Odpowiedzi zamieszczono w treści poniżej pod pytaniami:

Dotyczy: postępowania o udzielenie zamówienia publicznego na „Rozbudowa Muzeum Martyrologicznego w Żabikowie” - ***Nr postepowania: ZP.2131.6.2024***
W związku z prowadzonym przez Państwa postępowaniem pn. na „Rozbudowa Muzeum Martyrologicznego w Żabikowie” zwracamy się do Państwa z następującymi pytaniami:

1. W przedmiarze teletechnicznym zawarto nazwy własne punktów dostępowych: „Acces point FAP-231G-E Fortinet FortiAP 231G”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności punktów dostępowych. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

Access Point

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    a. Temperatura 0–50°C,
    b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n,
    b. 5 GHz 802.11a/n/ac/ax,
    c. 2.4/5/6 GHz 802.11a/b/g/n/ac/ax
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet: 10/100/1000 Base-TX oraz 100/1000/2500 Base-TX,
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    a. Tunnel,
    b. Bridge,
    c. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a. MIMO – 2x2,
    b. Maksymalna przepustowość dla poszczególnych modułów radiowych:
        i. 574 Mbps;
        ii. 1201 Mbps;

iii. 2401 Mbps;

c. Wymagana moc nadawania:
   i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
   ii. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
   iii. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
d. Wsparcie dla 802.11n 20/40Mhz HT,
e. Wsparcie dla kanałów 80 i 160MHz,
f. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz.
g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,

12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512;
13. Funkcje dodatkowe:
    a. OFDMA UL i DL
    b. Spatial Reuse (BSS Coloring)
    c. UL-MU-MIMO
    d. DL-MU-MIMO
    e. Enhanced Target Wake Time (TWT)
    f. Wbudowany analizator widma
    g. Wbudowane mechanizmy WIPS/WIDS

GWARANCJA ORAZ WSPARCIE

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2. W przedmiarze teletechnicznym zawarto nazwy własne kontrolerów sieci bezprzewodowej:
   „Kontroler sieci bezprzewodowej FG-90G-BDL-950-36 Fortinet FortiGate 90G”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kontrolerów. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

WYMAGANIA OGÓLNE

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.

- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

REDUNDANCJA, MONITORING I WYKRYWANIE AWARII

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

INTERFEJSY, DYSK, ZASILANIE:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 8 portami Gigabit Ethernet RJ-45.
   - 2 gniazdami SFP+ 10 Gbps wyposażonych we wkładki LR.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

PARAMETRY WYDAJNOŚCIOWE:

1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 124 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 4.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1.3 Gbps.

FUNKCJE SYSTEMU BEZPIECZEŃSTWA:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

POLITYKI, FIREWALL

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

POŁĄCZENIA VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

ROUTING I OBSŁUGA ŁĄCZY WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

FUNKCJE SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

ZARZĄDZANIE PASMEM

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

OCHRONA PRZED MALWARE

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

OCHRONA PRZED ATAKAMI

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

KONTROLA APLIKACJI

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

KONTROLA WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

UWIERZYTELNIANIE UŻYTKOWNIKÓW W RAMACH SESJI

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

ZARZĄDZANIE

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

LOGOWANIE

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania

i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

SERWISY I LICENCJE

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

GWARANCJA ORAZ WSPARCIE

System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

3. W przedmiarze teletechnicznym zawarto nazwy własne przełączników: „Przełącznik FS-148F-FPOE Fortinet FortiSwitch 148F-FPOE”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności przełączników. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

PRZEŁĄCZNIK SIECIOWY

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

PARAMETRY FIZYCZNE PLATFORMY

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Budżet mocy dla portów PoE min.: 740 W.
- Maksymalny pobór mocy bez budżetu dla PoE: 160 W.
- Minimalny zakres temperatury pracy: 0-40°C.

INTERFEJSY SIECIOWE - WYMAGANIA MINIMALNE

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.

- W tym porty PoE w ilości co najmniej: 48, zgodne ze standardem: 802.3af oraz 802.3at.

e) 4 porty 10 GE SFP+.

ZARZĄDZANIE

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

PARAMETRY WYDAJNOŚCIOWE

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

WYMAGANE FUNKCJE

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).

- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

DODATKOWE FUNKCJE URZĄDZENIA PRZY INTEGRACJI Z SYSTEMEM CENTRALNEGO ZARZĄDZANIA / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Centralne zarządzanie konfiguracją urządzenia
   - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   - Centralne zarządzanie sieciami VLAN.
   - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
   - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
   - Automatyczna detekcja i rekomendacje konfiguracji.
   - Przesyłanie logów na zewnętrzny serwer syslog.
   - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   - Obsługa białych i czarnych list adresów MAC.
   - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

FUNKCJE URZĄDZENIA PRZY INTEGRACJI Z SYSTEMEM CENTRALNEGO ZARZĄDZANIA LUB BEZPIECZEŃSTWA

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

GWARANCJA ORAZ WSPARCIE

System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach

tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

4. W przedmiarze teletechnicznym zawarto nazwy własne przełączników szkieletowych: „Przełącznik szkieletowy JG933A HPE 5130 24G SFP 4SFP+”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności przełączników. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

SPECYFIKACJA WYMAGAŃ, PRZEŁĄCZNIK SZKIELETOWY
W związku z zapowiedzą producenta w zakresie zakończenia sprzedaży w/w urządzeń i opublikowaniu parametrów następcy technologicznego (5140-24G-SFP-4SFP+ EI, PN: JL826A), projektant dokonuje aktualizacji specyfikacji.

1. Minimum 24 porty 100/1000BaseX ze stykiem definiowanym przez SFP
2. Minimum 8 portów gigabitowych w standardzie 100/1000BaseT (dopuszcza się porty typu Combo, współdzielone z portami SFP)
3. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP)
4. Wydajność: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
5. Przepustowość: minimum 95 Mp/s
6. Tablica adresów MAC o wielkości minimum 16000 pozycji
7. Pamięć stała (typu Flash): minimum 256MB
8. Pamięć operacyjna: minimum 512MB
9. Obsługa ramek Jumbo
10. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.
11. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT (z obsługą i bez obsługi standardu PoE+), nie mniej niż 210 portów 1000BaseX i ich kombinacji.
12. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))
13. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
14. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP
15. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng
16. Policy Based Routing
17. Wsparcie dla Bidirectional Forwarding Detection (BFD)
18. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
19. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
20. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN
21. Obsługa IEEE 802.1ad QinQ i Selective QinQ
22. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
23. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
24. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6)

25. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
26. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
27. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
28. Obsługa standardu 802.1p – min. 8 kolejek na porcie
29. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p
30. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP
31. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s
32. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring
33. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:
    • Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x
    • Możliwość uwierzytelniania wielu użytkowników na jednym porcie
    • Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS
    • Przypisanie profilu QoS dla użytkownika lub grupy użytkowników
34. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED
35. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC
36. TACACS+ i RADIUS Network Login
37. RADIUS Accounting
38. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
39. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
40. Syslog
41. Obsługa NETCONF
42. Obsługa sFlow
43. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3
44. Obsługa Network Time Protocol (NTP) i Simple Network Time Protocol (SNTP)
45. Obsługa IEEE 802.3AH
46. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter
47. Obsługa protokołu IPsec
48. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).
49. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
50. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
51. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego
52. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol

53. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych
54. Minimalny zakres pracy od -5°C do 45°C
55. Wysokość w szafie 19" – 1U, głębokość nie większa niż 36 cm
56. Maksymalny pobór mocy nie większy niż 60W
57. Wszystkie wymagane na przełączniku funkcje (o ile nie wyspecyfikowano inaczej) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. Jeżeli do działania którejkolwiek z wymaganych funkcji potrzebna jest licencja, należy ją dostarczyć.
58. Producent sprzętu musi być sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure" i znajdować się w kwadracie liderów (Leaders). Dane z najnowszego raportu aktualne na dzień ogłoszenia postępowania.
59. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.

5. W przedmiarze teletechnicznym zawarto nazwy własne przełączników brzegowych: „Przełącznik brzegowy JL260A Aruba 2930F 48G 4SFP"

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności przełączników. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

SPECYFIKACJA WYMAGAŃ, PRZEŁĄCZNIK BRZEGOWY

W związku z aktualizacją dokumentacji przełącznika przez producenta projektant dokonuje aktualizacji specyfikacji.

1. Minimum 48 portów gigabitowych w standardzie 100/1000BaseT
2. Minimum 4 porty 1Gb SFP
3. Przepustowość: minimum 104 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 77 Mp/s
5. Tablica adresów MAC o wielkości minimum 32000 pozycji
6. Obsługa ramek Jumbo
7. Routing IPv4 – minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
8. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
9. Wielkość sprzętowej tablicy rutingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
10. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
11. Obsługa VxLAN
12. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
13. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN
14. Funkcja Root Guard oraz BPDU protection
15. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z

punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania

16. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
17. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping
18. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
19. Obsługa standardu 802.1p – min. 8 kolejek na porcie
20. Funkcja mirroringu portów
21. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
22. Funkcja autoryzacji użytkowników zgodna z 802.1x
23. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
24. RADIUS Accounting
25. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3
26. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.
27. Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)
28. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.
29. Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow.
30. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
31. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
32. Obsługa Syslog
33. Obsługa NTP lub SNTPv4
34. Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku
35. Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
36. Wsparcie dla funkcji Private VLAN lub równoważnego
37. Obsługa protokołu VTP lub MVRP
38. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) lub Device Link Detection Protocol (DLDP) lub równoważnego
39. Minimalny zakres pracy od 0°C do 45°C
40. Wysokość w szafie 19” – 1U, głębokość nie większa niż 30 cm
41. Maksymalny pobór mocy nie większy niż 190W
42. Wszystkie wymagane na przełączniku funkcje (o ile nie wyspecyfikowano inaczej) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. Jeżeli do działania którejkolwiek z wymaganych funkcji potrzebna jest licencja, należy ją dostarczyć.
43. Producent sprzętu musi być sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” i znajdować się w kwadracie liderów (Leaders). Dane z najnowszego raportu aktualne na dzień ogłoszenia postępowania.
44. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez

producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.

6. W przedmiarze teletechnicznym zawarto nazwy własne czytników: „Czytnik HID R10”
Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności czytników. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

Poniżej podano specyfikację parametrów czytnika SIGNO S20 (następcy HID R10), w związku zapowiedzią producenta polegającą na planach wycofania ze sprzedaży czytników HID R10.

