Ostoja

30 gotowych diagnoz UniFi

Przypadki, testy rozstrzygające i bezpieczne naprawy



Jak korzystać z gotowych diagnoz

1

Wybierz przypadek podobny do swojej sytuacji. Porównaj miejsce, klienta i ostatnią zmianę; sam nagłówek objawu nie wystarcza.

2

Przed próbą zapisz wersję, czas, właściwy port lub AP oraz stan usługi. Przygotuj lokalny dostęp i sposób cofnięcia zmiany.

3

Wykonaj test rozstrzygający. Jego wynik ma odróżnić co najmniej dwie hipotezy; brak dowodu oznacza dalszy pomiar, a nie przypadkową naprawę.

4

Zastosuj działanie wyłącznie z potwierdzonej gałęzi. Zmieniaj jeden element naraz, zachowując poprzedni parametr oraz osobę odpowiedzialną za powrót.

5

Powtórz zadanie użytkownika i próbę porównawczą. Sprawdź również ograniczenie dostępu, jeśli naprawa dotyczy segmentacji lub VPN.

Przykładowy przebieg



Wybierz przypadek podobny do swojej sytuacji. Porównaj miejsce, klienta i ostatnią zmianę.

Przed próbą zapisz wersje, czas, właściwy port lub AP oraz stan usługi. Przygotuj lokalny dostęp i sposób cofnięcia zmiany.

Wykonaj test rozstrzygający.

Hipoteza A
Wynik nie potwierdza.

Hipoteza B
Wynik potwierdza.

Brak dowodu
oznacza dalszy pomiar,
a nie przypadkową naprawę.

Zastosuj działanie wyłącznie z potwierdzonej gałęzi. Zmieniaj jeden element naraz, zachowując poprzedni parametr oraz osobę odpowiedzialną za powrót.

Powtórz zadanie użytkownika i próbę porównawczą. Sprawdź również ograniczenie dostępu, jeśli naprawa dotyczy segmentacji lub VPN.

Przydatne pola incydentu

Miejsce

Klient

Ostatnia zmiana

Stan usługi

Przypadki są modelowe.
Adresy, możliwości sprzętu i oczekiwane wyniki porównaj z własnym projektem; nie kopiuj sekretów do notatek.

Zapis diagnozy:
przypadek ____; dowód ____; zmiana ____; wynik ____; cofnięcie ____.

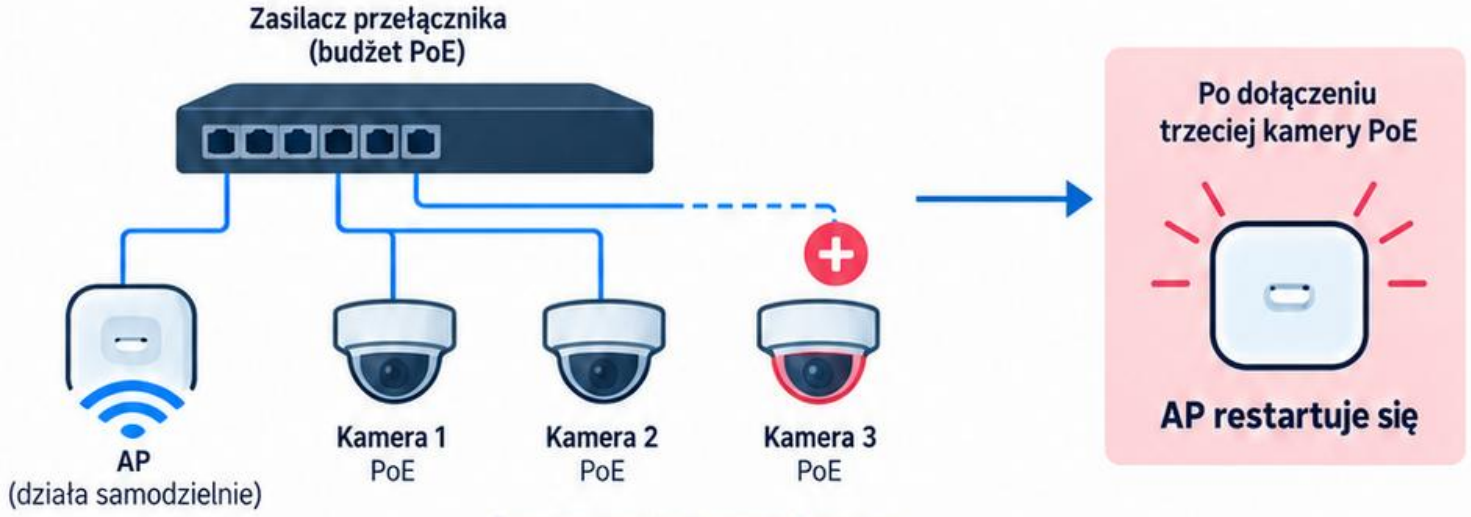
AP restartuje się dopiero po podłączeniu trzeciej kamery

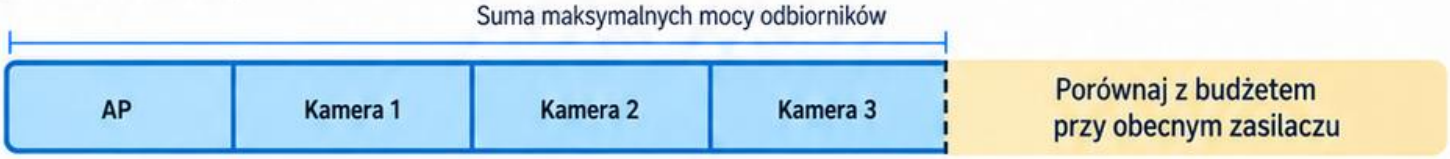
Ostoja • Diagnoza 01



Kontekst:
Paweł, 38 lat, administrator biura w Łodzi.

Objaw:
AP działa samodzielnie; restart pojawia się po dołączeniu trzeciej kamery PoE.





Test rozstrzygający:
Porównaj sumę maksymalnych mocy z budżetem przy obecnym zasilaczu; potem użyj sprawnego krótkiego przewodu.

Jeśli limit łączny przekroczony

Jeśli limit łączny nieprzekroczony

- Nie oceniaj rezerwy na podstawie spokojnej godziny.
- W specyfikacji odbiorników odczytaj wymagany standard oraz moc maksymalną.
- Zanotuj model zasilacza przełącznika i moment restartu AP.
- Zapisz, które odbiorniki pozostawały aktywne w chwili awarii.

Działanie:
Jeśli limit łączny przekroczony, rozdziel odbiorniki między zgodne źródła; jeśli nie, badaj port i tor kabla.

Walidacja i powrót:
Uruchom wszystkie odbiorniki równocześnie; bez poprawy przywróć poprzedni zestaw i zapisz pobór.

Źródła: [6], [4].

Ostoja • Diagnoza 02

Łącze działa z prędkością 100 Mb/s zamiast 1 Gb/s

Objaw: Paweł, 38 lat, administrator biura w Łodzi, mierzy około 90 Mb/s. Inne stanowiska przy tym samym przełączniku są szybsze.

Sprawdź: w UniFi Devices wybierz przełącznik i port stanowiska. Porównaj negocjowaną szybkość z informacją karty sieciowej oraz możliwościami obu końców.

A Test A: podłącz ten sam komputer krótkim, sprawdzonym przewodem do tego samego portu, pomijając gniazdo ścienne i patchpanel.

Oryginalny tor (przez gniazdo i patchpanel)



Tor testowy (pomijając gniazdo i patchpanel)

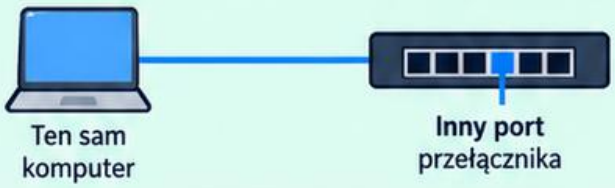


Jeśli pojawia się 1 Gb/s, badaj pominięty tor: patchcordy, gniazdo i zakończenia. Napraw wyłącznie potwierdzony odcinek.

Jeśli nadal jest 100 Mb/s, porównaj inny port i zgodny komputer testowy. Zmieniaj jeden element naraz.

B Test B: jeśli nadal jest 100 Mb/s, porównaj inny port i zgodny komputer testowy. Zmieniaj jeden element naraz.

Sprawdź inny port (ten sam komputer)



Sprawdź inny komputer (ten sam port)



Jeżeli problem podąża za komputerem, sprawdź kartę i jej ustawienia.

Jeśli pozostaje na jednym porcie, zbadaj jego konfigurację i stan.

Walidacja: ponownie sprawdź negocjację i transfer do tego samego celu. Zachowaj automatyczną negocjację; bez poprawy przywróć poprzedni port i ustawienia.

Wynik: port ____; negocjacja przed/po ____; potwierdzony odcinek ____.

Źródła: [4], [49].

Po zmianie sieci zarządzania AP znika, ale Wi-Fi działa

Ostoja • Diagnoza 03

Kontekst: Paweł, 38 lat, administrator biura w Łodzi.

Objaw: Klienci nadal korzystają z AP, lecz nie dociera do niego nowa konfiguracja.



Test rozstrzygający:
Z portu ratunkowego porównaj IP AP, natywny VLAN portu i drogę do hosta Network.

Oddziel przerwę w zarządzaniu od działania klientów.

Zapisz adres AP
przed zmianą i po niej.

Nie przenoś kolejnych urządzeń, dopóki pierwsze nie odbiera konfiguracji.

Działanie:
Jeśli AP ma adres starej sieci, odtwórz ostatni profil portu; przy nowym IP badaj trasę i filtry do hosta.

Walidacja i powrót:
Potwierdź Online oraz zastosowanie bezpiecznej zmiany nazwy; zachowaj stary dostęp do końca próby.

Źródła: [31], [32], [24].

Nowy AP pojawia się tylko przy kontrolerze

Ostoja • Diagnoza 04

Kontekst:
Paweł, 38 lat, administrator biura w Łodzi.

Objaw:
Ten sam egzemplarz jest wykrywany na stole, lecz nie w docelowym oddziale.

