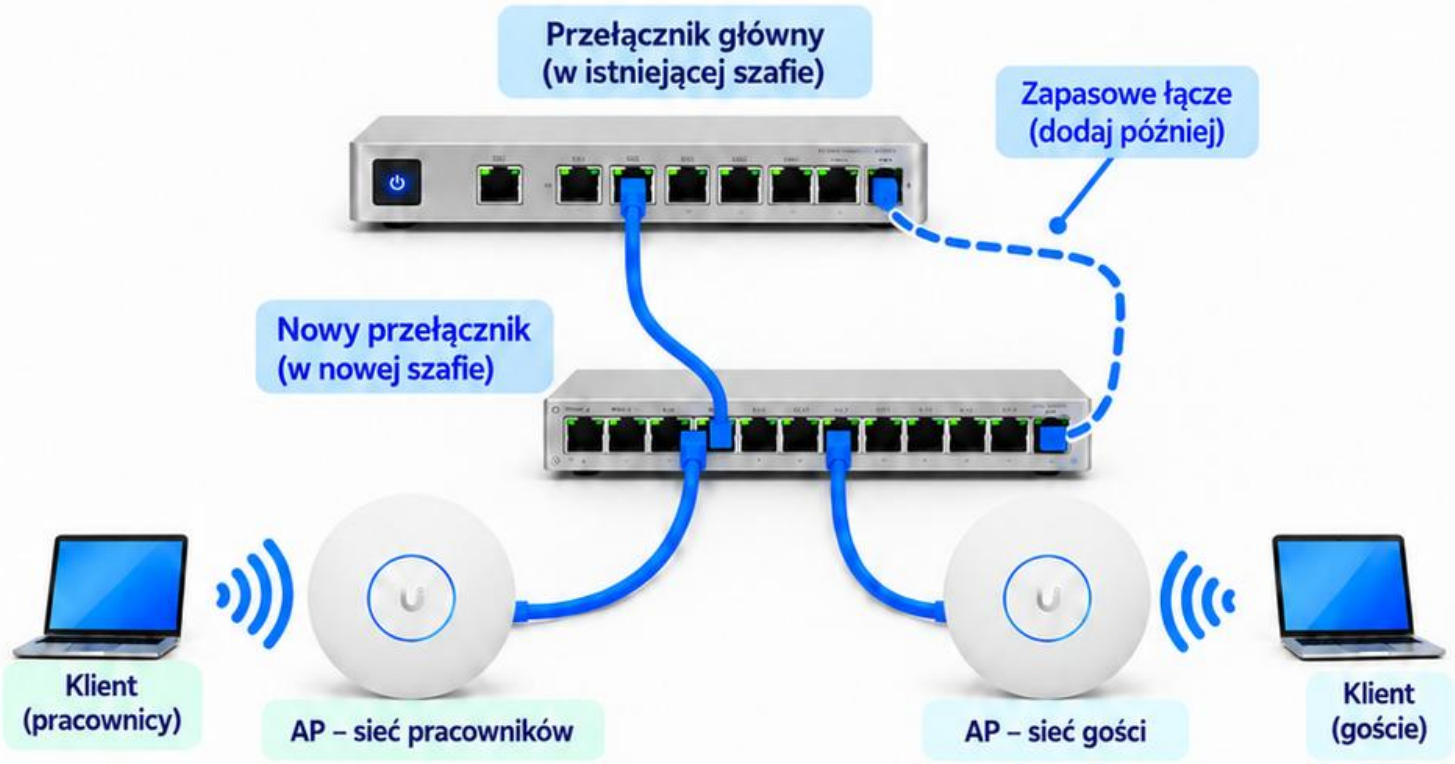
Przetestuj osobno każdy SSID i dostępność AP w kontrolerze. Działanie jednego SSID nie potwierdza pozostałych ścieżek.

- SSID Pracownicy ✓
- SSID Goście ✓
- AP w kontrolerze (VLAN zarządzający) ✓

Źródła: [4]

Dołącz kolejny przełącznik

Cel: rozszerzyć sieć bez pętli i utraty zarządzania.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1. Najpierw podłącz pojedynczy uplink.

Sprawdź zasilanie, wykrycie urządzenia i zgodność sieci zarządzającej na obu końcach.



2. Przenieś tylko VLAN-y potrzebne odbiornikom nowego przełącznika.

Opisz przewód, port nadrzędny oraz port po stronie nowego urządzenia.

3. Przykład: nowa szafa na piętrze wymaga sieci pracowników i gości. Nie przenosi automatycznie wszystkich sieci przedsiębiorstwa.



4. Podłącz klienta testowego w każdej wymaganej sieci.

Drugi przewód dodawaj dopiero po przygotowaniu STP lub zgodnej agregacji.

Schemat



Źródła: [4]

Podłącz telefon z VLAN-em głosowym

Cel: rozdzielić ruch telefonu i komputera na jednym stanowisku.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1 Sprawdź możliwości telefonu

Sprawdź obsługę LLDP-MED oraz VLAN-u głosowego w telefonie. Ustal, czy komputer korzysta z dodatkowego portu telefonu.



2 Skonfiguruj port przełącznika

W ustawieniach portu skonfiguruj Voice VLAN oraz właściwy Native VLAN dla zwykłego ruchu. Zachowaj obsługę wymaganych VLAN-ów.

Voice VLAN	VLAN 30 (Głos)
Native VLAN	VLAN 10 (Pracownicy)
LLDP-MED	Włączone

3 Przykład działania

Przykład: telefon korzysta z sieci Głos, a komputer z sieci Pracownicy. Nie zakładaj, że każdy telefon sam rozpozna konfigurację.

VLAN 30 (Głos)



VLAN 10 (Pracownicy)



4 Zweryfikuj poprawność

Zweryfikuj oddzielnie adres telefonu, rejestrację usługi głosowej i adres komputera. Test połączenia nie zastępuje sprawdzenia segmentacji.

- Telefon: poprawny adres IP i zarejestrowana usługa głosowa.
- Komputer: poprawny adres IP w sieci pracowników.
- Ruch rozdzielony zgodnie z VLAN-ami.

Źródła: [4]

Włącz zgodne PoE

Cel: zasilić odbiornik zgodnie z jego wymaganiami.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1. Sprawdź wymagania odbiornika

Odczytaj standard zasilania odbiornika i parametry konkretnego portu. Sprawdź dostępny budżet przełącznika oraz sposób jego zasilania.



Wymagania punktu dostępowego (przykład)

Standard PoE	802.3at
Pobór mocy	25 W
Tryb zasilania	PoE (negocjacja)

2. Sprawdź możliwości portu

Włącz odpowiedni tryb PoE dopiero po sprawdzeniu zgodności. Nie utożsamiaj pasywnego zasilania z automatycznie negocjowanym PoE.



Port przełącznika (przykład)

Standard PoE	802.3at
Maks. moc portu	30 W
Tryb PoE	Auto
Status	Enabled

3. Sprawdź budżet przełącznika

Przykład: punkt dostępowy wymaga innego poziomu mocy niż telefon. Sam napis PoE na przełączniku nie potwierdza zgodności portu.

Budżet PoE przełącznika (przykład)

Całkowity budżet	250 W
Wykorzystany	120 W
Dostępny	130 W
Zasilanie przełącznika	Zasilacz AC

4. Obserwuj działanie

Obserwuj uruchomienie i pobór po podłączeniu. Jeśli urządzenie restartuje się pod obciążeniem, sprawdź budżet, przewód i wymagania producenta.



Po podłączeniu (przykład)

Status PoE	OK
Pobór mocy	24 W
Stan urządzenia	Online

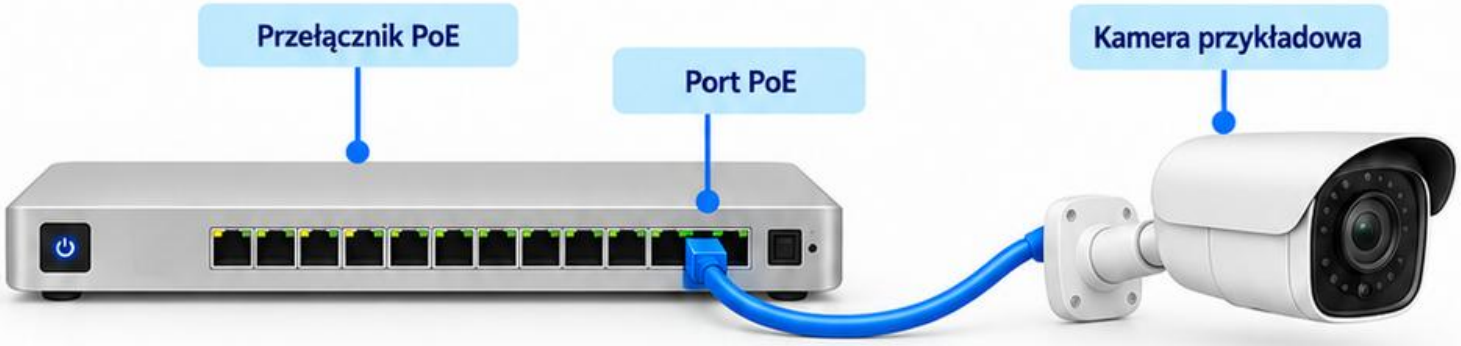
Nie włączaj PoE, gdy parametry są niezgodne.
Może to spowodować brak działania lub uszkodzenie urządzenia.

Włącz PoE po potwierdzeniu zgodności.
Upewnij się, że standard, moc portu i dostępny budżet spełniają wymagania odbiornika.

Źródła: [6]

Sprawdź pobór PoE portu

Cel: wykryć niedobór mocy zamiast zgadywać przyczynę restartów.
Gdzie: Devices > [Switch] > Ports > Port Manager.



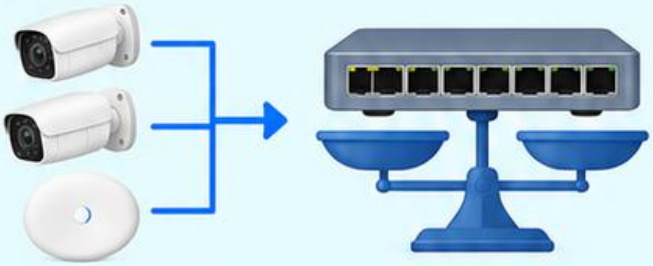
1. Odczytaj wskazania PoE

Zidentyfikuj odbiornik i odczytaj dostępne wskazania PoE. Porównaj je ze specyfikacją urządzenia oraz limitem danego portu.



2. Zestaw budżet przełącznika

Zestaw sumę odbiorników z dostępnym budżetem przełącznika. Uwzględnij urządzenia uruchamiające się jednocześnie po zaniku zasilania.



Suma odbiorników | Budżet przełącznika

3. Sprawdź specyfikację

Przykład: kamera działa w dzień, lecz restartuje się po uruchomieniu dodatkowych funkcji. Sprawdź zdarzenia z tej samej godziny.



4. Analizuj zdarzenia

Powtórz obserwację przy typowym obciążeniu. Chwilowy odczyt nie wyznacza maksymalnego zapotrzebowania; nie zwiększaj napięcia jako metody diagnostycznej.



Za mała moc powoduje restarty

Jeśli łączne zapotrzebowanie przekracza budżet lub limit portu, urządzenia mogą nie startować lub się restartować.

Dopasuj konfigurację

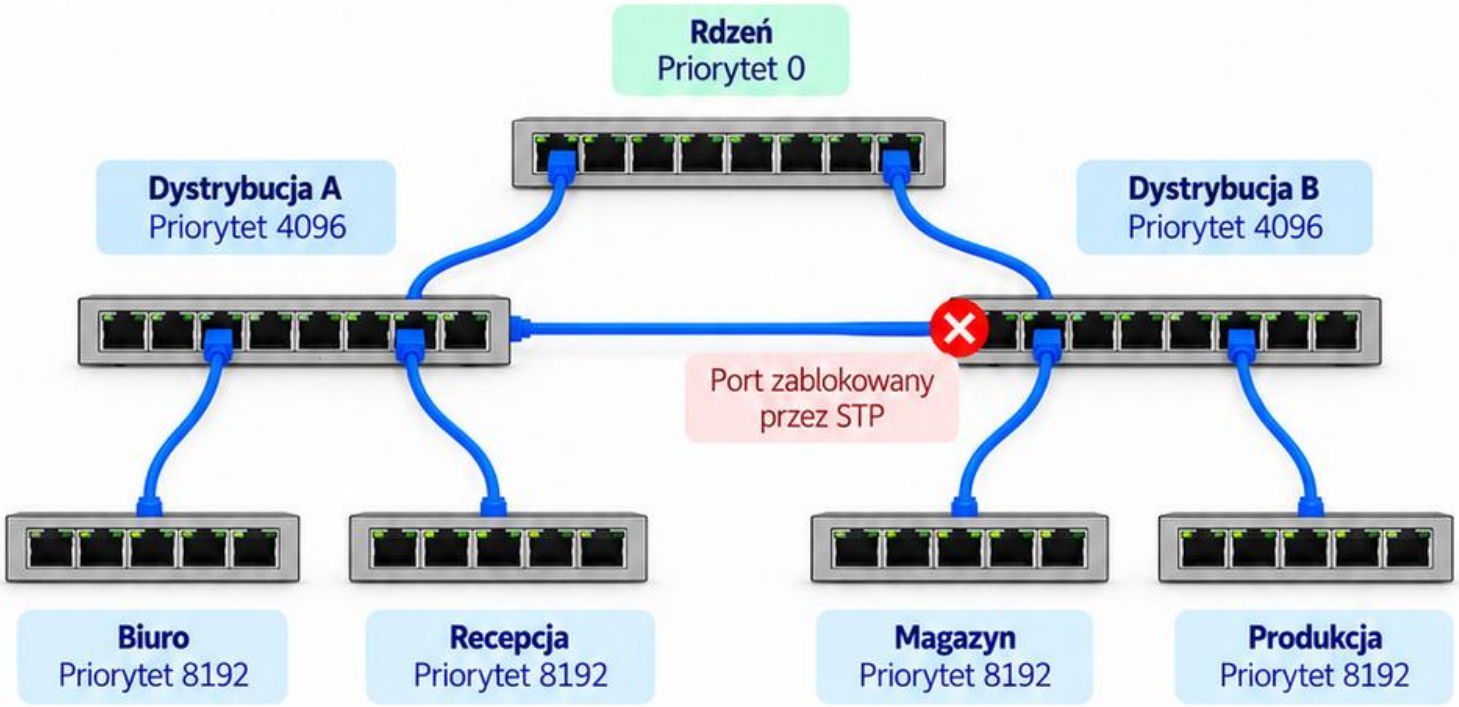
Zsumuj maksymalny pobór urządzeń i upewnij się, że mieścisz się w budżecie przełącznika oraz limitach portów.

Źródła: [6]

Ostoja · Mapa 070

Zaplanuj priorytety STP

Cel: wybrać przewidywalny korzeń topologii przełączników.
Gdzie: Devices > [Switch] > Settings > Spanning Tree.



1. Narysuj połączenia

Narysuj połączenia i wskaż przełącznik rdzeniowy. Sprawdź, które urządzenia uczestniczą w STP; porty bramy nie zastępują tej ochrony.

2. Ustaw priorytety

Przykład priorytetów: rdzeń 0, następna warstwa 4096, kolejna 8192. Niższa wartość oznacza wyższy priorytet wyboru korzenia.

Rdzeń	0
Dystrybucja A	4096
Dystrybucja B	4096
Biuro	8192
Recepcja	8192
Magazyn	8192

3. Zastosuj w menu

Gdzie: Devices > [Switch] > Settings > Spanning Tree.

4. Sprawdź wynik

Po zastosowaniu sprawdź wybrany korzeń i stan łączy nadmiarowych. Blokada zapasowej ścieżki może być prawidłowym wynikiem, a nie awarią.

5. Przykład scenariusza

Przykład: rdzeń w szafie głównej ma być korzeniem, a mały przełącznik recepcji urządzeniem podrzędnym.

Źródła: [5]

Zdiagnozuj pętlę sieciową

Cel: przerwać niekontrolowane krążenie ramek.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1. Porównaj objawy z ostatnim przepięciem przewodów.

Sprawdź blokady STP, nietypowy ruch i jednoczesne rozłączenia wielu urządzeń.



2. Zidentyfikuj nową lub nieplanowaną ścieżkę.

Odłącz podejrzany dodatkowy przewód po uzgodnieniu wpływu; zachowaj podstawowy uplink.



3. Przykład: dwa gniazda ścienne połączono krótkim przewodem w sali.

Problem dotyczy wielu klientów, choć ich kable są sprawne.



4. Sprawdź powrót stabilności i prawidłową topologię.

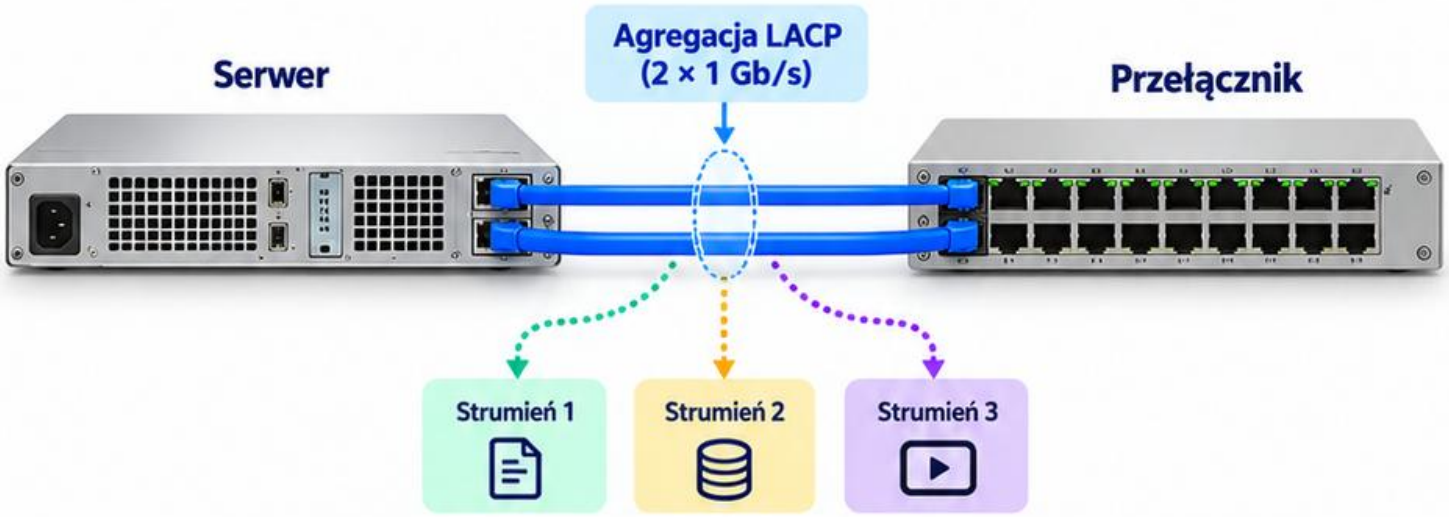
Nie wyłączaj STP, aby usunąć symbol blokady; najpierw usuń przyczynę pętli.



Źródła: [5]

Skonfiguruj zgodną agregację

Cel: zbudować uzgodnioną grupę łączy LACP.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1. Sprawdź zgodność

Sprawdź obsługę LACP po obu stronach oraz wymagania modelu i wersji dotyczące wyboru portów. Nie zakładaj zgodności wszystkich bram.



2. Zaplanuj konfigurację

Zaplanuj okno serwisowe. Przygotuj konfigurację od urządzenia podrzędnego w kierunku kontrolera, zanim dołączysz pozostałe przewody grupy.



3. Uzgodnij agregację

Przykład: serwer i przełącznik tworzą jedną grupę LACP.
Dwa niezależne porty bez zgodnej konfiguracji nie stanowią agregacji.



4. Sprawdź ruch i członkostwo

Sprawdź członkostwo grupy i ruch wielu strumieni. Jeden transfer nie musi wykorzystać sumy przepustowości wszystkich portów; zachowaj konfigurację wycofania.



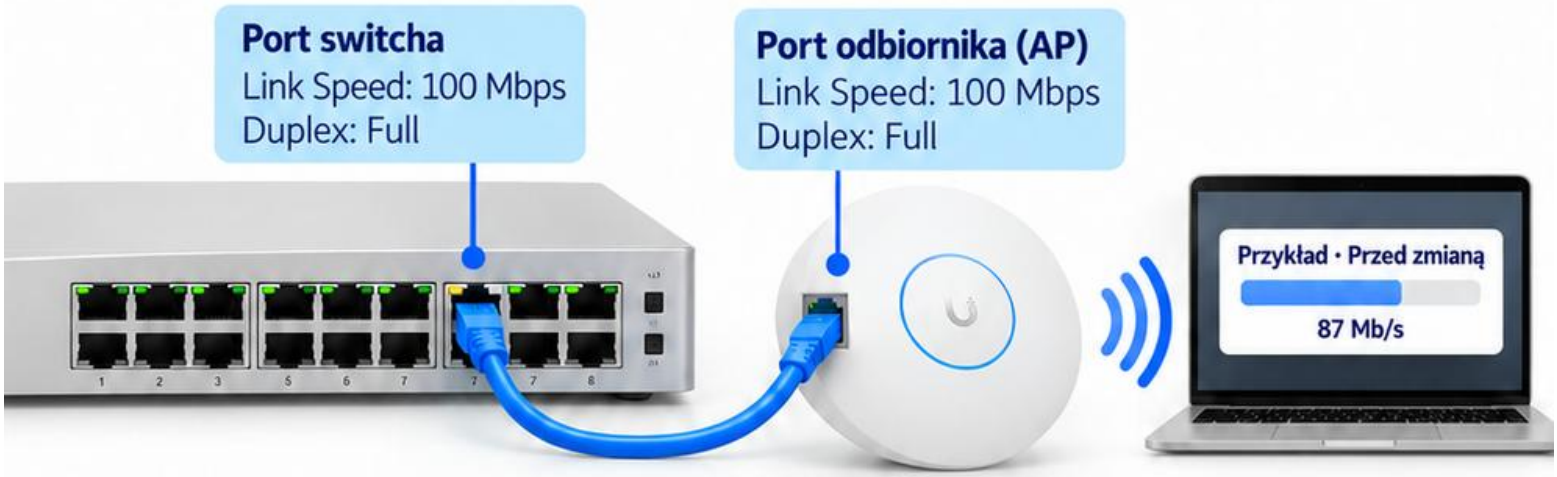
Dwa niezależne porty bez zgodnej konfiguracji nie stanowią agregacji.

Serwer i przełącznik tworzą jedną grupę LACP.

Źródła: [7]

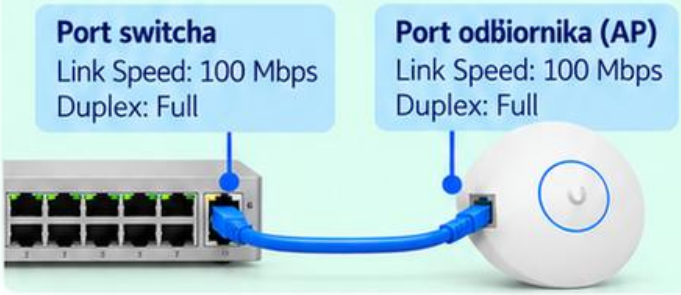
Ostoja · Mapa 073 · Sprawdź prędkość i dupleks

Cel: rozpoznać ograniczenie fizycznego łącza.
Gdzie: Devices > [Switch] > Ports > Port Manager.



1. Odczytaj parametry łącza

Odczytaj wynegocjowaną prędkość i ustawienie Link Speed. Porównaj możliwości portu, odbiornika, modułu oraz przewodu.



2. Sprawdź przewód zastępczy

Najpierw pozostaw autonegocjację i sprawdź przewód zastępczy. Wymuszenie prędkości wymaga zgodnego ustawienia i obsługi obu stron.



3. Zinterpretuj wynik

Przykład: szybki AP negocjuje wolniej po wymianie patchcordu. Test innym sprawnym przewodem odróżni problem kablowy od konfiguracji radiowej.



4. Po zmianie przetestuj

Po zmianie sprawdź ponowną negocjację, błędy i transfer lokalny. Prędkość łącza Ethernet nie jest gwarancją szybkości internetu ani Wi-Fi.



Źródła: [4]

Znajdź błędy portu

Cel: powiązać przerwy z konkretnym odcinkiem przewodowym.
Gdzie: Devices > [Switch] > Ports > Port Manager.



Przykład



1. Zapisz dane z portu

Zapisz port, czas objawu i dostępne liczniki błędów. Porównuj przyrost liczników, a nie wyłącznie ich wartość od uruchomienia.

Przed zmianą	Po zmianie
	

2. Sprawdź przewód

Sprawdź wtyki i wymień pojedynczy patchcord na sprawdzony. Następnie porównaj zachowanie przy podobnym ruchu oraz po obu stronach łącza.



3. Przykład z praktyki

Przykład: przerwy dotyczą jednego AP i pokrywają się z ponowną negocjacją uplinku. Zmiana kanału radiowego nie naprawi uszkodzonego przewodu.

4. Zweryfikuj rezultat

Potwierdź brak dalszego przyrostu błędów podczas testu. Jeśli objaw wraca, sprawdź stałe okablowanie i zgodność wkładek, zamiast restartować cały obiekt.





Źródła: [4]

Zweryfikuj drogę VLAN-u

Cel: sprawdzić pełny tor od klienta do jego bramy.
Gdzie: Devices > [Switch] > Ports > Port Manager oraz Settings > Networks.



1. Sprawdź port klienta

Zacznij od portu klienta i jego Native VLAN. Na każdym uplinku sprawdź, czy wymagany tag jest dopuszczony po obu stronach.



2. Sprawdź pierwszy uplink

Zapisz kolejne urządzenia i wynik każdego odcinka. Na końcu potwierdź sieć bramy, DHCP oraz oczekiwaną politykę dostępu.



3. Sprawdź drugi uplink

Na drugim końcu upewnij się, że ten sam tag VLAN 30 jest dopuszczony. Oba końce uplinku muszą mieć zgodną listę dozwolonych VLAN-ów.



4. Sprawdź bramę i usługi

Odnów adres i sprawdź bramę oraz usługę docelową. Nie dodawaj wszystkich VLAN-ów na wszystkich portach jako trwałego rozwiązania diagnostycznego.



5. Zinterpretuj wynik

Przykład: laptop działa na rdzeniu, lecz nie na piętrze. Różnica wskazuje odcinek między przełącznikami, a nie automatycznie serwer DHCP.



Źródła: [1]

Moduł 6. Wi-Fi

1 Dobre Wi-Fi zaczyna się od wymagań klientów i pomiaru miejsca. Sama liczba punktów dostępowych nie opisuje jakości usługi.



Wymagania klientów

Pomiar miejsca

2 Oddziel trzy pytania: czy klient widzi SSID, czy potrafi się uwierzytelnić i czy po połączeniu otrzymuje właściwą konfigurację IP.



Czy klient widzi SSID?

Czy potrafi się uwierzytelnić?

Czy otrzymuje właściwą konfigurację IP?

3 Pracuj etapami: przygotuj sieć, wybierz zabezpieczenia, ogranicz nadawanie do odpowiednich AP, a następnie oceń radio w rzeczywistych warunkach.



Przygotuj sieć

Wybierz zabezpieczenia

Ogranicz nadawanie do odpowiednich AP

Oceń radio w rzeczywistych warunkach

4 Przykład: czujnik magazynowy i nowy laptop mogą potrzebować innych pasm oraz ustawień bezpieczeństwa. Sprawdź oba, zamiast zakładać wspólną zgodność.



Czujnik magazynowy

Nowy laptop

5 Kanał, szerokość i moc wymagają oceny otoczenia, kraju instalacji oraz obciążenia. Nie przenoś gotowego zestawu wartości między budynkami.



Kanał

Szerokość

Moc

Otoczenie, kraj instalacji i obciążenie

6 Wynik zapisuj dla konkretnego klienta, miejsca i godziny. Powtarzalna próba aplikacji daje więcej informacji niż pojedynczy pomiar maksymalnej prędkości.



Klient

Miejsce

Godzina

Powtarzalna próba aplikacji

Źródła: [33], [19]

Ostoja · Mapa 076 · Utwórz firmowe SSID

Cel: uruchomić rozpoznawalną sieć pracowników.

Gdzie: Settings > WiFi.

Wybierz nazwę, docelową sieć oraz sposób uwierzytelniania zgodny z wymaganiami organizacji. Sprawdź możliwości klientów przed zmianą zabezpieczeń.

Utwórz SSID i przypisz odpowiednie AP. Dane uwierzytelniające przekaż zatwierdzonym kanałem, a w dokumentacji zachowaj jedynie odwołanie.



Przykład: firma używa nazwy Ostoja-Praca. Laptop testowy powinien otrzymać adres z sieci pracowników, a nie z sieci gościnnej.

Przetestuj połączenie, adres, DNS i aplikację służbową. Powtórz próbę po rozłączeniu; zapisany profil klienta może maskować błędne nowe ustawienia.

Próba odbiorowa: nowy laptop łączy się z Ostoja-Praca, otrzymuje adres Firmy i otwiera aplikację. Po rozłączeniu powtarza logowanie bez starego profilu.

Źródła: [33]

Połącz SSID z właściwą siecią

Cel: klient sieci Firma trafia do VLAN 10.



1. Przygotuj VLAN

Utwórz sieć Firma z bramą 192.168.10.1/24 i działającym DHCP.

2. Utwórz Wi-Fi

Otwórz ustawienia Wi-Fi. Dodaj SSID Firma i wybierz sieć Firma.

3. Wybierz punkty dostępowe

Wskaż AP-y, które mają rozgłaszać ten SSID.

4. Sprawdź całą ścieżkę

Port AP i wszystkie uplinki muszą przenosić VLAN 10.

5. Zastosuj zabezpieczenia

Dobierz WPA2/WPA3 do klientów.
Zapisz ustawienia i połącz urządzenie testowe.