1. Czytnik kart zbliżeniowych musi być zgodny ze standardami 13,56 MHz ISO 15693 i ISO 14443A, aby zapewnić kompatybilność produktu i przewidywalność działania.
2. Aby zapewnić bezpieczeństwo i prywatność danych, czytnik kart zbliżeniowych powinien być kompatybilny z modelem danych zbudowanym w oparciu o otwarte standardy, niezależnie od formy nośnika. Poświadczenia mogą znajdować się na dowolnej ilości nośników, takich jak tradycyjne zbliżeniowe karty kompozytowe ISO, breloki zbliżeniowe oraz w nośnikach cyfrowych takich jak poświadczenia mobilne obsługiwane z poziomu urządzeń mobilnych z systemami operacyjnymi Android, Android Wear lub iOS.
3. Czytnik kart zbliżeniowych powinien wspierać kompatybilność wsteczną z formatami kart 13.56 MHz stosowanych w systemach kontroli dostępu (np. 26-bitów, 32-bity, 35-bitów, 48-bitów, 56-bitów itd.).
4. Czytnik kart zbliżeniowych powinien czytać, interpretować oraz uwierzytelniać dane kontroli dostępu z kart zbliżeniowych w technologii 13.56 MHz lub poświadczeń mobilnych z urządzeń z systemami operacyjnymi Android lub iOS takich jak smartfony, tablety, smartwache przy wykorzystaniu protokołów komunikacyjnych Bluetooth Low Energy 2.4 GHz lub NFC (Near Field Communication) 13.56 MHz.
5. Czytnik kart zbliżeniowych musi domyślnie obsługiwać Enhanced Contactless Polling firmy Apple (ECP), aby obsługiwać poświadczenia w portfelu Apple Wallet.
6. Czytnik kart zbliżeniowych powinien wspierać funkcjonalność iBeacon, która umożliwia wzbudzanie aplikacji na urządzeniach mobilnych, znacząco poprawiając skuteczność pierwszych odczytów w danym dniu oraz ograniczając czas reakcji takiej transakcji.
7. Czytnik kart zbliżeniowych powinien występować w dwóch wariantach:
    a. Czytnik kart zbliżeniowych
    b. Czytnik kart zbliżeniowych z klawiaturą

    Przy czym gabaryty obu wersji czytnika nie powinny się zmienić zapewniając pełną elastyczność zmiany w przypadku konieczności skorzystania z urządzenia posiadającego klawiaturę numeryczną.
8. Czytnik kart zbliżeniowych posiadający klawiaturę powinien bazować na rozwiązaniu pojemnościowej klawiatury dotykowej, zapewniając niezawodne działanie w trudnych warunkach środowiskowych.
9. Czytnik kart zbliżeniowych posiadający klawiaturę powinien wspierać tryb pracy dla osób niedowidzących uwzględniając dodatkowy czas na znalezienie znaku orientacyjnego i wprowadzenie danych PIN bez wysyłania niezamierzonych bądź błędnych danych do systemu KD.
10. Czytnik kart zbliżeniowych powinien korzystać z bezpiecznego elementu (Secure Element Technology ™) w celu ochrony kluczy i zapewnienia bezpiecznych funkcji kryptograficznych. Bezpieczny element czytnika powinien być oceniony zgodnie z międzynarodową normą oceny bezpieczeństwa Common Criteria, uzyskując minimalne Evaluation Assurance Level (EAL) na poziomie EAL 5+.

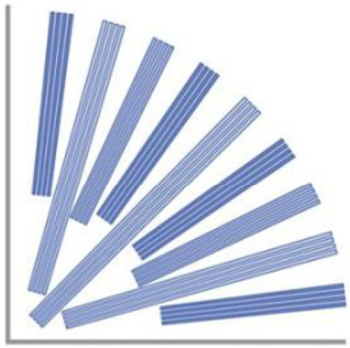
11. Aby zapewnić uniwersalną kompatybilność z większością systemów kontroli dostępu, czytnik kart zbliżeniowych powinien obsługiwać standard SIA AC-01 WIEGAND a także bezpieczną (szyfrowaną), dwukierunkową komunikację zgodnie z v2 standardu SIA OSDP (Open Supervised Device Protocol). Zmiana pomiędzy standardami powinna być dostępna przy użyciu odpowiedniej aplikacji bez konieczności zdejmowania czytnika ze ściany bądź rozbudowywania czytnika o dodatkowe elementy.
12. Czytnik kart zbliżeniowych powinien umożliwiać zmianę konfiguracji związanej z obsługą konkretnych typów kart, w celu możliwości podniesienia poziomu bezpieczeństwa w przyszłości lub w przypadku migracji ze starszego standardu na nowy.
13. Czytnik kart zbliżeniowych powinien umożliwiać aktualizację oprogramowania czytnika za pomocą narzędzi lub aplikacji bez konieczności zdejmowania czytnika ze ściany.
14. Czytnik kart zbliżeniowych powinien pozwalać na zmianę konfiguracji jego aplikacji z wykorzystaniem odpowiednich narzędzi bądź aplikacji. Funkcja powinna umożliwiać zmianę funkcjonalności poprzednio zainstalowanych czytników i dostosowaniu ich do zmian w późniejszym czasie.
15. Czytnik kart zbliżeniowych powinien umożliwiać zmianę konfiguracji audio-wizualnych:
    a. Buzzer generujący różne sygnały dźwiękowe charakterystyczne dla operacji: autoryzacji dostępu, braku autoryzacji dostępu, zasilenia oraz diagnostyki.
    b. Jasna, trójkolorowa (RGB), pozioma dioda LED powinna wyraźnie informować o zachowaniu i stanie czytnika.
16. Czytnik kart zbliżeniowych powinien mieć możliwość konfiguracji funkcji Velocity Checking (kontrola prędkości danych) w celu zabezpieczenia przed atakami elektronicznymi, opartymi na wielokrotnych nieprawidłowych próbach uwierzytelnienia.
17. Czytnik kart zbliżeniowych powinien w łatwy i przejrzysty sposób informować o karcie, która znajduje się polu zasięgu czytnika – zapobiegając wielokrotnym odczytom tej samej karty przed ponownym zbliżeniem do czytnika (notyfikacja anti-passback).
18. Czytnik kart zbliżeniowych powinien posiadać możliwość wygenerowania sygnału alarmowego poprzez zintegrowany czujnik mechaniczny (tamper) w momencie próby demontażu czytnika ze ściany.
19. Czytnik kart zbliżeniowych powinien mieć możliwość zapewnienia optymalnego zakresu odczytu poprzez funkcję automatycznego wykrywania powierzchni, która dostosowuje czytnik do środowiska montażu i tolerancji produkcyjnych w celu zwiększenia spójności odczytu.
20. Czytnik kart zbliżeniowych powinien umożliwiać bezpieczny montaż przy wykorzystaniu zabezpieczonych śrub montażowych (tamper resistant).
21. Czytnik kart zbliżeniowych powinien posiadać funkcję ograniczonego zużycia energii nawet o 50% przy wykorzystaniu trybu inteligentnego zarządzania energią (IPM – Intelligent Power Management).
22. Czytnik kart zbliżeniowych powinien być kompatybilny z globalnymi, międzynarodowymi dyrektywami dopuszczającymi: UL 294 / cUL, certyfikat FCC, IC, CE w tym RoHS II, RCM, SRRC , KCC, NCC, iDA, MIC, Bluetooth SIG certification (gdy wymagany jest dostęp mobilny).
23. Czytnik kart zbliżeniowych powinien być w pełni zgodny z dyrektywą RoHS (Restriction of Hazardous Substances) zakazującą użycia wybranych, niebezpiecznych materiałów w produkcji podzespołów elektronicznych. Substancjami zabronionymi przez RoHS są ołów (Pb), rtęć (Hg), kadm (Cd), sześciowartościowy chrom (CrVI), polibromowane bifenyle (PBB) i polibromowane etery difenylowe (PBDE).

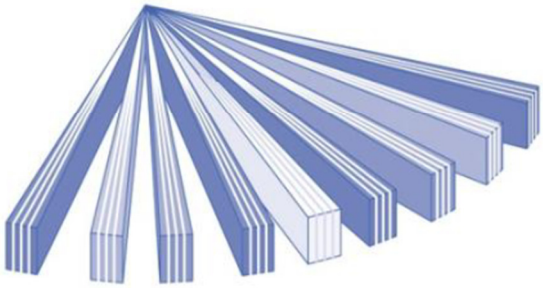
24. Czytnik kart zbliżeniowych powinien pracować w warunkach środowiskowych zgodnych z oceną Międzynarodowej Komisji Elektrotechnicznej i mieć klasę ochrony IP65, aby był odporny na wnikanie wody i pyłu, często występujące podczas montażu na zewnątrz

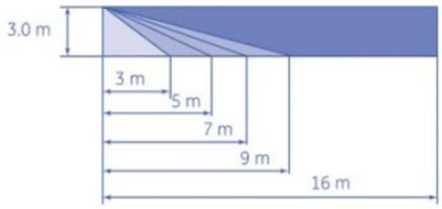
7. W przedmiarze teletechnicznym zawarto nazwy własne czujek ruchu: „Czujka ruchu Pir AM 16m VE-1016AM”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności czujek. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

VE1016AM
Dane techniczne, Ogólne
Technologia: PIR
Typ zastosowania: Montaż ścienny
Antymasking: Tak
Odporność na zwierzęta: Nie
Przetwarzanie sygnału Vector Verified Enhanced (VE2)
Zestaw antysabotażowy Na pokładzie
Wykrywanie:Maks. zasięg wykrywania 16 m
Pamięć alarmów: Tak
Wejścia / wyjścia
Linie zdalnego sterowania Test przejścia
Kolor Biały
Wysokość montażu od 1,8 do 3 m
Środowisko:Środowisko Wewnętrzne
Przepisy:EN50131: Klasa 3







Parametry

	VE1016	VE1016AM
Czujka	PIR	PIR + AM
Przetwarzanie sygnału	V2E	
Zakres	16 m	
Optyka	9 kurtyn lustrzanych o wysokiej gęstości	
Pamięć	Nie	Tak
Zasilanie	Napięcie stałe od 9 do 15 V (nominalnie 12 V)	
Dopuszczalne tętnienia (p-p)	2 V (przy napięciu stałym 12 V)	
Czas uruchamiania czujki	25 s	60 s
Nominalny pobór prądu	5,5 mA	10 mA
Pobór prądu w stanie alarmowym	1,1 mA	3,8 mA
Maksymalny pobór prądu	11 mA	24 mA

	VE1016	VE1016AM
Wysokość montażu	Od 1,8 do 3,0 m	Od 2,0 do 3,0 m
Zakres prędkości celu	Od 30 cm/s do 3 m/s	Od 20 cm/s do 3 m/s
Charakterystyka przekaźnika Alarm (NC) / Sabotaż	80 mA, 30 V (stałe)	80 mA, 30 V (stałe)
Zabezpieczenie przed oderwaniem	Opcjonalne	Zastosowane (Tak)
Charakterystyka przekaźnika AM	—	80 mA przy 30 V (maks.), prąd stały
Czas alarmu	3 s	
Temperatura działania:	od −10 do +55°C	
Wymiary (S x W x G)	108 × 60 × 46 mm	
Wilgotność względna	Maks. 95%	
Waga:	120 g	128 g
Klasa IP/IK	IP30 IK02	

