Podstrategia informatyzacji obszaru funkcjonalnego powiatu mikołowskiego

wraz z przygotowaniem Planu Operacyjnego na lata 2016-2025 w ramach projektu pod nazwą „J-ednolita S-trategia T-erytorialna = spójny obszar funkcjonalny powiatu mikołowskiego poprzez wzmocnienie mechanizmów efektywnej współpracy JST”

Załącznik. B. Szczegółowa koncepcja rozwiązania w zakresie Data Center

Zamawiający:

Zarząd Powiatu Mikołowskiego

ul. Żwirki i Wigury 4a

43-190 Mikołów

Wykonawca:

Centrum Doradztwa w Informatyce i Zarządzaniu Sp. z o.o.

ul. Mogilska 25

31-542 Kraków

Kraków 2015

Spis treści

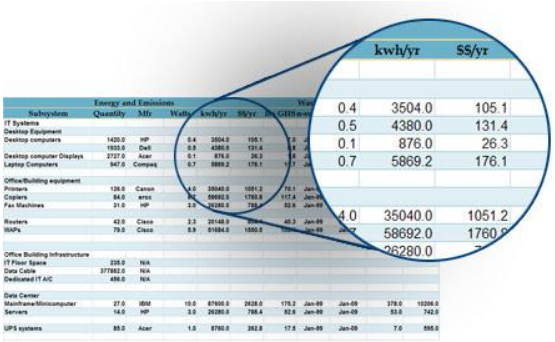
Załącznik. B. Szczegółowa koncepcja rozwiązania w zakresie Data Center

1. Serwerownia – podstawowy ośrodek przetwarzania danych

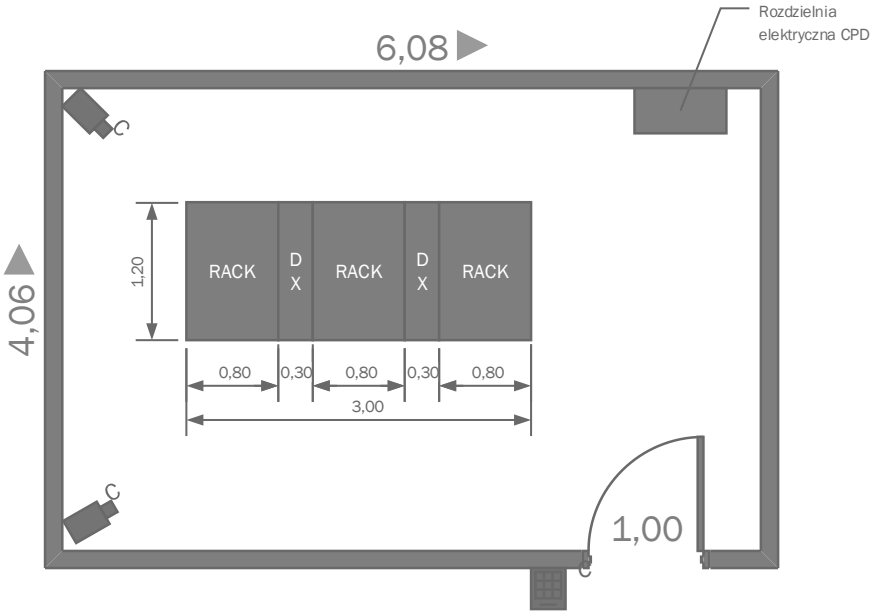
Jednym z elementów wymagającym modernizacji są serwerownie, które na dzień dzisiejszy nie spełniają wytycznych GIODO oraz wytycznych wynikających z ROZPORZĄDZENIA RADY MINISTRÓW z 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
W przedstawianych rozwiązaniach uwzględniane są aspekty wynikające z Ustawy w odniesieniu do Polskich Norm PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2, PN-ISO/IEC 27001, PN-ISO/IEC 17799, PN-ISO/IEC 24762.
Nowo projektowane rozwiązanie kładzie duży nacisk na bezpieczeństwo gromadzonych i przetwarzanych danych oraz zapewnienie optymalnych warunków danych dla zainstalowanego sprzętu IT.

Nowoczesne rozwiązania zastosowane w CPD będą uwzględniały najnowsze standardy wymagań energetycznych wpisując się w technologie Green IT oraz będą zapewniały możliwość zwiększenia mocy obliczeniowej w przypadku zaistnienia takiej potrzeby.

Zastosowany system zamkniętych szaf serwerowych ogranicza kubaturę konieczną do schłodzenia, co przekłada się bezpośrednio na zmniejszenie kosztów energii elektrycznej, zastosowane innowacyjne rozwiązanie Hyper Converge oparte na technologii VMWareESXi pozwala na optymalne wykorzystanie mocy obliczeniowej, łatwy przydział zasobów w zależności od potrzeb końcowego użytkownika oraz łatwą rozbudowę zarówno mocy obliczeniowej jak i przestrzeni do przechowywania danych.



W serwerowni CPD zlokalizowanej w wyznaczonym pomieszczeniu Starostwa Powiatowego, dla celów przechowywania urządzeń serwerowych na podłodze technicznej o wysokości 400 mm, zamontowany zostanie system składający się z jednego szeregu 3 szaf szczelnych serwerowych IP55 o głębokości 1200 mm, chłodzonych powietrzem z wykorzystaniem freonu R410A jako czynnika chłodniczego. Pomiędzy szafami serwerowymi zamontowane zostaną 2 urządzenia chłodzące jako klimatyzatory międzyrzędowe zintegrowane z szafami. Przykładową aranżację wnętrza przedstawia poniższy rysunek.



Szafy te zamykają infrastrukturę IT (serwery, macierze, urządzenia bezpieczeństwa), szafy krosownicze, klimatyzację, gaszenie w jednej szczelnej platformie systemowej.

Szafa serwerowa

Do klimatyzacji szaf szczelnie zamkniętych: szafa RACK o wysokości zabudowy 42U, przednie drzwi przeszklone o grubości szyby min 3mm, zamknięte tylne pełne drzwi dzielone pionowo 2x 400mm z blachy stalowej, wieloczęściowa płyta dachowa do bocznego wprowadzania kabli z obu stron, otwarta rama podłogowa, bez ścian bocznych. Dwie płaszczyzny mocowania 482,6 mm (19“) z przodu i z tyłu na wspornikach. Nośność szaf 1000kg.

Akcesoria montażowe 19“ i kompletny zestaw uziemienia dołączone luzem do zestawu. Ściany boczne, dwuczęściowe, dzielone poziomo z szybko zamykaczem, bezpiecznym zamknięciem i blokadą wewnętrzną uniemożliwiającą dostęp z zew. pomimo posiadania klucza, do wygodnego montażu jednoosobowego, szyna do mocowania podłogi. Na każdą jedną szafę serwerową należy zastosować płyty podłogowe modułowe dla kombinacji: pełne zamknięte oraz min. jedna wysokoszczelna z przejściem szczotkowym po szerokości szaf (klasa palności zgodnie z UL 94-V0), a także min. jeden moduł podłogi jako moduł wieloczęściowy płyty podłogi szafy o szer. 800mm do bocznego obustronnego wprowadzania kabli z płynną obustronną regulacją szer. wejścia dla okablowania. Wszystkie skręcone części poszycia podłogi z automatycznym wyrównaniem potencjałów i przygotowaniem do mocowania taśm uziemienia.

Wstępnie zmontowana szafa IT składająca się z odpornego na skręcanie, spawanego, symetrycznego stelażu ramy wykonanej z 16-krawędziowych, pionowych profili walcowanych w połączeniu z dwoma poziomymi ramami z 9-krawędziowych profili walcowanych ze zintegrowaną rynienką do montażu dołączonych uszczelek elementów płaskich do ochrony przed uszkodzeniami przez ewentualne agresywne media.

Wszystkie profile ramowe, ze zintegrowanym otworami systemowymi z podziałką DIN 25 mm, umożliwiają wygodną zabudowę zewnętrzną przez łatwe zawieszanie i zabezpieczanie poszczególnych komponentów. Wszystkie krawędzie profilu są zaokrąglone. Pionowe profile ramowe posiadają po dwie przemieszczone na szerokość i głębokość płaszczyzny montażowe, które można osobno wykorzystać w elastycznym mocowaniu komponentów.

Łączenie szaf w szeregi jest możliwe we wszystkich kierunkach, do przodu, do tyłu, w bok, jedna na drugiej, a nawet narożnikowo.

Przeszklone przednie drzwi z jedną szybą ESG 3mm z bezpiecznego szkła, oprawione w ramę z profili aluminiowych, z uszczelnieniem piankowym, 4-punktowe zamknięcie prętowe, uchwyt Komfort do wkładek cylindrycznych (30/10) mm, wyposażony w bezpieczne zamknięcie 3524 E. Poczwórne zawiasy z niewypadającymi kołkami, kąt otwarcia zawiasów przy zabudowie wolnostojącej 180°, możliwość wymiany zawiasów bez demontażu drążków zamka.

Tylne drzwi pełne z blachy stalowej, dzielone pionowo 2x 400mm, do optymalnego ustawiania szaf w pomieszczeniu i ułatwionego dostępu do komponentów. Drzwi z uszczelnieniem piankowym. Główne drzwi - 4-punktowe zamknięcie prętowe, uchwyt Komfort do wkładek cylindrycznych (30/10) mm, wyposażony w bezpieczne zamknięcie 3524E. Drzwi boczne z dodatkową wewnętrzną dźwignią i także z 2-punktowym zamknięciem prętowym. Drzwi główne i boczne z podwójnymi zawiasami z niewypadającymi kołkami, kąt otwarcia zawiasów przy zabudowie wolnostojącej 180°.

Wieloczęściowa płyta dachowa, do bocznego wprowadzania kabli przez listwy szczotkowe na całej głębokości szafy. Blacha dachowa do dozbrojenia z możliwością demontażu także już po wykonanej instalacji kabli. Zintegrowane wycięcie pod moduł wentylatora, zamknięte blachą zakrywającą. Do wzmocnienia wentylacji pasywnej możliwe jest uniesienie płyty dachowej za pomocą elementów dystansowych.

Wstępnie zmontowane z dwoma płaszczyznami mocowania 482,6mm (19“) z przodu i z tyłu. Łączna obciążalność statyczna obu 19” płaszczyzn montażowych musi wynosić min. 1500 kg.

Płaszczyzna montażowa 19" składa się z uniwersalnych szyn profilowych do zastosowań serwerowych, sieciowych i elektronicznych, z bezstopniową regulacją głębokości, mocowanie do poprzeczek.

Mocowanie szyn profilowych odbywa się elastycznie, bez użycia narzędzi, za pomocą szybkozłączy i równocześnie z możliwością skręcenia na sztywno. Szyny profilowe z przodu i z tyłu z dodatkowym otworowaniem w standardzie EIA 310 E. Wszystkie jednostki wysokości są oznakowane na szynach profilowych i ponumerowane w przeciwnych kierunkach. Oznakowanie U obu płaszczyzn montażowych jest czytelne od przodu, co ułatwia montaż jednoosobowy.

Wszystkie poprzeczki ze zintegrowaną podziałką do szybkiego określania odstępów montażowych i pozostałej wolnej przestrzeni z przodu.

Szyny profilowe z przodu są przygotowane do beznarzędziowego montażu elementów ułatwiających prowadzenie kabli i organizowania struktury okablowania o maksymalnej gęstości upakowania, albo do wyposażenia w listwę czujnikową do automatycznej identyfikacji elementów zabudowy z użyciem Radio Frequency Identification (RFID).

Szyny profilowe z tyłu są przygotowane do obustronnego zamocowania Power Distribution Unit (PDU) o współczynniku kształtu 1U do zelektryfikowania szafy bez zużywania objętości pod zabudowę dzięki szczególnie oszczędnemu montażowi pomiędzy płaszczyzną montażową a ścianą boczną, w przestrzeni zero-U.

Każda z szaf będzie posiadać po min. dwie pionowe listwy dystrybucji zasilania PDU 24xC13/4xC19 z zabezpieczeniem 2x16A typu C, opomiarowane na fazę i przełączalne na każde gniazdo. Listwy PDU muszą posiadać możliwość montażu w sposób beznarzędziowy w przestrzeni pomiędzy ścianą boczną a profilem 19" w dedykowanych zatokach szafy przeznaczonych na dystrybucję zasilania oraz alternatywnie po dwie bliźniaczo, na stronę lewą lub prawą w sposób beznarzędziowy.

System gaszenia szczelnie zamkniętych szaf

Każda z szaf wyposażona jest w system wczesnego wykrywania i gaszenia panelami gaśniczymi o wysokości montażowej max. 1U w układzie Master >Slave, dla każdego rzędu jeden panel gaśniczy nadrzędny i dwa panele podrzędne połączone w jeden system. Jako środek gaśniczy stosuje się Novec™ 1230 firmy 3MTM, który paruje w dyszy gaśniczej i równomiernie rozprasza się w strefie gaszenia. Pożar zostaje ugaszony przez odebranie energii cieplnej płomieniom. Detekcja pożaru następuje poprzez dwie czujki pożaru zintegrowane w każdym panelu gaśniczym. Informacje o alarmach i awariach mogą być przesyłane do systemu nadrzędnego (urządzenia dozorującego lub zarządzającego) poprzez styki bezpotencjałowe i poprzez system monitorowania globalny tworzony dla zarządzania całością projektowanej infrastruktury IT w tym połączony z projektowaną serwerownią zapasową.

Wentylator stale zasysa przez system rurek powietrze z chronionych szaf. Pobrane powietrze jest kierowane przez prowadnice i przepływa przez czujki pożaru. Pożar jest wykrywany, gdy pobrane powietrze zawiera dym. Sprawność czujek jest stale monitorowana przez elektronikę na karcie sterującej.

W przypadku osiągnięcia pierwszego progu alarmu pożarowego, elektronika analizująca uruchamia procedurę przewidzianą dla takiej sytuacji: na wyświetlaczu stan alarmu. Dodatkowo błyska, czerwona dioda na płycie czołowej urządzenia. Zostaje wysterowane wyjście przekaźnikowe „Alarm wstępny".

Po osiągnięciu drugiego progu alarmu pożarowego zostaje wysterowane wyjście przekaźnikowe „Pożar", po upłynięciu zadanego czasu analizowania następuje elektryczne uaktywnienie urządzenia wyzwalającego w wyniku czego otwiera się nabój gazowy i substancja robocza wypływa. Zostaje wysterowane wyjście przekaźnikowe „Gaszenie". Substancja robocza wyciska środek gaszący do dyszy gaśniczej. W dyszy następuje odparowanie środka gaśniczego i w chronionych szafach wytwarza się koncentracja potrzebna do zgaszenia ognia.

Zainstalowany w zbiorniku czujnik poziomu informuje o ubytku środka gaszącego elektronikę analizującą, która z kolei wyświetla tę awarię ubytek środka gaszącego na wyświetlaczu. Zostaje wysterowane wyjście przekaźnikowe „Zbiorczo awaria". Zasilanie elektryczne systemu jest zapewnione z dwóch źródeł. Po pierwsze z zasilacza, który zapewnia również ładowanie akumulatorów zasilania awaryjnego i po drugie jest to właśnie zasilanie awaryjne, podłączone w trybie gotowości równoległej. Zintegrowane zasilanie awaryjne jest przystosowane do nieprzerwanej pracy systemu w czasie min. 4h.

Zainstalowany w zbiorniku czujnik poziomu informuje o ubytku środka gaszącego elektronikę analizującą, która z kolei wyświetla tę awarię (ubytek środka gaszącego) na wyświetlaczu. Zostaje wysterowane wyjście przekaźnikowe „Zbiorczo awaria".