Wynik prawidłowy

SSID Firma | IP 192.168.10.58 | brama 192.168.10.1

Wynik nieprawidłowy

Adres z innej podsieci: sprawdź przypisanie SSID, porty i DHCP.

Przypisanie VLAN-u nie zastępuje reguł firewalla.

Schemat przykładowy | Źródła: [1], [2]

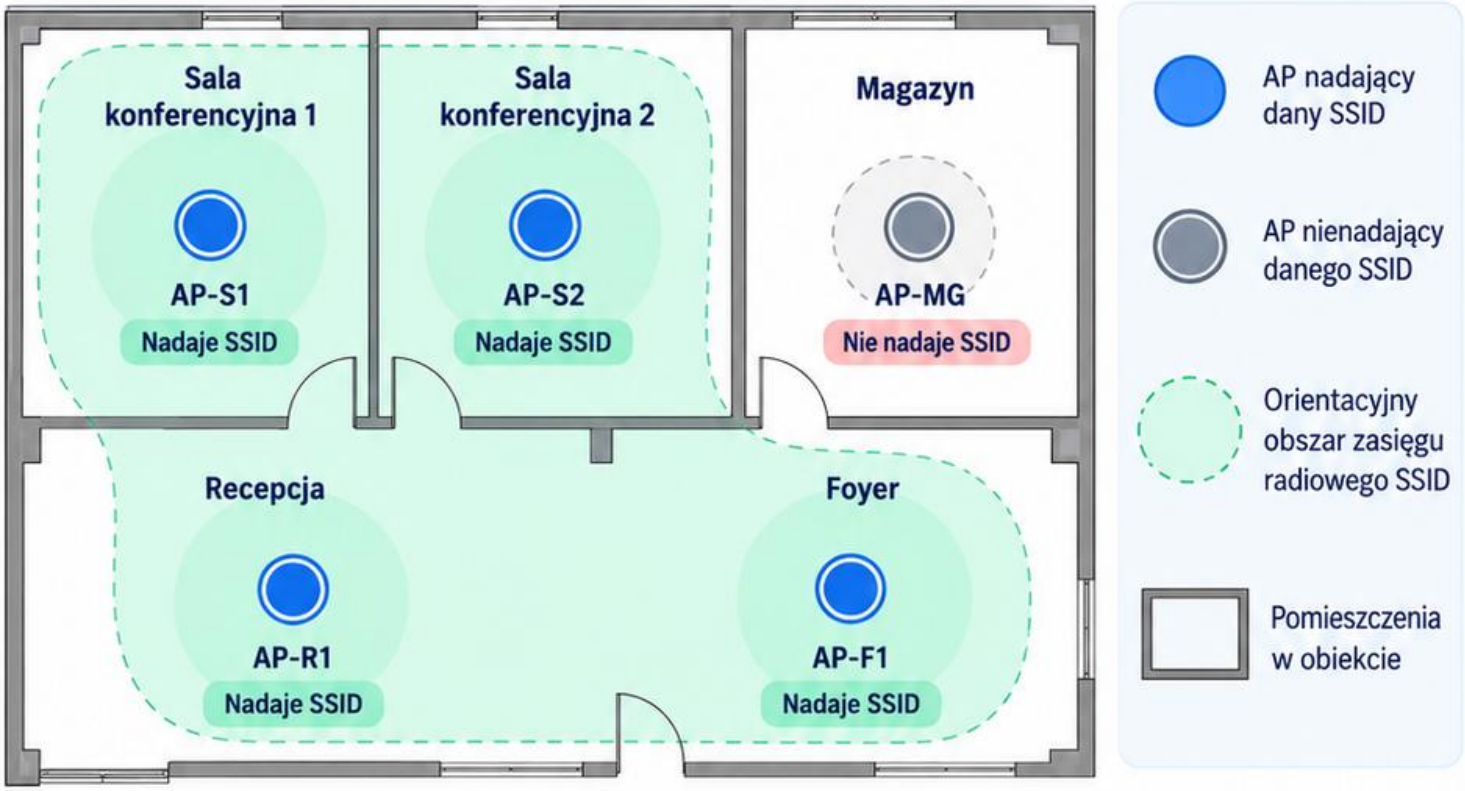
Ostoja · Mapa 078 · Wybierz AP nadające SSID

Cel: ograniczyć zasięg usługi do właściwej części obiektu.

Gdzie: Settings > WiFi > [SSID] > Broadcasting APs.

Zidentyfikuj punkty dostępowe według nazw i lokalizacji. Wybierz Specific lub Groups, jeśli nie wszystkie AP mają świadczyć daną usługę.

Sprawdź, czy każdy wybrany AP ma działającą drogę do sieci SSID.
Przy mesh uwzględnij jego uplink; grupa nie naprawia brakującego VLAN-u.



Przykład: sieć konferencyjna jest dostępna w salach i foyer.
AP magazynowy nie musi jej nadawać, choć należy do tego samego kontrolera.

Obejdź granice planowanego obszaru i sprawdź widoczność SSID.
Grupa nadawania nie tworzy precyzyjnej fizycznej granicy sygnału radiowego.

Przykład zasięgu rozgłaszania: wybierz grupę Recepcja zamiast All.
Przy AP spoza grupy sprawdź jego listę WLAN; sam telefon może słyszeć sąsiedni AP.

Źródła: [33], [24]

Ostoja · Mapa 079 · Dobierz zgodne zabezpieczenia

Cel: zachować ochronę przy rzeczywistej zgodności urządzeń.

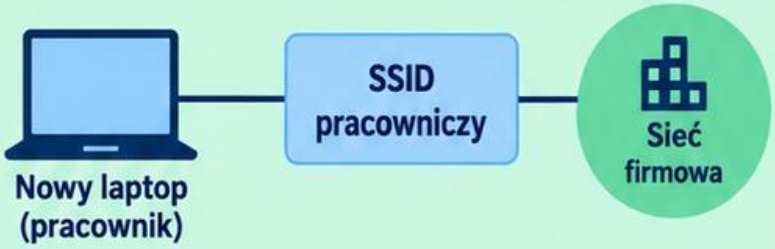
Gdzie: Settings > WiFi > [SSID].

Sporządź listę wymaganych klientów i obsługiwanych metod. Sprawdź, czy **organizacja** korzysta z hasła współdzielonego, czy infrastruktury uwierzytelniania przedsiębiorstwa.

Zmieniaj zabezpieczenia **na testowym SSID** lub w oknie serwisowym. Nie obniżaj ochrony całej firmy z powodu jednego starego odbiornika.

Przykład: starszy terminal działa **wyłącznie** w osobnej, ograniczonej sieci. Nowe komputery pozostają przy polityce przewidzianej dla pracowników.

Sieć pracownicza (nowoczesne zabezpieczenia)



Oddzielna sieć dla starszego urządzenia (ograniczona)



Zgodność i polityka zabezpieczeń (przykład)

Urządzenie	Obsługiwane metody	Przypisany SSID	Dostęp do zasobów
Nowy laptop (pracownik)	Zgodne z polityką pracowniczą	SSID pracowniczy	Sieć firmowa
Najstarszy terminal	Starsze metody (ograniczona zgodność)	SSID dla terminala	Ograniczony dostęp

Sprawdź nowe i istniejące profile klientów. Udana autoryzacja nie dowodzi prawidłowego VLAN-u ani ograniczeń dostępu; te elementy przetestuj osobno.

Porównaj dwa urządzenia: nowy laptop oraz najstarszy wspierany terminal. Jeżeli terminal zawodzi, odizoluj jego wariant SSID zamiast obniżać zabezpieczenia wszystkich pracowników.

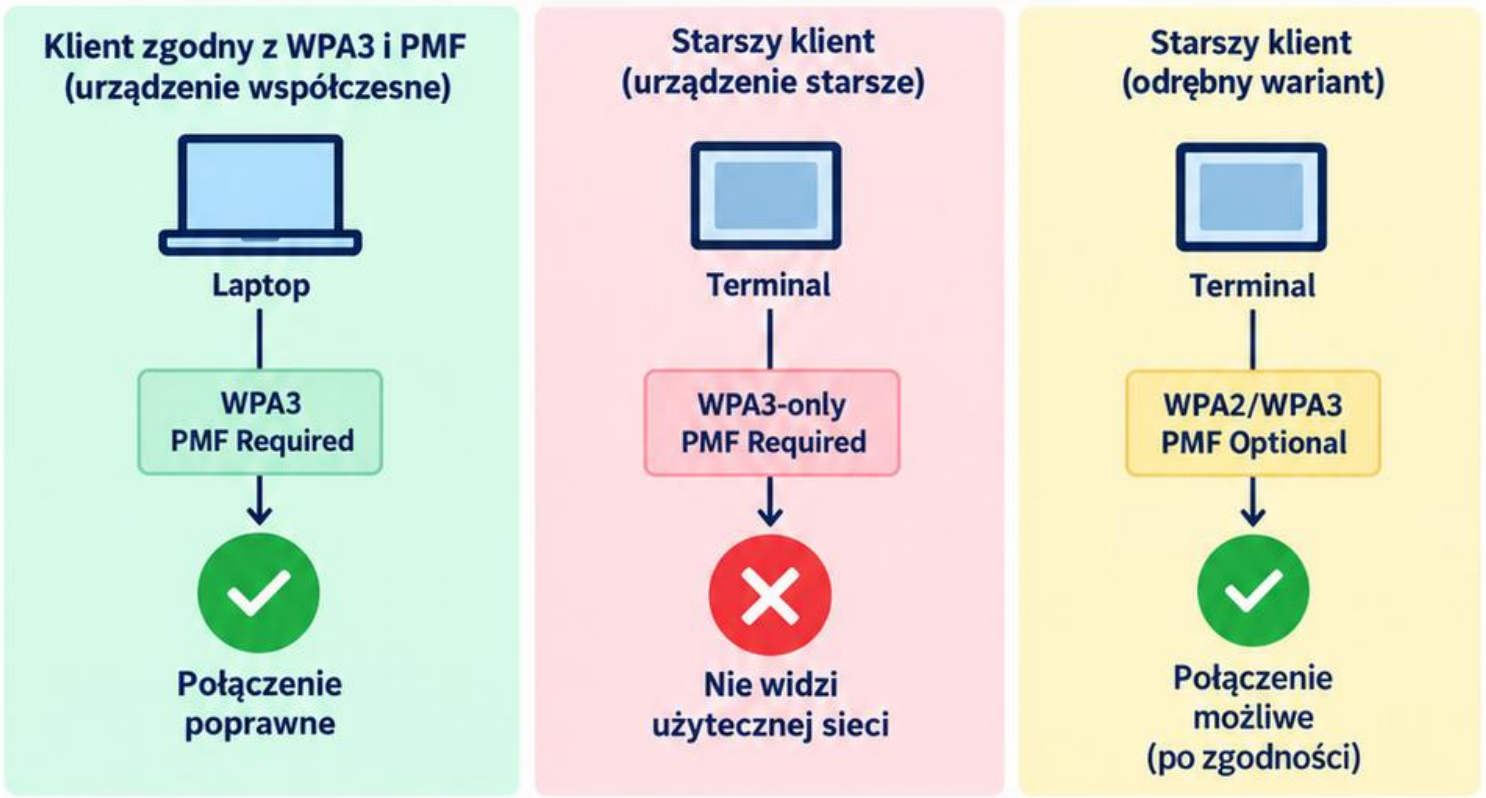
Źródła: [33]

Ostoja · Mapa 080 · Zaplanuj WPA3 i PMF

Cel:
wprowadzić ochronę ramek zarządzających bez nieprzewidzianych wykluczeń.

Gdzie:
Settings > WiFi > [SSID].

WPA3-only wymaga PMF Required.
Dla starszych klientów osobno przetestuj WPA2/WPA3 z PMF Optional; tryb przejściowy nie gwarantuje zgodności.



Przygotuj próbę z reprezentatywnymi urządzeniami.
Zapisz działającą konfigurację, zanim przełączysz wymagania zabezpieczeń na produkcyjnym SSID.

Przykład: laptop łączy się poprawnie, lecz terminal przestaje widzieć użyteczną sieć.
Sprawdź zgodność terminala, zanim zmienisz radio.

Powtórz połączenie po usunięciu starego profilu testowego.
Nie traktuj trybu przejściowego jako gwarancji zgodności każdego urządzenia i każdego pasma.

Test PMF: sprawdź nowe połączenie klienta WPA3 przy Required oraz starszego klienta na odrębnym wariancie.
Zapisz rzeczywiście wynegocjowaną ochronę, nie samą nazwę SSID.

Źródła: [33]

Ostoja · Mapa 081 · Utwórz SSID dla IoT

1 Cel

przyłączyć urządzenia techniczne z ograniczonym zakresem dostępu.

2 Gdzie

Settings > WiFi oraz Settings > Networks.

3 Planowanie

Ustal wymagania producenta: pasmo, zabezpieczenia, dostęp do usług lokalnych i chmurowych. Przygotuj odrębny segment z określoną polityką.

- pasmo
- zabezpieczenia
- usługi lokalne
- ustugi chmurowe

4 Przypisz SSID

Przypisz SSID do sieci IoT. Funkcje ułatwiające zgodność uruchamiaj dopiero po wykazaniu potrzeby, zamiast zmieniać wszystkie parametry naraz.

SSID IoT

5 Przykład

czujnik potrzebuje serwera czasu i usługi producenta, ale nie panelu administracyjnego. Zapisz wymagane połączenia przed tworzeniem wyjątków.



6 Testowanie

Sprawdź pierwszą konfigurację i ponowne połączenie po restarcie. Jeżeli aplikacja nie wykrywa urządzenia, oddziel odkrywanie usług od właściwego przesyłania danych.

Próba IoT: odłącz zasilanie jednego czujnika, uruchom ponownie i sprawdź DHCP oraz aplikację. Przetestuj jego rzeczywiste pasmo, na przykład wyłącznie 2,4 GHz.

- restart
- DHCP
- aplikacja
- pasmo 2,4 GHz

Źródła: [33]

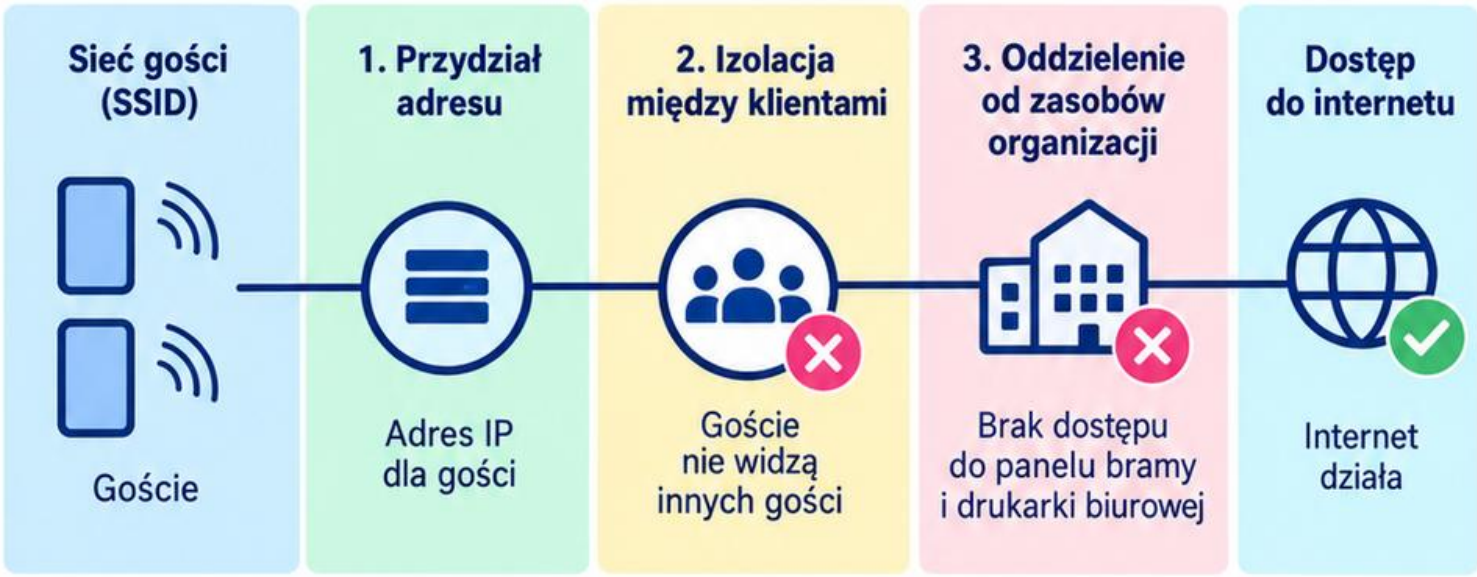
Ostoja · Mapa 082 · Utwórz SSID gości

Cel:
udostępnić internet
z oddzieleniem
od zasobów organizacji.

Gdzie:
Settings > WiFi
oraz Settings > Networks.

Najpierw przygotuj sieć gości i przypisz do niej SSID.
Zdecyduj oddzielnie o izolacji między sieciami
oraz między klientami.

Portal włącz tylko wtedy, gdy wymaga go sposób obsługi gości.
Ekran powitalny nie zastępuje sprawdzenia polityk dostępu.



Przykład: klient kawiarni korzysta z internetu, ale nie otwiera panelu bramy ani drukarki biurowej. Jego telefon nie powinien widzieć innych gości.

Przetestuj internet oraz próby zabronione, także z różnych AP.
Client Device Isolation na AP nie potwierdza izolacji całego segmentu.

Odbiór gości: dwa własne telefony, najpierw jeden AP, potem różne AP.
Internet ma działać, a znana usługa drugiego telefonu pozostać niedostępna.

Źródła: [34]

Ostoja · Mapa 083 · Dobierz pasma do klientów

Cel: udostępnić pasma obsługiwane przez rzeczywiste odbiorniki.

Gdzie: Settings > WiFi > [SSID] > WiFi Band.

Porównaj obsługę pasm przez AP i klienta. Uwzględnij miejsce pracy, przeszkody oraz wymagania urządzeń korzystających tylko z wybranego pasma.

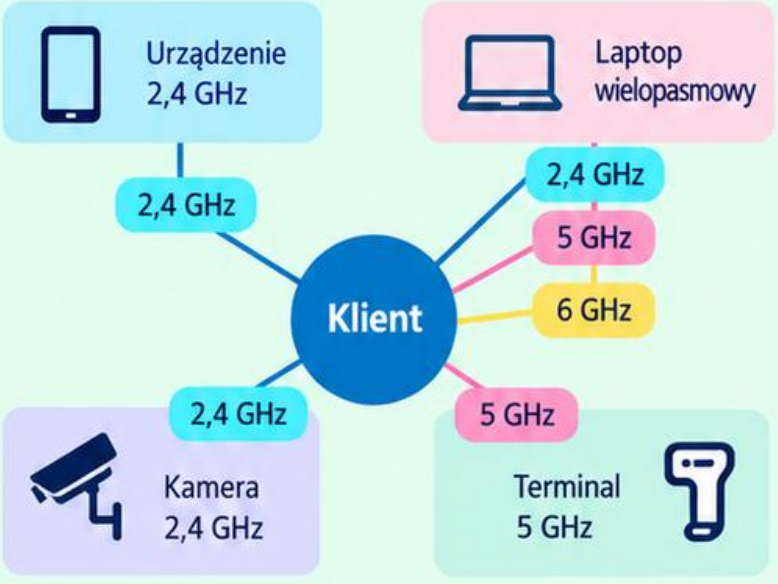
Przygotuj próbę z typowymi urządzeniami w ich normalnych lokalizacjach. Oceniaj stabilność i działanie aplikacji, nie samą nazwę standardu.

Przykład: terminal na zapleczu korzysta z innego pasma niż laptop w sali. Rozwiązanie powinno odpowiadać obu wymaganiom, bez wymuszania pozornej nowoczesności.

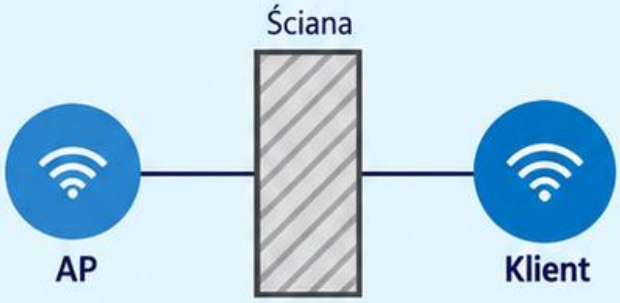
Sprawdź wybrane pasmo po ponownym połączeniu. Zmiana preferencji nie gwarantuje, że każdy klient wybierze ten sam AP lub częstotliwość.

Próba pasm: urządzenie 2,4 GHz i laptop wielopasmowy łączą się osobno. Zapisz faktyczne pasmo; pozostaw pasmo pomocnicze ułatwiające wykrywanie sieci 6 GHz.

Obsługa pasm przez klientów



Wpływ przeszkód na sygnał



Przeszkody, takie jak ściany, osłabiają sygnał. Uwzględnij miejsce pracy klientów przy doborze pasma.

Źródła: [33]

Ostoja · Mapa 084 · Zaplanuj kanały 2,4 GHz

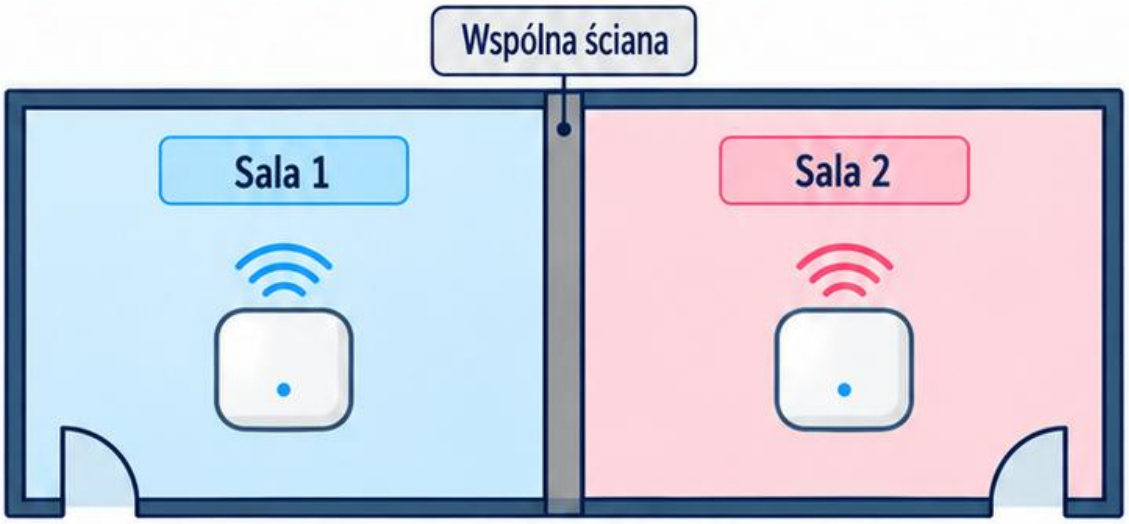
Cel: ograniczyć nakładanie kanałów w konkretnym otoczeniu.

Gdzie: Radios > AirView oraz ustawienia radiowe wybranego AP.

Sprawdź kraj instalacji i **dostępne kanały**. Zmierz zajętość oraz sąsiednie sieci w miejscach pracy klientów, nie tylko przy szafie.

Dla 2,4 GHz zacznij od 20 MHz. Rozplanuj sąsiednie AP na podstawie dostępnych kanałów i pomiaru; testuj także urządzenia wymagające tego pasma.

Przykład: dwie sale mają wspólną ścianę i silne sygnały obu AP. Wspólny kanał może powodować współdzielenie czasu antenowego.



Przydział kanałów na podstawie pomiaru.

Porównaj retransmisje i czas odpowiedzi przy podobnym obciążeniu.
Nie zmieniaj całego obiektu po jednym skanie wykonanym poza godzinami pracy.

Przykład planu 20 MHz: sprawdź kanały 1, 6 i 11 dostępne dla Polski.
To punkt startowy; o przydziale sąsiadujących AP decyduje pomiar.

Źródła: [19], [30]

Ostoja · Mapa 085 · Zaplanuj kanały 5 GHz

Cel: dobrać kanały do zakłóceń i wymagań ciągłości.

Gdzie: Radios > AirView oraz ustawienia radiowe wybranego AP.

Zapisz sąsiednie kanały i szerokości. Sprawdź dostępność kanałów zależną od kraju oraz wymagania DFS i zgodność klientów.

Dla zatłoczonego biura rozważ 40 MHz jako punkt wyjścia. Przed użyciem DFS uwzględnij zgodność klientów i zmianę kanału po wykryciu radaru.

Przykład: sala do rozmów wideo wymaga stabilności podczas pracy. Kanał pozornie pusty nie jest automatycznie najlepszym wyborem dla tej usługi.

Dobór kanału 5 GHz

- Kraj instalacji
- Zgodność klientów
- Wymagania DFS

Zdarzenie DFS – przebieg czasowy



Zapisz kanał faktycznie używany po zastosowaniu. Powtórz test po zmianie i obserwuj zdarzenia; nie przypisuj każdej przerwy słabemu sygnałowi.

Test stabilności: uruchom rozmowę wideo i sprawdź zdarzenia zmiany kanału. Nie wymuszaj radaru; przy ograniczeniach DFS porównaj zatwierdzony kanał bez DFS.

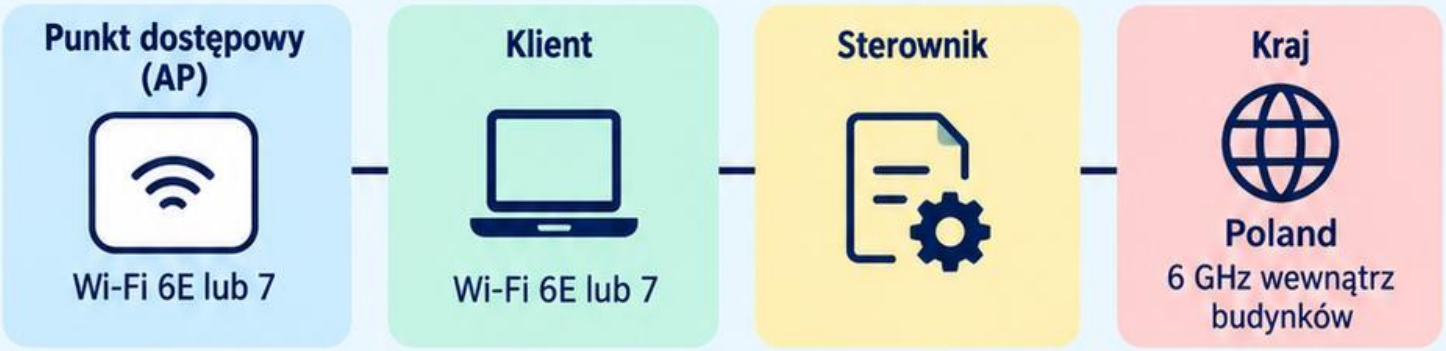
Źródła: [19], [30]

Ostoja · Mapa 086 · Zweryfikuj wymagania 6 GHz

Cel: potwierdzić pełną zgodność przed uruchomieniem nowego pasma.

Gdzie: Settings > WiFi > [SSID] oraz ustawienia wybranego AP.

Sprawdź AP i klienta Wi-Fi 6E lub 7, sterownik oraz kraj Poland.
Dla Polski tabela Ubiquiti wskazuje 6 GHz wewnątrz budynków.



Dla 6 GHz potwierdź **WPA3** albo **OWE** i wymaganą ochronę **PMF**.
Wielopasmowe SSID może ułatwiać wykrywanie; starsze urządzenia przetestuj osobno.

Przykład: nowy AP obsługuje 6 GHz, ale starszy laptop nie.
Brak tego pasma na laptopie nie dowodzi awarii AP.



Przetestuj wykrywanie sieci, uwierzytelnianie i stabilność w miejscu pracy.
Nie zakładaj, że nazwa Wi-Fi 6 oznacza obsługę 6 GHz.

Próba 6 GHz: klient Wi-Fi 6E potwierdza pasmo w szczegółach połączenia.
Starszy laptop korzysta z 5 GHz tego SSID albo osobnej zgodnej sieci.



Klient Wi-Fi 6E potwierdza pasmo w szczegółach połączenia.

Starszy laptop korzysta z 5 GHz tego SSID albo osobnej zgodnej sieci.

Źródła: [33], [21], [35]

Ostoja · Mapa 087 · Dopasuj szerokość kanału

Cel: zrównoważyć przepustowość i współdzielenie widma.

Gdzie: Radios lub Devices > [AP] > Settings.

Zapisz obecną szerokość, zakłócenia i wymagania aplikacji. Szerszy kanał zajmuje więcej widma i może zwiększać konkurencję z sąsiadami.

Zmień jedną szerokość na wybranym radiu. Porównaj ten sam zestaw klientów, tę samą trasę pomiarową i podobne obciążenie.

Przykład: większa szerokość poprawia pojedynczy transfer nocą, ale pogarsza rozmowy w zatłoczonym biurze. Oceniaj warunki faktycznego użytkowania.

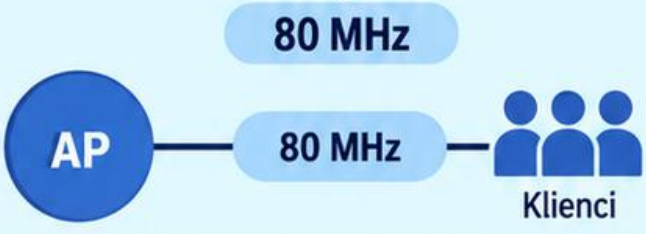
Zachowaj wariant spełniający wymagania usługi. Jeśli retransmisje lub opóźnienia rosną, wróć do poprzedniego ustawienia i udokumentuj porównanie.

Węższy kanał



- \+ Mniejsze zajmowanie widma.
- \+ Mniejsza konkurencja z sąsiadami.
- − Niższy pojedynczy transfer w porównaniu z szerszym kanałem.