8. W przedmiarze teletechnicznym zawarto nazwy własne czujek ruchu: „Czujka ruchu Pir AM 12m VE-1012AM”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności czujek. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

Dane techniczne, Ogólne
Technologia:PIR
Typ zastosowania: Montaż ścienny
Antymasking: Tak
Odporność na zwierzęta: Nie
Przetwarzanie sygnału: Vector Verified Enhanced (VE2)
Zestaw antysabotażowy: W zestawie
Wykrywanie:Maks. zasięg wykrywania 12 m
Pamięć alarmów: Tak
Wejścia / wyjścia
Konfiguracja przekaźnika Izolowany lub 4k7 EOL
Linie zdalnego sterowania: Test przejścia
Kolor Biały
Wysokość montażu od 1,8 do 3 m
Środowisko Wewnętrzne
Przepisy:EN50131: Klasa 3

Parametry

	VE1012	VE1012AM
Czujka	PIR	PIR + AM
Przetwarzanie sygnału	V2E	
Zakres	12 m	
Optyka	9 kurtyn lustrzanych o wysokiej gęstości	
Pamięć	Nie	Tak
Zasilanie	Napięcie stałe od 9 do 15 V (nominalnie 12 V)	
Dopuszczalne tętnienia (p-p)	2 V (przy napięciu stałym 12 V)	
Czas uruchamiania czujki	25 s	60 s
Nominalny pobór prądu	5,5 mA	12 mA
Pobór prądu w stanie alarmowym	1,1 mA	3,8 mA
Maksymalny pobór prądu	11 mA	24 mA
Wysokość montażu	Od 1,8 do 3,0 m	Od 2,0 do 3,0 m
Zakres prędkości celu	Od 30 cm/s do 3 m/s	Od 20 cm/s do 3 m/s
Charakterystyka przekaźnika Alarm (NC) / Sabotaż	80 mA, 30 V (stałe)	80 mA, 30 V (stałe)
Zabezpieczenie przed oderwaniem	Opcjonalne	Zastosowane (Tak)
Charakterystyka przekaźnika AM	—	80 mA przy 30 V (maks.), prąd stały
Czas alarmu	3 s	
Temperatura działania:	od −10 do +55°C	
Wymiary (S x W x G)	108 × 60 × 46 mm	
Wilgotność względna	Maks. 95%	
Waga:	120 g	128 g
Klasa IP/IK	IP30 IK02	

9. W przedmiarze teletechnicznym zawarto nazwy własne kamer: „Kamera M4318-PLVE”
Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

AXIS M4318-PLVE is a discreet, IK10 and IP66 outdoor-ready mini dome designed with 12 MP sensor and stereographic lens, that can deliver 360° or 180° panoramic views at up to 30 fps with no blind spots. Thanks to Sharpdome 360, this panoramic camera delivers greater sharpness at the edges of the image. Built on ARTPEC-8, it offers powerful artificial intelligence and deep learning analytics on the edge. including AXIS Object Analytics, it can accurately detect and classify moving objects for more effective monitoring. The camera can stream multiple, individually configurable H.264, H.265 and Motion JPEG streams, with support for digital PTZ. AXIS M4318-PLVE comes with build-in configurable IR, making it perfect for low light situations. Signed firmware and secure boot ensure firmware authenticity. Power over Ethernet.

Wymagania minimalne

Przetwornik obrazu
Skanowanie progresywne RGB CMOS 1/2,3"
Obiektyw
Długość ogniskowej: 1,2 mm, F2.2
Pole widzenia w poziomie: 182°
Pole widzenia w pionie: 182°
Stała przysłona, stała ostrość, korekcja podczerwieni
Dzień i noc
Automatyczny filtr odcinający promieniowanie IR
Minimalne oświetlenie
Kolor: 0,19 luksa przy 50 IRE F2.2
Obraz czarno-biały: 0,04 luksa przy 50 IRE F2.2
0 luksów przy włączonym oświetleniu w podczerwieni
Rozdzielczość
Ogólny: od 2992x2992 do 160x160
Panorama: od 3840x2160 do 192x72
Podwójna panorama: od 3584x2688 do 512x288
Widok poczwórny: od 3584x2688 do 384x288
Korytarz: od 2560x1920 do 256x144
Poklatkowość
Widok ogólny 360° do maksymalnej rozdzielczości bez WDR: 25/30 kl./s przy 50/60 Hz
Widok ogólny 360° i 4 widoki skorygowane do rozdzielczości maksymalnej z WDR: maks. 25/30 kl./s (50/60 Hz)
WDR
zaawansowana technologia obrazowania WDR: Maksymalnie 120 dB w zależności od sceny
Protokoły sieciowe
IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS, HTTP/2, TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, RTCP, DHCPv4/v6, SSH, LLDP, CDP, MQTT v3.1.1, Syslog, adres Link-Local (ZeroConf), IEEE 802.1X (EAP-TLS), IEEE 802.1AR
Interfejs programowania aplikacji (ang. Application Programming Interface, API)
Otwarty interfejs API umożliwiający integrację oprogramowania. Aplikacja zawiera macierzysty zestaw SDK i zestaw SDK dla widzenia komputerowego.

ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S i ONVIF® Profile T, specyfikacja pod adresem onvif.org
Obsługa protokołu Session Initiation Protocol (SIP) umożliwiającego integrację z systemami Voice over IP (VoIP), P2P lub zintegrowanych z SIP/PBX.
Wbudowana pomoc podczas montażu
Licznik pikseli, siatka poziomu,

Object Analytics
Klasy obiektów: ludzie, pojazdy (rodzaje: samochody, autobusy, ciężarówki, jednoślady)
Scenariusze: przekroczenie linii, obiekt w strefie, frekwencja w obszarze
Maksymalnie 10 scenariuszy
Metadane wizualizowane z trajektoriami, obwiedniami kodowanymi kolorami i tabelami
Wielokątne strefy detekcyjne/wykluczania
Alarm wyzwolony ruchem ONVIF
Metadane
Dane obiektu: Klasy: ludzie, twarze, pojazdy (rodzaje: samochody, autobusy, ciężarówki, jednoślady)
Atrybuty: kolor pojazdu, ufność, pozycja
Dane o zdarzeniu: Odwołanie do producenta, scenariusze, warunki wyzwalania
Zastosowania
W zestawie :analiza obiektów, wizyjna detekcja ruchu, aktywne zabezpieczenie antysabotażowe
Obsługiwane: Umożliwia instalowanie aplikacji innych firm

Łańcuch dostaw
Zgodność ze standardami TAA
EMC
EN 55035, EN 55032 klasa A, EN 50121-4, EN 61000-6-1, EN 61000-6-2, EN 61547

Zabezpieczenia
IEC/EN/UL 62368-1 wyd. 3, CAN/CSA C22.2 nr 62368-1 wyd. 3, IEC/EN 62471 (grupa ryzyka Zwolniona), UN ECE R118, IS 13252
Środowisko
IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, IEC/EN 62262 IK10, IEC/EN 60529 IP66, ISO 4892-2, NEMA 250 typ 4X, NEMA TS 2 (2.2.7-2.2.9), ISO 21207 (metoda B)
Sieć
NIST SP500-267
Bezpieczeństwo na obwodzie
Oprogramowanie: Podpisane oprogramowanie sprzętowe, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem, szyfrowanie kart SD AES-XTS-Plain64 256-bitowe
Sprzęt: platforma zabezpieczająca kryptograficznego modułu obliczeniowego
Zabezpieczony element (CC EAL 6 +), zabezpieczenia układu SoC (TEE), ID urządzenia producenta, bezpieczny magazyn kluczy, podpisane wideo, bezpieczne uruchamianie, szyfrowany system plików (AES-XTS-Plain64 256-bitowe)
Bezpieczeństwo w sieci
IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, filtrowanie adresów IP
Obudowa
IP66, NEMA 4X i IK10
Powlekana kopułka z poliwęglanu
Aluminium
Kolor: biały NCS S 1002-B
Akcesorium z opcją przemalowania obudowy
Zasilanie
Power over Ethernet (PoE) IEEE 802.3af/802.3at typ 1 klasa 3
Typowo 6,4 W, maks. 12,95 W
Oświetlenie w podczerwieni
Oświetlenie w podczerwieni z oszczędnymi diodami 850 nm o dużej żywotności
zasięg 15 m (49,2 ft), w zależności od sceny
Warunki robocze
od -40°C do 50°C (od -40°F do 122°F)
Temperatura rozruchu: -30°C
Wilgotność 10–100% RH (z kondensacją)

