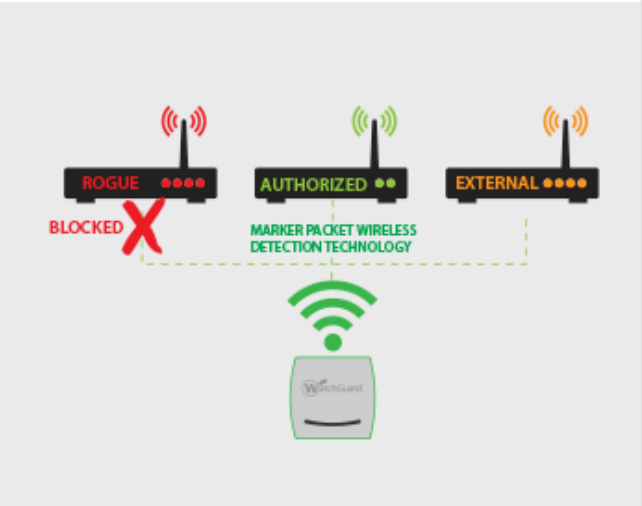
Wireless Intrusion Prevention System (WIPS) - system zapobiegania włamaniom w sieciach WiFi

Najlepszy system WIPS w przemyśle

Cyberprzestępcy dysponują obecnie wieloma narzędziami umożliwiającymi kradzież danych osobowych, podsłuchiwanie transmisji, zakłócanie pracy sieci oraz rozprzestrzenianie szkodliwego oprogramowania za pomocą sieci WiFi. Jak trudno przeprowadzić taki atak w Twojej sieci?
W serwisie YouTube jest obecnie dostępnych ponad 300,000 filmów prezentujących jak zaatakować sieć WiFi przy pomocy łatwych w użyciu i wydajnych narzędzi dostępnych on-line. Możliwości tych narzędzi rozciągają się od ataków typu „Man in the middle" i „Denial Of Service", do podłożenia w sieci nieautoryzowanych urządzeń i fałszywych punktów dostępowych.

Punkty dostępowe firmy WatchGuard zarządzane z poziomu chmury posiadają wbudowany system WIPS - który zapewnia ochronę Twojej sieci. Używając opatentowanej technologii znaczenia pakietów, WatchGuard chroni obszar Twojej sieci WiFi przez 24h na dobę i przez 7 dni w tygodniu przed: nieautoryzowanymi urządzeniami, fałszywymi punktami dostępowymi i złośliwymi atakami - przy zbliżonym do zera poziomie fałszywych alarmów.

Za pomocą zarządzanych z chmury punktów dostępowych firmy WatchGuard z uruchomionym systemem WIPS, administratorzy IT mogą dostarczać wysokowydajne połączenia bezprzewodowe - bez kompromisów w zakresie bezpieczeństwa.



Co powoduje, że rozwiązanie firmy WatchGuard jest unikalne?

WatchGuard WIPS jest opatentowaną technologią znakowania pakietów, która skutecznie wykrywa i klasyfikuje wszystkie widoczne w obszarze Twojej sieci punkty dostępowe i podłączone urządzenia - jak smartfony i tablety. Dzieli widoczne urządzenia na: autoryzowane, zewnętrzne oraz fałszywe.
Ten zaawansowany proces wykrywania fałszywych urządzeń, niemający odpowiedników na rynku, zapewnia, że tylko niebezpieczne połączenia zostaną zamknięte - bez zakłócania pracy sąsiednich sieci.

Opcje elastycznego wdrażania WIPS

Każdy punkt dostępowy WatchGuard może być instalowany jako dedykowany czujnik systemu WIPS. Oznacza to, że zamiast obsługi normalnego ruchu WiFi jest on w 100% dedykowany do skanowania sieci i zapobiegania atakom na nią. Istnieje również możliwość uruchomienia punktu dostępowego WatchGuard w trybie AP/WIPS, gdzie punkt dostępowy dzieli czas swojej pracy pomiędzy proces obsługi normalnego ruchu użytkowników a proces wykrywania ataków na sieć. Punkty dostępowe WatchGuard, mogą być instalowane jako dedykowane czujniki WIPS w środowisku z konkurencyjnymi punktami dostępowymi, dostarczając najlepszego mechanizmu WIPS dla istniejących sieci WiFi.

Wzmocnij swoją ochronę WiFi

Możesz łatwo wzmocnić ochronę, poprzez wprowadzenie punktów dostępowych WG do sieci zabezpieczonej urządzeniami Firebox.
Rozszerzenia ochrony UTM-owej jak - kontrola aplikacji i zabezpieczenie przed szkodliwym oprogramowaniem „Zero Day" - zabezpieczają również Twoją sieć WiFi.

Jak to działa ?

Używając zarządzanego z chmury punktu dostępowego firmy WatchGuard jako czujnika WIPS, można korzystać z technologii, która zabezpiecza Twoją sieć bezprzewodową - od stacji prowadzących szkodliwe działania, w tym fałszywych punktów dostępowych, złośliwych bliźniaków i od ataków mających na celu odmowę dostępu do usług (Denial Of Service / DOS).

