Ostoja

Wizualny poradnik VLAN, firewalla i VPN w UniFi

Od projektu segmentacji do bezpiecznego dostępu zdalnego



Jak przejść przez wdrożenie

1 Przygotuj środowisko

Cel: przeprowadzić jedną zmianę od projektu do odbioru. Czytaj strony kolejno; późniejsze polityki korzystają z wcześniej ustalonej adresacji i ról.



2 Sprawdź wymagania

Wymagania: zgodna brama UniFi, przełącznik obsługujący VLAN-y, AP oraz komputer administratora. Zapisz modele, Network, UniFi OS i firmware urządzeń.



3 Skonfiguruj bramę

Dla firewalla strefowego przyjmujemy Network 9.0.108+ oraz bramę 4.1+. Podawane ścieżki 9.4 mają oznaczenie; w 9.3 występuje Policy Engine.



4 Wprowadź zmianę

Każdy etap zawiera założenie, zmianę i dowód. Najpierw wykonaj backup, potem użyj jednego klienta testowego zamiast przenosić całe biuro jednocześnie.



5 Przetestuj przykład

Przykład: VLAN Goście najpierw sprawdzasz na wolnym porcie. Dopiero po poprawnym DHCP, DNS i izolacji przypisujesz do niego SSID.



6 Odbierz i zabezpiecz

Warunek zatrzymania: utrata lokalnego zarządzania lub podstawowych usług. Wycofaj ostatnią zmianę przez zachowaną ścieżkę administracyjną; nie dodawaj przypadkowych wyjątków.



Źródła: [3], [8]

Ostoja • Wdrożenie zintegrowane • 03

Biuro, które będziemy porządkować



Scenariusz przykładowy: Marta, 38 lat, prowadzi biuro projektowe w Krakowie. Dwanaście stanowisk współdzieli internet, drukarkę oraz salę spotkań.

Cel: oddzielić sprzęt pracowników od telefonów gości i urządzeń IoT. Administrator Paweł ma zachować bezpieczny dostęp przewodowy podczas przebudowy.

Projekt: Firma VLAN 10, Goście VLAN 20, IoT VLAN 30 i Zarządzanie VLAN 99. Każda sieć ma własną podsieć.

Drukarka ma rezerwację 192.168.30.50 i potwierdzoną obsługę IPP. System dokumentów działa jako HTTPS na 192.168.10.20.

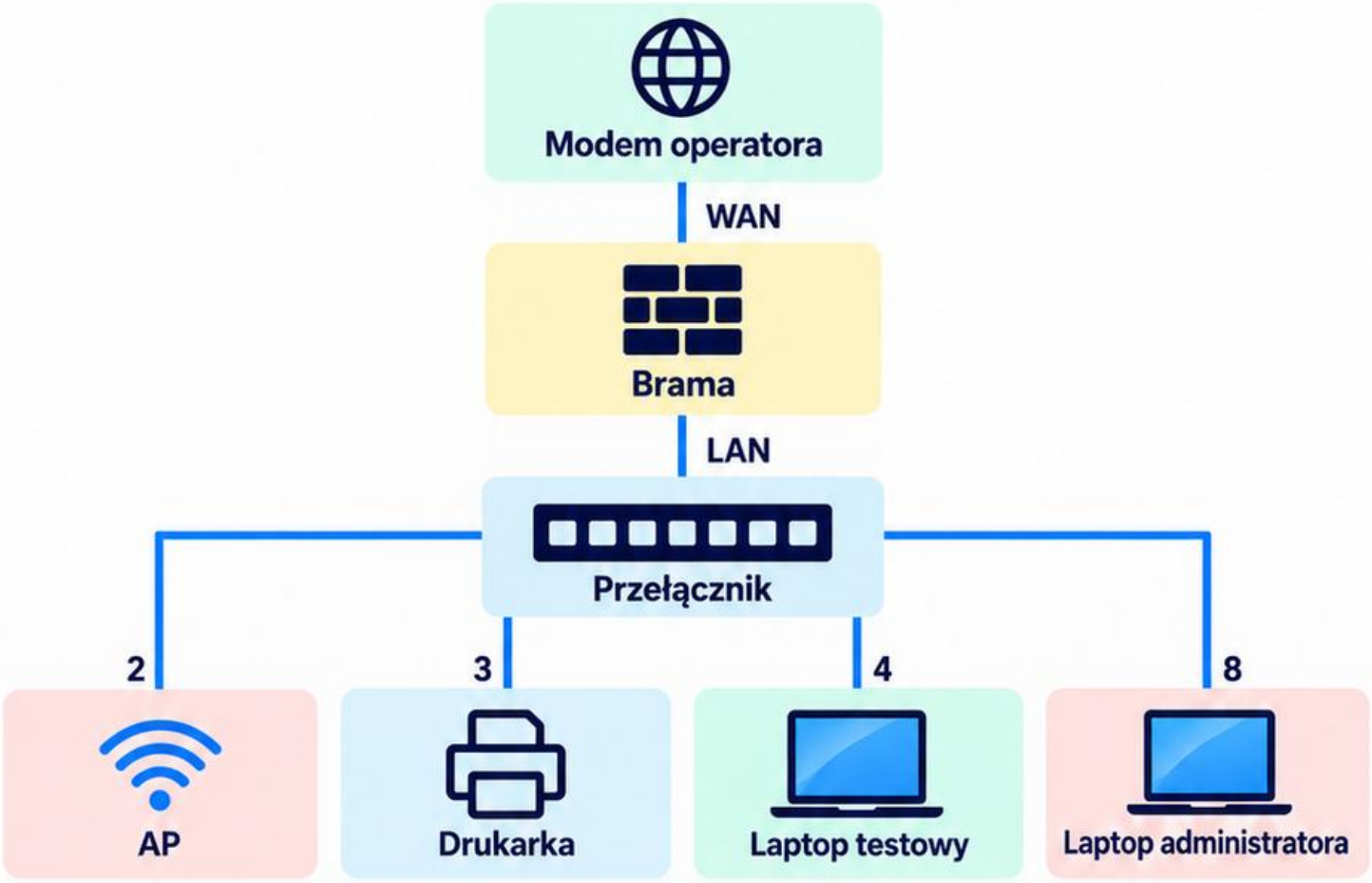
Marta pracuje czasem zdalnie: później dołączymy mały oddział w Poznaniu. Udostępnimy tylko wymagane usługi, bez łączenia sieci Gości.

Dowód sukcesu: wydruk i system dokumentów działają, gość nie osiąga Firmy, a IoT nie rozpoczyna połączeń do stanowisk pracowników.

Źródła: [3], [1], [22]

Ostoja | Wdrożenie zintegrowane • 04

Połącz urządzenia bez utraty kontroli



Cel: znać fizyczną drogę każdego VLAN-u. W biurze modem operatora łączy się z WAN bramy, a LAN bramy z portem 1 przełącznika.

Projekt portów: 1 uplink do bramy, 2 AP, 3 drukarka, 4 komputer testowy Firmy, 8 lokalny port ratunkowy administratora.

Spisz modele, numery portów i oznaczenia kabli. Sprawdź zasilanie AP oraz dostępny budżet PoE według specyfikacji wybranego sprzętu.

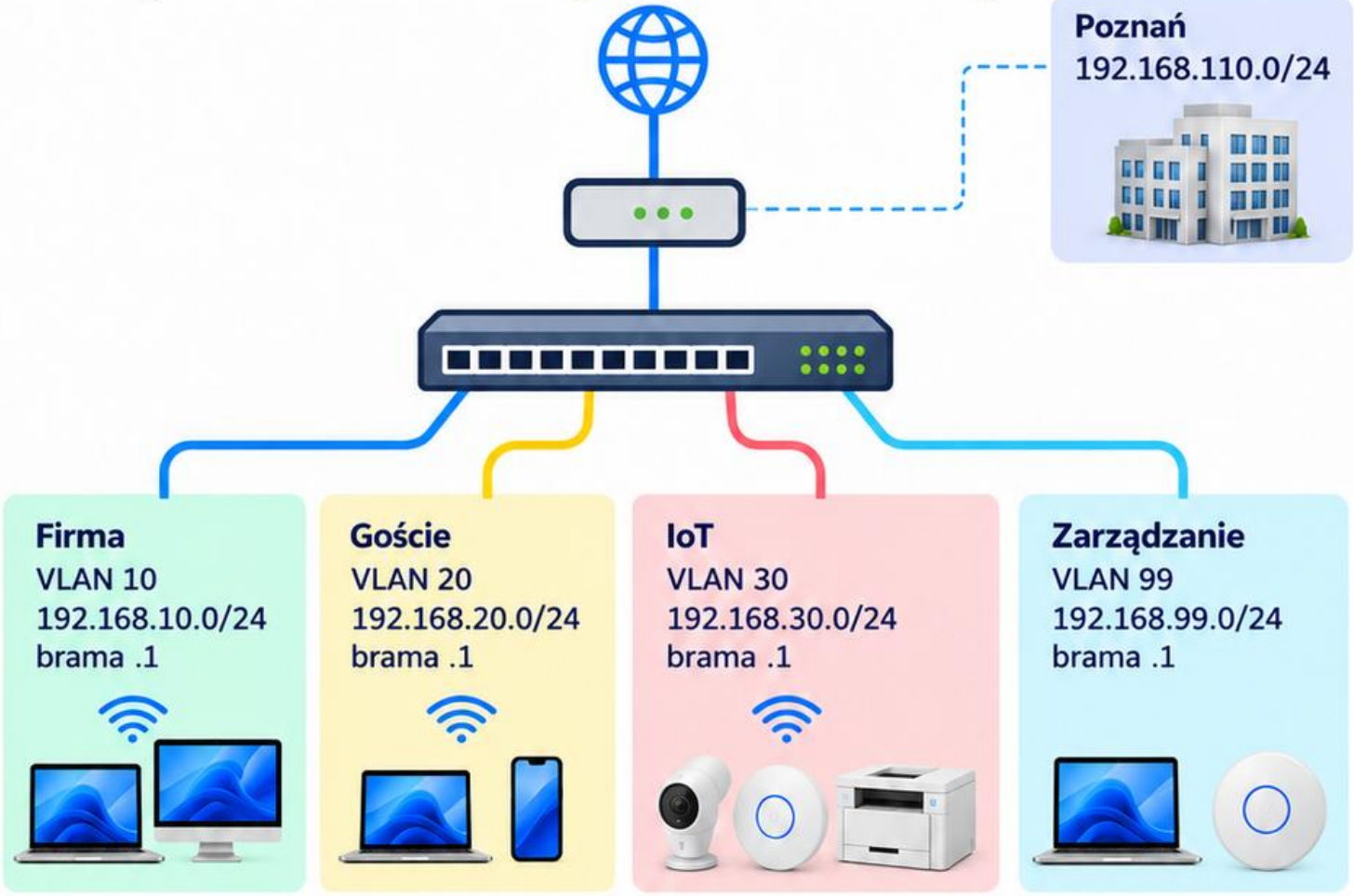
Przed zmianą uplinku Paweł potwierdza lokalne logowanie przez port 8. Ten port pozostaje w dotychczasowej, działającej sieci do zakończenia migracji.

Przykład: problem wszystkich SSID po zmianie portu 1 wskazuje wspólną ścieżkę. Awaria wyłącznie drukarki kieruje uwagę na port 3.

Test: ewidencja zgadza się z przewodami i widokiem Topology, Cofnięcie obejmuje jeden port; nigdy nie przebudowuj równocześnie uplinku i ścieżki ratunkowej.

Źródła: [1], [8]

Przydziel rozłączne adresy



VPN
10.250.0.0/24

Cel: każdy segment ma jednoznaczny zakres i bramę, Numery podsieci wybrano jako projekt tego biura, a nie domyślne ustawienie UniFi.

Firma: VLAN 10, 192.168.10.0/24, brama .1. **Goście:** VLAN 20, 192.168.20.0/24, brama .1. **IoT:** VLAN 30, 192.168.30.0/24, brama .1. **Zarządzanie:** VLAN 99, 192.168.99.0/24, brama .1.

Przykład puli DHCP: .100–.199 w każdym segmencie. Adresy infrastruktury rezerwujemy poza pulą; drukarka otrzymuje rezerwację 192.168.30.50.

Dodatkowo zarezerwuj pulę VPN 10.250.0.0/24. Poznań otrzyma 192.168.110.0/24 dla Firmy, bez nakładania się z Krakowem.

Test: sprawdź istniejące LAN-y, trasy i sieci domowe użytkowników przed zatwierdzeniem. Kolizję rozwiąż zmianą projektu, zanim przeniesiesz aktywne urządzenia.

Źródła: [1], [41]

Ustal dozwoloną komunikację

Cel: Marta akceptuje macierz przed konfiguracją. Reguły mają odpowiadać potrzebom firmy, zamiast zachowywać przypadkowy dostęp z wcześniejszej płaskiej sieci.



Firma	→	drukarka 192.168.30.50 TCP 631	✓	dozwolone
Firma	→	serwer 192.168.10.20 TCP 443	✓	dozwolone
Goście	→	internet	✓	dozwolone według polityki biura
IoT	→	Firma	✗	nowe połączenia zablokowane
Goście	→	Firma / IoT / Zarządzanie	✗	zablokowane

Firma → drukarka 192.168.30.50: TCP 631.
Firma → serwer 192.168.10.20: TCP 443.
Goście → internet: dostęp według polityki biura.

IoT → Firma: brak nowych połączeń.
Goście → Firma, IoT i Zarządzanie: blokada.
Zarządzanie → infrastruktura: dostęp tylko wskazanego administratora.

Wszystkie segmenty potrzebują własnego DHCP oraz zatwierdzonego DNS. Tutaj oba serwisy realizuje odpowiedni interfejs bramy; wyjątki przygotujemy przed ograniczeniem Gateway.

Ruch między klientami tego samego VLAN-u wymaga osobnej kontroli warstwy drugiej. Sama polityka między strefami nie gwarantuje izolacji gość–gość.

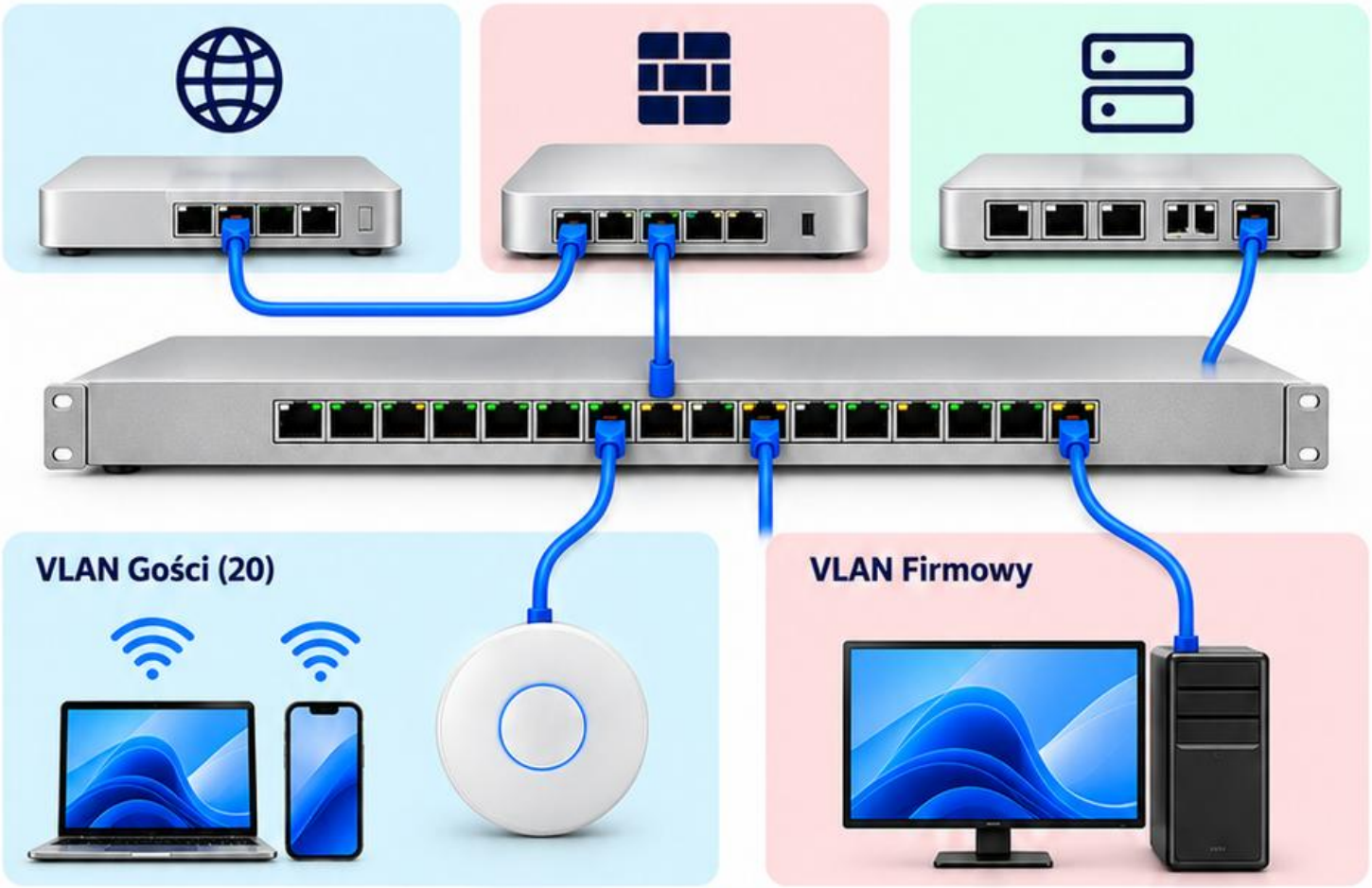
Test: każda dozwolona usługa ma właściciela i próbę odbiorową.
Cofnięcie nie oznacza otwarcia wszystkich segmentów; przywracamy konkretny poprzedni stan.

