LIVE

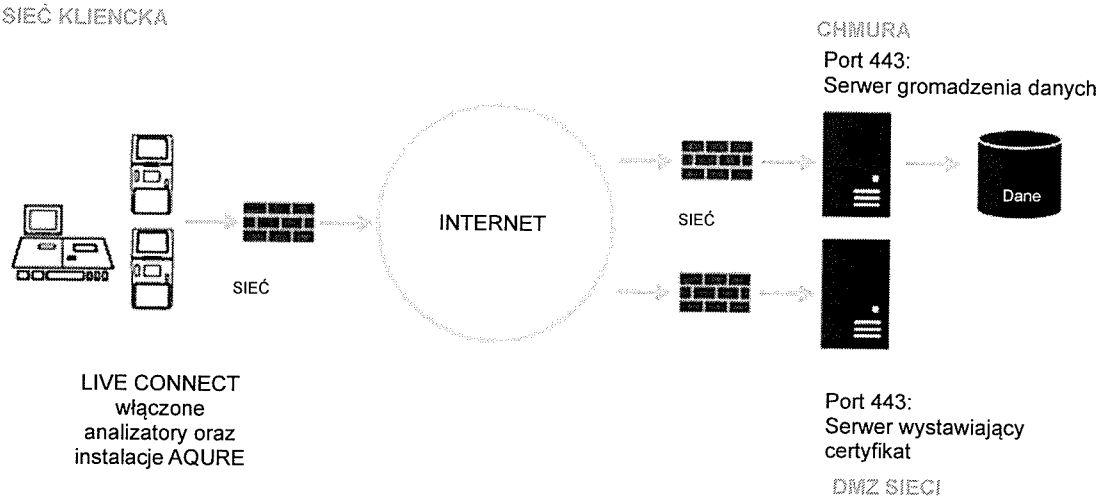
System IT **oraz rozwiązania IoT**

LIVE Connect, AQURE Peer Quality Control i Quality Manager

Od AQURE 2.4.2, LIVE Connect 2.4 oraz Quality Manager 1.0

Infrastruktura

Rysunek poniżej przedstawia typowego klienta (np. szpitale, laboratoria itp.), architekturę sieci i szczegóły komunikacji dotyczące systemu IT oraz rozwiązań IoT



RYS. 1: INFRASTRUKTURA

Definicja danych

Definicja danych znajduje się w pkt 1 dokumentu „Warunki spółki w zakresie przekazywania danych".

Warunki działania: Konfiguracja zapory klienckiej

1. Przypadek 1: Dostęp za pośrednictwem routera (brak dostępu do sieci szpitalnej)
   a. W celu podłączenia analizatorów do Live Connect należy wykorzystać routery Cisco Meraki skonfigurowane według szablonu
2. Przypadek 2: Dostęp przez sieć szpitalną – konfiguracja zapory klienckiej
   a. Zapora powinna zezwalać na ruch wychodzący na serwery
      i) punkty końcowe o adresach IP z zakresu od 195.41.216.129 do 195.41.216.254
      ii) TCP port 443
      iii) TCP port 80
   b. Zapora powinna zezwalać na ruch wychodzący na domeny Microsoft Azure określone poniżej. Zapory głębokiej inspekcji pakietów (DPI, ang. Deep Packet Inspection) muszą być tak skonfigurowane, aby wykluczyć inspekcję podczas komunikacji z przedmiotowymi domenami.

Domena	Port	Cel
global.azure-devices-provisioning.net	Serwer udostępniania urządzeń	Usługa udostępniania urządzeń (DPS – Device Provisioning Service) Hub IOT to usługa pomocnicza dla Hubu IoT, która umożliwia bezobsługowe i terminowe udostępnianie urządzeń odpowiedniemu hubowi IoT bez konieczności interwencji człowieka.
*.azure-devices.net	Hub IOT Microsoft Azure, punkt	Hub Azure IoT jest łącznikiem między Internetem rzeczy Microsoft a chmurą. To w pełni zarządzana