Języki
polski
Gwarancja
5-letnia gwarancja
Kontrola substancji
Nie zawiera PCW ani BFR/CFR zgodnie z normą JEDEC/ECA JS709
Zgodność z unijną dyrektywą RoHS 2011/65/UE/ i EN 63000:2018
Zgodność z rozporządzeniem REACH (KE) nr 1907/2006.
Odpowiedzialność za środowisko
Producent jest sygnatariuszem programu UN Global Compact. Więcej informacji pod adresem unglobalcompact.org.
Najważniejsze funkcje i technologie
Sztuczna inteligencja (AI)
Funkcja sztucznej inteligencji umożliwia detekcję i klasyfikowanie zarówno osób, jak i pojazdów. Menu konfiguracyjne urządzenia powinno umożliwiać detekcję tylko osób, tylko pojazdów lub zarówno osób, jak i pojazdów.
Funkcja sztucznej inteligencji do detekcji i klasyfikacji osób i pojazdów jest konfigurowana przez producenta i opiera się na zasadach głębokiego uczenia.
Urządzenie zapewniające funkcję sztucznej inteligencji powinno ją udostępniać bezpośrednio, bez konieczności stosowania dodatkowych aplikacji urządzenia.
Wbudowane cyberzabezpieczenia
Moduł kryptograficzny to bezpieczny kryptograficzny moduł obliczeniowy (zabezpieczony moduł lub zabezpieczony element), w którym identyfikator urządzenia producenta jest bezpiecznie oraz trwale zainstalowany i przechowywany.
Bezpieczne uruchamianie to proces składający się z nieprzerwanego łańcucha oprogramowania zweryfikowanego kryptograficznie, rozpoczynający się w pamięci niezmiennej (rozruchowej pamięci ROM). Dzięki podpisanemu oprogramowaniu sprzętowemu bezpieczny rozruch gwarantuje uruchomienie urządzenia wyłącznie z autoryzowanym oprogramowaniem sprzętowym. Bezpieczne uruchamianie gwarantuje, że Urządzenie producenta jest całkowicie pozbawione możliwego złośliwego oprogramowania po przywróceniu ustawień fabrycznych.
Podpisane oprogramowanie sprzętowe jest wdrażane przez dostawcę oprogramowania podpisującego obraz oprogramowania sprzętowego za pomocą klucza prywatnego, który nie jest ujawniany. Po dołączeniu tego podpisu urządzenie będzie sprawdzać oprogramowanie sprzętowe przed jego zaakceptowaniem i zainstalowaniem. Jeżeli urządzenie wykryje naruszenie integralności oprogramowania sprzętowego, odrzuci jego aktualizację. Podpisane oprogramowanie sprzętowe jest oparte na zweryfikowanej w branży metodzie szyfrowania RSA.
TPM to akronim wyrażenia Trusted Platform Module. Moduł TPM to składnik udostępniający zestaw funkcji kryptograficznych umożliwiający ochronę informacji przed nieupoważnionym dostępem. Klucz prywatny jest przechowywany w module TPM i nigdy go nie opuszcza. Wszystkie operacje kryptograficzne wymagające użycia klucza prywatnego są wysyłane do modułu TPM w celu przetworzenia. Dzięki temu tajny element certyfikatu pozostaje bezpieczny nawet w przypadku naruszenia bezpieczeństwa.
Zaawansowana technologia rejestracji obrazu przy słabym oświetleniu
Zaawansowana technologia słabego oświetlenia musi zapewniać światłoczułość kamery sieciowej, tak aby kamera pozostawała w trybie dziennym i w dalszym ciągu dostarcza obrazy w kolorze. W ramach dozoru kolor może być krytycznym czynnikiem umożliwiającym identyfikację osoby, obiektu lub pojazdu.
Kamera w zaawansowanej technologii słabego oświetlenia musi być w stanie korzystać z krótszych czasów ekspozycji, aby utrzymać rozmycie i szum na minimalnym poziomie.
Zaawansowana technologia słabego oświetlenia powinna łączyć obiektywy wysokiej jakości i przetworniki obrazu zoptymalizowane pod kątem dozoru przy użyciu cyfrowych algorytmów obrazów działających w układzie system-on-chip.
Kamera musi mieć wbudowane diody LED do oświetlenia w podczerwieni.
Kamera pracuje w technologii, która dynamicznie dostosowuje zasięg i natężenia oświetlenia w podczerwieni do zakresu zoomu kamery.
Technologia z wykorzystanie podczerwieni to mechanizm, który automatycznie i dynamicznie kontroluje natężenie promieniowania podczerwonego, zapewniając, że całe pole widzenia jest oświetlone proporcjonalnie, co zapewnia wysoką jakość i jednorodnie oświetlenie obrazu z kamery przy jednoczesnym ograniczaniu szumu.

Diody LED podczerwieni powinny emitować światło o długości fali 850 nm.
Kamera obsługująca technologię podczerwieni musi być zasilana przez PoE.

Technologia kompresji wideo

Technologia kompresji wideo musi umożliwić wykorzystanie wyższych rozdzielczości i zwiększyć użyteczność w kontekście postępowań dochodzeniowych, ograniczając jednocześnie koszty przechowywania zasobów.
Technologia kompresji wideo musi bazować na wdrożeniu wideoenkodera zgodnego ze standardami, które obniża zapotrzebowanie na przepustowość i zasoby pamięci średnio o 50% lub więcej w porównaniu z metodami standardowymi.
Istotne szczegóły i ruchy powinny zostać zarejestrowane w wysokiej jakości, a pozostałe dane dotyczące obrazu powinny być przefiltrowane w bardziej restrykcyjny sposób, aby zapewnić optymalne wykorzystanie dostępnej przepustowości.
Technologia bazuje na zestawie algorytmów służących do analizy strumienia wideo w czasie rzeczywistym:

- Dynamic ROI (dynamiczny obszar zainteresowania) — identyfikuje obszary zainteresowania w zależności od obiektów, osób lub ruchu w scenie i stosuje prawidłowy poziom kompresji z perspektywy rejestracji materiałów dowodowych.
- Dynamic GOP (dynamiczna grupa obrazów) — kamera wysyła rzadziej kluczowe ramki wymagające dużej przepustowości w przypadku braku ruchu w scenie.
- Dynamiczna FPS (dynamiczna liczba klatek na sekundę) — zmniejsza przepływność przy niewielkim natężeniu ruchu w scenie lub przy jego braku. Kamera umożliwia przechwytywanie i analizę obrazu wideo przy pełnej podklatkowości, ale niepotrzebne ramki nie są kodowane.

Technologia kompresji wideo powinna zapewniać wsparcie w zakresie funkcji kamery PTZ, w rozdzielczości 4K Ultra HD, kamer wielomegapikselowych i kamer panoramicznych 360-stopniowych, dynamicznego ograniczenia FPS dynamicznego pomijania ramek FPS.
Technologia kompresji wideo powinna obsługiwać format H.264 w przypadku wszystkich produktów, a także dodatkową obsługę formatu H.265 w przypadku wybranych produktów, umożliwiając elastyczną migrację w dłuższym okresie.

10. W przedmiarze teletechnicznym zawarto nazwy własne kamer: „Kamera zewnętrzna P1377-LE” Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

Wymagania minimalne

Przetwornik obrazu
1/2,7" skanowanie progresywne RGB CMOS
Obiektyw
Obiektyw z korekcją podczerwieni, mocowaniem CS i funkcją P-Iris
Zmiennoogniskowy, 2,8–8 mm, F1,2
Pole widzenia w poziomie: 90°–38°
Pole widzenia w pionie: 67°–28°
Dzień i noc
Automatyczny zdejmowalny filtr odcinający podczerwień
Minimalne oświetlenie
5 MP 25/30 kl./s z zaawansowaną technologią obrazowania WDR i technologią rejestracji obrazu w słabym oświetleniu:
Obraz kolorowy: 0,13 luksa przy 50 IRE F1,2
Obraz czarno-biały: 0,03 luksa przy 50 IRE F1,2
0 luksów przy włączonym oświetleniu w podczerwieni
Prędkość migawki
WDR: Od 1/33 500 s do 1/5 s
Bez WDR: Od 1/50 000 s do 1/5 s
Poklatkowość
Tryb rejestracji 5 MP: 25/30 kl./s (50/60 Hz)

Tryb rejestracji 4 MP: 25/30 kl./s (50/60 Hz)
Tryb rejestracji HDTV 720p: 180 kl./s

Protokoły sieciowe

IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS, HTTP/2, TLS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP™, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTP, SFTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, RTCP, ICMP, DHCPv4/v6, ARP, SSH, LLDP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), adres Link-Local (ZeroConf)

Interfejs programowania aplikacji (ang. Application Programming Interface, API)

Otwarty interfejs programowania aplikacji (API) umożliwiający integrację oprogramowania.
ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S i ONVIF® Profile T, specyfikacja pod adresem onvif.org

Wbudowana pomoc podczas montażu

Asystent ostrości, licznik pikseli, zdalny back focus, automatyczny obrót, zdalne ustawianie ostrości i zoomu z opcjonalnym obiektywem i-CS.

Object Analytics

Klasy obiektów: ludzie, pojazdy
Scenariusze: przekroczenie linii, obiekt w strefie, zliczanie obiektów przekraczających linię, czas przebywania na obszarze
Maksymalnie 10 scenariuszy
Metadane wizualizowane z trajektoriami, obwiedniami kodowanymi kolorami i tabelami
Wielokątne strefy detekcyjne/wykluczania
Konfiguracja perspektywy
Alarm wyzwolony ruchem ONVIF

Metadane

Dane obiektu: Klasy: ludzie, twarze, pojazdy (rodzaje: samochody, autobusy, ciężarówki, jednoślady), tablice rejestracyjne
Ufność, położenie
Dane o zdarzeniu: Odwołanie do producenta, scenariusze, warunki wyzwalania

Zastosowania

W zestawie
analiza obiektów, wizyjna detekcja ruchu, wykrywanie ruchu, ochrona ogrodzenia, zgłaszanie podejrzanych zachowań, aktywny alarm przeciwsabotażowy, detekcja dźwięku
Obsługiwane
Umożliwia instalowanie aplikacji innych firm

Bezpieczeństwo na obwodzie

Oprogramowanie: Podpisane oprogramowanie sprzętowe, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem, szyfrowanie kart SD AES-XTS-Plain64 256-bitowe
Sprzęt: Bezpieczne uruchamianie

Bezpieczeństwo w sieci

IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa hosta

Obudowa

Obudowa polimerowa na aluminiowej podstawie, z alarmem antysabotażowym, klasy ochrony IP66, IP67 i NEMA 4X, klasa odporności na uderzenia IK10
Osłona chroniąca przed wpływem warunków atmosferycznych z czarną powłoką przeciwodblaskową
Kolor: biały (NCS S 1002-B)

Zrównoważony rozwój

Wolny od związków PCW

Zasilanie

12–28 V DC, maks. 25,5 W (z podczerwienią i ogrzewaczem z przodu), typowo 10,5 W
Power over Ethernet (PoE) IEEE 802.3af/802.3at Typ 1 Klasa 4, maks. 25,5 W (z podczerwienią i ogrzewaczem z przodu), typowo 11,1 W

Oświetlenie w podczerwieni

Oświetlenie w podczerwieni z oszczędnymi diodami 850 nm o dużej żywotności
Zasięg 50 m (164 ft) lub więcej, w zależności od sceny

Warunki robocze
Od –40°C do 60°C (od –40°F do 140°F)
Maksymalna temperatura według NEMA TS 2 (2.2.7): 74°C (165°F)
Wilgotność 10–100% RH (z kondensacją)
Siła wiatru (stała): 55 m/s (123 mph)
Certyfikaty
Kompatybilność elektromagnetyczna
EN 55032 klasa A, EN 50121-4, IEC 62236-4, EN 61000-3-2, EN 61000-3-3, EN 55024, EN 61000-6-1, EN 61000-6-2, FCC część 15 podczęść B klasa A, ICES-003 klasa A, VCCI klasa A, RCM AS/NZS CISPR 32 klasa A, KCC KN32 klasa A, KN35
Zabezpieczenia
IEC/EN/UL 62368-1, CAN/CSA C22.2 nr 62368-1, IEC/EN/UL 60950-22, CAN/CSA-C22.2 nr 60950-22, IEC 62471, IS 13252
Środowisko
IEC/EN 60529 IP66/IP67, NEMA 250 Type 4X, NEMA TS 2 (2.2.7-2.2.9), IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, IEC/EN 62262 IK10
Sieć
NIST SP500–267
Gwarancja
5-letnia gwarancja

11. W przedmiarze teletechnicznym zawarto nazwy własne kamer: „Kamera wewnętrzna P3265-LV” Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

<u>Wymagania minimalne</u>
Przetwornik obrazu
1/2,8” skanowanie progresywne RGB CMOS
Obiektyw
Zmiennoogniskowy, 3,4–8,9 mm, F1.8
Pole widzenia w poziomie: 100°-36°
Pole widzenia w pionie: 53°-20°
Minimalna odległość ostrości: 50 cm (20 cali)
Korekcja podczerwieni, zoom w obiektywie zmiennoogniskowym, sterowanie przysłoną P-Iris
Dzień i noc
Automatycznie zdejmowany filtr odcinający podczerwień
Minimalne oświetlenie
Zaawansowana technologia obrazowania WDR oraz zaawansowana technologia rejestracji obrazów w słabym oświetleniu:
Kolor: 0,1 luksa przy 50 IRE F1,8
Obraz czarno-biały: 0 luksa przy 50 IRE F1,8
Prędkość migawki
Od 1/66 500 s do 2 s
Poklatkowość
Z WDR 25/30 kl./s przy częstotliwości zasilania 50/60 Hz
Bez WDR: 50/60 kl./s przy częstotliwości zasilania 50/60 Hz.
Protokoły sieciowe
IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS, HTTP/2, TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTCP, RTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, DHCPv4/v6, ARP, SSH, SIP, LLDP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), adres Link-Local (ZeroConf)
Interfejs programowania aplikacji (ang. Application Programming Interface, API)
Otwarty interfejs programowania aplikacji (API) umożliwiający integrację oprogramowania.

ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S i ONVIF® Profile T, specyfikacja pod adresem onvif.org
Obsługa protokołu Session Initiation Protocol (SIP) umożliwiającego integrację z systemami Voice over IP (VoIP), P2P lub zintegrowanych z SIP/PBX.

Wbudowana pomoc podczas montażu

Zdalny zoom i ostrość, prostowanie obrazu, Licznik pikseli, siatka poziomu

Object Analytics

Klasy obiektów: ludzie, pojazdy (rodzaje: samochody, autobusy, ciężarówki, jednoślady)
Scenariusze: przekroczenie linii, obiekt w strefie, zliczanie obiektów przekraczających linię, obecność w obszarze
Maksymalnie 10 scenariuszy
Metadane wizualizowane z trajektoriami, obwiedniami kodowanymi kolorami i tabelami
Wielokątne strefy detekcyjne/wykluczania
Konfiguracja perspektywy
Alarm wyzwolony ruchem ONVIF

Metadane

Dane obiektu: Klasy: ludzie, twarze, pojazdy (rodzaje: samochody osobowe, autobusy, samochody ciężarowe, motocykle), tablice rejestracyjne
Atrybuty: kolor pojazdu, kolor odzieży górnej/dolnej, ufność, pozycja
Dane o zdarzeniu: Odwołanie do producenta, scenariusze, warunki wyzwalania

Zastosowania

W zestawie
analiza obiektów
wizyjna detekcja ruchu, aktywne zabezpieczenie antysabotażowe, detekcja dźwięku
Umożliwia instalowanie aplikacji innych firm

EMC

EN 55035, EN 55032 klasa A, EN 50121-4, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2

Zabezpieczenia

CAN/CSA C22.2 nr 62368-1, IEC/EN/UL 62368-1, IEC/EN 62471, IS 13252

Środowisko

IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78
IEC/EN 60529 IP52, IEC/EN 62262 IK10

Sieć

NIST SP500-267

Cyberbezpieczeństwo

ETSI EN 303 645

Bezpieczeństwo na obwodzie

Oprogramowanie: Podpisane oprogramowanie sprzętowe, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem, szyfrowanie kart SD AES-XTS-Plain64 256-bitowe
Sprzęt: platforma zabezpieczająca kryptograficznego modułu obliczeniowego
Zabezpieczony element (CC EAL 6 +), zabezpieczenia układu SoC (TEE), ID urządzenia producenta, bezpieczny magazyn kluczy, podpisane wideo, bezpieczne uruchamianie, szyfrowany system plików (AES-XTS-Plain64 256-bitowe)

Bezpieczeństwo w sieci

IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa hosta

Obudowa

Stopień ochrony IP52 i IK10
Powlekana kopułka z poliwęglanu
Obudowa poliwęglanowa
Kolor: biały (NCS S 1002-B)

Zrównoważony rozwój

Nie zawiera PCW, bez BFR/CFR, 30.2% tworzyw sztucznych z recyklingu

Zasilanie
Power over Ethernet (PoE) IEEE 802.3af/802.3at typ 1 klasa 3
Typowo 4,8 W, maks. 8,9 W
Oświetlenie w podczerwieni
Oświetlenie w podczerwieni z oszczędnymi diodami 850 nm o dużej żywotności
Zasięg 40 m (130 ft) lub więcej, w zależności od sceny
Warunki robocze
od 0°C do 50°C (od 32°F do 122°F)
Wilgotność 10–85% RH (bez kondensacji)

Gwarancja
5-letnia gwarancja

12. W przedmiarze teletechnicznym zawarto nazwy własne kamer: „Kamera wewnętrzna P3225-LVE”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

Wymagania minimalne
Przetwornik obrazu
1/2,8” skanowanie progresywne RGB CMOS
Obiektyw
9 mm:
Zmiennoogniskowy, 3,4–8,9 mm, F1.8
Pole widzenia w poziomie: 100°-36°
Pole widzenia w pionie: 53°-20°
Minimalna odległość ostrości: 50 cm (20 cali)
Korekcja podczerwieni, zoom w obiektywie zmiennoogniskowym, sterowanie przysłoną P-Iris
Dzień i noc
Automatycznie zdejmowany filtr odcinający podczerwień
Minimalne oświetlenie
Zaawansowana technologia obrazowania WDR oraz zaawansowana technologia rejestracji obrazów w słabym oświetleniu:
Kolor: 0,1 luksa przy 50 IRE, F1.8/F1.6 (9 mm/22 mm)
Obraz czarno-biały: 0 luksa przy 50 IRE, F1.8/F1.6 (9 mm/22 mm)
Prędkość migawki
Od 1/66 500 s do 2 s
Poklatkowość
Z WDR 25/30 kl./s przy częstotliwości zasilania 50/60 Hz
Bez WDR: 50/60 kl./s przy częstotliwości zasilania 50/60 Hz.
Protokoły sieciowe
IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS, HTTP/2, TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTCP, RTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, DHCPv4/v6, ARP, SSH, SIP, LLDP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), adres Link-Local (ZeroConf)
Interfejs programowania aplikacji (ang. Application Programming Interface, API)
Otwarty interfejs programowania aplikacji (API) umożliwiający integrację oprogramowania. Medatane i dane techniczne są dostępne pod adresem /developer-community. Platforma ACAP zawiera macierzysty zestaw SDK i zestaw SDK dla widzenia komputerowego.

ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S i ONVIF® Profile T, specyfikacja pod adresem onvif.org
Obsługa protokołu Session Initiation Protocol (SIP) umożliwiającego integrację z systemami Voice over IP (VoIP), P2P lub zintegrowanych z SIP/PBX.

Wbudowana pomoc podczas montażu
Zdalny zoom i ostrość, prostowanie obrazu, Licznik pikseli, siatka poziomu
Object Analytics
Klasy obiektów: ludzie, pojazdy (rodzaje: samochody, autobusy, ciężarówki, jednoślady)
Scenariusze: przekroczenie linii, obiekt w strefie, zliczanie obiektów przekraczających linię, obecność w obszarze, czas przebywania na obszarze
Maksymalnie 10 scenariuszy
Metadane wizualizowane z trajektoriami, obwiedniami kodowanymi kolorami i tabelami
Wielokątne strefy detekcyjne/wykluczania
Konfiguracja perspektywy
Alarm wyzwolony ruchem ONVIF
Metadane
Dane obiektu: Klasy: ludzie, twarze, pojazdy (rodzaje: samochody osobowe, autobusy, samochody ciężarowe, motocykle), tablice rejestracyjne
Atrybuty: kolor pojazdu, kolor odzieży górnej/dolnej, ufność, pozycja
Dane o zdarzeniu: Odwołanie do producenta, scenariusze, warunki wyzwalania
Zastosowania
W zestawie
analiza obiektów
wizyjna detekcja ruchu, aktywne zabezpieczenie antysabotażowe, detekcja dźwięku
Umożliwia instalowanie aplikacji innych firm
EMC
EN 55035, EN 55032 klasa A, EN 50121-4, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2
Zabezpieczenia
CAN/CSA C22.2 nr 60950-22, CAN/CSA C22.2 nr 62368-1, IEC/EN/UL 62368-1, IEC/EN/UL 60950-22, IEC/EN 62471, IS 13252
Środowisko
IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78
IEC/EN 60529 IP66, IEC/EN 62262 IK10, NEMA 250 typ 4X,NEMA TS 2 (2.2.7-2.2.9)
Sieć
NIST SP500-267
Cyberbezpieczeństwo
ETSI EN 303 645
Bezpieczeństwo na obwodzie
Oprogramowanie: Podpisane oprogramowanie sprzętowe, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem, szyfrowanie kart SD AES-XTS-Plain64 256-bitowe
Sprzęt: platforma zabezpieczająca kryptograficznego modułu obliczeniowego
Zabezpieczony element (CC EAL 6 +), zabezpieczenia układu SoC (TEE), ID urządzenia producenta, bezpieczny magazyn kluczy, podpisane wideo, bezpieczne uruchamianie, szyfrowany system plików (AES-XTS-Plain64 256-bitowe)
Bezpieczeństwo w sieci
IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa hosta
Obudowa
IP66, NEMA 4X i IK10
Powlekana kopułka z poliwęglanu
Obudowa poliwęglanowa i osłona chroniąca przed wpływem warunków atmosferycznych
Kolor: biały (NCS S 1002-B)
Zrównoważony rozwój
Nie zawiera PCW, wyprodukowana w 4,1% z tworzyw sztucznych pochodzących z recyklingu
Zasilanie
Power over Ethernet (PoE) IEEE 802.3af/802.3at typ 1 klasa 3
Typowo 4,8 W, maks. 10,7 W
Oświetlenie w podczerwieni
Oświetlenie w podczerwieni z oszczędnymi diodami 850 nm o dużej żywotności

Zasięg 40 m (130 ft) lub większy, w zależności od sceny

Warunki robocze

od -40°C do 50°C (od -40°F do 122°F)
Maksymalna temperatura według NEMA TS 2 (2.2.7): 74°C (165°F)
Temperatura rozruchu: Od -30°C do 50°C (-22°F do 122°F)
Wilgotność 10–100% RH (z kondensacją)

Gwarancja

5-letnia gwarancja

13. W przedmiarze teletechnicznym zawarto nazwy własne obudów kamer: „Obudowa do kamery TP3820-E CASING BLACK 4P”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności obudów kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

Akcesoria producenta kamer umożliwiające zmianę kolorów obudów kamer na kolor czarny.