Źródła: [3], [20]

Oddziel VLAN od podsieci

Cel: zrozumieć dwie różne role. VLAN rozdziela domeny warstwy drugiej, a podsieć określa adresację i decyzje routingu klienta.

W projekcie numer 20 oznacza VLAN Gości, natomiast **192.168.20.0/24** jest jego podsiecią. Zbieżność liczb ułatwia pamięć, lecz nie stanowi wymogu.



Podsieć: 192.168.20.0/24

Podsieć: 192.168.10.0/24

Przełącznik przypisuje ruch do VLAN-u, a brama zapewnia odpowiedni interfejs IP. Sama nazwa Goście w kontrolerze nie przenosi klientów.

Przykład: laptop z 192.168.10.120 podłączony do niewłaściwego VLAN-u nie naprawi się przez ręczną zmianę samego DNS. Sprawdź przypisanie portu.

Najpierw utwórz sieć i DHCP, potem przygotuj jej drogę przez uplinki, następnie przypisz klienta. Firewall kończy projekt ograniczeniami komunikacji.

Test: klient otrzymuje adres właściwej podsieci i widzi właściwą bramę. Nie wprowadzaj statycznego adresu, aby ukryć problem z tagowaniem lub DHCP.

Źródła: [1]

Ustal tagowanie i VLAN natywny

Ostoja • Wdrożenie zintegrowane • 08

Cel: każda strona przewodu ma jednakowo rozumieć ramki oznaczone i nieoznaczone. Rozbieżna sieć natywna może odciąć urządzenia administracyjne.

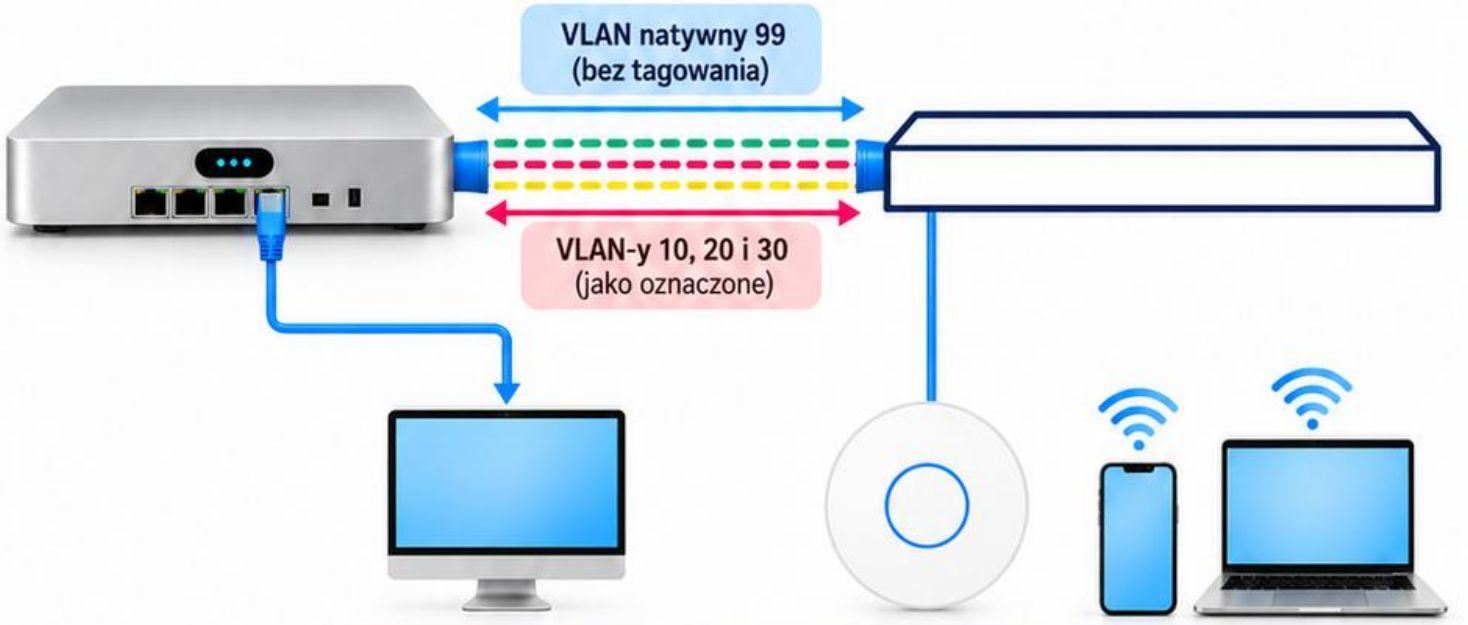
Projekt końcowy: uplink brama–przełącznik przenosi potrzebne VLAN-y, a Zarządzanie 99 jest świadomie uzgodnioną siecią natywną na obu końcach.

Na porcie zwykłego komputera ruch pozostaje nieoznaczony i trafia do przypisanej sieci. Uplink przenosi dodatkowe VLAN-y jako oznaczone.

AP w tym projekcie zarządzamy bez tagowania przez natywny VLAN 99; SSID używają tagowanych 10, 20 i 30. Nie włączaj równocześnie sprzecznego Network Override.

Migrację natywnego VLAN-u przeprowadź dopiero po przygotowaniu sieci i przetestowaniu niezależnego dostępu administratora. Zachowaj zapis konfiguracji obu końców.

Test: po zmianie AP pozostaje online, a klient każdego SSID otrzymuje właściwy adres. Gdy znika zarządzanie, przywróć poprzedni profil portu.



Źródła: [1], [2]

Utwórz sieci na bramie

1. **Cel:** brama ma obsługiwać wszystkie cztery segmenty projektu, zanim dołączą do nich aktywni użytkownicy. Zachowaj dotychczasową sieć ratunkową.

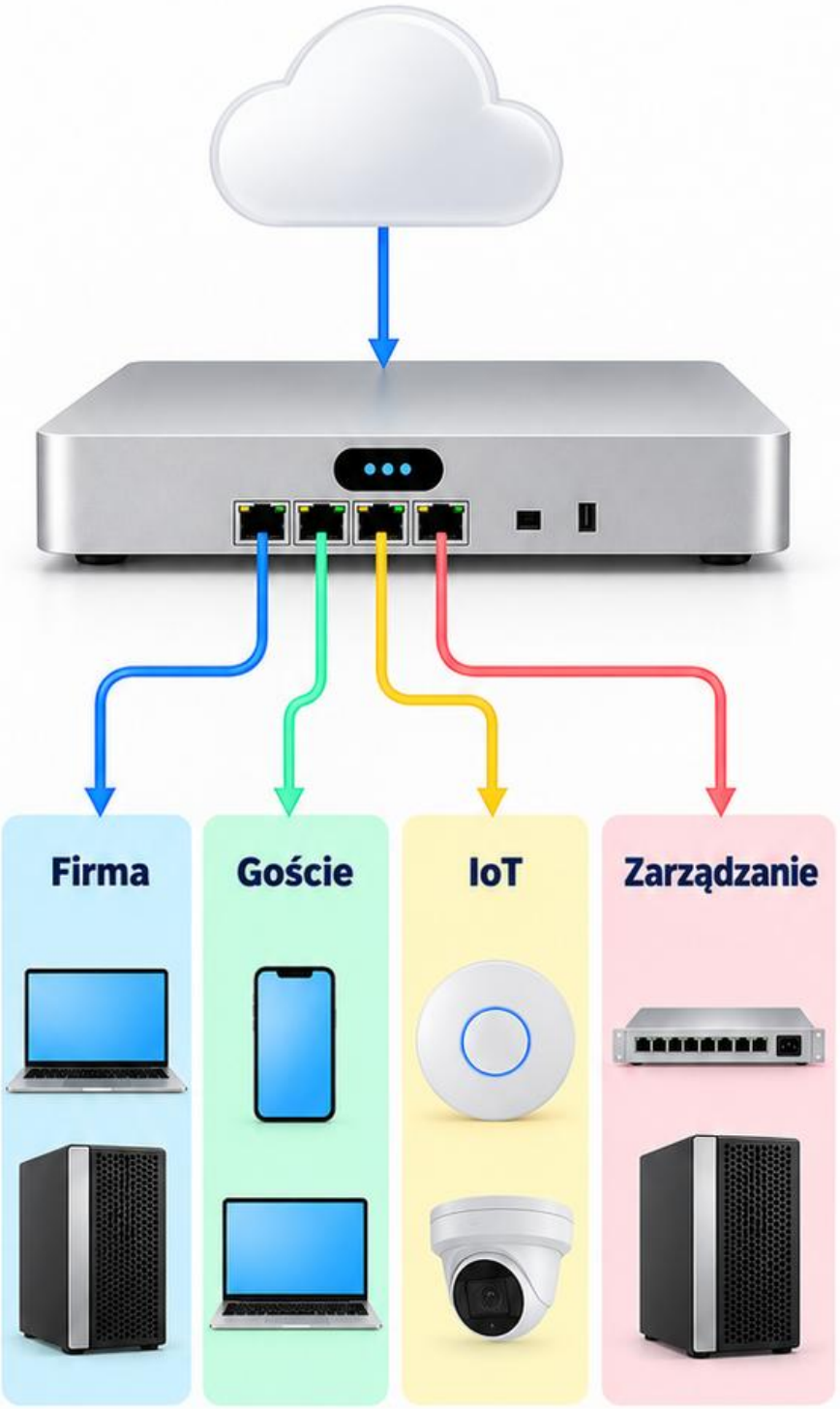
2. W Network otwórz **Settings > Networks** i utwórz kolejne sieci. Nadaj nazwy **Firma, Goście, IoT i Zarządzanie** zgodnie z planem.

3. Dla każdej wpisz VLAN ID, bramę z maską /24 oraz przygotowaną pulę DHCP. Sprawdź, czy wybranym routerem jest właściwa brama UniFi.

4. Przykład: **IoT** otrzymuje VLAN 30, 192.168.30.1/24 i pulę 192.168.30.100–199. Rezerwacja drukarki .50 pozostaje poza pulą dynamiczną.

5. Nie włączaj jednocześnie dodatkowego serwera DHCP na starym routerze. Przy bramie innego producenta usługi trzeba skonfigurować również na niej.

6. **Test:** przenieś jeden port testowy do nowej sieci i sprawdź dzierżawę, bramę oraz DNS. Błąd popraw przed zmianą uplinków i SSID.



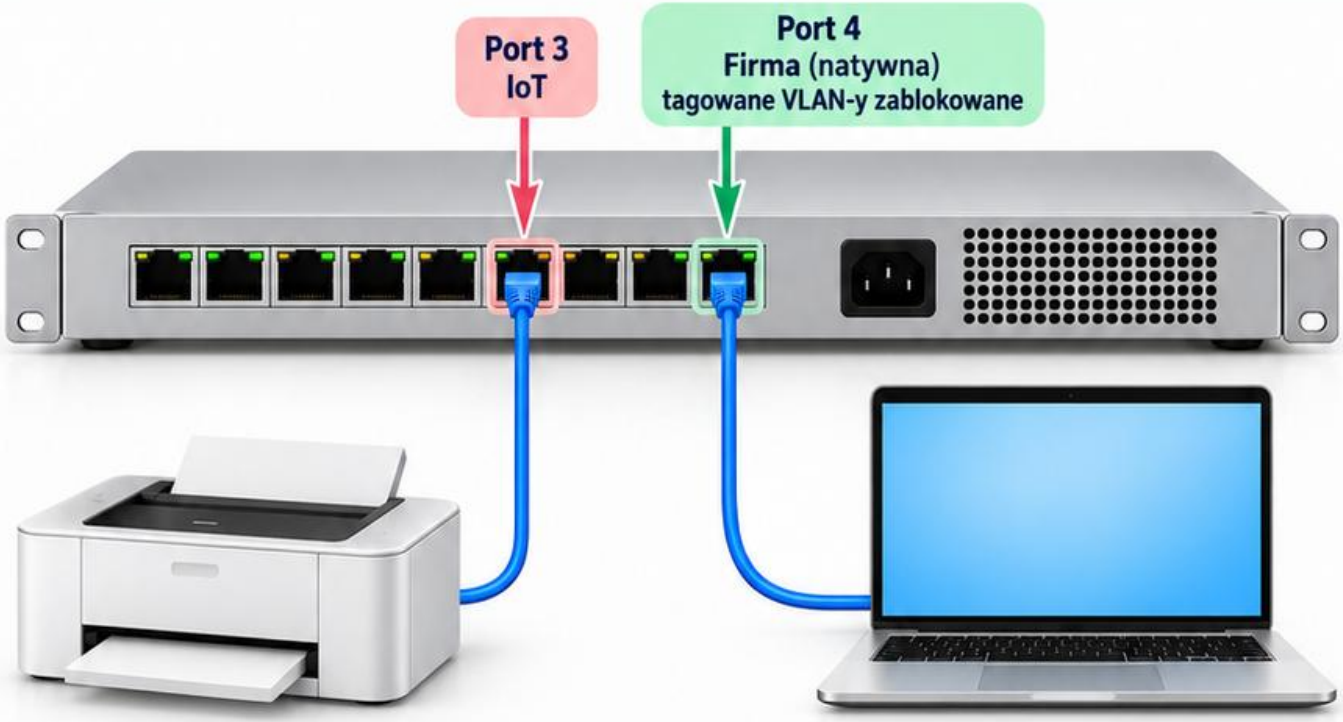
Źródła: [1]

Przypisz porty stanowisk

Ostoja • Wdrożenie zintegrowane • 10

1 **Cel:** zwykły komputer ma trafić do Firmy bez konfiguracji tagowania w systemie użytkownika. Najpierw użyj portu testowego 4.

2 W Network wybierz przełącznik w Devices i skonfiguruj właściwy port. Ustaw sieć natywną Firma; zablokuj zbędne tagowane VLAN-y dla zwykłego stanowiska.



3 Podłącz laptop testowy, odśwież jego dzierżawę i sprawdź adres 192.168.10.100–199. Zapisz MAC i oznaczenie gniazda w pokoju.

4 Drukarka na porcie 3 otrzyma osobny profil IoT. Nie kopiuj profilu stanowiska na uplink lub port AP, ponieważ te połączenia przenoszą więcej sieci.

5 **Przykład:** pracownik przenosi się do nowego biurka. Administrator zmienia przypisanie konkretnego portu, zachowując zasadę jednej roli dla zwykłego gniazda.

6 **Test:** laptop uzyskuje prawidłowy adres i internet; nie widzi Zarządzania. **Cofnięcie:** przywróć poprzedni profil i ponownie odnów dzierżawę.

Źródła: [1]

Przeprowadź VLAN-y przez uplink

Cel: port 1 przełącznika i odpowiadający port bramy mają zapewniać ciągłość wszystkich wymaganych VLAN-ów. Uplink nie jest zwykłym portem pracownika.