Test rozstrzygający:
Sprawdź DHCP w oddziale oraz trasę urządzenie→host, DNS i TCP 8080.

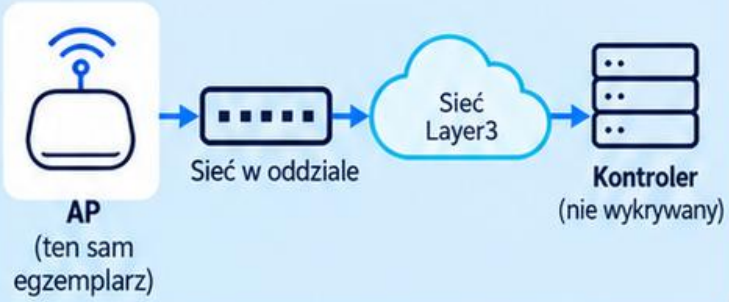
Próba na stole

Próba na stole potwierdza sprawność egzemplarza, ale nie całej drogi w oddziale.



Docelowy oddział

Ten sam egzemplarz nie jest wykrywany w docelowym oddziale.



Sprawdź DHCP w oddziale.

Brak dzierżawy

Działanie:
Brak dzierżawy kieruje do VLAN.

Poprawna dzierżawa

Sprawdź trasę urządzenie→host, DNS i TCP 8080.

Brak TCP 8080

Działanie:
poprawna dzierżawa z brakiem TCP 8080 do trasy lub wąskiego filtra, potem metoda Layer3.

Adres inform musi wskazywać host Network.
Nie zastępuj go adresem dowolnego routera.

Nie otwieraj panelu zarządzania do publicznego internetu dla samego wykrywania.

Walidacja i powrót:
Online utrzymuje się po ponownym uruchomieniu; usuń wyłącznie zbędne reguły tymczasowe.

Źródła: [27], [24], [31].

Urządzenia wracają do starego hosta po migracji

Ostoja • Diagnoza 05

Kontekst: Paweł, 38 lat, administrator biura w Łodzi.

Objaw: Po uruchomieniu nowego hosta część sprzętu ponownie kontaktuje się ze starą instancją.



Test rozstrzygający: Porównaj MAC, adresy hostów i zdarzenia; sprawdź, czy stara instancja nadal zarządza instalacją.

Zachowaj osobne etykiety starego i nowego hosta.

Przed wyłączeniem starego zarządzania potwierdź kopię oraz właściciela.

Samo przemianowanie lokalizacji nie przenosi urządzeń między instancjami.

Zapisz czas ostatniego kontaktu urządzenia z każdą instancją oraz wynik zastosowania testowej zmiany nazwy.

Działanie: Jeśli potwierdzono konkurencję instancji, dokończ udokumentowaną migrację; nie resetuj masowo odbiorników.

Walidacja i powrót: Jedna docelowa instancja przyjmuje zmiany; zachowaj starą kopię do potwierdzenia odbioru.

Źródła: [8], [24], [27].

Chmura działa, lecz lokalne logowanie jest niemożliwe

Ostoja • Diagnoza 06



Kontekst:
Paweł, 38 lat, administrator biura w Łodzi.



Objaw:
Paweł otwiera lokalizację z Site Manager, ale nie po lokalnym adresie.

Niezależne testy dostępu

Dostęp z chmury działa



Otwórz lokalizację z Site Manager.

Lokalne logowanie jest niemożliwe



Nie otwiera się po lokalnym adresie.

Test rozstrzygający

Sprawdź adres IP i osiągalność właściwego hosta, HTTPS 443 lub port własnego Network Server oraz przygotowane dane lokalne.



Sprawdź drugi raz adres hosta, zamiast automatycznie używać bramy domyślnej.



CloudKey i router mogą mieć inne adresy.



MFA konta UI nie zastępuje przygotowania lokalnego dostępu.



Działanie:
Brak drogi napraw w LAN; przy działającym panelu i odmowie konta sprawdź uprawnienia i dostępne metody logowania.



Walidacja i powrót:
Nowa sesja lokalna działa podczas kontrolowanej próby bez WAN; przywróć WAN i nie zamykaj jedynej sprawnej sesji.



Źródła:
[10], [14].

DHCP działa rano, lecz po południu brakuje adresów

Ostoja • Diagnoza 07



Kontekst:
Anna, 34 lata, opiekunka sieci szkoły w Gdańsku.

Objaw:
Nowi goście nie uzyskują adresu przy pełnej sali, a wcześniej podłączeni pracują.



Rano



DHCP
są wolne adresy

Po południu
(przy pełnej sali)



DHCP
brakuje adresów

Test rozstrzygający:
Porównaj wolne dzierżawy, rozmiar puli i rotację MAC; potwierdź brak drugiego serwera.



Zapisz liczbę wolnych adresów przed próbą nowego połączenia.

Sprawdź, czy problem występuje wyłącznie przy szczycie.



Tak
(tylko przy szczycie)



Nie
(również poza szczytem)



Krótsza dzierżawa nie powiększa podsieci i nie jest limitem sesji Wi-Fi.



Działanie:
Przy wyczerpaniu dostosuj pulę lub czas do liczby klientów; jeśli pula wolna, badaj transport i serwer.



Walidacja i powrót:
Nowy i odnawiający klient działają przy obciążeniu; zapisz stary zakres oraz czas do cofnięcia.



Źródła:
[12], [32].

Po podłączeniu obcego routera klienci dostają inną bramę

Ostoja • Diagnoza 08



Kontekst:
Anna, 34 lata, opiekunka sieci szkoły w Gdańsku.

Objaw:
Część stanowisk otrzymuje nieoczekiwany DNS i adres bramy.

Test rozstrzygający:
Porównaj parametry kilku świeżych dzierżaw oraz źródło odpowiedzi DHCP z ewidencją.



Odpowiedź DHCP z zatwierdzonego serwera

Właściwa brama i DNS



Zatwierdzony serwer

Nie przypisuj winy urządzeniu wyłącznie po obcej nazwie.

Odpowiedź DHCP musi wskazywać rzeczywiste źródło.

Odpowiedź DHCP z niezatwierdzonego routera

Inna brama i DNS



Obcy router

1. Przygotowanie

Najpierw potwierdź port i uzgodnij odłączenie z właścicielem sali.

2. Działanie

Jeśli odpowiada niezatwierdzony router, odizoluj jego potwierdzony port; nie wyłączaj uzgodnionego serwera.

3. Walidacja i powrót

Nowe dzierżawy mają jedną właściwą bramę i DNS; udokumentuj odłączony port.

4. Weryfikacja

Potwierdź stabilność połączenia.

Dowód: źródło odpowiedzi DHCP ____; port obcego routera ____; wynik odnowienia po izolacji ____.

Źródła: [12], [4].

Rezerwacja drukarki nie zmienia jej adresu

Ostoja • Diagnoza 09



Kontekst: Anna, 34 lata, opiekunka sieci szkoły w Gdańsku.

Objaw: Nowa rezerwacja istnieje, lecz drukarka nadal używa starego IP.

Test rozstrzygający: Sprawdź rzeczywisty MAC interfejsu oraz czy drukarka korzysta z DHCP czy ręcznego IP.

Nie resetuj drukarki, aby wymusić nowy adres.

Drukarka

Panel urządzenia pokaże sposób przydziału.

Czy drukarka korzysta z DHCP czy ręcznego IP?

Ręczny IP

DHCP

Działanie: Dla ręcznego IP zmień urządzenie zgodnie z planem.

Działanie: Dla **DHCP** popraw MAC i odnów dzierżawę w oknie.

Przy dwóch interfejsach porównaj MAC przewodowy z przewodowym, a nie z wpisem Wi-Fi.

Walidacja i powrót: Po restarcie adres jest zgodny i wydruk działa; zachowaj poprzedni sposób przydziału.

Zapisz: interfejs _____; rzeczywisty MAC _____; ręczny adres czy **DHCP** _____.

Źródła: [12], [26].

Telefon wpada do innego VLAN-u po zmianie prywatnego MAC

Ostoja • Diagnoza 10

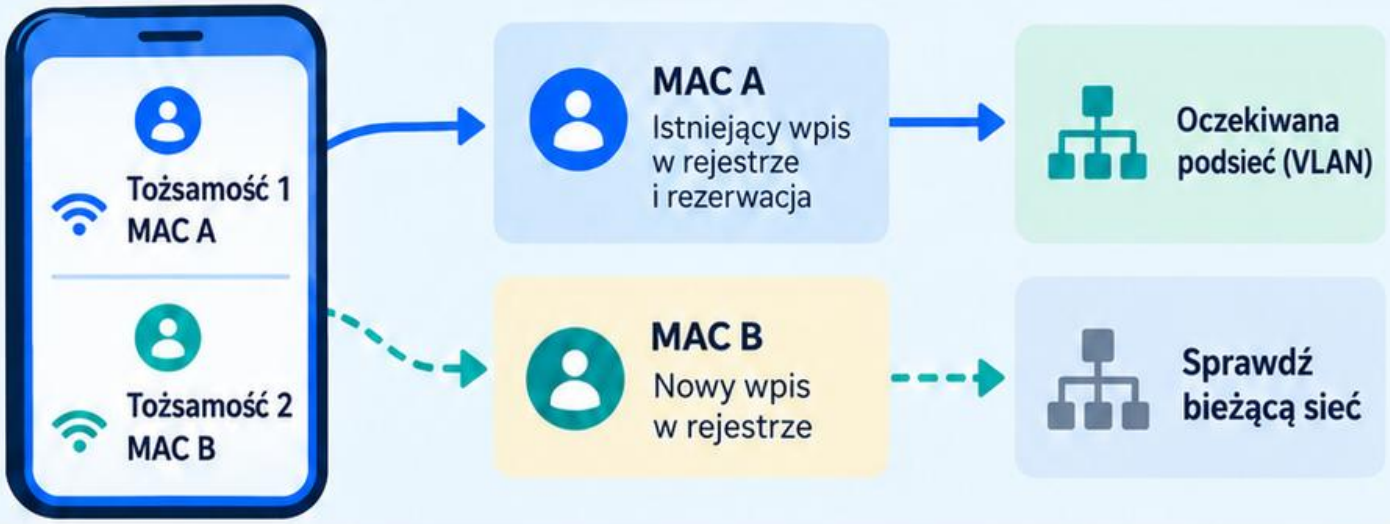


Kontekst:

Anna, 34 lata, opiekunka sieci szkoły w Gdańsku.