14. W przedmiarze teletechnicznym zawarto nazwy własne kamer: „Kamera wewnętrzna P3265-V”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

Wymagania minimalne

Przetwornik obrazu

1/2,8” skanowanie progresywne RGB CMOS

Obiektyw

Zmiennoogniskowy, 3,4–8,9 mm, F1.8
Pole widzenia w poziomie: 100°-36°
Pole widzenia w pionie: 53°-20°
Minimalna odległość ostrości: 50 cm (20 cali)
Korekcja podczerwieni, zoom w obiektywie zmiennoogniskowym, sterowanie przysłoną P-Iris

Dzień i noc

Automatycznie zdejmowany filtr odcinający podczerwień

Minimalne oświetlenie

Zaawansowana technologia obrazowania WDR oraz zaawansowana technologia rejestracji obrazów w słabym oświetleniu:
Kolor: 0,1 luksa przy 50 IRE F1,8
Obraz czarno-biały: 0 luksa przy 50 IRE F1,8

Prędkość migawki

Od 1/66 500 s do 2 s

Poklatkowość

Z WDR 25/30 kl./s przy częstotliwości zasilania 50/60 Hz
Bez WDR: 50/60 kl./s przy częstotliwości zasilania 50/60 Hz.

Protokoły sieciowe

IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS, HTTP/2, TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTCP, RTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, DHCPv4/v6, ARP, SSH, SIP, LLDP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), adres Link-Local (ZeroConf)

Interfejs programowania aplikacji (ang. Application Programming Interface, API)

Otwarty interfejs programowania aplikacji (API) umożliwiający integrację oprogramowania.

ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S i ONVIF® Profile T, specyfikacja pod adresem onvif.org
Obsługa protokołu Session Initiation Protocol (SIP) umożliwiającego integrację z systemami Voice over IP

(VoIP), P2P lub zintegrowanych z SIP/PBX.

Wbudowana pomoc podczas montażu

Zdalny zoom i ostrość, prostowanie obrazu, Licznik pikseli, siatka poziomu

Object Analytics

Klasy obiektów: ludzie, pojazdy (rodzaje: samochody, autobusy, ciężarówki, jednoślady)
Scenariusze: przekroczenie linii, obiekt w strefie, zliczanie obiektów przekraczających linię, obecność w obszarze
Maksymalnie 10 scenariuszy
Metadane wizualizowane z trajektoriami, obwiedniami kodowanymi kolorami i tabelami
Wielokątne strefy detekcyjne/wykluczania
Konfiguracja perspektywy
Alarm wyzwolony ruchem ONVIF

Metadane

Dane obiektu: Klasy: ludzie, twarze, pojazdy (rodzaje: samochody osobowe, autobusy, samochody ciężarowe, motocykle), tablice rejestracyjne
Atrybuty: kolor pojazdu, kolor odzieży górnej/dolnej, ufność, pozycja
Dane o zdarzeniu: Odwołanie do producenta, scenariusze, warunki wyzwalania

Zastosowania

W zestawie
analiza obiektów
wizyjna detekcja ruchu, aktywne zabezpieczenie antysabotażowe, detekcja dźwięku
Umożliwia instalowanie aplikacji innych firm

EMC

EN 55035, EN 55032 klasa A, EN 50121-4, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2

Zabezpieczenia

CAN/CSA C22.2 nr 62368-1, IEC/EN/UL 62368-1, IEC/EN 62471, IS 13252

Środowisko

IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78
IEC/EN 60529 IP52, IEC/EN 62262 IK10

Sieć

NIST SP500-267

Cyberbezpieczeństwo

ETSI EN 303 645

Bezpieczeństwo na obwodzie

Oprogramowanie: Podpisane oprogramowanie sprzętowe, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem, szyfrowanie kart SD AES-XTS-Plain64 256-bitowe
Sprzęt: platforma zabezpieczająca kryptograficznego modułu obliczeniowego
Zabezpieczony element (CC EAL 6 +), zabezpieczenia układu SoC (TEE), ID urządzenia producenta, bezpieczny magazyn kluczy, podpisane wideo, bezpieczne uruchamianie, szyfrowany system plików (AES-XTS-Plain64 256-bitowe)

Bezpieczeństwo w sieci

IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa hosta

Obudowa

Stopień ochrony IP52 i IK10
Powlekana kopułka z poliwęglanu
Obudowa poliwęglanowa
Kolor: biały (NCS S 1002-B)

Zrównoważony rozwój

Nie zawiera PCW, bez BFR/CFR, 30.2% tworzyw sztucznych z recyklingu

Zasilanie

Power over Ethernet (PoE) IEEE 802.3af/802.3at typ 1 klasa 3
Typowo 4,8 W, maks. 8,9 W

Warunki robocze

od 0°C do 50°C (od 32°F do 122°F)

Wilgotność 10–85% RH (bez kondensacji)

Gwarancja
5-letnia gwarancja

15. W przedmiarze teletechnicznym zawarto nazwy własne kamer: „Kamera wewnętrzna P3268-LV” Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

Wymagania minimalne

Przetwornik obrazu
1/1,8” skanowanie progresywne RGB CMOS
Obiektyw
Zmiennoogniskowy, 4,3–8,6 mm, F1.5
Pole widzenia w poziomie: 100°–53°
Pole widzenia w pionie: 54°–30°
Minimalna odległość ostrości: 50 cm (20 cali)
Korekcja podczerwieni, zoom w obiektywie zmiennoogniskowym, sterowanie przysłoną P-Iris
Dzień i noc
Automatycznie zdejmowany filtr odcinający podczerwień
Minimalne oświetlenie
Zaawansowana technologia obrazowania WDR oraz rejestracji obrazów w słabym oświetleniu:
Kolor: 0,14 luksa przy 50 IRE F1.5
Obraz czarno-biały: 0 luksa przy 50 IRE F1.5
Prędkość migawki
Od 1/8500 s do 1/5 s
Poklatkowość
25/30 kl./s przy częstotliwości zasilania 50/60 Hz
Protokoły sieciowe
IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS, HTTP/2, TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTCP, RTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, DHCPv4/v6, ARP, SSH, SIP, LLDP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), adres Link-Local (ZeroConf)
Interfejs programowania aplikacji (ang. Application Programming Interface, API)
Otwarty interfejs programowania aplikacji (API) umożliwiający integrację oprogramowania.

ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S i ONVIF® Profile T, specyfikacja pod adresem onvif.org
Obsługa protokołu Session Initiation Protocol (SIP) umożliwiającego integrację z systemami Voice over IP (VoIP), P2P lub zintegrowanych z SIP/PBX.
Wbudowana pomoc podczas montażu
Zdalny zoom i ostrość, prostowanie obrazu, Licznik pikseli, siatka poziomu
Object Analytics
Klasy obiektów: ludzie, pojazdy (rodzaje: samochody, autobusy, ciężarówki, jednoślady)
Scenariusze: przekroczenie linii, obiekt w strefie, zliczanie obiektów przekraczających linię, obecność w obszarze, czas przebywania na obszarze
Maksymalnie 10 scenariuszy
Metadane wizualizowane z obwiedniami kodowanymi kolorami
Wielokątne strefy detekcyjne/wykluczania
Konfiguracja perspektywy
Alarm wyzwolony ruchem ONVIF
Metadane
Dane obiektu: Klasy: ludzie, twarze, pojazdy (rodzaje: samochody osobowe, autobusy, samochody ciężarowe, motocykle), tablice rejestracyjne
Atrybuty: kolor pojazdu, kolor odzieży górnej/dolnej, ufność, pozycja

Dane o zdarzeniu: Odwołanie do producenta, scenariusze, warunki wyzwalania
Zastosowania
W zestawie: analiza obiektów
wizyjna detekcja ruchu, aktywne zabezpieczenie antysabotażowe, detekcja dźwięku
Umożliwia instalowanie aplikacji innych firm
EMC
EN 55035, EN 55032 klasa A, EN 50121-4, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2
Środowisko
IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, IEC/EN 60529 IP52, IEC/EN 62262 IK10
Sieć
NIST SP500-267
Cyberbezpieczeństwo
ETSI EN 303 645
Bezpieczeństwo na obwodzie
Oprogramowanie: Podpisane oprogramowanie sprzętowe, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem, szyfrowanie kart SD AES-XTS-Plain64 256-bitowe
Sprzęt: platforma zabezpieczająca kryptograficznego modułu obliczeniowego
Zabezpieczony element (CC EAL 6 +), zabezpieczenia układu SoC (TEE), ID urządzenia producenta, bezpieczny magazyn kluczy, podpisane wideo, bezpieczne uruchamianie, szyfrowany system plików (AES-XTS-Plain64 256-bitowe)
Bezpieczeństwo w sieci
IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa hosta
Obudowa
Stopień ochrony IP52 i IK10
Powlekana kopułka z poliwęglanu
Obudowa poliwęglanowa
Kolor: biały (NCS S 1002-B)

Zrównoważony rozwój
Wolny od związków PCW, BFR/CFR
Zasilanie
Power over Ethernet (PoE) IEEE 802.3af/802.3at typ 1 klasa 3
Typowo 5,5 W, maks. 10.0 W
Oświetlenie w podczerwieni
Oświetlenie w podczerwieni z oszczędnymi diodami 850 nm o dużej żywotności
Zasięg 40 m (130 ft) lub więcej, w zależności od sceny
Warunki robocze
od 0°C do 50°C (od 32°F do 122°F)
Wilgotność 10–85% RH (bez kondensacji)
Gwarancja
5-letnia gwarancja

16. W przedmiarze teletechnicznym zawarto nazwy własne kamer: „Kamera wewnętrzna Q3536-LVE 9MM DOME CAMERA”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

<u>Wymagania minimalne</u>

Przetwornik obrazu
1/1,8” skanowanie progresywne RGB CMOS
Obiektyw
Zmiennoogniskowy 4,3–8,6 mm, F1.5–2,4
Pole widzenia w poziomie: 103°–53°
Pole widzenia w pionie: 56°–30°
Obiektyw zmiennoogniskowy, funkcja zdalnego zoomu i ustawiania ostrości, sterowanie przysłoną P-Iris, korekcja podczerwieni
Dzień i noc
Automatycznie zdejmowany filtr odcinający podczerwień
Minimalne oświetlenie
Kolor: 0,06 luksa przy 50 IRE F1.5
Obraz czarno-biały: 0 luksa przy 50 IRE F1.5
Prędkość migawki
Od 1/91 000 s do 1 s
Poklatkowość
Z WDR 25/30 kl./s przy częstotliwości zasilania 50/60 Hz
Bez WDR: 50/60 kl./s przy częstotliwości zasilania 50/60 Hz.
Protokoły sieciowe
IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS, HTTP/2, TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTCP, RTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, DHCPv4/v6, ARP, SSH, SIP, LLDP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), adres Link-Local (ZeroConf)
Interfejs programowania aplikacji (ang. Application Programming Interface, API)
ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S i ONVIF® Profile T, specyfikacja pod adresem onvif.org
Wbudowana pomoc podczas montażu
Asystent poziomowania, prostowanie obrazu, siatka obrazu, licznik pikseli
Object Analytics
Klasy obiektów: ludzie, pojazdy (rodzaje: samochody, autobusy, ciężarówki, jednoślady)
Scenariusze: przekroczenie linii, obiekt w strefie, zliczanie obiektów przekraczających linię, obecność w obszarze, czas przebywania na obszarze
Maksymalnie 10 scenariuszy
Metadane wizualizowane z trajektoriami, obwiedniami kodowanymi kolorami i tabelami
Wielokątne strefy detekcyjne/wykluczania
Konfiguracja perspektywy
Alarm wyzwolony ruchem ONVIF
Metadane
Dane obiektu: Klasy: ludzie, twarze, pojazdy (rodzaje: samochody osobowe, autobusy, samochody ciężarowe, motocykle), tablice rejestracyjne
Atrybuty: kolor pojazdu, kolor odzieży górnej/dolnej, ufność, pozycja
Dane o zdarzeniu: Odwołanie do producenta, scenariusze, warunki wyzwalania
~~Zastosowania~~
W zestawie
analiza obiektów
Video Motion Detection (wizyjna detekcja ruchu)
Obsługiwane
Umożliwia instalowanie aplikacji innych firm
EMC
CISPR 35, EN 50121-4, EN 55032 klasa A, EN 55035, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2
Zabezpieczenia
CAN/CSA-C22.2 No. 60950-22, CAN/CSA C22.2 No. 62368-1, IEC/EN/UL 62368-1, IEC/EN/UL 60950-22, IEC 62471, IS 13252
Środowisko
IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, IEC/EN 60529 IP66, ISO 20653 IP6K9K, IEC/EN 62262 IK10+ (50J), NEMA 250 typ 4X, NEMA TS 2 (2.2.7-2.2.9)