Szerszy kanał



- \+ Wyższy pojedynczy transfer w sprzyjających warunkach (np. nocą).
- − Większe zajmowanie widma.
- − Większa konkurencja z sąsiadami.
- − Może pogarszać rozmowy w zatłoczonym biurze.

Przykład biurowy: porównaj 40 i 80 MHz w 5 GHz przy kilku aktywnych klientach. Wybierz wariant zapewniający rozmowy bez pogorszenia, nie najwyższy pojedynczy transfer.

Źródła: [19]

Ostoja • Mapa 088 • Dostosuj moc na podstawie pomiaru

Cel: poprawić pokrycie bez tworzenia niepotrzebnych nakładających się komórek.

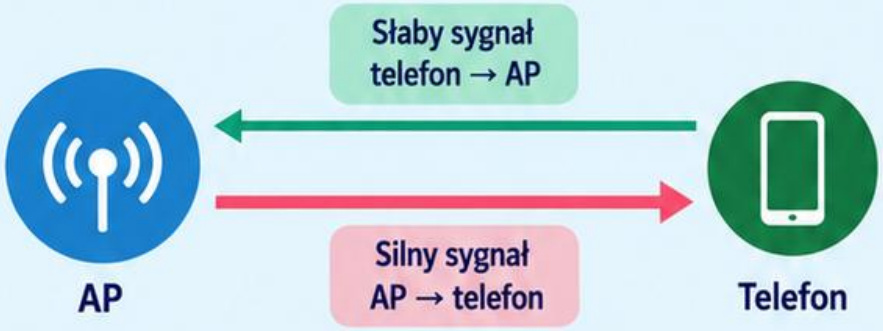
Gdzie: Devices > [AP] > Settings oraz Radios.

Zmierz sygnał i zachowanie klienta w miejscach pracy. Oceń oba kierunki komunikacji; silny sygnał AP nie zwiększa mocy nadajnika telefonu.

Zmieniaj moc wybranego radia stopniowo. Po każdej zmianie sprawdź granice komórki, retransmisje i przechodzenie do sąsiedniego AP.

Asymetryczna komunikacja – przykład

Przykład: telefon słyszy daleki AP, lecz AP słabo słyszy telefon. Dalsze zwiększanie mocy AP może nie usunąć asymetrii.



Skutki w pokryciu



Powtórz trasę z tym samym klientem. Jeśli brakuje pokrycia przez przeszkody, rozważ położenie AP zamiast uniwersalnego ustawienia maksymalnej mocy.



Próba mocy: w jednym radiu porównaj Medium z poprzednią wartością. Zapisz sygnał przy biurku i drzwiach; pogorszenie rozmowy oznacza cofnięcie zmiany.



Źródła: [19]

Ostoja · Mapa 089 · Oceń przechodzenie między AP

Cel:
sprawdzić ciągłość usługi podczas ruchu klienta.

Gdzie:
Clients oraz
Settings > WiFi > [SSID].

Przygotuj stałą trasę między AP i reprezentatywny telefon. Uruchom aplikację wrażliwą na przerwę oraz obserwację połączenia klienta.

Zapisz zmianę AP, pasma i moment utraty usługi. Sprawdź pokrycie oraz zgodność opcji roamingu przed ich modyfikacją.



Przykład: pracownik przechodzi z recepcji do sali. Problem występujący zawsze przy drzwiach może oznaczać lukę pokrycia lub zbyt nakładające się komórki.

Powtórz trasę w obu kierunkach. Decyzję o zmianie AP podejmuje klient; włączenie Fast Roaming nie zastępuje prawidłowego projektu radiowego.

Próba ruchowa: przejdź recepcja–sala i z powrotem podczas tej samej rozmowy. Zapisz AP przed przejściem, AP po nim i moment przerwy.

Źródła: [33]

Ostoja · Mapa 090 · Zweryfikuj połączenie i DHCP Wi-Fi

Cel: oddzielić uwierzytelnienie od otrzymania adresu.

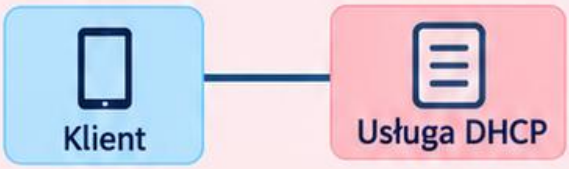
Gdzie: Clients oraz Settings > WiFi i Settings > Networks.

1 Połączenie Wi-Fi



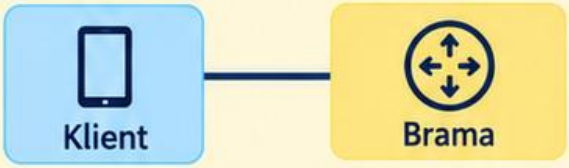
Sprawdź, czy klient jest połączony z oczekiwanym SSID i AP. Następnie odczytaj jego adres, maskę, bramę oraz DNS.

2 Dzierżawa DHCP



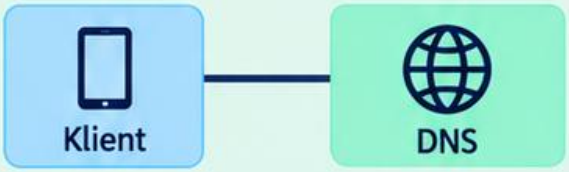
Jeśli nie ma poprawnej dzierżawy, prześledź przypisanie sieci SSID i VLAN na uplinku AP. Nie zaczynaj od zmiany kanałów.

3 Brama domyślna



Przykład: telefon pokazuje połączenie Wi-Fi, lecz nie otrzymuje adresu z sieci Goście. Uwierzytelnianie działa, ale ścieżka usługi DHCP wymaga kontroli.

4 Rozwiązywanie nazw



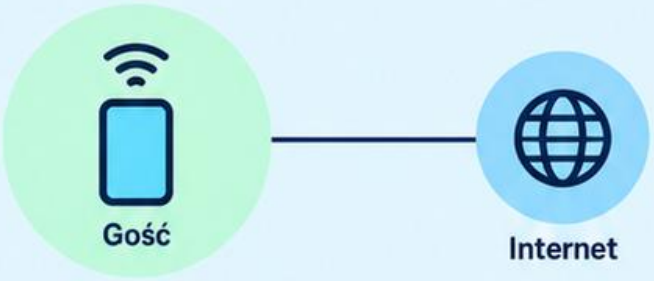
Po poprawce odnów połączenie i sprawdź bramę oraz nazwę internetową. Testuj też drugi model klienta, aby oddzielić profil urządzenia od problemu infrastruktury.

Próba DHCP: po usunięciu profilu testowego połącz klienta ponownie. Adres z innej podsieci oznacza błąd przypisania; brak dzierżawy wymaga sprawdzenia transportu VLAN-u.

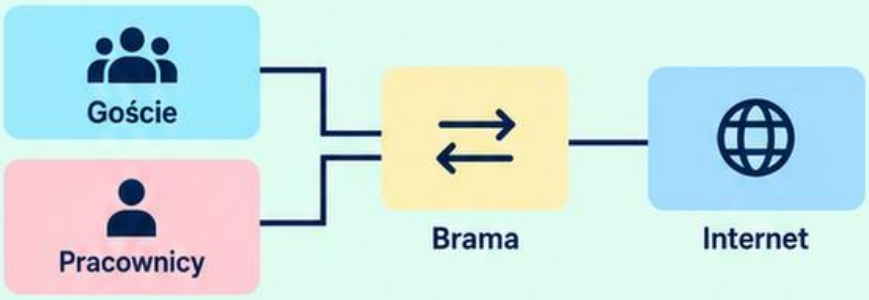
Źródła: [1], [12]

Moduł 7. Goście i izolacja

Sieć gościnna ma umożliwić wygodne korzystanie z internetu i ograniczyć dostęp do cudzych urządzeń. Te zadania wymagają osobnych testów.



Najpierw rozdziel ruch na sieci, potem zaplanuj komunikację między segmentami. Następnie sprawdź komunikację gości wewnątrz ich własnego segmentu.



Izolacja klientów na AP, izolacja sieci na bramie i ACL przełącznika działają w różnych miejscach. Jedno ustawienie nie potwierdza wszystkich granic.



Przykład: hotel pozwala gościom otwierać strony internetowe, lecz blokuje dostęp do recepcji. Dwa telefony gości również wymagają sprawdzenia wzajemnej osiągalności.



Portal służy obsłudze wejścia do usługi. Limity pasma, harmonogram i vouchery dobieraj do faktycznego sposobu korzystania.



Zakończ testem całej wizyty: nowe połączenie, adres, portal, internet, próby zabronione i ponowne połączenie po zakończeniu uprawnienia.

Źródła: [20], [36]

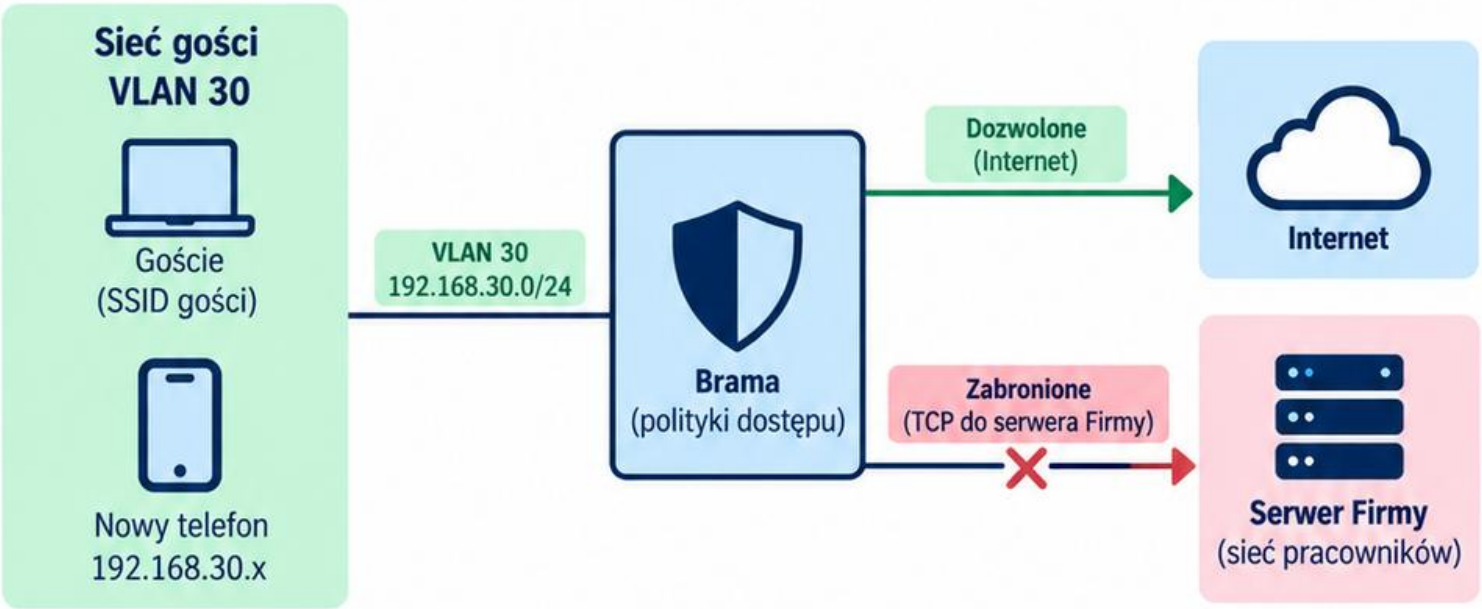
Ostoja · Mapa 091 · Oddziel sieć odwiedzających

Cel:
nadać gościom własny segment i przewidywalną politykę.

Gdzie:
Settings > Networks oraz Settings > WiFi.

Utwórz sieć o niekolidującej adresacji. Zapewnij usługę DHCP i przypisz SSID do tej właśnie sieci, a nie tylko do podobnej nazwy.

Sprawdź drogę VLAN-u od AP do bramy. Następnie ustal, które usługi goście mogą osiągać i co ma być zabronione.



Przykład: sala szkoleniowa ma własną sieć gości, natomiast komputery organizatora pozostają w sieci pracowników. Nazwy SSID nie stanowią granicy bezpieczeństwa.

Przetestuj: adres klienta oraz próbę dostępu do zasobu pracowników. Oddzielny VLAN nie dowodzi blokady routingu między sieciami.

Przykład projektu: Goście VLAN 30, 192.168.30.0/24. Nowy telefon otrzymuje 192.168.30.x; próba TCP do serwera Firmy ma być blokowana, internet działa.

Źródła: [34]

Ostoja · Mapa 092 · Izoluj klientów SSID

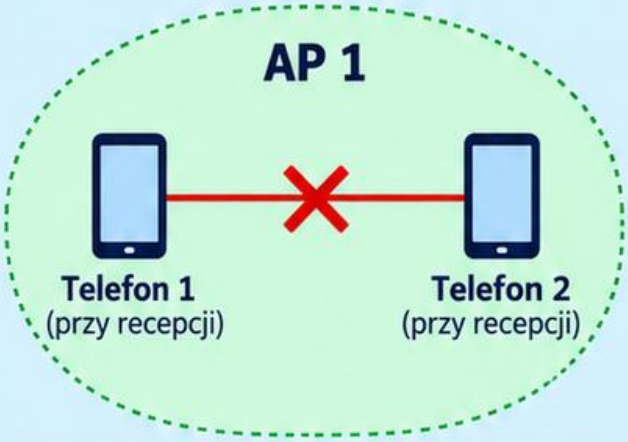
Cel: ograniczyć bezpośrednią komunikację klientów na tym samym AP.

Gdzie: Settings > WiFi > [SSID] > Client Device Isolation.

Włącz ustawienie dla wybranego SSID. Zanotuj, że ta ochrona dotyczy klientów obsługiwanych przez ten sam punkt dostępowy.

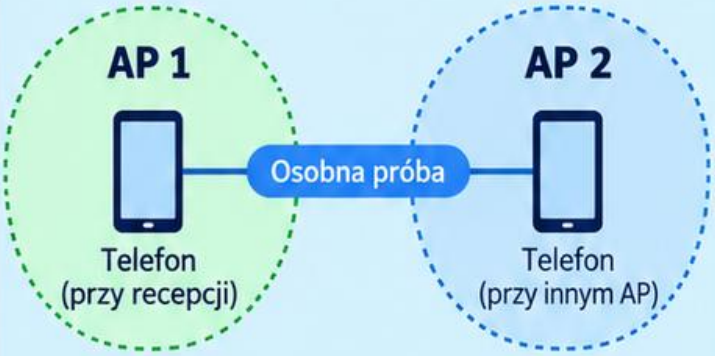
Zaplanuj dodatkowe zabezpieczenia dla innych ścieżek: między AP, do klientów przewodowych oraz między sieciami. Sprawdź zgodność sprzętu z ACL.

Izolacja na tym samym AP



Brak bezpośredniej komunikacji między klientami na tym samym AP.

Osobna ścieżka między AP



Telefon przy innym AP wymaga osobnej próby.

Przykład: dwa telefony przy recepcji nie powinny łączyć się ze sobą. Telefon przy innym AP wymaga osobnej próby.

Testuj znaną usługę na kontrolowanym odbiorniku. Nie oceniaj całego segmentu na podstawie samego braku odpowiedzi ping jednego telefonu.

Test rozstrzygający: najpierw uruchom znaną usługę między własnymi klientami bez izolacji. Włącz izolację i ponów identyczną próbę na tym samym AP.

Źródła: [20]

Ostoja · Mapa 093 · Zastosuj izolację sieci

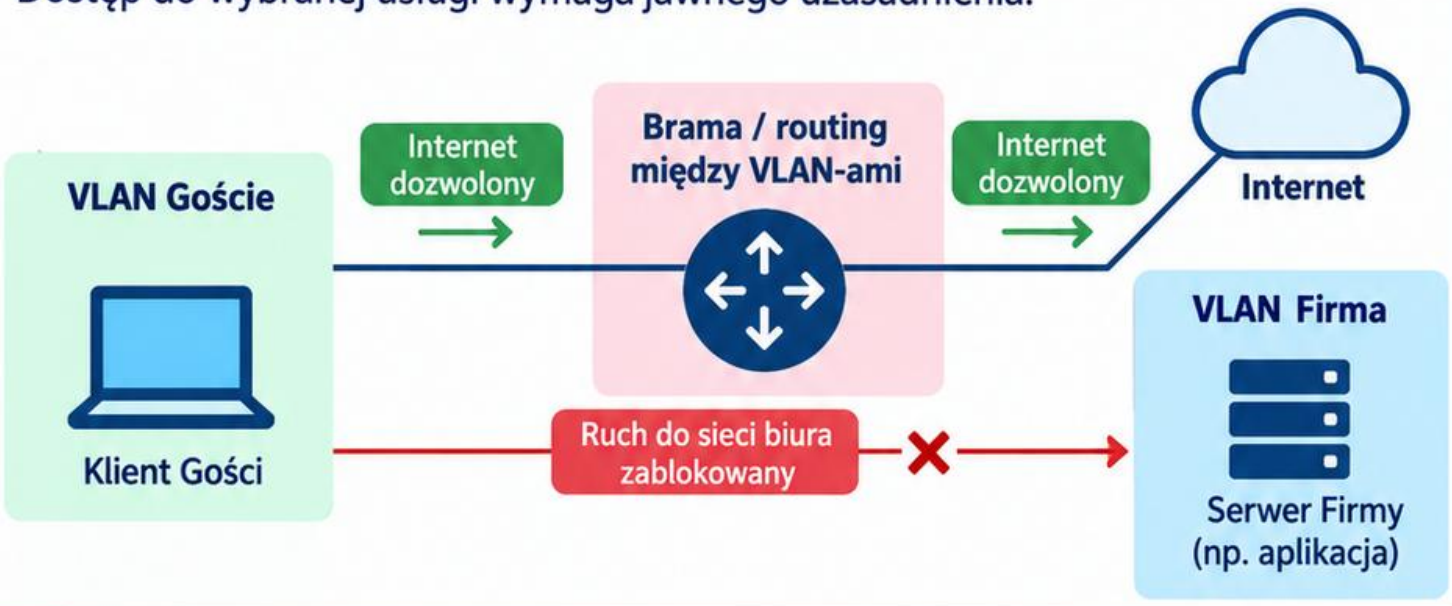
Cel: ograniczyć ruch między segmentem gości a innymi sieciami.

Gdzie: Settings > Networks > [sieć] > Network Isolation.

Sprawdź, które urządzenie realizuje routing. Włącz izolację w obsługiwanej konfiguracji lub przygotuj odpowiednie polityki na rzeczywistej bramie.

Zapisz wymagane wyjątki, na przykład dostęp do wskazanej usługi. W przypadku niestandardowych wymagań sprawdź zasady firewalla i kolejność ich działania.

Przykład: goście mają internet, ale nie otwierają aplikacji w sieci biura. Dostęp do wybranej usługi wymaga jawnego uzasadnienia.



Wykonaj próby dozwolone i zabronione dla używanych protokołów IP. Izolacja między VLAN-ami nie blokuje automatycznie komunikacji wewnątrz jednego VLAN-u.

Przykład testu: klient Gości nie otwiera TCP 443 serwera Firmy, lecz nadal uzyskuje DHCP i DNS. Nie ograniczaj całego Gateway bez wyjątków usługowych.

Źródła: [20]

Ostoja · Mapa 094 · Zaplanuj portal gościnny

Cel: ustalić sposób wejścia i utrzymania dostępu.

Gdzie: Settings > WiFi > [SSID] > Hotspot Portal > Captive Portal.

Zdefiniuj scenariusz pierwszego połączenia i obsługę użytkownika. Sprawdź wymagania dostępności kontrolera oraz infrastruktury obsługującej wybraną metodę autoryzacji.

1 Scenariusz pierwszego połączenia

Nowy telefon łączy się z siecią Wi-Fi (SSID). → Wyświetla się strona powitalna (portal captive). → Użytkownik uzyskuje dostęp zgodnie z regułą. → Aktywna sesja dostępu dla gościa. → Po zakończeniu sesji użytkownik traci uprawnienie.

2 Przygotowanie strony powitalnej

Po włączeniu przejdź do Insights > Hotspot > Landing Page.
Przygotuj czytelny komunikat i przetestuj stronę na typowych telefonach.

3 Przykład komunikatu dla gościa

Przykład: recepcja informuje gościa, jak uzyskać dostęp i gdzie zgłosić problem. Portal nie powinien wymagać niepotrzebnych danych osobowych.

Komunikat dla gościa

4 Testy i weryfikacja

Sprawdź nową sesję, autoryzację i dostęp po jej zakończeniu. Osobno zweryfikuj izolację; poprawnie wyświetlona strona nie potwierdza bezpieczeństwa sieci.

5 Próby portalu

Nowy telefon przechodzi stronę powitalną, otrzymuje dostęp i traci uprawnienie zgodnie z regułą.

Osobno sprawdź telefon, który nie otwiera automatycznego okna.

Źródła: [36]

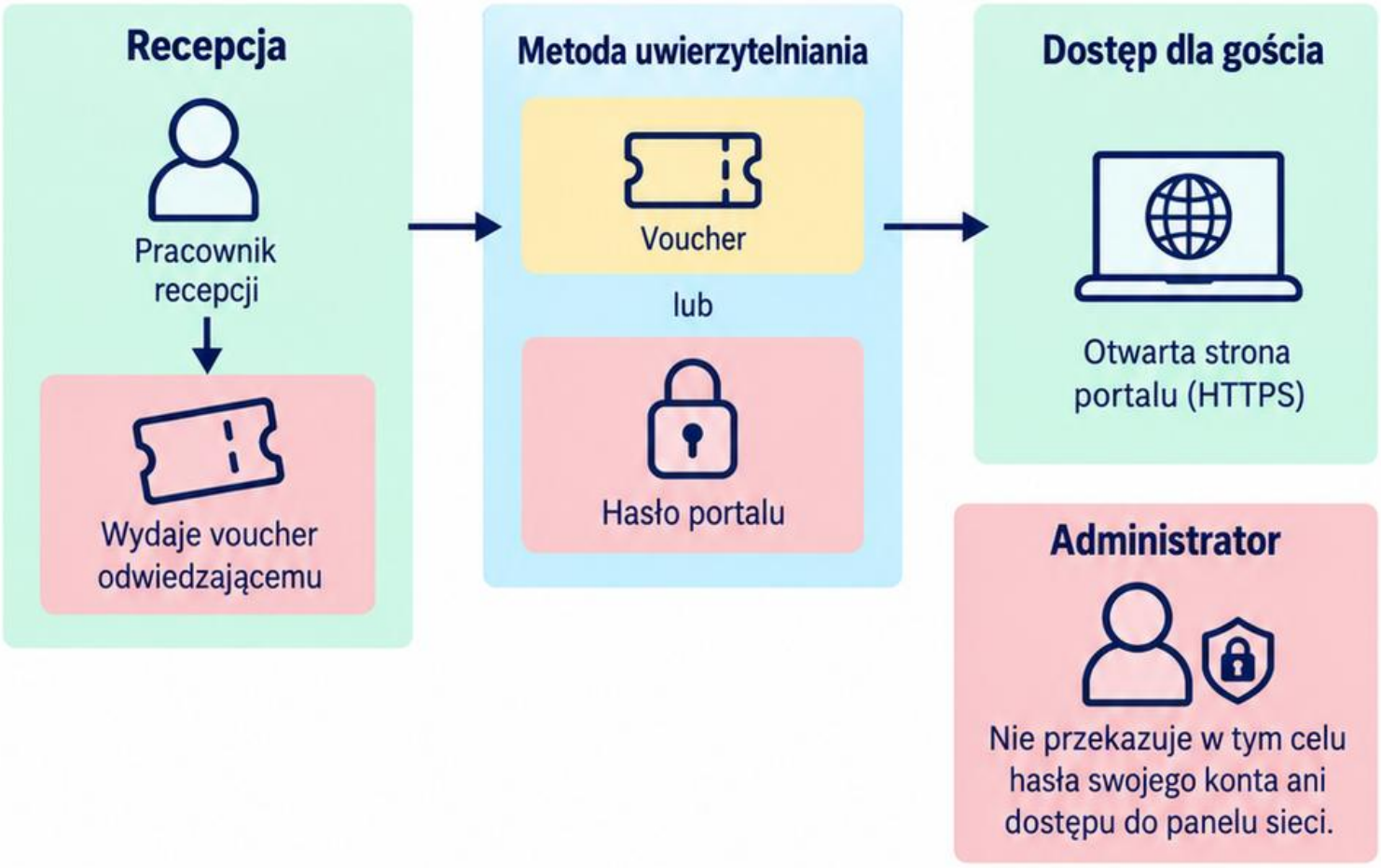
Ostoja · Mapa 095 · Dobierz uwierzytelnianie portalu

Cel: dopasować kontrolę wejścia do sposobu obsługi gości.

Gdzie: Insights > Hotspot > Landing Page po włączeniu portalu.

Wybierz metodę dostępną w danej instalacji, na przykład voucher lub hasło portalu. Sprawdź zależności usług zewnętrznych przed ich użyciem.

Przygotuj procedurę wydawania dostępu i cofnięcia uprawnienia. Oddziel dane logowania do Wi-Fi od ewentualnej dodatkowej autoryzacji portalu.



Administrator

Nie przekazuje w tym celu hasła swojego konta ani dostępu do panelu sieci.

Przykład

Pracownik recepcji wydaje voucher odwiedzającemu. Administrator nie przekazuje w tym celu hasła swojego konta ani dostępu do panelu sieci.

Test działania

Wykonaj próbę z nowym urządzeniem i błędnym uprawnieniem. Potwierdź prawidłowy komunikat odmowy oraz działanie po użyciu poprawnej metody.

Próba odmowy

Nieprawidłowe hasło portalu nie daje dostępu; poprawne pozwala otworzyć stronę HTTPS. Hasło portalu i hasło SSID zapisuj jako odrębne mechanizmy.

Źródła: [36]

Ostoja · Mapa 096 · Przygotuj vouchery

Cel: wydawać kontrolowane uprawnienia do portalu.

Gdzie: Insights > Hotspot; dostępność opcji zależy od konfiguracji.

Sprawdź, czy wybrany portal udostępnia uwierzytelnianie voucherami. Ustal okres dostępu oraz ewentualne limity zgodnie z zasadami miejsca.

Utwórz pulę testową i przetestuj pojedynczy voucher przed przekazaniem recepcji. Zapisz zasady wydania oraz sposób obsługi niewykorzystanych kodów.



Przykład: uczestnik szkolenia otrzymuje dostęp na czas wizyty. Parametry wynikają z programu wydarzenia, a nie ze stałej recepty dla wszystkich obiektów.

Sprawdź użycie, wygaśnięcie i ponowną próbę logowania. W dokumentacji zachowuj identyfikator puli oraz reguły, bez publikowania aktywnych kodów.

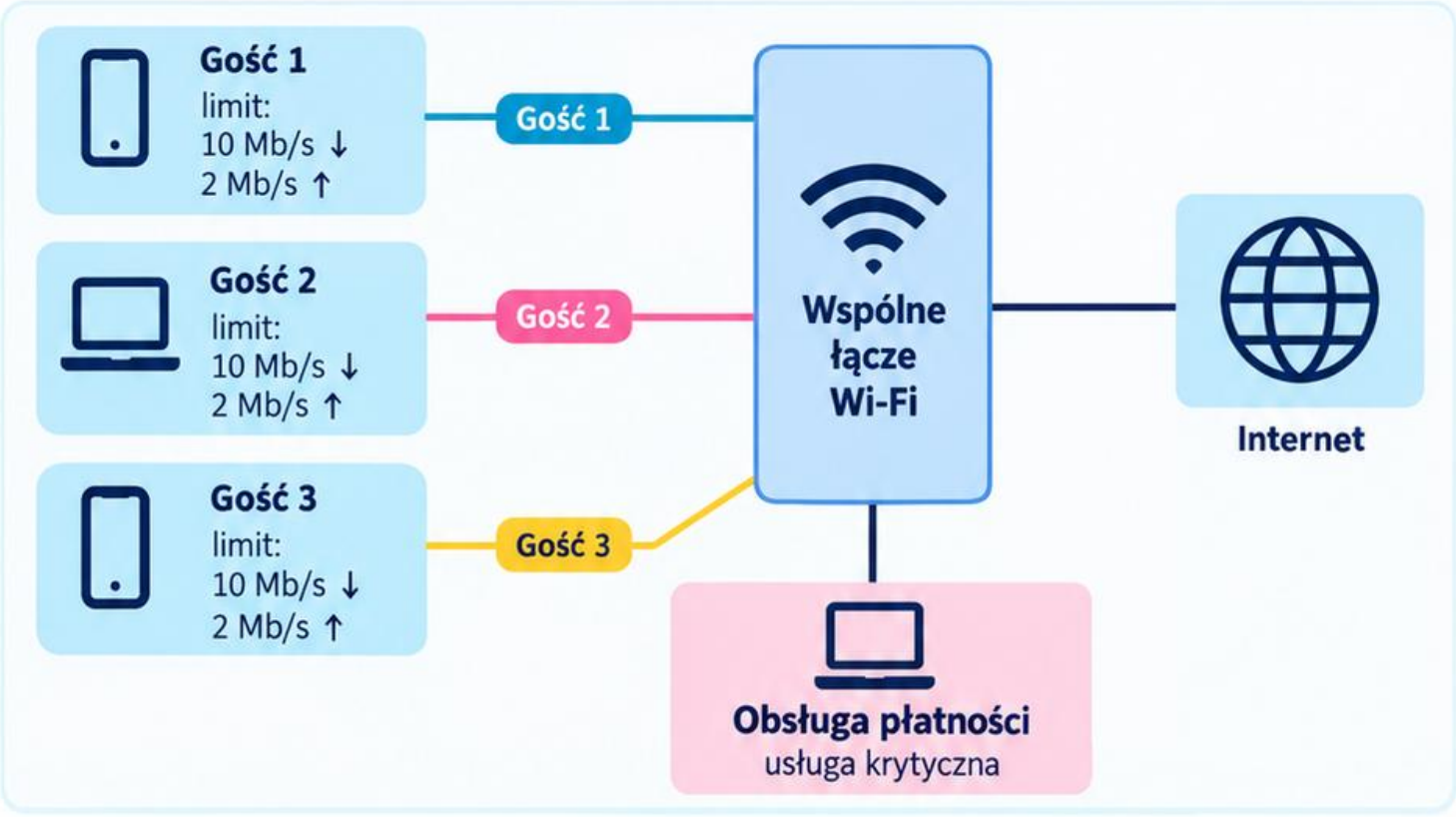
Przykład polityki recepcji: ważność vouchera 2 godziny. Sprawdź przyjęcie kodu, początek odliczania i odmowę po wygaśnięciu; nie zmieniaj zegara produkcyjnej konsoli.