Objaw:

Ten sam użytkownik widzi nowe wpisy klienta i nie trafia w oczekiwaną rezerwację.



Nowy MAC może omijać dotychczasową rezerwację lub zatwierdzoną regułę przypisania. Samo pojawienie się nowego wpisu nie dowodzi zmiany VLAN-u.

Test rozstrzygający:

Porównaj MAC dla danego SSID z rejestrem, bieżącą siecią i zasadą przypisania.

Najpierw zapisz rzeczywisty adres i sieć.

Zapisz osobno poprzedni i aktualny MAC oraz sposób przypisania sieci.

Działanie:

Jeśli zmienił się identyfikator, popraw zatwierdzony wpis lub politykę klienta; jeśli nie, badaj przypisanie SSID/portu.

Walidacja i powrót:

Świeże połączenie trafia do właściwej podsieci; nie wyłączaj prywatności wszystkim użytkownikom.

Źródła: [12], [30].

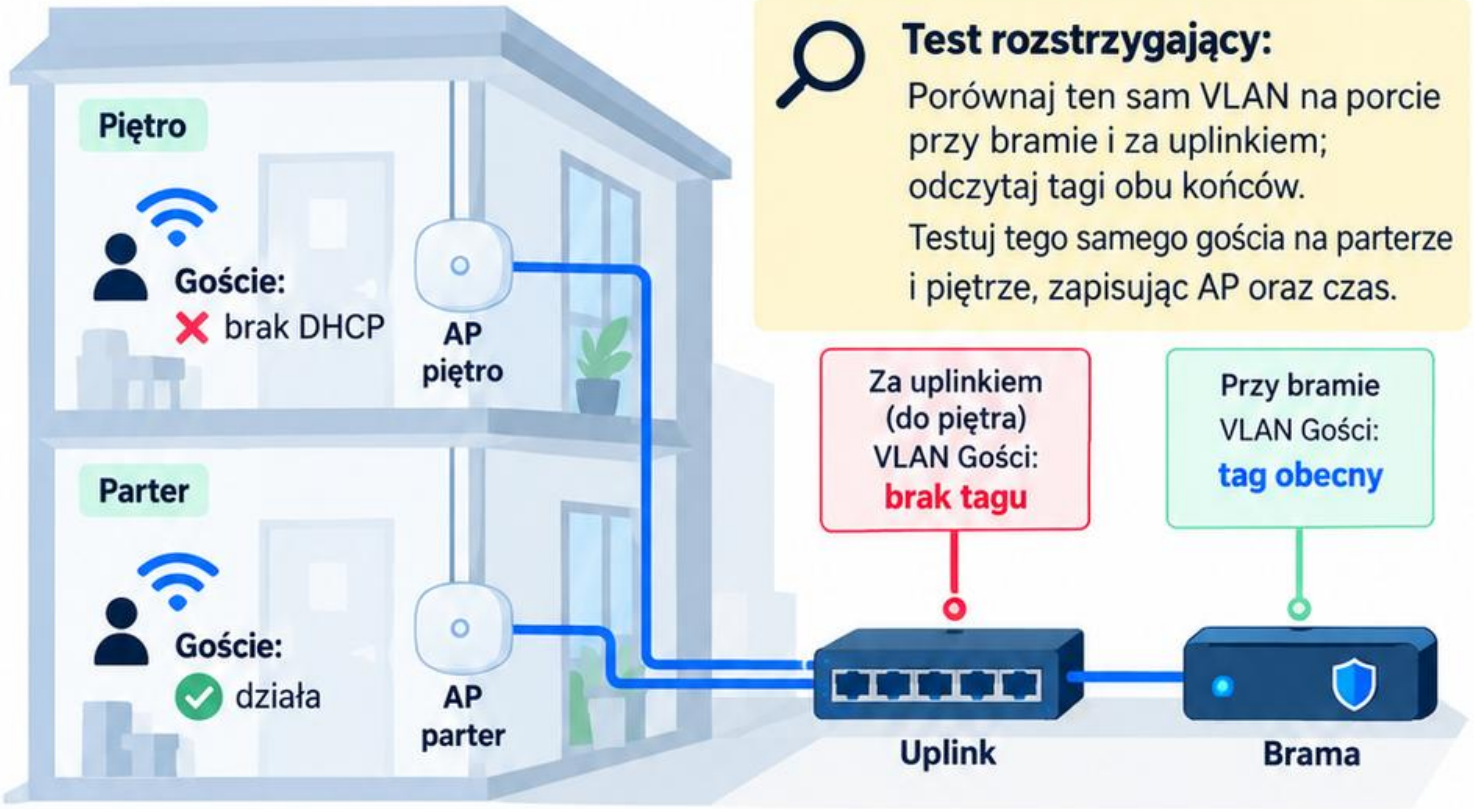
Goście działają na parterze, lecz nie na piętrze

Ostoja • **Diagnoza 11**



Kontekst:
Anna, 34 lata, opiekunka sieci szkoły w Gdańsku.

Objaw:
Firma działa na obu piętrach; tylko nowe połączenia Gości na piętrze nie dostają DHCP.



Test rozstrzygający:
Porównaj ten sam VLAN na porcie przy bramie i za uplinkiem; odczytaj tagi obu końców.
Testuj tego samego gościa na parterze i piętrze, zapisując AP oraz czas.

Działający VLAN Firmy nie dowodzi transportu VLAN-u Gości.

Nie otwieraj zapory przed kontrolą tagów.

Działanie:
Jeśli działa przy bramie, uzupełnij pierwszy brakujący tag na potwierdzonym uplinku; inaczej sprawdź DHCP tej sieci.

Walidacja i powrót:
Nowy gość otrzymuje właściwe IP/DNS, a zarządzanie pozostaje niedostępne; zachowaj profil sprzed zmiany.

Źródła: [32], [4].

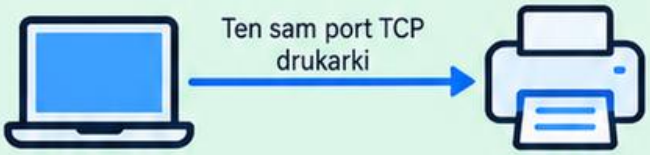
Drukarka działa lokalnie, lecz nie z innej sieci

Ostoja • Diagnoza 12

Kontekst: Anna, 34 lata, opiekunka sieci szkoły w Gdańsku.

Objaw: Drukarka przyjmuje zadanie z klienta w swoim VLAN-ie, lecz ta sama usługa nie odpowiada pracownikowi z innej podsieci.

Ten sam VLAN – drukowanie działa



Inna sieć – brak odpowiedzi



Test rozstrzygający:
Porównaj ten sam port TCP drukarki z zatwierdzonego klienta lokalnego i zdalnego.

Sprawdź maskę, bramę drukarki, drogę powrotną i pasującą politykę.



Działanie:
Jeśli błędna maska lub brama blokuje odpowiedź, popraw tylko potwierdzony parametr.

Przy poprawnej drodze sprawdź wąski wyjątek TCP do tej drukarki i lokalną kontrolę dostępu urządzenia.

Walidacja i powrót:
Wykonaj rzeczywisty wydruk z obu źródeł oraz próbę niezatwierdzonej usługi.
Bez poprawy przywróć ostatni parametr; zachowaj poprzednią konfigurację drukarki.

Nie zmieniaj rezerwacji DHCP, jeżeli drukarka używa ręcznego adresu.
Zapisz bieżący prefiks i bramę z jej panelu.
Testuj rzeczywiste drukowanie, nie tylko odpowiedź ping.

Źródła: [25], [3].

Skaner przestaje łączyć się po zmianie PMF

Ostoja • Diagnoza 13

Kontekst:
Marta, 41 lat, administratorka przychodni w Krakowie.

Objaw:
Nowy laptop działa, ale konkretny starszy skaner odmawia połączenia po zmianie ochrony.

Test rozstrzygający:
Porównaj sterownik i obsługę zabezpieczeń; wykonaj kontrolowany test zgodności na odrębnym SSID.



Widoczna nazwa sieci nie potwierdza obsługi jej zabezpieczeń.

Zapisz model skanera i poprzednią konfigurację.

Próba zgodności obejmuje także właściwy VLAN oraz dostęp do aplikacji.

Test potwierdza niezgodność

Test nie potwierdza niezgodności

Działanie:
Jeśli test potwierdza niezgodność, zastosuj zatwierdzony ograniczony profil dla skanera; inaczej badaj etap uwierzytelniania.

Walidacja i powrót:
Czysty profil łączy oba modele do właściwych sieci; usuń testowe SSID i zachowaj ochronę produkcji.

Dowód zgodności:
model skanera ____; sterownik ____; wynik kontrolowanego połączenia ____.

Źródła: [33], [37].