Sieć
NIST SP500-267
Cyberbezpieczeństwo
ETSI EN 303 645
Bezpieczeństwo na obwodzie
Oprogramowanie: Podpisane oprogramowanie sprzętowe, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem, szyfrowanie kart SD AES-XTS-Plain64 256-bitowe
Sprzęt: platforma zabezpieczająca kryptograficznego modułu obliczeniowego
Moduł TPM 2.0 (CC EAL4 +, FIPS 140-2 poziomu 2), zabezpieczony element (CC EAL 6 +), zabezpieczenia układu SoC (TEE), ID urządzenia producenta, bezpieczny magazyn kluczy, podpisane wideo, bezpieczne uruchamianie, szyfrowany system plików (AES-XTS-Plain64 256-bitowe)
Bezpieczeństwo w sieci
IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa hosta
Obudowa
Klasa ochrony IP66, IP6K9K, NEMA 4X i IK10+
Powlekana kopułka z poliwęglanu
Obudowa z aluminium i tworzywa sztucznego, kopułka z poliwęglanu, osłona przeciwsłoneczna (poliwęglan/ASA)
Kolor: biały (NCS S 1002-B)
Zrównoważony rozwój
Bez PCW
Zasilanie
Power over Ethernet (PoE) IEEE 802.3at typ 2 klasa 4
Typowo 9 W, maks. 23 W
10–28 V DC, typowo 9 W, maks. 24 W
Oświetlenie w podczerwieni
Oświetlenie w podczerwieni z oszczędnymi diodami 850 nm o dużej żywotności
zasięg 40 m (130 ft) lub więcej, w zależności od sceny
Warunki robocze
Od -50°C do 55°C (-58°F do 131°F)
Maksymalna temperatura według NEMA TS 2 (2.2.7): 74°C (165°F)
Temperatura rozruchu: –40°C (–40°F)
Wilgotność 10–100% RH (z kondensacją)
Gwarancja
5-letnia gwarancja

17. W przedmiarze teletechnicznym zawarto nazwy własne kamer: „Kamera wewnętrzna Q6135-LE 50HZ”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

<u>Wymagania minimalne</u>
Przetwornik obrazu
1/2,8” skanowanie progresywne CMOS
Obiektyw
Zmiennoogniskowy, 4,3–137,6 mm, F1,4–4,0
Pole widzenia w poziomie: 58.3˚–2.4˚
Pole widzenia w pionie: 34.9˚–1.3˚
Automatyczne ustawianie ostrości i przysłony
Dzień i noc
Automatyczny zdejmowalny filtr odcinający podczerwień

Minimalne oświetlenie
Kolor: 0,06 luksa przy 30 IRE F1.4
Obraz czarno-biały: 0,008 luksa przy 30 IRE F1,4, 0 luksów przy włączonym oświetleniu w podczerwieni
Kolor: 0,09 luksa przy 50 IRE F1.4
Obraz czarno-biały: 0,01 luksa przy 50 IRE F1,4, 0 luksów przy włączonym oświetleniu w podczerwieni
Prędkość migawki
Od 1/66 500 s do 2 s
Poklatkowość
Maks. 50/60 kl./s (50/60 Hz) w rozdzielczości 1080p
Protokoły sieciowe
IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS, HTTP/2, TLS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTP, SRTP/RTSPS, SFTP, TCP, UDP, IGMP, RTCP, ICMP, DHCPv4/v6, ARP, SSH, NTCIP, LLDP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), adres Link-Local (ZeroConf)
Interfejs programowania aplikacji (ang. Application Programming Interface, API)
Otwarty interfejs programowania aplikacji (API) umożliwiający integrację oprogramowania.
ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S i ONVIF® Profile T, specyfikacja pod adresem onvif.org
Wbudowana pomoc podczas montażu
Licznik pikseli, poziomica
Object Analytics
Klasy obiektów: ludzie, pojazdy
Scenariusze: przekroczenie linii, obiekt w strefie, zliczanie obiektów przekraczających linię, czas przebywania na obszarze
Maksymalnie 10 scenariuszy
Metadane wizualizowane z trajektoriami, obwiedniami kodowanymi kolorami i tabelami
Wielokątne strefy detekcyjne/wykluczania
Konfiguracja perspektywy
Alarm wyzwolony ruchem ONVIF
Metadane
Dane obiektu: Klasy: ludzie, twarze, pojazdy (rodzaje: samochody, autobusy, ciężarówki, jednoślady), tablice rejestracyjne
Ufność, położenie
Dane o zdarzeniu: Odwołanie do producenta, scenariusze, warunki wyzwalania
Zastosowania
Umożliwia instalowanie aplikacji innych firm
EMC
EN 55032 klasa A, EN 55035,EN 55024, EN 50121-4, IEC 62236-4, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2
Zabezpieczenia
IEC/EN/UL 62368-1, IEC/EN/UL 60950-22, IEC/EN 62471 grupa ryzyka 2, IS13252
Środowisko
IEC/EN 62262 IK08, IEC/EN 60529 IP66, NEMA 250, typ 4X, NEMA TS 2 (2.2.7–2.2.9), IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-30, IEC 60068-2-78, ISO4892-2
Sieć
NIST SP500-267
Cyberbezpieczeństwo
ETSI EN 303 645
Bezpieczeństwo na obwodzie
Oprogramowanie: Podpisane oprogramowanie sprzętowe, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem, szyfrowanie kart SD AES-XTS-Plain64 256-bitowe
Sprzęt: platforma zabezpieczająca kryptograficznego modułu obliczeniowego
Moduł TPM 2.0 (CC EAL4 +, FIPS 140-2 poziomu 2), bezpieczny magazyn kluczy, bezpieczne uruchamianie
Bezpieczeństwo w sieci
IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa

hosta

Obudowa

IK08, IK10 obudowa i montaż, IP66 i NEMA 4 X

Metalowa (aluminiowa) obudowa do przemalowywania, powlekana przezroczysta kopułka z poliwęglanu (PC)

Zrównoważony rozwój

Wolny od związków PCW

Zasilanie

Zasilacz High PoE midspan 1 port: 100–240 V AC, maks. 74 W

Pobór mocy przez kamerę: typowo 13,5 W (bez oświetlenia w podczerwieni), maks. 51 W

Zasilacz PoE+ midspan 1 port: 100–240 V AC, maks. 37 W

IEEE 802.3at Typ 2 Klasa 4

Pobór mocy przez kamerę: typowo 13.5 W, maks. 25 W

Oświetlenie w podczerwieni

Wbudowane oszczędne oświetlenie LED w podczerwieni z (850 nm) automatycznym dostosowaniem kąta oświetlenia i natężenia.

Z zasilaczem midspan o mocy 30 W: Zasięg 190 m (623 ft) lub więcej, w zależności od sceny

Z zasilaczem midspan o mocy 60 W: Zasięg 250 m (820 ft) lub więcej, w zależności od sceny

Warunki robocze

Z zasilaczem midspan o mocy 30 W: od -30°C do 50°C (-22°F do 122°F)

Z zasilaczem midspan o mocy 60 W: od -50°C do 50°C (-58°F do 122°F)

Maksymalna temperatura według NEMA TS 2 (2.2.7): 74°C (165°F)

Inteligentna technologia ogrzewania kamer: Rozruch już przy –40°C (–40°F)

Wilgotność 10–100% RH (z kondensacją)

Gwarancja

5-letnia gwarancja

18. W przedmiarze teletechnicznym zawarto nazwy własne kamer: „Kamera wewnętrzna Q6225-LE 50 HZ”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

<u>Wymagania minimalne</u>

Przetwornik obrazu

1/2" skanowanie progresywne CMOS

Obiektyw

Długość ogniskowej: 6,91–214,64 mm, F1.36 – F4.6

Pole widzenia w poziomie: 63.8°– 2.2°

Pole widzenia w pionie: 37°– 1.3°

Autofokus, technologia sterowania przysłoną P-Iris

Dzień i noc

Automatycznie wyłączany filtr odcinający podczerwień

Minimalne oświetlenie

Kolor: 0,05 luksa przy 30 IRE F1.36

Obraz czarno-biały: 0,001 luksa przy 30 IRE F1.36, 0 luksów przy włączonym oświetleniu w podczerwieni

Kolor: 0,08 luksa przy 50 IRE F1.36

Obraz czarno-biały: 0,008 luksa przy 50 IRE F1.36, 0 luksów przy włączonym oświetleniu w podczerwieni

Prędkość migawki

Od 1/111000 s do 1/2 s

Pan/Tilt/Zoom — funkcja panoramowania, pochylenia i zbliżenia

Panoramowanie: 360° bez ograniczeń, od 0,05°/s do 150°/s

Pochylenie: Od -90° do +90°, od 0,05°/s do 150°/s

Zoom: 31-krotny zoom optyczny, 12-krotny zoom cyfrowy

Dokładność prepozycji: 0.10°

300 prepozycji, zapis trasy, trasa strażnika, kolejka sterowania, narzędzie do orientacji PTZ, przywracanie ostrości

Poklatkowość

Maksymalnie 60/50 kl./s (60/50 Hz) we wszystkich rozdzielczościach

Bezpieczeństwo

Filtrowanie adresów IP, szyfrowanie HTTPS, kontrola dostępu do sieci w standardzie IEEE 802.1x (EAP-TLS), dziennik dostępów użytkowników, centralne zarządzanie certyfikatami

