Warianty rozwiązań IP

HUAWEI

S4E

2014

ROZWIĄZANIA DLA FIRM WIELOODDZIAŁOWYCH

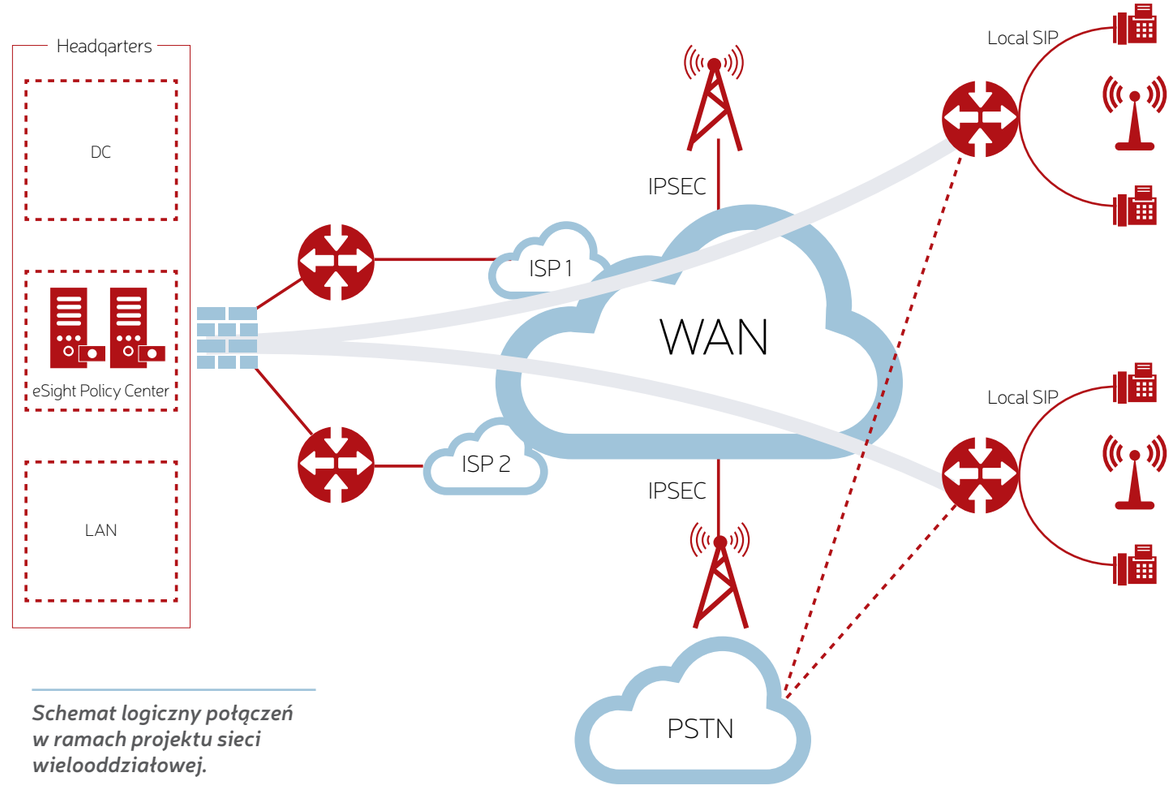
Restauracje, stacje benzynowe

OPIS ROZWIĄZANIA

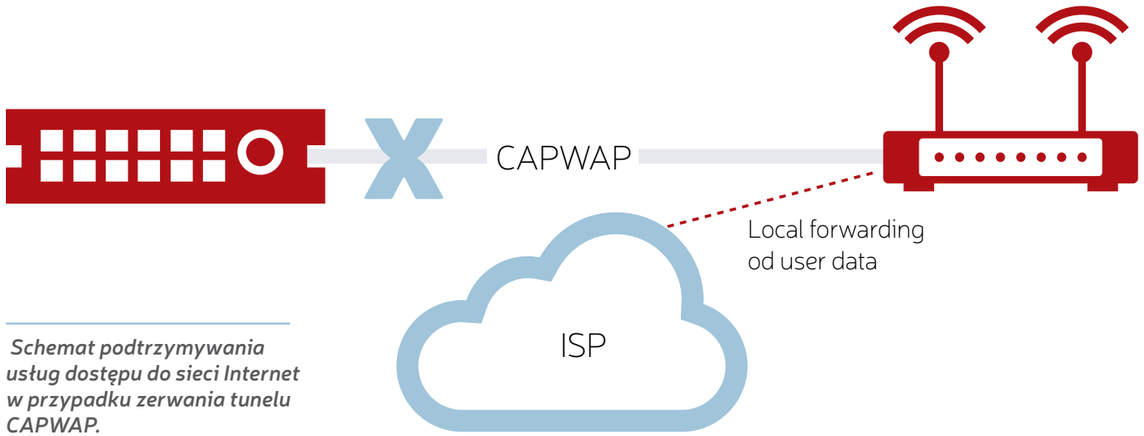
Rozwiązanie dedykowane m.in. firmom wielooddziałowym (stacje benzynowe, restauracje itd.), charakteryzującym się licznymi, nieskomplikowanymi pod względem infrastruktury sieciowej oddziałami oraz centralą, w której dane przechowywane są w sposób zcentralizowany.

Oddziały połączone są z centralą za pomocą tuneli VPN IPSec. Dodatkowo, każdy z nich oprócz łącza podstawowego posiada łącze zapasowe realizowane za pomocą technologii 3G lub LTE służące do komunikacji z siecią Internet w przypadku awarii głównego łącza.

