PRYWATNA AUTOSTRADA PRZEZ INTERNET

WPROWADZENIE

DO KOŃCA 2018 ROKU 11,4 MLD MASZYN I URZĄDZEŃ ZNAJDZIE SIĘ W GLOBALNEJ SIECI. PODŁĄCZENIE URZĄDZEŃ DO INTERNETU MA OCZYWISTE ZALETY, ALE POŁĄCZENIA SIECIOWE TO RÓWNIEŻ ZAGROŻENIA.

Jeżeli widzieli Państwo film Terminator, gdzie maszyny przejmują kontrolę na Światem i zagrażają ludzkości, mam dobrą wiadomość:
PRZYNAJMNIEJ DO KOŃCA 2018 ROKU, TO SIĘ NIE WYDARZY!

ALE MASZYNY I URZĄDZENIA SĄ NARAŻONE NA RYZYKO PRZEJĘCIA Z ZEWNĄTRZ A TO OZNACZA: STRATY FINANSOWE, AWARIE I PRZESTOJE DLA KLIENTÓW, UTRATĘ REPUTACJI DLA PRODUCENTÓW... OD MOMENTU KIEDY WIRUS STUXNET ZNISZCZYŁ IRAŃSKIE WIRÓWKI WZBOGACANIA URANU, DLA ŚWIATA URZĄDZEŃ INTERNETU RZECZY STAŁO SIĘ JASNE, ŻE POŁĄCZENIA SIECIOWE MUSZĄ IŚĆ W PARZE Z BEZPIECZEŃSTWEM.

Ta prezentacja jest poświęcona idei, jak w przystępny i pewny sposób podłączyć maszyny i urządzenia do Internetu, zabezpieczyć dostęp do nich i chronić dane transmitowane przez sieć publiczną.

INTERNET RZECZY (IoT): ATRAKCYJNY CEL DLA HAKERÓW

Niedostateczne zabezpieczenie dostępu do urządzeń podłączonych do Internetu. Błędy w oprogramowaniu, brak lub długi czas dostarczenia aktualizacji dla SCADA/HMI/PLC/PAC/BMS, czynią je podatne na zagrożenia w sieci.

782%

Wzrost liczby incydentów zagrażających bezpieczeństwu urządzeń automatyki w latach 2006-2012

458%

Wzrost prób skanowania systemów w poszukiwaniu podatności urządzeń IoT w 2015 roku.

Do roku 2020

25%

wszystkich ataków będzie skierowanych na IoT.

Obecnie tylko JEDEN NA CZTERECH administratorów IT odpowiedzialnych za sieć komputerową jest przekonany co do bezpieczeństwa urządzeń podłączonych do sieci Internet.

CELE ATAKÓW CYBERPRZESTĘPCÓW

KRADZIERZ WŁASNOŚCI INTELEKTUALNEJ
-patenty,
-składy receptur,
-listy klientów,

SZPIEGOSTWO PRZEMYSŁOWE
Włamanie do systemu w celu zebrania informacji lub zmiany ustawień.

SABOTAŻ
Atak na urządzenia sieci przemysłowej w celu sparaliżowania sieci korporacyjnej.

PRZEJĘCIE URZĄDZEŃ
Zagrożenie dla ludzi.
Wykorzystanie do ataków DDoS*

*Przejęcie i użycie urządzeń podłączonych do Internetu w celu ataku na zasoby firm trzecich. Np. atak na firmę Dyn w celu zablokowania serwisu Twtter.

JAK ZMIEJSZYĆ RYZYKO ATAKU?

Autoryzacja, uwierzytelnienie dostępu oraz szyfrowanie danych są istotnymi elementami, które chronią maszyny podłączone do Internetu przed przejęciem.

DOBRE ZASADY podłączania maszyn do sieci Internet:

-Urządzenie/system powinno być podłączone do Internetu poprzez **PUNKT DOSTĘPU** pozwalający na:

-DWUSKŁADNIKOWE UWIERZYTELNIENIE, COŚ CO FIZYCZNIE MAM + COŚ CO WIEM, np. sprzętowy token USB podłączany do komputera przechowujący certyfikaty elektroniczne, który jest zabezpieczony hasłem,

- **AUTORYZACJĘ,** nadanie użytkownikom praw dostępu do wybranych elementów w systemie, np. dostęp do jednego sterownika PLC i jednego panelu HMI w podsieci lokalnej,

- **KRYPTOGRAFIĘ,** szyfrowanie danych przesyłanych przez sieć publiczną. Złamanie powszechnie używanego klucza AES-128 bitów metodą *brute force* * mogłaby zająć nawet kilka miliardów lat!

- Sieć lokalna, w której znajduje się urządzenie/system powinna być chroniona zaporą ogniową

UNIKAĆ podłączania maszyn do sieci Internet poprzez:

-Punkt dostępu nie wyposażony w zaporę ogniową zabezpieczony słabym lub domyślnym hasłem
- Punkt dostępu nie wspierający szyfrowania danych
- Publiczny adres IP
- Przekierowanie portów
- Serwisy typu DynDNS

*Atak brute force – algorytm, który opiera się na sukcesywnym sprawdzeniu wszystkich możliwych kombinacji w poszukiwaniu rozwiązania problemu. W kryptologii, przykład zastosowania algorytmu brute force to metoda, w której wypróbowywane są wszystkie możliwe kombinacje cyfr, liter i innych znaków kodu (kluczy), do momentu, aż klucz pasujący do szyfru zostanie znaleziony, czyli otrzymana zostanie informacja w postaci jawnej, odszyfrowanej.

(źródło: cisco

Podłączenie urządzeń przemysłowych do Internetu nie jest zadaniem trywialnym. Szyfrowana dwukierunkowa transmisja danych z urządzeń umieszczonych w lokalnej sieci przemysłowej poprzez firewall, strefę zdemilitaryzowaną (DMZ), sieć korporacyjną, kolejny firewall, sieć publiczną do innej zabezpieczonej sieci lokalnej wymaga angażowania specjalistów i zaawansowanych urządzeń sieciowych.