Protokoły sieciowe

IPv4/v6, ICMPv4/ICMPv6, HTTP, HTTP/2, HTTPS, TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, RTCP, ICMP, DHCPv4/v6, ARP, SOCKS, SSH, LLDP, NTCIP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), adres Link-Local (ZeroConf)

Interfejs programowania aplikacji (ang. Application Programming Interface, API)

Otwarty interfejs programowania aplikacji (API) do integracji oprogramowania,
ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S i ONVIF® Profile T, specyfikacja pod adresem onvif.org

Wbudowana pomoc podczas montażu

Licznik pikseli
Automatyczna orientacja

Zastosowania

W zestawie
analiza obiektów, metadane sceny, wizyjna detekcja ruchu, automatyczne śledzenie, funkcja strażnika
Umożliwia instalowanie aplikacji innych firm

Object Analytics

Klasy obiektów: ludzie, pojazdy
Scenariusze: przekroczenie linii, obiekt w strefie, zliczanie obiektów przekraczających linię, czas przebywania na obszarze
Maksymalnie 10 scenariuszy
Inne cechy: wyzwalane obiekty wizualizowane z trajektoriami, obwiedniami kodowanymi kolorami i tabelami
Wielokątne strefy detekcyjne/wykluczania
Konfiguracja perspektywy
Alarm wyzwolony ruchem ONVIF

EMC

EN 55035, EN 55032 klasa A, EN 50121-4, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2
Australia / Nowa Zelandia: RCM AS/NZS CISPR 32 klasa A
Kanada: ICES-3(A)/NMB-3(B)
Japonia: VCCI klasa A
Korea: KS C 9835, KS C 9832 klasa A
USA: FCC część 15 podczęść B klasa A

Zabezpieczenia

CAN/CSA C22.2 nr 62368-1, CAN/CSA-C22.2 nr 60950-22, IEC/EN/UL 62368-1, IEC/EN/UL 60950-22, IEC/EN 62471 grupa ryzyka 2, IS 13252

Środowisko

IEC/EN 60529 IP66/IP68, NEMA 250 typ 4X, NEMA TS 2 (2.2.7-2.2.9), IEC/EN 62262 IK10, MIL-STD-810G (metoda 500.5, 501.5, 502.5, 503.5, 505.5, 506.5, 507.5, 509.5, 510.5, 521.3), IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78

Sieć

NIST SP500-267

Cyberbezpieczeństwo

ETSI EN 303 645, FIPS 140
Zasilacz midspan: EN 60950-1, GS, UL, cUL, CE, FCC, VCCI, CB

Bezpieczeństwo na obwodzie

Oprogramowanie: Podpisane oprogramowanie sprzętowe, ochrona przed atakami brute force, uwierzytelnianie szyfrowane i OAuth 2.0 RFC6749 OpenID Authorization Code Flow do scentralizowanego zarządzania kontami ADFS, ochrona hasłem, szyfrowanie kart SD AES-XTS-Plain64 256-bitowe
Sprzęt: platforma zabezpieczająca kryptograficznego modułu obliczeniowego
Moduł TPM 2.0 (CC EAL4+, FIPS 140-2 poziomu 2), zabezpieczony element (CC EAL 6+), ID urządzenia producenta, bezpieczny magazyn kluczy, podpisane wideo, bezpieczne uruchamianie

Bezpieczeństwo w sieci
IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), infrastruktura klucza publicznego z certyfikatami X.509, zapora sieciowa hosta
Obudowa
Aluminiowa obudowa o klasie ochrony IP66, IP68, NEMA 4X i IK10.
Kolor: Szary Urban Grey NCS S 5502–B
W zestawie wycieraczka (pióro silikonowe)
Zrównoważony rozwój
Bez PCW
Zasilanie
High Power over Ethernet, maks. 90 W
Power over Ethernet (PoE) IEEE 802.3bt typ 4
Możliwości optymalizacji zużycia energii w kamerze:
Full power (Pełna moc): typowo 16 W (bez oświetlenia w podczerwieni), maks. 71 W
Low power (Niska moc): typowo 16 W (bez oświetlenia w podczerwieni), maks. 32 W. Z oświetleniem w podczerwieni: 53 W
Funkcje: profile zasilania, miernik mocy
Oświetlenie w podczerwieni
Oświetlenie w podczerwieni z oszczędnymi diodami 850 nm o dużej żywotności
Zasięg 400 m (1300 ft) lub więcej, w zależności od sceny
Warunki robocze
Temperatura przy pełnej mocy: od -50°C do 55°C (-58°F do 131°F)
Temperatura przy niskiej mocy: od 0°C do 55°C (od 32°F do 131°F)
Maksymalna temperatura według NEMA TS 2 (2.2.7): 74°C (165°F)
Inteligentna technologia ogrzewania kamer: Rozruch już przy –40°C (–40°F)
Wilgotność: 10–100% RH (z kondensacją)
Siła wiatru (stała): 68 m/s (245 km/h, 150 mph)
Gwarancja
5-letnia gwarancja

19. W przedmiarze teletechnicznym zawarto nazwy własne rejestratora: „Rejestrator S1264 RACK 64 TB”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności kamer. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

<u>Wymagania minimalne</u>

Licencje
64 Licencje na stację zarządzania wideo producenta są dołączone i powiązane ze sprzętem. Można je rozszerzyć za pomocą licencji dodatkowych (sprzedawanych oddzielnie).
Skalowalność systemu
Maksymalnie 192 drzwi oraz szybkość zapisu 850 Mbit/s, 96 kanały wideo przy 4 MP, 30 kl./s w obiektach handlowych.
Pamięć
Jednostka 64 TB 2 x 8 GB
Pamięć masowa
Enterprise Class HDD z możliwością wymiany podczas pracy (tzw. hot-swap)
Łączna liczba gniazd HDD: 12
Wolne gniazdo HDD: 4
Pamięć masowa gotowa do użycia po rozpakowaniu: 56 TB po zastosowaniu macierzy RAID 5
Gotowość do pracy od razu po rozpakowaniu bez macierzy RAID: 64 TB (8 X 8 TB)
RAID
Jednostka 64 TB

Fabryczny poziom RAID: 5
Obsługiwane poziomy RAID: 0, 1, 5, 6, 10
Zasilanie
2 zasilacze nadmiarowe 800 W typu Hot Plug (w zestawie)
(100–240 V AC, 9,2–4,7 A, 50/60 Hz)
Złącza
Z przodu:
1x USB 2.0
1x VGA
1 port bezpośredni iDRAC
Tylna strona:
1x USB 2.0
1x USB 3.0
1x VGA
1 dedykowany port Ethernet iDRAC
2 x RJ45 1 GB/s
System operacyjny
Microsoft® Windows® 10 IoT Enterprise LTSC 2021
Wbudowana funkcja odzyskiwania systemu operacyjnego: tak
Dysk systemu operacyjnego: 240 GB SSD
Zdalne zarządzanie serwerem
Licencja ekspresowa na kontroler iDRAC 9
Bezpieczeństwo
Obsługa zaszyfrowanych dysków systemu operacyjnego i zapisu
Moduł Trusted Platform Module (TPM 2.0) z certyfikatem FIPS 140-2 poziom 2
Warunki robocze
od 10°C do 35°C (od 50°F do 95°F)
Wilgotność 20–80% RH (bez kondensacji)
Certyfikaty
Kompatybilność elektromagnetyczna
EN 55032 klasa A, EN 55024, EN 55035, EN 61000-3-2, EN 61000-3-3, FCC części 2 i 15 klasa A, ISED ICES-003 klasa A, RCM AS/NZS CISPR 32 klasa A, KS C 9832 klasa A, KS C 9835, VCCI 32-1 klasa A, BSMI
Zabezpieczenia
IEC/EN/UL 60950-1, IEC/EN/UL 62368-1, EN 62311, NOM-019-SCFI-1998
Zgodność
TAA (ustawa porozumieniach handlowych)
Usługi
Interwencja na miejscu awarii w następnym dniu roboczym
Zachowanie dysku po wymianie
Gwarancja
5-letnia gwarancja

STACJA DOZORU

Procesor
Procesor Intel® Core
Pamięć
16 GB (2 X 8 GB)
Karta graficzna
Intel® UHD graphics
Złącza
Z przodu:
1x Universal Audio Jack, gniazdo uniwersalne
2x USB 2.0
1x USB 3.2
1x port USB 3.2 gen 2 2x2 USB-C
Tylna strona:
1x Universal Audio Jack, gniazdo uniwersalne

1x DisplayPort 1.4a
1 złącze główkowe zdalnego przycisku zasilania
4x USB 3.2
2x USB 2.0
1x RJ45 Ethernet
3x Mini DisplayPort 1.4
Strumieniowanie wideo
Podgląd na żywo:
1 strumień x 4K przy 30 kl./s
Podział 4 x 1080p przy 30 kl./s
Podział 9 x 720 przy 30 kl./s
Podział 16 x 360p przy 15 kl./s
Podział 25 x 360p przy 15 kl./s
Podział 36 x 360p przy 15 kl./s
Dowolna kombinacja powyższych opcji dla maksymalnie czterech monitorów 4K, przy czym tylko na dwóch monitorach można wyświetlać strumienie przy 30 kl./s.
Odtwarzanie:
Obsługa takich samych scenariuszy podziału, jak w podglądzie na żywo.
Odtwarzanie z dużą szybkością może wpływać na wydajność wideo.

System operacyjny
Microsoft® Windows® 10 IoT Enterprise LTSC 2021
Wbudowana funkcja odzyskiwania systemu operacyjnego
Dysk systemu operacyjnego: 256 GB SSD
Bezpieczeństwo
Obsługa zaszyfrowanego dysku z systemem operacyjnym
Moduł Trusted Platform Module (TPM 2.0) z certyfikatem FIPS 140-2 poziom 2
Warunki robocze
od 0°C do 45°C (od 32°F do 113°F)
Wilgotność 20–80% RH (bez kondensacji)
Certyfikaty
Kompatybilność elektromagnetyczna
EN 55032 klasa B, EN 55035, EN 61000-3-2, EN 61000-3-3, FCC część 2 i 15 klasa B, ISED ICES-003 klasa B, RCM AS/NZS CISPR 32 klasa B, KS C 9832 klasa B, KS C 9835, VCCI 32-1 klasa B, BSMI
Zabezpieczenia
IEC/EN/UL 62368-1, EN 62311, NOM-019-SCFI-1998
Zgodność
TAA (ustawa porozumieniach handlowych)
Usługi
Interwencja na miejscu awarii w następnym dniu roboczym
Gwarancja
5-letnia gwarancja

20. W przedmiarze teletechnicznym zawarto nazwy własne rejestratora: „Rejestrator S1264 RACK 64 TB”

Brak określenia parametrów minimalnych oraz brak parametrów kluczowych do określenia równoważności rejestratora. Wnioskujemy o dołączenie do dokumentacji powyższego zestawienia zgodnie z Prawem Zamówień Publicznych art. 99 ust. 6.

Jak dla pkt 19