Źródła: [36]

Ostoja · Mapa 097 · Ustal limit pasma

Cel:
ograniczyć wpływ gości na wspólne łącze.

Gdzie: Settings > WiFi > [SSID] > WiFi Speed Limit; limity voucherów w Insights > Hotspot.



Zmierz dostępne łącze i wymagania usług.
Rozróżnij limit przypisany klientowi lub uprawnieniu od łącznej pojemności internetu.

Ustaw limit dostępny dla danego trybu i zapisz jego zakres działania.
Nie traktuj ograniczenia prędkości jako rezerwacji pasma dla innych użytkowników.

Przykład: kawiarnia chroni obsługę płatności podczas pracy gości.
Wartość limitu wynika z pomiaru i priorytetów działalności.

Sprawdź wysyłanie oraz pobieranie z reprezentatywnego klienta.
Powtórz próbę z kilkoma klientami i obserwuj, czy krytyczna usługa nadal działa prawidłowo.

Przykład limitu klienta: 10 Mb/s pobierania i 2 Mb/s wysyłania.
Dwa telefony testuj równocześnie; limit każdego klienta nie jest wspólną pulą 10 Mb/s.

Źródła: [36], [33]

Ostoja • Mapa 098 • Ustaw harmonogram SSID

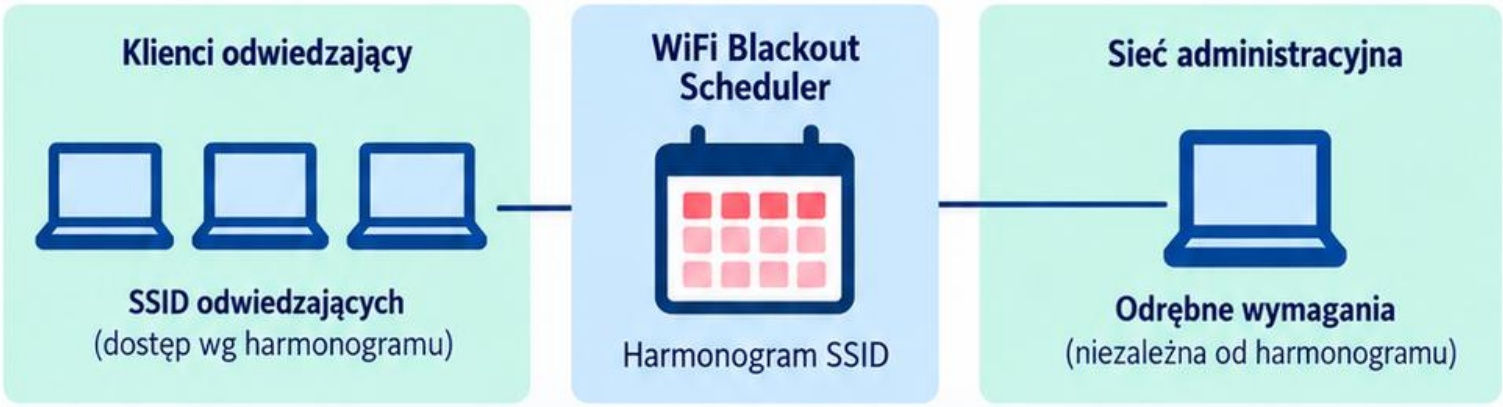
Cel:
udostępniać sieć w zatwierdzonych godzinach.

Gdzie:
Settings > WiFi > [SSID].

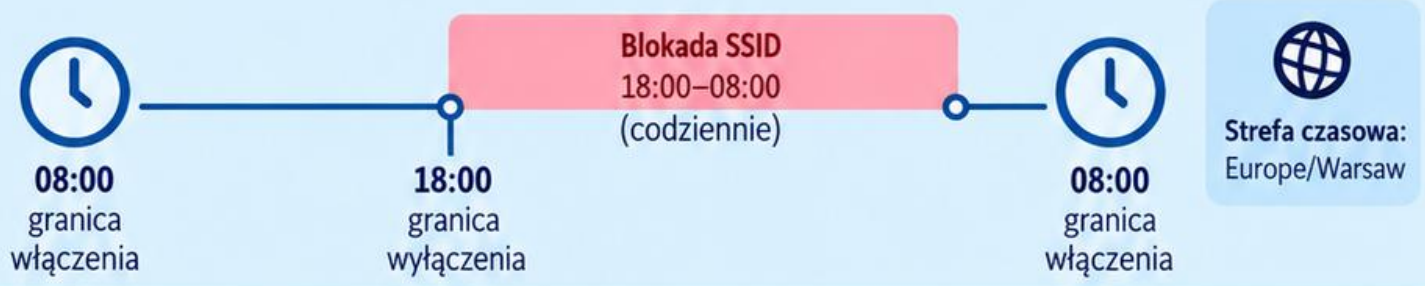
Sprawdź strefę czasową instalacji. W opcjach SSID odszukaj WiFi Blackout Scheduler; zapisz dni, godziny blokady i wyjątki wymagające ręcznej obsługi.

Zaplanuj test granicy włączenia i wyłączenia.
Poinformuj obsługę, co stanie się z klientami korzystającymi z sieci po godzinach.

Przykład: biblioteka nadaje SSID odwiedzających podczas otwarcia. Sieć administracyjna ma odrębne wymagania i nie powinna zależeć od tego harmonogramu.



Przykład biblioteki: blokada SSID codziennie 18:00–08:00, strefa Europe/Warsaw.



Sprawdź granice harmonogramu i zachowanie aktywnego klienta; nie przestawiaj zegara produkcji.

Sprawdź widoczność SSID i działanie aktywnej sesji po zmianie czasu harmonogramu.
Nie zakładaj automatycznie zachowania wszystkich klientów; zanotuj wynik próby.

Źródła: [33], [37]

Ostoja • Mapa 099 • Chroń dostęp administracyjny

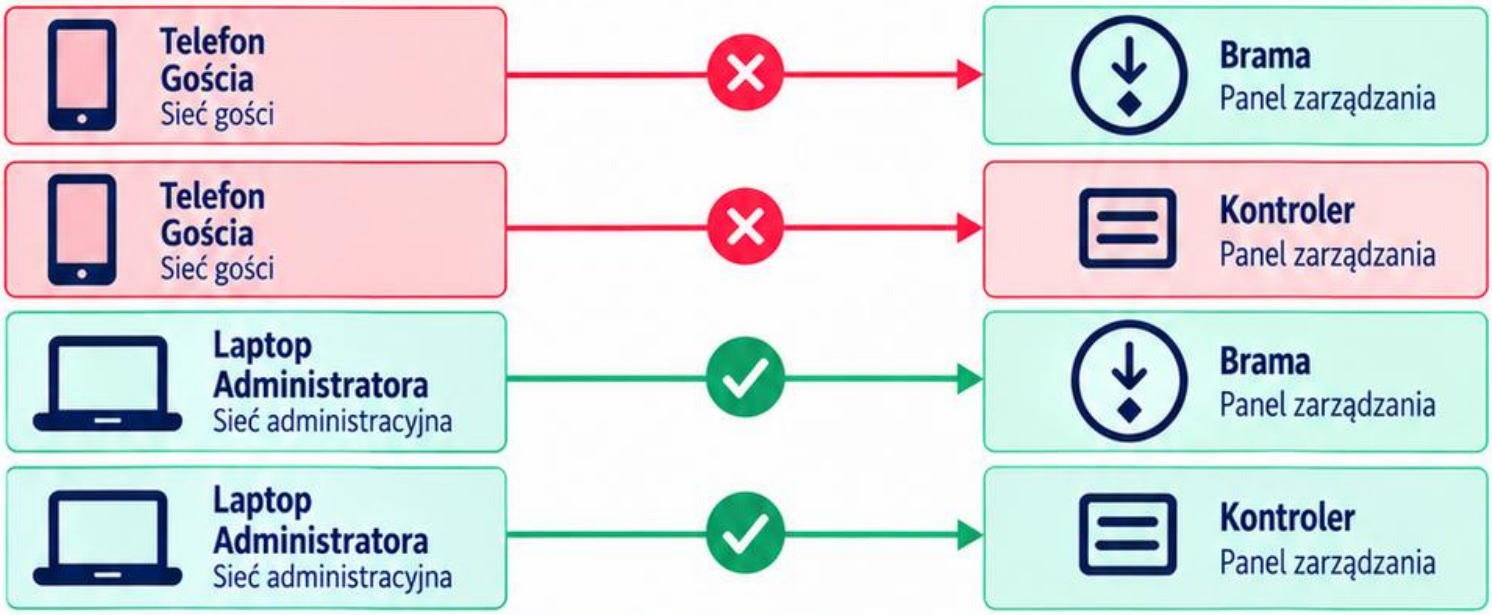
Cel: uniemożliwić gościom korzystanie z paneli zarządzania.

Gdzie: Network 9.4: Settings > Zones; 9.3: Settings > Policy Engine > Zones w konfiguracji strefowej.

Wskaż adresy i strefy usług administracyjnych, w tym samą bramę. Oddziel ochronę bramy od blokowania zasobów w innych sieciach.

Zapewnij zatwierdzoną drogę administratora przed zastosowaniem ograniczeń. Sprawdź kolejność polityk oraz dostęp używany podczas zmiany.

Przykład: telefon gościa ma internet, ale nie otwiera panelu bramy ani kontrolera. Laptop administratora korzysta z osobnej drogi.



Testuj kontrolowane próby z segmentu gości oraz z sieci administracyjnej. Blokada między VLAN-ami nie wystarcza do potwierdzenia ochrony usług samej bramy.

Odbiór ochrony: telefon Gościa nie otwiera panelu bramy ani kontrolera, lecz działa DNS. Administrator wykonuje świeże logowanie przez przygotowany port lokalny.

Źródła: [3]

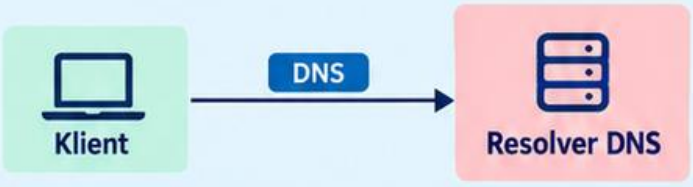
Ostoja

Ostoja · Mapa 100 · Zachowaj potrzebny DNS

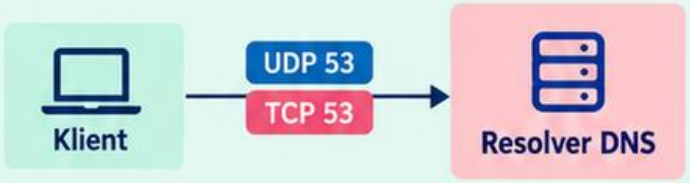
Cel:
umożliwić rozwiązywanie nazw bez nadmiernego otwarcia sieci.

Gdzie:
Settings > Networks oraz
Network 9.4: Settings > Zones;
9.3: Settings > Policy Engine > Zones.

1 Odczytaj DNS przekazywany klientom.
Ustal, czy resolver znajduje się na bramie, w innej sieci czy poza instalacją.



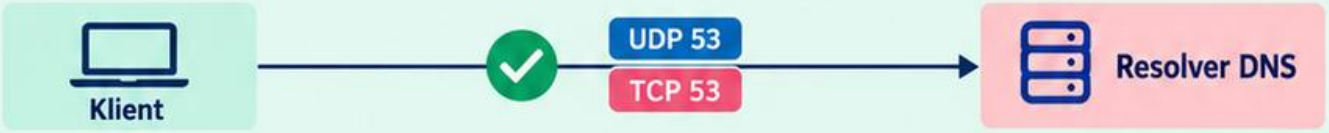
2 Sprawdź politykę dla rzeczywistego adresu docelowego i usługi.
Wyjątek ogranicz do potrzebnego resolvera zamiast otwierać cały segment infrastruktury.



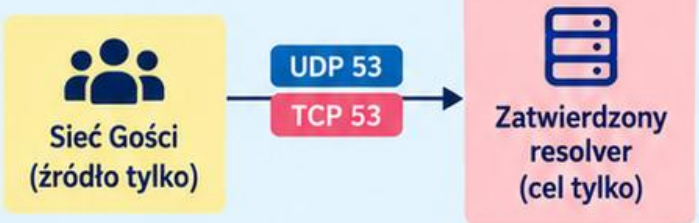
3 Przykład: klient otrzymuje adres, ale strony po nazwie nie działają.
Porównaj zapytanie do przydzielonego DNS z osiągalnością znanego celu.



4 Po poprawce ponów zapytanie i otwórz usługę po nazwie.
Nie diagnozuj DNS wyłącznie na podstawie testu ping do przypadkowej strony internetowej.



5 Wyjątek DNS: źródło tylko sieć Gości, cel tylko zatwierdzone resolvery, UDP i TCP 53.
Dla DNS na bramie wybierz Gateway jako cel.



6 Test: zapytanie UDP i TCP do właściwego DNS działa; panel bramy pozostaje niedostępny. Zezwolenie DNS nie otwiera wszystkich usług Gateway.



Źródła: [3], [18]

Ostoja • Mapa 101 • Zachowaj potrzebny DHCP

Cel: umożliwić klientowi uzyskanie konfiguracji po izolacji.

Gdzie: Settings > Networks oraz odpowiednie polityki bramy.

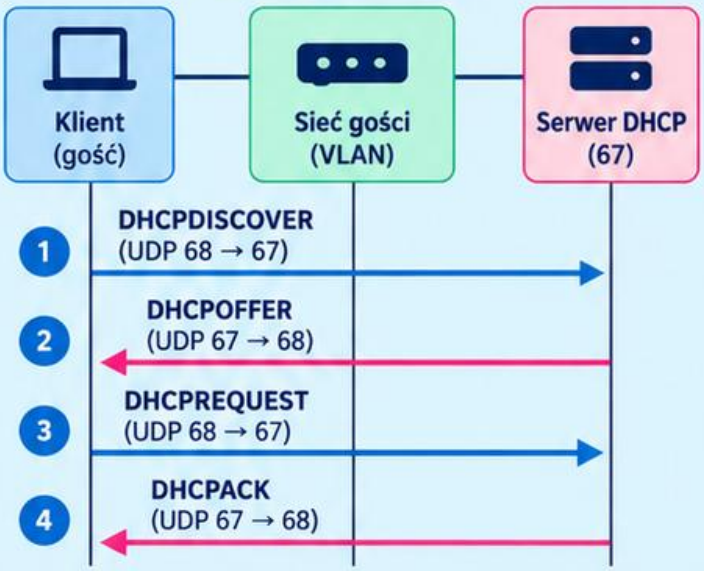
Ustal, gdzie działa DHCP dla sieci gości.
Sprawdź zakres, dostępność adresów i drogę VLAN-u przed modyfikowaniem reguł.

Zweryfikuj, czy polityki nie blokują wymaganej wymiany z usługą.
Nie dodawaj szerokiego dostępu do całej sieci zarządzającej jako obejścia.

Przykład: gość po nowym połączeniu nie uzyskuje prawidłowej dzierżawy, choć wcześniej zapisane urządzenie jeszcze działa. Porównaj świeżą i istniejącą sesję.

Nowy klient – pełna wymiana DHCP

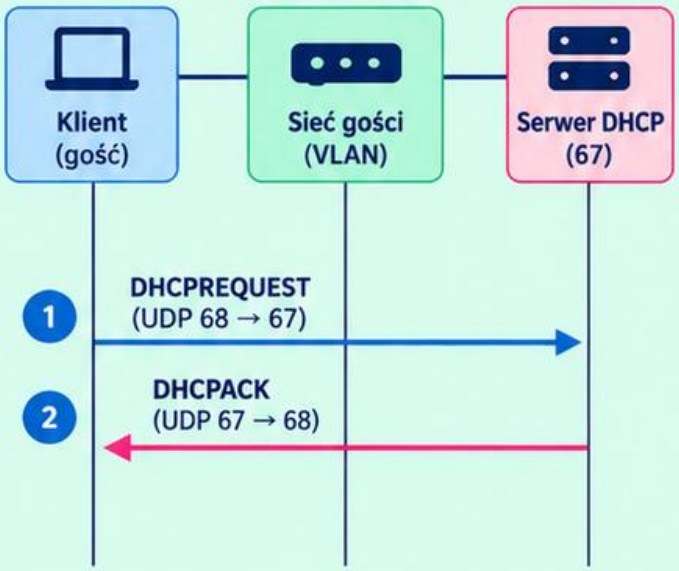
Klient bez zapisanej dzierżawy uzyskuje konfigurację przez sieć gości (VLAN).



Klient otrzymuje adres, maskę, bramę i DNS zgodnie z odpowiedzią serwera.

Istniejący klient – odnowienie dzierżawy

Wcześniej zapisane urządzenie może nadal działać. Porównaj ze świeżą sesją.



Działanie starej dzierżawy nie potwierdza aktualnej dostępności DHCP.

Odnów dzierżawę na kliencie testowym i sprawdź adres, maskę, bramę oraz DNS.
Działanie starej dzierżawy nie potwierdza aktualnej dostępności DHCP.

DHCPv4: klient UDP 68 → serwer 67; odpowiedź serwera 67 → klienta 68.
Zachowaj pierwsze żądanie rozgłoszeniowe klienta, który jeszcze nie ma adresu.

Nie ograniczaj pierwszej wymiany do już nadanej podsieci źródłowej.
Przy DHCP na bramie zachowaj usługę Gateway bez otwierania panelu administracyjnego.

Test: nowy klient bez zapisanej dzierżawy uzyskuje adres, odnawia go i korzysta z DNS.
Serwer zewnętrzny lub relay wymaga osobnego projektu.

Źródła: [1], [3], [12]

Ostoja · Mapa 102 · Udostępnij konkretną usługę

Cel:
zezwolić na uzasadniony wyjątek bez znoszenia izolacji.

Gdzie:
Network 9.4: Settings > Zones;
9.3: Settings > Policy Engine > Zones;
ustawienia odkrywania usług osobno.

Zapisz źródło, adres celu, usługę i osobę zatwierdzającą dostęp.
Rozdziel odnajdywanie urządzenia od komunikacji potrzebnej do działania aplikacji.

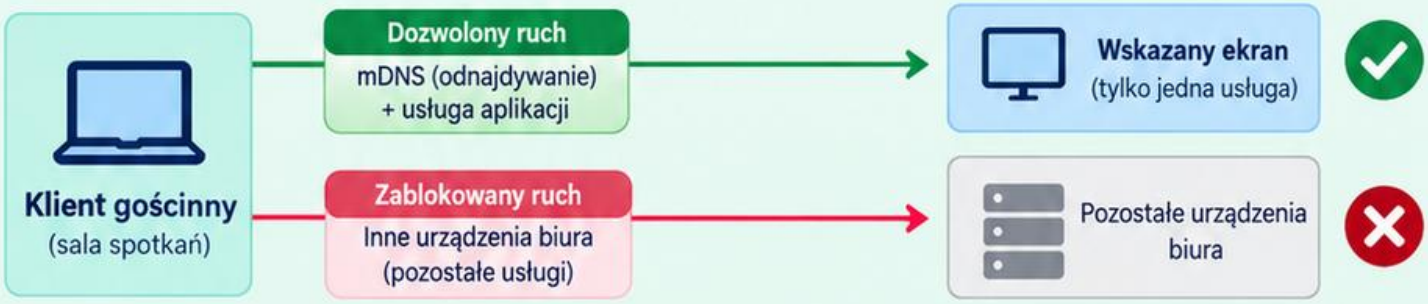
Dodaj możliwie wąską politykę, uwzględniając jej kolejność.
Jeśli potrzebne jest mDNS, sprawdź jego zakres zamiast włączać je wszędzie.

Przykład: sala spotkań udostępnia wskazany ekran, lecz goście nadal nie mają dostępu do pozostałych urządzeń biura.



Przetestuj usługę docelową i sąsiedni zabroniony zasób.
Sama widoczność nazwy urządzenia nie dowodzi, że ruch aplikacji został dopuszczony.

Przykład wyjątku: wybrany klient → jeden ekran, tylko potwierdzony port usługi.
Testuj odtwarzanie oraz próbę wejścia na inny port; samo mDNS nie wystarcza.



Źródła: [3]

Ostoja · Mapa 103 · Oceń izolację przez ACL

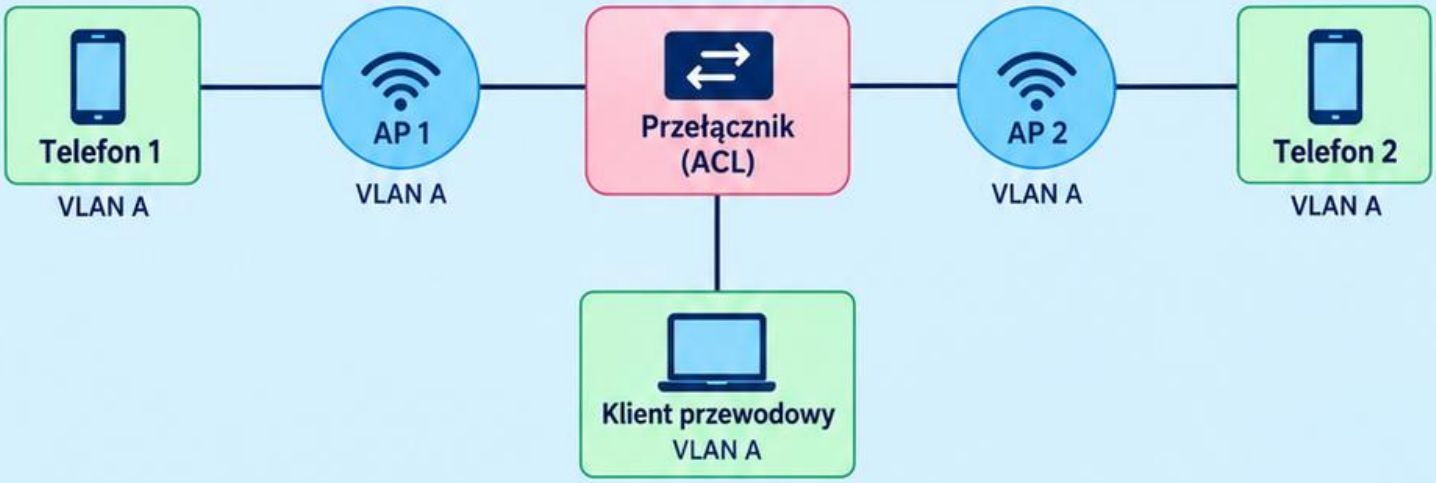
Cel: zastosować ochronę w przełączniku obsługującym daną funkcję.

Gdzie: Settings > Networks > Device Isolation (ACL), jeśli opcja jest dostępna.

Sprawdź zgodność modelu, wersji i sposobu routingu.
Obecność innego ustawienia izolacji nie oznacza automatycznie dostępności ACL.

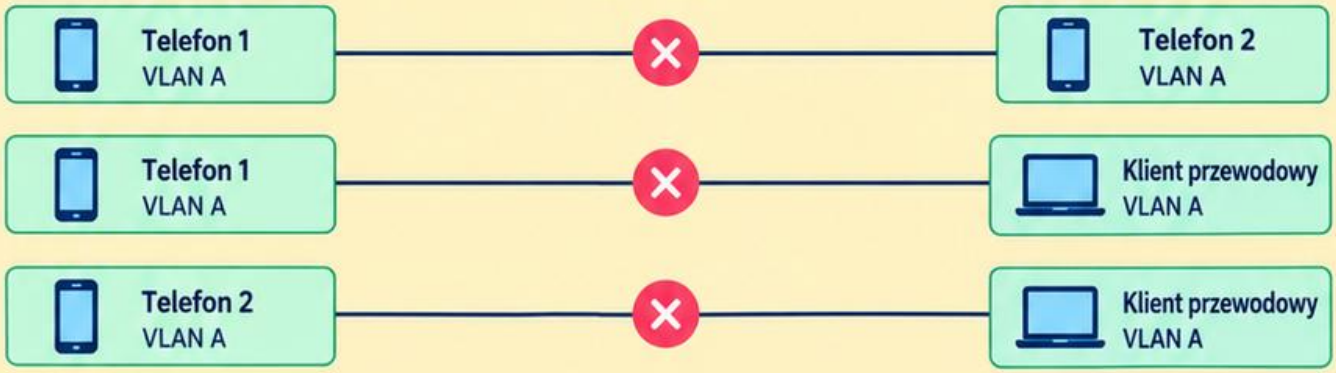
Narysuj drogi między klientami i wskaż przełączniki egzekwujące ograniczenia.
Uwzględnij urządzenia podłączone przewodowo oraz przez różne AP.

Ten sam VLAN (klienci z różnych AP i przewodowy)



Przykład: dwa telefony trafiają do tego samego VLAN-u przez różne AP. Izolacja jednego AP nie zamyka całej tej drogi.

Przykładowe kierunki ruchu w tym samym VLAN-ie (ACL na przełączniku)



Zweryfikuj osobno ruch w obrębie VLAN-u i między VLAN-ami, także dla używanych rodzin IP. Zakres ACL musi odpowiadać wymaganej granicy ochrony.

Próba ACL: dwa kontrolowane urządzenia w jednym VLAN-ie przez różne AP, następnie klient przewodowy. Zapisz switch egzekwujący blokadę; niesprawna aplikacja sama nie dowodzi izolacji.

Źródła: [20]

Ostoja · Mapa 104 · Przetestuj izolację gości

Cel: udowodnić działanie każdej wymaganej granicy.

Gdzie: Clients oraz kontrolowane urządzenia testowe.

Przygotuj dwa własne urządzenia i znaną usługę testową. Sprawdź, czy usługa odpowiada przed włączeniem badanej blokady.

Wykonaj pary prób: ten sam AP, różne AP, klient przewodowy, inny segment oraz panel bramy. Zapisz wynik każdej drogi.

Przykład: brak komunikacji dwóch telefonów na jednym AP jest poprawny, ale po przejściu jednego telefonu do drugiego AP wymaga ponownej kontroli.

Potwierdź jednocześnie działanie internetu. Brak odpowiedzi na ping nie jest pełnym dowodem izolacji, jeśli odbiornik sam ignoruje ten rodzaj ruchu.

Zachowaj wynik początkowy działającej usługi kontrolnej. Po izolacji odmowa ma wynikać z polityki, a nie uśpienia telefonu lub jego lokalnego firewalla.

Para testowa (źródło → cel)	Schemat logiczny	Usługa kontrolna	Oczekiwany wynik po izolacji	Internet (źródło)
1 Ten sam AP (dwa urządzenia klienckie)	Klient A (AP 1) — Klient B (AP 1)	Znana usługa testowa	✗ Dostęp zablokowany po próbie kontrolnej	✓ Działa
2 Różne AP (dwa urządzenia klienckie)	Klient A (AP 1) — Klient B (AP 2)	Znana usługa testowa	✗ Dostęp zablokowany po próbie kontrolnej	✓ Działa
3 Klient przewodowy oraz klient z sieci gościnnej	Klient przewodowy — Klient (gość)	Znana usługa testowa	✗ Dostęp zablokowany po próbie kontrolnej	✓ Działa
4 Klient gościnny oraz inny segment	Klient (gość) — Inny segment	Znana usługa testowa	✗ Dostęp zablokowany po próbie kontrolnej	✓ Działa
5 Klient gościnny oraz panel bramy	Klient (gość) — Panel bramy	HTTPS panelu	✗ Dostęp zablokowany po próbie kontrolnej	✓ Działa

Źródła: [20]

Ostoja • Mapa 105 • Sprawdź całą wizytę gościa

Cel: potwierdzić użyteczność i ograniczenia od wejścia do wygaśnięcia.

Gdzie: Settings > WiFi, Clients oraz Insights > Hotspot, jeśli używany.

Użyj nowego profilu klienta. Sprawdź widoczność SSID, uwierzytelnienie, adresację i pojawienie się portalu w przewidzianym scenariuszu.

Uzyskaj dostęp zatwierdzoną metodą. Sprawdź stronę internetową, rozwiązywanie nazw i zakazane kierunki; zanotuj zachowanie po zakończeniu uprawnienia.

1. Recepcja

Gość hotelu otrzymuje dostęp w recepcji.

OK: profil klienta jest nowy.

NIE: użyto wcześniejszego profilu.

2. Wi-Fi

Sprawdź widoczność SSID i uwierzytelnienie.

OK: SSID jest widoczny i możliwe uwierzytelnienie.

NIE: SSID niewidoczny lub brak możliwości uwierzytelnienia.

3. Portal

Sprawdź pojawienie się portalu i uzyskaj dostęp zatwierdzoną metodą.

OK: portal pojawia się w przewidzianym scenariuszu.

NIE: portal nie otwiera się automatycznie.

4. Internet

Sprawdź stronę internetową, rozwiązywanie nazw i zakazane kierunki.

OK: strona internetowa i rozwiązywanie nazw działają, a zakazane kierunki są zablokowane.

NIE: brak internetu, błędy w rozwiązywaniu nazw lub dostęp do zakazanych kierunków.

5. Wygaśnięcie

Po zakończeniu uprawnienia dostęp wygasa.

OK: po zakończeniu uprawnienia dostęp wygasa.

NIE: dostęp nadal działa po wygaśnięciu.

Ponownie przejdź przewidziany proces.

Przykład: gość hotelu otrzymuje dostęp w recepcji, korzysta z internetu i po wygaśnięciu musi ponownie przejść przewidziany proces.