Wewnątrz każdego z oddziałów znajdują się punkty dostępowe, które mogą pracować w trybie FAT AP lub FIT AP i być zarządzane. Funkcjonalność kontrolera WLAN może zostać zrealizowana za pomocą rutera znajdującego się w danym oddziae bądź przez dedykowane kontrolery WLAN umieszczone w centrali. Pomiędzy kontrolerem a punktami dostępowymi w oddziałach zestawiany jest tunel CAPWAP. Ruch z access-pointów może być przesyłany bezpośrednio do najbliższej bramy (tryb local-forwarding), bądź do kontrolera który znajduje się w centrali w celu jego analizy i kontroli (tryb tunnel-forwarding). W przypadku utraty komunikacji access-pointa z kontrolerem WLAN znajdującym się w centrali tryb local-forwarding w dalszym ciągu umożliwia dostęp do siec Internet podłączonym wcześniej użytkownikom jak również uwierzytelnienie nowych użytkowników.



Schemat logiczny połączeń w ramach projektu sieci wielooddziałowej.



Schemat podtrzymywania usług dostępu do sieci Internet w przypadku zerwania tunelu CAPWAP.

Routery znajdujące się w oddziałach pełnią funkcję lokalnych serwerów SIP, dzięki czemu rozmowy w obrębie oddziału nie muszą być przekazywane do bramki PBX i głównego serwera SIP znajdującego się w centrali.

W centrali zostały umieszczone systemy do zarządzania eSight oraz Agile Controller. Służą one do monitorowania i zarządzania oraz kontroli dostępu wszystkich urządzeń w obrębie firmy w sposób scentralizowany. Dzięki instalacji specjalnych modułów istnieje możliwość zarządzania routerami, switchami, firewallami, urządzeniami WLAN, UC. Agile Controller posiada dodatkowo wbudowany serwer RADIUS. Istnieje również możliwość uruchomienia tzw. *Captive Portal* dla klientów oddziałów.

Zastosowane urządzenie typu Next Genaration Firewall zabezpiecza sieć wewnętrzną w centrali, a także chroni dane zbierane z oddziałów przed wyciekiem. Firewall terminuje tunele IPSec obsługując „IPSec failover" – w przypadku gdy jeden z routerów brzegowych lub łącze internetowe do jednego z ISP ulegnie uszkodzeniu, tunel IPSec zostanie poprowadzony ścieżką zapasową.

MODELE URZĄDZEŃ WYKORZYSTYWANE W ROZWIĄZANIU

Lista urządzeń wykorzystywanych w tym scenariuszu wraz z istotną specyfikacją:

Router brzegowy w centrali: **AR3260 SRU200**

Przepustowość	40 Mpps
Przepustowość IPSec	7 Gbps
Ilość tuneli IPSec	6 000
FIBv4	800 000
Instancje VRF	2 000
Wydajność FW	10 Gbps

Routery oddziałowe: **AR157VW, AR207V, AR1220V**

	AR157VW	AR207V	AR1220V
Porty LAN/WAN	4 FE/ 1 ADSL + 4FXS 1FXO	8 FE/ 1 ADSL + 4FXS 1FXO	9 FE/ 2 GE + 2 sloty na karty rozszerzeń
3G port	T	T	T
Przepustowość	300 kpps	450 kpps	450 kpps
Przepustowość IPSec	80Mbps	100Mbps	200Mbps
Ilość jednoczesnych połączeń (PBX)	20	30	125
Ilość zarejestrowanych kont SIP	16	64	256

Router AR161FG-L

Porty LAN/WAN	4 GE/ 1 GE
Port Combo WAN	T
Modem LTE	T
Prędkość łącza z uruchomionymi	150 Mbps
Wydajność	350 kpps

Firewall USG 6650

Przepustowość FW	20 Gbps
Przepustowość IPS	10 Gbps
Przepustowość IPSec	12 Gbps
Ilość jednoczesnych połączeń	8 mln
Ilość nowych połączeń	300 000/s

Access Pointy: **AP6010DN-AGN, AP5030DN**

	AP6010DN	AP5030DN
MIMO	2x2:2	3x3:3
802.11	a/b/g/n	a/b/g/n/ac
Przepustowość max	300 Mbps	1.75 Gbps
Moc anten	20 dBm	20 dBm
Ilość użytkowników	128	256

KORZYŚCI

- **Redundancja i wysoka dostępność do oferowanych usług**

  W przypadku awarii nadmiarowe urządzenia w sieci centralnej zapewniają ciągłość dostępu do usług dla osób pracujących w oddziale i pracowników znajdujących się w zdalnych lokalizacjach.

  Wbudowane porty USB we wszystkich routerach Huawei obsługują modemy 3G oraz 4G. Podłączenie modemu 3G bądź 4G zapewnia tanią alternatywę łącza zapasowego.

- **Urządzenia „all-in-one”**

  Dzięki szerokiej ofercie dostępnych urządzeń Huawei istnieje możliwość zastąpienia wielu urządzeń innych producentów jednym urządzeniem Huawei, łączącym wszystkie zalety. Routery Huawei AR łączy w sobie cechy takich urządzeń jak router, kontroler WLAN, firewall, switch, centralka IPPBX oraz inne.