Zasilanie elektryczne systemu jest zapewnione z dwóch źródeł. Po pierwsze jest to zasilacz, który zapewnia również ładowanie akumulatorów zasilania awaryjnego. Po drugie jest to właśnie zasilanie awaryjne, podłączone w trybie gotowości równoległej. Zasilanie awaryjne jest przystosowane do nieprzerwanej pracy systemu w czasie 4 h.

System automatycznego awaryjnego otwarcia drzwi szaf serwerowych oraz szaf zasilania awaryjnego

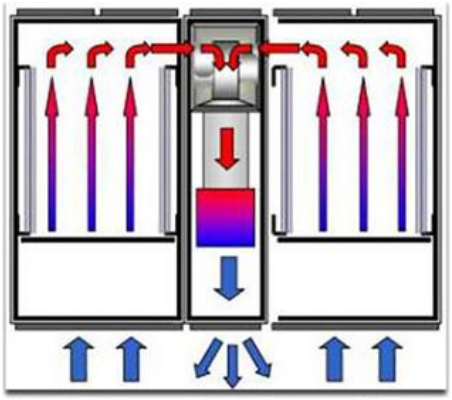
Każda z szaf serwerowych oraz szafy zasilania awaryjnego UPS muszą być zaprojektowane i dostarczone wraz z zintegrowanym system awaryjnego automatycznego otwarcia drzwi przednich i tylnych szaf. Zadaniem automatyki systemu jest otwarcie drzwi szaf w sposób automatyczny w przypadku braku zasilania oraz awarii układu chłodzenia od ustawionego wzrostu temp. wewnątrz szczelnie zamkniętych szaf. Dodatkowo zaprojektowany system centralnego monitorowania i zarządzania zdalnego układu szaf będzie sprzężony z projektowanymi odrębnie klimatyzatorami pomieszczenia typu Split tak aby w przypadku awarii układu chłodzenia i wzrostu temp. wew. szaf po awarii zostały one natychmiast uruchomione w celu chłodzenia awaryjnego pomieszczenia. Każda z szaf odrębnie musi zostać wyposażona w system otwarcia drzwi: lokalnego manualnego z klamki dla drzwi przednich oraz odrębnie dla drzwi tylnych, zdalnego oraz automatycznego w przypadku awarii. Dodatkowo z uwagi na możliwe podciśnienie panujące w szafach serwerowych w czasie pracy

urządzeń szczelnie zamkniętych wewnątrz należy wyposażyć każde drzwi szaf serwerowych w system elektrycznego wspomagającego otwarcia drzwi niwelujący efekt podciśnienia.

Każda z szaf musi zostać wyposażona w odrębny niezależny moduł sterujący otwarciem drzwi szaf wraz z dedykowanym czujnikiem NTC. Każdy moduł sterujący musi być zasilany w redundancji, a w przypadku modułów elektrycznych niwelujących podciśnienie systemu musi być zasilony z UPS.

Każdy z modułów sterujących zainstalowanych w szafie musi posiadać min.: 3 wejścia cyfrowe dla sygnału Alarmu z zewnętrznego systemu/ drzwi przednich / drzwi tylnych, min. 1 wejście dla czytników zamek cyfrowy / czytnik transponderów, min. 2 wyjścia dla systemu zwolnienia otwarcia drzwi, min. 2 wyjścia dla elektrycznego systemu niwelowania podciśnienia w szafie, 2 złącza magistrali przyłączeniowej Can Bus.

Klimatyzacja międzyrzędowa na bazie systemu bezpośredniego odparowania dedykowana do szczelnie zamkniętych szaf



W celu zapewnienia optymalnego chłodzenia urządzeń dla szczelnie zamkniętych szaf zaprojektowane będą min. dwa klimatyzatory międzyrzędowe typu Split zintegrowane gabarytowo z szafami serwerowymi tego samego producenta o wysokości 42U o mocy chłodzenia wg EN 14511 12 kW dla L35/L30 i wydajności powietrza 4800 m^3/h. Projektowane urządzenia chłodnicze będą służyły do odprowadzania dużych mocy cieplnych z szaf serwerowych wzgl. do efektywnego chłodzenia urządzeń wbudowanych w szafie serwerowej. Prowadzenie powietrza będzie opierać się na zasadzie chłodzenia wbudowanych w szafie urządzeń "front to back". Ciepłe powietrze wydmuchiwane przez urządzenia w szafie serwerowej będzie bezpośrednio zasysane przez wentylatory z tyłu szafy i prowadzone przez moduł wymiennika ciepła.

W module wymiennika ciepła podgrzane powietrze będzie prowadzone przez wymiennik ciepła (parownik czynnika chłodniczego) i oddawać swoją energię cieplną (moc stratna z szafy serwerowej) do czynnika chłodniczego. Przy tym powietrze schładzane będzie do dowolnej temperatury w podanym zakresie, a następnie wprowadzane bezpośrednio przed płaszczyznę 19" szafy serwerowej w odseparowanej strefie powietrza zimnego i ciepłego. W rozwiązaniu regulacja temperatury wdmuchiwanego zimnego powietrza odbywa się poprzez stałe wyrównanie temperatury rzeczywistej z ustawioną temperaturą zadaną. Gdy temperatura rzeczywista przekracza wartość zadaną, wówczas automatycznie zwiększa się prędkość sprężarki, dzięki czemu wymiennik ciepła dostarcza większej mocy chłodniczej, aż do osiągnięcia zadanej temperatury. Na podstawie różnicy temperatur pomiędzy wartością zadaną i odsysanego ciepłego powietrza odbywa się wyznaczenie niezbędnej prędkości obrotowej wentylatorów i odpowiednia regulacja. Ewentualnie tworzące się w urządzeniu skropliny zbierane są przez zintegrowany kolektor kondensatu pod wymiennikiem ciepła i stamtąd kierowane na zewnątrz przez wąż odpływu kondensatu w sposób grawitacyjny. Klimatyzator może być szeregowany do wyboru po lewej lub prawej stronie szafy serwerowej lub też pomiędzy

dwoma szafami serwerowymi. Klimatyzatory międzyrzędowe wraz z szeregowaną szafą serwerową tworzą zamknięty powietrznie system chłodzenia z poziomym prowadzeniem powietrza, który nie stawia żadnych dodatkowych wymagań dotyczących klimatyzacji pomieszczenia.

W opisywanym systemie moduł wymiennika ciepła klimatyzatora składa się z następujących komponentów:

- **Sprężarka**- spręża czynnik chłodniczy i powoduje jego obieg od strony niskiego ciśnienia (parownik) do strony wysokiego ciśnienia (zewnętrzny skraplacz). Silnik jest uruchamiany przez zewnętrzny inwerter umożliwiający regulację obrotów sprężarki, a przez to dokładne dopasowanie mocy chłodniczej do rzeczywistego zapotrzebowania na chłodzenie;
- **Parownik** (wymiennik ciepła powietrze/chłodziwo)- umieszczony centralnie w urządzeniu;
- **Elektroniczny zawór rozprężny**- doprowadza do parownika potrzebną ilość czynnika chłodniczego w celu zapewnienia odpowiedniej do aktualnych warunków otoczenia mocy chłodniczej;
- **Skraplacz** - umieszczany poza miejscem zainstalowania klimatyzatora międzyrzędowego, na zewnątrz budynku;
- **Czujniki temperatury** - z przodu urządzenia, w pobliżu wentylatorów są zainstalowane trzy czujniki temperatury. Mierzą one temperaturę zimnego powietrza i przekazują wartości do sterownika. Trzy kolejne czujniki temperatury są zainstalowane z tyłu parownika. Mierzą one temperaturę ciepłego powietrza zasysanego z części tylnej szafy i również przekazują wartości do sterownika;
- **Wentylatory** - działające płynnie w zakresie prędkości obrotowej od 30 % do 100 %. Moduły wentylatorowe zostały zamontowane w przedniej części urządzenia na wsuwanych półkach. Czas wymiany pojedynczego modułu bez przerywania eksploatacji wynosi ok. 2 minuty.

Urządzenie wewnętrzne, klimatyzator i zewnętrzny skraplacz będą połączone odpowiednim miedzianym przewodem rurowym wg PN-EN 378-2.

Dla potrzeb podłączenia skraplacza i parownika zostaną wykonane przyłącza energetyczne odpowiednio – zewnętrzne 230V, 50/60 Hz z zabezpieczeniem 1,8 A, wewnętrzne w pomieszczeniu serwerowni 380V 50/60 Hz, 20A.

Szafy zasilania awaryjnego UPS

W projektowanym rozwiązaniu uwzględniono modułowy system szaf zasilania awaryjnego zapewniający wymaganą dla podtrzymania zasilania moc czynną z modułem redundantnym. Moduł szafy na moduły mocy zasilania awaryjnego musi zapewniać możliwość rozbudowy. Należy przyjąć dodatkową szafę na zlokalizowanie baterii zapewniających autonomię 13 min. podtrzymania zasilania dla 100% obciążenia. Zarówno szafa na moduły mocy jak i bateryjna muszą być szczelnie zamknięte i przystosowane do gaszenia panelami 19” wczesnego wykrywania i gaszenia pożaru wraz z integrowanym systemem awaryjnego i automatycznego otwierania drzwi przednich i tylnych obu szaf w przypadku awarii układu chłodzenia. Zestaw szaf chłodzony będzie przez wymiennik ciepła powietrze / woda wpięty do projektowanego dla serwerowni układu hydraulicznego schładzanej

przez agregat wody. Projektowany UPS o mocy 40kWA będzie wyposażony w kartę SNMP oraz wspólny system monitorowania i zarządzania jak wymienniki ciepła powietrze/ woda, agregat chłodzenia cieczy, system dystrybucji energii w szafach PDU, system centralnego monitorowania parametrów fizycznych w obrębi projektowanej serwerowni, system automatycznego awaryjnego otwarcia drzwi szaf, system wczesnego wykrywania i gaszenia pożaru w szafach. Do projektowanego systemu zasilania awaryjnego UPS należy podłączyć min. agregat chłodzenia cieczy poprzez specjalne dedykowane w nim złącze. Pozostałe elementy infrastruktury chłodzenia muszą posiadać niezależnie gwarantowane źródło zasilania.

Monitoring zarządzanie zdalne budowaną infrastrukturą IT serwerowni

Dla projektowanych urządzeń szaf serwerowych jako kluczowych elementów: zasilania awaryjnego UPS, listew dystrybucji zasilania PDU, systemu wczesnego wykrywania i gaszenia pożaru w szafach szczelnych, systemu automatycznego awaryjnego otwarcia drzwi szaf, powiadamiania SMS, oprogramowania DCIM. Będzie zastosowany system umożliwiający komunikację urządzeń, zdalną kontrolę i zarządzanie urządzeniami.

Oprogramowanie zarządzające dla CPD

Dla infrastruktury serwerowni głównej oraz zapasowej zostało przewidziane oprogramowanie zarządzające. Zadaniem oprogramowania jest optymalne wspieranie administratora IT przy obserwacji i sterowaniu poszczególnymi zaprojektowanymi urządzeniami aż po całościową optymalizację centrum obliczeniowego z uwzględnieniem ekonomicznych warunków brzegowych, jak też w aspektach dostępności i bezpieczeństwa.

Oprogramowanie monitoruje i steruje wszystkimi komponentami infrastruktury niezbędnymi do bezpiecznej pracy serwerów, pamięci masowych, routerów i switchy.

Są to min. projektowane urządzenia:

- zasilania prądem i zabezpieczanie mocy,
- wytwarzanie i rozdział zimna,
- monitorowanie pomieszczeń i szaf,
- bezpieczeństwo centrum obliczeniowego (dostęp, temperatura, gaszenie),
- wydajność i zużycie energii,
- zewnętrzne komponenty, niezależne także od serwerowni obsługujące SNMP.

Oprogramowanie może przedstawiać łączne zużycie (kW/h, CO2) i wydajność centrum obliczeniowego za pomocą analizy trendów. Pozwala na zdefiniowanie obwodów regulacyjnych w celu optymalnego ustawienia punktu pracy centrum obliczeniowego w zależności od potrzeb.

Oprogramowanie współpracuje z Microsoft System Center Operations Manager (MS SCOM), dzięki czemu administrator IT może obserwować i sterować serwerami, klientami, usługami i infrastrukturą fizyczną za pomocą interfejsu SCOM. Wszystkie komunikaty alarmu fizycznej infrastruktury IT są przekazywane do SCOM. Pomiary wydajności i analizy trendów całej infrastruktury centrum

obliczeniowego są wizualizowane w interfejsie SCOM. Dodatkowo możliwe jest powiązanie komunikatów o zakłóceniach w infrastrukturze centrum obliczeniowego z odpowiednimi usługami, przez co administrator IT może działać proaktywnie. Ponadto istnieje możliwość integracji centralnego oprogramowania zarządzania z IBM Tivoli, które służy do zarządzania serwerami i działającymi na nich aplikacjami oraz możliwość integracji centralnego oprogramowania z HP OpenView, które umożliwia pakiet do administrowania infrastrukturą serwerową i jej aplikacjami, najważniejszym komponentem jest Network Mode Manager (monitorowanie komponentów sieci: routery &switche) oraz OpenView Operations zarządzanie aplikacjami i systemem.

Pomieszczenie serwerowni

Pomieszczenie przeznaczone na serwerownię, w której zamontowany zostanie system szaf i sprzęt IT będzie miało powierzchnię ok. 25 m^2 i zlokalizowane zostanie budynku Starostwa Powiatowego w Mikołowie. Powyżej określona powierzchnia pozwala na swobodne ustawienie planowanej ilości zabudowy systemu szaf klimatycznych z możliwością rozbudowy o jedną szafę RACK 19" z jednostką urządzenia chłodzącego.

Wyznaczone pomieszczenie będzie wymagało adaptacji dla celów CPD. W ramach adaptacji zostaną wykonane prace:

- Wykonanie podłogi technicznej z wysoko sprasowanej płyty wiórowej z pokryciem górnym PVC ułożonej na konstrukcji wsporczej wykonanej z profili C82x40 o wysokości min. 400mm, o obciążeniu powierzchniowym 25kN/m^2 i współczynniku bezpieczeństwa 2 klasa E1, zgodnej z wymaganiami normy PN-EN12825;
- Wykonanie systemu alarmowego klasy SA3 zintegrowanego z kontrolą dostępu (wykorzystującą karty procesorowe) i monitoringiem wizyjnym;
- Montaż drzwi antywłamaniowych klasy C zgodnych z PN-90/B-92270, PN-EN 1627:2011**,** posiadających certyfikat IMP;
- Montaż systemu szaf szczelnych klimatyzowanych;
- Wykonanie systemu monitoringu parametrów środowiskowych wyposażonego w czujki temperatury, wilgotności, wycieków (w przypadku systemu szaf szczelnych klimatycznych będzie on zintegrowany z platformą systemową);
- Usunięcie urządzeń grzewczych;
- Montaż krat okiennych lub rolet antywłamaniowych lub zabezpieczenie folią antywłamaniową;
- Wykonanie przyłącza sieci WAN;
- Wykonanie rozdzielni elektrycznej dla serwerowni i zasilania gwarantowanego.