Powtórz próbę na drugim systemie telefonu. Jeśli portal nie otwiera się automatycznie, sprawdź pełny proces, zamiast uznawać samo Wi-Fi za niesprawne.

Odbiór wizyty: Android i iOS, świeży profil, dostęp, internet oraz wygaśnięcie. Zapisz różnice obsługi portalu i przekaż recepcji sposób ponownego uzyskania uprawnień.

Źródła: [36]

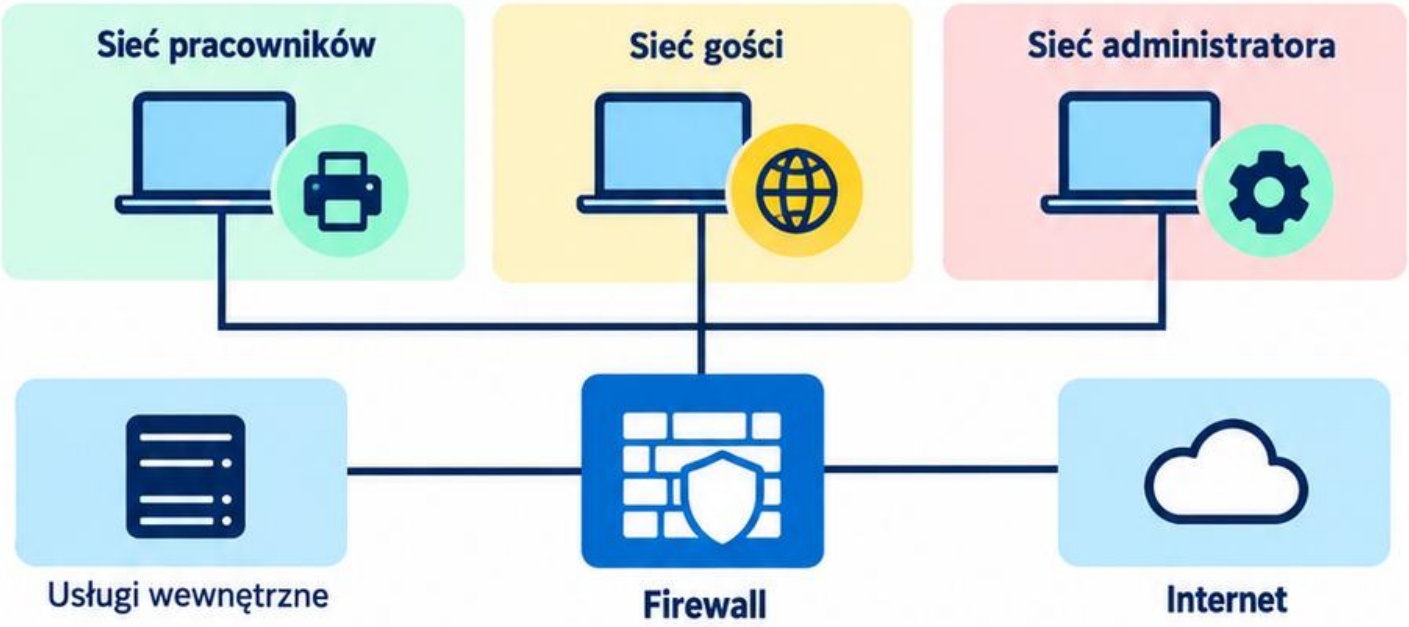
Ostoja • Moduł 8

Firewall i bezpieczeństwo

Zacznij od listy dozwolonych połączeń, a nie od przycisku blokowania.
Każde odstępstwo powinno mieć właściciela i uzasadnienie.

W tym module przejdziesz od rozpoznania firewalla do testów rzeczywistego dostępu. Zachowaj działającą ścieżkę administracyjną i kopię konfiguracji.

Przykład: pracownicy drukują na jednym urządzeniu IoT, goście korzystają wyłącznie z internetu, administrator zarządza przez wydzieloną sieć.



Najpierw ustal **źródło, cel, protokół i port**. Osobno rozpatruj połączenia do bramy oraz ruch przechodzący przez bramę.

Rezultat: macierz komunikacji, minimalne wyjątki i potwierdzone blokady. Jeśli znika DNS albo dostęp administratora, zatrzymaj wdrożenie i wycofaj ostatnią zmianę.

Każdą zmianę zatwierdzaj na podstawie pomiaru.

Zapisz wyniki testów odbiorowych.

Źródła: [3], [8]

Rozpoznaj typ firewalla

Ostoja • Mapa 106 • Moduł 8

Cel: wybierz instrukcję zgodną z instalacją, Firewall strefowy wymaga zgodnej bramy UniFi; starszy USG nie otrzymuje automatycznie tych możliwości.

Sprawdź wersję Network i oprogramowania bramy.
ZBF udostępniono w Network 9.0.108; wymagane oprogramowanie bramy to co najmniej 4.1.

Network 9.4: Settings > Zones.
Network 9.3: Settings > Policy Engine > Zones.
Brak stref oznacza konieczność sprawdzenia zgodności i migracji.



Reguły w starej instalacji

- Reguły LAN IN w starej instalacji należą do innego modelu.
- Brak automatycznego ZBF.
- Wymagana weryfikacja zgodności i migracja.

Macierz stref w Network 9.4

	LAN	IoT	Guest	WAN
LAN	●	●	●	●
IoT	●	●	●	●
Guest	●	●	●	●
WAN	●	●	●	●

Schemat — sprawdź własne polityki.

Przykład: Network 9.4 na zgodnej bramie pokazuje macierz stref. Reguły LAN IN w starej instalacji należą do innego modelu.

Test: zapisz wersje i nazwę widocznej sekcji. Przed migracją wykonaj backup i zestaw testów; nie przepisuj kierunków reguł mechanicznie.

Źródła: [3], [38], [8]

Przypisz interfejsy do stref

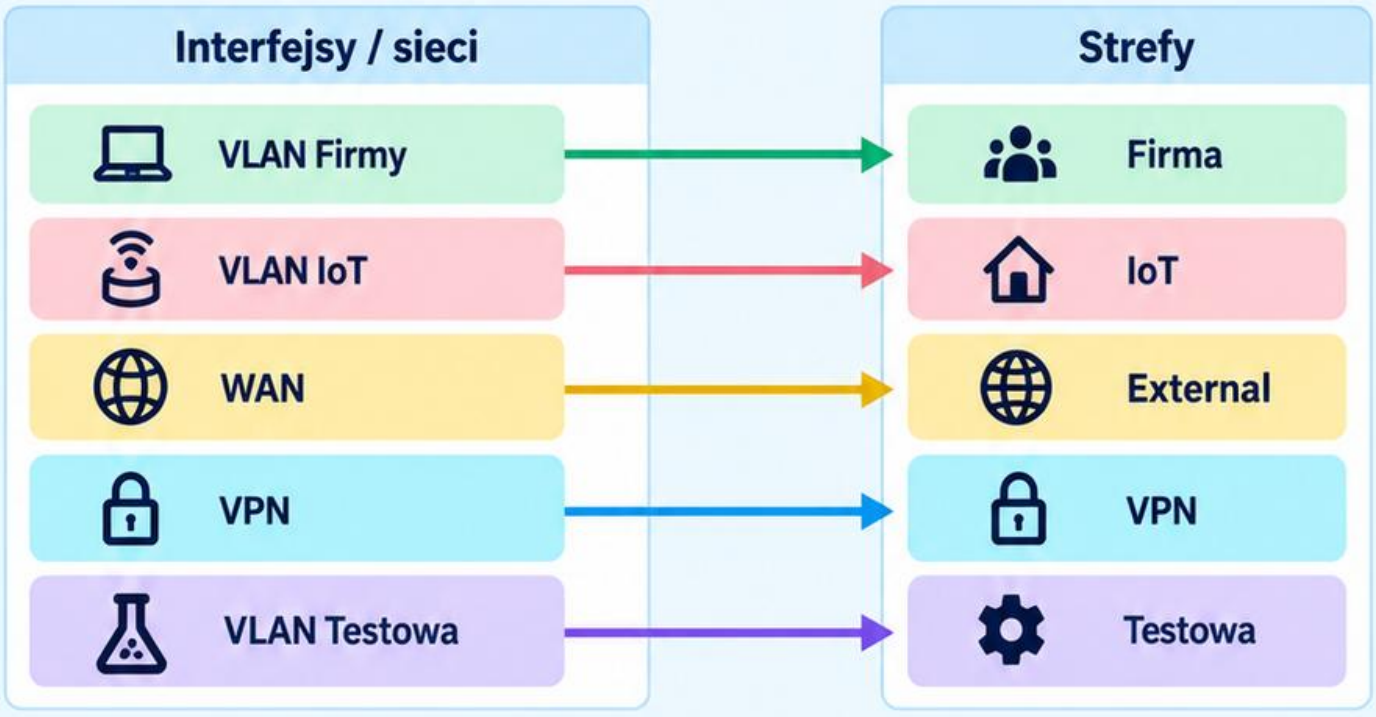
Ostoja • Mapa 107 • Moduł 8

1 **Cel:** każda sieć ma trafić do strefy odpowiadającej poziomowi zaufania. Jedna sieć może należeć tylko do jednej strefy.

2 W Network 9.4 otwórz **Settings > Zones**; w 9.3 użyj **Settings > Policy Engine > Zones.** Przejrzyj członków stref przed edycją.

3 **Zapisz** obecny przydział VLAN-ów, WAN i VPN. Najpierw przenieś sieć testową, ponieważ zmiana strefy natychmiast zmienia zestaw stosowanych polityk.

4 **Przykład:** IoT trafia do własnej strefy, WAN pozostaje External. Ruch do usług samej bramy nadal rozpatrujesz względem Gateway.



5 **Test:** sprawdź DNS, internet i zakaz dostępu do Firmy z urządzenia IoT.
Cofnięcie: przywróć poprzednią strefę i ponów testy.

Źródła: [3]

Czytaj macierz stref

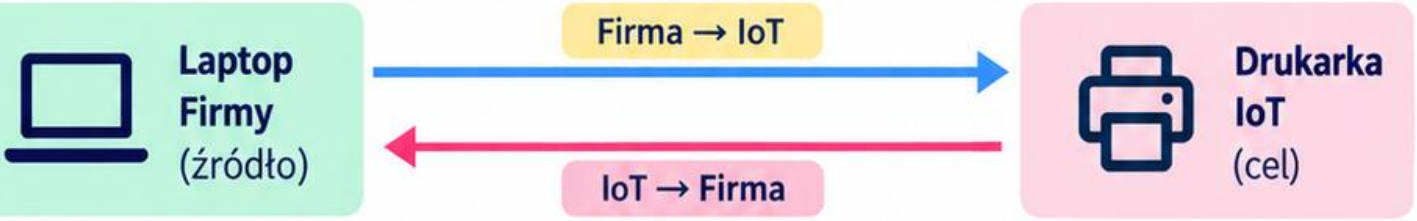
Cel: znajdź komórkę opisującą rzeczywisty kierunek inicjowania połączenia. Wiersz to źródło, kolumna to cel; odwrotny kierunek stanowi osobną relację.

Network 9.4: Settings > Zones. Wybierz przecięcie strefy źródłowej i docelowej, następnie obejrzyj obowiązujące polityki oraz ich kolejność.

Przykład: laptop Firmy łączy się z drukarką IoT. Czytaj Firma → IoT, a nie IoT → Firma tylko dlatego, że drukarka odpowiada.

Schemat kierunku — pozostałe polityki sprawdź w instalacji.

Źródło (wiersz)	Firma	Serwery	Internet	IoT	Goście
Firma	–	–	–	Policies	–
Serwery	–	–	–	–	–
Internet	–	–	–	–	–
IoT	–	–	–	–	–
Goście	–	–	–	–	–



Rozróżniaj Allow All, Block All, Allow Return Traffic oraz Policies. Sam kolor komórki nie zastępuje sprawdzenia adresów i portów.

Test: rozpocznij nowe połączenie z obu stron. Zapisz dwa wyniki i usługę testową. Nie uznawaj samego pinga za dowód działania aplikacji.

Źródła: [3]

Utwórz własną strefę

Ostoja • Mapa 109 • Moduł 8

1

Cel: oddziel urządzenia o podobnych potrzebach dostępu, na przykład czujniki i drukarki, od zaufanych stacji pracowników.

2

W Network 9.4 otwórz **Settings > Zones**. Utwórz strefę IoT, następnie sprawdź jej polityki przed przypisaniem działającej sieci produkcyjnej.

3

Przydziel testowy VLAN i przygotuj wyjątki usługowe. Nie przenoś równocześnie sieci administratora ani wszystkich urządzeń, bo utrudni to znalezienie błędu.

4

Przykład: strefa IoT obejmuje VLAN 30. Połączenia do Firmy mają być blokowane, a wydruk z Firmy do drukarki otrzyma wąski wyjątek.



5

Test: nowa strefa zawiera właściwy VLAN i zachowuje usługi wymagane przez urządzenia.

!

Cofnięcie: przywróć przydział; usunięcie strefy usuwa powiązane polityki.

Źródła: [3]

Ostoja

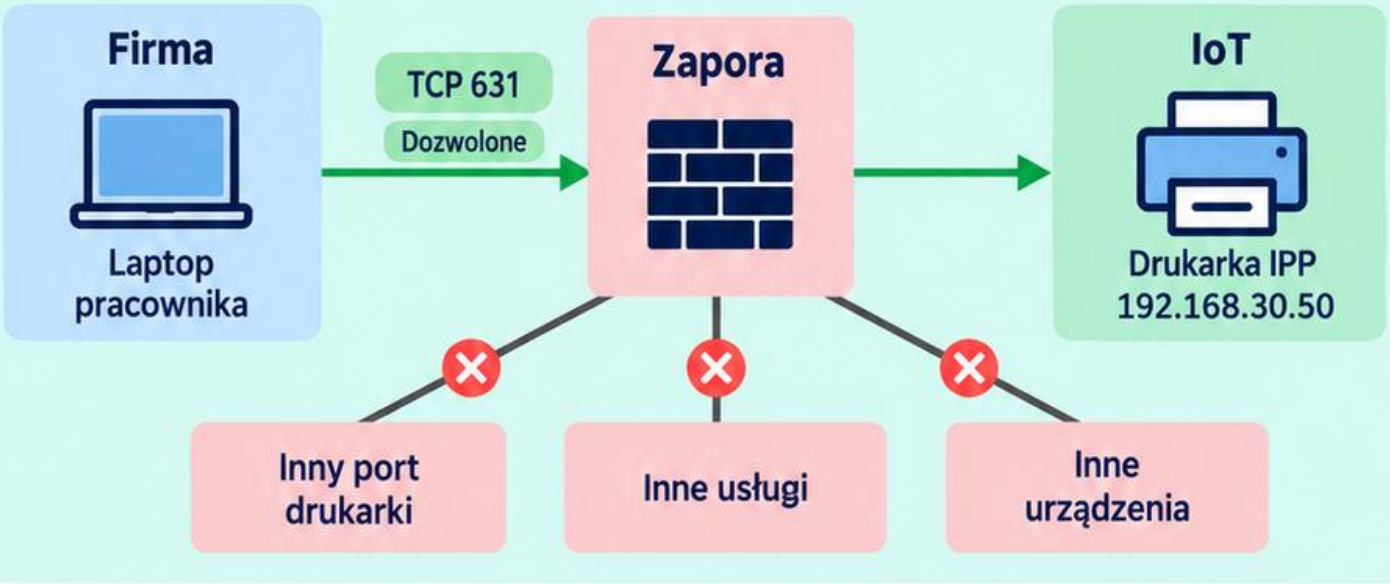
Ostoja • Mapa 110 • Moduł 8

Zezwól na konkretną usługę

Cel: otwórz tylko uzasadniony przepływ.
Opisz źródło, cel, port docelowy i protokół, zanim utworzysz politykę.

Network 9.4: Settings > Zones > Create Policy.
W 9.3: Settings > Policy Engine > Zones > Create Policy.

Ustaw Allow, właściwe strefy i adres usługi.
Przykład projektowy: Firma → IoT, cel 192.168.30.50, TCP 631 dla potwierdzonej drukarki IPP.



Port 631 jest przykładem usługi, nie uniwersalnym wymaganiem każdej drukarki. Sprawdź dokumentację urządzenia i zapewnij potrzebny ruch powrotny.

Test: wykonaj rzeczywisty wydruk, następnie spróbuj wejść na inny port drukarki. Pozytywny wydruk i negatywny test potwierdzają zawężenie wyjątku.

Wpisz właściciela oraz datę przeglądu wyjątku.

Źródła: [3]

Zablokuj ruch między segmentami

Cel: powstrzymaj nowe połączenia IoT do sieci pracowników, zachowując wcześniejsze, uzasadnione wyjątki i usługi niezbędne do działania urządzeń.

W Network 9.4 użyj **Settings > Zones > Create Policy**. Wskaż źródło IoT, cel Firma oraz działanie **Block**.

Sprawdź pełną listę polityk tej pary stref. Bardziej szczegółowe zezwolenia muszą być rozpatrywane przed ogólną blokadą odpowiedniego ruchu.



Przykład: czujnik 192.168.30.60 nie rozpoczyna sesji do laptopa 192.168.10.100. Drukowanie inicjowane przez pracownika pozostaje oddzielnie dopuszczone.

Test: użyj nowej sesji aplikacji z IoT do Firmy. Potwierdź też DNS i internet czujnika; cofnięcie polega na wyłączeniu ostatniej blokady.

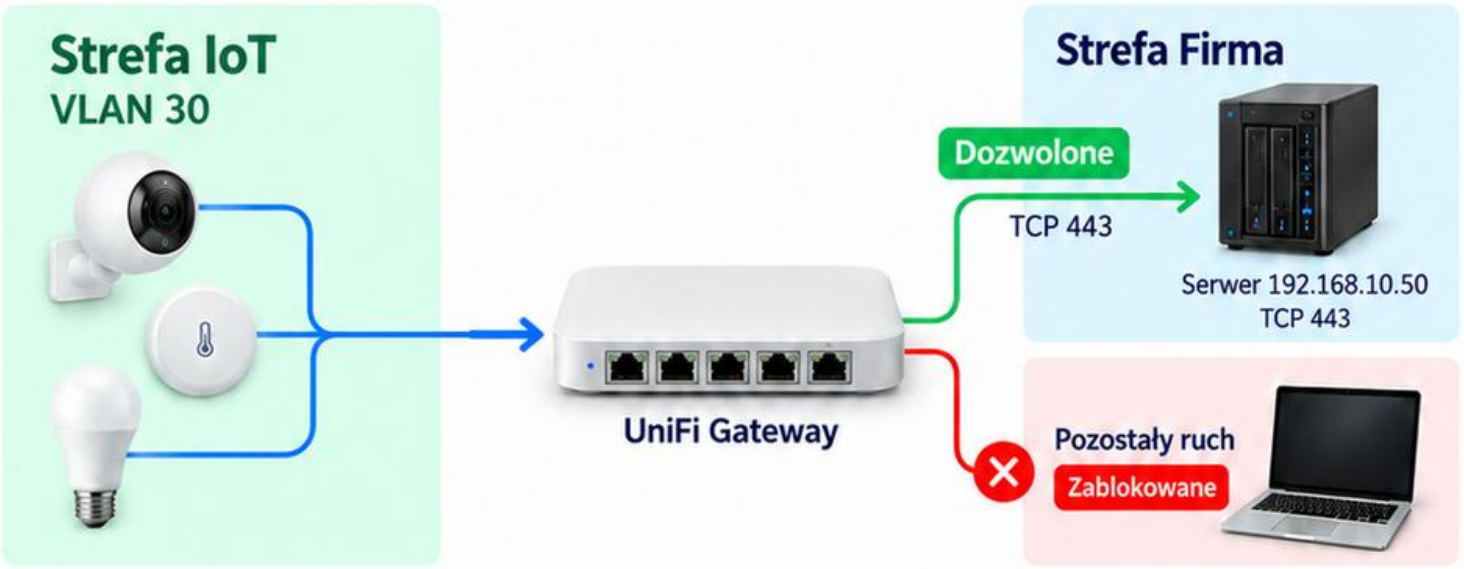
Zapisz uzasadnienie blokady i datę walidacji.

Źródła: [3]

Zezwól na wyjątek przed blokadą

Przykład: IoT może korzystać z jednej usługi, ale nie z całej sieci firmy.

Wymagania: UniFi Network 9.0.108+ i UniFi Gateway 4.1+.



1

1. Przypisz sieci do stref

Utwórz własne strefy IoT i Firma. Przypisz do nich odpowiednie sieci.

2

2. Dodaj wyjątek

Źródło: IoT. Cel: Firma, 192.168.10.50, TCP 443. Działanie: zezwól.

3

3. Zapewnij ruch powrotny

Włącz automatyczne zezwolenie na odpowiedzi, jeśli nie zapewnia go istniejąca polityka.

4

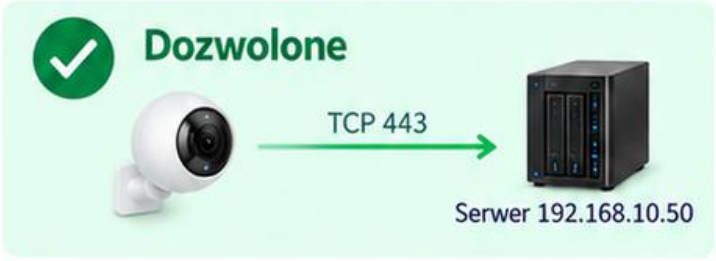
4. Dodaj blokadę

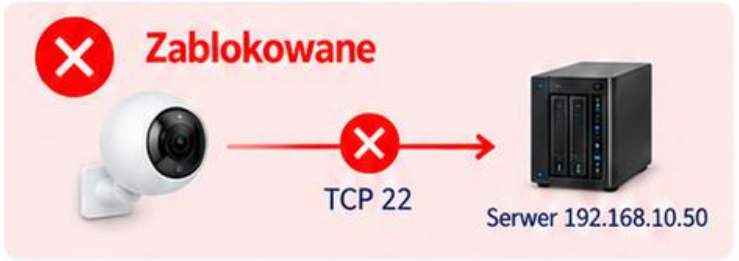
Zablokuj pozostały ruch ze strefy IoT do strefy Firma.
Umieść wyjątek wyżej niż blokadę.

5

5. Sprawdź obie próby

HTTPS do serwera działa. Inne połączenie do sieci firmy jest blokowane.





Nie blokuj usług DHCP i DNS ani własnego dostępu administracyjnego.

Schemat polityki przykładowej | Źródło: [3]

Zrozum ruch powrotny

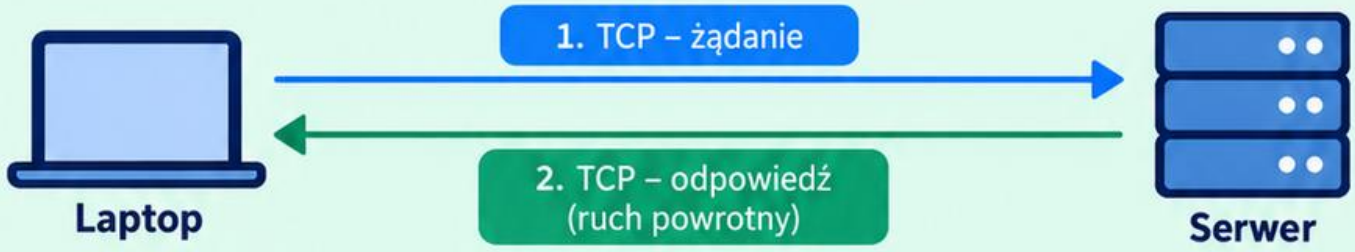
Ostoja • Mapa 113 • Moduł 8

Cel: pozwól usłudze odpowiedzieć bez otwierania wszystkim urządzeniom możliwości rozpoczynania połączeń w przeciwnym kierunku. Odpowiedź nie oznacza symetrycznego dostępu.

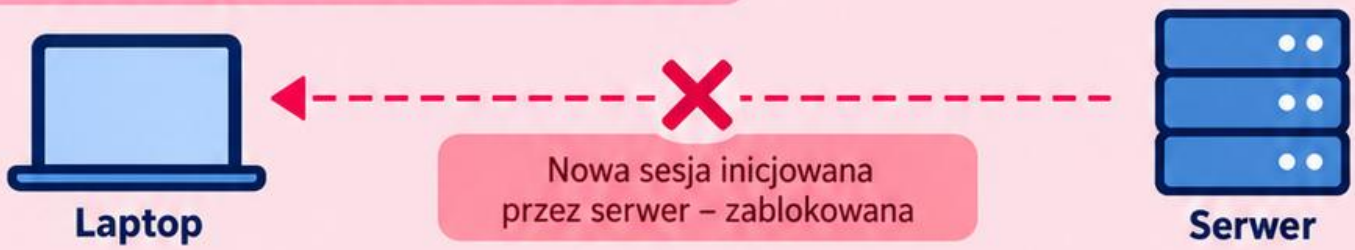
W edycji polityki Allow sprawdź **Auto Allow Return Traffic**. Funkcja dodaje politykę odpowiedzi; oceń, czy istniejące reguły już jej nie zapewniają.

Przykład: laptop inicjuje TCP do serwera. Pakiety należące do zestawionego połączenia wracają, ale serwer nie otrzymuje dowolnego dostępu do laptopa.

1. Żądanie i odpowiedź – dozwolone



2. Nowa sesja z serwera – zablokowana



Po zmianie testuj nowe sesje. Stare połączenie może nadal działać dzięki zapisowi stanu; zamknij aplikację lub rozłącz sesję testową.

Test: wykonaj żądanie oraz odpowiedź, potem niezależną próbę inicjowaną przez serwer. Wycofując wyjątek, sprawdź również automatycznie utworzoną politykę powrotną.

Źródła: [3]

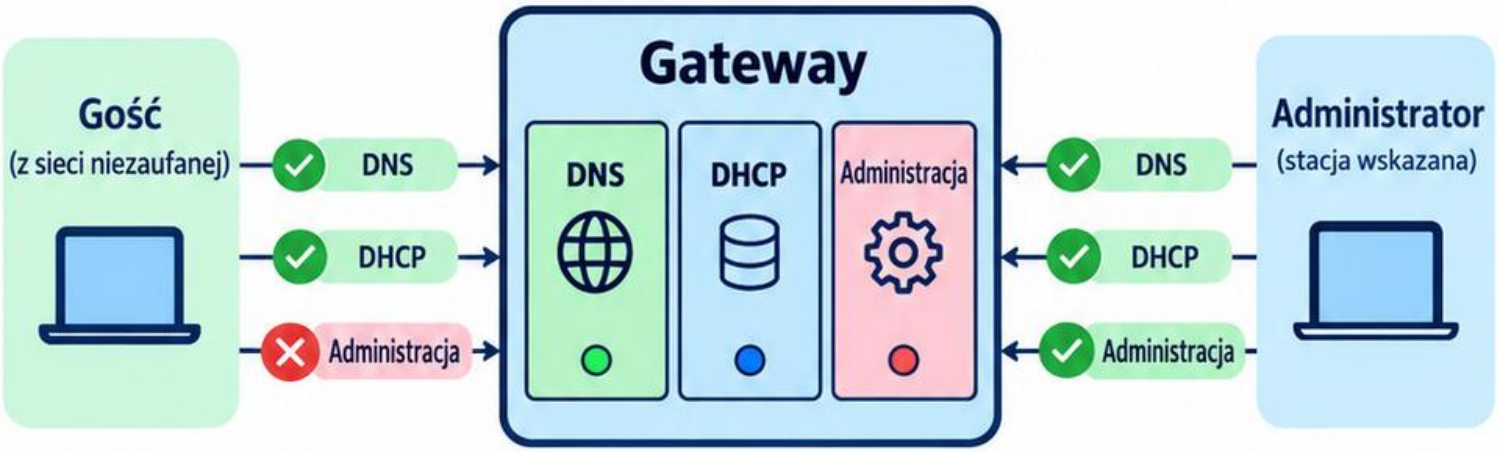
Chroń usługi bramy

Ostoja • Mapa 114 • Moduł 8

Cel: ogranicz administrację, zachowując **DNS** i **DHCP** potrzebne klientom. Gateway oznacza samą bramę, a nie wszystkie urządzenia w innych VLAN-ach.

Network 9.4: Settings > Zones. Najpierw przejrzyj polityki do Gateway i ustal, gdzie faktycznie działają serwery DNS oraz DHCP.

Zezwól wyłącznie wskazanej stacji administratora na wymagany dostęp lokalny. Przygotuj wyjątki usługowe przed szeroką blokadą z sieci niezaufanych.