- **Wydajność i bezpieczeństwo**

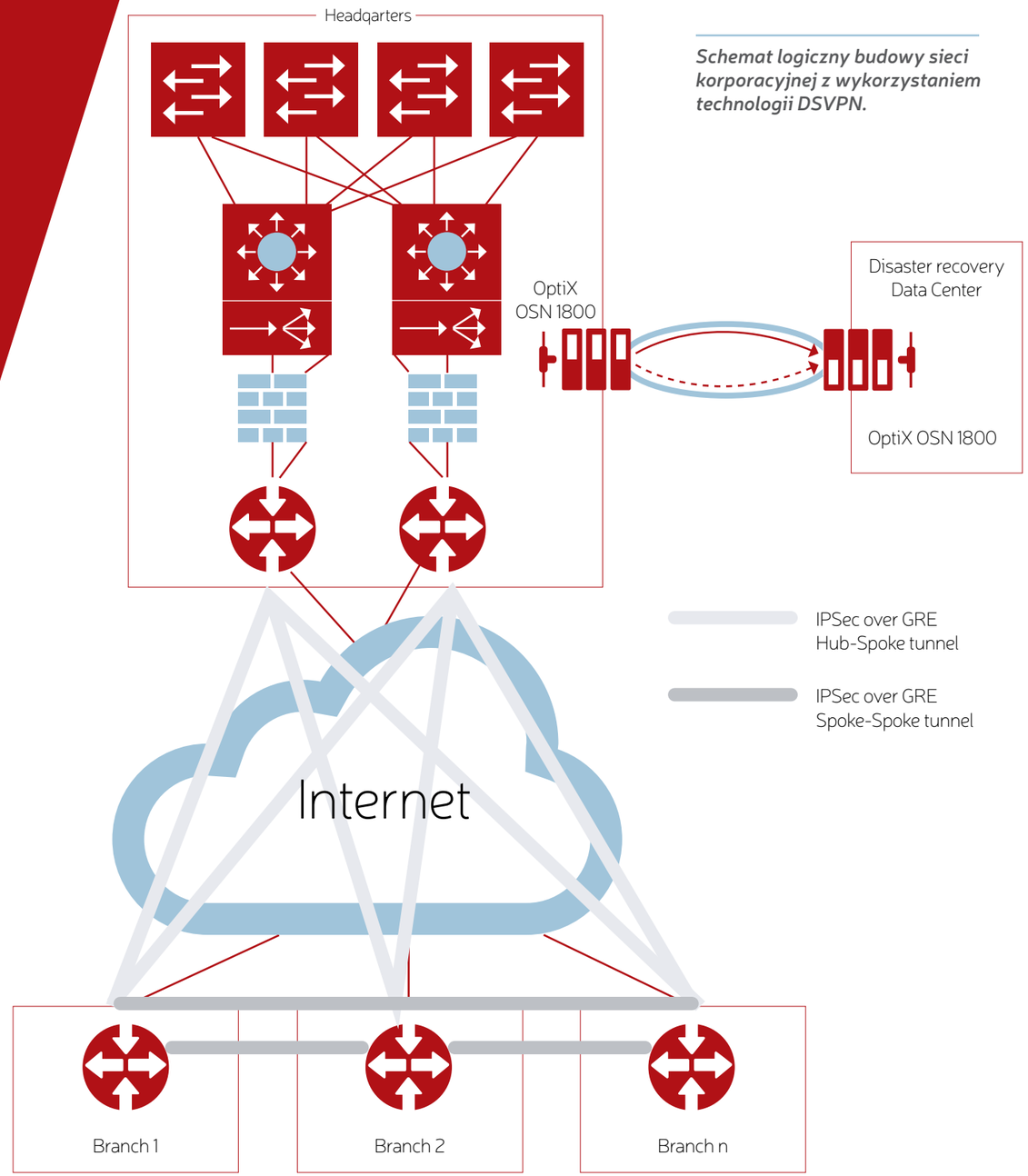
  Zastosowane urządzenia są jednymi z najwydajniejszych urządzeń w swojej klasie. USG 6600 poza pełnieniem tradycyjnej funkcji zapory sieciowej jest również urządzeniem klasy UTM, a więc zapewnia funkcjonalności IPS/AV/URL Filtering oraz ochronę przed wieloma rodzajami ataków. Zastosowanie systemu Agile Controller zapewnia prostsze zarządzenie kontrolą dostępu dla użytkowników końcowych.

Sieć korporacyjna

OPIS ROZWIĄZANIA

Rozwiązanie przeznaczone jest m.in dla dużych firm korporacyjnych lub banków charakteryzujących się rozbudowaną centralą, wieloma oddziałami oraz Data Center podstawowym i zapasowym.