WYBRANE METODY PODŁĄCZANIA MASZYN DO INTERNETU.

ZRÓB TO SAM

Konfiguracja tuneli VPN do maszyn sterowanych przez różne PROTOKOŁY KOMUNIKACYJNE (Profibus, Profinet, Modbus, Modbus/TCP czy EtherNet/IP), umieszczonych za zaporami ogniowymi i zarządzanie prawami dostępów pracowników jest skomplikowane i czasochłonne.

- wymaga angażowania specjalistów działu IT klienta w celu integracji
- wymaga zakupu i instalacji różnorodnego sprzętu i oprogramowania
- wymaga uzyskania statycznego adresu IP od operatora Internetu
- długi czas oczekiwania na zgodę klienta na podłączenie maszyny do Internetu

VPN W CHMURZE

Aby korzystać z pełnej funkcjonalności systemu trzeba wykupić płatną licencję. Koszty rosną wraz z liczbą użytkowników i ilością danych przesyłanych przez serwery dostawcy.

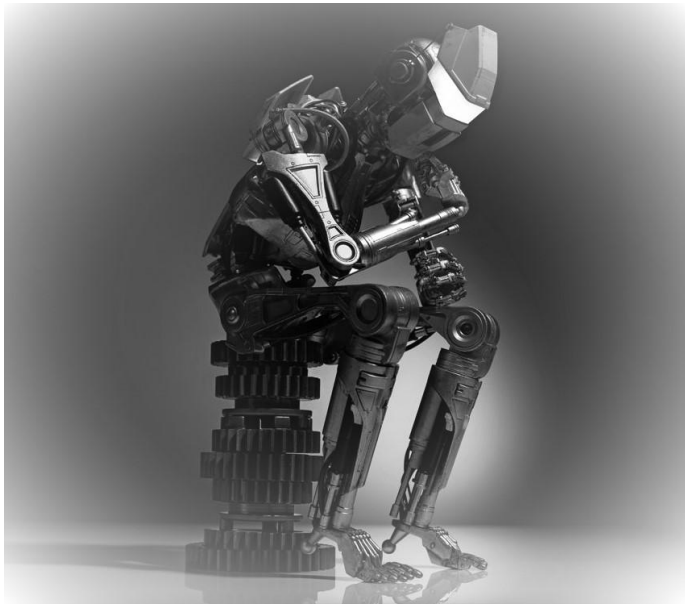
- wymaga zakupu dedykowanych urządzeń dostawcy usługi
- konieczność rejestracji kont użytkowników na serwerze dostawcy usługi
- konieczność instalacji oprogramowania i konfiguracji urządzeń
- dane są przesyłane przez serwery dostawcy usługi ich ilość jest MONITOROWANA

POŁĄCZENIA PC DO PC

Łatwa konfiguracja połączenia do komputera PC podłączonego do maszyny/instalacji. Wymagana opłata za licencję w cyklu miesięcznym. Konieczność rejestracji kont użytkowników na serwerze dostawcy usługi. Dane są przesyłane przez serwery dostawcy usługi.

ZDALNY MONITORING

Urządzenia skonfigurowane w celu prewencyjnego monitoringu podstawowych parametrów instalacji. Najczęściej z wykorzystaniem modemów GSM i płatnej usługi prywatnego APN.



Urządzenia sieciowe i oprogramowanie Tosibox® dedykowane są dla integratorów systemów: sterowania, monitoringu oraz producentów maszyn i urządzeń, którzy chcą on-line **SERWISOWAĆ, DIAGNOZOWAĆ, ZBIERAĆ DANE z jednej lub tysięcy** instalacji podłączonych do Internetu.

URZĄDZENIA TOSIBOX®

gwarantują szyfrowaną transmisję danych poprzez sieć publiczną.

Podstawowy zestaw składa się z routera Tosibox® Lock, sprzętowego klucza TOSIBOX® Key oraz aplikacji TOSIBOX® Mobile Client instalowanej na urządzeniu mobilnym.

Router Tosibox® Lock działa z każdym rodzajem sieci Internet WAN/WLAN/GSM (3G/4G) i pełni rolę punktu dostępowego do podłączonych do niego urządzeń np. sterowników PLC, paneli HMI, kamer CCTV czy komputerów PC.

Konfiguracja urządzenia nie wymaga posiadania specjalistycznej wiedzy czy instalacji oprogramowania.

TOSIBOX® Key pozwala na dwustopniowe uwierzytelnienie (2FA) zdalnego szyfrowanego połączenia VPN pomiędzy komputerem użytkownika a routerem Tosibox Lock i urządzeniami podłączonymi do routera.

TOSIBOX® Mobile Client jest rozszerzeniem systemu TOSIBOX® o zdalny szyfrowany dostęp VPN do maszyn z urządzeń mobilnych.

JAK DZIAŁA TOSIBOX®?