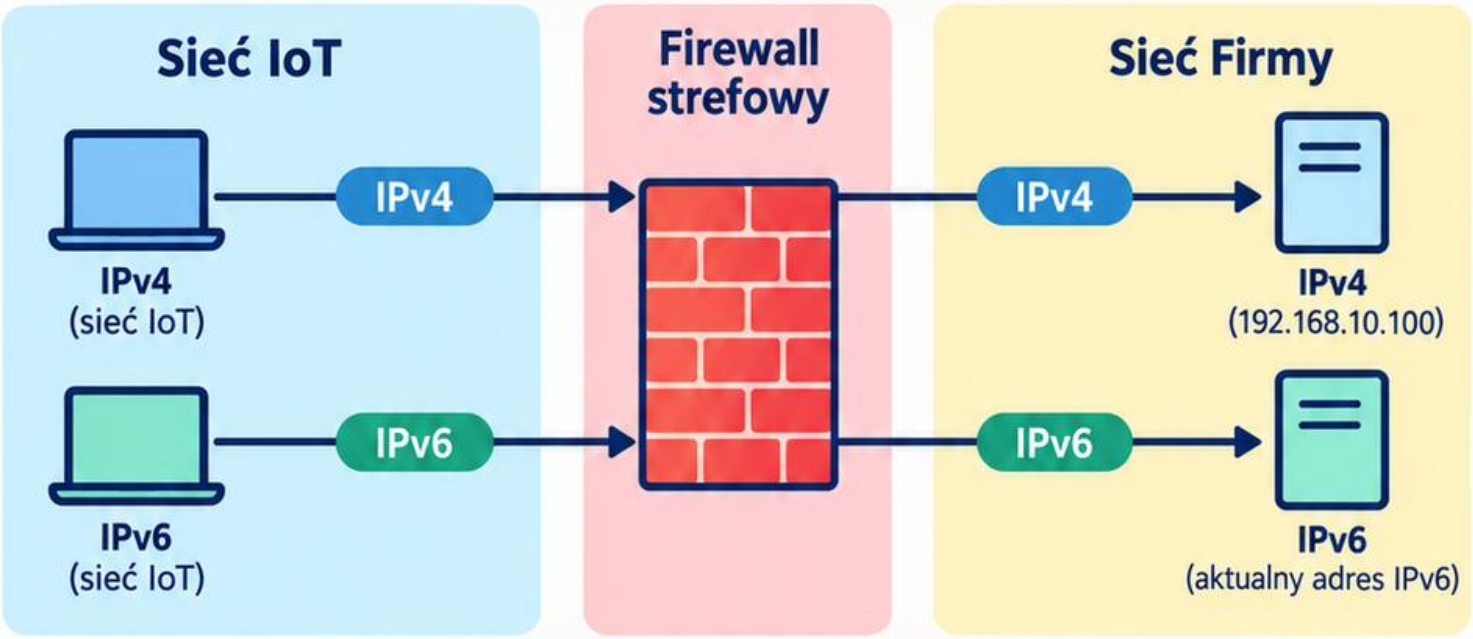
Przykład: gość uzyskuje adres oraz rozwiązuje nazwy przez bramę, ale nie otwiera jej panelu administracyjnego. Administrator zachowuje połączenie przewodowe.

Test: odnowienie dzierżawy, zapytanie DNS i próba panelu gościa muszą dać różne oczekiwane wyniki. Przy utracie usług wyłącz ostatnią blokadę lokalnie.

Źródła: [3]

Uwzględnij IPv4 oraz IPv6

Cel: uniknij obejścia segmentacji drugą rodziną adresów. Reguła ograniczająca wyłącznie IPv4 nie stanowi dowodu blokady połączeń IPv6.



W polityce firewalla strefowego sprawdź **IP Version.** Wybierz obie rodziny, jeśli intencja dostępu jest wspólna, a użyte kryteria to obsługują.

Dla kryteriów adresowych przygotuj odpowiadające sobie **obiekty IPv4 i IPv6.** Nie kopiuj maski IPv4 do obiektu IPv6 ani nie blokuj bezmyślnie ICMPv6.

Przykład: IoT nie inicjuje ruchu do Firmy przez adres 192.168.10.100 ani przez jej aktualny adres IPv6. Mechanizmy IPv6 wymagają osobnej walidacji.

Test: powtórz próbę usługi dla obu rodzin. Gdy IPv6 nie jest wdrożone, zapisz to jawnie i sprawdź brak nieplanowanej konfiguracji klientów.

Źródła: [3]

Ostoja

Filtruj aplikacje świadomie

Ostoja • Mapa 116 • Moduł 8

Cel: ogranicz konkretną kategorię ruchu, jeśli brama i oprogramowanie zapewniają odpowiednią identyfikację. Filtr aplikacji nie zastępuje izolacji adresowej.

W Network 9.4 otwórz Settings > Zones > Create Policy i sprawdź dostępne kryteria App. Wybierz testową sieć zamiast całej firmy.

Ustal oczekiwany efekt biznesowy, na przykład ograniczenie rozrywki na urządzeniach służbowych. Zachowaj osobne wyjątki dla usług używanych podczas pracy.



Zaszyfrowany ruch, zmiany aplikacji i współdzielona infrastruktura mogą komplikować klasyfikację. Przetestuj funkcje aplikacji, a nie sam widok strony głównej.

Test: konto testowe otwiera potrzebną usługę, a wskazana aplikacja jest ograniczona. Przy fałszywej blokadzie zawęź zakres lub wyłącz politykę testową.

Źródła: [3]

Wprowadź IDS oraz IPS etapami

Ostoja • Mapa 117 • Moduł 8

Cel: wykrywać podejrzany ruch bez przypadkowego przerwania pracy. Najpierw ustal wydajność bramy oraz wymagania krytycznych aplikacji.

1 Obserwacja

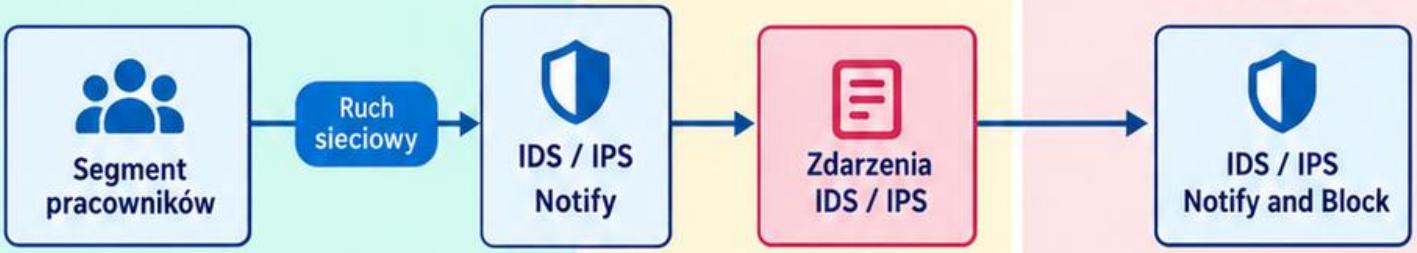
Włącz IPS w trybie Notify.

2 Analiza

Przeanalizuj zdarzenia i oceń ryzyko.

3 Blokowanie

Przejdź do Notify and Block tam, gdzie korzyść uzasadnia ryzyko.



Przykładowe zdarzenie zagrożenia

Przykład: biuro najpierw obserwuje segment pracowników. Każdy alarm wiąże z klientem, czasem i sygnaturą, zanim uzna aplikację za szkodliwą.

Wydajność i opóźnienia



Przepustowość i opóźnienia jako punkt odniesienia

Aktualna dokumentacja wskazuje Settings > CyberSecure > Protection. Włącz Intrusion Prevention, wybierz sieci oraz tryb Notify do obserwacji.

Po analizie zdarzeń przejdź do Notify and Block tam, gdzie korzyść uzasadnia ryzyko. Zachowaj punkt odniesienia dla przepustowości i opóźnień.

Test: sprawdź dziennik detekcji i działanie usług. Fałszywe trafienie obsłuż wąskim wyjątkiem; w razie awarii wróć do Notify zamiast wyłączać segmentację.

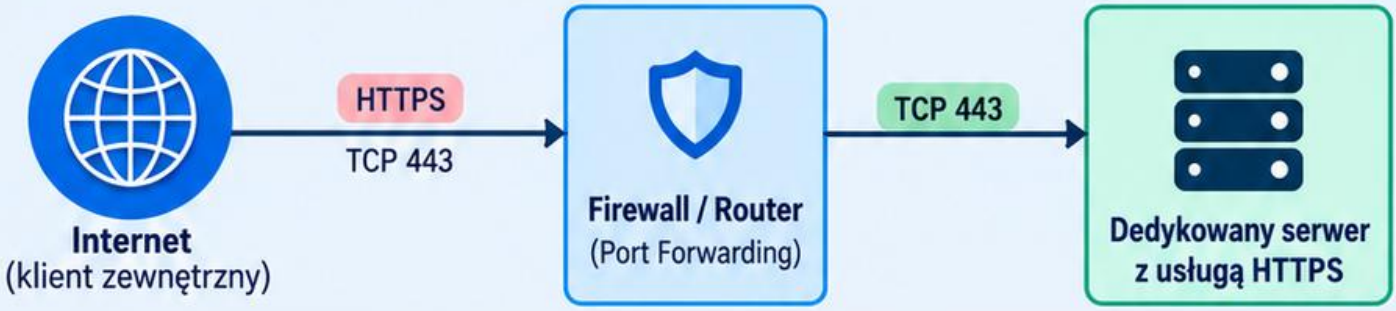
Źródła: [39]

Uzasadnij przekierowanie portu

Cel: opublikuj usługę tylko wtedy, gdy musi być dostępna bez VPN. W dokumentacji decyzji wskaż właściciela i termin ponownego przeglądu.

W aktualnym interfejsie znajdź ustawienia Port Forwarding zgodne z wersją Network. Najpierw potwierdź publiczny adres oraz brak niekontrolowanej podwójnej translacji.

Przykład projektowy: HTTPS do dedykowanego serwera przez TCP 443. Zdefiniuj jeden cel, potrzebny port i dopuszczone źródła, jeśli są znane.



Nie przekierowuj panelu UniFi ani SSH administracyjnego na WAN.
Publiczna usługa wymaga własnego uwierzytelniania, aktualizacji oraz monitorowania.



Test: sprawdź usługę spoza biura i zamknięcie innych portów.
Cofnięcie: wyłącz przekierowanie i potwierdź zewnętrznie, że dostęp faktycznie zniknął.

Źródła: [40]

Przejrzyj automatyczne otwieranie portów

Cel: ustal, czy automatyczne mapowania UPnP są potrzebne i kontrolowane. Każde mapowanie to dodatkowa ścieżka dostępu wymagająca oceny.

Sprawdź ustawienia UPnP w swojej wersji Network oraz aktywne mapowania. Zapisz urządzenie, usługę i uzasadnienie przed zmianą konfiguracji.

Przykład: kamera potrzebuje chmury wychodzącej, lecz użytkownik włączył UPnP bez sprawdzenia instrukcji producenta. Najpierw potwierdź rzeczywiste wymagania.

W biurze preferuj jawnie zatwierdzone usługi i dostęp VPN. Zmianę wykonuj na grupie testowej, aby wykryć zależności telefonii lub aplikacji.

Test: po wyłączeniu zbędnych mapowań sprawdź funkcje urządzeń oraz dostęp z internetu. Nie naprawiaj awarii przez przypadkowe otwieranie szerokiego zakresu portów.

Karta przeglądu mapowań

Urządzenie	Usługa	Uzasadnienie	Data przeglądu
Do ustalenia	Sprawdź wymagania	Do weryfikacji	_____

Źródła: [40]

Sprawdź macierz dostępu

Cel: udowodnij działanie wyjątków i blokad.
Każda próba musi mieć źródło, cel, usługę, oczekiwanie, wynik oraz datę.

Przygotuj klientów w trzech segmentach i stację administratora.
Testuj nowe sesje po każdej zmianie, zachowując działające lokalne połączenie administracyjne.

Firma
(klienci)

IoT
(klienci)

Goście
(klienci)

Administrator
(stacja)

Przykład:
Firma → drukarka TCP 631: działa. IoT → laptop Firmy: blokada. Goście → panel bramy: blokada. Goście → DNS: działa.

Źródło	Cel	Usługa	Oczekiwanie	Wynik	Data
Firma	drukarka	TCP 631	działa	działa	2024-04-12
IoT	laptop Firmy	—	blokada	blokada	2024-04-12
Goście	panel bramy	—	blokada	blokada	2024-04-12
Goście	DNS	—	działa	działa	2024-04-12

Powtórz kluczowe próby po IPv6, jeśli jest wdrożone.
Sprawdź także odnowienie DHCP i rzeczywiste drukowanie; ping nie opisuje wszystkich usług.

Odbiór: wszystkie wyniki odpowiadają macierzy.
Niezgodność oznacza powrót do ostatniej polityki, sprawdzenie kolejności i ponowny test jednego przepływu.

Źródła: [3]

Ostoja • Moduł 9

VPN i routing

Tunel szyfruje połączenie, ale nie zastępuje decyzji o uprawnieniach. Najpierw określ, kto ma korzystać z jakiego zasobu.

W tym module oddzielisz dostęp pojedynczej osoby od połączenia placówek. Sprawdzisz adresację, osiągalność WAN, trasę do celu i drogę powrotną.

Dostęp zdalnej osoby



Połączenie placówek



Przykład: księgowa potrzebuje systemu w biurze, a oddział potrzebuje jednego serwera. Żaden przypadek nie uzasadnia automatycznie dostępu do zarządzania.

Przygotuj rozłączne podsieci lokalne i pulę **VPN**. Profil klienta traktuj jak sekret; w dokumentacji pozostaw nazwę właściciela i datę unieważnienia.

Rezultat: działający tunel z minimalnym dostępem, poprawnym DNS oraz sprawdzonym zachowaniem podczas awarii. Zawsze zachowuj możliwość lokalnego wycofania zmian.

Zapisz wyniki testów odbiorowych.

Źródła: [22], [41], [42]

Wybierz właściwy rodzaj VPN

Cel: dopasuj architekturę do odbiorcy. VPN Server przyjmuje użytkowników, VPN Client łączy bramę z dostawcą, a Site-to-Site spina sieci.

W UniFi Network otwórz sekcję VPN i porównaj dostępne rodzaje dla modelu bramy. Nie zakładaj zgodności na podstawie samego kontrolera.

Przykład: pracownik z laptopem korzysta z WireGuard lub Teleport; druga placówka z własną podsiecią wymaga połączenia między sieciami.

Zapisz liczbę użytkowników, zarządzane urządzenia, wymagane zasoby i sposób odebrania dostępu. Uwzględnij publiczną osiągalność oraz zaufanie do końcówek.

Test: wybrany wariant pozwala rozdzielić tożsamości i ograniczyć zasoby. Jeżeli nie można unieważnić dostępu jednej osobie, zmień projekt przed wdrożeniem.

Kto ma się połączyć?

Pojedynczy użytkownik
(np. pracownik z laptopem)

VPN Server
Użytkownicy zdalni łączą się z bramą za pomocą WireGuard lub Teleport.

Brama łączy się z dostawcą VPN
(np. zewnętrzną usługą)

VPN Client
Bramą nawiązuje połączenie z dostawcą, aby uzyskać dostęp do zasobów.

Dwie placówki z własnymi sieciami
(np. oddziały firmy)

Site-to-Site
Łączy ze sobą sieci dwóch lokalizacji, umożliwiając dostęp między nimi.

Źródła: [22], [43], [41]

Sprawdź publiczną osiągalność

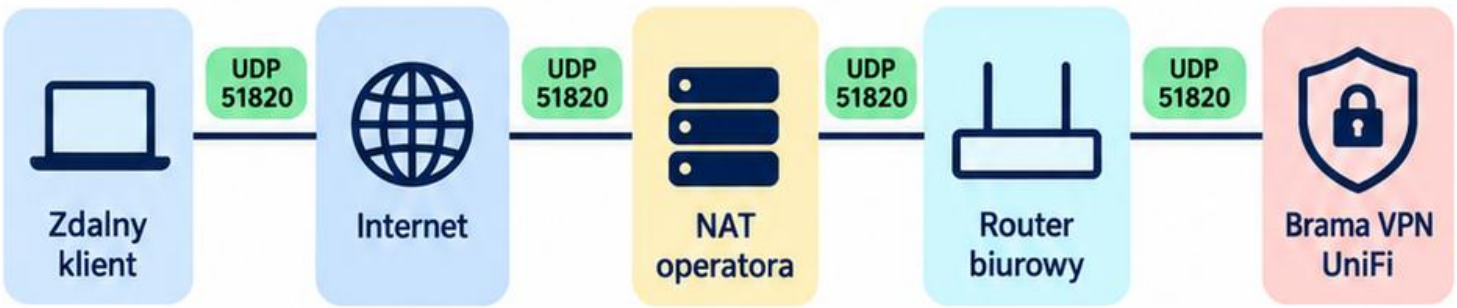
Cel: potwierdź, czy zdalny klient dosięgnie serwera VPN. Adres na WAN może być prywatny albo należeć do sieci operatora.

Porównaj adres WAN z adresem widocznym w internecie. Sprawdź urządzenie operatora, umowę i możliwość otrzymania publicznego adresu.

Dla WireGuard za własnym routerem nadrzędnym potrzebne jest przekierowanie wybranego portu UDP do WAN bramy UniFi. Domyślnie używany jest **51820**.

CGNAT operatora nie zniknie po dodaniu przekierowania w biurze. Uzgodnij publiczny adres lub rozważ zgodny wariant dostępu działający za NAT.

Test: uruchom klienta z sieci komórkowej, sprawdź handshake i usługę. Nie testuj wyłącznie z tego samego LAN-u ani przez otwieranie panelu zarządzania.



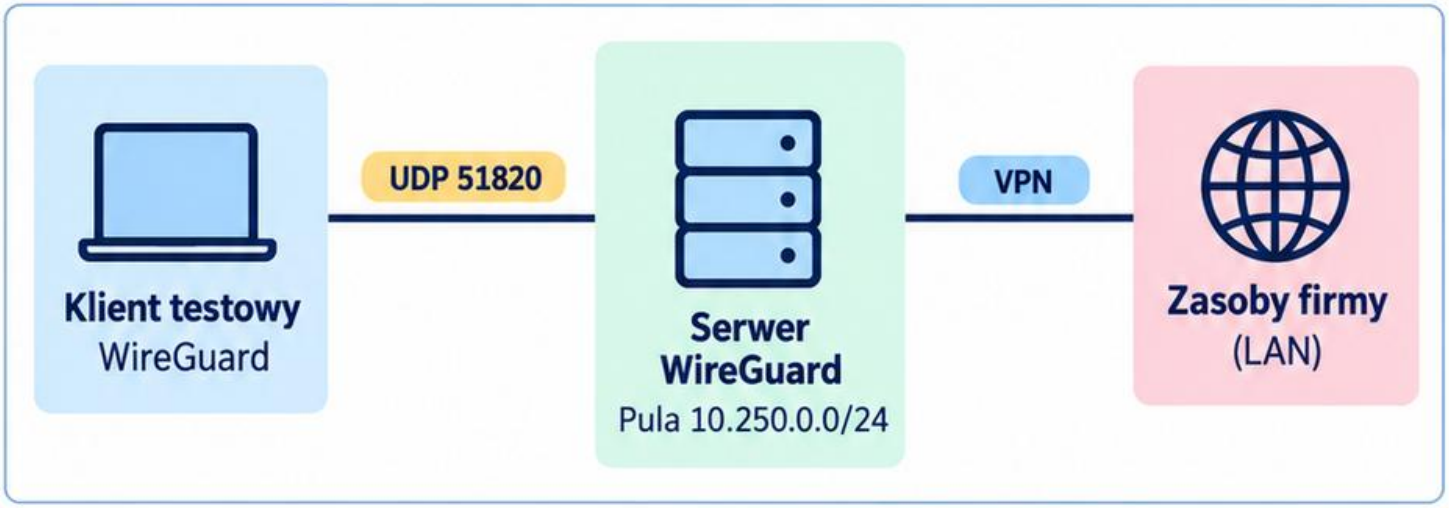
Źródła: [22], [43], [40]

Uruchom serwer WireGuard

1 **Cel:** zapewnij zdalny dostęp na zgodnej bramie UniFi. Przed konfiguracją przygotuj osiągalny adres końcowy i pulę niekolidującą z sieciami.

2 W aplikacji Network otwórz VPN i konfigurację serwera WireGuard. Nazwij go tak, by wskazywał lokalizację i przeznaczenie.

3 Przykład projektu: pula **10.250.0.0/24**, port UDP **51820**. Najpierw sprawdź brak nakładania z LAN-em firmy, oddziałami i typowymi sieciami użytkowników.



4 Dodaj jednego klienta testowego. Dostęp do zasobów ogranicz osobnymi politykami; uruchomiony serwer nie oznacza zaakceptowania wszystkich domyślnych uprawnień VPN.

5 **Test:** połącz się spoza biura, potwierdź handshake i dozwoloną usługę. Cofnięcie: wyłącz serwer testowy oraz usuń niepotrzebne przekierowanie nadrzędnego routera.

Źródła: [22], [3]

Dodaj klienta WireGuard

Ostoja • Mapa 124 • Moduł 9

1 Cel

przypisz dostęp konkretnej osobie i urządzeniu. Współdzielony profil utrudnia ustalenie odpowiedzialności oraz odebranie dostępu pojedynczej końcówce.



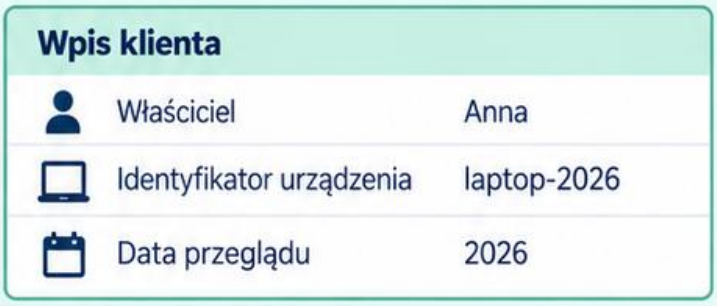
2 Dodaj klienta

W sekcji VPN otwórz serwer WireGuard i dodaj klienta. Nadaj jednoznaczną nazwę, na przykład Anna-laptop-2026, bez wpisywania sekretów.



3 Zarejestruj dane

Zarejestruj właściciela, identyfikator urządzenia i datę przeglądu. Jeden profil przeznacz dla jednej końcówki; kolejna końcówka otrzymuje osobny wpis.



4 Przekaż konfigurację bezpiecznie

Przekaż konfigurację bezpiecznym kanałem osobie uprawnionej. Plik i kod QR mogą zawierać klucz prywatny, więc nie umieszczaj ich w instrukcji odbiorowej.



5 Test i unieważnienie

Test: sprawdź dostęp klienta i możliwość unieważnienia jego wpisu. Po odebraniu uprawnień potwierdź z zewnątrz, że nowa sesja nie powstaje.



Źródła: [22]

Importuj profil bez ujawniania kluczy

Cel: uruchom klienta, zachowując poufność konfiguracji. Osoba posiadająca profil może uzyskać uprawnienia przypisane temu urządzeniu.

1 Pobierz oficjalnego klienta WireGuard na obsługiwany system. Zaimportuj otrzymany plik; na telefonie użyj kodu QR tylko w kontrolowanych warunkach.



2 **Przykład:** Anna importuje profil na służbowym laptopie, następnie zapisuje w rejestrze jedynie nazwę klienta i termin następnego przeglądu.



3 Sprawdź adres końcowy, zakres tras i DNS. Nie wysyłaj profilu do publicznego zgłoszenia, komunikatora grupowego ani repozytorium dokumentacji.

- ✓ Adres końcowy
- ✓ Zakres tras
- ✓ DNS



4 **Test:** po aktywacji sprawdź handshake i usługę firmową. Jeżeli profil został ujawniony, unieważnij go i wydaj nowy; samo usunięcie wiadomości nie wystarcza. Zapisz też datę wydania.



Źródła: [22]

Sprawdź tunel i dostęp

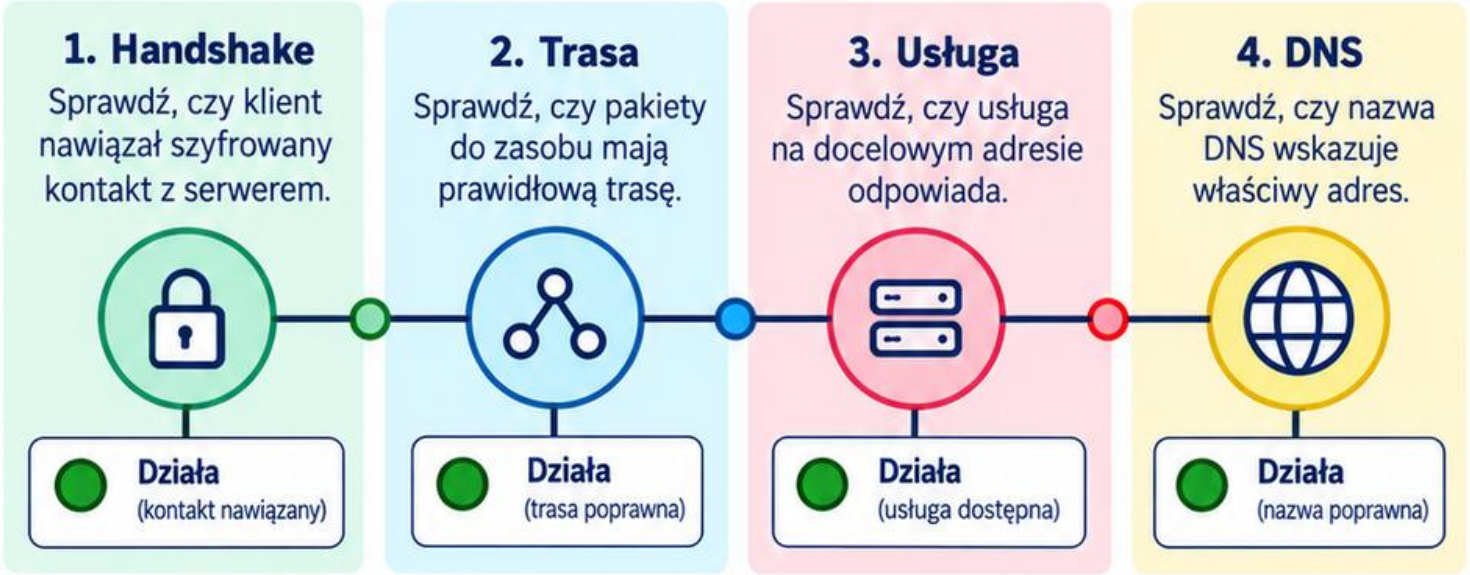
Cel: oddziel działające szyfrowanie od działającej aplikacji. Aktualny handshake potwierdza kontakt końcówek, lecz nie poprawność tras, DNS i polityk.

1. Z sieci komórkowej uruchom klienta. Zanotuj czas próby, adres klienta VPN oraz adres docelowego zasobu. Sprawdź liczniki wysyłania i odbierania.

2. Kolejno przetestuj adres zasobu, jego usługę oraz nazwę DNS. Przykład: najpierw test osiągalności portu TCP 443, potem HTTPS z właściwą nazwą.

3. Gdy handshake działa, a aplikacja nie odpowiada, sprawdź trasę klienta, firewall docelowy, polityki VPN i drogę powrotną. Nie otwieraj całego LAN-u.

4. **Odbiór:** dozwolona aplikacja działa, zarządzanie pozostaje niedostępne. **Cofnięcie:** wyłącz profil klienta testowego, zachowując dowody potrzebne do dalszej diagnozy.



Źródła: [22], [3]

Ogranicz użytkowników VPN strefami

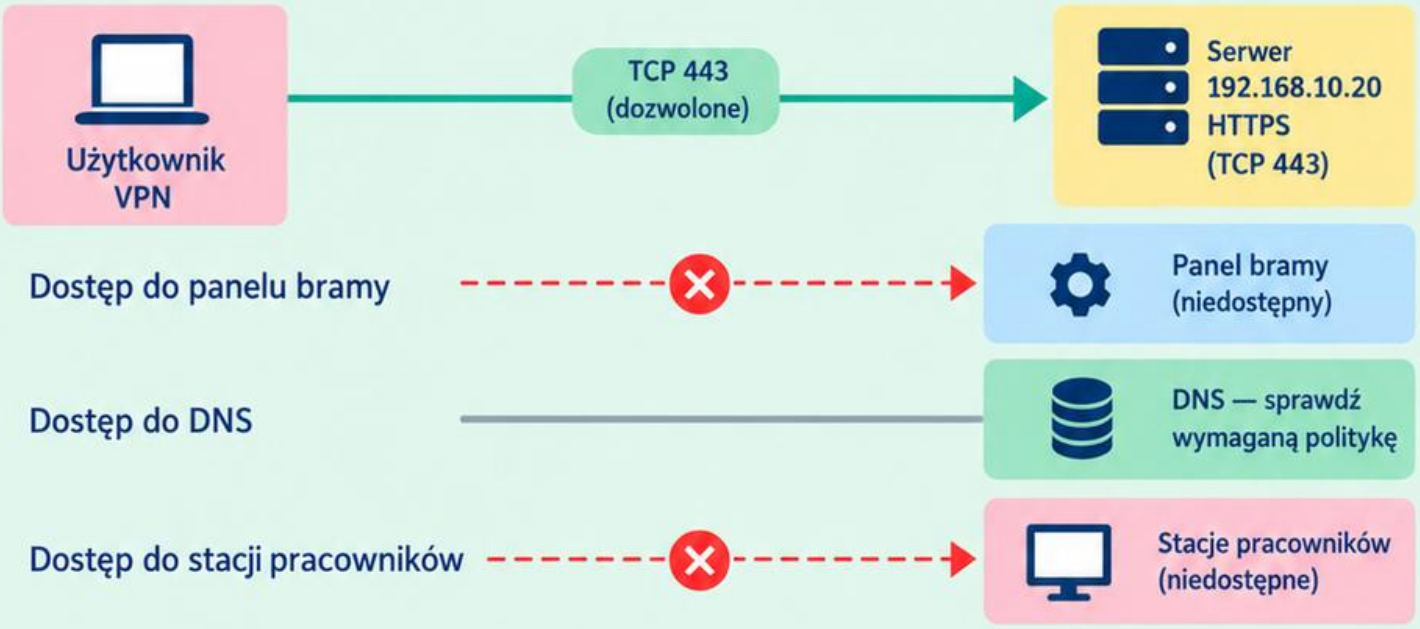
Ostoja • Mapa 127 • Moduł 9

1 **Cel:** zdalny pracownik ma dotrzeć do potrzebnej aplikacji, zachowując brak dostępu do infrastruktury i niepowiązanych segmentów.

2 W Network 9.4 przejrzyj Settings > Zones i relacje VPN do pozostałych stref. Zidentyfikuj interfejs oraz zakres adresów klientów.



3 Dodaj wąskie zezwolenie, na przykład klient testowy → serwer 192.168.10.20, TCP 443. Następnie ogranicz pozostałe nowe połączenia zgodnie z macierzą.