	końcowy zbierania danych	usługa w chmurze umożliwiająca niezawodną i bezpieczną komunikację dwukierunkową między urządzeniami IoT a rozwiązaniem typu back-end.
*.azure-api.net	Usługi Microsoft Azure API Management	API Management (APIM) to sposób na tworzenie spójnych i nowoczesnych bram API pozwalających na bezpieczną ekspozycję usług typu back-end w Azure Cloud.
*.trafficmanager.net	Azure Traffic Manager	Azure Traffic Manager to sposób na równoważenie ruchu w oparciu o technologię DNS, umożliwiający optymalną dystrybucję ruchu na serwerach.
*.cloudapp.net	Aplikacja Azure – usługa związana z nazwami poddomen	Microsoft Azure przydziela poddomenę cloudapp.net dla indywidualnie stworzonych aplikacji. Dla przykładu, jeśli nasza usługa w chmurze nazywa się „LIVEConnect. ", użytkownicy będą mogli połączyć się z aplikacją przez URL o postaci http://LIVEConnect. cloudapp.net
*.ods.opinsights.azure.com	Usługa analityczna Microsoft Cloud Log	Azure Log Analytics to usługa w OMS (Operations Management Suite) pomagająca zbierać i analizować logi oraz dane dotyczące zdarzeń generowane przez zasoby w naszych środowiskach lokalnych, a także w chmurze.

c. Zapory głębokiej inspekcji pakietów (DPI, ang. Deep Packet Inspection) muszą być tak skonfigurowane, aby wykluczyć inspekcję podczas komunikacji z tymi domenami w odniesieniu do uruchomionych lokalnie usług LIVE Connect.

Domena	**Cel**	**Szczegóły**	
* net	Domeny obejmujące serwery do udostępniania pulpitu zdalnego, usługi gromadzenia danych i odwoływania certyfikatów	**Poddomena**	**Cel**
		heimdall. net	Serwer gromadzenia danych
		Remotedk. net	Serwer udostępniania pulpitu zdalnego
		Remotedk4. .net	Serwer udostępniania pulpitu zdalnego
		Remotedk5. .net	Serwer udostępniania pulpitu zdalnego
		Remotedk6. .net	Serwer udostępniania pulpitu zdalnego
		Remotedk7 .net	Serwer udostępniania pulpitu zdalnego
		Remotedk8 net	Serwer udostępniania pulpitu zdalnego
		subca. net	Serwer odwoływania certyfikatów
		Icccis. net	Serwer wystawiający certyfikat
		Icdes. net	Analizator i serwer instalacji typu enrollment

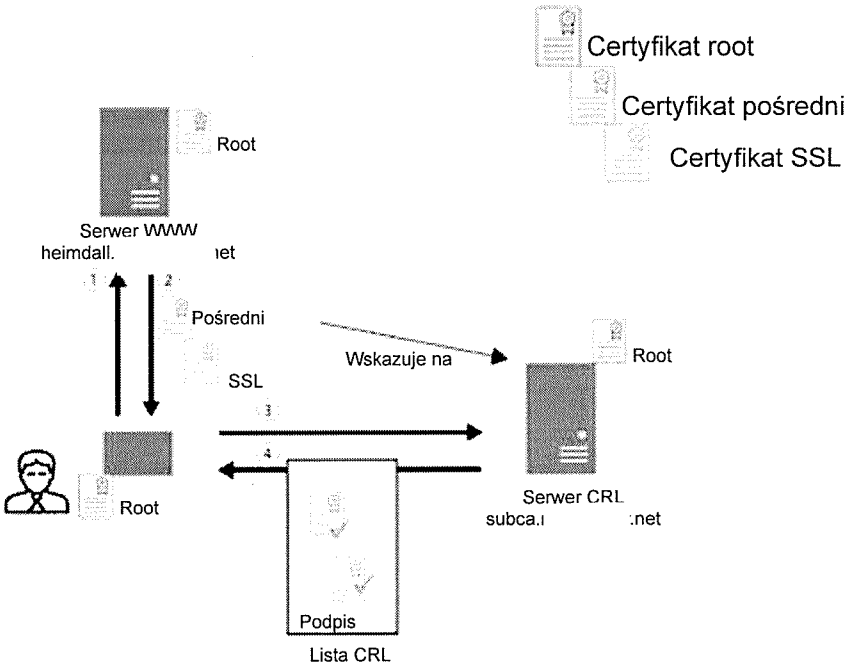
d. System IT oraz rozwiązania IoT będą działać jedynie, jeśli analizator lub instalacja posiadają ważny certyfikat klienta podpisany przez Po stronie klienta technik serwisu terenowego (FSE) inicjuje proces wystawiania certyfikatu klienta, przedstawiając swoje ważne uprawnienia w celu potwierdzenia prawa do wystawienia nowego certyfikatu.