PLUG & GO™ - PATENT FIRMY TOSIBOX®

1. PAROWANIE SPRZĘTOWE Lock-a z kluczem (10 sekund). Następuje wymiana cyfrowych certyfikatów pomiędzy urządzeniami.

2. INSTALACJA INTERFEJSU KLUCZA na dowolnej liczbie komputerów PC.

3. PODŁĄCZENIE URZĄDZEŃ IP do portów LAN routera. Podłączenie routera do Internetu poprzez sieć (WAN, Wi-Fi, GSM).

4. ZESTAWIENIE POŁĄCZENIA, PATENT FIRMY TOSIBOX®

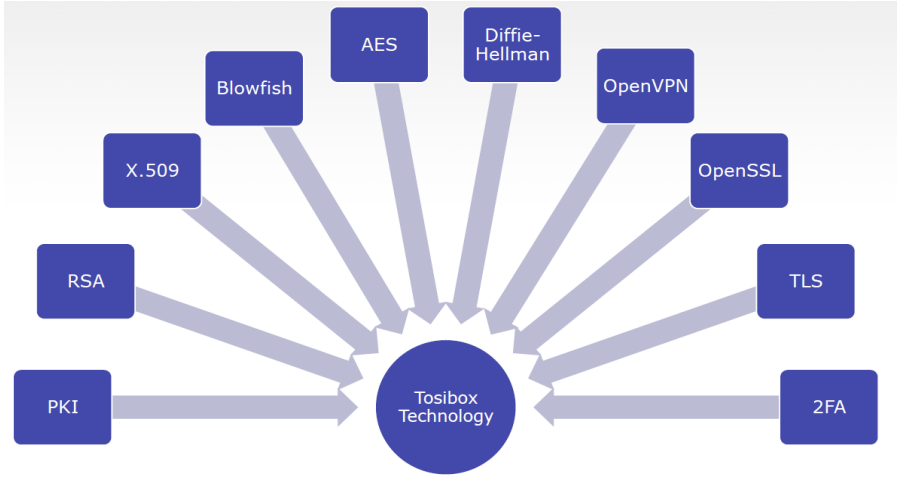
Router umieszczony za zaporą ogniową lub NAT-em w sieci LAN klienta **AUTOMATYCZNIE** zestawia szyfrowane połączenie VPN z kluczem sprzętowym, który został z nim sparowany.

ZESTAWIANIE POŁĄCZENIA

1. Użytkownik wyposażony w klucz Tosibox podłączony do komputera wysyła żądanie połączenia do wybranego routera Tosibox Lock wcześniej sparowanego z kluczem.

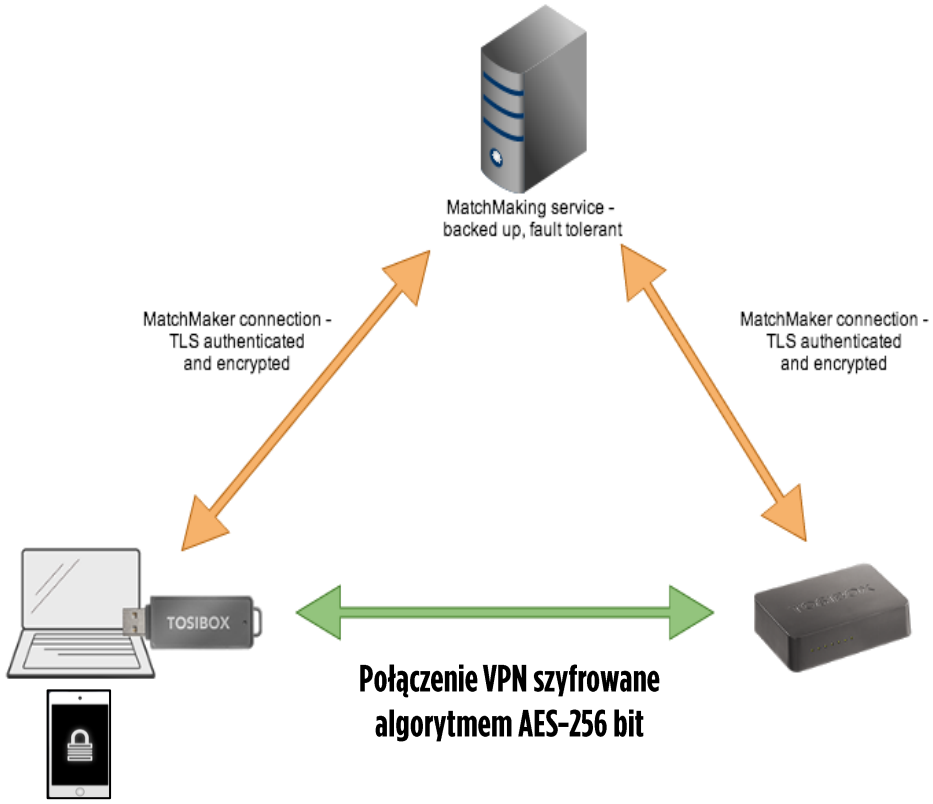
2. Klucz i router, które są on-line łączą się szyfrowanym tunelem do centrum MatchMaking service firmy TOSIBOX OY, (rys. strona prawa).

3. Zanim nastąpi transfer danych MatchMaking service automatycznie sprawdza i uwierzytelnienia certyfikaty urządzeń, następnie zestawia i zatwierdza **BEZPOŚREDNIE POŁĄCZENIE VPN**.