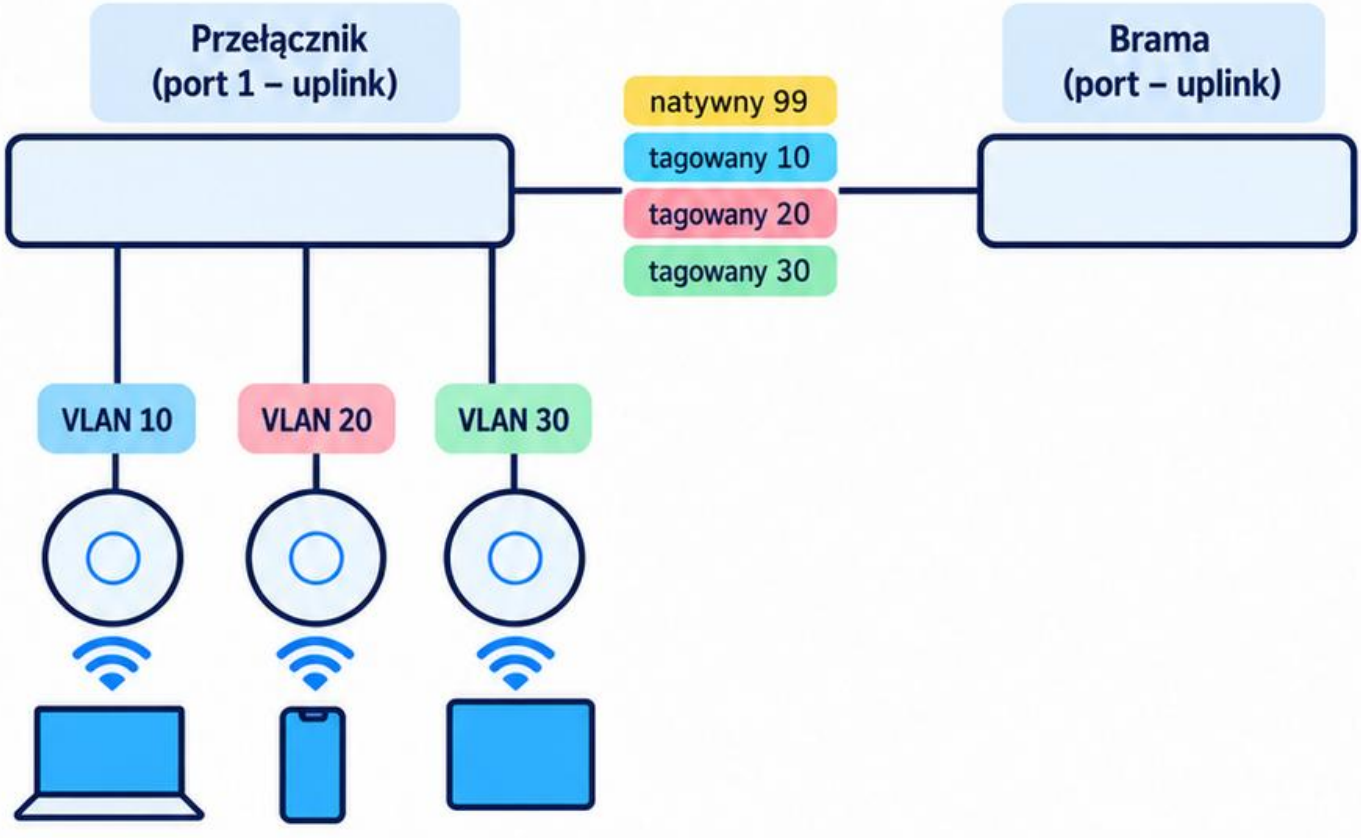
Sprawdź konfigurację obu końców. Dopuść tagowane VLAN-y 10, 20 i 30 oraz uzgodniony natywny 99 w końcowym projekcie.

Jeśli po drodze jest przełącznik innego producenta, wprowadź zgodne tagowanie również na nim. Sama konfiguracja kontrolera UniFi nie zmienia obcego urządzenia.

Przykład: Firma działa, lecz Goście nie otrzymują adresu. Sprawdź obecność VLAN 20 na całej drodze, zanim otworzysz firewall.

Migruj zarządzanie dopiero po próbie przez nową sieć i zachowaniu niezależnego portu ratunkowego. Zapisz stary profil uplinku przed zastosowaniem.

Test: po jednym kliencie w każdym segmencie otrzymuje właściwy DHCP i DNS. Utrata wszystkich VLAN-ów wskazuje wspólny uplink lub bramę.



Źródła: [1], [2]

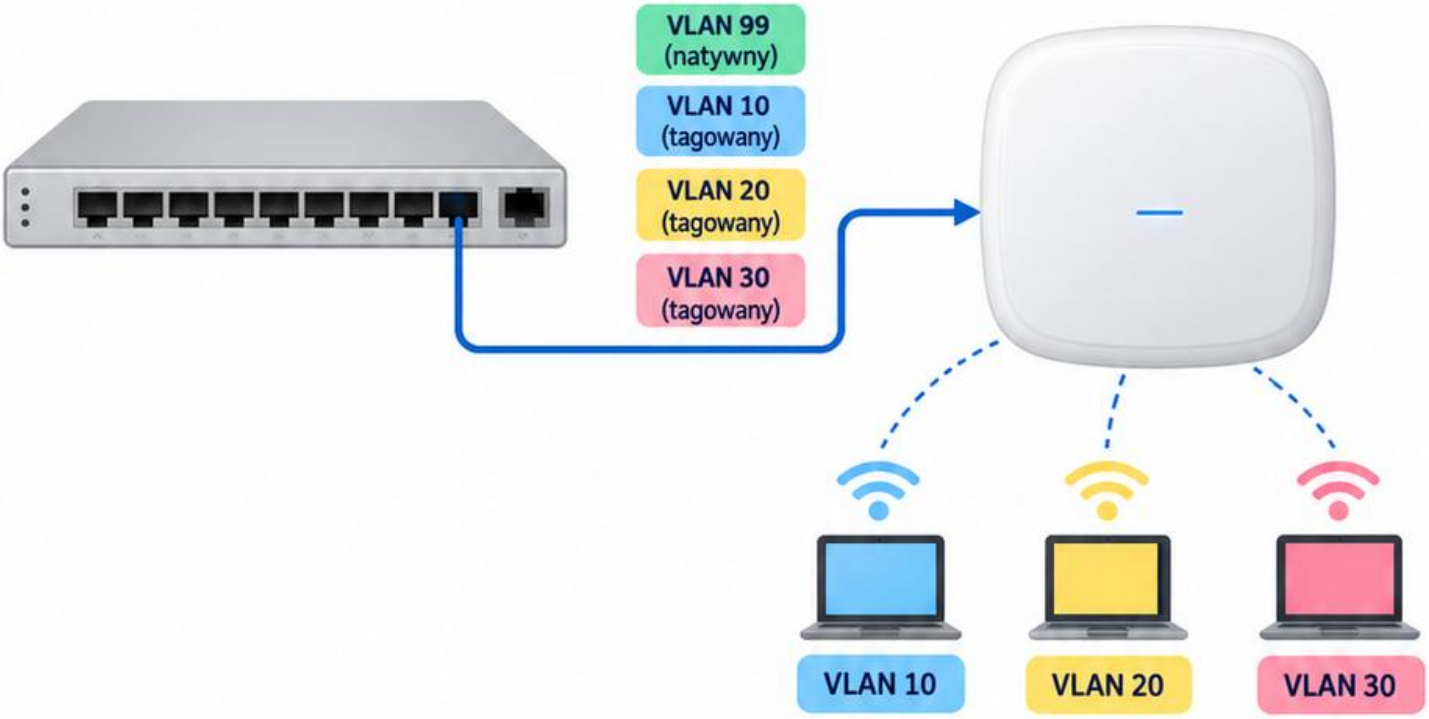
Przygotuj port punktu dostępowego

Cel: AP ma zachować łączność administracyjną i przenosić trzy sieci bezprzewodowe. Sprawdź jednocześnie wymagania zasilania i rolę VLAN-ów.

Na porcie 2 przełącznika ustaw docelowy natywny VLAN 99 oraz tagowane VLAN-y 10, 20 i 30. Zachowaj zgodność z konfiguracją AP.

W tym projekcie AP pobiera adres zarządzania bez tagowania, z 192.168.99.0/24. Nie ustawiamy dodatkowego tagowanego Network Override dla tego samego przepływu.

Po migracji sprawdź nowy adres AP i status online, zanim rozgłosisz SSID produkcyjne. Stara sesja panelu może nie potwierdzać nowej drogi.



Przykład: AP działa, ale tylko jedno SSID nie ma DHCP. Sprawdź tag właściwego VLAN-u zamiast zmieniać natywną sieć zarządzania.

Test: AP online, trzej klienci testowi mają właściwe podsieci.
Cofnięcie: lokalnie odtwórz poprzedni profil portu i konfigurację zarządzania AP.

Źródła: [2], [1]

Powiąż SSID z sieciami

Cel: nazwa Wi-Fi ma kierować klienta do właściwego segmentu. W naszym biurze używamy trzech czytelnych SSID zamiast jednej wspólnej sieci.

W Network otwórz Settings > WiFi. Utwórz **Firma**, **Goscie** oraz IoT; w polu Network wybierz odpowiadającą sieć VLAN.



Wybierz AP-y, które mają nadawać daną nazwę. Zweryfikuj zabezpieczenia na rzeczywistych klientach; starsze IoT może wymagać odrębnych ustawień zgodności.

Zarządzanie pozostaje przewodowe i nie otrzymuje ogólnodostępnego SSID. Hasła przechowuj poza dokumentacją wdrożenia, w zatwierdzonym magazynie.

Przykład: telefon gościa wybiera Goscie i otrzymuje 192.168.20.x. Nazwa SSID sama nie izoluje klientów ani nie definiuje całego firewalla.

Test: połącz jedno urządzenie z każdym SSID, sprawdź IP, bramę, DNS i polityki. Przy błędzie wróć do przypisania Network oraz tagowania uplinku.

Źródła: [2], [20]

Zapewnij DHCP i DNS

Ostoja • Wdrożenie zintegrowane • 14

Cel: wszystkie segmenty mają działać bez ręcznego wpisywania adresów klientów. W tym scenariuszu DHCP i DNS obsługuje interfejs bramy każdej sieci.

W Settings > Networks sprawdź pulę .100–.199, bramę .1 i adres DNS .1 we właściwej podsieci. Nie mieszaj parametrów między VLAN-ami.

Przykład Gości: adres 192.168.20.120, maska /24, brama 192.168.20.1, DNS 192.168.20.1. Drukarka ma rezerwację 192.168.30.50.

DHCP wymaga ruchu lokalnego klient–serwer; DNS potrzebuje zarówno UDP, jak i TCP 53. Późniejsza blokada Gateway musi zachować te usługi.

Najpierw sprawdź dzierżawę, potem nazwę publiczną, następnie usługę aplikacyjną. Sam ping do internetu nie weryfikuje dostarczonego DNS.

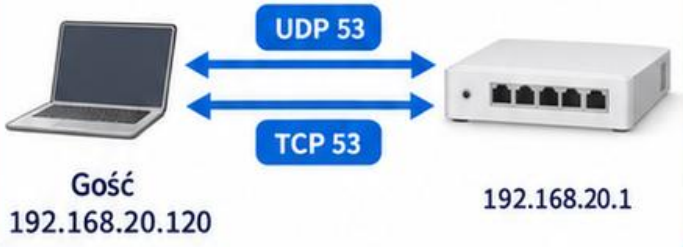
Test: nowy klient i klient odnawiający dzierżawę otrzymują właściwe dane. Przy błędzie sprawdź tagowanie, serwer i polityki, zamiast rozdawać adresy statyczne.



Dzierżawa DHCP klienta

Adres IP	192.168.20.120
Maska	/24
Brama	192.168.20.1
DNS	192.168.20.1

Ruch DNS do bramy

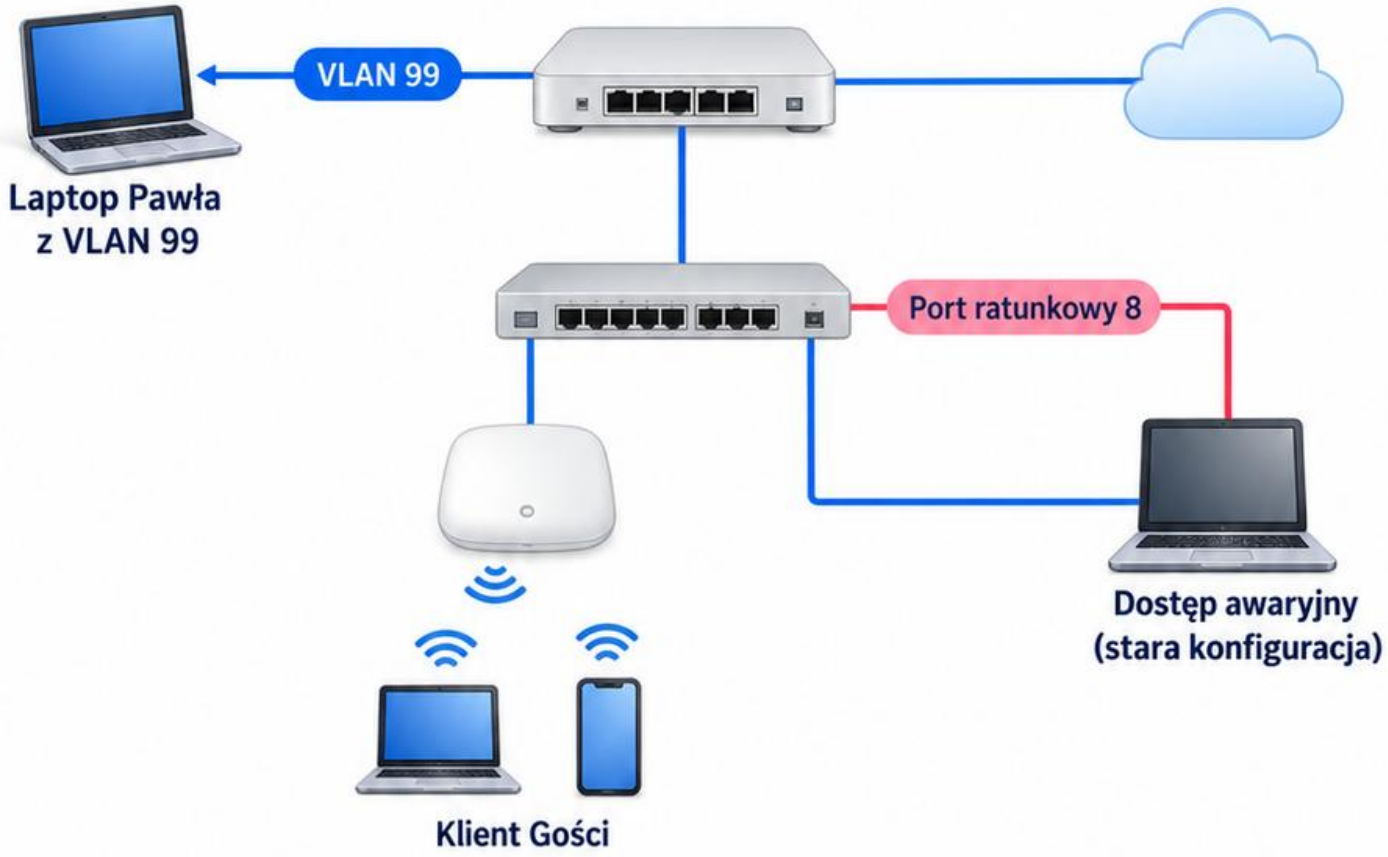


Źródła: [1], [3]

Przenieś zarządzanie bezpiecznie

Cel: Paweł zarządza przez VLAN 99, ale zachowuje możliwość odzyskania kontroli. Migracja jest osobnym etapem, poprzedzającym szerokie blokady.

Przygotuj sieć 192.168.99.0/24, działający port administratora i wymagane trasy. Laptop Pawła otrzymuje rezerwację 192.168.99.10.



Najpierw sprawdź lokalne logowanie z nowej sieci. Następnie przenoś pojedynczo przełącznik i AP, zachowując zgodność natywnego VLAN-u po obu stronach.

Port ratunkowy 8 pozostaje w starej, działającej konfiguracji do potwierdzenia nowej drogi. Nie usuwaj starej ścieżki podczas tej samej operacji.

Przykład: AP pojawia się pod nowym adresem, ale panel znika z laptopa. Sprawdź adres laptopa i drogę administracyjną przed restartem.

Test: świeże logowanie z VLAN 99 działa, a klient Gości nie otwiera panelu. **Cofnięcie:** użyj portu ratunkowego i przywróć ostatni zmieniony profil.