Czujnik 2,4 GHz nie widzi nowego SSID

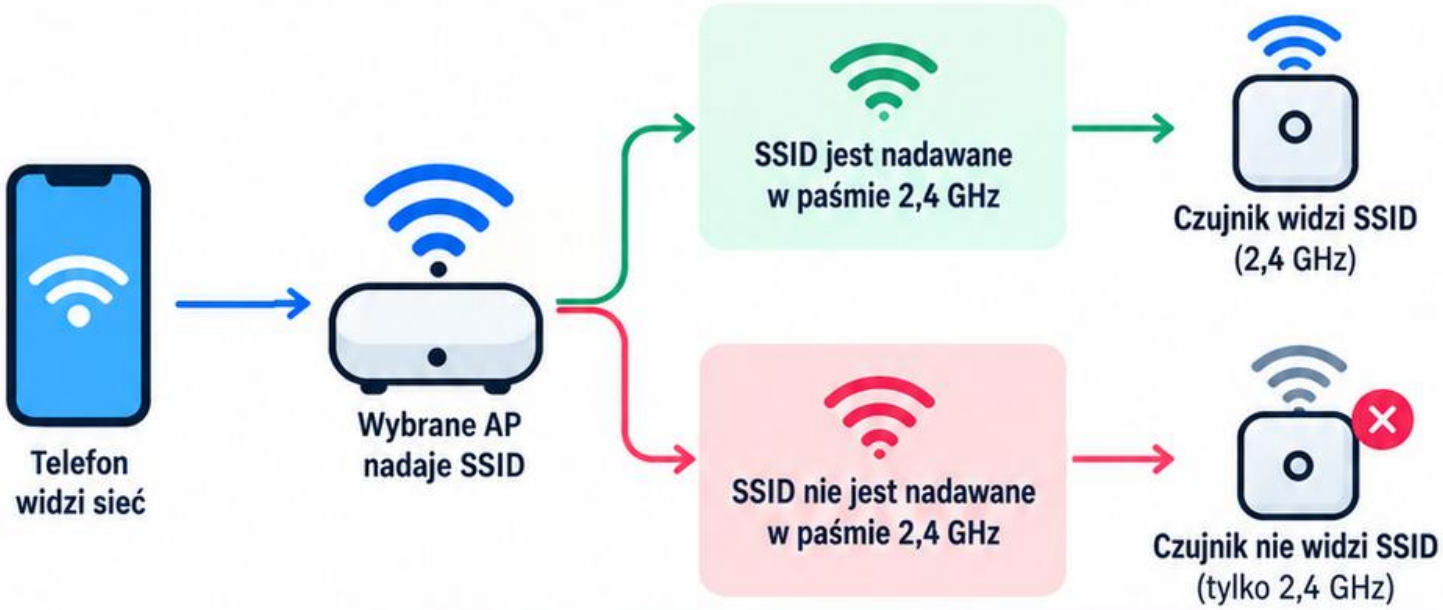
Ostoja • Diagnoza 14



Kontekst: Marta, 41 lat, administratorka przychodni w Krakowie.

Objaw: Telefon widzi sieć, a czujnik obsługujący wyłącznie 2,4 GHz jej nie pokazuje.

Test rozstrzygający: Sprawdź pasma nadawane przez wybrane AP, zabezpieczenia i zgodność czujnika; nie oceniaj tylko telefonu.



Sprawdź dokumentację konkretnego czujnika i faktyczne nadawanie na wybranym AP.

Nie przenoś automatycznie ustawień telefonu.

Pozostaw segmentację IoT i tylko uzasadnione wyjątki do usług.

Działanie: Jeśli brak zgodnego pasma, udostępnij zatwierdzony wariant IoT; przy widocznym SSID przejdź do uwierzytelniania.

Walidacja i powrót: Czujnik ponownie łączy się po restarcie i uruchamia aplikację; cofnij testowe zmiany niepotrzebne do zgodności.

Zapisz pasmo czujnika i listę AP rzeczywiście nadających testową nazwę.

Źródła: [33], [37].

Silny sygnał nie zapobiega opóźnieniom w sali

Ostoja • Diagnoza 15



Kontekst: Marta, 41 lat, administratorka przychodni w Krakowie.



Objaw: W sali konferencyjnej sygnał jest dobry, lecz podczas spotkań rosną opóźnienia.



Test rozstrzygający:
Porównaj zajętość kanału, retransmisje i test przewodowy w tej samej godzinie.

Dobry wskaźnik siły sygnału nie opisuje dostępnego czasu radiowego.

Powtórz pomiar przed spotkaniem i podczas niego.

Porównuj tego samego klienta, miejsce i serwer testowy.

Działanie:
Jeśli WAN i przewód stabilne, zmień jeden potwierdzony parametr radiowy; przy wspólnym spowolnieniu badaj uplink/WAN.

- Jeśli WAN i przewód stabilne, zmień jeden potwierdzony parametr radiowy.
- Przy wspólnym spowolnieniu badaj uplink/WAN.

Walidacja i powrót:
Powtórz tę samą aplikację przy podobnym obciążeniu; bez poprawy odtwórz kanał i szerokość.

Notatka: godzina ____; klient ____; kanał ____; zajętość ____; wynik przewodowy ____.

Źródła: [19], [30].

Rozmowa urywa się tylko przy drzwiach między AP

Ostoja • Diagnoza 16



Kontekst: Marta, 41 lat, administratorka przychodni w Krakowie.

Objaw: Telefon działa w obu pokojach osobno; rozmowa zanika podczas przejścia.

Test rozstrzygający:
Powtórz trasę w obu kierunkach, zapisz AP i czas; porównaj zgodność SSID i transport VLAN po zmianie AP.



Zerwanie rozmowy może dotyczyć klienta, pokrycia albo odmiennej konfiguracji odcinka.

Samo przyłączenie do innego AP nie dowodzi poprawnego roamingu.

Działanie: Przy błędzie konfiguracji odcinka popraw go; przy zgodnej sieci oceń pokrycie i zachowanie konkretnego klienta.

Dołącz czas zerwania rozmowy oraz identyfikatory AP przed przejściem i po nim.

Walidacja i powrót: Ta sama rozmowa przechodzi trasę bez utraty usługi; przywróć nietrafioną zmianę radiową.

Źródła: [19], [30].

Nowe urządzenie 6 GHz działa, starsze nie widzi sieci

Ostoja • Diagnoza 17



Kontekst:
Marta, 41 lat, administratorka przychodni w Krakowie.

Objaw:
Dwa laptopy w tym samym miejscu mają różne możliwości wykrywania.



Nowe urządzenie 6 GHz działa



Starsze nie widzi sieci

Test rozstrzygający:
Sprawdź obsługę 6 GHz, sterownik, zabezpieczenia i kraj rzeczywistej instalacji.

- Obsługa 6 GHz
- Sterownik
- Zabezpieczenia
- Kraj rzeczywistej instalacji

Czy urządzenie obsługuje 6 GHz?

Nie

Nie wybieraj innego kraju, aby odsłonić pasmo lub kanały. W Polsce sprawdź regionalne warunki i przeznaczenie modelu.

Tak

Test zgodności obejmuje również metodę uwierzytelniania klienta.

Działanie:
Przy braku obsługi pozostaw zatwierdzone zgodne pasmo; przy zgodnym sprzęcie badaj konfigurację bez zmiany kraju.

Walidacja i powrót:
Oba modele korzystają z przeznaczonych dla nich pasm; zapisz warianty i cofnij testowe profile.

Zapisz model każdego laptopa, sterownik oraz pasmo użyte podczas udanego połączenia.

Źródła: [21], [35].

Połączenie wraca dopiero po usunięciu profilu Wi-Fi

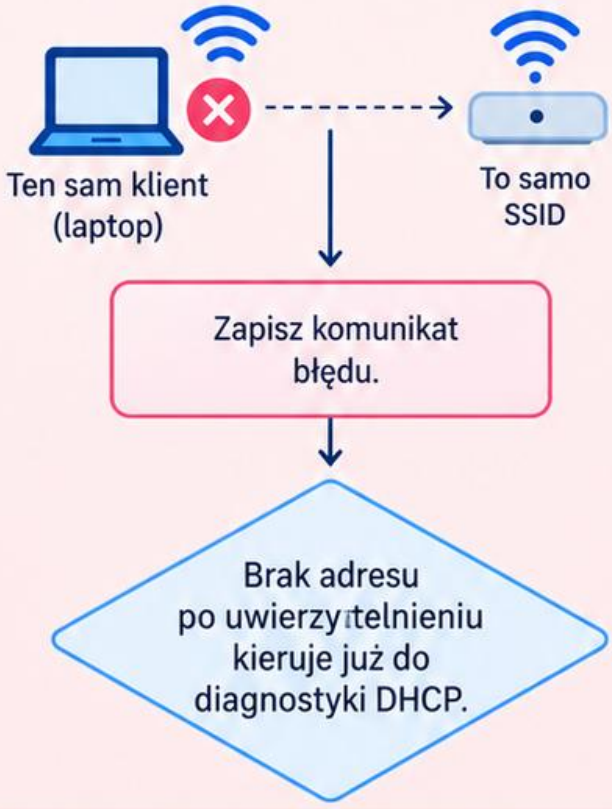
Ostoja • Diagnoza 18

Kontekst: Marta, 41 lat, administratorka przychodni w Krakowie.

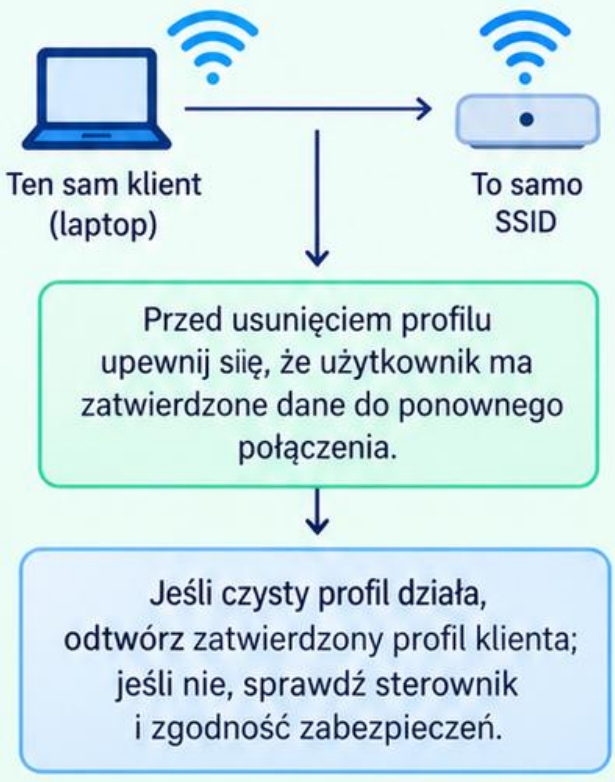
Objaw: Jeden laptop odmawia połączenia po zmianie hasła, inne działają.

Test rozstrzygający: Potwierdź etap awarii i bieżące dane; porównaj czysty profil tego samego klienta.