Technologie wykorzystane w produktach Tosibox

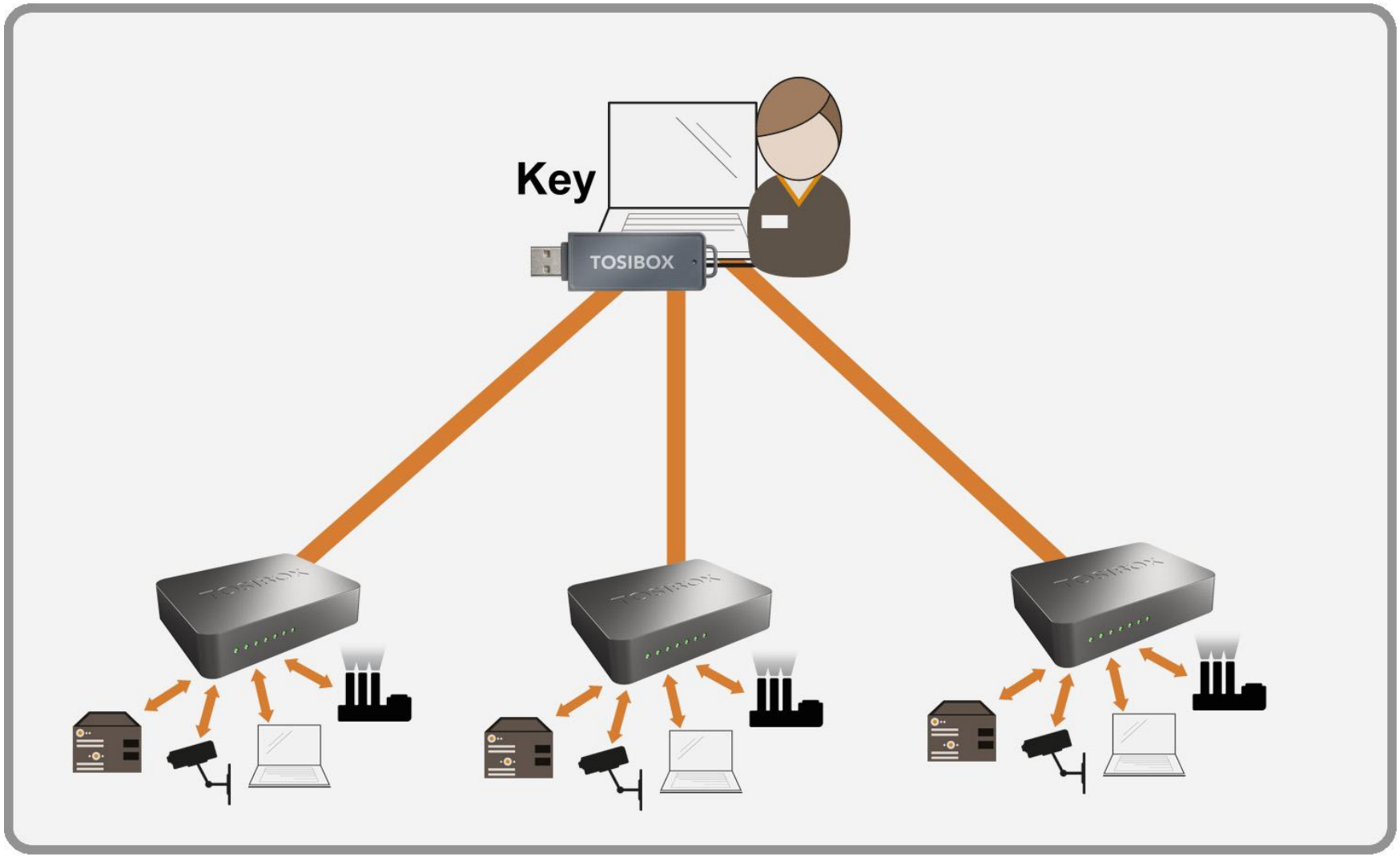
Po zestawieniu połączenia MatchMaking service **NIE JEST POTRZEBNY**. Szyfrowanie i deszyfrowanie danych przesyłanych poprzez sieć publiczną odbywa się **SPRZĘTOWO** w urządzeniach Tosibox. Przesyłane dane są **NIEWIDOCZNE** dla firmy Tosibox oraz innych użytkowników sieci Internet.