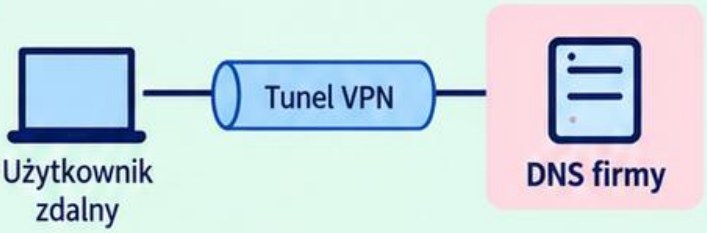
4 Nie zakładaj, że domyślna strefa VPN realizuje minimalne uprawnienia. Sprawdź również dostęp do Gateway, DNS i sposób rozróżniania klientów.

5 **Test:** aplikacja działa, panel bramy i stacje pracowników są niedostępne. Zachowaj oddzielnego administratora lokalnego; przy błędzie wyłącz ostatnią politykę.

Źródła: [3], [22]

Zapewnij DNS użytkownikowi zdalnemu

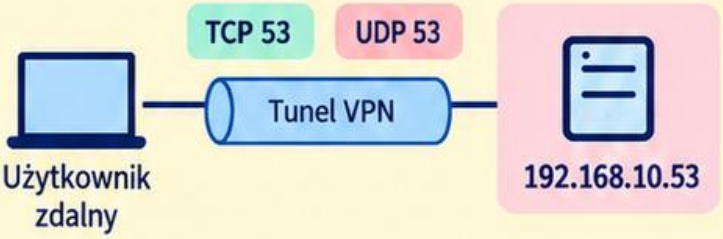
1 **Cel:** nazwy wewnętrzne mają działać przez tunel bez wysyłania ich do przypadkowego resolvera. Najpierw ustal rzeczywisty serwer DNS firmy.



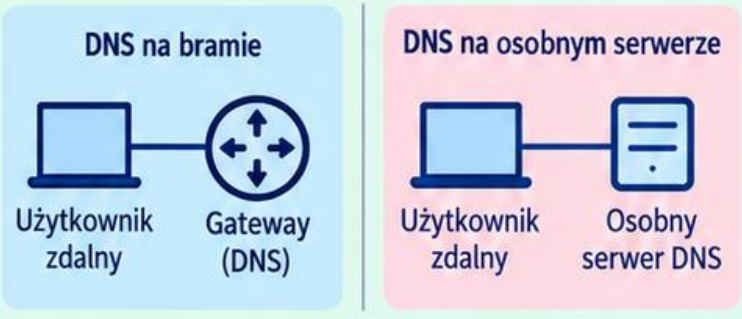
2 **Sprawdź ustawienia DNS w profilu klienta oraz trasę do resolvera.** Sam wpis adresu DNS nie zapewnia jego osiągalności ani odpowiednich uprawnień.



3 **Przykład projektu:** resolver 192.168.10.53 odpowiada użytkownikom VPN. Zezwól na TCP i UDP 53 do tego adresu, jeśli faktycznie świadczy usługę.



4 **Jeśli DNS działa na bramie**, oceniaj relację VPN → Gateway. Jeśli działa na osobnym serwerze, polityka musi obejmować jego sieć.



5 **Test:** odpytaj wskazany resolver o nazwę wewnętrzną i publiczną. Przy błędzie porównaj wynik po adresie IP; przywróć poprzedni profil po zakończeniu próby.



Źródła: [22], [3]

Wybierz tunel dzielony lub pełny

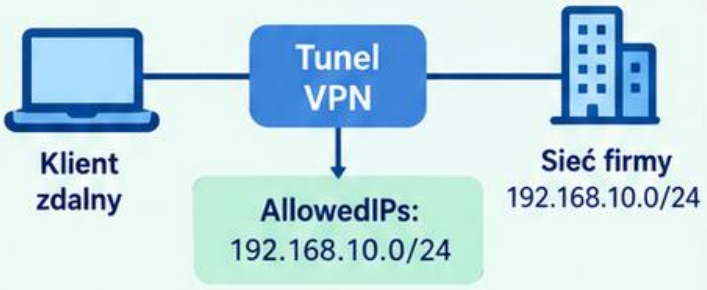
Cel: zdecyduj, czy przez biuro przechodzi tylko ruch firmowy, czy cały ruch internetowy klienta. Decyzja wpływa na prywatność i przepustowość.

Sprawdź zakres tras klienta oraz jego AllowedIPs. Tunel dzielony obejmuje potrzebne prefiksy firmowe; pełny wymaga obsługi domyślnej trasy.

Przykład: zdalna księgowa potrzebuje 192.168.10.0/24. Dodanie 0.0.0.0/0 obejmuje cały IPv4; ruch IPv6 wymaga osobnej świadomej decyzji.

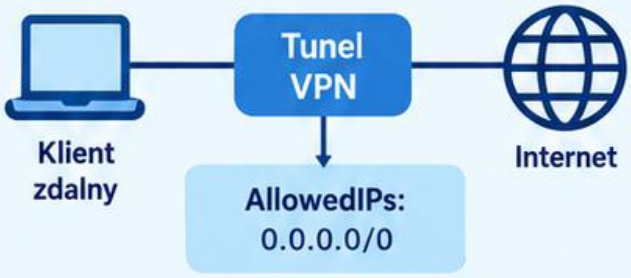
Pełny tunel musi mieć poprawne wyjście internetowe i DNS. Nie obiecuj ochrony całego ruchu, jeśli druga rodzina adresów omija tunel.

Tunel dzielony



IPv6: decyzja osobno
Ruch IPv6 nie jest objęty, jeśli nie dodasz odpowiednich tras.

Tunel pełny



IPv6: decyzja osobno
Aby objąć cały ruch IPv6, dodaj odpowiednie trasy.

Test: sprawdź trasę firmową, publiczny adres wyjściowy i zachowanie po rozłączeniu. **Cofnięcie:** przywróć zatwierdzony zakres tras klienta i ponów test DNS.

Źródła: [22], [42]

Użyj Teleport na zgodnym sprzęcie

Ostoja • Mapa 130 • Moduł 9

1 | **Cel:** uprość dostęp pojedynczemu urządzeniu bez ręcznej dystrybucji profilu WireGuard. Wymagana jest obsługiwana brama działająca z UniFi OS.

2 | Otwórz **Network Settings > VPN** i włącz **Teleport**. Wygeneruj zaproszenie dla konkretnego odbiorcy; WiFiman obsługuje je na urządzeniu końcowym.



3 | **Zaproszenie wygasa po 24 godzinach** i może być wykorzystywane przez jedno urządzenie jednocześnie. Przekazuj je tak samo ostrożnie jak profil VPN.



4 | **Teleport** może działać za NAT; w niektórych warunkach potrzebuje IPv6 na WAN. Nie oznacza to konieczności uruchamiania IPv6 w LAN-ie.



5 | **Test:** sprawdź połączenie spoza biura i ograniczenia zasobów. Nieprzyjęte zaproszenie odwołaj w historii; przyjęty dostęp unieważnij przez odpowiedniego klienta.



Źródła: [43]

Zaplanuj rozłączne podsieci placówek

Cel: obie placówki muszą jednoznacznie rozpoznawać, gdzie znajduje się adres docelowy. Powtarzanie 192.168.1.0/24 zwykle komplikuje zwykły routing.

Zbierz wszystkie LAN-y, pule VPN i trasy z obu stron. Porównaj całe prefiksy, a nie tylko adresy bram lub numery VLAN.

Przykład projektu:

Kraków 192.168.10.0/24, Poznań 192.168.110.0/24, użytkownicy zdalni 10.250.0.0/24. Każdy zakres ma osobną rolę.



Wyznacz jedynie sieci wymagające komunikacji. Numery VLAN mogą się powtarzać między odległymi placówkami, lecz ich trasowane podsieci pozostają rozłączne.

Test: tabela tras wskazuje jednoznaczną drogę do każdego prefiksu. Jeśli wykryjesz nakładanie, popraw adresację przed zestawieniem tunelu zamiast przypadkowo dodawać NAT.

Sprawdź również maski istniejących tras.

Źródła: [41], [44]

Zestaw zgodny tunel IPsec

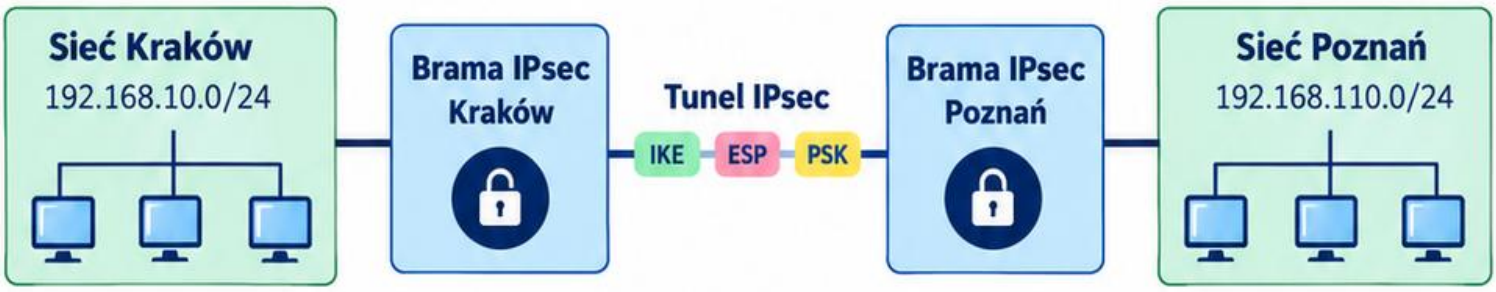
Ostoja • Mapa 132 • Moduł 9

1. **Cel:** połącz sieci, także przy bramie innego producenta. Najpierw uzgodnij parametry obu końców i zakres uprawnionych zasobów.

2. W sekcji VPN aplikacji Network wybierz konfigurację Site-to-Site IPsec. Porównaj adresy końców, tryb route-based lub policy-based oraz ustawienia uwierzytelniania.

3. Po obu stronach uzgodnij IKE, szyfrowanie, integralność, DH, PFS i czasy życia. Zgodność konfiguracji jest warunkiem działania; nie kopiuj przypadkowych ustawień domyślnych.

4. **Przykład:** Kraków 192.168.10.0/24 ↔ Poznań 192.168.110.0/24.
W policy-based selektory muszą odpowiadać sobie; w route-based sprawdź trasy i firewall.



Parametry IPsec – Kraków

IKE:	uzgodnione ustawienia
Szyfrowanie:	uzgodnione ustawienia
Integralność:	uzgodnione ustawienia
DH:	uzgodnione ustawienia
PFS:	uzgodnione ustawienia
Czasy życia:	uzgodnione ustawienia
Tryb:	route-based lub policy-based
Selektory / Trasy:	zgodnie z uzgodnieniem

PSK



Przechowuj w menedżerze sekretów.

Parametry IPsec – Poznań

IKE:	uzgodnione ustawienia
Szyfrowanie:	uzgodnione ustawienia
Integralność:	uzgodnione ustawienia
DH:	uzgodnione ustawienia
PFS:	uzgodnione ustawienia
Czasy życia:	uzgodnione ustawienia
Tryb:	route-based lub policy-based
Selektory / Trasy:	zgodnie z uzgodnieniem

5. **Test:** zweryfikuj zestawienie i aplikację w obu kierunkach. PSK przechowuj w menedżerze sekretów; cofnięcie: wyłącz tunel testowy i usuń jego zbędne trasy.

Źródła: [41]

Oceń SD-WAN i Site Magic

Ostoja • Mapa 133 • Moduł 9

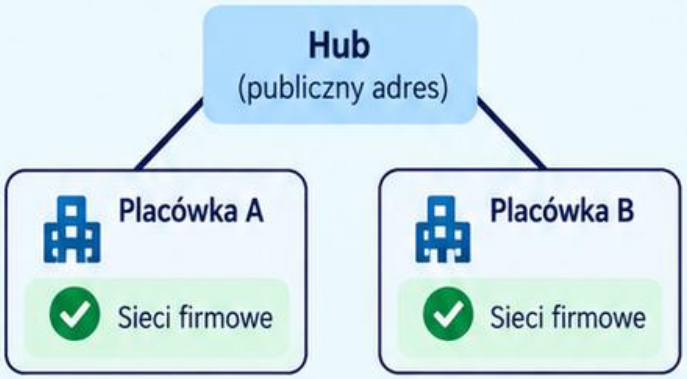
Cel: wybierz automatyzowane połączenia zgodnych bram UniFi. Dostępność zależy od topologii, modelu oraz sposobu zarządzania urządzeniami.

Dla **Hub & Spoke** dokumentacja wymaga Network 9.0.108+, bramy 4.1.3+ i zgodnego huba z publicznym adresem. Sprawdź listę modeli.

W Site Manager otwórz **Settings > SD-WAN.** Wspólny właściciel konta albo odpowiednie zarządzanie Fabric stanowi warunek organizacyjny.

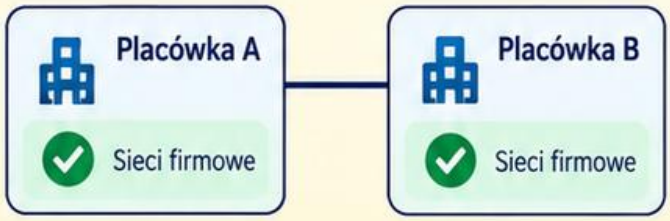
Hub & Spoke

Zgodne połączenia



Mesh

Zgodne połączenia



Nie dołączaj do wymiany

Goście

Zarządzanie

Przykład: dwie placówki z rozłącznymi podsieciami udostępniają wyłącznie sieci firmowe. Nie dołączaj automatycznie Gości ani Zarządzania do wymiany.

Test: sprawdź reklamowane prefiksy i polityki w obu lokalizacjach. Mesh wymaga rozłącznych podsieci; nie przenoś możliwości NAT z *Hub* & Spoke na Mesh.

Źródła: [44]

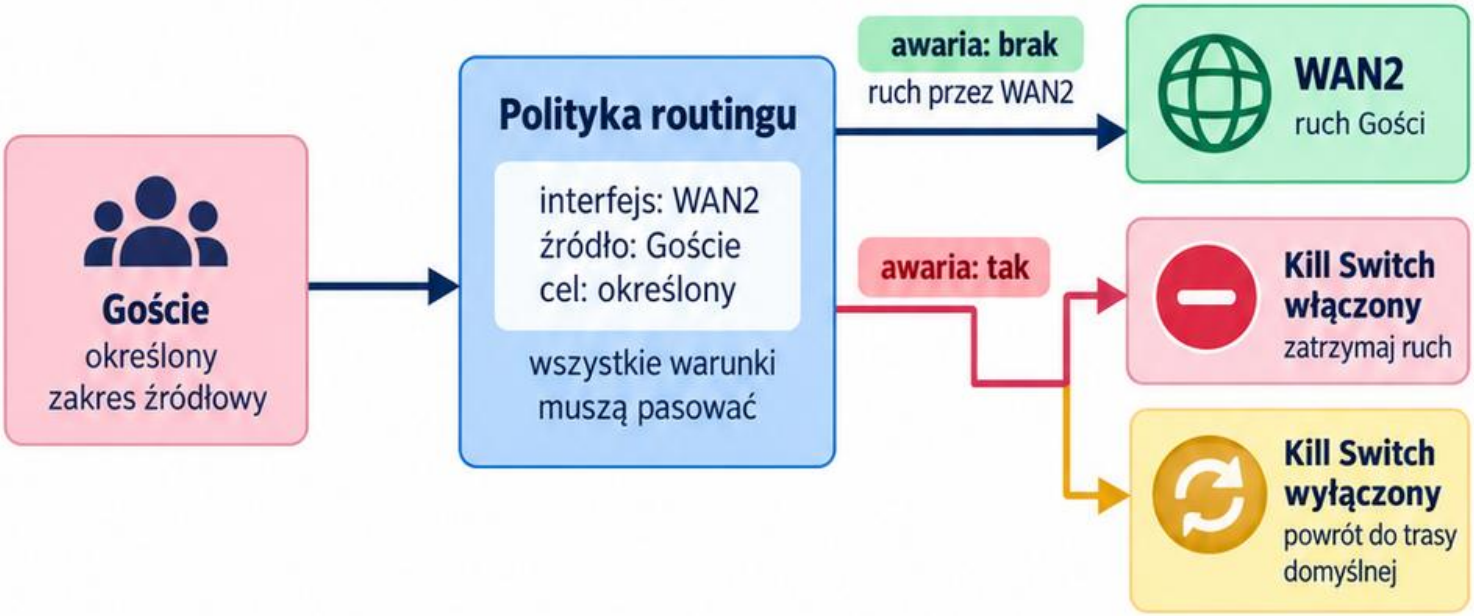
Skieruj ruch według polityki

Ostoja • Mapa 134 • Moduł 9

Cel: wybierz wyjście dla określonego źródła i celu, na przykład WAN2 dla Gości. Routing nie nadaje uprawnień do usługi.

Network 9.4: Settings > Policy Table > Create New Policy > Route.
W 9.3: Settings > Policy Engine > Policy-Based Routes > Create Route.

Wskaż interfejs, zakres źródłowy i docelowy. Wszystkie wybrane warunki muszą pasować. Zacznij od jednego klienta i obserwuj rzeczywistą trasę.



Przykład: Goście korzystają z WAN2. Kill Switch włączony zatrzymuje ruch po awarii wybranego interfejsu; wyłączony dopuszcza powrót do trasy domyślnej.

Test: sprawdź publiczny adres wyjściowy, a potem kontrolowaną awarię.
Cofnięcie: wyłącz konkretną trasę polityki i potwierdź przywrócenie zatwierdzonego wyjścia.

Źródła: [42]

Przetestuj awarię trasy VPN

Ostoja • Mapa 135 • Moduł 9

1. **Cel:** ustal, czy utrata tunelu zatrzymuje dane wrażliwe, czy dopuszcza zatwierdzoną drogę zapasową. Zachowanie musi wynikać z wymagań.

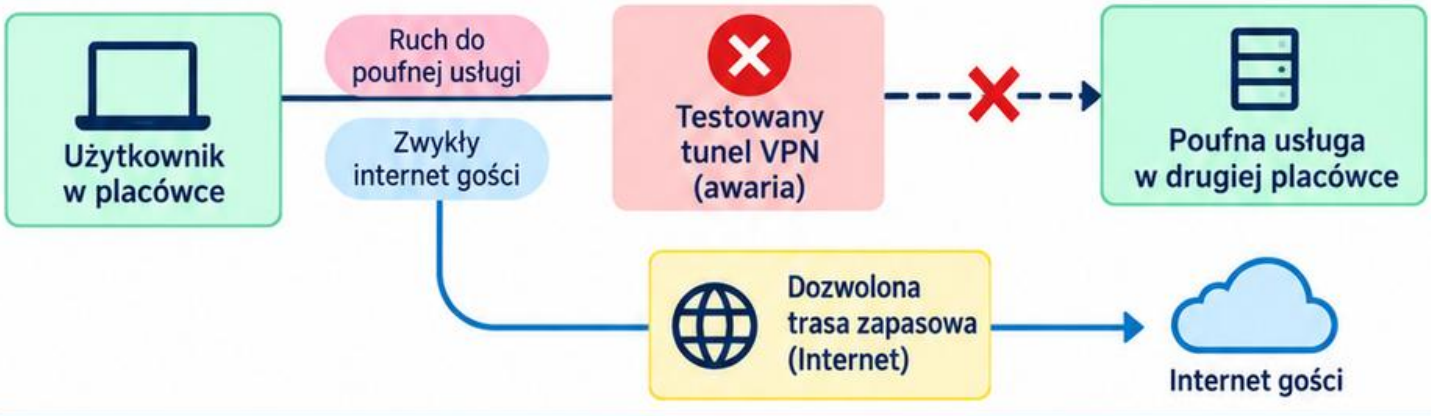
2. Przejrzyj trasę polityki i stan Kill Switch: Zaplanuj krótkie okno testowe, lokalnego administratora oraz obserwatora w drugiej placówce.

3. **Przykład:** ruch do poufnej usługi przez VPN powinien zatrzymać się po awarii. Zwykły internet gości może wrócić przez dozwoloną trasę zapasową.

4. Przerwij wyłącznie testowany tunel lub interfejs, a następnie sprawdź aplikację, adres wyjściowy i logi. Nie odłączaj równocześnie wszystkich łączy.

5. **Odbiór:** awaria i powrót dają oczekiwany wynik. Zapisz zmierzony czas wznowienia; nie obiecuj zerowej przerwy dla każdej topologii. Przywróć pierwotny stan.

Scenariusz testu



Oś czasu testu



Źródła: [42], [44]

Utrzymanie i odbiór

Działająca sieć potrzebuje punktu odniesienia, właściciela i sprawdzonej drogi odtworzenia. Sam zielony status urządzeń nie stanowi kompletnego odbioru.



W tym module połączysz obserwację topologii, zdarzeń i wydajności z kopiami konfiguracji. Każdy pomiar opisuj miejscem, czasem i użytym urządzeniem.



Przykład: biuro działa poprawnie rano, lecz po południu użytkownicy zgłaszają opóźnienia. Porównanie portów, radia i WAN pozwala zawęzić przyczynę.



Przekaż administratorowi mapę VLAN-ów, macierz dostępu, wyniki testów i procedurę odtworzenia. Sekrety pozostają w osobnym, kontrolowanym magazynie.



Rezultat: uzgodniony odbiór oraz rutyna przeglądu. Przed aktualizacją sprawdzaj backup, wymagania wersji i dostęp lokalny; po zmianie ponawiaj testy krytycznych usług.



Zapisz wyniki testów odbiorowych.

Źródła: [8], [45], [23]

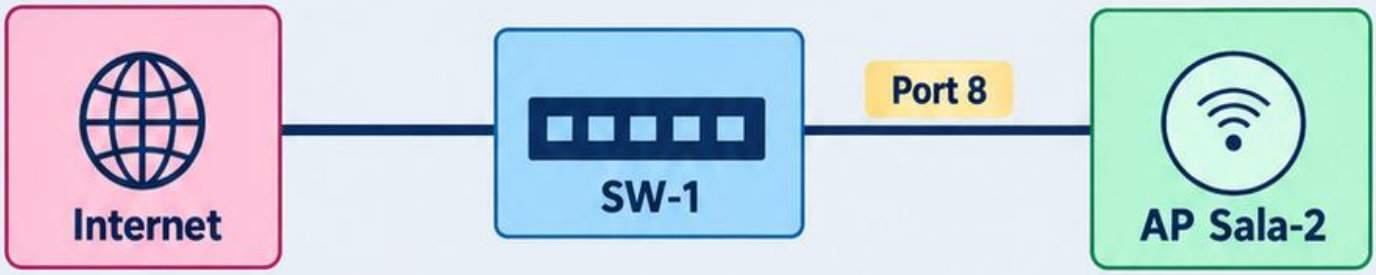
Czytaj topologię i status

Ostoja • Mapa 136 • Moduł 10

Cel: ustal, gdzie znajduje się urządzenie i którędy przepływa jego ruch. Mapa logiczna wymaga porównania z rzeczywistymi przewodami.

W aplikacji **Network** otwórz **Topology.** Wybierz urządzenie, zapisz jego nadrzędny przełącznik, port oraz adres; porównaj z ewidencją instalacji.

Przykład



Przykład: AP Sala-2 jest widoczny pod przełącznikiem SW-1, port 8. Sprawdź oznaczenie przewodu i konfigurację tego portu przed zmianą VLAN-u.

Elementy innych producentów albo niepełna widoczność mogą uprościć rysunek. Nie traktuj każdej narysowanej relacji jako niezależnego pomiaru fizycznego.

Test: identyfikator urządzenia, port i lokalizacja zgadzają się w dokumentacji. Rozbieżność popraw w ewidencji po sprawdzeniu; nie restartuj urządzeń tylko dla uporządkowania widoku.

Źródła: [1]

Znajdź klienta po adresie

Cel: przypisz zgłoszenie do właściwego urządzenia, a nie do niepewnej nazwy hosta. Adres dynamiczny mógł zmienić właściciela.

Otwórz **Client Devices** i odszukaj klienta po IP lub MAC. Zapisz czas obserwacji, sieć, punkt podłączenia i aktualny adres.

Wyszukiwanie klienta

IP: 192.168.10.120

lub

MAC: XX:XX:XX:XX:XX:XX

Wyszukaj

Karta klienta

- **Użytkownik** Nazwa / alias
- **MAC** XX:XX:XX:XX:XX:XX
- **VLAN** Nazwa sieci
- **Czas obserwacji** RRRR-MM-DD GG:MM:SS
- **Punkt podłączenia** Port / AP
- **Aktualny adres IP** 192.168.10.120

Przykład: zgłoszenie dotyczy 192.168.10.120. Porównaj MAC z urządzeniem użytkownika oraz dzierżawą DHCP, zanim wykonasz rezerwację lub blokadę.

Losowe adresy MAC telefonów mogą tworzyć odrębne wpisy. Rozróżniaj urządzenia aktywne i historyczne; sam alias nie jest wystarczającym identyfikatorem.

Test: użytkownik potwierdza urządzenie, a port lub AP odpowiada jego lokalizacji. Zachowaj dowód bez haseł i danych niezwiązanych ze zgłoszeniem.

Zapisz także numer zgłoszenia.

Źródła: [45], [30]

Ostoja

Ostoja • Mapa 138 • Moduł 10

Zbuduj oś zdarzeń

Cel: określ, co wydarzyło się przed awarią.
Kolejność zdarzeń pomaga odróżnić przyczynę od skutku i uniknąć przypadkowych restartów.

W aktualnym Network kliknij Logs w lewym pasku. Filtruj czas, kategorię oraz klienta lub urządzenie, którego dotyczy zgłoszenie.

Przykład: 14:03 zmiana konfiguracji portu, 14:04 rozłączenie AP, 14:05 utrata klientów. Najpierw sprawdź port, zamiast wymieniać wszystkie punkty dostępowe.



Zapisz strefę czasową i porównaj czas urządzeń. Brak wpisu nie dowodzi braku zdarzenia, jeśli retencja lub zakres logowania były niewystarczające.

Test: jedna hipoteza odpowiada kolejności i miejscu wystąpienia awarii. Wycofaj powiązaną zmianę w kontrolowanym oknie i sprawdź, czy objaw ustępuje.

Źródła: [45]

Sprawdź obciążenie portów

Cel: znajdź wąskie gardło przewodowej części sieci. Porównuj negocjowaną szybkość, obciążenie i błędy w tym samym przedziale czasu.

W Devices wybierz przełącznik i właściwy port. Zidentyfikuj podłączone urządzenie oraz uplink; sprawdź dostępne statystyki i zdarzenia portu.

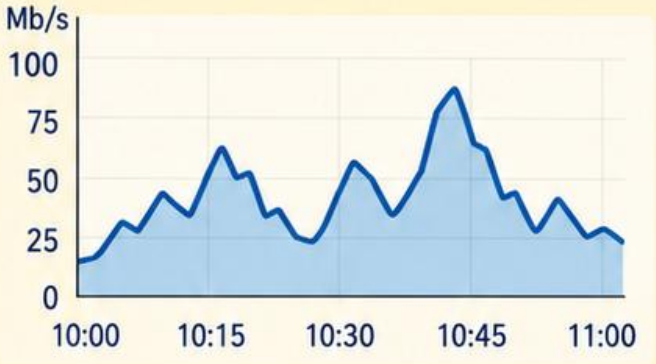
Przykład: stanowisko osiąga około 90 Mb/s, a łącze negocjuje 100 Mb/s. Sprawdź przewód, złącza i możliwości obu końców przed strojeniem Wi-Fi.



Obciążenie portu (stanowisko)



Obciążenie uplinku (wspólne)



Wysokie wykorzystanie uplinku może ograniczać wiele stanowisk jednocześnie. Sam chwilowy szczyt nie potwierdza przeciążenia; porównaj kilka prób oraz godziny zgłoszeń.

Test: po wymianie sprawdzonego przewodu powtórz pomiar tą samą metodą. Nie wymuszaj duplexu bez ustalenia przyczyny; zachowaj poprzednią konfigurację portu.

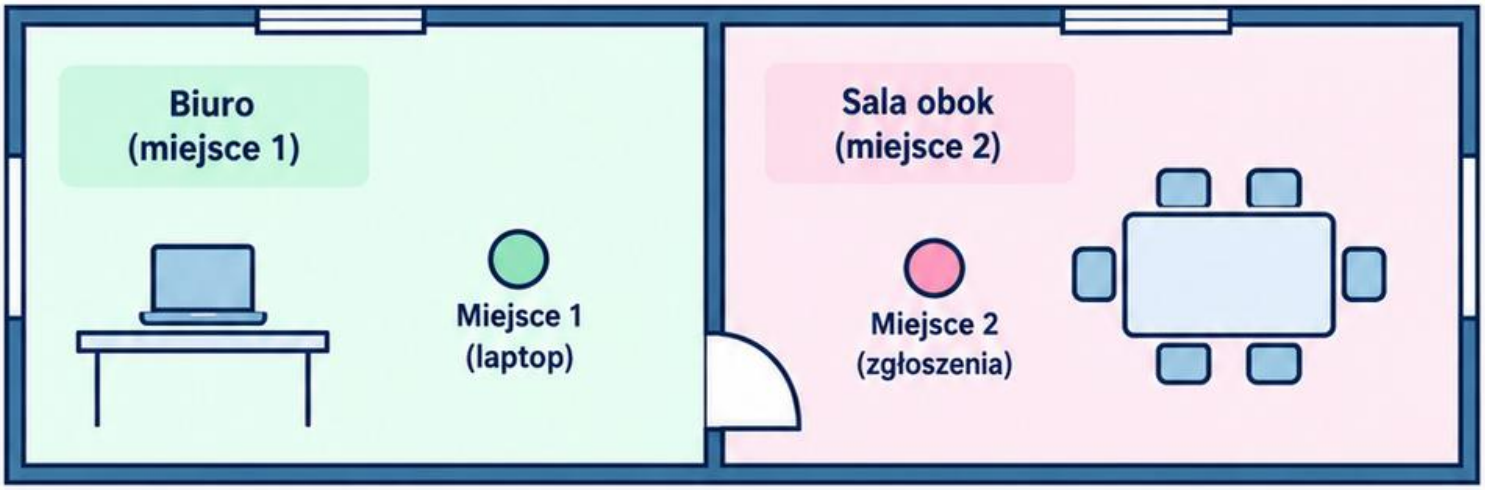
Źródła: [45], [30]

Zmierz radio w miejscu pracy

Cel: oddziel słaby sygnał od zatłoczonego kanału. Dwa miejsca o podobnej sile sygnału mogą dawać zupełnie różną jakość pracy.