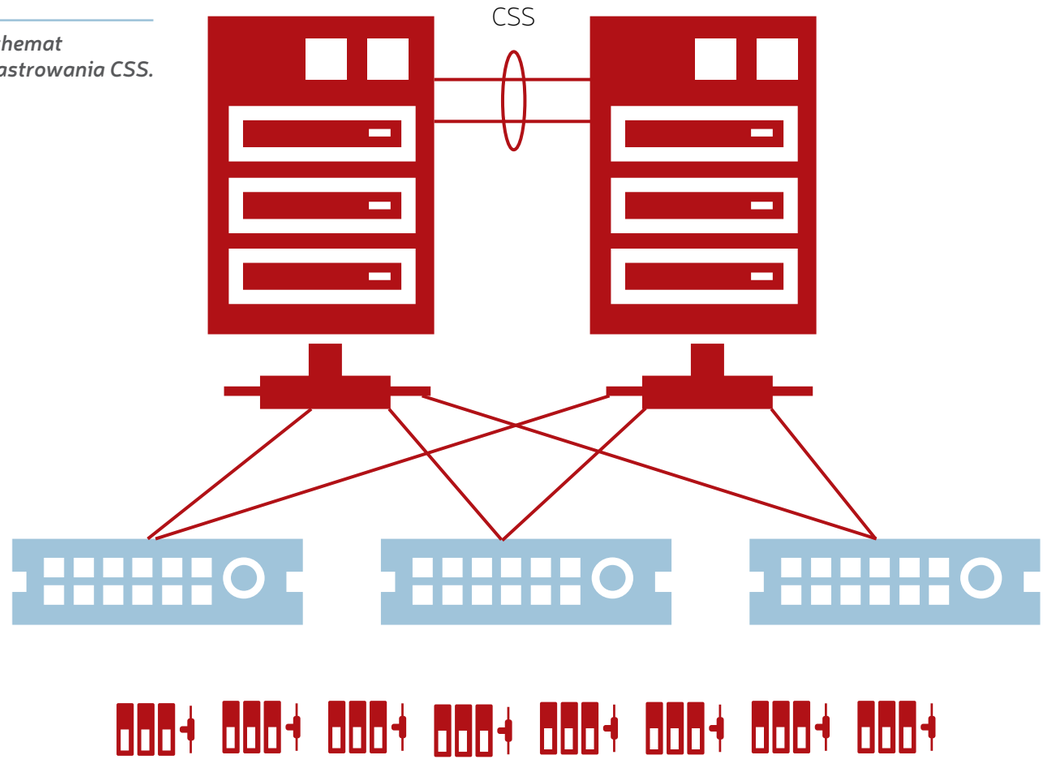
Do realizacji połączeń VPN została użyta technologia DSVPN (ang. Dynamic Smart Virtual Private Netowrk), która umożliwia budowę skalowalnych sieci VPN z wykorzystaniem zalet protokołów mutlipoint-GRE, NHRP oraz IPSec. Technologia ta umożliwia zdalnym oddziałom firmy komunikację z centralą lub z innymi zdalnymi oddziałami w sposób bezpośredni, za pomocą protokołu IPSec.



Schemat logiczny budowy sieci korporacyjnej z wykorzystaniem technologii DSVPN.

W centrali ulokowane zostały dwa firewalle nowej generacji, mogące pracować w trybie active/active lub active/passive, gdy wdrażana jest opcja failover.

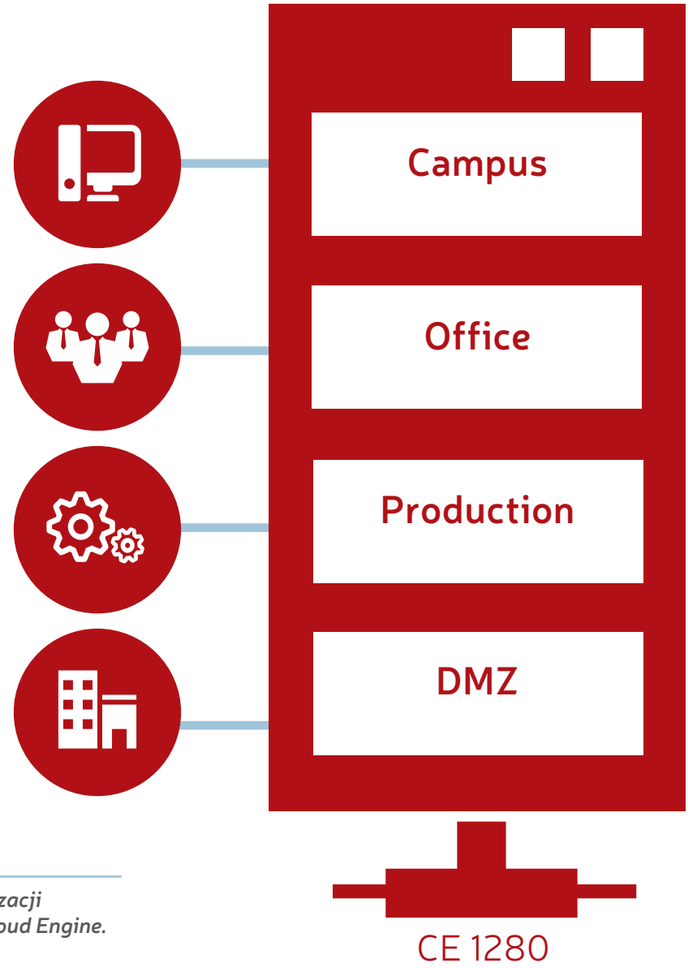
Dla zapewnienia bardzo dużej wydajności, skalowalności oraz redundancji w podstawowym Data Center zostały zastosowane przełączniki z serii Cloud Engine



Schemat klastrowania CSS.

Jedną z zalet przełączników Cloude Engine (CE) jest możliwość ich klastrowania dzięki czemu zapewniamy prostszą topologię sieciową jak również łatwiejsze zarządzanie. Możliwość wirtualizacji urządzeń per port bądź per karta liniowa zapewnia również elastyczne skalowanie środowiska dzięki cemu jedno urządzenie może pracować zarówno w strefie DMZ jak i w sieci produkcyjnej czy Data Center.

VS (Virtal System)



Schemat wirtualizacji przełączników Cloud Engine.

Dodatkowo, przy użyciu technologii zwielokrotniania falowego – DWDM za pomocą urządzeń Huawei OSN1800, uzyskano szybkie i wydajne połączenie z zapasowym Data Center w celu zapewnienia backupu zgromadzonych danych. Za pomocą dedykowanej infrastruktury światłowodowej możliwe jest połączenie ze sobą produkcyjnego oraz zapasowego Data Center.