ROZBUDOWA SIECI, ZARZĄDZANIE DOSTĘPAMI

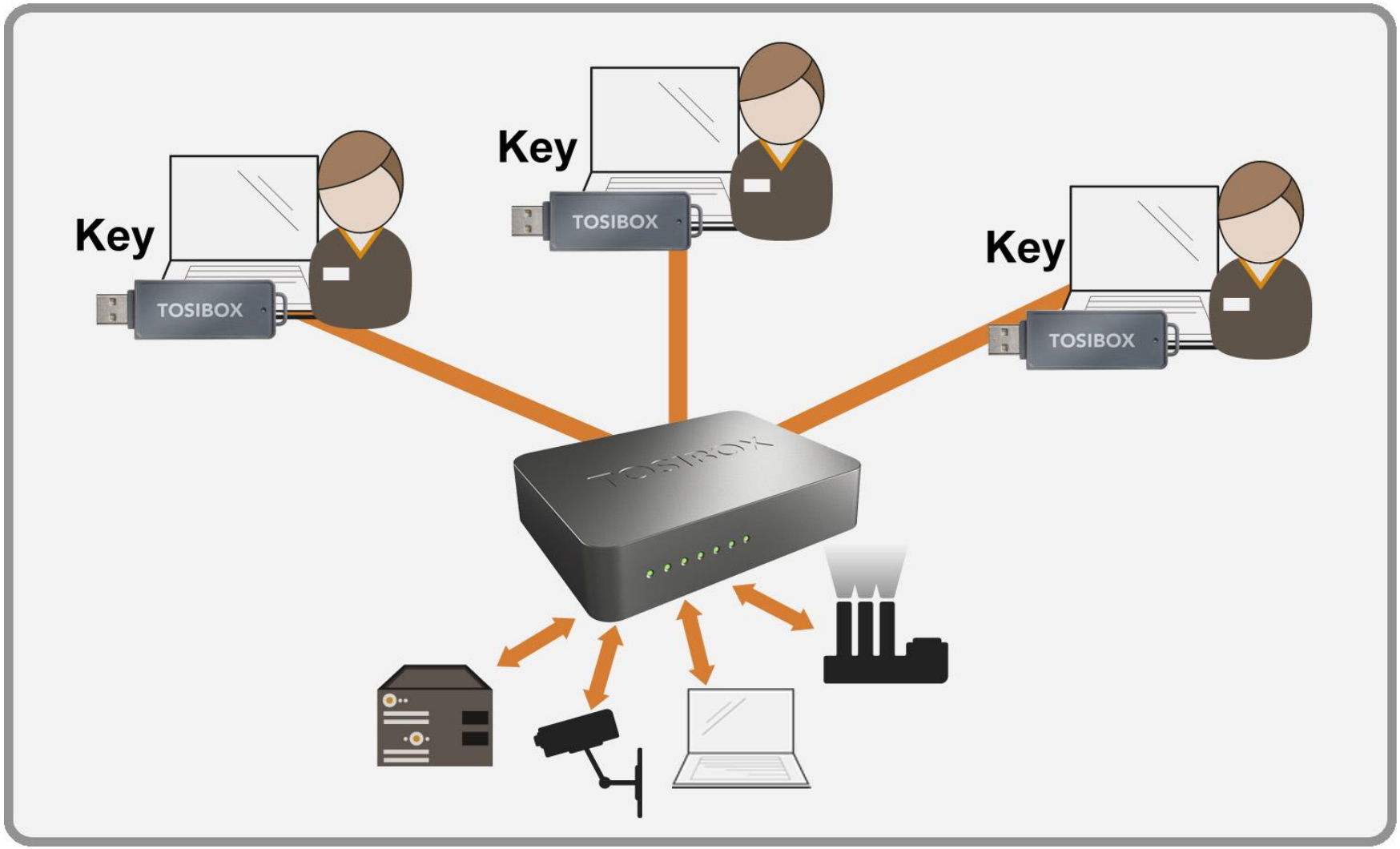
DODAWANIE NOWYCH ROUTERÓW

Jeden Klucz Tosibox może być sparowany z dowolną liczbą routerów Tosibox Lock.



DODAWANIE NOWYCH KLUCZY

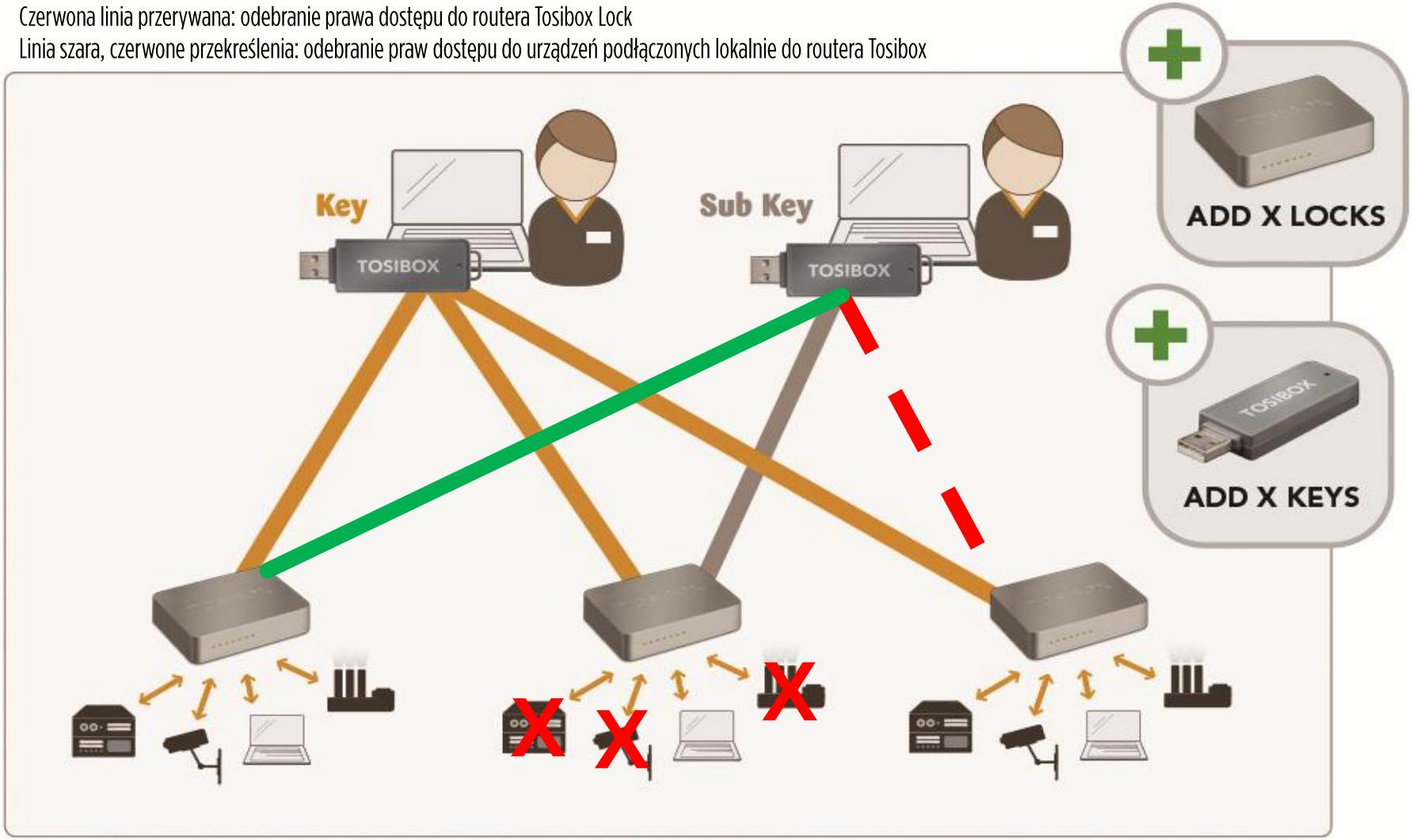
Administrator może dodawać kolejne klucze Tosibox. Użytkownicy mają równoczesny dostęp do systemu.