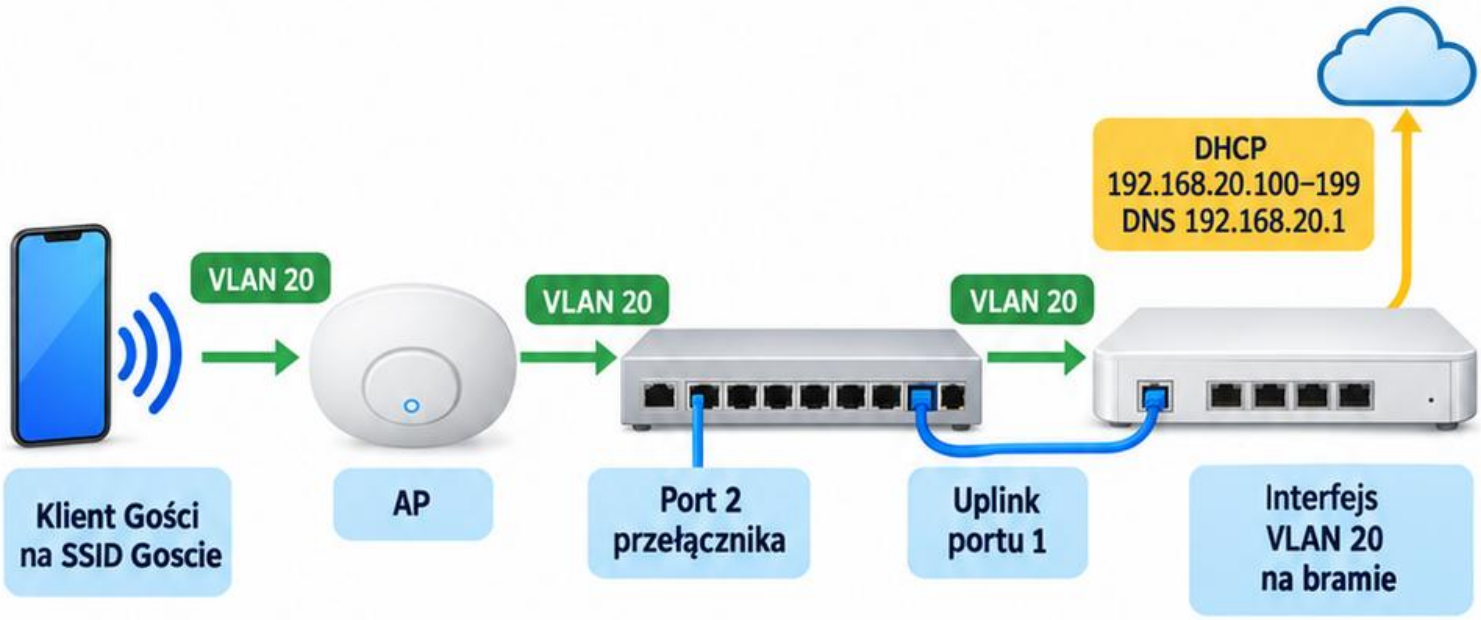
Źródła: [3], [2], [8]

Prześledź cały szlak VLAN-u

Ostoja • Wdrożenie zintegrowane • 16

1. **Cel:** udowodnić, że oznaczanie działa od klienta do bramy. Test obejmuje port, uplink i usługi; sam widok sieci w panelu nie wystarcza.

2. Weź klienta Gości na SSID **Goscie.** Zanotuj AP, port 2 przełącznika, uplink portu 1 oraz interfejs VLAN 20 na bramie.



3. **Oczekiwanie:** klient otrzymuje 192.168.20.100–199 i DNS 192.168.20.1. Sprawdź również brak przydziału adresu Firmy lub Zarządzania.

4. Jeśli adresu nie ma, porównaj wynik na przewodowym porcie testowym VLAN 20. Działający przewód zawęża problem do AP, SSID lub jego portu.

5. **Nie zmieniaj firewalla**, gdy błąd wskazuje brak transportu VLAN-u. Zachowaj wynik kontroli każdego odcinka, aby później nie wracać do zgadywania.

6. **Odbiór:** po ponownym połączeniu i odnowieniu DHCP klient nadal trafia do właściwej sieci. Cofnięcie dotyczy ostatniego zmienionego odcinka.

7. **Źródła:** [2], [1]

Przypisz sieci do stref

Cel: polityki mają odzwierciedlać cztery role naszego biura. Strefy grupują interfejsy, a nie zastępują VLAN-ów ani konfiguracji portów.

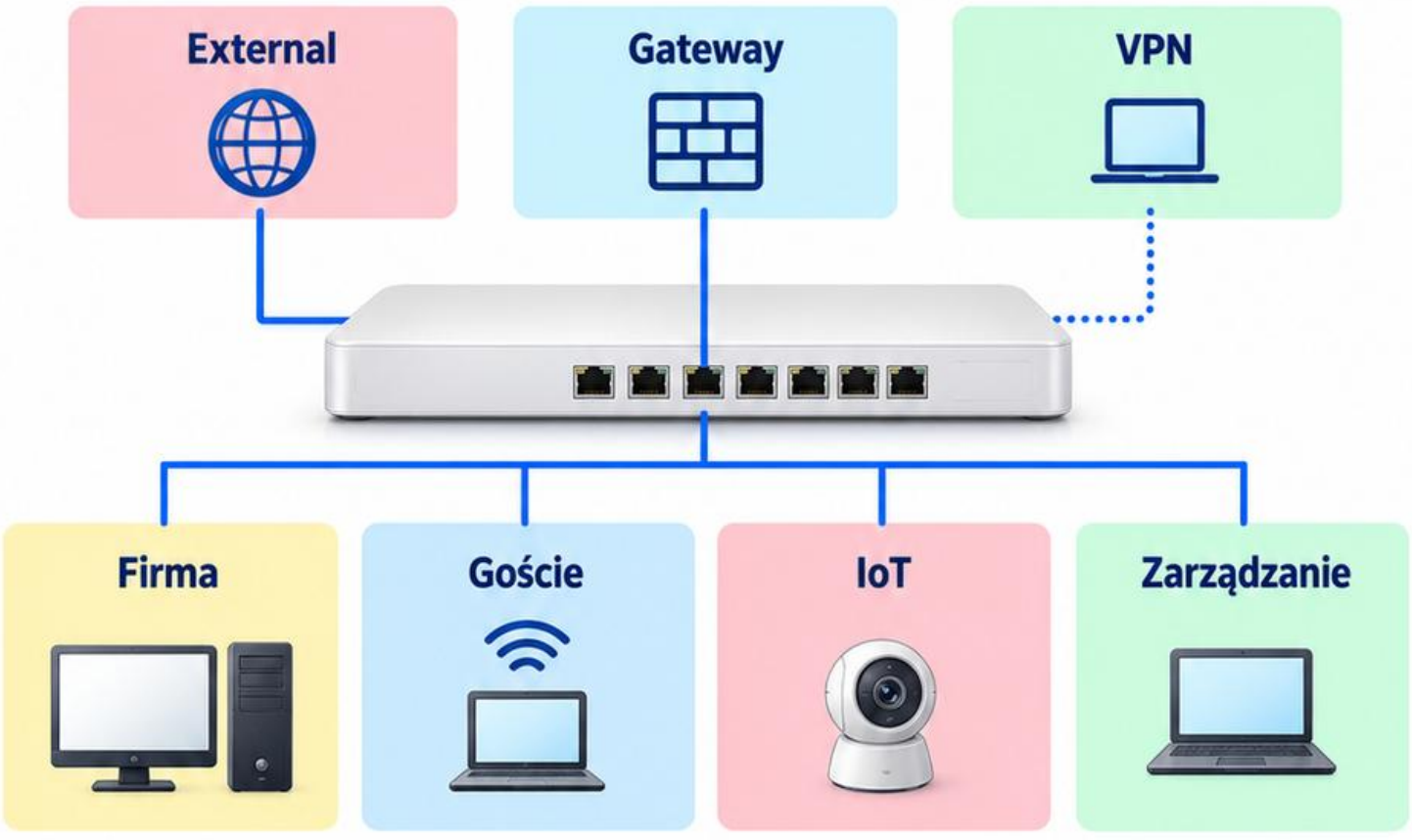
W Network 9.4 otwórz Settings > Zones; w 9.3 Settings > Policy Engine > Zones. Sprawdź przydział domyślny przed zmianą.

Utwórz projektowe strefy **Firma, Goście, IoT** i **Zarządzanie** albo odpowiednio wykorzystaj istniejące. Jedna sieć należy tylko do jednej strefy.

External opisuje WAN, a **Gateway** ruch do samej bramy. Pula zdalnego WireGuard wymaga sprawdzenia w relacjach strefy VPN.

Przykład: VLAN 30 przypisz do **IoT** dopiero po przygotowaniu DNS i DHCP. Zmiana strefy może natychmiast zmienić obowiązujące zasady dostępu.

Test: klient każdego segmentu zachowuje podstawowe usługi. **Cofnięcie:** przywróć poprzedni przydział sieci; nie usuwaj pochopnie stref wraz z jej politykami.



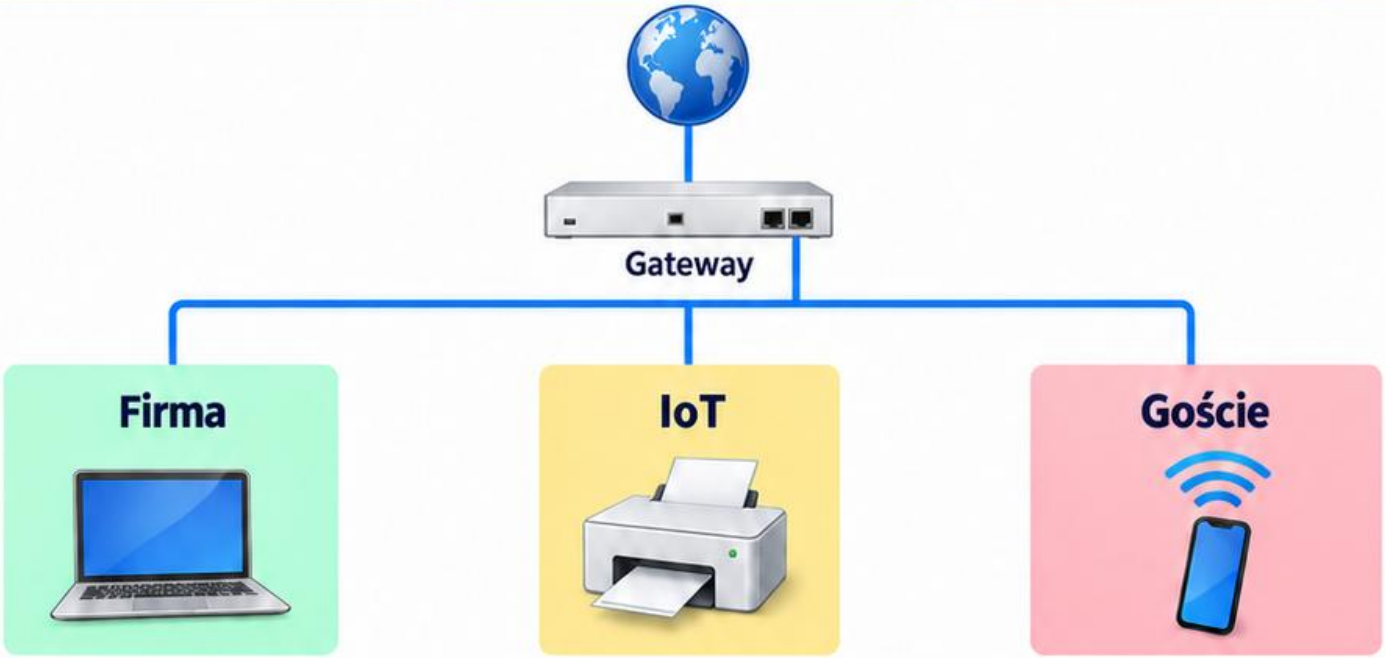
Źródła: [3]

Przeczytaj właściwe komórki macierzy

Cel: konfiguruj kierunek inicjowania połączenia. Wiersze macierzy to źródła, kolumny to cele; odpowiedź usługi rozpatruj przez stan połączenia.

W **Settings > Zones** wybierz **Firma → IoT.** To tutaj szukasz wyjątku drukowania, ponieważ laptop pracownika rozpoczyna połączenie do drukarki.

Następnie obejrzyj **Goście → Firma** i **IoT → Firma.** Są to odrębne relacje, które w projekcie mają ograniczać nowe połączenia.



Relacja	Zakres do sprawdzenia
Firma → IoT	Drukowanie: TCP 631 do 192.168.30.50
Goście → Firma	Nowe połączenia: blokada
IoT → Firma	Nowe połączenia: blokada
Firma → Gateway	DNS i DHCP: odrębna polityka

Przykład: odpowiedź drukarki na wydruk nie oznacza, że drukarka może rozpoczynać dowolną sesję do laptopa. Unikaj szerokiego zezwolenia zwrotnego.

Oddziel Firma → Gateway od **Firma → IoT.** Serwer DNS na bramie i drukarka w innym VLAN-ie wymagają innych celów polityki.

Test: zapisz źródło, cel i port dla każdej próby. Jeśli wybrana komórka nie odpowiada rzeczywistemu przepływowi, popraw ją przed zapisem reguły.
Źródła: [3]

Sprawdź stan domyślny

Cel: wiedzieć, co działa przed dodaniem własnych reguł. Domyślne strefy i wcześniej zapisane polityki mogą dopuszczać więcej niż projekt biura.

W Settings > Zones obejrzyj pary stref oraz pełną kolejność polityk. Zanotuj wbudowane reguły i wszystkie istniejące wyjątki administratorów.

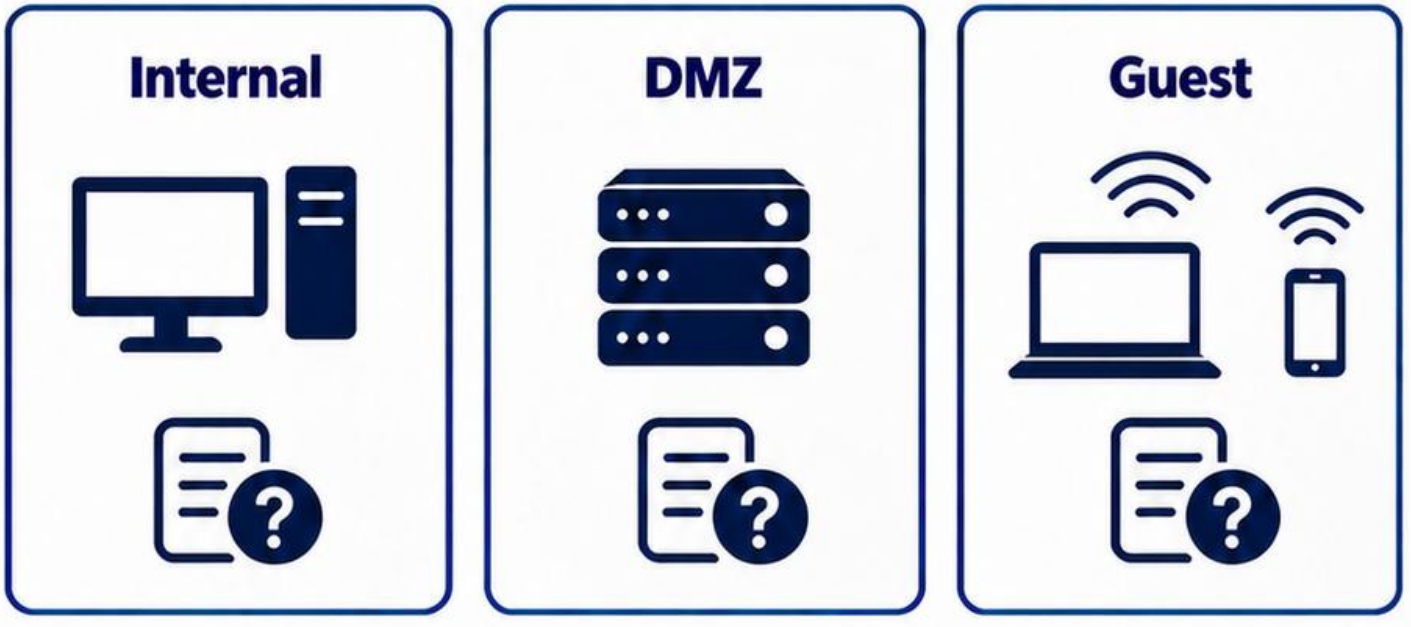
Przykład: urządzenia w Internal mogą mieć szeroki dostęp. Przeniesienie sieci do osobnych stref nie zastępuje sprawdzenia ich realnej komunikacji.