MODELE URZĄDZEŃ WYKORZYSTYWANE W ROZWIĄZANIU

Lista urządzeń wykorzystywanych w tym scenariuszu wraz z istotną specyfikacją:

Router brzegowy w centrali: **AR3260 SRU200**

Przepustowość	40 Mpps
Przepustowość IPSec	7 Gbps
Ilość tuneli IPSec	6 000
FIBv4	800 000
Instancje VRF	2 000
Wydajność FW	10 Gbps

Firewall USG6680

Przepustowość FW	40 Gbps
Przepustowość IPS	20 Gbps
Przepustowość IPSec	20 Gbps
Ilość jednoczesnych połączeń	12 mln
Ilość nowych połączeń	400 000/s
Wirtualne firewalle	1000
Wbudowane interfejsy	4x10GE+16GE+8SFP

Przełączniki warstwy dostępowej : S5700-52X-LI

Switching Capacity	256 Gbps
Przepustowość	132 Mpps
Ilość portów 1 GE	48
Ilość portów 10 GE SFP+	4
Tablica MAC	16 000
Trasy statyczne	16

Przełączniki warstwy rdzenia/dystrybucji: **S9706**

Switching Capacity	3,84 Tbps
Przepustowość	2880 Mpps
Przepustowość/slot	320 Gbps
Ilość slotów na karty liniowe	6
Upakowanie portów	288GE/288*10GE/48*40GE
Karty zarządzające	1+1
Wsparcie dla:	RIP,RIPv2,OSPF,IS-IS,BGP,MPLS

Sieć transportowa: **OptiX OSN 1800 II**

Ilość slotów	8
Access Capacity	120 G
Zasięg	Single reach: Max. 140 km (39 dB)
Karty usługowe	LQM2: 8 x Any → 2.5G ELOM: 8 x Any → 10G LSX: 10G Any → 10G LDX: 2 x 10G Any → 10G
System Capacity	DWDM: 40-channel (max), 192.1–196.0 THz (Band-C, ITU-T G.694.1)

Przełączniki Data Center: **Seria Cloud Engine, przełączniki modularne oraz Top of Rack**

	CE12812	CE12808	CE12804
Switching Capacity	48 Tbps	32 Tbps	16 Tbps
Przepustowość	14400 Mpps	9600 Mpps	4800 Mpps
Przepustowość/slot	2 Tbps	2 Tbps	2 Tbps
Przepustowość IPSec	80Mbps	100Mbps	200Mbps
Ilość slotów na karty liniowe	12	8	4
Upakowanie portów	576*10 GE 288*40 GE/1152*10 GE 96*100 GE	384*10 GE 192*40 GE/768*10 GE 64*100 GE	192*10 GE 96*40 GE/384*10 GE 32*100 GE

	CE6850-48S4Q-EI	CE6850-48T4Q-EI
Downlink	48*10 G SFP+	48*10 G Base-T
Uplink	4*40 G QSFP+	4*40 G QSFP+
Switching Capacity	1.28 Tbps	1.28 Tbps
Przepustowość	960 Mpps	960 Mpps

KORZYŚCI

- **Prosta i bezpieczna komunikacja pomiędzy oddziałami**

  Dzięki wykorzystaniu technologii DSVPN, konfiguracja połączeń oddział-centrala oraz oddział-oddział odbywa się w sposób dynamiczny.

- **Bezpieczna sieć campusowa**

  Bezpieczeństwo wewnątrz sieci campusowej zostało zagwarantowane dzięki użyciu firewalli nowej generacji z serii USG 6600, charakteryzujących się wysoką wydajnością oraz możliwością zapewnienia redundancji poprzez zastosowanie nadmiarowości zarówno pod względem połączeń jak i urządzeń pracujących w trybach active/active lub active/standby wraz ze wsparciem protokołów takich jak VRRP lub technik – PBR.

- **Wydajne i efektywna Data Center**

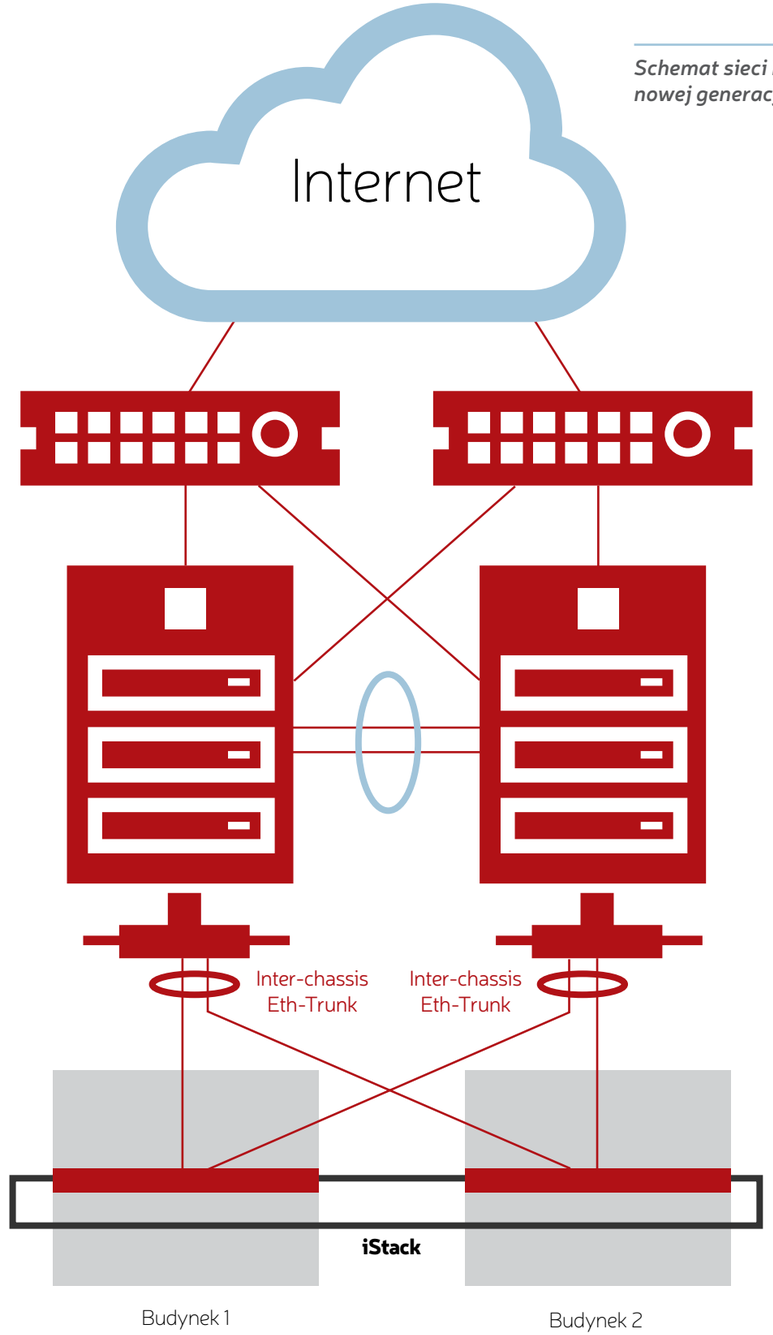
  Urządzenia z serii Cloud Engine charakteryzują się ogromną wydajnością oraz wsparciem dla interfejsów 100GE. Zastosowanie technologii DWDM sprawia, że dane gromadzone w Data Center są w szybki sposób backupowane w zapasowym Data Center. Dodatkowo dzięki wirtualizacji przełączników modularnych istnieje możliwość efektywnego wykorzystania takich urządzeń – mogą one pracować jednocześnie w Data Center jak i w szkielecie sieci campusowej.