Profil z pamięci (problem)



Czysty profil (test)



Działanie: Jeśli czysty profil działa, odtwórz zatwierdzony profil klienta; jeśli nie, sprawdź sterownik i zgodność zabezpieczeń.

Walidacja i powrót: Ponowne połączenie po restarcie daje właściwy IP i aplikację; nie obniżaj zabezpieczeń całego SSID.

Dowód: komunikat przed odtworzeniem profilu ____; etap połączenia po poprawce _____.

Źródła: [37], [30].

Ostoja • Diagnoza 19

Drukowanie po IP działa, wykrywanie drukarki nie



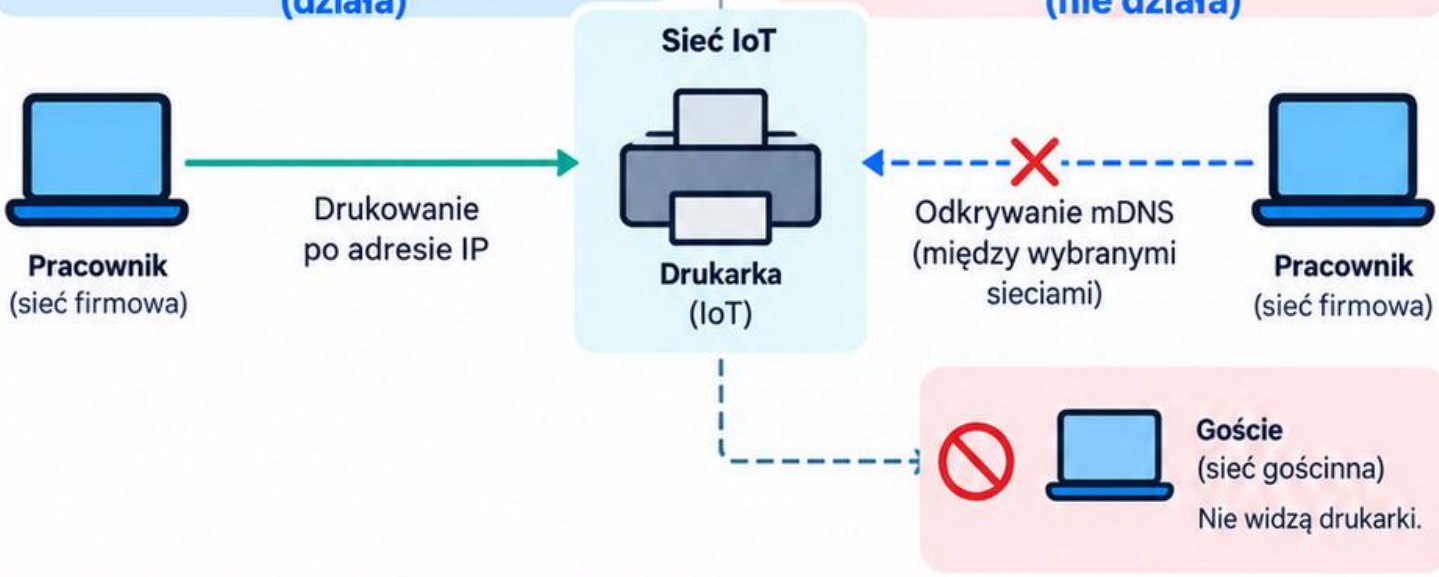
Kontekst: Tomasz, 45 lat, informatyk hotelu w Poznaniu.

Objaw: Pracownik drukuje bezpośrednio do urządzenia w IoT, ale nie znajduje go na liście.

Test rozstrzygający: Potwierdź działający port usługi; osobno sprawdź wymagane odkrywanie mDNS między wybranymi sieciami.

Drukowanie po IP (działa)

Odkrywanie drukarki (nie działa)



Odkrywanie i sesja drukowania są niezależnymi przepływami.

Nie otwieraj wszystkich usług między segmentami dla wygody listy drukarek.

Zachowaj bezpośredni adres jako kontrolowaną próbę porównawczą.

Działanie: Jeśli aplikacja wymaga odkrywania, ogranicz proxy do potrzebnych VLAN/usług; inaczej użyj udokumentowanego adresu.

Walidacja i powrót: Wydruk i odkrywanie działają, Goście nie widzą drukarki; przy nadmiarowym ujawnieniu cofnij mDNS.

Zapisz oddzielnie wynik wydruku po adresie i wynik wyszukiwania tej samej drukarki.

Źródła: [29], [3].

Wyjątek drukowania przestaje działać po nowej blokadzie

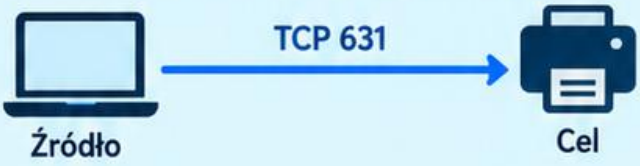
Ostoja • Diagnoza 20

Kontekst:
Tomasz, 45 lat,
informatyk hotelu w Poznaniu.

Objaw:
Wydruk działał przed dodaniem Block dla tej samej relacji stref.

Test rozstrzygający:
Zapisz źródło/cel/TCP 631 i porównaj kolejność pasujących polityk oraz nową sesję.

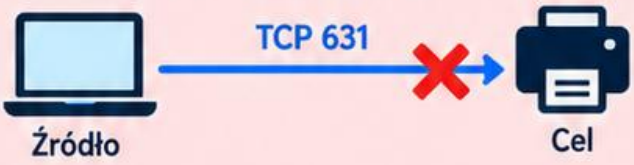
Przed nową blokadą



Kolejność pasujących polityk

Allow (wyjątek)
dla tej samej relacji stref →

Po dodaniu nowej blokady



Kolejność pasujących polityk

Block (ogólna blokada)
dla tej samej relacji stref →

Allow (wyjątek)
dla tej samej relacji stref →

- Nazwa polityki nie określa pierwszeństwa.
- Porównuj reguły pasujące do tego samego źródła, celu i usługi.

Zamknij poprzednie zadanie drukowania, aby sprawdzić nową sesję. →

Czy ogólna blokada poprzedza wyjątek?

Tak →

Działanie:
Jeśli ogólna blokada poprzedza wyjątek, przywróć wąski Allow przed nią.

Nie ↓

Działanie:
Inaczej badaj adres i usługę drukarki.

Walidacja i powrót:
Nowy wydruk działa, niezatwierdzony port pozostaje blokowany; zachowaj poprzednią kolejność.

Notatka: wyjątek _____; pozycja blokady _____; źródło testu _____; nowa sesja _____; wydruk _____.

Źródła: [3].

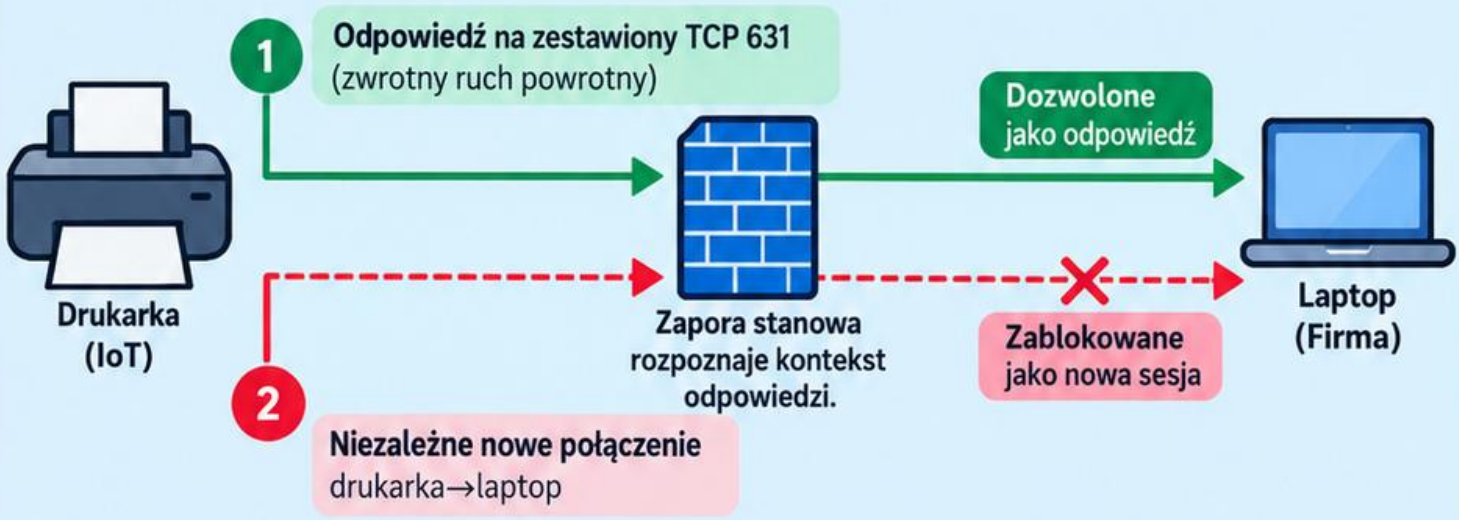
Ostoja • Diagnoza 21

Drukarka odpowiada, lecz nie może rozpocząć sesji do laptopa

Kontekst: Tomasz, 45 lat, informatyk hotelu w Poznaniu.

Objaw: Wydruk działa pomimo blokady nowych IoT→Firma; administrator podejrzewa błąd zapory.

Test rozstrzygający:
Oddziel odpowiedź na zestawiony TCP 631 od niezależnego nowego połączenia drukarka→laptop.



Nie testuj blokady nowej sesji pakietem należącym do starego połączenia.
Oddziel dwie próby i zapisz oczekiwany wynik każdej.

Działanie: Jeśli działa wyłącznie oczekiwana odpowiedź, nie dodawaj szerokiego Allow zwrotnego; sprawdź automatyczny ruch powrotny.

Walidacja i powrót: Wydruk działa, świeża niezamówiona sesja nie; cofnij zbędny szeroki wyjątek po potwierdzeniu.

Zapisz osobne wyniki:
odpowiedź na wydruk _____;
nowa sesja drukarka–laptop ____.
Nie myl tych dwóch prób.

Źródła: [3].