Instalacja alarmowa klasy SA3 wg. Polskiej Normy PN-90/B-92270, PN-86/E-06600, PN-93 E-08390/14 - zgodnie z zaleceniami Dz.U.2005 nr 200 poz. 1651,

Niezależnie od zabezpieczenia fizycznego opisanego powyżej, zostanie wprowadzony system alarmowy klasy SA3 posiadający następujące komponenty:

- pasywne czujki podczerwieni (wykrywanie osób w pomieszczeniu),
- akustycznej czujki stłuczenia szyb (dla serwerowni wyposażonych w okna),

- czujki magnetyczne stykowe (kontaktrony – wykrywają działania związane z otwarciem drzwi lub okien),
- opcjonalnie czujki antynapadowe (uruchamiane ręcznie przez personel w przypadku wystąpienia zagrożenia, np. napadu czy włamania),
- centrala alarmowa (kontrolująca działanie systemu alarmowego, sterująca czujkami, itd.),
- sygnalizator wystąpienia alarmu (przynajmniej w dwóch postaciach: sygnalizacja świetlna, sygnalizacja dźwiękowa). Sygnalizacja może być instalowana wewnątrz chronionego pomieszczenia, na zewnątrz pomieszczenia oraz na zewnątrz budynku, w którym znajduje się pomieszczenie podlegające ochronie, zalecane jest zastosowanie systemu transmisji sygnału alarmowego do centrum nadzorczego (np. wartownia w budynku, firma ochroniarska, policja),
- zalecane jest zapewnienie zasilania zapasowego systemu alarmowego (np. w postaci akumulatorów zintegrowanych z centralką alarmu).

System Kontroli Dostępu

System KD który będzie zainstalowany w Ośrodku Przetwarzani Danych pozwala na rozbudowę w sposób umożliwiający objęcie w przyszłości wszystkich pomieszczeń, z komunikacją po sieci LAN. System KD jest oparty o zintegrowana platformę bezpieczeństwa. Platforma integruje system kontroli dostępu, monitoring wideo IP oraz system sygnalizacji włamania i napadu, co pozwala zapewnić użytkownikowi jedną spójną platformę sprzętową oraz oprogramowania skupiającego w sobie wszystkie te systemy. System fabrycznie wyposażony jest w oprogramowanie wszystkimi zintegrowanymi urządzeniami. W procesie komunikacji wykorzystywane jest kodowanie AES 128 bitowe, które znakomicie zabezpiecza transmisję danych zwłaszcza w przypadku połączeń internetowych z siecią WAN.

Kontroler wyposażony jest w specjalne wejście linii dozorowej do podłączenia czujnika sabotażowego obudowy kontrolera - jest to funkcja przypisana na stałe do tego wejścia. Kontroler ciągle monitoruje stan zasilania sieciowego i akumulatora. Wszystkie zmiany stanu są raportowane komunikatami wysyłanymi do programu zarządzającego. Są to komunikaty typu: „Zasilanie AC utracone", „Niski poziom zasilania z akumulatora", „Brak zasilania z akumulatora" itp. Wyjścia napięć zasilających są zabezpieczone przed uszkodzeniem na wypadek zwarcia i kontrolowane. Podobnie jest z wyjściami do sterowania zamków.

Do urządzenia zostanie podpięty czytnik kart, elektrozamek, przycisk wyjścia, czujnik magnetyczny (tylko w serwerowni).

Czytnik kart, posiadają zwartą budowę, mają wbudowany czytnik zbliżeniowy i 12 przyciskową klawiaturę dzięki czemu ich możliwość wykorzystania staje się uniwersalna. Posiadają zwartą obudowę pozwalającą na wykorzystanie wewnątrz i na zewnątrz budynku, a także odporną na akty wandalizmu. Typowy zasięg czytnika zbliżeniowego wynosi ok. 16,5 cm , czytnik może być oddalony od kontrolera do 300m, posiadać wbudowany brzęczyk, oraz dwukolorowy wskaźnik LED prezentujący stan zadziałania czytnika.

Instalacja CCTV

Do obserwacji pomieszczeń serwerowni oraz ewentualnie terenu zewnętrznego obiektu projektuje się system monitoringu wizyjnego CCTV w oparciu o technologię TCP IP. System do transmisji sygnałów wizyjnych będzie wykorzystywał okablowanie sieci LAN będącej częścią okablowania strukturalnego obiektu. Okablowanie sieci LAN dla potrzeb CCTV nie jest przedmiotem niniejszego opracowania.

System będzie składał się z następujących elementów:

- Rejestrator sieciowy;
- Urządzenie do przechowywania obrazów z kamer;
- Kamery kopułkowe wewnętrzne z zasilaniem PoE.

Serwer systemu CCTV będzie zainstalowany w serwerowni i będzie posiadał zainstalowane oprogramowanie do obsługi kontrolerów oraz obsługę rejestratora. Kamery podłączone zostaną do przełącznika 100Mbit z zasilaniem PoE znajdujących się w CPD.

Zasilanie gwarantowane

Zasilanie gwarantowane ma za zadanie zabezpieczyć ciągłość działania CPD w przypadku odcięcia zasilania energetycznego z głównej sieci, zapewniając ciągłość działania usług.

W tym celu należy wykonać instalację elektryczną zasilania elektryczną zintegrowaną z instalacją zasilania głównego, UPS-em, wyposażoną w agregat prądotwórczy o mocy 50kVA z układem automatycznego przełączania o mocy umożliwiającej podtrzymanie infrastruktury IT. Agregat powinien być wyposażony w zbiornik paliwa umożliwiający 8-mio godziną pracę agregatu.

2. Architektura sprzętowa

Najważniejszym elementem CPD, tworzącym chmurę obliczeniową dla Powiatu Mikołowskiego będzie infrastruktura wirtualizacyjna oraz sieć LAN w Ośrodku Przetwarzania Danych oparta o wysokowydajne przełączniki pozwalające na osiągnięcie przepustowości 10Gbit/s na każdym porcie.

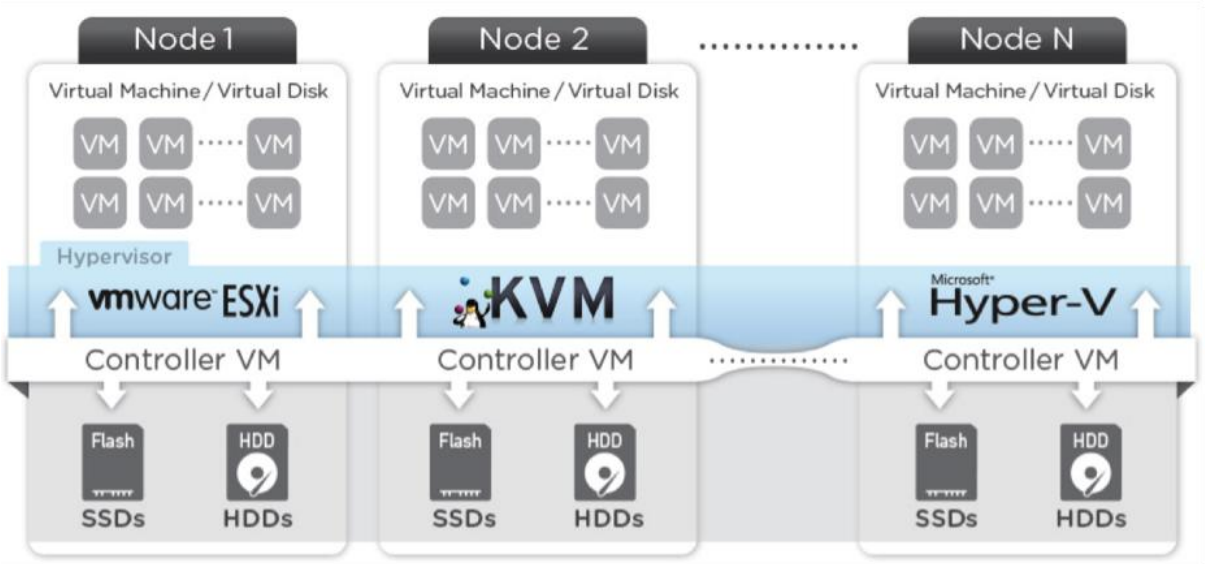
Architektura sprzętowa będzie zapewniała nie tylko wydajność dla istniejących i planowanych e-usług, ale również bezpieczeństwo przetwarzania i przechowywania zgromadzanych danych m.in. zgodnie z wytycznymi KRI oraz systemów ISO27001.

Zastosowane zostanie nowoczesne rozwiązanie HyperConverge. HyperConverge to rodzaj infrastruktury systemowej integrującej za pomocą aplikacji moc obliczeniową, pamięć masową, sieć i zwirtualizowane zasoby w jednym zintegrowanym urządzeniu. W tym nowoczesnym rozwiązaniu nie jest wymagane stosowanie fizycznej macierzy, jest ona wirtualna. Tego typu rozwiązania stosowane są w nowoczesnych ośrodka CPD , np. Google, Facebook, Amazon.

Wirtualizacja serwerów znana jest już od kilku lat, jako rozwiązanie pozwalające na wykorzystanie jednego serwera fizycznego, jako kilku wirtualnych. W przypadku macierzy brak im elastyczności, jeżeli chodzi o ich rozbudowę. Każda macierz ma ograniczone możliwości rozbudowy o konkretną ilość

dysków oraz pamięci czy też procesora, co powoduje, że jeżeli użytkownik „wyrośnie" z danego rozwiązania powinien zakupić nową większą macierz. HyperConwergencja polega na tym, że wirtualizujący wszystkie fizyczne dyski przypisane do danego serwera i tworzymy z nich jedną logiczną macierz zabezpieczoną odpowiednią parzystością danych - **Node**. W przypadku konieczności zwiększenia mocy obliczeniowej i przestrzeni do zapisywania dodajemy do infrastruktury kolejny węzeł **Node**. Administratorzy IT mogą zarządzać środowiskiem wirtualnym z wykorzystaniem polityk opartych na potrzeby każdego obciążenia, zamiast zarządzać indywidualnie LUN-ami, wielkościami lun grupami RAID. Modułowa architektura pozwala w sposób zrównoważony na wzrost wydajności i pojemności, dzięki czemu możemy środowisko szybko i łatwo dostosowywać do dynamicznych, ciągle zmieniających się wymagań.

Rozwiązanie takie w znacznym stopniu upraszcza infrastrukturę obniżając przy tym jej koszty. Poniższy rysunek obrazuje możliwości systemu opartego o przykładowe rozwiązanie DELL XC series, który może być oparty o trzech najbardziej popularnych producentów HyperVisorów: VMware, HyperV oraz KVM. W naszym założeniach wybraliśmy VMware.



Środowisko macierzowo - serwerowe będzie zawierać:

1. Replikację danych;
2. Możliwość wyliczania parzystości pojedynczej / podwójnej;
3. Wydajność do obsługi minimum 100 wirtualnych maszyn;
4. Pojemność 30-40Tb po deduplikacji;

Środowisko sieci Data Center będzie zawierać:

1. Dwa przełączniki 24 portowe 10Gbit/s Ethernet z opóźnieniem max 800ns;
2. Przełączniki będą obsługiwać DCB;

3. Przełączniki będą posiadać porty uplink 40Gbit/s;

Budowa tak zaawansowanego środowiska będzie możliwa przy zastosowaniu urządzeń referencyjnych - Przełącznik N4032F, system HyperConvarge XC630-1, VmwarevSphereCloudSiute Standard

Przełączniki N4032F

Seria N to rodzina energooszczędnych i przystępnych cenowo przełączników 1 GbE i 10 GbE przeznaczonych do modernizowania i skalowania infrastruktury sieciowej. Urządzenia serii N4000 zapewniają uniwersalność połączenia przewodowego z szybkością 10/40 GbE w istniejącej sieci kompleksów biurowych dzięki bardzo wydajnym przełącznikom nieblokującym, które:

- Wykorzystują funkcję MLAG w celu zapewnienia pozbawionej zapętleń nadmiarowości wielu ścieżek bez drzewa rozszerzonego, aby umożliwić pełne wykorzystanie przepustowości i uzyskanie wysokiej dostępności;
- Gwarantują lepszą współpracę przez interfejsy z urządzeniami RPVST+ (Rapid Per VLAN SpanningTree)1 firmy Cisco i urządzeniami wykorzystującymi protokół CDP (Cisco Discovery Protocol);
- Umożliwiają utworzenie bardziej uniwersalnej sieci dzięki obsłudze przez urządzenia najnowszych protokołów o otwartym standardzie;
- Obsługują zaawansowany routing warstwy 3 protokołów IPv4 i IPv6 oraz funkcje zabezpieczeń i skalowania;
- Obsługują sieci zbieżne dla funkcji DCB ze sterowaniem priorytetem przepływu (802.1Qbb), ETS (802.1Qaz), DCBx, obsługa funkcji SCSI TLV.
- Zapewnią konfigurację plug-and-play z macierzami pamięci masowej Dell EqualLogiciSCSI za pomocą jednopoleceniowej konfiguracji iSCSI eliminującej wieloetapową konfigurację i jej potencjalne błędy;

Przełączniki z serii N4000 zostały opracowane z myślą o obniżeniu kosztów operacyjnych, a dzięki technologii FreshAir mogą działać w temperaturze do 113°F (45°C), co pozwala ograniczyć nakłady na chłodzenie. Funkcje powodujące zwiększenie ogólnej wydajności obejmują:

- Dwa wydajne zasilacze wewnętrzne z certyfikatem 80PLUS i funkcją wymiany bez wyłączania systemu;
- Nadmiarowe wentylatory o zmiennej prędkości;
- Energooszczędny interfejs Ethernet i warstwy fizyczne zasilane niskim napięciem ograniczające zużycie energii przez nieaktywne porty i bezczynne połączenia.

Urządzenia Dell Networking serii N4000 są łatwe we wdrożeniu, charakteryzują się wyjątkowymi możliwościami współdziałania, a zarządzanie nimi przez administratorów sieci nie wymaga długich szkoleń. Jedna wersja systemu operacyjnego (Dell Networking OS 6) umożliwia utrzymanie spójnej konfiguracji wszystkich produktów serii N dzięki kompleksowemu zestawowi funkcji, które obejmują:

- Jeden wspólny interfejs wiersza polecenia (CLI) i graficzny interfejs użytkownika (GUI), które wykorzystują dobrze znany język poleceń w celu ułatwienia wykwalifikowanym administratorom szybkiego rozpoczęcia pracy;
- Automatyczną konfigurację przez port USB, która umożliwia administratorom szybkie wdrożenie lustrzanych konfiguracji na wielu urządzeniach po podłączeniu dysku flash USB;
- Wiele funkcji klasy korporacyjnej o znanej i intuicyjnej konfiguracji oraz polecenia zarządzania;
- Najnowsze protokoły o otwartym standardzie i inteligentne technologie integracji, które ułatwiają tworzenie wydajnych sieci złożonych z urządzeń różnych dostawców. Uniwersalna architektura łączenia kaskadowego urządzeń serii N4000 zapewnia wydajną pracę sieci i wysoką gęstość w wymagających środowiskach sieciowych. Ułatwia także przygotowanie sieci do przyszłych inwestycji w przypadku modernizacji sieci przedsiębiorstwa w celu zmiany szybkości z 10 GbE na 40 GbE;
- Szybkość przesyłania danych do 1,28 Tb/s (pełny dupleks) i szybkość przekazywania do 952 Mp/s;
- Łatwe skalowanie dzięki możliwości kaskadowego łączenia portów użytkownika 10/40 Gb/s do wartości 160 Gb/s w przypadku przełącznika N4032 i 320 Gb/s dla przełącznika N4064 (w trybie pełnego dupleksu) na odległość do 100 metrów;
- Do 64 portów 10 GbE działających z prędkością łącza na przełącznik za pomocą kabli rozdzielających i do 672 portów 10 GbE w dwunastu urządzeniach połączonych kaskadowo;
- Moduł rozszerzeń z możliwością wymiany bez wyłączania systemu obsługuje dwa porty QSFP+ (8 x 10 GbE), cztery porty 10 G BaseT i cztery porty SFP+;
- Po kaskadowym połączeniu maksymalnie 12 urządzeń można nimi zarządzać za pomocą uniwersalnej funkcji łączenia kaskadowego portów użytkowników przy szybkości 10 Gb/s lub 40 Gb/s;
- Zestaw ReadyRails niewymagający użycia narzędzi umożliwia szybką instalację przełączników.