SIECI LAN NOWEJ GENERACJI

Wydajny model campusowy

OPIS ROZWIĄZANIA

Sieci LAN nowej generacji zapewniają elastyczność orazto sieci wewnątrz których używa się infrastruktury min. 1/10 GE. Ruch przewodowy i bezprzewodowy jest zunifikowany, ale przede wszystkim dzięki swojej budowie oraz urządzeniom w nichzastosowanych, zapewniają one użytkownikom końcowym nieprzerwany dostęp do sieci internet i innych współdzielonych zasobów.



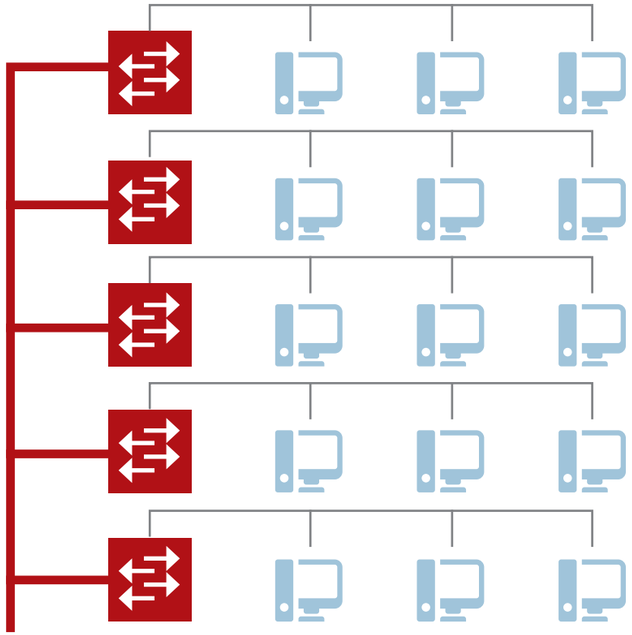
Schemat sieci LAN nowej generacji.

Routery AR3260 z SRU 400 pozwalają na uzyskanie przepustowości rzędu 5,5 Gbps. Zapewniają szybkie i niezawodne połączenie z siecią Internet.

Dodatkowo w takich routerach możliwa jest instalacja kart usługowych – kart z dedykowanym procesorem, dyskiem twardym oraz pamięcią RAM, która może służyć do instalacji systemu IPS lub systemu monitoringu i zarządzania wszystkimi urządzeniami znajdującymi się w sieci – eSight.

W warstwie dystrybucji zastosowano przełączniki modularne S9712. Zostały one ze sobą połączone technologią CSS. Takie połączenie pozwala na uzyskanie większych wydajności oraz pełne wykorzystanie redundancji.

Następnie w warstwie dystrybucji lub warstwie dostępu zastosować można przełączniki S6700. Switche te oparte o standard 10GE SFP+ dają możliwość łączenia w stos na odległość za pomocą iStack pozwalając na maksymalną odległość do 40km. Dzięki temu istnieje możliwość zarządzania poprzez jeden adres IP urządzeń, znajdujących się w różnych budynkach. Switche Sx700 umożliwiają utworzenie połączeń Eth-trunk zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie.



Schemat wykorzystania przełączników z baterią.

Data Center + Core/Dist.
Layer Protected by UPS

W warstwie dostępowej zastosowano nowe rozwiązanie Huawei. Są to switche S5700 z wbudowaną baterią. Pozwalają na podtrzymanie pracy takich urządzeń bez konieczności zastosowania dodatkowych, drogich UPSów.