Przed blokadami upewnij się, że **Paweł** z **192.168.99.10** zachowuje lokalne zarządzanie. Potwierdź również DHCP i DNS każdego segmentu.

Reguły wbudowane mogą być oznaczone **kłódką.** Nie zakładaj, że wymagają usunięcia; własne polityki porządkuj tak, by realizowały zamierzony efekt.

Test: wykonaj macierz początkową i zapisz niespodziewane dostępy. To punkt odniesienia; po zmianach te same próby pokażą, co rzeczywiście ograniczono.

Reguły wbudowane mogą być oznaczone kłódką.



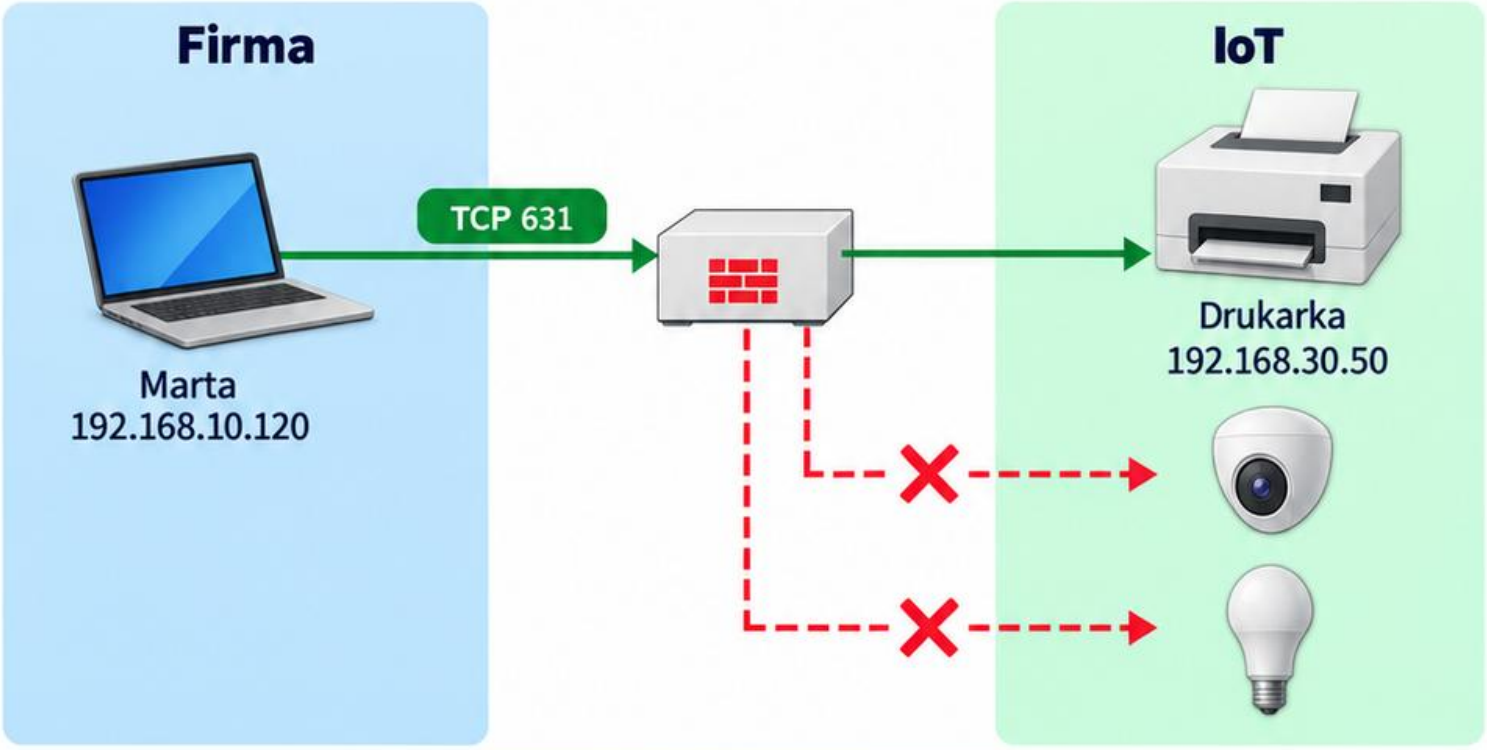
Sprawdź i zapisz wynik testu

Źródła: [3]

Dopuść minimalne usługi

Cel: pracownicy drukują, a pozostała komunikacja między Firmą i IoT pozostaje ograniczona. Nie potrzebujemy szerokiego dostępu do wszystkich urządzeń.

Network 9.4: Settings > Zones > Create Policy. Utwórz Allow dla Firma → IoT, cel 192.168.30.50 i protokół TCP z portem 631.



Parametry wynikają z potwierdzonego IPP tej drukarki. Jeżeli konkretne urządzenie wymaga innej usługi, najpierw zweryfikuj jej dokumentację oraz potrzebę biznesową.

Sprawdź ruch powrotny i położenie wyjątku względem blokady. Administracja drukarką nie otrzymuje automatycznie tego samego dostępu co samo drukowanie.

Przykład: Marta wysyła dokument z 192.168.10.120. Wydruk przechodzi, ale ten sam laptop nie otwiera dowolnych portów urządzeń IoT.

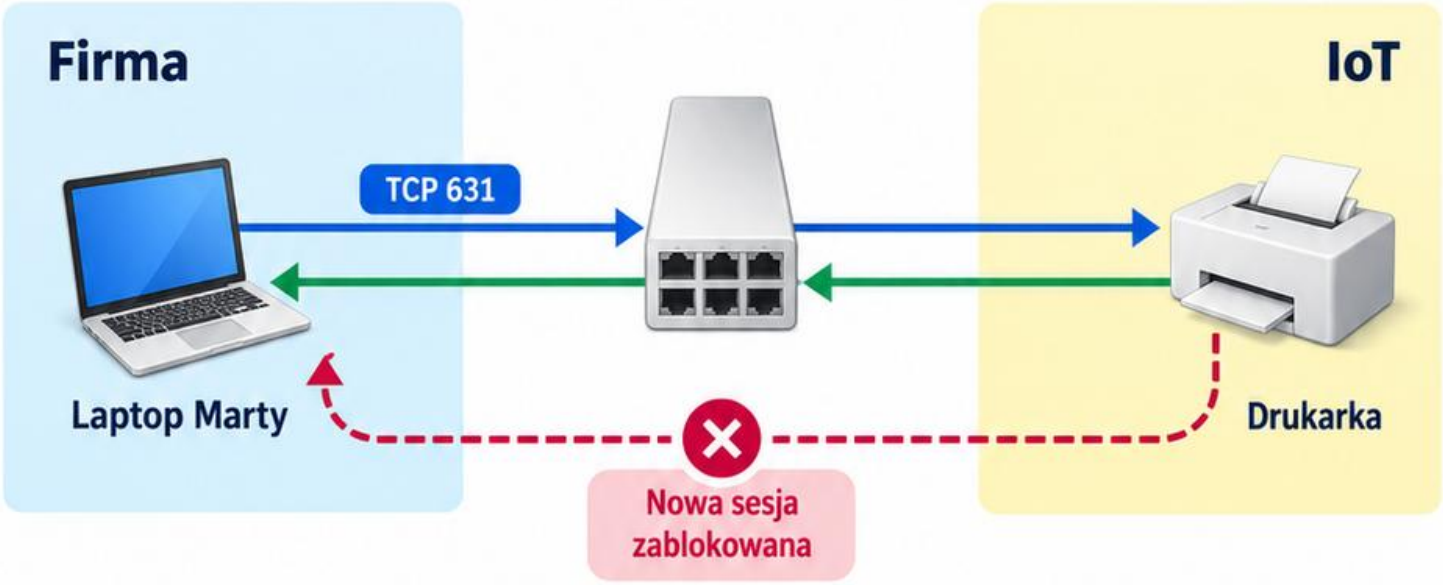
Test: rzeczywisty wydruk oraz próba niezatwierdzonej usługi. Jeśli wyjątek jest za szeroki, zawęź cel i port; nie rozszerzaj całej pary stref.

Źródła: [3]

Zachowaj odpowiedzi bez otwarcia dostępu

Cel: drukarka może odpowiadać na połączenie Marty bez uzyskania prawa inicjowania sesji do całej Firmy. Stan połączenia określa kontekst.

W polityce Allow sprawdź Auto Allow Return Traffic oraz istniejące zasady odpowiedzi. Nie dodawaj drugiego, ogólnego Allow z IoT do Firmy.



Przykład: TCP 631 laptop → drukarka otrzymuje odpowiedź.
Nowa sesja drukarka → laptop ma nadal być blokowana zgodnie z macierzą.

Przy diagnostyce rozróżniaj nowe i już zestawione sesje. Zapis zmienionej polityki nie musi od razu zakończyć wcześniej działającego połączenia.

Zamknij aplikację testową i utwórz nową sesję. Dla innego portu użyj oddzielnej próby, aby nie pomylić odpowiedzi z niezależnym dostępem.

Odbiór: wydruk działa, a nowa próba z IoT do Firmy nie przechodzi.
Cofając wyjątek, sprawdź także utworzoną automatycznie politykę odpowiedzi.

Źródła: [3]

Ułóż wyjątki przed blokadą

Cel: wąskie zezwolenie ma zostać rozpatrzone przed ogólną blokadą pasującego ruchu. Nazwa polityki nie ustala jej pierwszeństwa.

W widoku polityk Network 9.4 sprawdź kolejność i użyj **Reorder**. Analizuj wyłącznie reguły pasujące do tej samej pary stref i przepływu.

Projekt: Firma → drukarka TCP 631 otrzymuje Allow, a pozostałe niezatwierdzone połączenia Firma → IoT są blokowane poniżej.

Osobno IoT → Firma blokuje nowe połączenia. Nie przesuwaj przypadkowo szerokiego zezwolenia powyżej ograniczeń tylko po to, aby naprawić jedną aplikację.

Przykład błędu: drukarka przestaje odpowiadać poo dodaniu Block All nad wyjątkiem. Cofnij zmianę kolejności, zamiast otwierać wszystkie porty.

Test: nowy wydruk działa, inne usługi pozostają zablokowane. Zapisz kolejność w dokumentacji, bo same nazwy i adresy nie opisują efektu końcowego.



Kolejność polityk dla ruchu Firma → IoT

1	Firma → drukarka TCP 631	Allow
2	Firma → IoT (pozostałe)	Block

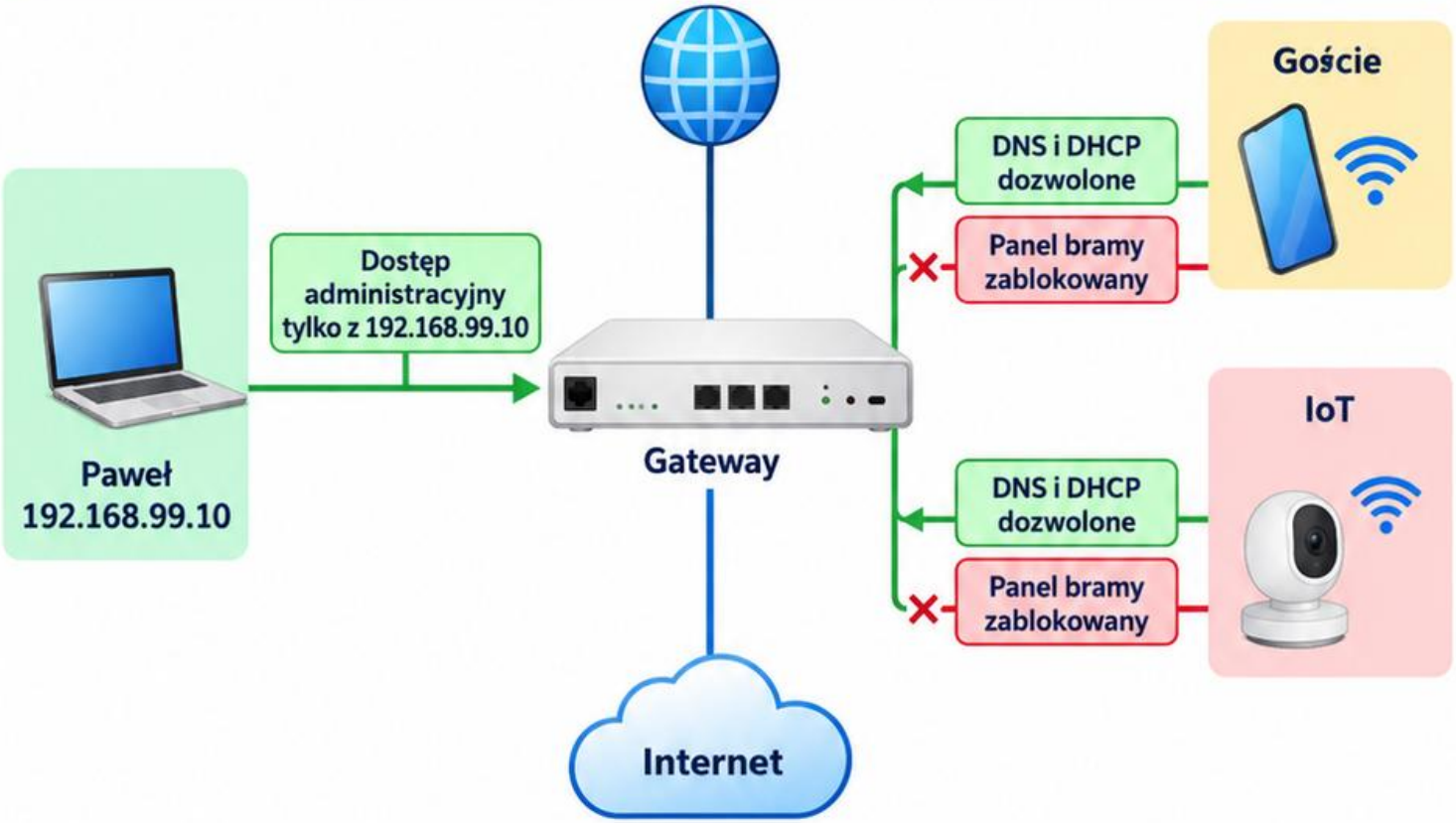
Polityka dla ruchu IoT → Firma

1	IoT → Firma (nowe połączenia)	Block

Źródła: [3]

Ogranicz panel bramy

Cel: Goście i IoT korzystają z potrzebnych usług, lecz nie administrują bramą. Dostęp Pawła pozostaje niezależny od ogólnej sieci Firmy.



1. Najpierw sprawdź lokalne logowanie z 192.168.99.10. W macierzy stref oceniaj ruch do Gateway oddzielnie od ruchu pomiędzy sieciami.

2. Zachowaj wymagany DNS i DHCP, a potem ogranicz pozostałe połączenia z Gości oraz IoT do bramy zgodnie z zatwierdzoną macierzą.

3. Dostęp administracyjny dopuszczaj z ustalonego źródła i tylko do wymaganych usług. Nie publikuj panelu HTTPS ani SSH na WAN.

4. Przykład: telefon Gościa rozwiązuje nazwy przez 192.168.20.1, ale próba otwarcia panelu pod tym adresem nie daje dostępu administracyjnego.

5. **Test:** nowa dzierżawa, DNS, internet, panel Gościa oraz świeże logowanie Pawła. Jeśli ostatni test zawodzi, wycofaj blokadę przez zachowaną ścieżkę lokalną.