Wieczysta gwarancja - ograniczona gwarancja na sprzęt wraz z podstawowym serwisem sprzętu (naprawą lub wymianą) obejmującym wybrane produkty Dell Networking zapewnia ochronę inwestycji przez cały czas posiadania urządzenia.

Ruch standardowy — cechy portów	N4032	N4032F	N4064	N4064F
Cechy portów standardowych	24 porty stałe RJ45 10 GbE z automatycznym wykrywaniem prędkości (10 Gb/1 Gb/100 Mb)	24 porty stałe 10 GbE SFP+ z automatycznym wykrywaniem prędkości (10 Gb/1 Gb)	48 portów stałych RJ45 10 GbE z automatycznym wykrywaniem prędkości (10 Gb/1 Gb/100 Gb)	48 portów stałych 10 GbE SFP+ z automatycznym wykrywaniem prędkości (10 Gb/1 Gb)
Zintegrowane dedykowane porty 40GbE QSFP+	N	N	2	2
Cechy łączenia kaskadowego	**N4032**	**N4032F**	**N4064**	**N4064F**
Maksymalna prędkość łączenia kaskadowego (pełny dupleks)	160 Gb/s	160 Gb/s	320 Gb/s	320 Gb/s
Cechy przełączania	**N4032**	**N4032F**	**N4064**	**N4064F**
Prędkość przełączania struktury (pełny dupleks):	640 Gb/s	640 Gb/s	1,28 Tb/s	1,28 Tb/s
Prędkość przekazywania	476 Mp/s	476 Mp/s	952 Mp/s	952 Mp/s
Obudowa	**N4032**	**N4032F**	**N4064**	**N4064F**
Przybliżona masa w funtach (bez modułów):	21,67	21,14	24,07	23,28
Przybliżona masa w kg (bez modułów):	9,83	9,59	10,92	10,56
Warunki środowiska pracy	**N4032**	**N4032F**	**N4064**	**N4064F**
Maksymalne wydzielanie ciepła (BTU/godz.)	823,44	603,86	1353,53	754,82
Maksymalne zużycie energii (W)	240	176	395	220

System HyperConvarge XC630-1

Oprogramowanie Nutanix zaimplementowane na platformie Dell PowerEdge R630 nosi nazwę produktową XC630-1. Produkt ten posiada zalety serwerów Dell PowerEdge w postaci przejrzystego interfejsu do zarządzania oraz elastycznej platformy serwerowej.

PowerEdge R630 to dwuprocesorowy serwer o wysokości 1U do montażu w szafie serwerowej, który zapewnia bezkonkurencyjną gęstość i wydajność. Model R630 należy do trzynastej generacji

serwerów PowerEdge. Doskonale nadaje się do wirtualizacji oraz obsługi dużych aplikacji biznesowych lub transakcyjnych baz danych.

Sprawna obsługa zadań z dużą liczbą jednoczesnych użytkowników oraz duża częstotliwość dostępu losowego do wszystkich tabel, danych i plików dziennika w przypadku serwera R630 w konfiguracji z samymi dyskami flash SSD.

Serwer R630 oferuje elastyczną, pojemną pamięć masową i wydajne przetwarzanie, umożliwiając szybką obsługę aplikacji. Wyższa wydajność maszyn wirtualnych, w tym krótszy czas reakcji i obsługa większej liczby jednoczesnych użytkowników, dzięki szybkiej pamięci DDR4 oraz lepszej mocy przetwarzania procesorów Intel® Xeon® z serii E5-2600 v3.

Model R630 można skonfigurować, jako niezawodny serwer do obsługi najważniejszych aplikacji biznesowych z funkcjami zautomatyzowanego zarządzania i wysokiej dostępności, takimi jak:

- Zasilacze nadmiarowe (PSU);
- Dyski twarde i zasilacze nadmiarowe z możliwością wymiany bez wyłączania systemu;
- Opcjonalna obsługa dwóch kart SD na potrzeby awaryjnego przełączania monitorów maszyn wirtualnych;

Oprogramowanie NOS – Nutanix

Oprogramowanie Nutanix wprowadza infrastrukturę serwerową w nową erę konwergencji, dotychczas dominująca wirtualizacja serwerów stała się niewystarczająca dla nowych środowisk. Skalowanie oraz utrzymywanie rozwiązań starego typu jest coraz droższe i bardziej skomplikowane co skutkuje częstymi awariami oraz długotrwałymi operacjami migracji danych. Rozwiązanie HyperConverge XCpozwala na zaoszczędzenie czasu oraz zwiększenie dostępności systemów Informatycznych.

Według wymagań osiągnięto następujące przestrzenie dyskowe:

		RAM (TiB)	HDD (TiB)	SSD (TiB)
Raw Capacity	162.72	2.33	72.76	7.28
CVM Overhead	-40.02	-0.15	-0.76	-2.27
Usable Capacity (RAW-Overhead)	122.70	2.18	72.00	5.00
Spare Capacity (Usable-Workload Total)	89.38	1.79	59.06	3.05

% Utilized	45.07	23.18	18.83	58.10

Oraz następujące przestrzenie RACK wraz ze zużyciem prądu i emisją ciepła.

Podstawowe funkcjonalności XC630:

- Wirtualizacja macierzy – pozwala na stworzenie macierzy dyskowej współdzielonej pomiędzy wieloma hostami z lokalnych dysków hostów. Macierz posiada kontroler w postaci wirtualnej maszyny będącej częścią każdego Hosta, tego typu rozwiązanie powoduje, iż przy każdym zwiększeniu ilości hostów zwiększamy wydajność macierzy nie tylko dyskami, ale również procesorem czy też pamięcią. Dodatkowo macierz tego typu posiada nie jeden czy dwa kontrolery a kilka lub nawet kilka set kontrolerów macierzowych, umożliwia to dość zaawansowane balansowanie wydajnością pomiędzy maszynami fizycznymi i wirtualnymi.
- Skalowanie – system taki możemy skalować do setek a nawet tysięcy fizycznych hostów, aktualnie ograniczenia są związane ze stosowaniem HyperVisorów typu VMware czy HyperV jednak w przyszłości Nutanix zamierza uruchomić własny system Acropolis, który zniesie te obostrzenia.
- Zarządzanie – Systemem można zarządzaj z jednego miejsca poprzez czytelne GUI PRISM zbudowane w HTML5 co oznacza iż natywnie obsługuje on REST API do którego możemy odwołać się jakimkolwiek językiem programowania.
- Wirtualizacja Serwerów – Nutanix wpiera HyperV, Vmware oraz KVM a w przyszłości Acropolis oznacza to że możemy mieć wirtualizację dowolnego producenta bez ograniczeń.
- Ochrona Danych – posiada wbudowane rozwiązanie ochrony danych w postaci parzystości oraz replikacji danych do innych lokalizacji. Nutanix opracował metody replikacji do wielu lokalizacji jak również metody replikacji synchronicznej do ośrodków odległych od siebie. Dodatkowo wprowadzone zostało S3 API które umożliwia komunikację z chmurą AZURE lub AMAZON

- Deduplikacja – każde rozwiązanie posiada wbudowaną funkcjonalność deduplikacji danych, która odbywa się po każdym zapisaniu informacji, dzięki czemu możemy zwiększyć użyteczność naszego storage.

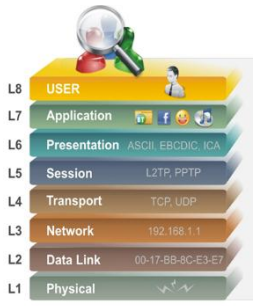
3. Bezpieczeństwo Centrum Przetwarzania Danych

W Data Center będą przechowywane duże ilości danych, które są nie tylko poufne, ale często krytyczne dla funkcjonowania organizacji. Z tego powodu centra danych coraz częściej pojawiają się na celowniku cyberprzestępców. Obecnie włamania do systemów informatycznych oraz kradzież danych przechowywanych w Data Center stały się bardzo dochodowym biznesem. Stąd niezwykle istotne jest zaprojektowanie kompleksowej wielowarstwowej infrastruktury bezpieczeństwa dla sieci i danych w Data Center.

Projektując rozwiązania ochronne dla Data Center należy wziąć pod uwagę aktualne i przyszłe trendy dotyczące przetwarzania i przesyłania danych oraz środowisko w jakim funkcjonują. Wśród tych trendów wyróżniamy: wirtualizację serwerów, pracę w chmurach obliczeniowych i olbrzymią popularyzację urządzeń mobilnych. Trendy te sprawiają, że zapewnienie odpowiedniego bezpieczeństwa sieciom komputerowym staje się coraz bardziej złożone i zaawansowane. Do zagrożeń zewnętrznych takich jak: ataki cyberprzestępców, wirusy, konie trojańskie, spam, coraz częściej dołączają zagrożenia ze strony pracowników organizacji: pobieranie nielegalnych treści i obciążanie łącz internetowych poprzez aplikacje P2P, odwiedzanie niedozwolonych stron internetowych i kradzież danych.

W celu zapewnienia maksymalnego bezpieczeństwa danych w CPD oraz jednostkach korzystających z usług CPD, rozwiązanie zostanie wyposażone w kompleksowy system bezpieczeństwa składający się z wysokowydajnych urządzeń UTM typu NextGeneration Firewall (NGFW) umożliwiających kontrolę do warstwy 7 aplikacyjnej i warstwy 8 kontrola tożsamości. Rozwiązanie zapewni wysoki poziom bezpieczeństwa sieci, połączeń sieciowych, ciągłej dostępności i bezpiecznego zdalnego dostępu z kontrolowanym dostępem do sieci dla mieszkańców, telepracowników, partnerów, klientów. Dostarczone urządzenia UTM będą dostarczały zabezpieczenia klasy korporacyjnej oraz wysoką elastyczność ochrony przed zagrożeniami hybrydowymi, malware, trojany, DoS, DDoS, atakami IP spoofing, spamem, włamaniami i wyciekiem danych. Na jednej platformie sprzętowej dostarczony zostanie szereg modułów ochronnych takich jak:

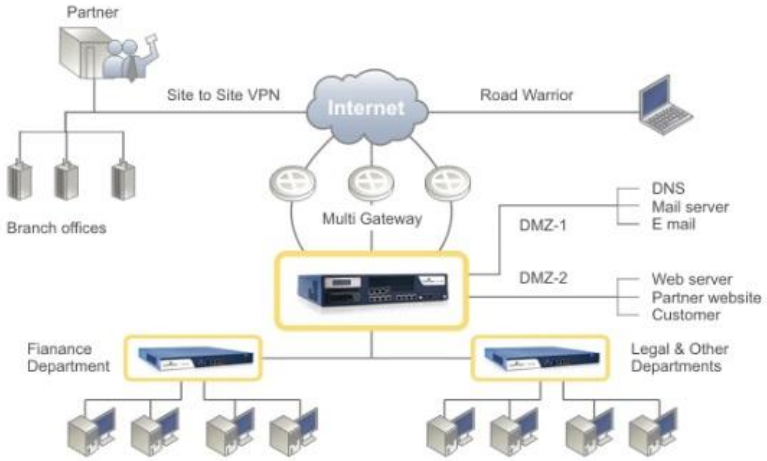
- Firewall;
- VPN (IPSec& SSL VPN);
- IPS;
- Anti-Virus&Anti-Spyware;
- Anti-Spam;
- Web Filtering;
- Zarządzanie pasmem;
- Zarządzanie wieloma łączami.



Celem wdrażania ochrony wielowarstwowej jest minimalizacja ryzyka stania się ofiarą ataku cyberprzestępców i utraty danych. Jeśli jedna warstwa ochrony zostanie przełamana, pozostają kolejne, które wydłużą czas niezbędny do kompletnego włamania do sieci, a często mogą skutecznie zniechęcić atakującego, który poszuka łatwiejszego celu.

Rozwiązanie zapewni zaawansowane bezpieczeństwo sieci zapewniając ciągłość biznesową, szybki uptimes, wysoką przepustowość sieci, szybki rozwój sieci, spełniające wymagania bezpieczeństwa i zgodności regulacyjnych poprzez następujące możliwości:

- Wysoką dostępność w stanowej failover;
- Routing dynamiczny;
- Wiele stref tworzenie grup VLAN opartych na całym profilu zawodowym rozproszonych lokalizacjach;
- Możliwość wirtualnego hosta, umożliwiając bezpieczny hosting usług wewnątrz sieci LAN i DMZ;
- Scentralizowane zarządzanie i logowanie, raportowanie.



Odpowiednio dobrane urządzenia NGFW pozwalają na pełne wykorzystanie infrastruktury sieciowej Data Center o przepustowościach 10 Gb/s oraz bardzo szybkich łącz internetowych, eliminując problem „wąskich gardeł" w sieci.

Konsolidacja wielu funkcji ochronnych w obrębie jednej platformy sprzętowej w rozwiązaniu NGFW niesie ze sobą istotne korzyści finansowe dla Data Center w postaci obniżenia nakładów inwestycyjnych na zakup rozwiązań do zabezpieczania sieci, a następnie kosztów ich utrzymania - mniejsza liczba subskrypcji na licencje ochronne i umów serwisowych.

Rozwiązania NGFW oferują zaadresowanie wielu wyzwań stojących przed Data Center m.in.:

- utrzymanie i wzrost poziomu zaufania klientów i partnerów poprzez skuteczną ochronę sieci przed atakami cyberprzestępców i utrzymanie stałego dostępu do systemów informatycznych;

- utrzymanie ciągłości działania sieci i bezpieczne połączenia zdalne VPN – obsługa łącz internetowych od kilku ISP (dodatkowo modemów 3G/4G/LTE);
- wydajne i szybkie połączenie internetowe – definiowanie polityk QoS i priorytetów dla usług, aplikacji i urządzeń sieciowych;
- zgodność z regulacjami prawnymi - spełnienie założeń standardów, norm i rozporządzeń dotyczących konieczności i zasad ochrony firmowych danych i zasobów.
- wysoka produktywność pracowników - monitoring i kontrola dostępu do stron internetowych np. ograniczenie czasu spędzanego w portalach społecznościowych;
- ułatwienie pracy administratorów sieci, którzy mają do dyspozycji jedną konsolę zarządzającą, mogą szybko konfigurować wszystkie niezbędne reguły bezpieczeństwa.

Celem wdrażania ochrony wielowarstwowej jest minimalizacja ryzyka stania się ofiarą ataku cyberprzestępców i utraty danych. Jeśli jedna warstwa ochrony zostanie przełamana, pozostają kolejne, które wydłużą czas niezbędny do kompletnego włamania do sieci, a często mogą skutecznie zniechęcić atakującego, który poszuka łatwiejszego celu.

Warstwa 1: Ochrona sieci.

Do ochrony sieci Data Center służą moduły: firewall (zapora ogniowa) i IPS.

Firewall ma za zadanie zarządzać dostępem do sieci i jej zasobów, zarówno z zewnątrz, jak i wnętrza organizacji. Administrator dzieli sieć na segmenty definiując na firewall'u odpowiednie strefy i określa do nich prawa dostępu, wykorzystując adresy IP, adresy MAC, nazwy domenowe, nazwy krajów oraz protokoły i usługi. Dodatkowo zapora obsługuje wirtualne sieci lokalne (VLAN), które umożliwiają logiczny podział sieci komputerowej za pomocą przełączników.