MODELE URZĄDZEŃ WYKORZYSTYWANE W ROZWIĄZANIU

Router brzegowy w centrali: **AR3260 SRU200**

Przepustowość	40 Mpps
Przepustowość IPSec	7 Gbps
Ilość tuneli IPSec	6 000
FIBv4	800 000
Instancje VRF	2 000
Wydajność FW	10 Gbps

Switche dostępowe: **S5700-28P-LI-BAT**

Switching Capacity	128 Gbps
Przepustowość	42 Mpps
Ilość portów 1 GE	24
Ilość portów 1 GE SFP	4
Tablica MAC	16 000
Trasy statyczne	16
Bateria	8AH, praca do 11h

Przełączniki warstwy rdzenia/dystrybucji: **S9706**

Switching Capacity	3,84 Tbps
Przepustowość	1152 Mpps
Przepustowość/slot	2880 Gbps
Ilość slotów na karty liniowe	6
Upakowanie portów	288GE/288*10GE/48*40GE
Karty zarządzające	1+1
Wsparcie dla:	RIP,RIPv2,OSPF,IS-IS,BGP,MPLS

S9706

KORZYŚCI

- **Wielousługowe routery**

  Routery z serii AR3260 zapewniają dużą przepustowość oraz wiele funkcjonalności. Instalacja specjalnych kart pozwala na rozszerzenie funkcjonalności routera. Poza wbudowanym firewallem oraz między innymi systemem IPS, router może pełnić funkcję serwera eSight, co pozwala na monitoring i zarządzanie wszystkimi urządzeniami w sieci.

- **Wydajność warstwy agregacji**

  Przełączniki s9700 to urządzenia charakteryzujące się wysokimi wydajnościami. Dzięki redundantnej pracy umożliwiają stworzenie szybkiej i niezawodnej sieci lokalnej. Połączenie między urządzeniami odbywa się bezpośrednio między Switching Fabrics i jest realizowane za pomocą technologii CSS.

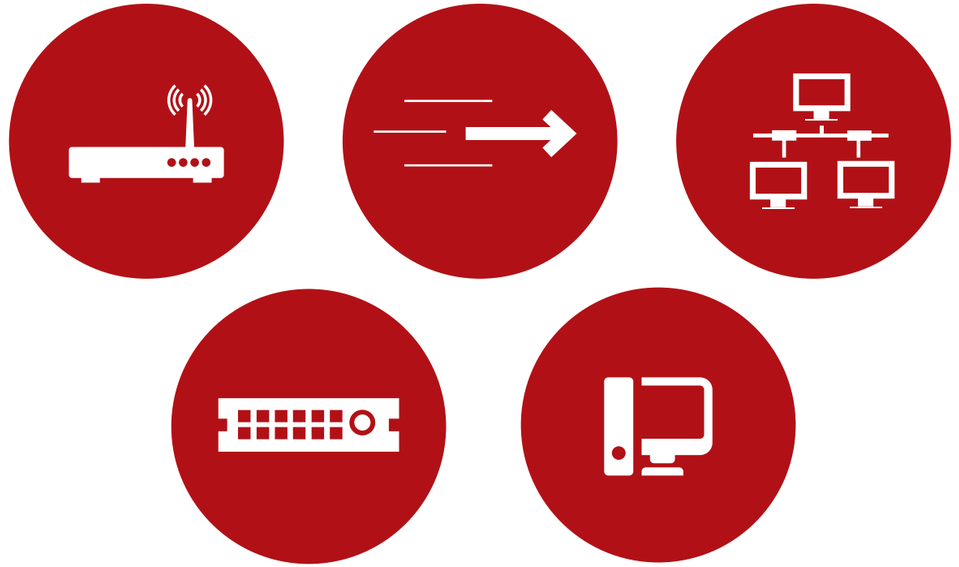
- **iStack, inter-chassis Eth-Trunk**

  Łączenie urządzeń w stos oraz połączenia między urządzeniami pracującymi w stosie znacznie ułatwiają zarządzanie, zapewniają redundancję oraz upraszczają topologię drzewa sieci.

  Połączenia między urządzeniami Huawei serii LI oraz EI odbywają się za pomocą optycznych portów uplink, dzięki temu możliwe jest łączenie urządzeń pracujących w znacznej odległości od siebie (nawet do 40 km). Urządzenia pracujące w oddzielnych budynkach w obrębie tej samej organizacji mogą być traktowane jako jedno logiczne urządzenie.

- **UPS wewnątrz urządzenia**

  Przełączniki z wbudowanymi akumulatorami są nowością na rynku enterprise. Urządzenie jest odporne na brak zasilania a także na chwilowe skoki napięcia, dzięki czemu bez konieczności zakupu dedykowanych zasilaczy UPS, praca urządzenia jest podtrzymana.