Gdy analizator lub instalacja otrzyma certyfikat klienta, podłączy się do serwera gromadzenia danych. Serwer będzie podłączony tak długo, jak analizator lub instalacja będzie uruchomiony/uruchomiona. Podłączony analizator lub instalacja będzie wysyłać dane do serwera gromadzenia danych.

Informacja o odwołaniu certyfikatu

System IT oraz rozwiązania IoT działają tylko wówczas, gdy ruch jest podpisywany za pomocą certyfikatu

1. Przeglądarka chce ustanowić połączenie https.
2. Serwer odpowiada pośrednimi i publicznymi certyfikatami SSL.
3. Ponieważ certyfikat pośredni zawiera adres URL CRL (Certificate Revocation List – listy odwołanych certyfikatów), przeglądarka zażąda od serwera podpisanej listy odwołanych certyfikatów.
4. Podpisana lista odwołanych certyfikatów jest zwracana do klienta. W tym momencie nawiązanie połączenia za pomocą certyfikatów zależy od klienta. Typowe kontrole przeprowadzane w odniesieniu do certyfikatu to sprawdzenie daty wygaśnięcia i czy nie został on odwołany.



Dalsze informacje techniczne i dotyczące bezpieczeństwa

Transmisja danych

- Transmisja danych między analizatorami lub instalacjami a systemem IT oraz rozwiązaniami IoT jest szyfrowana indywidualnymi certyfikatami TLS X.509.

Uwierzytelnienie punktu końcowego

- Aby zagwarantować, że informacje i usługi pochodzą od oczekiwanych serwerów, LIVE Connect Performance Insights (statystyki wydajności) umożliwiają uwierzytelnienie punktu końcowego przy użyciu protokołu Secure Sockets Layer (SSL). Wszystkie certyfikaty stosowane przy uwierzytelnieniu punktu końcowego są wydawane przez Certyfikaty są instalowane w analizatorach, aby zapewnić zdolność każdego analizatora do potwierdzenia, że jest on podłączony do autoryzowanej usługi

Szyfrowanie dwukierunkowe

- Aby zapewnić prywatność komunikacji w sieci między analizatorem lub instalacją a systemem IT oraz rozwiązaniami IoT, stosowane jest zaawansowane szyfrowanie z wykorzystaniem szyfru blokowego Advanced Encryption Standard (256-bitowy AES) w kombinacji ze standardem szyfrowania TLS 1.2 (lub wyższym). Zabezpieczenie to będzie automatyczne i przejrzyste za każdym razem, gdy zostanie nawiązane połączenie z analizatorem lub instalacją.

HTTPS

- Wszelkie dane przesyłane do i z analizatora lub instalacji do systemu IT oraz rozwiązań IoT są przesyłane za pomocą protokołu HTTPS i dodatkowo podpisane certyfikatami publikowanymi przez
- HTTPS to standardowa technologia internetowa implementująca środki ochronne w zakresie następujących elementów:
  - Uwierzytelnienie (serwer jest tym, za kogo się podaje).
  - Prywatność (wszystkie dane są szyfrowane).
  - Integralność (protokół zapewnia, że dane nie są zmieniane podczas przesyłu).
  - Zabezpieczenie przed atakami typu *man-in-the-middle*.
  - Zabezpieczenie przed podsłuchem.

Uwierzytelnienie użytkownika

- Systemu IT oraz rozwiązań IoT mogą używać tylko upoważnieni technicy serwisu terenowego (FSE)
- Technologia uwierzytelnienia systemu IT oraz rozwiązań IoT wykorzystuje standard Microsoft Active Directory.
  W przypadku opuszczenia przez technika serwisu terenowego, jego konto zostaje automatycznie wyłączone.
- Obowiązkiem każdego technika serwisu terenowego jest częsta zmiana silnego hasła do Active Directory.
- Wszyscy technicy serwisu terenowego są corocznie szkoleni w zakresie ochrony danych.