Firewall chroni przed atakami sieciowymi takimi jak DoS i DDoS, które poprzez generowanie olbrzymiego ruchu mają za zadanie uniemożliwić dostęp do serwerów i usług hostowanych w Data Center.

Oprócz zapory ogniowej zostanie uruchomiony moduł zapobiegania włamaniom (IPS), który ma za zadanie chronić Data Center przed wykorzystaniem podatności i luk w wykorzystywanych systemach informatycznych w celu włamania do sieci komputerowej. Przykładowo hakerzy mogą próbować wykorzystać luki w powszechnie używanym oprogramowaniu np. Microsoft Windows lub Adobe Acrobat, aby uzyskać nieautoryzowany dostęp do sieci. Ponadto moduł IPS potrafi wykrywać anomalie w protokołach sieciowych i automatyczne zablokowanie podejrzanego ruchu.

Wymagana funkcjonalność dla modułu firewall:

- szyfrowanie komunikacji pomiędzy konsolą zarządzającą a zarządzanymi urządzeniami,
- obsługa wielu stref,
- ograniczanie dostępu na bazie harmonogramu (accessscheduling),
- translacja adresów sieciowych (NAT),
- wsparcie dla VLAN zgodnie z 802.1q,
- ochrona przed atakami DoS i DDoS,

- filtrowanie adresów MAC, IP, ochrona przed IP Spoofingiem,
- kryteria kontroli dostępu: tożsamość użytkownika, strefa źródłowa/docelowa, adresy MAC oraz IP, rodzaj usługi sieciowej.

Wymagana funkcjonalność dla modułu IPS:

- wsparcie dla protokołów: HTTP, FTP, SMTP, POP3, IMAP,
- automatyczne wykrywanie, blokowanie, odrzucanie podejrzanego ruchu,
- własna baza sygnatur,
- tworzenie własnych sygnatur IPS,
- automatyczne aktualizacje.

Warstwa 2: Szyfrowane połączenia z lokalizacjami zdalnymi.

Data Center zostanie połączone bezpiecznymi połączeniami VPN ze wszystkimi lokalizacjami zdalnymi (59). Dane między Data Center a lokalizacjami zdalnymi będą przesyłane w szyfrowanych tunelach, które będą zapewniać ich poufność i integralność.

Przy wykorzystaniu drugiego lub większej liczby łącz internetowych będzie możliwe uruchomienie mechanizmu VPN failover. W przypadku niedostępności jednego z łącz, tunel VPN zostanie automatycznie połączony przy wykorzystaniu kolejnego dostępnego łącza.

Wymagana funkcjonalność dla modułu VPN:

- obsługa protokołów: IPSec VPN, SSL VPN,
- uwierzytelnianie przez współdzielony klucz (PSK) lub z użyciem certyfikatów cyfrowych,
- wsparcie dla: IPSec NAT Traversal, Dead Peer Detection,
- redundancja tuneli VPN,
- wsparcie dla połączeń typu hub & spoke.

Warstwa 3: Ochrona aplikacji webowych.

Serwery webowe, które posiadają dostęp do Internetu będą chronione za pomocą modułu Web Application Firewall (WAF). Będzie on przechwytywał ruch przychodzący (żądania) i wychodzący (odpowiedzi) z serwerów webowych, działając jako reverseproxy i zapewniając ochronę przed atakami.

Wymagana funkcjonalność dla modułu WAF:

- W zakresie zabezpieczania aplikacji webowych (Web Application Firewall) ochrona przed atakami:
    - Brute Force,
    - CookiePoisoning,

- SQL injection,
- Cross-sitescripting (XSS),
- Bufferoverrun,
- wymienionymi na liście Top 10 organizacji OWASP.

Warstwa 4: Ciągłość działania.

Urządzenia NGFW w Data Center będą pracować w klastrze wysokiej dostępności (HA) w trybie Active-Active. W przypadku awarii jednego z nich, drugie urządzenie automatycznie przejmie wszystkie funkcje ochronne.

Urządzenia będą oferować funkcjonalność link failover i loadbalancing. Można wykorzystać łącza internetowe od kilku dostawców (ISP), aby zapewnić nieprzerwany dostęp do sieci Internet. Administrator może uruchomić mechanizm loadbalancingu i kierować wybrany ruch na jedno z kilku posiadanych łącz.

Wymagana funkcjonalność dla urządzenia NGFW:

- obsługa loadbalancing i failover dla przynajmniej 3 łącz internetowych
- powiadomienie o zmianie statusu urządzenia (w postaci wiadomości e-mail)
- wsparcie dla dowolnych modemów 3G/4G/LTE podłączanych poprzez port USB
- praca w klastrze active-active.
- szyfrowanie ruchu pomiędzy dwoma urządzeniami w klastrze
- automatyczna i ręczna synchronizacja urządzeń w klastrze.

Warstwa 5: Tożsamość użytkowników.

Aspekt uwierzytelniania użytkowników w sieci jest niezwykle istotny dla utrzymania odpowiedniego poziomu bezpieczeństwa. Administratorzy i użytkownicy muszą podać przynajmniej nazwę użytkownika (login) i poprawne hasło, aby otrzymać dostęp do ściśle określonych zasobów sieciowych. Dzięki temu można przydzielać prawa dostępu do sieci w zależności od wykonywanych obowiązków zawodowych, a także gromadzić szczegółowe dane dotyczące działań użytkowników na potrzeby raportowania i audytów.

Wymagana funkcjonalność dla modułu uwierzytelniania użytkowników:

- obsługa protokołów: IPSec VPN, SSL VPN,
- wbudowana baza lokalna,
- integracja z Active Directory (AD), LDAP lub RADIUS,
- wsparcie dla Windows Single Sign On,
- wsparcie dla cienkich klientów (Microsoft i Citrix).

Warstwa 6: Audyt i raportowanie.

Oprócz rozwiązań zabezpieczających istotnym elementem infrastruktury sieciowej są narzędzia do zbierania logów i generowania raportów dotyczących zdarzeń w chronionej sieci. Pokazują próby włamań, wykryte wirusy i spam, pozwalają na monitoring uruchamianych aplikacji sieciowych, przeglądanych stron www, zużycia łącz internetowych, ilość pobieranych danych.

Moduły raportowania są niezwykle istotne dla korelacji informacji zebranych z różnych źródeł. Przykładowo analizując informacje z modułu IPS i modułu filtrowania treści, operator może uzyskać informacje o próbach ataku, aplikacjach wykorzystywanych podczas ataków i konkretnych podatnościach tych aplikacji, które nie zostały jeszcze „załatane" przez producenta. Pozwala to na podejmowanie działaniach proaktywnych i bardziej precyzyjną konfigurację posiadanych systemów bezpieczeństwa.

Na podstawie informacji o aktualnym i historycznym wykorzystaniu łącz internetowych oraz dostępności bram sieciowych operator może wnioskować o zwiększenie przepustowości wykorzystywanego łącza, zakup nowego łącza, uruchomienie łącza backupowego lub zablokowanie dostępu do wybranych aplikacji sieciowych. Dzięki temu wzrasta wydajność sieci i możliwe staje się zagwarantowanie dostępności wszystkich usług dla organizacji.

Logi zbierane przez urządzenia zabezpieczające są wykorzystywane do tworzenia raportów dla kierownictwa, które wymaga cyklicznych audytów stanu bezpieczeństwa sieci.

Wymagana funkcjonalność dla modułu raportowania:

- składowanie oraz archiwizacja logów
- gromadzenie informacji o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać je z nazwami użytkowników
- monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników
- przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących
- eksport raportów do plików HTML i PDF
- eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych)
- wysyłanie raportów na pocztę elektroniczną
- wsparcie dla kilku serwerów syslog (przynajmniej 3)

Warstwa 7: Centralne zarządzanie.

System (konsola) do centralnego zarządzania

W Data Center zostanie wdrożone rozwiązanie, które umożliwi centralne zarządzanie urządzeniami wdrożonymi we wszystkich lokalizacjach zdalnych, redukując koszty operacyjne związane z utrzymaniem w nich niezbędnego poziomu bezpieczeństwa.

Zarządzanie bezpieczeństwem – natychmiastowa implementacja polityk bezpieczeństwa

System do centralnego zarządzania upraszcza proces zarządzenia bezpieczeństwem sieci, umożliwiając centralne tworzenie oraz implementację polityk bezpieczeństwa, odnawianie licencji oraz aktualizację oprogramowania (firmware) dla urządzeń NGFW zainstalowanych w lokalizacjach zdalnych. Dotyczy to wszystkich funkcjonalności urządzeń NGFW m.in. firewall, VPN, IPS, filtrowanie stron www, kontrola aplikacji sieciowych, antywirus, antyspam, QoS.

Elastyczność zarządzania

Konsola do centralnego zarządzania umożliwia administratorowi elastyczne grupowanie urządzeń NGFW zainstalowanych w oddziałach. Grupy mogą być tworzone na podstawie lokalizacji geograficznej urządzeń, modeli lub wersji oprogramowania.

Grupowanie urządzeń znacznie usprawnia i przyspiesza proces zarządzania nimi. Graficzny interfejs użytkownika oferuje dynamiczne widoki, które upraszczają zarządzanie, wyszukiwanie oraz sortowanie urządzeń. Administrator ma możliwość tworzenia indywidualnych paneli zarządzania dedykowanych dla konkretnych grup urządzeń, dzięki którym możliwe jest szybkie monitorowanie stanu bezpieczeństwa sieci i podejmowanie odpowiednich działań.

Logi audytowe i alerty

Konsola wyświetla logi i podgląd działań administracyjnych zarówno dla systemu do centralnego zarządzania, jak i pojedynczych urządzeń NGFW. Możliwe jest zdefiniowanie powiadomień e-mail na podstawie daty wygasania subskrypcji dla danego modułu, nadmiernego zużycia przestrzeni dyskowej, liczby wykrytych zagrożeń (próby włamań i wirusy), połączeń z niebezpiecznymi witrynami internetowymi oraz innych parametrów.

Wymagana funkcjonalność dla konsoli do centralnego zarządzania

Architektura

- szyfrowanie komunikacji pomiędzy konsolą zarządzającą a zarządzanymi urządzeniami
- administracja poprzez bezpieczne kanały komunikacji: HTTPS i SSH
- aktualizacja polityk na zarządzanych urządzeniach w czasie rzeczywistym
- automatyczne wykrywanie nowych urządzeń

Centralne repozytorium konfiguracji

- centralne repozytorium konfiguracji do przechowywania kopii zapasowych konfiguracji wszystkich zarządzanych urządzeń
- przechowywanie do 5 kopii zapasowych konfiguracji zarządzanych urządzeń
- możliwość ustawienia określonej kopii zapasowej konfiguracji jako ostatnia znana poprawna konfiguracja
- tworzenie kopii zapasowej swojej własnej konfiguracji wg zdefiniowanych harmonogramów lokalnie oraz przez FTP i email

Centralne zarządzanie

- tworzenie różnych ról administracyjnych
- grupowanie urządzeń w oparciu o minimum następujące kryteria: lokalizację geograficzną, firmę/dział, wersję firmware i model urządzenia
- kontrola dostępu w oparciu o lokalną bazę, a także Radius, LDAP i Active Directory
- tworzenie, edycja, usuwanie polityk na firewallu. Polityki mogą być wysyłane do pojedynczych urządzeń, grup lub wszystkich urządzeń
- konfiguracja i synchronizacja polityk antywirusowych i antyspamowych na zarządzanych urządzeniach
- tworzenie/edycja/usuwanie polityk filtra treści (www i aplikacji sieciowych)
- praca jako serwer do dystrybucji aktualizacji sygnatur (antywirus, filtrowanie treści, IPS) oraz firmware

Centralny monitoring

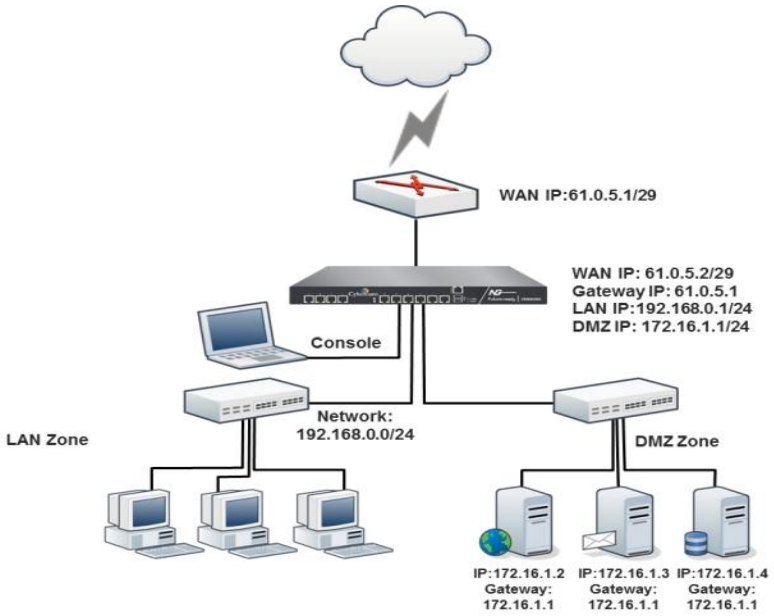
- zbieranie logów audytowych dotyczących:
    - wszystkich zmian konfiguracji wykonanych przez lokalnych administratorów bezpośrednio na urządzeniu
    - wszystkich zmian konfiguracji wykonanych przez centralnego administratora przy użyciu systemu do centralnego zarządzania.

Główny węzeł CPD zostanie wyposażony w dwa urządzenia o wysokiej wydajności pracujące w trybie wysokiej dostępności (HA), pozwalające na bezpieczne połączenia tunelami IPSec VPN (site to site) z jednostkami wyposażonymi w pojedyncze urządzenia o mniejszej wydajności.

Dostarczony system bezpieczeństwa będzie zapewniać wszystkie funkcjonalności i parametry wymienione w minimalnych wymaganiach dla systemu bezpieczeństwa niezależnie od dostawcy łącza.

Elementy wchodzące w skład systemu bezpieczeństwa służące do aktywnej ochrony oraz centralnego zarządzania będą zrealizowane w postaci zamkniętej platformy sprzętowej posiadającej certyfikaty ICSA lub EAL4 – dla funkcjonalności Firewall oraz ICSA lub Checkmark – dla wszystkich wymienionych funkcjonalności: IPS, VPN, antywirus.

Całość rozwiązania będzie mogła być zarządzana z jednego miejsca.



System bezpieczeństwa będzie:

1. Zapewniać aktywną ochronę sieci w Data Center i Oddziałach. Przy czym aktywna ochrona w każdej lokalizacji musi być zapewniana nawet w przypadku braku łączności z Data Center.
2. Umożliwiać podłączenie nielimitowanej liczby hostów i użytkowników.
3. Umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Mechanizmu typu Single Sign On w środowisku Active Directory.
4. W ramach zarządzania:
   - Umożliwiać tworzenie kont administracyjnych o różnych uprawnieniach.
   - Automatycznie wylogować administratora po określonym czasie bezczynności.
   - Umożliwiać określanie złożoności polityk hasłowych dla administratorów.
   - Wspierać SNMP v1, v2 i v3.
   - Monitorować na bieżąco stan urządzenia (obciążenie interfejsów sieciowych, CPU, pamięć RAM).
   - Przechowywać przynajmniej dwie wersji firmware.
   - Wykonywać automatycznie kopie zapasowe konfiguracji systemu.
5. Posiadać system (konsolę) do centralnego zarządzania urządzeniami do aktywnej ochrony znajdującymi się w Oddziałach.
6. Być wyposażony w moduł logowania zdarzeń i raportowania, który gromadzi informacje o zdarzeniach dotyczących protokołów www, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz pozwala na powiązanie tych zdarzeń z nazwami użytkowników.