Zarządzanie w każdej postaci

OPIS ROZWIĄZANIA

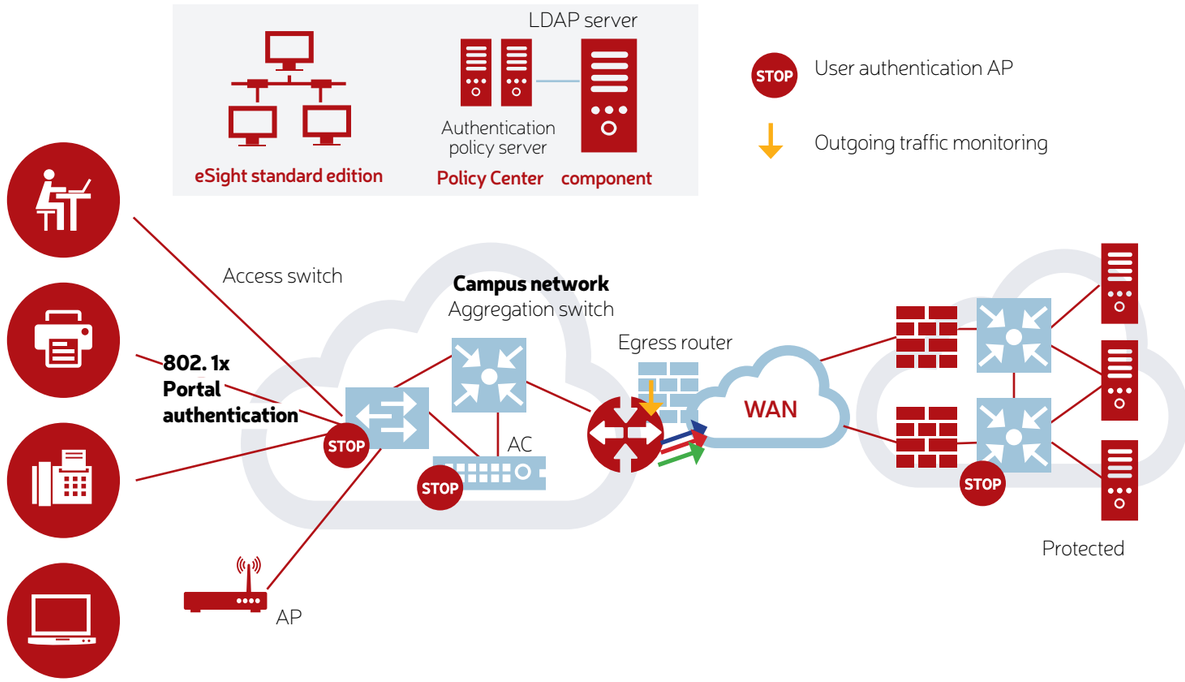
Nowoczesne sieci LAN nieodderwalnie wiążą się z unifikowanym i scentralizowanym sposobem zarządzania i monitorowania siecią oraz urządzeniami. Pojęcie oddzielnej infrastruktury i oddzielnego zarządzania sieciami przewodowymi i bezprzewodowymi należy uznać za nieaktualne.

eSight zapewnia skuteczne narzędzie do monitoringu i zarządzania siecią. Za pomocą protokołu SNMP oraz SNMP Traps administrator sieci jest informowany o występujących zagrożeniach w sieci. ESight zapewnia także możliwość konfiguracji urządzeń sieciowych z poziomu aplikacji, backupowanie konfiguracji urządzeń, planowanie okien serwisowych oraz wiele innych funkcjonalności.

Aplikację można rozbudowywać o dodatkowe moduły czyniąc z niej środowisko zarządzające nie tylko dla tradycyjnych urządzeń sieciowych, ale także sektora UC&C, Storage, WLAN, Data Center. Moduły te wprowadzają dodatkowe funkcjonalności rozszerzające możliwości OA&M.

Uzupełnieniem zaawansowanej kontroli sieciowej może być Policy Center czyli system do zarządzania tożsamością użytkownika. Policy Center nieoderwalnie wiąże się z pojęciem BYOD (ang. *Bring Your Own Device*).

BYOD to coraz bardziej popularne zjawisko polegające na korzystaniu z zasobów firmowych (poczynając od poczty elektronicznej poprzez wszelkiego rodzaju współdzielone zasoby) z prywatnych urządzeń pracowników firmy. Istnieje wówczas potrzeba odpowiedniej autoryzacji urządzeń oraz ochrony danych.



Policy Center umożliwia tworzenie polityk bezpieczeństwa oraz reguł dostępu w zależności od użytkownika lub od urządzeń danego użytkownika. Dodatkowo możliwe jest zarządzanie administracyjne zasobami – tworzenie takich polityk jak blokowanie przenoszenia konkretnych rozszerzeń plików na dyski zewnętrzne, instalowanie tylko autoryzowanych aplikacji i wiele innych.

KORZYŚCI

- **Zarządzanie z jednego miejsca**

  Za pomocą aplikacji eSight administrator jest w stanie monitorować i zarządzać wszystkimi urządzeniami znajdującymi się w sieci niezależnie od typu urządzeń. Unifikacja zarządzania sprawia, że z poziomu jednej aplikacji zarządzanie routerami, przełącznikami, terminalami UC&C, Data Center, Storage staje się dużo prostsze.

- **5W1H**

  Tworzenie polityk dostępu i bezpieczeństwa za pomocą Policy Center za pomocą świadomości kontekstu z wykorzystaniem metody 5W1H – Who?,Where?, When?, Whose device?, What device?,How?

- **Bezpieczny dostęp z każdej lokalizacji**

  Policy Center daje możliwość skutecznej implementacji BYOD w sieci. Umożliwia tworzenie stron uwierzytelniania w zależności od typu urządzenia jakie próbuje się uwierzytelnić, tworzenie wielu polityk na tym samym koncie użytkownika w zależności od urządzenia z którego się loguje, umożliwia zdalny restart urządzeń do ustawień fabrycznych w przypadku utraty urządzenia przez pracownika

- **Wysokie bezpieczeństwo i zabezpieczenie przed wyciekiem danych**

  Policy Center wspiera wiele mechanizmów uwierzytelniania, współpracuje z Radiusem oraz LDAP. Zapewnia ochronę terminali końcowych, aktualizacje wykonywane z poziomu administratora oraz zarządzanie pulpitem. Kontroluje również zachowanie terminali końcowych, przeprowadzając wiele rodzajów audytów sprawdzających bezpieczeństwo danych. Umożliwia również monitorowanie aplikacji, szyfrowanie dysków przenośnych, dysków twardych oraz dokumentów.

Zapraszam do kontaktu

ADAM PRZETAK
Huawei Product Manager

tel: **603 753 793**
e-mail: **adam.przetak@s4e.pl**