ZARZĄDZANIE UPRAWNIENIAMI

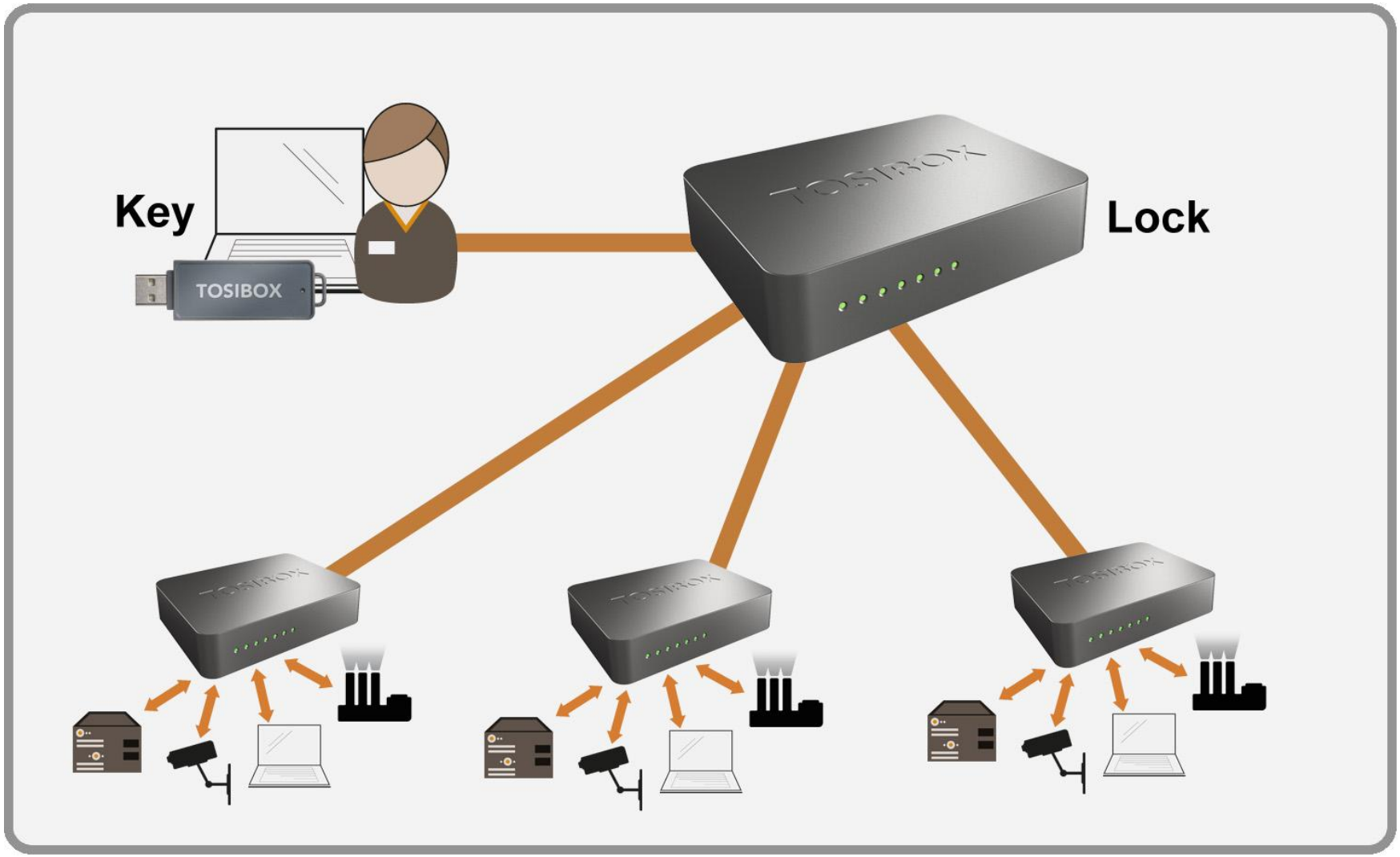
Administrator (Key) dodaje nowe routery i klucze Tosibox. Administrator ma możliwość zdalnej zmiany praw dostępu użytkowników wyposażonych w klucz (Sub Key).

Linia zielona: nadanie nowego prawa dostępu do routera Tosibox Lock
Czerwona linia przerywana: odebranie prawa dostępu do routera Tosibox Lock
Linia szara, czerwone przekreślenia: odebranie praw dostępu do urządzeń podłączonych lokalnie do routera Tosibox