7. Posiadać certyfikat ISO 15408/CommonCriteria na poziomie EAL 4+. Do oferty należy dołączyć kopię certyfikatu.

System bezpieczeństwa w CPD

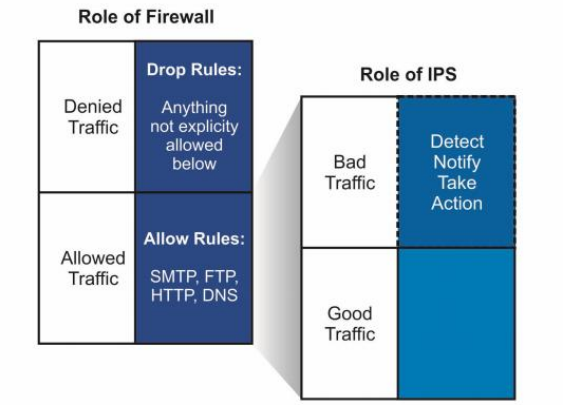
Firewall.

Firewall ma za zadanie zarządzać dostępem do infrastruktury sieciowej Data Center i jej zasobów, zarówno z zewnątrz, jak i wnętrza organizacji. Administrator dzieli sieć na segmenty definiując na firewall'u odpowiednie strefy i określa do nich prawa dostępu, wykorzystując adresy IP, adresy MAC, nazwy domenowe, nazwy krajów oraz protokoły i usługi. Dodatkowo zapora obsługuje wirtualne sieci lokalne (VLAN), które umożliwiają logiczny podział sieci komputerowej za pomocą przełączników.

Wymagania.

Urządzenia w zakresie funkcjonalności firewall będą zapewniać:

1. Indywidualną konfigurację każdego fizycznego portu Ethernet jako strefy: LAN, WAN lub DMZ.
2. Wsparcie dla VLAN zgodnie z 802.1q
3. Tworzenie reguł firewallowych w oparciu o: każdą ze stref (LAN, WAN, DMZ, VPN, VLAN), adresy IP, adresy MAC, lokalizację geograficzną na poziomie państw np. Iran, Irak, usługi, protokoły, harmonogramy czasowe, nazwy użytkowników, nazwy grup użytkowników.
4. Firewall kontrolujący wszystkie połączenia przychodzące i wychodzące ze stref LAN, WAN, DMZ, VPN, VLAN.
5. Wbudowany analizator ruchu (sniffer).
6. Kształtowanie pasma (QoS): określanie priorytetów i poziomu pasma dla konkretnego użytkownika, na poziomie reguły firewallowej, dla kategorii stron www oraz konkretnej aplikacji.
7. Konfigurator reguł, który pozwala na niezależne włączanie/wyłączanie ochrony dla modułów: antywirus, filtr webowy, filtr aplikacyjny, IPS, pasmo QoS.



Firewall i IPS jako kolejne warstwy ochrony.

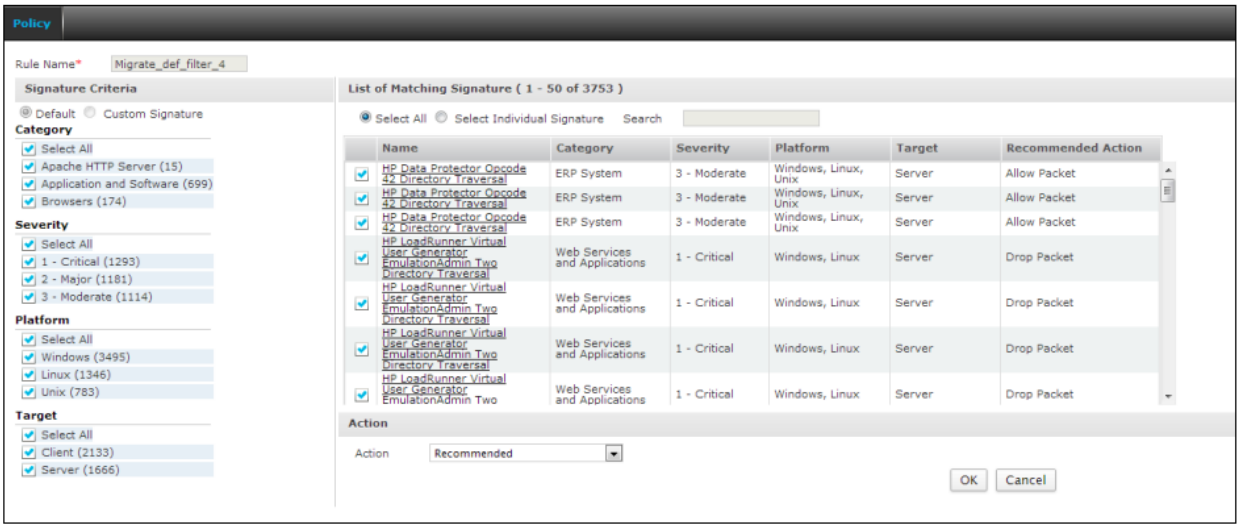
IPS.

Oprócz zapory ogniowej zostanie uruchomiony moduł zapobiegania włamaniom (IPS), który ma za zadanie chronić Data Center przed wykorzystaniem podatności i luk w wykorzystywanych systemach informatycznych w celu włamania do sieci komputerowej. Przykładowo hakerzy mogą próbować wykorzystać luki w powszechnie używanym oprogramowaniu np. Microsoft Windows lub Adobe Acrobat, aby uzyskać nieautoryzowany dostęp do sieci. Ponadto moduł IPS potrafi wykrywać anomalie w protokołach sieciowych i automatyczne zablokować podejrzany ruch (np. ataki typu DoS/DDoS).

Wymagania.

Urządzenia w zakresie funkcjonalności IPS będą:

1. Wspierać protokoły: HTTP, FTP, SMTP, POP3, IMAP w zakresie ochrony IPS.
2. Opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać, co najmniej 4000 wpisów.
3. Pozwalać na definiowanie własnych wyjątków lub sygnatur.
4. Wykrywać anomalie protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
5. Pozwalać administratorowi na włączanie i wyłączanie określonych sygnatur w celu zminimalizowania opóźnień w przesyłaniu pakietów.
6. Generować alerty w przypadku prób ataków.



Wybrane sygnatury w module IPS.

Szyfrowane połączenia z oddziałami (VPN).

Data Center zostanie połączone bezpiecznymi połączeniami VPN ze wszystkimi oddziałami (59 lokalizacji). Dane między Data Center a oddziałami będą przesyłane w szyfrowanych tunelach, które będą zapewniać ich poufność i integralność.

Przy wykorzystaniu drugiego lub większej liczby łącz internetowych będzie możliwe uruchomienie mechanizmu VPN failover. W przypadku niedostępności jednego z łącz, tunel VPN zostanie automatycznie połączony przy wykorzystaniu kolejnego dostępnego łącza.

Wymagania.

Urządzenia w zakresie funkcjonalności VPN będą:

1. Pozwalać na zestawianie połączeń w topologii IPSec: Site-to-site oraz Client-to-site, L2TP, PP2P, SSL VPN.
2. Monitorować stan tuneli VPN i stale utrzymywać ich aktywność.
3. Pracować w topologii Hub and Spoke.
4. Obsługiwać mechanizmy: IPSec NAT Traversal, DPD.
5. Posiadać wbudowane centrum certyfikacji (CA).
6. Umożliwiać wykorzystywanie zewnętrznych centrów certyfikacji (CA).
7. Pozwalać na wykorzystanie klientów IPSec VPN innych niż pochodzących od producenta urządzenia.
8. Umożliwiać zarządzanie pasmem przy połączeniach VPN.
9. Umożliwiać zestawianie tuneli SSL VPN poprzez przeglądarkę internetową oraz dedykowanego klienta. Korzystanie z SSL VPN musi być możliwe bez zakupu dodatkowej licencji.
10. Zapewniać ochronę antywirusową tuneli VPN.

Ochrona aplikacji webowych (WAF).

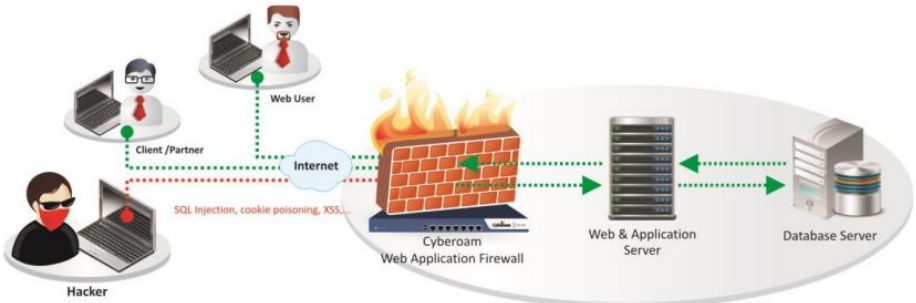
Serwery webowe, które posiadają dostęp do Internetu będą chronione za pomocą modułu Web Application Firewall (WAF). Będzie on przechwytywał ruch przychodzący (żądania) i wychodzący (odpowiedzi) z serwerów webowych, działając jako reverseproxy i zapewniając ochronę przed atakami.

Wymagania.

Urządzenia w zakresie funkcjonalności WAF będą zapewniać ochronę przed atakami:

- Brute Force
- CookiePoisoning
- SQL injection

- Cross-sitescripting (XSS)
- Bufferoverrun
- wymienionymi na liście Top 10 organizacji OWASP



Schemat działania modułu Web Application Firewall (WAF).

Ochrona antywirusowa.

System bezpieczeństwa w Data Center będzie posiadał moduł ochrony antywirusowej. Wbudowany antywirus będzie skanował, wykrywał i usuwał kod złośliwy podczas transmisji danych przez protokoły sieciowe.

Wymagania.

Urządzenia w zakresie funkcjonalności antywirus będą:

- Skanować następuje protokoły: SMTP, POP3, IMAP, FTP, HTTP, HTTPS.
- Automatycznie aktualizować bazę sygnatur nie rzadziej niż raz w ciągu godziny i umożliwiać ręczne aktualizacje.
- Umożliwiać dodawanie podpisu/stopki do wiadomości email.
- Oferować moduł kwarantanny z możliwością samoobsługi przez użytkowników.

Kontrola aplikacji sieciowych.

System bezpieczeństwa będzie posiadał moduł służący do głębokiej analizy pakietów (tzw. Deep Packet Inspection). Dzięki temu będzie możliwe rozpoznawanie, monitoring i kontrola aplikacji sieciowych uruchamianych przez użytkowników np. proxy lub peer-to-peer. Każda z rozpoznanych aplikacji będzie sklasyfikowana pod kątem ryzyka dla bezpieczeństwa sieci, które wiąże się z jej uruchamianiem

Wymagania.

Urządzenia w zakresie funkcjonalności filtra aplikacji będą:

- Kontrolować ruch na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Posiadać bazę co najmniej 2000 aplikacji.
- Blokować komunikatory internetowe przynajmniej: GG (dawne Gadu-Gadu) w wersji klienckiej i webowej, Skype, Gmail Web Chat, Facebook Chat).
- Blokować media strumieniowe przynajmniej: YouTube, Vimeo, radio internetowe.
- Blokować uruchamianie aplikacji i gier w serwisie Facebook.
- Blokować aplikacje proxy przynajmniej: TOR, Ultrasurf, JAP.
- Blokować aplikacje P2P przynajmniej: Gnutella, BitTorrent, uTorrent, eMule.
- Przydzielać polityki QoS dla kategorii aplikacji np. komunikatory i dla konkretnej aplikacji np. Skype.

System (konsola) do centralnego zarządzania.

W Data Center zostanie wdrożone rozwiązanie, które umożliwi centralne zarządzanie urządzeniami wdrożonymi we wszystkich lokalizacjach zdalnych, redukując koszty operacyjne związane z utrzymaniem w nich niezbędnego poziomu bezpieczeństwa.

System do centralnego zarządzania upraszcza proces zarządzenia bezpieczeństwem sieci, umożliwiając centralne tworzenie oraz implementację polityk bezpieczeństwa, odnawianie licencji oraz aktualizację oprogramowania (firmware) dla urządzeń NGFW zainstalowanych w lokalizacjach zdalnych. Dotyczy to wszystkich funkcjonalności urządzeń NGFW m.in. firewall, VPN, IPS, filtrowanie stron www, kontrola aplikacji sieciowych, antywirus, antyspam, QoS.

Konsola do centralnego zarządzania umożliwia administratorowi elastyczne grupowanie urządzeń NGFW zainstalowanych w oddziałach. Grupy mogą być tworzone na podstawie lokalizacji geograficznej urządzeń, modeli lub wersji oprogramowania.

Grupowanie urządzeń znacznie usprawnia i przyspiesza proces zarządzania nimi. Graficzny interfejs użytkownika oferuje dynamiczne widoki, które upraszczają zarządzanie, wyszukiwanie oraz sortowanie urządzeń. Administrator ma możliwość tworzenia indywidualnych paneli zarządzania dedykowanych dla konkretnych grup urządzeń, dzięki którym możliwe jest szybkie monitorowanie stanu bezpieczeństwa sieci i podejmowanie odpowiednich działań.

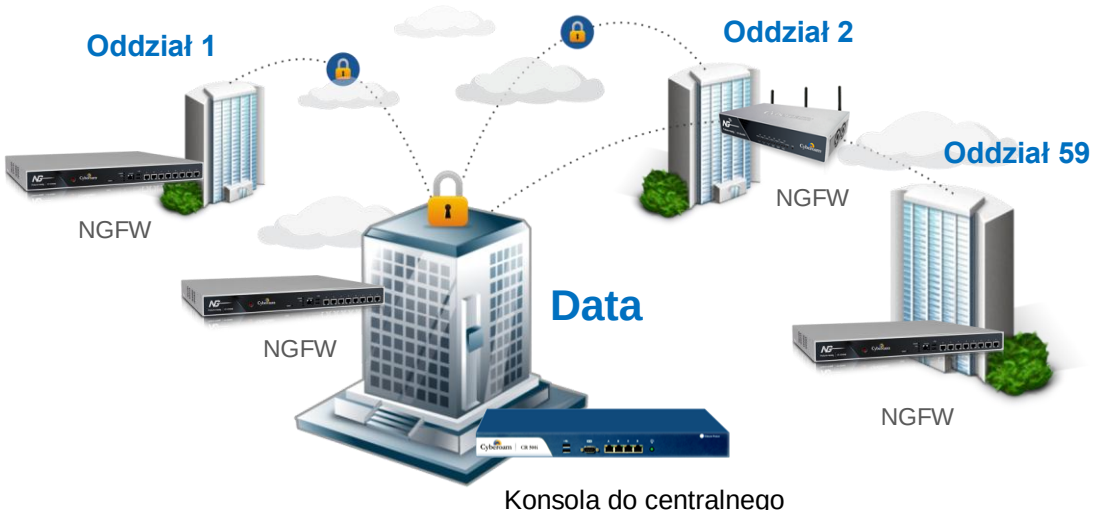
Wymagania.

System centralnego zarządzania musi zostać dostarczony w postaci urządzenia lub maszyny wirtualnej dedykowanego do zarządzania urządzeniami do aktywnej ochrony i pochodzącego od tego samego producenta, co pozostałe elementy systemu bezpieczeństwa.

System centralnego zarządzania musi umożliwiać zarządzanie minimum 65 urządzeniami do aktywnej ochrony wchodzącymi w skład systemu bezpieczeństwa.