W widoku AP sprawdź dostępne metryki radia; na telefonie z WiFiman Mobile porównaj **Signal** i pomiary w miejscach zgłoszeń.

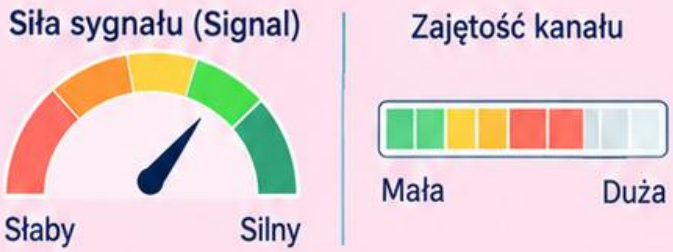
Przykład projektu: laptop przy biurku działa poprawnie, lecz sala obok ma niestabilne połączenie. Zapisz AP, pasmo, kanał, szerokość i czas pomiaru.



Miejsce 1 – wynik pomiaru



Miejsce 2 – wynik pomiaru



Porównaj zajętość kanału, powtórzenia transmisji i zmiany opóźnienia. Nie zwiększaj automatycznie mocy ani szerokości, ponieważ może to pogorszyć współdzielenie pasma.

Test: jedna zmiana na raz, ten sam klient i ta sama trasa. Zachowaj wynik przed zmianą; jeśli poprawy nie ma, przywróć ustawienie.

Źródła: [46], [30]

Diagnozuj za pomocą WiFiman

Ostoja • Mapa 141 • Moduł 10

Cel: zbierz porównywalne pomiary telefonu w sieci użytkownika. Nie przenoś możliwości aplikacji mobilnej na wersję komputerową.

W **WiFiman Mobile** użyj Speed do prób przepustowości i Signal do obserwacji połączenia. Część metryk wymaga zgodnej bramy UniFi.



Speed
do prób przepustowości

Signal
do obserwacji połączenia

WiFiman Desktop obsługuje wykrywanie urządzeń UniFi i Teleport. Nie zakładaj, że udostępnia mobilne pomiary radia czy mapowanie zasięgu.



Wykrywanie urządzeń UniFi

Teleport

Przykład: zmierz opóźnienie przy recepcji, sali spotkań i stanowisku pracy. Zapisz model telefonu, AP, pasmo oraz godzinę każdej próby.

1. Recepcja



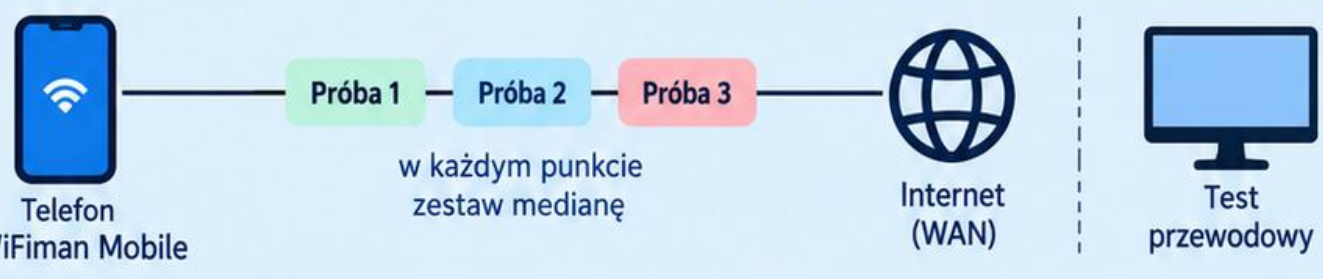
2. Sala spotkań



3. Stanowisko pracy



Test: wykonaj trzy porównywalne próby w każdym punkcie i zestaw medianę. Pomiar internetu zależy również od WAN; porównaj go z testem przewodowym.



Źródła: [46]

Oddziel problem DNS od łączności

Cel: ustal, czy nie działa rozwiązywanie nazwy, droga do zasobu, czy sama usługa. Każda z tych sytuacji wymaga innego działania.



Na kliencie sprawdź adres IP, bramę i otrzymany DNS. Następnie porównaj zapytanie do znanego resolvera oraz dostęp do zatwierdzonej usługi.

Przykład: serwer odpowiada po adresie, ale nazwa nie istnieje. Sprawdź rekord i wybrany DNS zamiast restartować przełącznik lub zmieniać kanały.

Samo niepowodzenie pinga nie dowodzi braku internetu, ponieważ ICMP może być filtrowany. Zastosuj test portu lub aplikacji właściwy dla zgłoszenia.

Test: nazwa daje poprawny adres, aplikacja działa, a klient używa zatwierdzonego resolvera. Cofnij tymczasowy DNS po diagnozie i odnowieniu ustawień klienta.

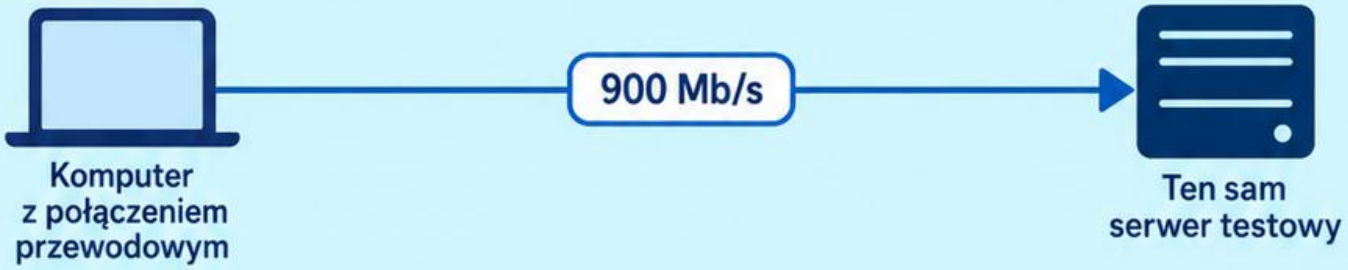
Źródła: [30], [3]

Porównaj pomiar przewodowy i Wi-Fi

Cel: znajdź etap ograniczający wydajność. Wynik bez informacji o kliencie, połączeniu i serwerze testowym trudno porównać z kolejnym pomiarem.

Wykonaj test przewodowy i bezprzewodowy do tego samego celu. Wyłącz dodatkowe transfery testowego komputera i sprawdź negocjowaną szybkość przewodu.

Test przewodowy



Test bezprzewodowy



Przykład: przewód daje 900 Mb/s, a telefon 280 Mb/s. Sprawdź możliwości telefonu, pasmo i szerokość kanału przed uznaniem wyniku za awarię.

Powtórz trzy próby, zapisując medianę oraz opóźnienie. Oddziel test lokalny od internetowego, bo drugi dodatkowo obejmuje operatora i zewnętrzny serwer.

Odbiór: uzyskany wynik spełnia uzgodnione wymaganie dla danego stanowiska. Zmiana konfiguracji jest uzasadniona konkretnym ograniczeniem, a nie samą różnicą między urządzeniami.

Źródła: [46], [30]

Skonfiguruj użyteczne alarmy

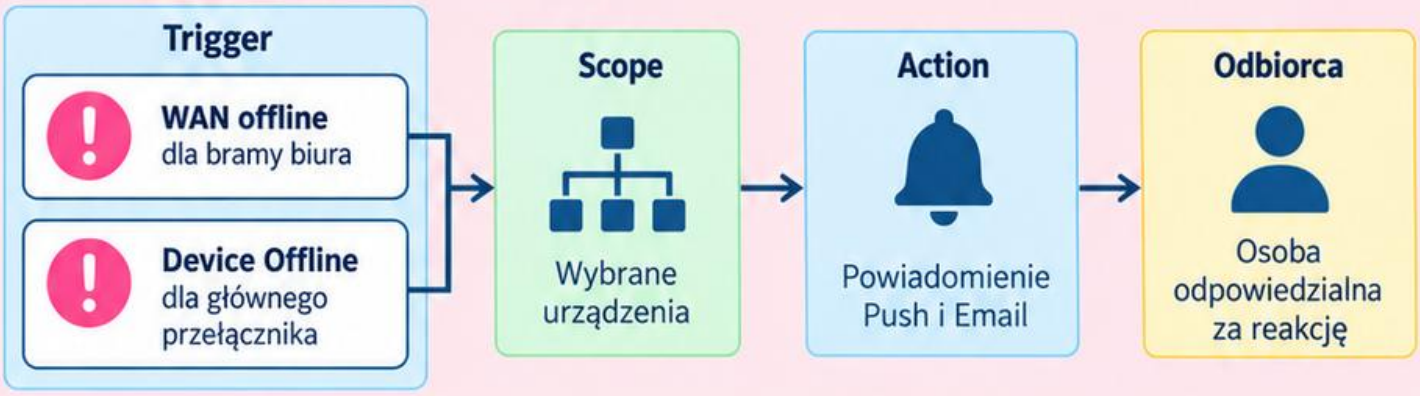
Ostoja • Mapa 144 • Moduł 10

Cel: administrator ma dowiedzieć się o istotnej awarii, bez powtarzających się powiadomień o każdym zwykłym zdarzeniu klienta.

Alarm Manager jest dostępny w Network 9.3+. Otwórz go z lewego paska, wybierz **Create Alarm**, następnie **Trigger**, **Scope** i **Action**.

Przykład: WAN offline dla bramy biura oraz Device Offline dla głównego przełącznika. Skieruj powiadomienie do osoby odpowiedzialnej za reakcję.

Przykład konfiguracji alarmów



Sprawdź My Notifications: Push i Email są ustawiane osobno. Jeżeli wyzwalacz na to pozwala, ogranicz powtórzenia i uwzględnij okna serwisowe.

Test powiadomienia (po potwierdzeniu)



Test: wywołaj bezpieczne zdarzenie próbne i sprawdź odbiór przez właściwą osobę. Po teście usuń alarm próbny; brak wiadomości wymaga sprawdzenia dostarczania.

Źródła: [47]

Przekaż plik wsparcia bezpiecznie

Ostoja • Mapa 145 • Moduł 10

Cel: dostarcz materiał diagnostyczny, ograniczając ujawnienie informacji o firmie. Plik wsparcia nie jest dokumentem przeznaczonym do publicznego udostępniania.

Dla konsoli:
w Site Manager wybierz Management, następnie Support File > Download. Ścieżkę porównaj z dokumentacją rodzaju hosta.

Dla urządzenia:
Network > Devices > wybrane urządzenie > Settings > Manage > Generate Support File, następnie Download Support File.



Nie udostępniaj publicznie
Plik wsparcia nie jest dokumentem przeznaczonym do publicznego udostępniania.

Przykład:
zgłoszenie zawiera czas awarii, wersje i identyfikator urządzenia. Do zgłoszenia nie dołączaj profilu VPN, kluczy prywatnych ani haseł.

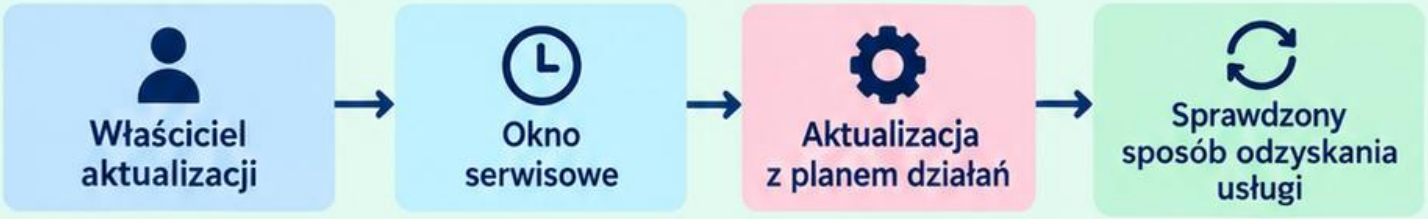
Test:
sprawdź adresata i zakres pliku przed wysłaniem prywatnym kanałem wsparcia. Zachowaj kopię zgodnie z ustaloną retencją i usuń zbędne materiały.

Źródła: [48]

Zaplanuj okno serwisowe

Ostoja • Mapa 146 • Moduł 10

1 **Cel:** aktualizacja ma mieć właściciela, czas i sprawdzony sposób odzyskania usługi. Nie rozpoczynaj od jednoczesnej aktualizacji całej infrastruktury.



2 **Aktualne ustawienia konsoli i aplikacji:** Settings > Control Plane > Updates. Aktualizacje urządzeń są zarządzane w odpowiedniej aplikacji; sprawdź informacje o wydaniu.



3 **Przykład:** najpierw testowy AP, potem pozostałe AP-y, następnie kolejny zatwierdzony etap. Harmonogram dopasuj do zależności i zaleceń konkretnego wydania.



4 **Przed zmianą** pobierz backup i zapewnij lokalny dostęp. Zapisz wersję wyjściową, kryterium przerwania oraz listę usług sprawdzanych po każdym etapie.



5 **Test:** DHCP, DNS, aplikacja firmowa i dostęp administracyjny działają po zmianie. Backup odtwarza konfigurację; nie zakładaj, że automatycznie cofa firmware.



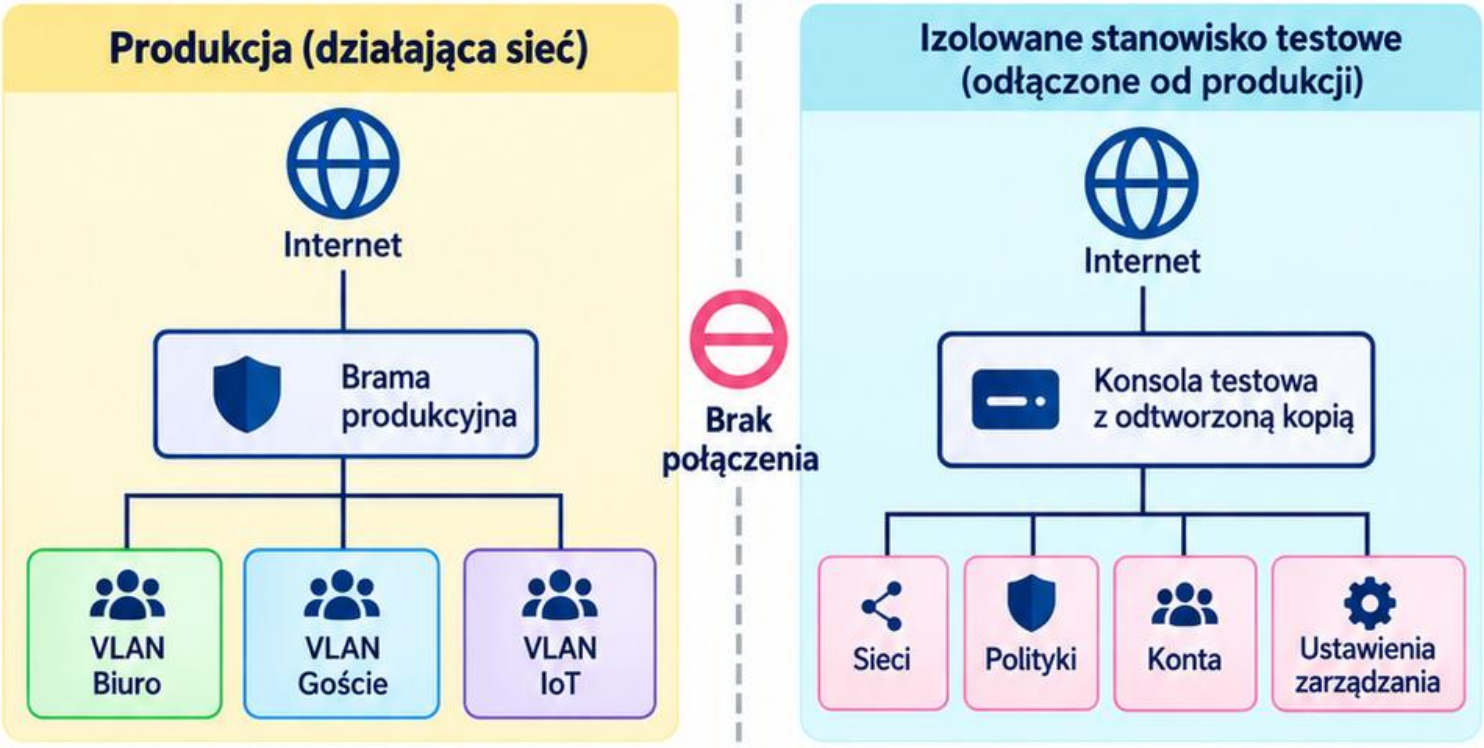
Źródła: [23], [8]

Odtwórz kopię w środowisku kontrolowanym

Cel: sprawdź użyteczność kopii bez uruchomienia drugiej, kolidującej bramy w tej samej produkcyjnej sieci. Odizoluj stanowisko testowe.

Dla aktualnej konsoli użyj **Settings > Control Plane > Backups > Restore**. Wybierz właściwą kopię systemową albo odpowiedni plik Network.

Sprawdź zgodność hosta i wersji; migracja między różnymi modelami konsoli wymaga według dokumentacji UniFi OS co najmniej 3.1.



Przykład: odtworzenie na odłączonej konsoli testowej. Potwierdź sieci, polityki, konta i ustawienia zarządzania, nie podłączając jej do tych samych VLAN-ów.

Odbiór: zapisujesz czas oraz zakres odzyskanych ustawień.
Powrót: odłącz środowisko próbne i zachowaj sprawdzoną kopię; nie resetuj działającej produkcji dla samego testu.

Źródła: [8]

Przeprowadź próbę odzyskania

Cel: zmierz, czy administrator potrafi przywrócić kluczowe usługi w uzgodnionym czasie. Samo pobranie pliku nie potwierdza zdolności odtworzenia.

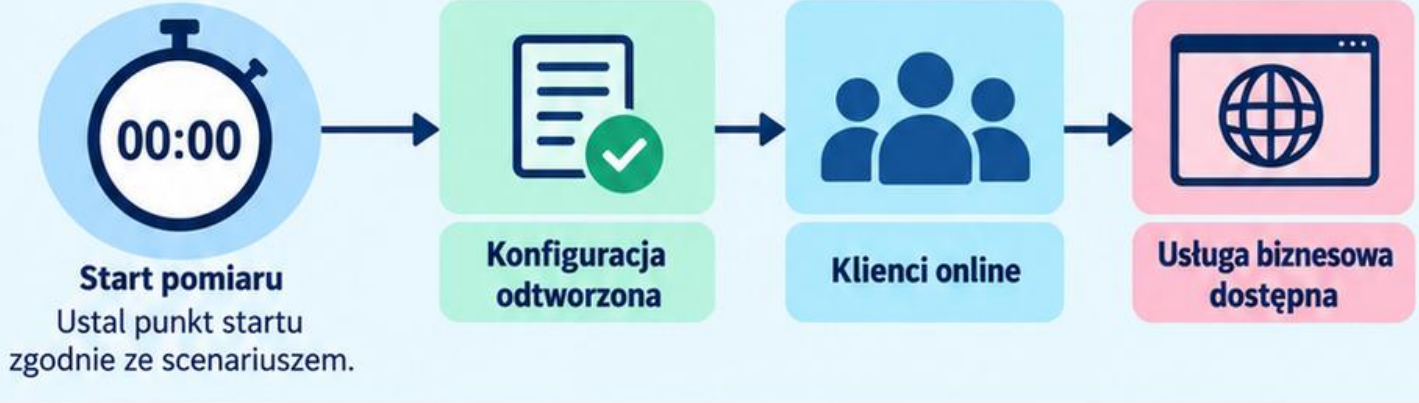
Przygotuj zatwierdzony scenariusz, kopię, dostęp lokalny i listę kontaktów. Ustal punkt startu pomiaru oraz warunek uznania usługi za odzyskaną.

Przykład projektu: awaria konsoli testowej; administrator odtwarza konfigurację i sprawdza DHCP, DNS, sieć pracowników oraz panel dostępny z Zarządzania.

Oddziel czas odtworzenia od ponownego uruchomienia urządzeń i aplikacji. **RPO** oraz RTO ustala firma; wpisz zmierzone wartości zamiast marketingowej gwarancji.

Test końcowy: drugi administrator odtwarza kroki z instrukcji. Uzupełnij brakujące zależności i przywróć bezpieczny stan stanowiska próbnego po zakończeniu ćwiczenia.

Przebieg próby odzyskania



Źródła: [8]

Zarejestruj odbiór wdrożenia

Cel: firma i wykonawca potwierdzają konkretne działanie sieci oraz znane ograniczenia. Odbiór opieraj na wynikach, nie na samym podglądzie panelu.

Zestaw plan adresacji, wersje, macierz dostępu i protokół testów.
Każda pozycja zawiera oczekiwanie, wynik, datę i osobę sprawdzającą.

- Plan adresacji
- Wersje
- Macierz dostępu
- Protokół testów

Przykład: DHCP we wszystkich VLAN-ach działa, Goście nie docierają do Firmy, VPN otwiera aplikację, a backup został sprawdzony na stanowisku testowym.

DHCP we wszystkich VLAN-ach działa → Goście nie docierają do Firmy → VPN otwiera aplikację → Backup został sprawdzony na stanowisku testowym

Wpisz odchylenia wraz z właścicielem i terminem.
Nie oznaczaj problemu jako rozwiązany tylko dlatego, że zastosowano tymczasowy szeroki wyjątek firewalla.

Odbiór: uprawniona osoba akceptuje wyniki i harmonogram usunięcia usterek. Przekaż instrukcję eskalacji oraz bezpieczny dostęp administracyjny poza ogólnym dokumentem sieci.

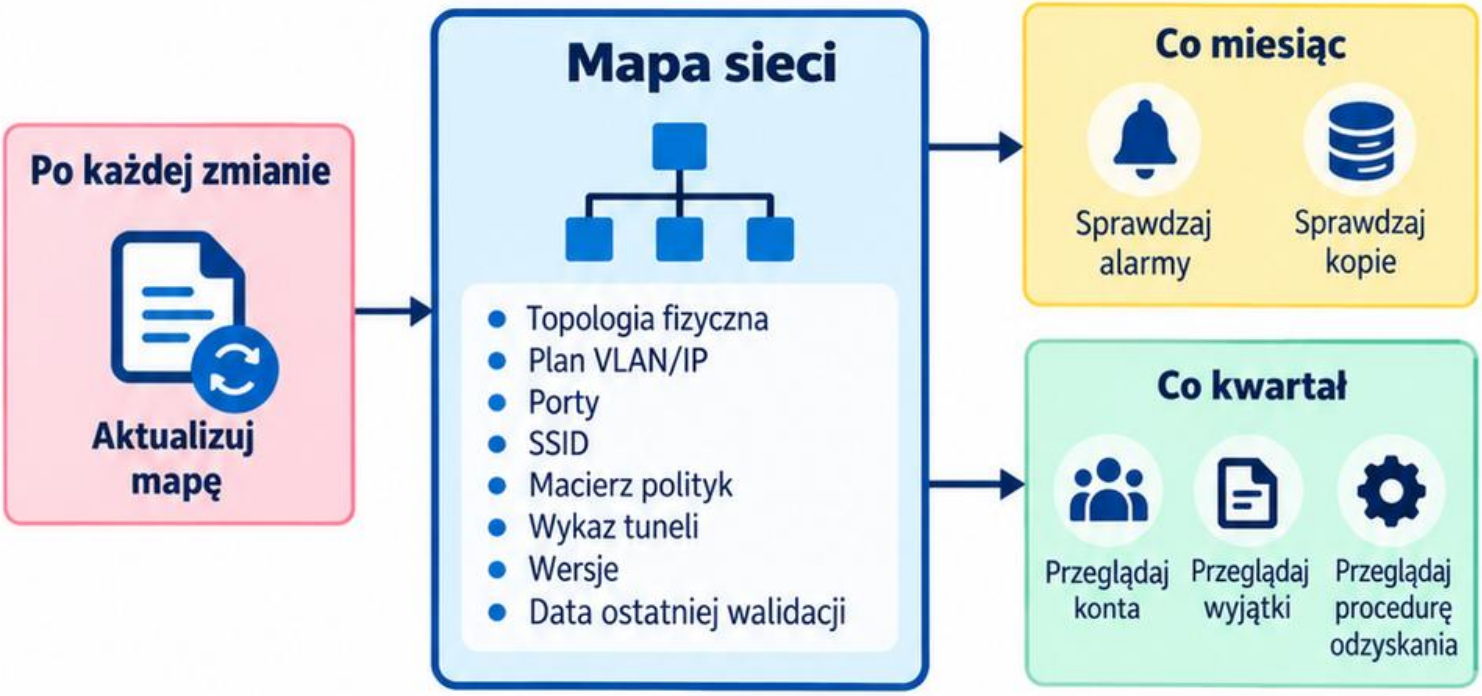
Firma akceptuje wyniki i harmonogram — **Protokół odbioru (z podpisem)** — **Wykonawca** potwierdza realizację

Źródła: [3], [8]

Przekaż mapę i rytm przeglądów

Cel: następny administrator ma rozumieć sieć bez odgadywania funkcji portów i wyjątków. Dokumentacja powinna odpowiadać stanowi po zakończeniu wdrożenia.

Przekaż topologię fizyczną, plan VLAN/IP, porty, SSID, macierz polityk oraz wykaz tuneli. Wpisz wersje i datę ostatniej walidacji.



Przykład rutyny: po każdej zmianie aktualizuj mapę; co miesiąc sprawdzaj alarmy i kopie; kwartalnie przeglądaj konta, wyjątki oraz procedurę odzyskania.

To proponowany harmonogram organizacyjny, nie wymóg producenta. Firma może go zaostrzyć zależnie od ryzyka i częstotliwości zmian.

Test: inny administrator odnajduje port AP, właściciela wyjątku i lokalizację backupu. Klucze prywatne, PSK i hasła pozostają poza mapą w magazynie sekretów.

Magazyn sekretów
Klucze prywatne
PSK
Hasła

Źródła: [8], [45], [23]

Ostoja
Źródła • 1/2

Dokumentacja Ubiquiti. Stan sprawdzenia: 21.10.2026. Numery odpowiadają odwołaniom w materiale.

[1] Tworzenie sieci VLAN
https://help.ui.com/hc/en-us/articles/9761080275607

[2] Tworzenie sieci Wi-Fi
https://help.ui.com/hc/en-us/articles/26136823938583

[3] Zapora strefowa
https://help.ui.com/hc/en-us/articles/115003173168

[4] Ustawienia przełączników
https://help.ui.com/hc/en-us/articles/33402927617047

[5] Pętle i STP
https://help.ui.com/hc/en-us/articles/24292724428311

[6] Tryby i dostępność PoE
https://help.ui.com/hc/en-us/articles/115000263008

[7] Agregacja portów
https://help.ui.com/hc/en-us/articles/360007279753

[8] Kopie i migracja
https://help.ui.com/hc/en-us/articles/360008976393

[9] Pierwsze uruchomienie UniFi
https://help.ui.com/hc/en-us/articles/4416276882327

[10] Zarządzanie lokalne
https://help.ui.com/hc/en-us/articles/28457353760919

[11] Wybór hosta zarządzania
https://help.ui.com/hc/en-us/articles/30127033090071

[12] Serwer DHCP
https://help.ui.com/hc/en-us/articles/360012097513

[13] Konfiguracja IPv6
https://help.ui.com/hc/en-us/articles/115005868927

[14] Dodawanie administratorów
https://help.ui.com/hc/en-us/articles/28692158912279

[23] Aktualizacje UniFi
https://help.ui.com/hc/en-us/articles/7605005245975

Ostoja
Źródła • 2/2

Dokumentacja Ubiquiti. Stan sprawdzenia: 21.10.2026. Numery odpowiadają odwołaniom w materiale.

[25] Tablice i protokoły routingu
https://help.ui.com/hc/en-us/articles/115005986348

[26] Lokalne nazwy DNS
https://help.ui.com/hc/en-us/articles/15179064940439

[27] Adopcja między podsieciami
https://help.ui.com/hc/en-us/articles/204909754

[28] BGP i łącza prywatne
https://help.ui.com/hc/en-us/articles/44199240807703

[29] Proxy mDNS
https://help.ui.com/hc/en-us/articles/12648701398807

[34] Dobre praktyki sieci gości
https://help.ui.com/hc/en-us/articles/23948850278295

[35] Uruchamianie 6 GHz
https://help.ui.com/hc/en-us/articles/20407971377815

[36] Hotspot i portal
https://help.ui.com/hc/en-us/articles/115000166827

[37] Problemy z łączeniem Wi-Fi
https://help.ui.com/hc/en-us/articles/23283660456599

[38] Migracja zapory strefowej
https://help.ui.com/hc/en-us/articles/28223082254743

[39] Wykrywanie i blokowanie zagrożeń
https://help.ui.com/hc/en-us/articles/360006893234

[45] Dzienniki i integracja SIEM
https://help.ui.com/hc/en-us/articles/33349041044119

[46] Korzystanie z WiFiman
https://help.ui.com/hc/en-us/articles/205204150

[47] Menedżer alarmów
https://help.ui.com/hc/en-us/articles/27721287753239

[48] Pliki i dzienniki wsparcia
https://help.ui.com/hc/en-us/articles/360049956374

Pozostałe pozycje bibliografii głównej znajdują się w dołączonych poradnikach.
Wskazane strony zawierają pełne adresy źródeł.

Checklista wdrożenia, str. 15: [15], [16], [17], [18], [19], [20], [21], [22].

VLAN, firewall i VPN, str. 38: [40], [41], [42], [43], [44].

Diagnostyka, str. 26: [24], [30], [31], [32], [33].

Przed zmianą porównaj model, wersję i dostępność funkcji.
Przykładowe adresy oraz kryteria testów są elementem opracowania Ostoja.