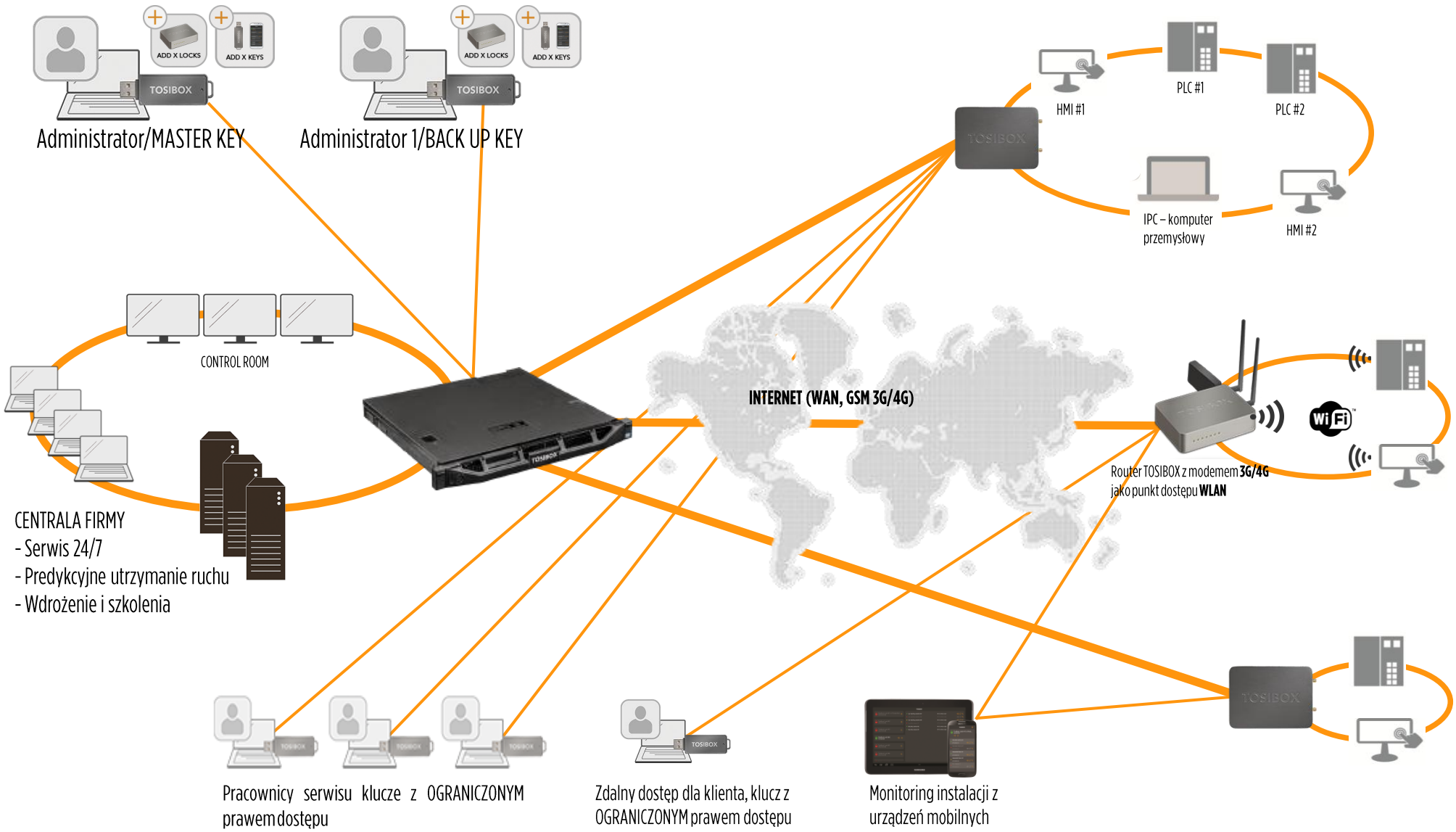
STAŁE ŁĄCZE VPN

Podłączenie instalacji zdalnych do lokalizacji głównej w celu ciągłego zapisu danych np. w bazie SQL. Z zachowaniem dostępu zdalnego poprzez klucz Tosibox.



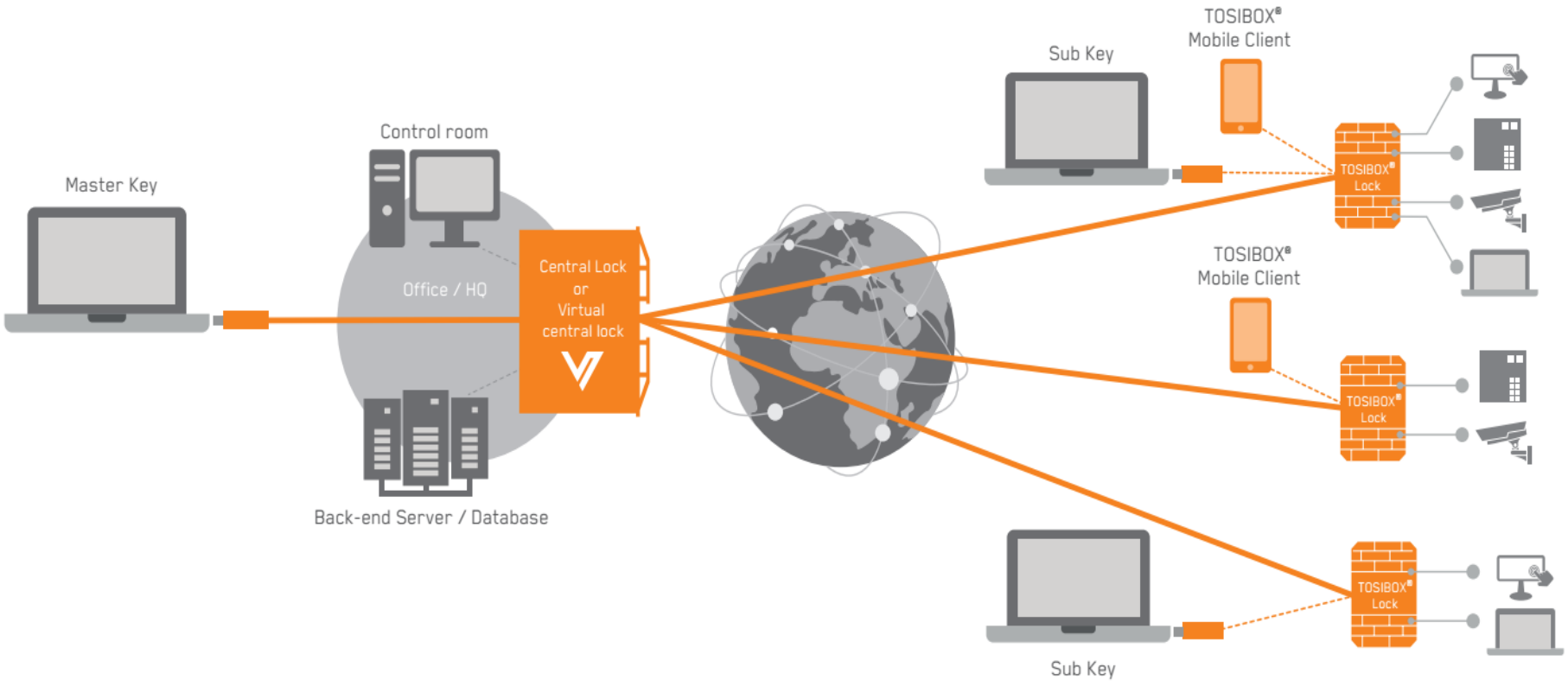
TOSIBOX® KONCENTRATORY VPN

SPRZĘTOWY CENTRAL LOCK – KONCENTRATOR VPN, OBSŁUGUJĄCY DO 4000 KONKURENCYJNYCH TUNELI VPN. Ciągły monitoring instalacji klientów, zarządzanie uprawnieniami, zapis logów, alarmy, archiwizacja danych.