Rozwiązanie (urządzenie lub maszyna wirtualna) do centralnego zarządzania będzie:

1. Posiadać centralne repozytorium konfiguracji służące do przechowywania kopii zapasowych konfiguracji wszystkich zarządzanych urządzeń i zapewniające co najmniej:
   - Przechowywanie do 5 kopii zapasowych konfiguracji zarządzanych urządzeń.
   - Możliwość ustawienia określonej kopii zapasowej konfiguracji jako ostatnia znana poprawna konfiguracja.
   - Tworzenie kopii zapasowej swojej własnej konfiguracji lokalnie oraz przez FTP i email.
2. Szyfrować komunikację pomiędzy konsolą zarządzającą a zarządzanymi urządzeniami.
3. Umożliwiać administrację poprzez bezpieczne kanały komunikacji: HTTPS i SSH.
4. Oferować aktualizację polityk konfiguracyjnych na zarządzanych urządzeniach w czasie rzeczywistym.
5. Umożliwiać automatyczne wykrywanie nowych urządzeń.
6. Zawierać wbudowane narzędzie diagnostyczne.
7. Posiadać graficzny interfejs do zarządzania.
8. Posiadać możliwość aktualizacji swojego firmware.
9. Posiadać opcję posiadania redundantnego firmware.
10. Umożliwiać tworzenie różnych ról administracyjnych.
11. Umożliwiać grupowanie urządzeń w oparciu o minimum następujące kryteria: lokalizację geograficzną, wersję firmware i model urządzenia.
12. Wspierać kontrolę dostępu w oparciu o lokalną bazę, a także Radius, LDAP i Active Directory.



Konsola do centralnego

Przykład zastosowania konsoli do centralnego zarządzania.

13. Wspierać centralne tworzenie/edycję/usuwanie obiektów takich jak: hosty, strefy, interfejsy.
14. Umożliwiać centralne tworzenie, edycję, usuwanie polityk na urządzeniach do aktywnej ochrony w zakresie:

- VPN
- IPS
- antywirus
- filtra webowego
- filtra aplikacyjnego

15. Umożliwiać tworzenie szablonów ustawień i egzekwować zmiany tych samych ustawień na dowolnej ilości urządzeń wchodzących w skład systemu bezpieczeństwa.
16. Oferowane rozwiązanie powinno umożliwiać pracę jako serwer do dystrybucji aktualizacji sygnatur (antywirus, filtr webowy, filtr aplikacyjny, IPS) oraz firmware.
17. Wspierać zbieranie logów audytowych dotyczących:
    - wszystkie zmiany konfiguracji wykonane przez lokalnych administratorów bezpośrednio na urządzeniu
    - wszystkie zmiany konfiguracji wykonane przez centralnego administratora przy użyciu systemu do centralnego zarządzania.

Logowanie zdarzeń i raportowanie.

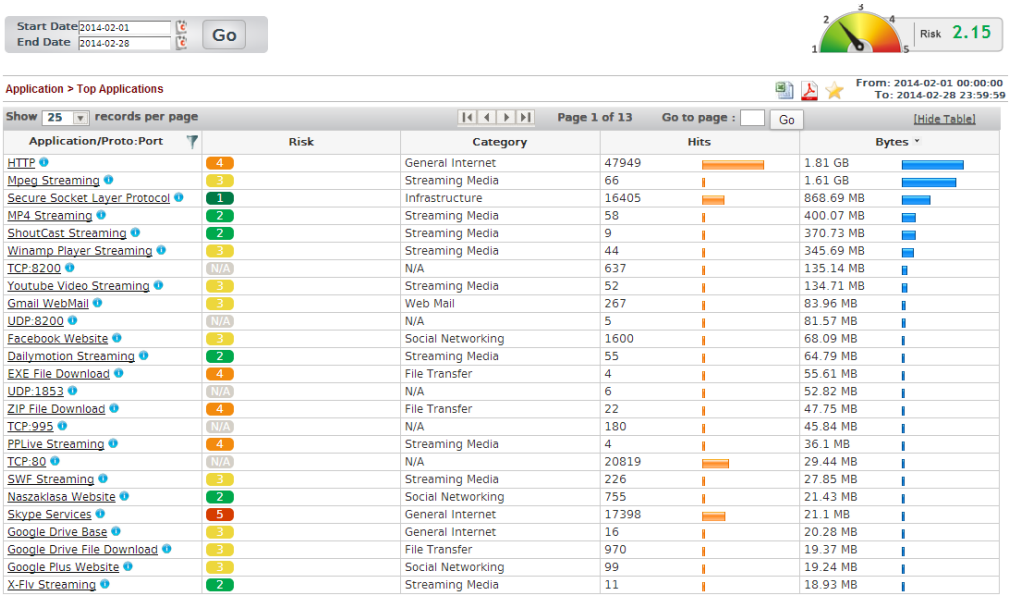
Oprócz rozwiązań zabezpieczających istotnym elementem infrastruktury sieciowej są narzędzia do zbierania logów i generowania raportów dotyczących zdarzeń w chronionej sieci. Pokazują próby włamań, wykryte wirusy i spam, pozwalają na monitoring uruchamianych aplikacji sieciowych, przeglądanych stron www, zużycia łącz internetowych, ilość pobieranych danych.

Moduły raportowania są niezwykle istotne dla korelacji informacji zebranych z różnych źródeł. Przykładowo analizując informacje z modułu IPS i modułu filtrowania treści, operator może uzyskać informacje o próbach ataku, aplikacjach wykorzystywanych podczas ataków i konkretnych podatnościach tych aplikacji, które nie zostały jeszcze „załatane" przez producenta. Pozwala to na podejmowanie działaniach proaktywnych i bardziej precyzyjną konfigurację posiadanych systemów bezpieczeństwa.

Na podstawie informacji o aktualnym i historycznym wykorzystaniu łącz internetowych oraz dostępności bram sieciowych operator może wnioskować o zwiększenie przepustowości wykorzystywanego łącza, zakup nowego łącza, uruchomienie łącza backupowego lub zablokowanie dostępu do wybranych aplikacji sieciowych. Dzięki temu wzrasta wydajność sieci i możliwe staje się zagwarantowanie dostępności wszystkich usług dla organizacji.

Logi zbierane przez urządzenia zabezpieczające są wykorzystywane do tworzenia raportów dla kierownictwa, które wymaga cyklicznych audytów stanu bezpieczeństwa sieci.

System bezpieczeństwa musi zawierać moduł logowania zdarzeń i raportowania. Moduł logowania i raportowania może być zrealizowany w postaci wbudowanego modułu w urządzeniach do ochrony sieci lub dedykowanej zamkniętej platformy sprzętowej lub dedykowanego oprogramowania pochodzącego od tego samego producenta co pozostałe elementy systemu bezpieczeństwa.



Start Date 2014-02-01
End Date 2014-02-28
Go

Risk 2.15

Application > Top Applications

From: 2014-02-01 00:00:00
To: 2014-02-28 23:59:59

Show 25 records per page — Page 1 of 13 — Go to page : Go — [Hide Table]

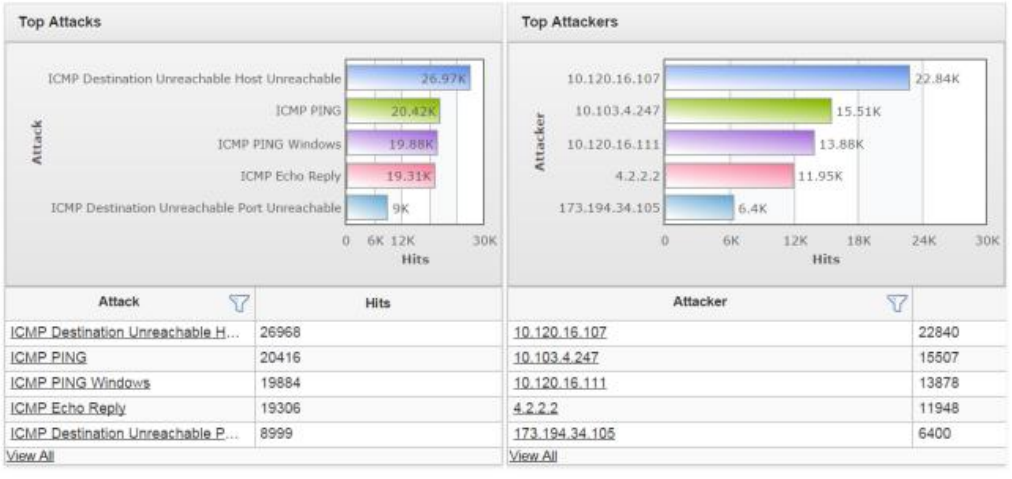
Application/Proto:Port	Risk	Category	Hits	Bytes
HTTP	4	General Internet	47949	1.81 GB
Mpeg Streaming	3	Streaming Media	66	1.61 GB
Secure Socket Layer Protocol	1	Infrastructure	16405	868.69 MB
MP4 Streaming	2	Streaming Media	58	400.07 MB
ShoutCast Streaming	2	Streaming Media	9	370.73 MB
Winamp Player Streaming	3	Streaming Media	44	345.69 MB
TCP:8200	N/A	N/A	637	135.14 MB
Youtube Video Streaming	3	Streaming Media	52	134.71 MB
Gmail WebMail	3	Web Mail	267	83.96 MB
UDP:8200	N/A	N/A	5	81.57 MB
Facebook Website	3	Social Networking	1600	68.09 MB
Dailymotion Streaming	2	Streaming Media	55	64.79 MB
EXE File Download	4	File Transfer	4	55.61 MB
UDP:1853	N/A	N/A	6	52.82 MB
ZIP File Download	4	File Transfer	22	47.75 MB
TCP:995	N/A	N/A	180	45.84 MB
PPLive Streaming	4	Streaming Media	4	36.1 MB
TCP:80	N/A	N/A	20819	29.44 MB
SWF Streaming	3	Streaming Media	226	27.85 MB
Naszaklasa Website	2	Social Networking	755	21.43 MB
Skype Services	5	General Internet	17398	21.1 MB
Google Drive Base	3	General Internet	16	20.28 MB
Google Drive File Download	3	File Transfer	970	19.37 MB
Google Plus Website	3	Social Networking	99	19.24 MB
X-Fly Streaming	2	Streaming Media	11	18.93 MB

Przykładowy raport: monitoring ryzyka aplikacji sieciowych.

Wymagania.

W ramach modułu raportowania system będzie zapewniać:

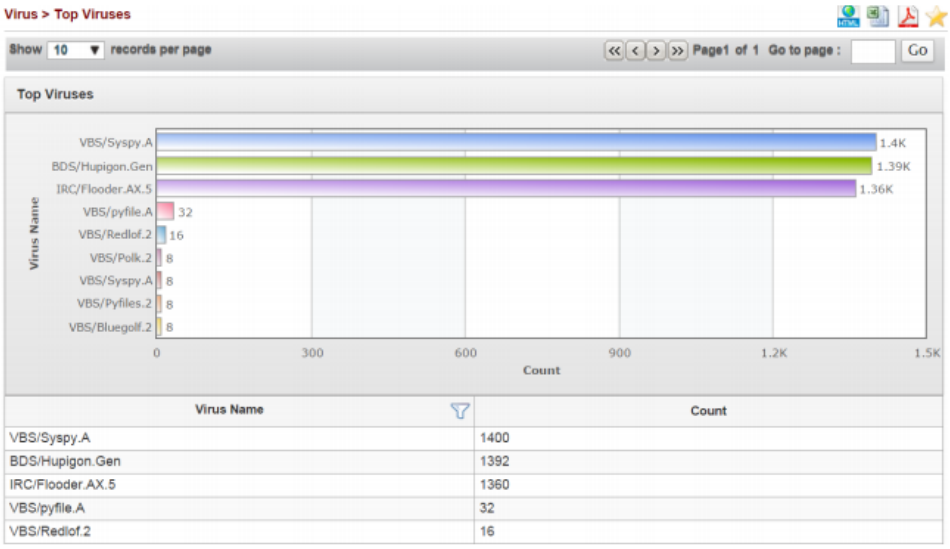
- Gromadzenie, przechowywanie oraz archiwizację logów.
- Gromadzenie informacji o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych.
- Monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. poprzez wykorzystanie skali.
- Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
- Eksport raportów do plików PDF i xls, wysyłanie raportów (PDF) na pocztę elektroniczną.
- Eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).



Attack	Hits
ICMP Destination Unreachable H...	26968
ICMP PING	20416
ICMP PING Windows	19884
ICMP Echo Reply	19306
ICMP Destination Unreachable P...	8999
View All	

Attacker	
10.120.16.107	22840
10.103.4.247	15507
10.120.16.111	13878
4.2.2.2	11948
173.194.34.105	6400
View All	

Przykładowy raport: wykryte ataki i ich pochodzenie.



Virus Name	Count
VBS/Syspy.A	1400
BDS/Hupigon.Gen	1392
IRC/Flooder.AX.5	1360
VBS/pyfile.A	32
VBS/Redlof.2	16

Urządzenia wyposażone w 8 interfejsów miedzianych Gigabit Ethernet 10/100/1000 oraz 4 interfejsy 10 GbE SFP+ będą zapewniać:

- Przepustowość Firewall – 25 Gbps.
- Wydajność skanowania ruchu w celu ochrony przed atakami IPS – 8 Gbps.
- Wydajność skanowania antywirus – 4 Gbps
- Wydajność IPSec VPN – 4 Gbps.
- Obsługę nowych połączeń na sekundę – 200 000
- Obsługę nie mniej niż równoczesnych połączeń – 6 000 000.

System bezpieczeństwa w Jednostkach organizacyjnych

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łączy dla poszczególnych lokalizacji. Integralność systemu musi być zapewniona także w przypadku różnych dostawców dla poszczególnych lokalizacji. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

- System powinien być zaprojektowany w taki sposób aby możliwa była jego rozbudowa w celu wyeliminowania pojedynczego punktu awarii. W tym celu powinien zapewnić co najmniej:
    - Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.

  - Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
  - Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów zgodnie z trasą definiowaną przez protokół OSPF.
- System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
- System realizujący funkcję Firewall musi dysponować co najmniej 8 portami Ethernet 10/100/1000 Base-TX
- Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
- W zakresie Firewall'a obsługa nie mniej niż 400 tys jednoczesnych połączeń oraz 3 tys. nowych połączeń na sekundę Przepustowość Firewall'a: nie mniej niż 1 Gbps
- Wydajność szyfrowania 3DES: nie mniej niż 500 Mbps.
- W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:
  - kontrola dostępu - zapora ogniowa klasy StatefulInspection;
  - ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar;
  - poufność danych- IPSec VPN oraz SSL VPN;
  - ochrona przed atakami- Intrusion Prevention System [IPS/IDS];
  - kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM;
  - kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP);
  - kontrola pasma oraz ruchu [QoS, Trafficshaping];
  - kontrola aplikacji oraz rozpoznawanie ruchu P2P;
  - ochrona przed wyciekiem poufnej informacji (DLP).
- Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 40 Mbps.
- Wydajność skanowania ruchu w celu ochrony przed atakami (IPS)min 150 Mbps.
- W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
  - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site;
  - Dostawca musi dostarczyć nielimitowanego klienta VPN współpracującego z proponowanym rozwiązaniem;
  - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności ;
  - Praca w topologii Hub and Spoke oraz Mesh;
  - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF;
  - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth;
- Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.

- Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
- Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
- Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
- Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
- Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
- Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
- Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
- Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, spam, Proxy avoidance). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
- Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
- System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
  - 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;
  - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.
- Funkcje bezpieczeństwa oferowanego systemu powinny posiadać certyfikaty ICSA dla funkcjonalności Firewall, IPS, Antywirus

Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami wchodzącymi w skład systemu. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

4. Okablowanie LAN wraz z dedykowanym zasilaniem elektrycznym

Stabilna praca oraz duża wydajność ma ogromne znaczenie w dla pracy nowych bardziej wymagających aplikacji, rozwoju usług publicznych, transmisji danych multimedialnych, itp. Wymagana jest więc dla CPD sieci LAN wraz z dedykowanym zasilaniem elektrycznym i obwodami zasilania gwarantowanego współpracującym z systemem UPS i agregatem prądotwórczym.

System okablowania strukturalnego.

W związku z rosnącym poziomem informatyzacji oraz podnoszeniem wymagań wydajnościowych dla sprzętu informatycznego, komputerów oraz aplikacji, a także ze względu na dynamiczną zmienność charakteru stanowisk końcowych wymaga się od systemu okablowania strukturalnego możliwości jego dopasowania do zmieniających się wymagań technicznych, funkcjonalnych i użytkowych. W związku z powyższym należy zastosować system okablowania strukturalnego w wersji hybrydowej, tj. łączącej klasyczny system okablowania zamkniętego, oraz jak najbardziej uniwersalny system otwarty, tj. taki, w którym wszelkiego rodzaju zmiany i rozbudowy będą mogły być samodzielnie prowadzone przez uprawniony personel szybko, a dodatkowo w sposób jak najbardziej prosty i łatwy, bez konieczności prowadzenia prac budowlanych, poprawek i remontów związanych z ingerencją zewnętrznych grup instalatorskich.

Biorąc pod uwagę aktualne wymagania użytkownika, należy zapewnić wydajność całego systemu otwartego na poziomie Klasy FA, a elementów okablowania strukturalnego na poziomie Kategorii 6A przy zastosowaniu RJ45 jako interfejsu końcowego dla połączeń na skrętce miedzianej 4 parowej w wersji ekranowanej.

Dodatkowo, ze względu na charakter obiektu, wydajność okablowania ma gwarantować najwyższy możliwy zapas dla aplikacji 10 Gigabit Ethernet, co ma być potwierdzone zgodnością z najnowszą aktualizacją normy ISO IEC 11801 z dodatkami Amendment 1 i Amendment 2, które określają pasmo przenoszenia dla systemów Klasy EA i komponentów Kategorii 6A do 500MHz, a dla systemów Klasy FA i komponentów Kategorii 7A do 1000MHz. W celu minimalizacji przesłuchu obcego oraz wielkości separacji od kabli zasilających zgodnie z wytycznymi TR 50173-99-1, EN50173-1/A1 oraz EN50174-2 do budowy systemu transmisyjnego przewidzianego dla aplikacji 10 Gigabit Ethernet należy stosować system ekranowany.

W związku z powyższym projektowany system okablowania strukturalnego powinien bezwzględnie spełniać wszystkie następujące warunki:

- Ilość stanowisk roboczych musi być uzgodniona i wynikać ze wskazówek Użytkownika końcowego;
- Maksymalna długość kabla instalacyjnego w łączu stałym okablowania poziomego (od punktu dystrybucyjnego do gniazda końcowego) nie może przekroczyć 90 metrów;
- Projektowane okablowanie poziome obsługiwane jest przez odpowiednią ilość punktów dystrybucyjnych PD zorganizowanych hierarchicznie, w architekturze gwiazdy oraz ringu, połączone z punktem centralnym GPD, co dokładnie ma być pokazane na schemacie ideowym oraz na podkładach budowlanych;

- Wymagana jest jednolita 25-letnia bezpłatna gwarancja na system od producenta systemu okablowania strukturalnego zawierająca w sobie również gwarancję na komponenty (m.in.: kable instalacyjne, gniazda, panele krosowe, elementy przyłączeniowe, kable krosowe i przyłączeniowe, szafę kablową i elementy zarządzające, kable i osprzęt do połączeń telefonicznych, itp);
- Wszystkie elementy okablowania (w szczególności: kabel, panele krosowe, gniazda, kable krosowe, prowadnice kablowe i inne) mają być oznaczone logo lub nazwą tego samego producenta i pochodzić z jednolitej oferty rynkowej (mają być wytwarzane przez jednego producenta);
- System ma być zaprojektowany zgodnie z wymaganiami najnowszych specyfikacji normatywnych norm
  - ISO/IEC11801:2011 - Information technology - Generic cabling for customer premises
  - PN-EN 50173-1:2011 Technika Informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne
  - PN-EN 50173-2:2008/A1:2011 Technika Informatyczna – Systemy okablowania strukturalnego – Część 2: Budynki biurowe
  - PN-EN 50174-1:2010/A1:2011 Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja i zapewnienie jakości
  - PN-EN 50174-2:2010/A1:2011 Technika informatyczna. Instalacja okablowania – Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków
  - PN-EN 50174-3:2005 Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków
  - PN-EN 50346:2004/A2:2010 Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania
  - PN-ISO/IEC 14763-3:2009/A1:2010 Technika informatyczna - Implementacja i obsługa okablowania w zabudowaniach użytkowych - Część 3: Testowanie okablowania światłowodowego
  - EN 50288-4-1, IEC 61156-7 Norma komponentowa dotycząca wydajności kabli symetrycznych do 600MHz oraz kabli dla kat.7A – częstotliwości 1200MHz
  - IEC 60332-1-2, IEC 60332-3-24, IEC 60332-3-22, IEC 60754-1, IEC 60754-2, IEC 61034-2, EN 50266-2-2 - Normy międzynarodowe związane z palnością powłoki kabla
- Ze względów bezpieczeństwa należy zastosować ekranowane kable logiczne 4 parowe o konstrukcji S-FTP (indywidualne ekranowanie każdej pary transmisyjnej folią i dodatkowy ekran wszystkich par z siatki ekranującej). Biorąc pod uwagę przyszłościową rozbudowę, zmiany wydajności z Kat.7_A do wyższych standardów oraz możliwości integracji różnych usług w ramach okablowania kable muszą mieć odpowiedni zapas transmisyjny – zastosować kable typu S/FTP (PiMF) kat.7_A ISO LSFRZH o wydajności zgodnej z wymaganiami draftu kat 8.2 (2000MHz);
- System w całości tj. zarówno części zamkniętej jak i otwartej ma mieć możliwość uruchomienia funkcji monitoringu i zarządzania połączeniami fizycznymi w czasie rzeczywistym, poprzez

zainstalowanie na panelach sensorowych zestawów uzupełniających i połączenia ich poprzez analizatory sieciowe do relacyjnej otwartej bazy danych. Licencje dostępowe do bazy danych mają być bezpłatnie zaimplementowane i udostępnione w analizatorze, przy czym analizatory monitorujące wraz z oprogramowaniem mają być dostarczane i dostępne w ofercie producenta okablowania strukturalnego. Na etapie projektu należy przewidzieć implementację oprogramowania do zarządzania systemem okablowania strukturalnego, którego wdrożenie i działanie jest uniezależnione od części sprzętowej systemu zarządzania.

- Punkt logiczny stanowi zakończenie dla 4 kabli transmisyjnych, zbudowany w oparciu o dwa ekranowane modularne gniazda RJ45 kat. 6_A (system zamknięty) oraz dwa uniwersalne gniazda systemu otwartego kat. 7_A, pozwalające na rekonfigurację ilości i typów interfejsów oraz zmianę wydajności w zależności od potrzeb Użytkownika.

Okablowanie poziome.

System uniwersalny (otwarty) kat. 7_A:

- Okablowanie ma być zaprojektowane w oparciu o ekranowane złącze typu 110, zarabiane metodą narzędziową. Ekranowane złącze w osprzęcie połączeniowym ma zapewnić 360O kontakt ekranu każdej pary kabla i obudowy zewnętrznej z ekranem ogólnym wszystkich par transmisyjnych;
- System należy zaprojektować w oparciu o płyty czołowe 45x45mm w uchwycie do osprzętu typu Mosaic, co daje dużą uniwersalność i możliwość dopasowania do różnego osprzętu elektroinstalacyjnego;
- Złącze zakańczające kabel ma pozwać na wymianę interfejsów końcowych bez konieczności zmiany zakończenia kabla oraz posiadać pozytywne parametry transmisyjne w paśmie do 2GHz.
- System ma pozwalać na rozbudowę ilości gniazd (interfejsów) końcowych bez konieczności dokładania kabla – jedynie przez elementy zakończeniowego wymiennego z pojedynczego (np. 1xRJ45) na podwójny (2xRJ45), potrójny (3xRJ45) lub czterokrotny (4xRJ45)
- Elementy zakończeniowe 2xRJ45 muszą być dostępne w różnych konfiguracjach (2x komputer, 2x telefon, telefon + komputer) zarówno z gniazdami Kat.6A, Kat.6, jak i Kat.5e
- System ma pozwalać na zmianę typu interfejsu dowolnego punktu przyłączeniowego bez zmiany w rozszyciu kabla, tj. poprzez wymianę elementu zakończeniowego wymiennego na odpowiedni w panelu krosowym lub w gnieździe końcowym użytkownika. Budowa systemu ma gwarantować zastosowanie dowolnego interfejsu, który może być wykorzystany zgodnie ze specyfiką pracy obiektu – wśród nich muszą być RJ45, Tera Connector, ARJ45, DB9, RJ12, BNC, złącze F. Zmiana interfejsu końcowego nie może być realizowana za pomocą dodatkowych rozgałęźników czy adapterów – a jedynie przez wymianę elementu zakończeniowego wymiennego, w gnieździe końcowym. Nie dopuszcza się stosowania niestandardowych, specjalizowanych interfejsów.
- Połączenia systemu uniwersalnego mają pozwalać na rozbudowę ilości gniazd (interfejsów) końcowych bez konieczności dokładania kabla i ponownej terminacji kabla na złączu oraz bez potrzeby wymiany lub dodawania paneli krosowych. Rozbudowa nie może być realizowana przez rozdzielone (rozparowane) kable krosowe;

- System ma pozwalać na zmianę wydajności (kategorii, klasy okablowania) na odpowiednią (zarówno w górę jak i w dół), jedynie poprzez zmianę elementów końcowych – bez zmian kabla transmisyjnego i bez zmian w jego stałym zakończeniu;
- System ma mieć możliwość realizacji transmisji wielokanałowej (kilka aplikacji na tym samym kablu) przez wymianę elementu zakończeniowego w gnieździe użytkownika i panelu krosowym;
- Wszystkie interfejsy końcowe na elementach wymiennych mają zawierać trwałe oznaczenie opisujące wydajność i zastosowanie każdego interfejsu;
- Elementy wymienne, niezależnie od typu, mają mieć takie same wymiary zewnętrzne, aby rozbudowa czy rekonfiguracja systemu nie powodowała konieczności wymiany lub zakupu nowych paneli krosowych i gniazd;
- System ma gwarantować przesyłanie sygnału CATV w paśmie do 862MHz oraz integrację transmisji CATV w ramach istniejącej infrastruktury kablowej przez zamontowanie / wymianę elementu zakończeniowego na odpowiedni (z interfejsem typu F) bez konieczności ingerencji w zakończenie kabla;
- System ma posiadać możliwości transmisyjne min. Klasy FA 1GHz (przy wykorzystaniu odpowiednich interfejsów wymiennych), które mają być realizowane co najmniej przez 2 różne interfejsy, dostępne w postaci elementów wymiennych, np. interfejs TERA i ARJ-45;
- W fazie projektowej należy skonfigurować gniazda końcowe tak, aby spełniały obecne wymagania kategorii 6A/klasy EA – wykorzystując we wszystkich gniazdach wkładki 1xRJ45 Kat.6A (10Gigabit Ethernet). Wyjątek stanowić będą niektóre miejsca wskazane po uzgodnieniach z użytkownikiem;
- Wymagany interfejs w zespole gniazda naściennego – RJ45 o wydajności kat.6A, pozwalający na wykorzystanie standardowych kabli przyłączeniowych RJ45/RJ45;
- Panel krosowy w szafie kablowej ma być wyposażony w 8/16/24 ekranowane porty zawierające ekranowane złącze modularne typu 110, umieszczone w zamkniętej, ekranowanej, metalowej obudowie;
- Do paneli okablowania poziomego należy zastosować narożne otwierane-zamykane prowadnice boczne, z gumowym, dwustronnym przepustem kablowym;
- Montaż / wymiana elementów wymiennych nie może wymagać ponownej terminacji kabla na złączu.

Wymagania gwarancyjne.

- Wymagana gwarancja ma być bezpłatną usługą serwisową oferowaną Użytkownikowi końcowemu (Inwestorowi) przez producenta okablowania.
- Ma obejmować swoim zakresem całość systemu okablowania od głównego punktu dystrybucyjnego do gniazda końcowego wraz z kablami krosowymi i przyłączeniowymi, w tym również okablowanie szkieletowe i poziome, zarówno dla części logicznej, jak i telefonicznej.
- Należy zapewnić objęcie wykonanej instalacji gwarancją systemową producenta, gdzie okres gwarancji udzielonej bezpośrednio przez producenta nie może być krótszy niż 25 lat (Użytkownik

wymaga certyfikatu gwarancyjnego producenta okablowania udzielonego bezpośrednio Użytkownikowi końcowemu i stanowiącego 25-letnie zobowiązanie gwarancyjne producenta w zakresie dotrzymania parametrów wydajnościowych, jakościowych, funkcjonalnych i użytkowych wszystkich elementów oddzielnie i całego systemu okablowania).

- 25 letnia gwarancja systemowa producenta ma obejmować:
  - gwarancję materiałową (Producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji bądź 25-letniej eksploatacji wykryte zostaną wady lub usterki fabryczne, to produkty te zostaną naprawione bądź wymienione);
  - gwarancję parametrów łącza/kanału (Producent zagwarantuje, że łącze stałe bądź kanał transmisyjny zbudowany z jego komponentów przez okres 25 lat będzie charakteryzował się parametrami transmisyjnymi przewyższającymi wymogi stawiane przez normę ISO/IEC 11801 Am. 1, 2 dla określonej klasy wydajności);
  - gwarancję aplikacji (Producent zagwarantuje, że na jego systemie okablowania przez okres 25 lat będą pracowały dowolne aplikacje (współczesne i opracowane w przyszłości), które były (lub będą) dla systemów okablowania w rozumieniu normy ISO/IEC 11801 Am. 1, 2.

Dedykowane zasilanie elektryczne

Dedykowana instalacja elektryczna przeznaczona jest wyłącznie do zasilania urządzeń komputerowych. W obrębie każdego punktu abonenckiego zastosowano zestaw gniazd elektrycznych 2x230V. Obwody odbiorcze dedykowanej instalacji zasilającej będą zasilane z jednej rozdzielnicy. Poszczególne obwody odbiorcze będą zbudowane z wykorzystaniem przewodu YDY 3x2,5mm2 i zabezpieczone wyłącznikami nadprądowymi C10A z członem różnicowo-prądowym o prądzie zadziałania In=0,03A Rozdzielnica będzie zasilona z zamontowanego w serwerowni UPS-a, który zostanie podłączony do gniazd istniejącej sieci elektrycznej. W instalacji zastosujemy zabezpieczenia przeciwprzepięciowe.

Zadaniem UPS-a będzie również podtrzymywanie napięcia w przypadku zaniku zasilania w instalacji ogólnej.

Budując system o podwyższonym stopniu niezawodności zasilania, warto zwrócić uwagę na koszty wynikające z eksploatacji zasilaczy UPS. Zakłada się zastosowanie modułowo – redundancyjnego zasilacza UPS wykonanego w technologii True on-line (podwójne przetwarzanie) zgodnej z normą EN500091-3.