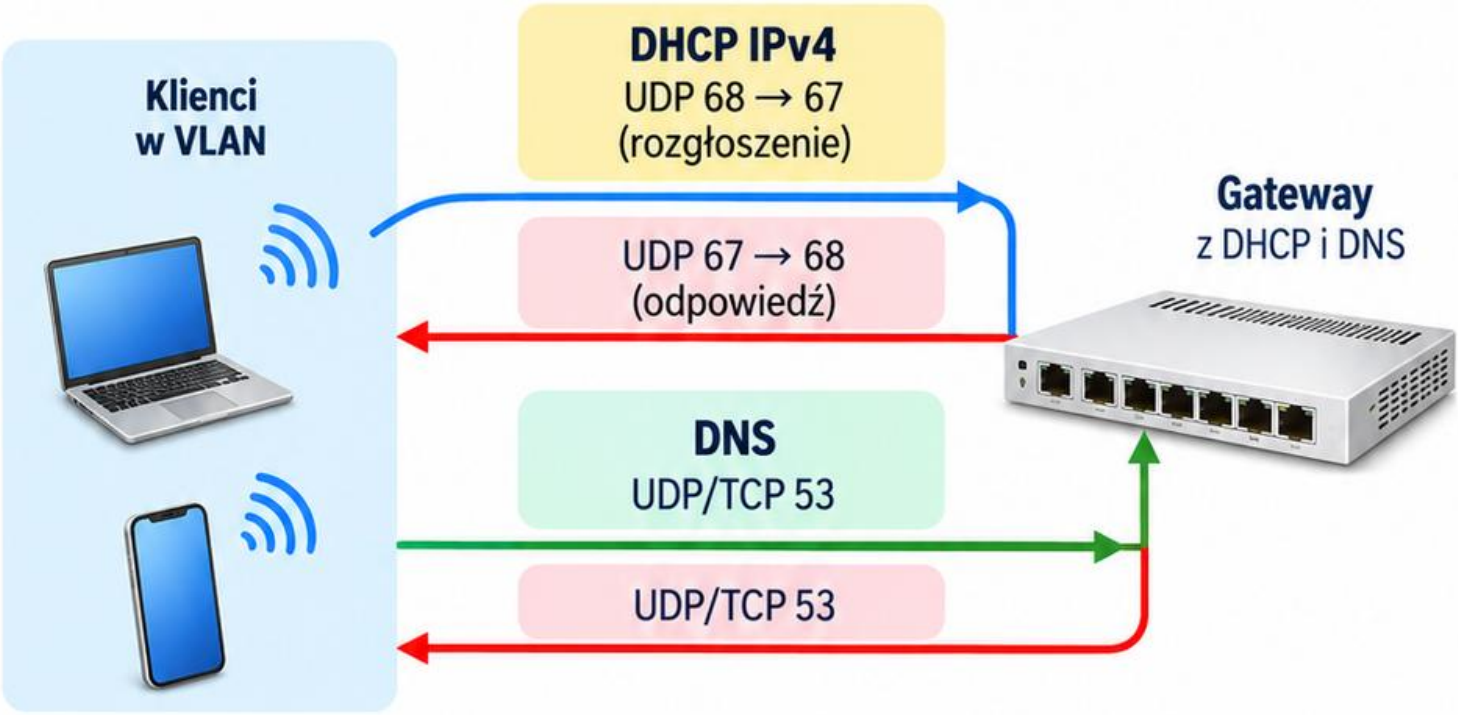
Źródła: [3]

Zachowaj wyjątki DHCP oraz DNS

Ostoja • Wdrożenie zintegrowane • 24

Cel: uniknąć awarii wszystkich klientów podczas ochrony Gateway. W scenariuszu serwery DNS i DHCP działają na interfejsach bramy właściwych VLAN-ów.

DNS: dopuść zapytania klientów do właściwego adresu .1 przez UDP i TCP 53. Nie otwieraj przez pomyłkę wszystkich usług Gateway.



DHCP IPv4: uwzględnij UDP klient 68 → serwer 67 oraz odpowiedzi; początkowe pozyskanie adresu może używać rozgłoszenia, nie zwykłego unicastu.

Przykład: nowy telefon Gościa bez dzierżawy musi otrzymać 192.168.20.x. Polityka dopuszczająca tylko aktualne adresy klientów może pominąć tę fazę.

Sprawdź istniejące polityki wbudowane i zachowaj potrzebne przepływy. Jeśli serwer jest zewnętrzny lub działa relay, projekt wyjątków będzie inny.

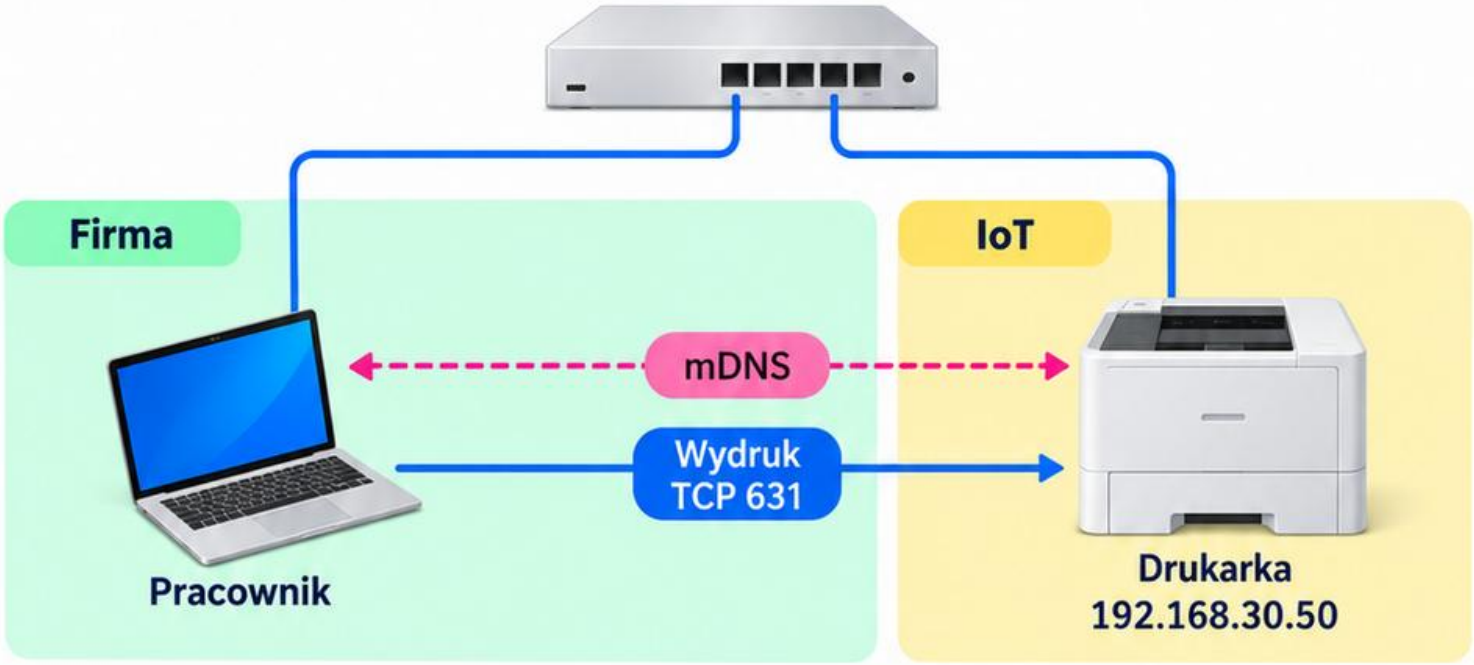
Test: urządzenie bez zapisanej dzierżawy uzyskuje adres, odnawia go i rozwiązuje nazwę. Przy awarii wycofaj ostatnią blokadę Gateway, zachowując logi.

Źródła: [3], [1]

Udostępnij drukarkę świadomie

Cel: pracownik odnajduje i wykorzystuje drukarkę, ale IoT nie zyskuje szerokiego dostępu do Firmy. Odkrywanie usługi to osobny przepływ.

Najpierw potwierdź wydruk bezpośrednio do 192.168.30.50. Jeżeli działa, podstawowy routing i TCP 631 są poprawne; problem może dotyczyć wykrywania.



Preferuj udokumentowaną konfigurację drukarki po stałym adresie lub nazwie. Refleksję mDNS rozważ dopiero wtedy, gdy aplikacja rzeczywiście jej wymaga.

W ustawieniach mDNS swojej wersji wybierz tylko potrzebne sieci Firma i IoT. Nie włączaj wymiany z Gośćmi ani Zarządzaniem bez uzasadnienia.



Samo pojawienie się urządzenia na liście nie otwiera jego usługi. Zachowaj oddzielny, wąski wyjątek do drukarki i kontrolę kierunku połączeń.

Test: wydruk działa także po ponownym połączeniu klienta. Gość nie odkrywa zasobów firmy; przy nadmiarowym ujawnianiu wyłącz refleksję i użyj adresu.

Źródła: [3], [1]

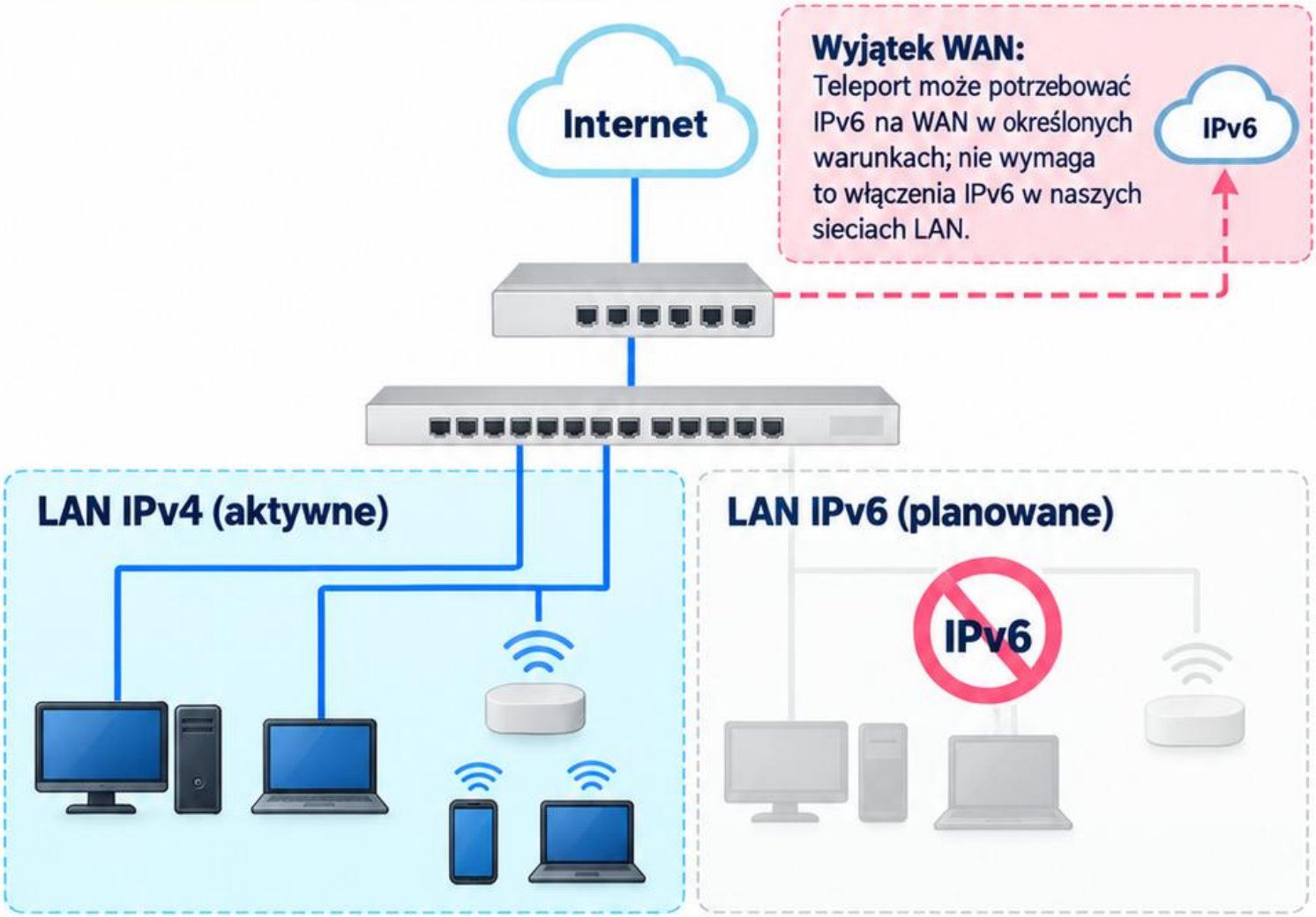
Zapisz decyzję o IPv6

Cel: segmentacja ma obejmować każdą używaną rodzinę adresów. W tym wdrożeniu LAN działa początkowo wyłącznie z planowaną adresacją IPv4.

Nie uruchamiamy IPv6 na VLAN-ach, dopóki nie ma prefiksu operatora, projektu /64 na segment i równoważnych testów firewalla. To decyzja projektu.

Lokalne adresy link-local klientów nie oznaczają automatycznie globalnej łączności IPv6. Sprawdź otrzymywane trasy, router advertisements oraz rzeczywisty dostęp między sieciami.

Gdy dodasz IPv6, polityki obejmą obie rodziny, z zachowaniem mechanizmów ICMPv6 niezbędnych do działania. Nie stosuj ogólnego zakazu ICMPv6 jako skrótu.



Test: zapisz brak nieplanowanej globalnej trasy IPv6. Po przyszłym wdrożeniu powtórz całą macierz dostępu osobno dla IPv4 i IPv6.

Źródła: [3], [43]

Przeprowadź próby zakazanego dostępu

Cel: odbiór obejmuje również to, co ma nie działać. Każdy wynik opisuj źródłem, celem, usługą i świeżą sesją testową.

Goście → system dokumentów 192.168.10.20: blokada.



Goście → panel bramy: blokada.



IoT → stanowisko Firmy: blokada.



Firma → drukarka TCP 631: działa.



Goście → DNS własnej bramy: działa.



Paweł → wymagane zarządzanie z 192.168.99.10: działa.



Osobno sprawdź komunikację dwóch gości w tym samym VLAN-ie. Jej ograniczenie zależy od izolacji klientów lub zgodnych mechanizmów warstwy drugiej.



Przykład: dwa telefony przy różnych AP-ach nie powinny wymieniać danych, jeśli taki jest wymóg biura. Zweryfikuj wszystkie możliwe drogi, również przewodowe.

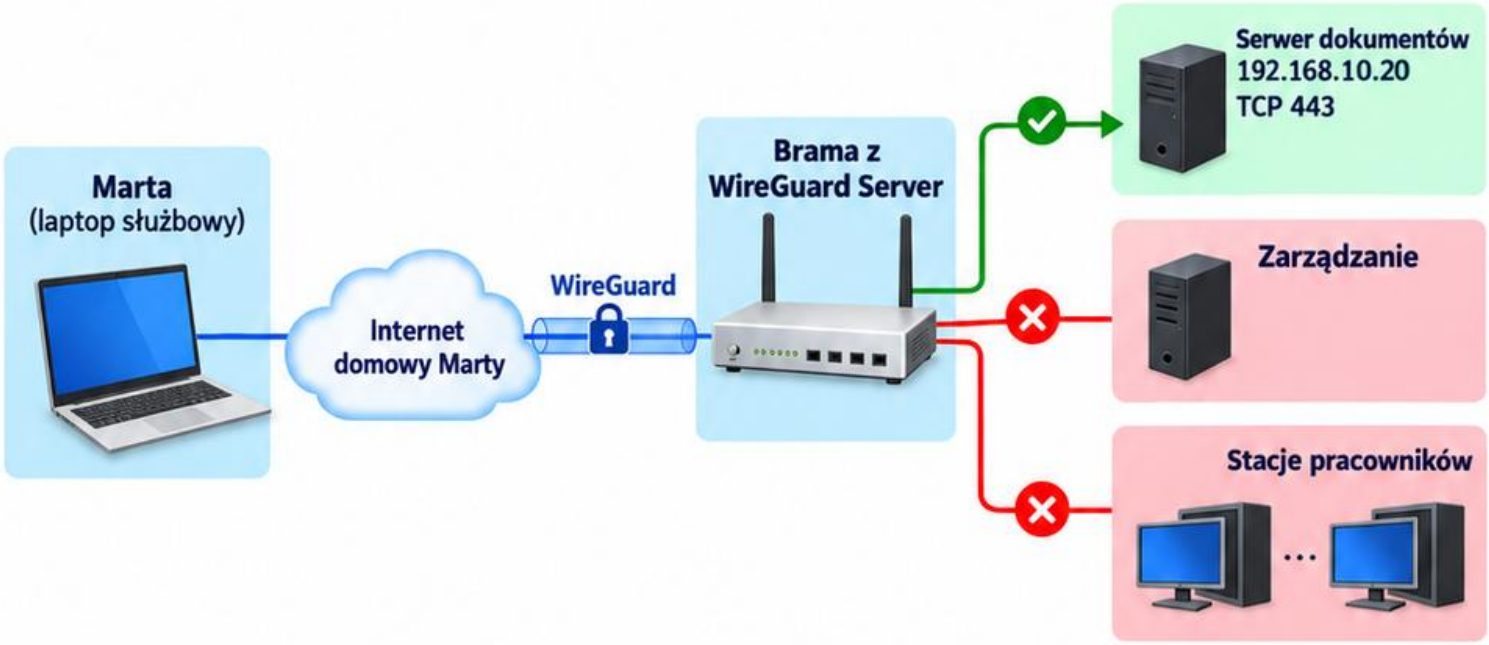
Odbiór: wszystkie próby odpowiadają macierzy i żaden wyjątek nie jest szerszy niż potrzeba. Rozbieżność popraw przed włączeniem zdalnego dostępu.