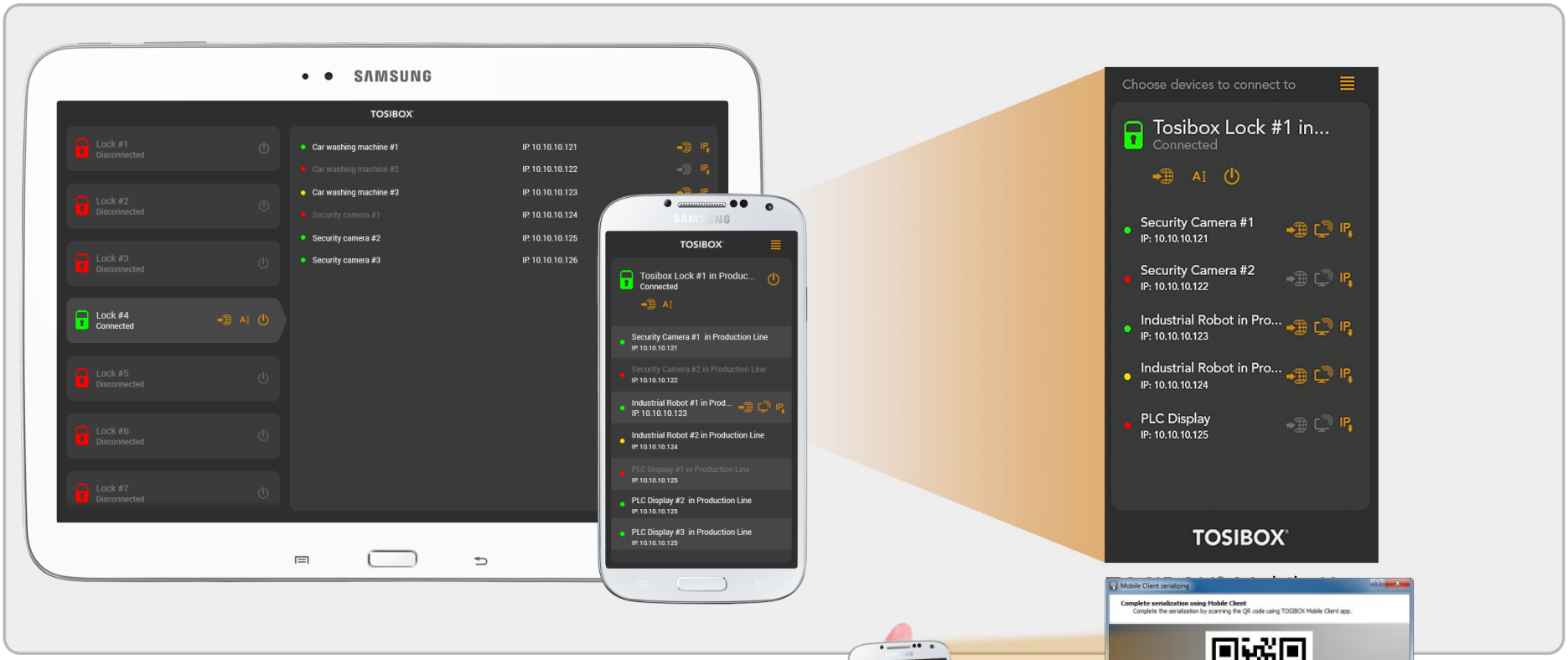
WIRTUALNY CENTRAL LOCK – KONCENTRATOR VPN DLA URZĄDZEŃ TOSIBOX

Oprogramowanie kompatybilne z platformami wirtualizacyjnymi (**VMWARE ESXi, Microsoft Hyper-V, Linux KVM**). Dostępne w elastycznym modelu licencyjnym.



TOSIBOX® APLIKACJA MOBILNA I AKCESORIA GSM

POŁĄCZENIA VPN Z URZĄDZEŃ MOBILNYCH dostęp do urządzeń przemysłowych po pobraniu aplikacji Tosibox Mobile Client i autoryzacji urządzeń mobilnych.



Aplikacja TOSIBOX® Mobile Client działa z systemem ANDROID i iOS. **AUTORYZACJA** urządzenia mobilnego wymaga zeskanowania kodu QR lub wprowadzenia kodu cyfrowego generowanego w interfejsie klucza Tosibox Key.

PRZEMYSŁOWY MODEM* 4G/3G

Podłączany zewnętrznie do routerów Tosibox pozwala na połączenia VPN poprzez sieć GSM niezależnie od operatora sieci, nie jest wymagana karta SIM ze statycznym adresem IP.

Konfiguracja połączeń sieciowych jest trudna , ich zabezpieczenie jest jeszcze trudniejsze.

DANE DO KONTAKTU PACE POLAND | REGIONALNY DYSTRYBUTOR TOSIBOX

DARIUSZ NOWAK

email: dariusz.nowak@pacepoland.pl

www.pacepoland.pl

Tel. +48 513 188 627

Pace Poland reprezentuje na rynku polskim fińską firmę TOSIBOX Oy producenta rozwiązań sieciowych do bezpiecznego przesyłania danych i zabezpieczania dostępu do urządzeń podłączonych do Internetu.

Klientami firmy Pace Poland w Polsce są producenci maszyn, integratorzy systemów automatyki przemysłowej, automatyki budynkowej, systemów bezpieczeństwa oraz systemów CCTV.

NAGRODY DLA TOSIBOX

CONTROL ENGINEERING Polska

PRODUKT ROKU 2014

Tytuł Produkt Roku w kategoriach:
- Komunikacja bezprzewodowa
- Aplikacje mobilne

WYBRANI PARTNERZY PACE POLAND

OMRON

FlexLink®

RAFAMET

SPOMASZ PLESZEW SA

ControlTec optymalizacja procesów

PiAZAP nowoczesne technologie w Twoim zasięgu

TELESTE