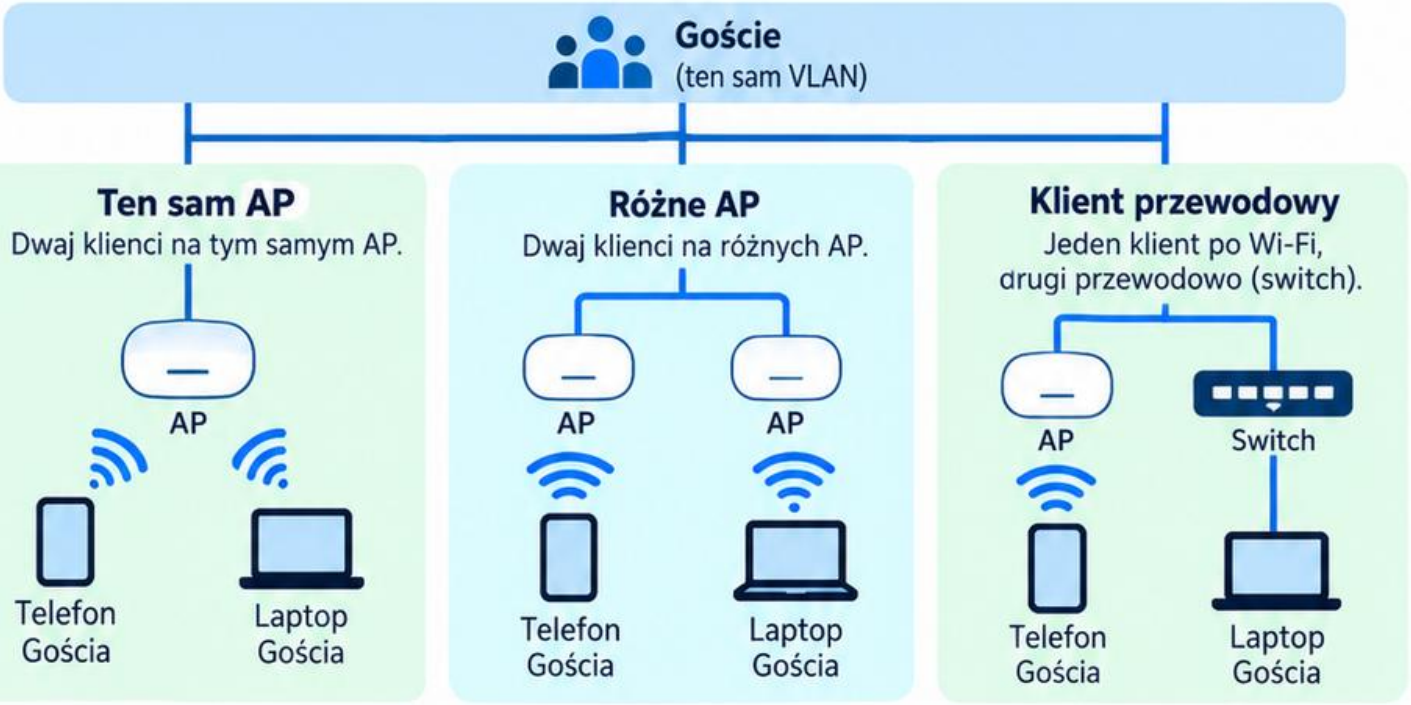
Dwaj goście widzą się mimo blokady Goście→Firma

Ostoja • Diagnoza 22

Kontekst:
Tomasz, 45 lat, informatyk hotelu w Poznaniu.

Objaw:
Telefon i laptop Gościa w tym samym VLAN-ie wymieniają dane, chociaż Firma jest odcięta.

Test rozstrzygający:
Porównaj parę na tym samym AP, na różnych AP i drogę przewodową; sprawdź dostępne mechanizmy L2.



Ruch dwóch klientów w jednym segmencie może nie przechodzić przez bramę.

Dlatego reguła między strefami nie zastępuje izolacji klientów ani zgodnych ograniczeń przełącznika.

Działanie: Jeśli wymagana izolacja nie obejmuje danej drogi, zastosuj zgodny mechanizm klienta/switcha; nie szukaj wyłącznie reguły routowanej.

Walidacja i powrót: Wszystkie wymagane pary izolowane, DHCP/DNS/internet działają; zachowaj poprzednią konfigurację izolacji.

Wyniki par:
ten sam AP ____; różne AP ____; klient przewodowy ____.

Źródła: [20], [4].

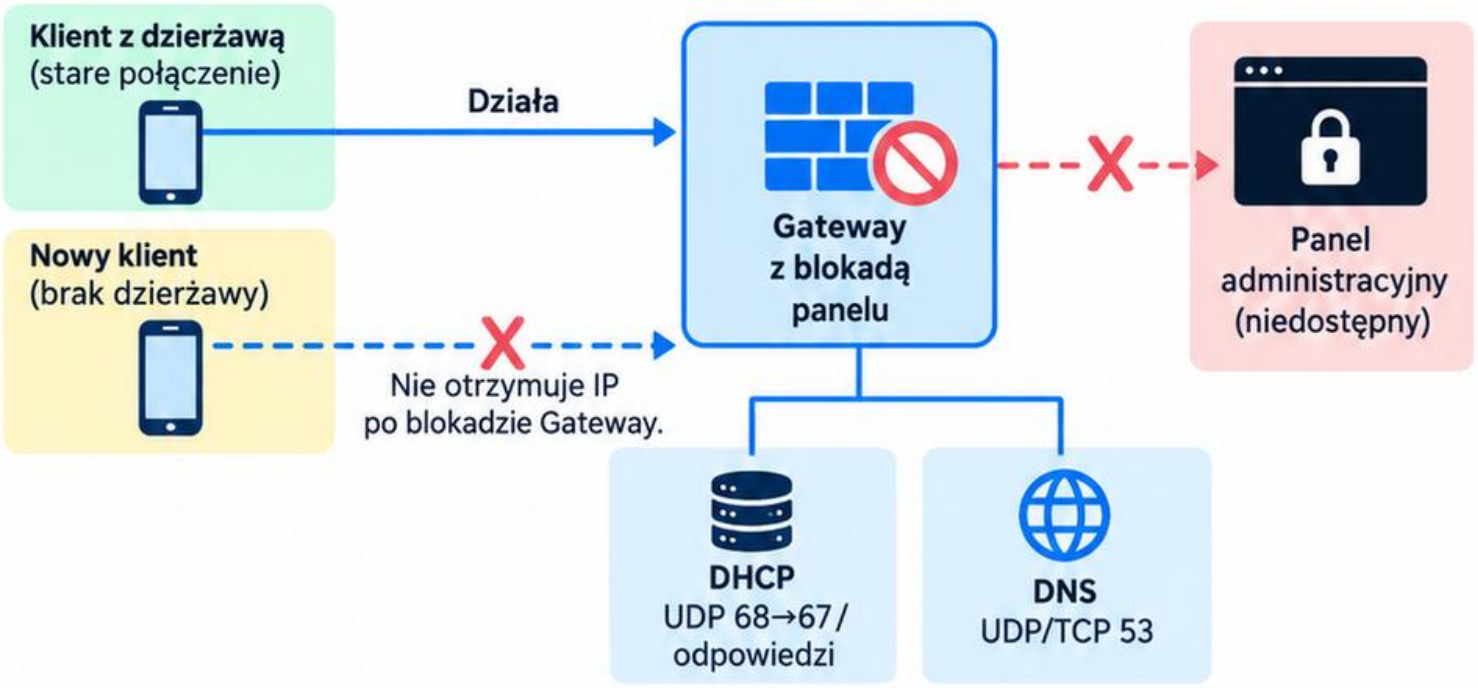
Po ochronie panelu Goście tracą nowe dzierżawy

Ostoja • Diagnoza 23



Kontekst: Tomasz, 45 lat, informatyk hotelu w Poznaniu.

Objaw: Stare połączenia działają, ale nowe telefony nie otrzymują IP po blokadzie Gateway.



Test rozstrzygający: Porównaj klienta z dzierżawą i bez niej; sprawdź lokalny DHCP UDP 68→67/odpowiedzi oraz DNS UDP/TCP 53.

Adres klienta podczas pierwszego pozyskania dzierżawy może jeszcze nie należeć do planowanej puli.

Wąski wyjątek oparty wyłącznie na aktualnych adresach nie dowodzi obsługi rozgłoszenia.

Działanie: Jeśli ostatnia blokada obejmuje niezbędne usługi, cofnij ją i odtwórz wąskie wyjątki, uwzględniając fazę rozgłoszenia.

Walidacja i powrót: Nowy klient i klient odnawiający dzierżawę działają, panel nadal niedostępny; zachowaj lokalną sesję administratora.

Zapisz czas nowej dzierżawy, otrzymaną bramę oraz wynik kontrolnego zapytania DNS.

Źródła: [3], [12].

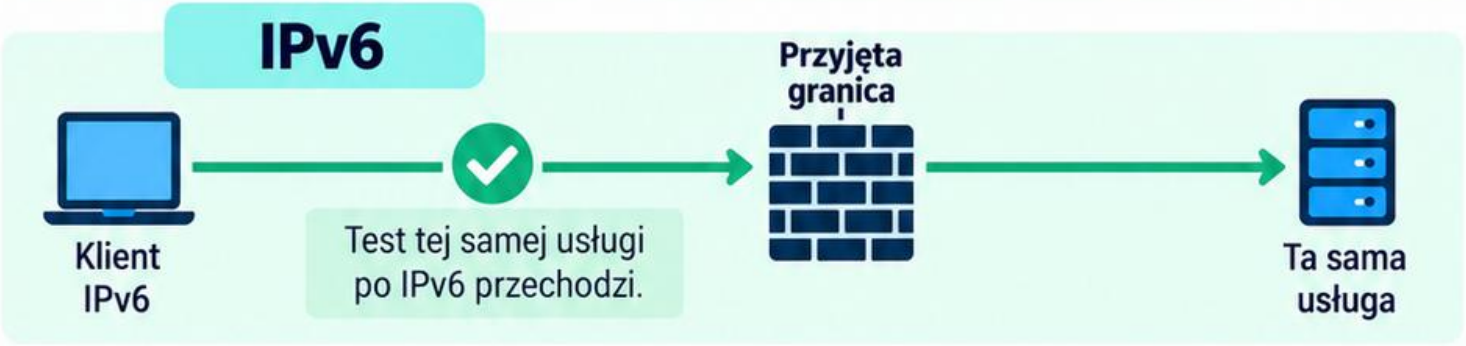
IPv4 jest odizolowane, lecz IPv6 omija przyjętą granicę

Kontekst:
Tomasz, 45 lat, informatyk hotelu w Poznaniu.