Źródła: [3], [20]

Wybierz dostęp zdalny Marty

Cel: Marta potrzebuje systemu dokumentów, a nie całej infrastruktury biura. Dostęp przypisz jej służbowemu laptopowi i zaplanuj odebranie uprawnień.

Wybieramy **WireGuard Server** na zgodnej bramie, z jednym profilem na urządzenie. Alternatywny **Teleport** wymaga osobnego sprawdzenia warunków i sposobu zarządzania klientami.



Dozwolony zasób to 192.168.10.20, TCP 443. Nie udostępniamy przez VPN Zarządzania ani wszystkich stacji pracowników.

Pula VPN 10.250.0.0/24 jest oddzielna od LAN-u Krakowa i planowanego Poznania. Sprawdź także sieć domową Marty przed testem.

Przykład: Marta korzysta z internetu domowego, a dokumenty otwiera przez tunel. Nie publikujemy panelu bramy ani serwera dokumentów jako skrótu do wdrożenia.

Test: połączenie spoza biura, właściwa aplikacja i brak dostępu do infrastruktury. **Cofnięcie:** unieważnij klienta testowego i potwierdź brak nowej sesji.

Źródła: [22], [3], [43]

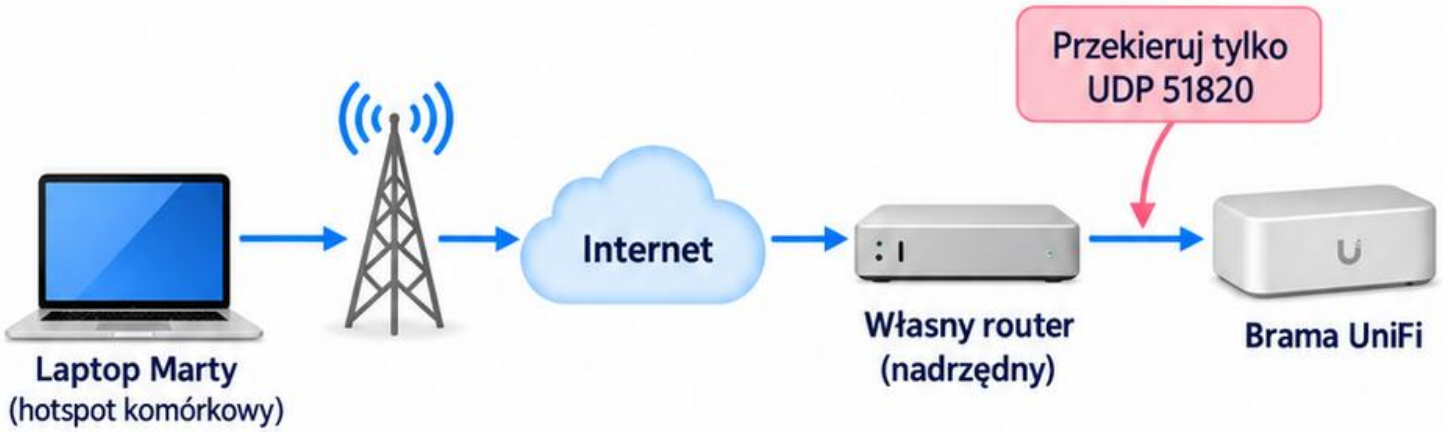
Zweryfikuj WAN i NAT przed VPN

Cel: laptop Marty musi dosięgnąć końca tunelu. Ustal, czy WAN bramy ma publiczny adres i czy operator nie stosuje CGNAT.

Porównaj adres WAN z publicznym adresem widocznym z internetu. Gdy są różne, sprawdź własny router nadrzędny oraz warunki usługi operatora.

W projekcie prosimy operatora o publiczną osiągalność. Jeśli przed UniFi stoi własny router, przekieruj wyłącznie ustalony port WireGuard do WAN UniFi.

Domyślny port WireGuard to UDP 51820. Przekierowanie tego portu nie oznacza otwarcia panelu zarządzania; panel pozostaje niedostępny z WAN.



Przykład: test we własnym Wi-Fi może ukryć problem osiągalności zewnętrznej. Marta przeprowadza próbę przez hotspot komórkowy.

Test: handshake pojawia się z zewnątrz. Przy CGNAT uzgodnij rozwiązanie z operatorem lub zweryfikuj alternatywny VPN; nie dodawaj losowych przekierowań.

Źródła: [22], [40]

Uruchom pilotażowy WireGuard

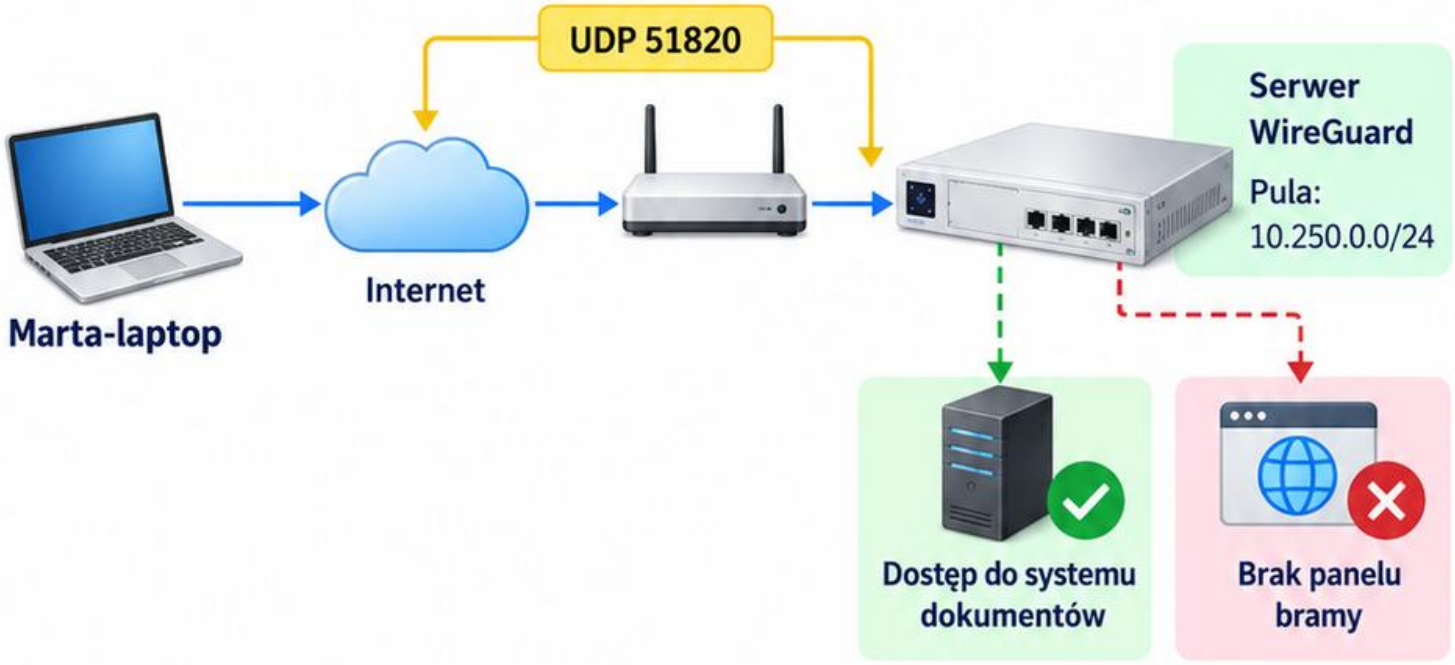
Cel: zestaw jedno kontrolowane połączenie przed wydaniem dostępu produkcyjnego. LAN i izolacja powinny być już odebrane na wcześniejszych stronach.

1 **W sekcji VPN aplikacji Network utwórz serwer WireGuard.**

Użyj zatwierdzonego adresu końcowego i zaplanowanej puli 10.250.0.0/24.

2 **Ustal port UDP 51820 albo świadomie wybrany inny port.**

Jeżeli występuje własny router nadrzędny, jego przekierowanie musi wskazywać ten sam port.



3 **Dodaj klienta Marta-laptop.**

Przed pierwszą próbą przygotuj minimalne polityki VPN i DNS, zamiast pozostawiać szerokie domyślne uprawnienia.

4 **Przykład:**

klient pilotażowy otrzymuje adres z puli VPN, lecz dostęp do systemu dokumentów nadal zależy od trasy oraz reguł.

5 **Test:**

aktualny handshake, działający TCP 443 do serwera i brak panelu bramy:

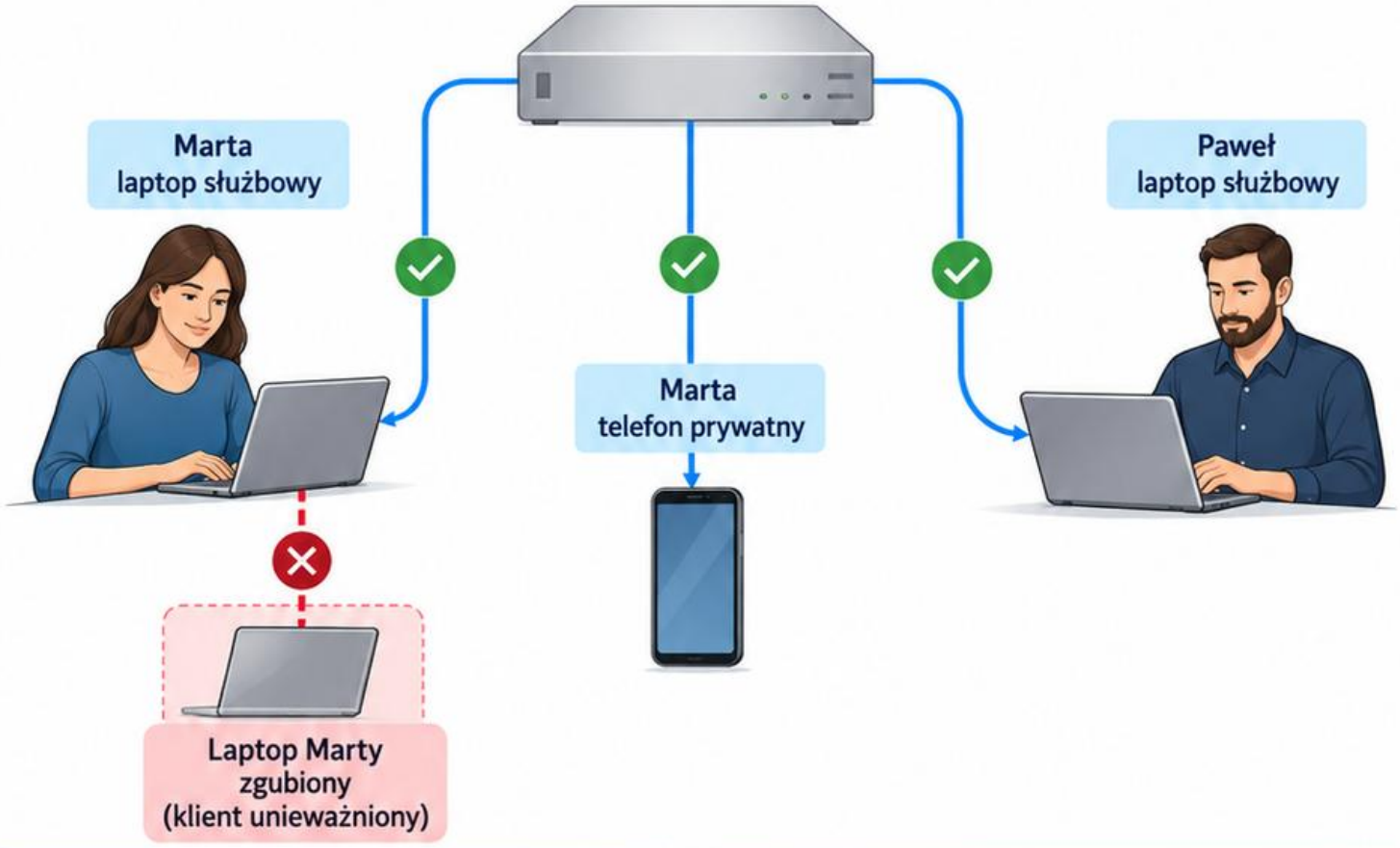
Cofnięcie: wyłącz serwer pilotażowy, zachowując konfigurację LAN.

Źródła: [22], [3]

Wydaj profil i zapisz właściciela

Cel: dostęp Marty ma być identyfikowalny oraz odwoływalny bez wpływu na innych użytkowników. Jedno urządzenie otrzymuje **jeden profil.**

W konfiguracji **WireGuard** dodaj klienta o jednoznacznej nazwie. W rejestrze zapisz właściciela, sprzęt, datę wydania i termin przeglądu.





Profil oraz kod QR mogą zawierać klucz prywatny. Przekaż je prywatnie i nie umieszczaj w PDF-ie dokumentacji, zgłoszeniu publicznym ani zrzucie ekranu.



Marta importuje profil do oficjalnego klienta na służbowym laptopie. Drugi telefon wymaga osobnego wpisu zamiast skopiowania tego samego pliku.



Przykład zdarzenia: laptop zostaje zgubiony. Paweł unieważnia jego klienta, a pozostałe urządzenia zachowują własne, niezależne dostępy.



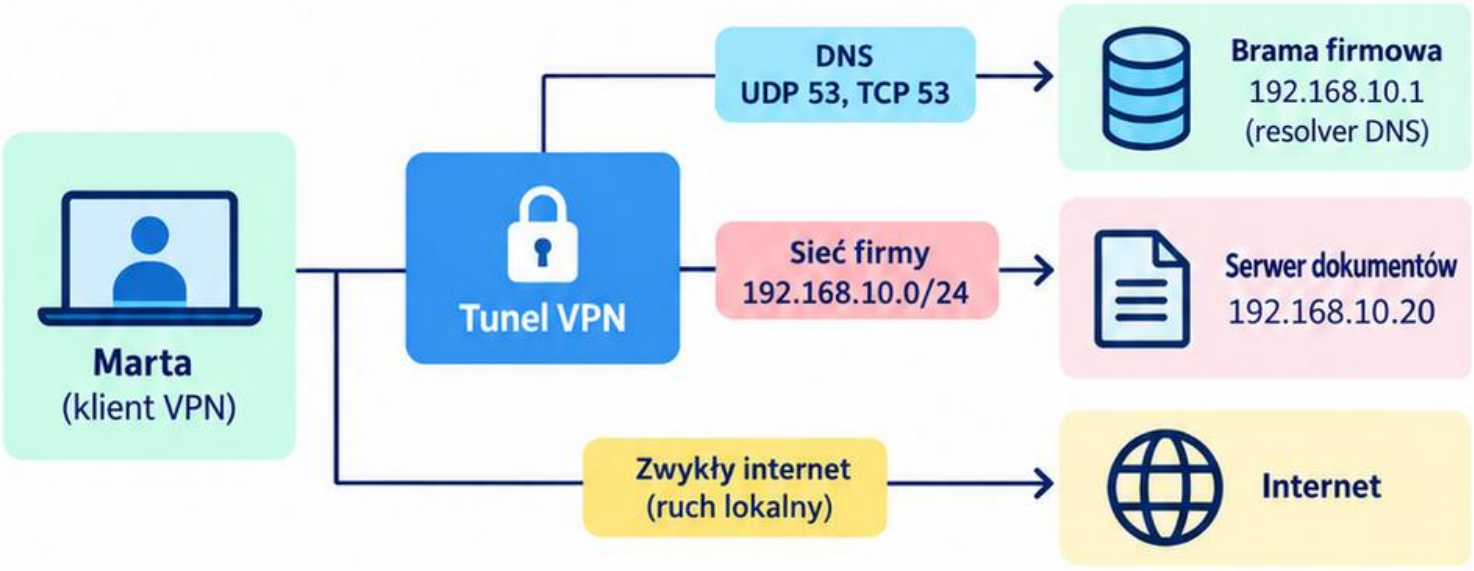
Test: po odebraniu profilu nowa sesja nie powstaje. Jeśli konfiguracja wyciekła, wydaj nowy profil z nowymi kluczami; samo usunięcie kopii z dokumentu nie wystarcza.

Źródła: [22]

Dostarcz trasę i DNS przez tunel

Ostoja • Wdrożenie zintegrowane • 32

Cel: Marta odnajduje serwer po nazwie i dociera do niego przewidywalną drogą. W tym projekcie stosujemy tunel dzielony dla zasobów firmy.



Sprawdź trasy klienta obejmujące 192.168.10.0/24.
Profil musi też zapewniać drogę do DNS 192.168.10.1, bo resolver działa na bramie.

