Router Asus RT-N18U

Położenie: (nie dotyczy)

Opcje

Jumbo Frames – w tym trybie, ilość bajtów w ramkach ethernetowych (MTU) zostaje zwiększona ze standardowych 1500 do 9000. Oszczędza to zasoby procesora i zwiększa wydajność przesyłu danych o jakieś 4%. Nie jest jednak zgodne ze standardem. Ewentualne wady: może być mniejsza płynność w przypadku multimediów (strumieniowe odtwarzanie muzyki / video), ale to tylko w przypadku słabszej przepustowości łącza.
Aby włączyć obsługę tej technologii na komputerze klienta z *Windows*, należy ustawić odpowiednią opcję we właściwościach karty sieciowej (nie każda karta to obsługuje): *Właściwości / Zaawansowane / Jumbo Frames: 9014 Bytes.*
W systemie *Linux*, ustawiamy po prostu opcję MTU w */etc/conf.d/net*.

Protected Management Frames – opcja w sekcji *Wireless / Ogólne*, inaczej standard IEEE 802.11w mający na celu zwiększenie bezpieczeństwa przesyłanych pakietów poprzez autentykację i integrację danych. Jeśli wystąpią problemy przy połączeniach 5GHz, należy tę opcję wyłączyć.

WDS (*Wireless Distribution System*) – router może pracować jako bezprzewodowy klient AP (funkcja: *Wireless / WDS*). W tym przypadku router i AP muszą emitować sygnał na tym samym kanale. Należy także podać MAC zdalnego AP oraz ten sam SSID i przepustowość.

WMM Capable – przyspiesza transmisję danych multimedialnych (zalecane).

APSD Capable – funkcja automatycznego oszczędzania energii.

UPnP – protokół będący podstawą tzw. „*Internet of Things*" (urządzenia spełniające standard DLNA). Z informacji opublikowanych przez *WikiLeaks* w 2017 roku, wynika, że CIA miała (i ma) możliwość podsłuchiwania ruchu na routerach z włączoną funkcją *UPnP*. Aby sprawdzić, czy nasz router (system) jest zhakowany przez CIA: *http://numerIP_routera/CherryWeb* (powinien pojawić się panel administracyjny zdalnego dostępu hakera) lub przeszukać system pod kątem występowania skryptu **cherrytree**.

SPI Firewall (*Stateful Packet Inspection*) - mechanizm śledzenia stanów połączeń. W niektórych przypadkach może powodować problemy z dostępem do drukarki (*ping*).

TKIP (*Temporal Key Integrity Protocol*) – kontrola integralności wiadomości i mechanizm ponownej negocjacji klucza (*rekeying*). Standard IEEE 802.11n nie obsługuje TKIP.

AES (*Advanced Encryption Standard*) – szyfrowanie kluczem symetrycznym, konieczne gdy korzystamy ze standardu IEEE 802.11n.

MAC – w routerach Asus, MAC LAN i WAN jest domyślnie taki sam. Można zmienić te ustawienia w sekcji WAN.

Przekierowanie portów - w regułkach „*Port Forwarding*" numery portów nie mogą się powtarzać, a docelowy komputer musi mieć stałe IP. Jeśli regułki z jakiś powodów nie działają, warto całość sprawdzić przy wyłączonym firewallu. Przykłady reguł:

Nazwa usługi	***Source Target (Adres źródłowy)***	***Zakres portów (lub port)***	***Lokalny IP***	***Port lokalny***	***Protokół***
Drukarka	(opcjonalnie, tylko jeśli chcemy określić IP zdalnego nadawcy – połączenie będzie możliwe tylko z tego adresu)	631	192.168.17.10	631	BOTH
Apache		80	192.168.17.100	80	TCP

Nazwa usługi	*Source Target (Adres źródłowy)*	*Zakres portów (lub port)*	*Lokalny IP*	*Port lokalny*	*Protokół*
Jakaś usługa	82.12.34.56	1000:1500	192.168.17.20	(puste, gdy wcześniej określono zakres portów)	BOTH

Informacje:
- Przekierowanie portów może przebiegać przez kilka routerów (kaskadowo).
- Do działania protokołu *IPsec* oraz *VoIP* nie może być podwójnego NATa (dwa routery).

Blokowanie portów

Counter Strike
TCP: 27014-27050.
UDP: 1200,3487,4379-4380,6003,7002,27000-27030.

Problemy

Problem z cache
Podczas próby logowania zdalnego w trybie https, pojawia się czasami komunikat: „*Ustawienia zostały zaktualizowane. Strona sieci Web zostanie teraz odświeżona. Zmieniono adres IP lub numer portu. Połączenie z urządzeniem RT-N18U zostanie teraz rozłączone. Aby uzyskać dostęp do ustawień urządzenia RT-N18U, ponownie nawiąż połączenie z siecią i skorzystaj z zaktualizowanego adresu IP i numeru portu*" (*Settings have been updated. Web Page will now refresh. Changes have been made to the IP address or port number. You will now be disconnected...*).
Należy w takich przypadku usunąć certyfikaty w przeglądarce internetowej oraz wyczyścić pamięć podręczną (w starszych wersjach): *(Firefox) → Preferancje / Zaawansowane / Sieć / Treści dla trybu offline i dane użytkownika / IP witryny / Usuń.*
W nowszych przeglądarkach: *(Firefox) → Preferencje / Prywatność i bezpieczeństwo / Ciasteczka i dane stron / Wyczyść dane...: Ciasteczka i dane stron* oraz *Treści zachowane w pamięci podręcznej...*

Adres MAC
Uwaga! O dziwo, dla Asusa wielkość liter w adresie MAC ma znaczenie. Wszystko powinno być wprowadzane wielkimi literami.

Reset miękki
Aby zresetować jedynie hasło dostępu i ustawienia, należy przytrzymać wciśnięty przycisk RESET przez 15 sekund. Nie jest czyszczona NVRAM.

Reset twardy 30/30/30
Aby zresetować routery Asus (ale także innych marek) do ustawień fabrycznych (czyszczenie NVRAM) należy:
- odłączyć od niego wszystkie kable oprócz zasilającego;
- przez 30 sekund trzymać wciśnięty przycisk *RESET*;
- odłączyć kabel zasilania nadal trzymając przycisk *RESET* przez kolejne 30 sekund;
- podpiąć kabel zasilania, włączyć urządzenie nadal trzymając przycisk *RESET* przez kolejne 30 sekund.

Uwaga: W przypadku niektórych routerów *Asus* (np. *RT-N16*), zamiast przycisku *RESET* należy użyć przycisk WPS.

Ostatnia aktualizacja: 7 listopada 2019.