Obrona przed fałszywymi punktami dostępowymi

nieautoryzowany punkt dostępowy w Twojej sieci

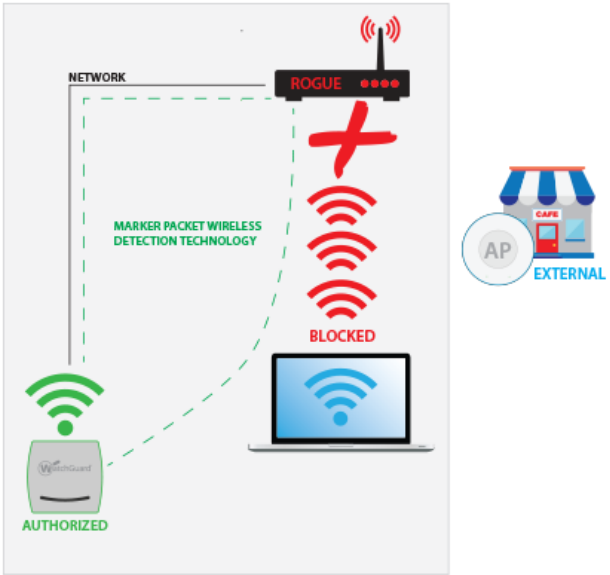
WatchGuard WIPS bez przerwy skanuje wszystkie inne punkty dostępowe w okolicy i klasyfikuje je jako autoryzowane, zewnętrzne lub fałszywe.

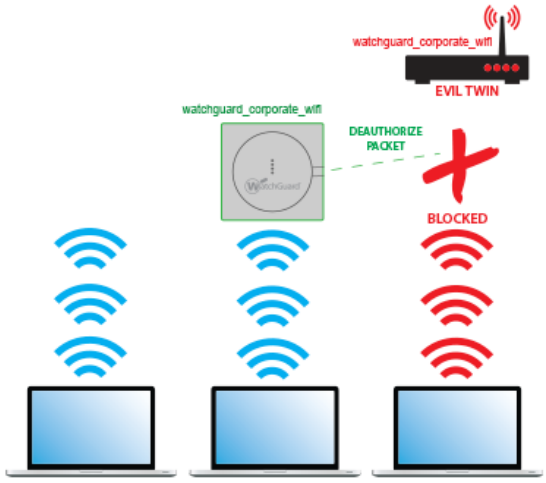
Autoryzowane - znane punkty dostępowe, które są przyłączone do Twojej sieci.

Zewnętrzne - punkty dostępowe, które nie są przyłączone do Twojej sieci.

Fałszywe - nieznane punkty dostępowe, ale włączone do Twojej sieci.

Używając opatentowanej, state-of-the-art Marker Packet wireless detection technology, WatchGuard WIPS szybko i niezawodnie odróżnia bliskie, zewnętrzne punkty dostępowe od punktów dostępowych, które są fałszywe. Jeśli fałszywy punkt dostępowy zostaje wykryty, wszystkie przychodzące do tego punktu połączenia są natychmiast blokowane.





Zapobieganie połączeniom ze „złymi bliźniakami”

punkty dostępowe podszywające się pod Twoje punkty dostępowe

WatchGuard WIPS prowadzi rejestr wszystkich klientów łączących się z autoryzowanymi punktami dostępowymi, śledząc ich adresy sprzętowe i zapamiętując w bazie danych. Jeśli jakiś znany klient rozpoczyna połączenie ze złośliwym punktem dostępowym, to połączenie takie jest natychmiastowo blokowane, poprzez wysłanie pakietu cofającego autoryzację.

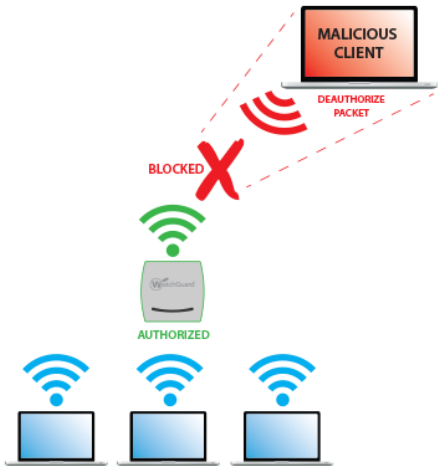
Zatrzymanie ataków typu Denial Of Service

świadome działanie atakującego, prowadzące do sparaliżowania pracy sieci przez rozłączanie klientów

Złośliwi klienci mogą użyć de-autoryzacyjnych pakietów celem zablokowania możliwości połączenia się z Twoją siecią przez pożądanych klientów.

WIPS udaremnia taki atak poprzez nieustanne śledzenie źródeł podejrzanie często nadawanych pakietów de-autoryzacyjnych.

Kiedy takie źródła zostaną zidentyfikowane, to ich przyszła transmisja jest zagłuszana poprzez wysyłanie zaawansowanych technologicznie zakłóceń.



Net Complex Sp. z o.o.
ul. Cieszyńska 79
43-300 Bielsko-Biała
tel.: 33 472 03 18 l 33 816 04 11
faks: 33 486 70 02 l kom: 508 872 270

www.netcomplex.pl
e-mail: netcomplex@netcomplex.pl
NIP: 5472165461 **REGON:** 365444659
Bank ING: 37 1050 1070 1000 0090 3104 7385