W politykach zachowaj VPN → Gateway dla DNS przez UDP oraz TCP 53.
Dostęp do serwera dokumentów jest osobnym wyjątkiem VPN → Firma.

Przykład nazwy wewnętrznej: dokumenty.biuro.example.
To nazwa demonstracyjna; produkcyjnie użyj domeny kontrolowanej przez firmę i zgodnego certyfikatu HTTPS.

Najpierw sprawdź adres serwera, potem zapytanie do wskazanego DNS, następnie nazwę w aplikacji.
Publiczny resolver nie zna automatycznie prywatnych rekordów.

Test: aplikacja działa po nazwie, a zwykły internet używa zatwierdzonej drogi.
Przy błędzie cofnij zmianę profilu, nie otwierając całej strefy Gateway.

Źródła: [22], [3]

Ogranicz zdalny dostęp do aplikacji

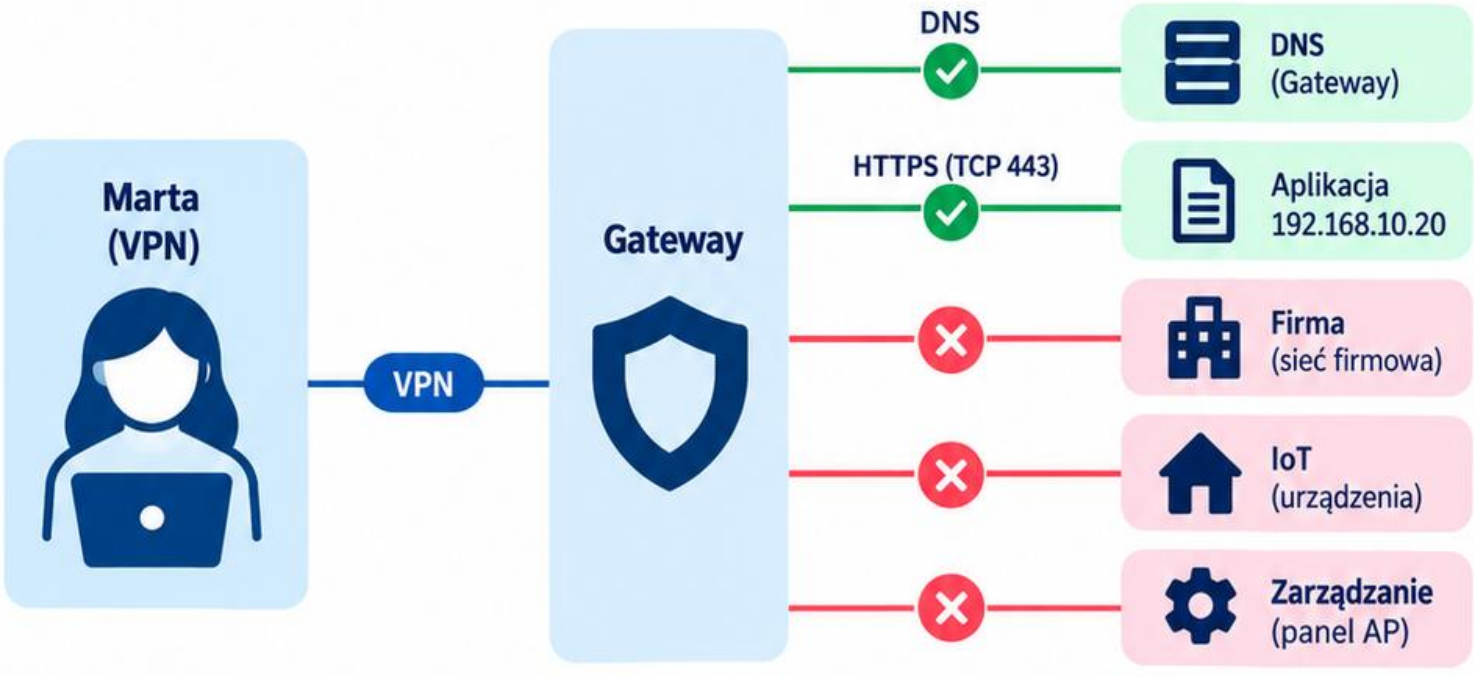
Cel: samo posiadanie tunelu nie daje dostępu do Zarządzania. Uprawnienia Marty mają odzwierciedlać jej rolę w biurze.

W Network 9.4 otwórz Settings > Zones. Dla właściwego klienta lub zakresu VPN dopuść cel **192.168.10.20, TCP 443**, z potrzebnym ruchem powrotnym.

Zachowaj osobny wyjątek DNS do Gateway, a następnie zablokuj niezatwierdzone nowe połączenia VPN do Firmy, IoT i Zarządzania.

Przykład: Marta odczytuje dokumenty, ale **nie otwiera panelu AP** ani sesji do komputera koleżanki. Administrator korzysta z odrębnego zatwierdzonego dostępu.

Sprawdź rzeczywisty przydział strefy i możliwość rozróżnienia klientów w swojej wersji. Nie zakładaj, że nazwa profilu sama tworzy regułę uprawnień.

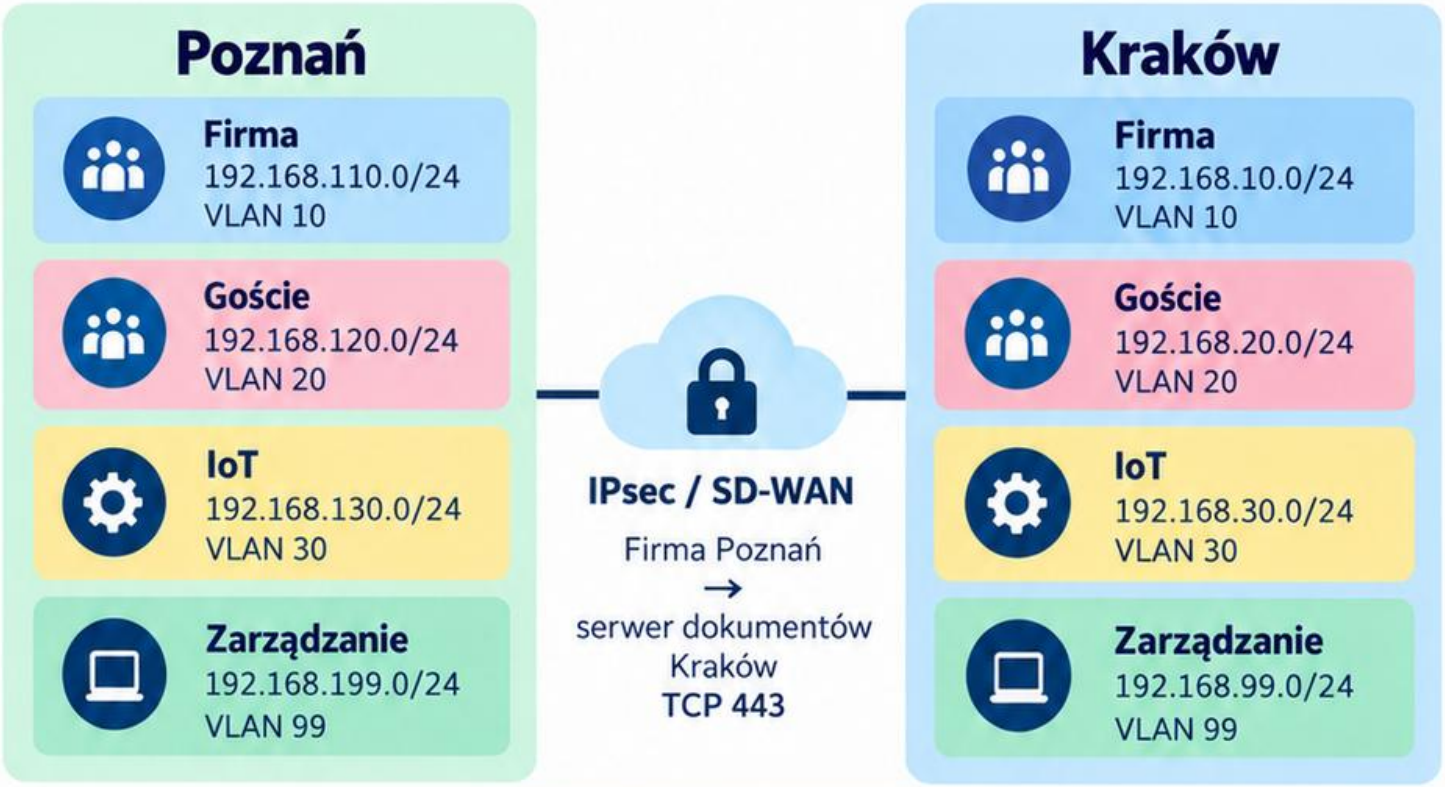


Test: aplikacja i DNS działają, trzy próby zakazanego dostępu są blokowane. Paweł potwierdza lokalne zarządzanie po każdej zmianie.

Źródła: [3], [22]

Dołącz oddział w Poznaniu

Cel: oddział wymienia wyłącznie potrzebne dane z Krakowem. Nie rozciągamy wspólnej domeny VLAN między miastami ani nie kopiujemy podsieci.



Poznań: Firma 192.168.110.0/24, Goście 192.168.120.0/24, IoT 192.168.130.0/24, Zarządzanie 192.168.199.0/24. Numery VLAN pozostają 10, 20, 30, 99.

Kraków zachowuje 192.168.10.0/24, .20.0/24, .30.0/24 i .99.0/24. Pula użytkowników VPN 10.250.0.0/24 również pozostaje rozłączna.

W zgodnym IPsec lub SD-WAN udostępnij wyłącznie sieci wymagane przez aplikację. Preferujemy Firma Poznań → serwer dokumentów Kraków, TCP 443.

Uzgodnij parametry tunelu, trasy i firewall po obu stronach. Przy SD-WAN sprawdź wymagania modeli, konta właściciela lub Fabric oraz topologii.

Test: Poznań otwiera dokumenty, lecz Goście i Zarządzanie nie uzyskują nieplanowanej łączności. Cofnięcie: wyłącz tunel i związane z nim trasy.

Źródła: [41], [44], [3]

Zdecyduj o drodze podczas awarii

Cel: awaria tunelu nie może wysłać poufnego ruchu przypadkową drogą. Ustal zachowanie przed pierwszym testem przeciążenia lub zaniku WAN.

Network 9.4: Settings > Policy Table > Create New Policy > Route.
W 9.3 użyj Settings > Policy Engine > Policy-Based Routes.

Jeśli stosujesz PBR, wskaż źródło, cel i zatwierdzony tunel.
Kill Switch włączony zatrzymuje pasujący ruch po utracie wybranego interfejsu.

Dla zwykłej trasy do prywatnej podsieci sprawdź również brak niepożądanej **drogi domyślnej;** sam tunel nie definiuje wszystkich reguł awarii.

Awaria tunelu: ruch poufny zostaje zatrzymany



Awaria tunelu: goście przechodzą na WAN2



Przykład: Goście mogą przejść na WAN2, ale dokumenty między placówkami mają pozostać dostępne wyłącznie przez zatwierdzony tunel. To różne wymagania.

Test: kontrolowanie przerwij tunel, sprawdź zatrzymanie usługi i zmierz powrót. Przywróć pierwotny stan; zapisz wynik zamiast obiecywać zerową przerwę.

Źródła: [42], [44]

Przygotuj wspólny plan wycofania

Cel: cofnięcie zmian ma działać także po utracie części sieci. Zachowaj logiczną kolejność i dostęp lokalny w obu placówkach.

1. **Przed oknem pobierz kopię przez Settings > Control Plane > Backups.** Zapisz poprzednie przydziały stref, profile portów i konfiguracje tuneli.



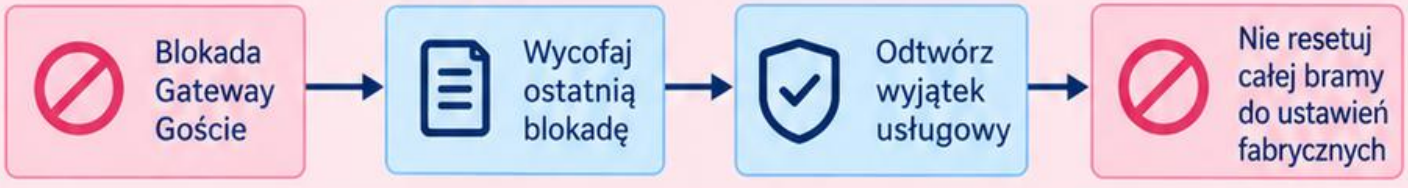
2. **Najpierw wyłącz ostatnią trasę PBR lub tunel testowy,** jeśli to one spowodowały awarię. Potem przywróć konkretną politykę albo profil portu.



3. **Migrację zarządzania cofaj przez przygotowany port ratunkowy.** Nie usuwaj wszystkich stref, ponieważ usunięcie strefy kasuje również powiązane polityki.



4. **Przykład: po blokadzie Gateway Goście tracą DHCP.** Wycofaj ostatnią blokadę i odtwórz wyjątek usługowy; nie resetuj całej bramy do ustawień fabrycznych.



5. **Test:** druga osoba odnajduje kopię i wykonuje instrukcję na stanowisku kontrolowanym. Backup konfiguracji nie jest automatycznym sposobem cofnięcia firmware.

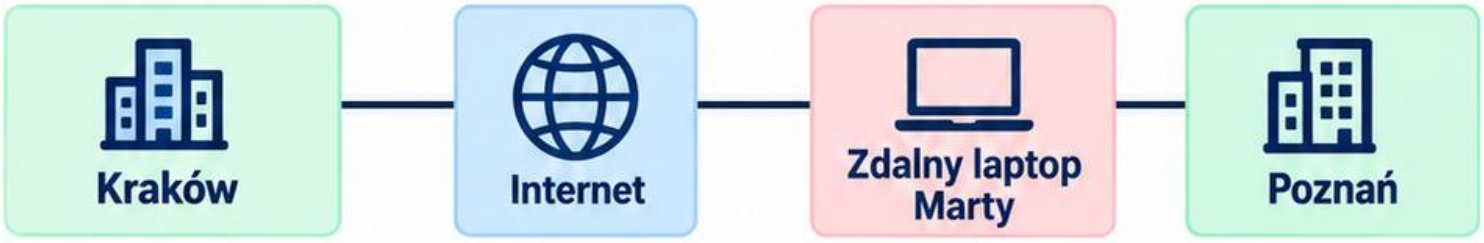


Źródła: [8], [3], [42]

Zamknij przypadek wynikami

Ostoja • Wdrożenie zintegrowane • 37

Cel: Marta akceptuje sieć na podstawie sprawdzonych usług i ograniczeń. Protokół obejmuje Kraków, zdalny laptop i dostęp z Poznania.



Wyniki pozytywne:

- DHCP i DNS czterech VLAN-ów
- wydruk z Firmy
- system dokumentów lokalnie i przez VPN
- lokalna administracja Pawła

Wyniki negatywne:

- Goście nie osiągają Firmy ani panelu
- IoT nie inicjuje sesji do pracowników
- Marta nie administruje infrastrukturą przez swój profil.

Dodatkowo: awaria tunelu zachowuje zatwierdzoną politykę, a próba odtworzenia potwierdza użyteczność kopii. Dopisz rzeczywiste daty, wersje i zmierzone czasy.

Przykład wpisu: test VPN-03, laptop Marty przez sieć komórkową, dokumenty HTTPS dostępne, panel bramy niedostępny, wynik zgodny z oczekiwaniem.

Odbiór: właściciele podpisują wyniki i listę otwartych usterek. Przegląd uprawnień oraz kopii wpisz do harmonogramu; sekrety przekaż oddzielnie.

Źródła: [3], [8], [22]

Źródła

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

[8] **Kopie i migracja**
https://help.ui.com/hc/en-us/articles/360008976393

[20] **Izolacja sieci i klientów**
https://help.ui.com/hc/en-us/articles/18965560820247

[22] **Serwer WireGuard**
https://help.ui.com/hc/en-us/articles/115005445768

[40] **VPN i przekierowanie portów**
https://help.ui.com/hc/en-us/articles/30050679793431

[41] **IPsec z zewnętrzną bramą**
https://help.ui.com/hc/en-us/articles/7983431932439

[42] **Routing według polityk**
https://help.ui.com/hc/en-us/articles/12566175125783

[43] **VPN Teleport**
https://help.ui.com/hc/en-us/articles/5246403561495

[44] **Konfiguracja SD-WAN**
https://help.ui.com/hc/en-us/articles/16750417515159