Objaw:
Próba po IPv4 jest blokowana, a test tej samej usługi po IPv6 przechodzi.

Test rozstrzygający:
Sprawdź adres globalny, trasę i polityki obu rodzin; odróżnij link-local od ruchu między VLAN-ami.





Nie uznawaj samego adresu fe80:: za dowód dostępu między segmentami.

Sprawdź konkretny cel i usługę.

Wspólny wynik ping nie zastępuje testu aplikacji dla obu rodzin.

Działanie:
Przy brakującej polityce IPv6 uzupełnij równoważne ograniczenie, zachowując potrzebne ICMPv6; nie blokuj całego ICMPv6.

Walidacja i powrót:
Dozwolone i zakazane próby zgodne dla obu rodzin;
cofnij ostatnią zmianę przy utracie podstawowej łączności.

Notatka:
cel _____; port _____; wynik IPv4 _____; wynik IPv6 _____.

Źródła: [13], [3].

PPPoE działa na starej bramie, ale nie na nowej



Kontekst:

Ewa, 39 lat, administratorka dwóch biur we Wrocławiu.

Objaw:

Przewód ma link; nowa brama nie zestawia sesji podczas wymiany sprzętu.

Stara brama
PPPoE działa



Nowa brama
Nie zestawia sesji

Test rozstrzygający:

Rozróżnij odmowę uwierzytelniania i brak odpowiedzi; potwierdź dane usługi, VLAN i jednoczesną sesję starego routera.

Odmowa uwierzytelniania

Działanie:
Przy odmowie potwierdź dane z operatorem.

Brak odpowiedzi

Działanie:
Przy braku odpowiedzi sprawdź przekazanie VLAN i limit aktywnych sesji.

Hasło panelu klienta operatora może różnić się od hasła PPPoE.

Porównuj sekrety w zatwierdzonym magazynie.
Nie zapisuj ich w karcie diagnozy ani na zrzucie ekranu.

Walidacja i powrót:

Nowa sesja i HTTPS klienta działają; w razie niepowodzenia wróć do zapisanej konfiguracji starej bramy.

Źródła: [16], [9].

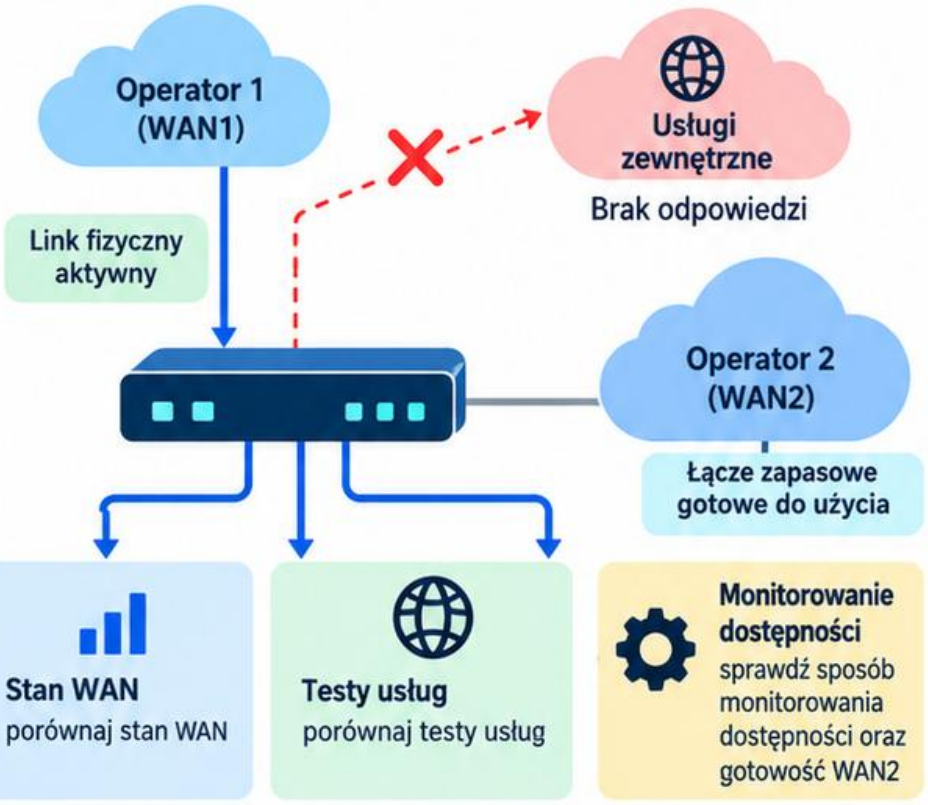
Ethernet WAN działa, lecz failover nie reaguje na awarię operatora

Ostoja • Diagnoza 26



Kontekst: Ewa, 39 lat, administratorka dwóch biur we Wrocławiu.

Objaw: Link fizyczny pozostaje aktywny, a usługi zewnętrzne przestają odpowiadać.



Monitor dostępności i fizyczny link opisują różne warstwy.

Sprawdź osobno limit danych oraz konfigurację zapasowego operatora.

Awaria nie musi zachować wszystkich wcześniej zestawionych sesji.

Test rozstrzygający:
Porównaj stan WAN, testy usług i sposób monitorowania dostępności oraz gotowość WAN2.

Działanie:
Jeśli monitor nie odzwierciedla awarii, dostosuj obsługiwane cele/progi po potwierdzeniu; jeśli WAN2 nie działa, napraw go osobno.

Walidacja i powrót:
Kontrolowany zanik usługi przełącza nowe sesje; przywróć WAN1 i wcześniejsze ustawienia nietrafionego testu.

Zapisz moment utraty usługi, wykrycia awarii oraz pierwszej udanej nowej sesji.

Źródła: [16].

WireGuard działa z biura, lecz nie przez sieć komórkową

Ostoja • Diagnoza 27



Kontekst:
Ewa, 39 lat, administratorka dwóch biur we Wrocławiu.

Objaw:
Lokalna próba wygląda poprawnie, ale zewnętrzny laptop nie ma aktualnego handshake.

WAN serwera

Adres publiczny

Router nadrzędny / CGNAT

UDP 51820

Test z sieci komórkowej

Test rozstrzygający:
Porównaj WAN z adresem publicznym; ustal router nadrzędny, CGNAT i drogę UDP 51820.

Próba we własnym Wi-Fi nie potwierdza publicznej osiągalności.

Zapisz czas testu zewnętrznego i endpoint klienta.

DDNS nie usuwa translacji operatora ani brakującego przekierowania.

Działanie:
Przy własnym NAT popraw tylko zatwierdzone przekierowanie; przy CGNAT uzgodnij osiągalność z operatorem lub zgodną alternatywę.

Walidacja i powrót:
Świeży handshake spoza LAN i osobny test aplikacji; usuń zbędne tymczasowe reguły, panel WAN zamknięty.

Dowód:
publiczny endpoint _____;
port UDP _____;
czas świeżego handshake ____.

Źródła: [22], [40].

Tunel działa, ale domowa podsieć pokrywa się z biurem

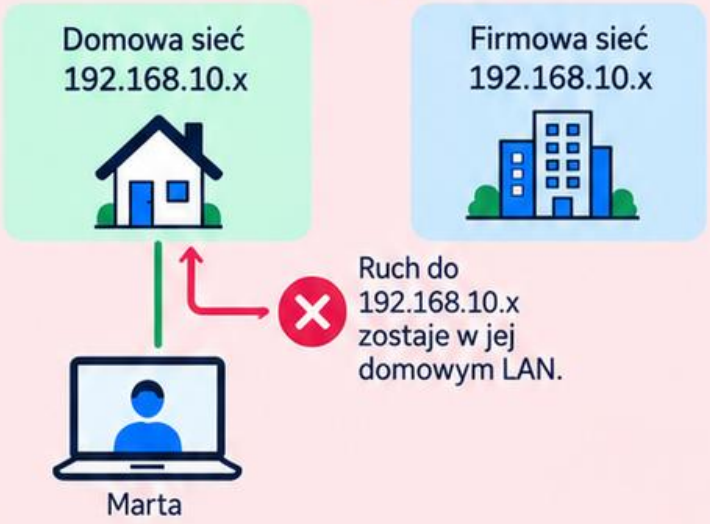
Ostoja • Diagnoza 28



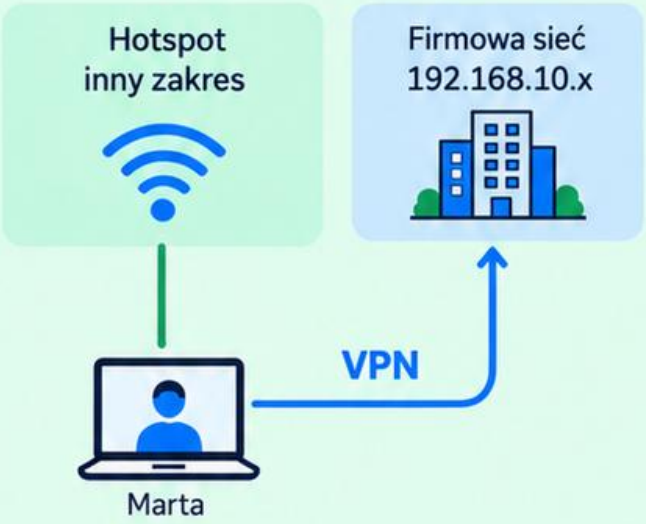
Kontekst: Ewa, 39 lat, administratorka dwóch biur we Wrocławiu.

Objaw: Marta ma handshake; ruch do firmowego 192.168.10.x zostaje w jej domowym LAN.

Pokrywające się podsieci – ruch zostaje w domu



Inny zakres w hotspocie – ruch trafia do biura



Test rozstrzygający: Sprawdź faktyczną trasę klienta i prefiksy obu lokalizacji; porównaj próbę przez hotspot o innym zakresie.

Działający handshake potwierdza połączenie tunelu, lecz nie wybór drogi do serwera. Porównaj wynik tablicy tras przed zmianą i przez hotspot.

Nie rozszerzaj uprawnień innych klientów.

Działanie: Jeśli test potwierdza kolizję, przeprojektuj rozłączne adresy w uzgodnionym oknie; nie maskuj problemu szerokim firewallem.

Walidacja i powrót: Ta sama usługa działa przez tunel z zatwierdzonych lokalizacji; zachowaj poprzedni profil i plan adresacji do cofnięcia.

Źródła: [22], [25].

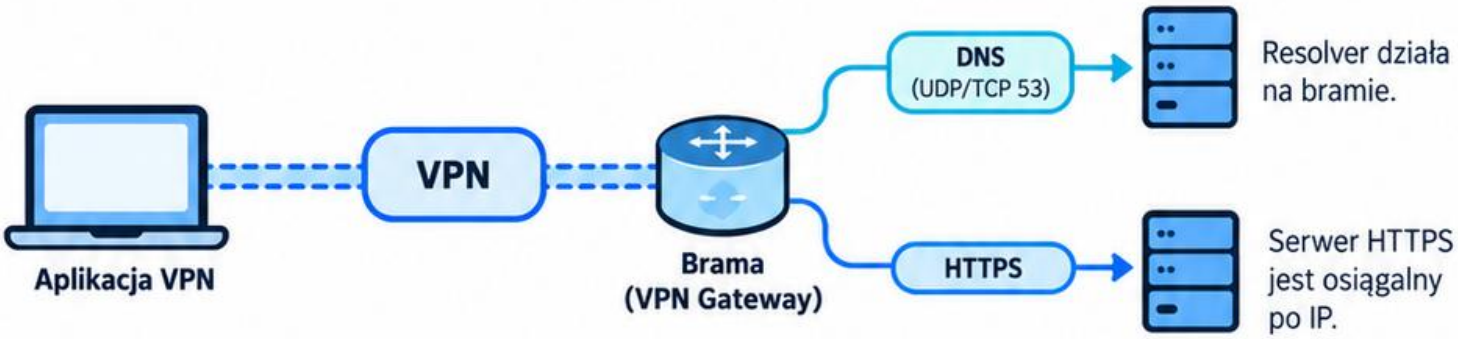
Ostoja • Diagnoza 29

Aplikacja VPN działa po IP, lecz nie po nazwie



Kontekst:
Ewa, 39 lat, administratorka dwóch biur we Wrocławiu.

Objaw:
HTTPS serwera jest osiągalny, a firmowa nazwa nie rozwiązuje się przez tunel. Resolver działa na bramie.



Test rozstrzygający:
Sprawdź resolver profilu, drogę do niego i VPN→Gateway **UDP/TCP 53**; osobno potwierdź rekord wewnętrzny.

Nazwa nie rozwiązuje się przez tunel.

Publiczny resolver nie musi znać prywatnej nazwy firmy.

Zapisz dokładną nazwę i odpowiedź właściwego serwera.

Po IP serwer HTTPS jest osiągalny.

Dostęp DNS i HTTPS wymagają osobnych, wąskich reguł.

Działanie:
Przy brakującej trasie lub wyjątku DNS dodaj tylko potrzebny zakres; przy złym rekordzie popraw go u właściwego administratora.

Walidacja i powrót:
Nazwa i aplikacja działają, inne zasoby pozostają niedostępne; cofnij tymczasowy resolver.

Zapisz resolver, pytaną nazwę i zwrócony adres; pomiń sekrety profilu.

Źródła: [22], [3].

Po zerwaniu tunelu poufny ruch wybiera inną drogę

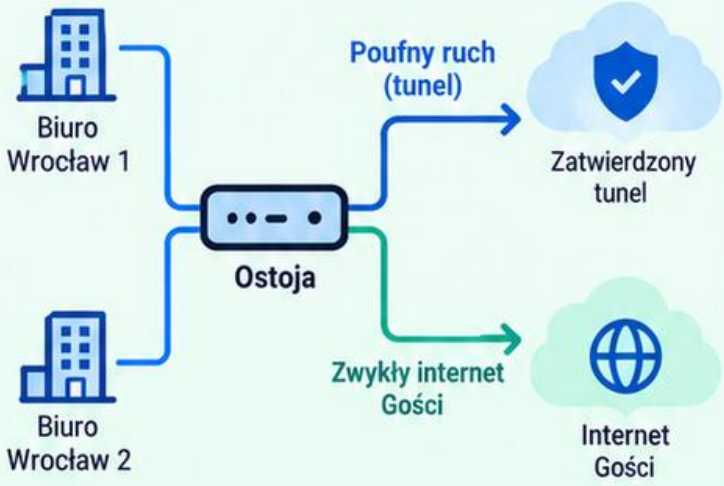
Ostoja • Diagnoza 30



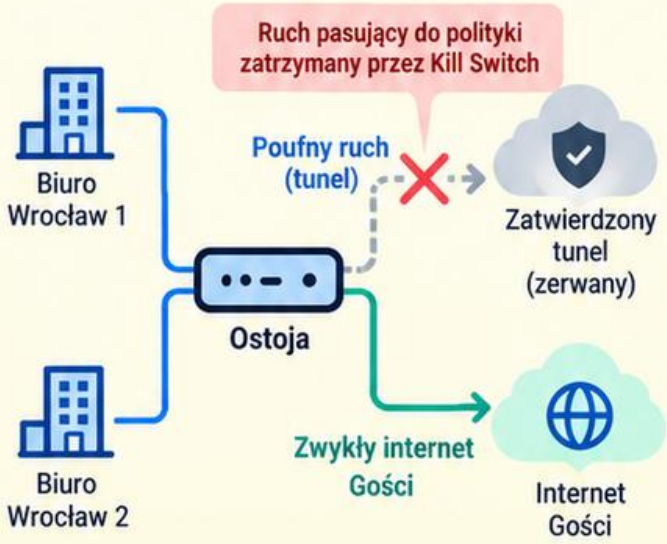
Kontekst: Ewa, 39 lat, administratorka dwóch biur we Wrocławiu.

Objaw: Podczas kontrolowanej awarii zatwierdzonego tunelu zachowanie różni się od polityki firmy.

Tunel działa – normalny ruch



Tunel zerwany – rozdzielne zachowanie



Test rozstrzygający: Porównaj trasę docelową, PBR, wybrany interfejs i Kill Switch; osobno sprawdź zwykły internet Gości.

Kill Switch dotyczy ruchu pasującego do wskazanej polityki, nie każdej sesji w sieci.

Zapisz źródło i cel próby.

Nie utożsamiaj awarii tunelu z awarią całego WAN.

Działanie: Jeśli pasujący PBR ma zatrzymywać ruch, ustaw zatwierdzone zachowanie; dla zwykłych tras usuń niepożądaną drogę po analizie.

Walidacja i powrót: Test awarii zatrzymuje wrażliwą usługę bez wycieku, Goście zachowują uzgodniony fallback; przywróć tunel i poprzednią regułę przy błędzie.

Źródła: [42], [16].

Źródła

Ostoja • Źródła

Dokumentacja Ubiquiti. Numery odpowiadają odwołaniom w diagnozach. Stan sprawdzenia: 21.10.2026.

Zapora i sieć

[3] Zapora strefowa
https://help.ui.com/hc/en-us/articles/115003173168

Przełączniki i PoE

[4] Ustawienia przełączników
https://help.ui.com/hc/en-us/articles/33402927617047

[6] Tryby i dostępność PoE
https://help.ui.com/hc/en-us/articles/115000263008

Kopie zapasowe i migracja

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

Pierwsze uruchomienie i zarządzanie

[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

Usługi sieciowe

[12] Serwer DHCP
https://help.ui.com/hc/en-us/articles/360012097513

[13] Konfiguracja IPv6
https://help.ui.com/hc/en-us/articles/115005868927

Administracja i bezpieczeństwo

[14] Dodawanie administratorów
https://help.ui.com/hc/en-us/articles/28692158912279

[15] Uwierzytelnianie wieloskładnikowe
https://help.ui.com/hc/en-us/articles/115012986607

Połączenie z internetem

[16] Failover i porty WAN
https://help.ui.com/hc/en-us/articles/360052548713

[17] Dynamiczny DNS
https://help.ui.com/hc/en-us/articles/9203184738583

Wi-Fi i klienci

[19] Stabilność i opóźnienia Wi-Fi
https://help.ui.com/hc/en-us/articles/221029967

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

[21] Regiony obsługujące 6 GHz
https://help.ui.com/hc/en-us/articles/8691786444567

Źródła — ciąg dalszy

Dokumentacja Ubiquiti. Numery odpowiadają odwołaniom w diagnozach.
Stan sprawdzenia: 21.10.2026.

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

[24] Adopcja urządzeń
https://help.ui.com/hc/en-us/articles/360012622613

[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

[29] Proxy mDNS
https://help.ui.com/hc/en-us/articles/12648701398807

[30] Diagnostyka Wi-Fi
https://help.ui.com/hc/en-us/articles/32064585817495

[31] Łączność urządzeń UniFi
https://help.ui.com/hc/en-us/articles/7258465146519

[32] Diagnostyka VLAN
https://help.ui.com/hc/en-us/articles/9592924981911

[33] Ustawienia SSID i AP
https://help.ui.com/hc/en-us/articles/32065480092951

[35] Uruchamianie 6 GHz
https://help.ui.com/hc/en-us/articles/20407971377815

[37] Problemy z łączeniem Wi-Fi
https://help.ui.com/hc/en-us/articles/23283660456599

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

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

[46] Korzystanie z WiFiman
https://help.ui.com/hc/en-us/articles/205204150

[49] Optymalizacja szybkości sieci przewodowej
https://help.ui.com/hc/en-us/articles/6949005136919