Kompleksowa ochrona sieci przedsiębiorstwa

Rozwiązania firmy WatchGuard®

Prowadzący:

Jakub Wojnarowicz

CCNS S.A.

Agenda

- **Przykład 1 – Firma z rozproszonymi oddziałami**
  - Urządzenia rodziny Firebox® X Edge
  - Urządzenia rodziny Firebox® X Core
- **Przykład 2 – Przedstawiciele handlowi**
  - Urządzenie Firebox® SSL VPN Gateway
- **Przykład 3 - Firma udostępniająca dane pomiarowe**
  - Urządzenia rodziny Firebox® X Peek
- **Cechy wspólne urządzeń firmy WatchGuard**
  - Centralne zarządzanie
  - Sposób licencjonowania
- **Wsparcie techniczne**

Firma z rozproszonymi oddziałami
Przykład #1

- **Opis przypadku**
  - Niewielka firma z oddziałami
  - 6 oddziałów rozproszonych geograficznie
  - W siedzibie firmy serwery aplikacyjne i bazodanowe
  - Zewnętrzne biuro rachunkowe z dostępem do serwerów
  - Oddziały: 2-5 komputerów
  - W każdym oddziale podział na 2 strefy:
    - z dostępem do Internetu
    - z dostępem do aplikacji firmowej

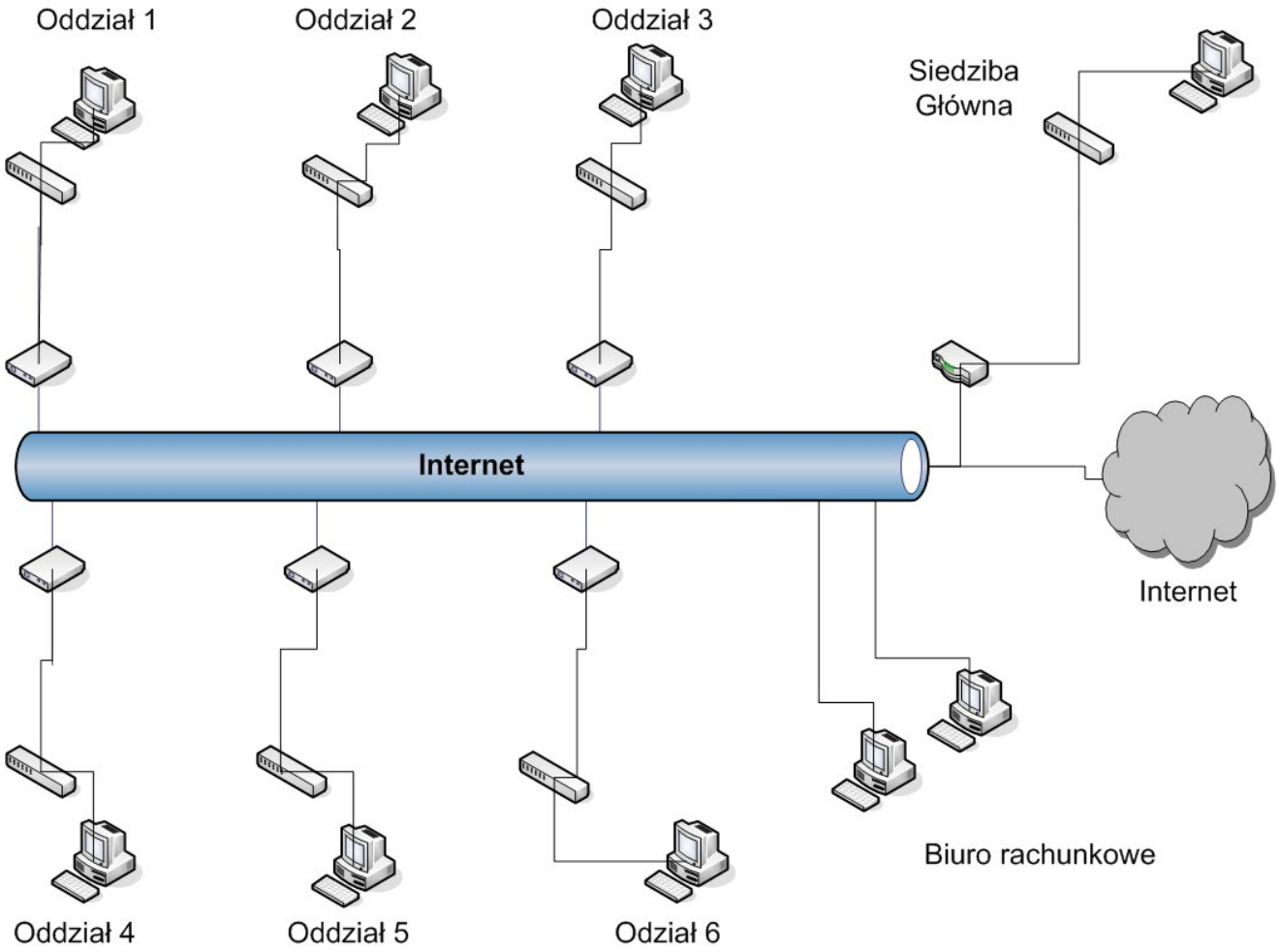
- **Opis potrzeb**
  - Bezpieczne połączenie wszystkich lokalizacji w jedną sieć
  - Zapewnienie bezpieczeństwa korzystania z sieci Internet w każdej z lokalizacji
  - Zapewnienie dostępu do serwerów aplikacji przez biuro rachunkowe (bez ingerencji w strukturę jego sieci)
  - Możliwość centralnego zarządzania wszystkimi urządzeniami oraz politykami bezp.
  - Niski całkowity koszt wdrożenia

Firma z rozproszonymi oddziałami
Rozwiązanie firmy CCNS S.A.

- **Oddziały firmy**
  - Wyposażone w niewielkie urządzenia spełniające rolę końcówki VPN oraz zapory sieciowej
  - Cały ruch z/do sieci oddziału jest szyfrowany przesyłany do siedziby firmy
  - Nie ma możliwości wyjścia do Internetu poza tunelem VPN
- **Biuro rachunkowe**
  - Na komputerach uprawnionych do łączenia się z serwerem firmy zainstalowano oprogramowanie mobilnego klienta IPSec VPN (Mobile User VPN)
- **Siedziba firmy**
  - Sieć firmy chroniona za pomocą zintegrowanej zapory i koncentratora VPN
  - Cały ruch z/do oddziałów jest filtrowany i kierowany odpowiednio do Internetu lub do serwerów aplikacji i bazodanowych

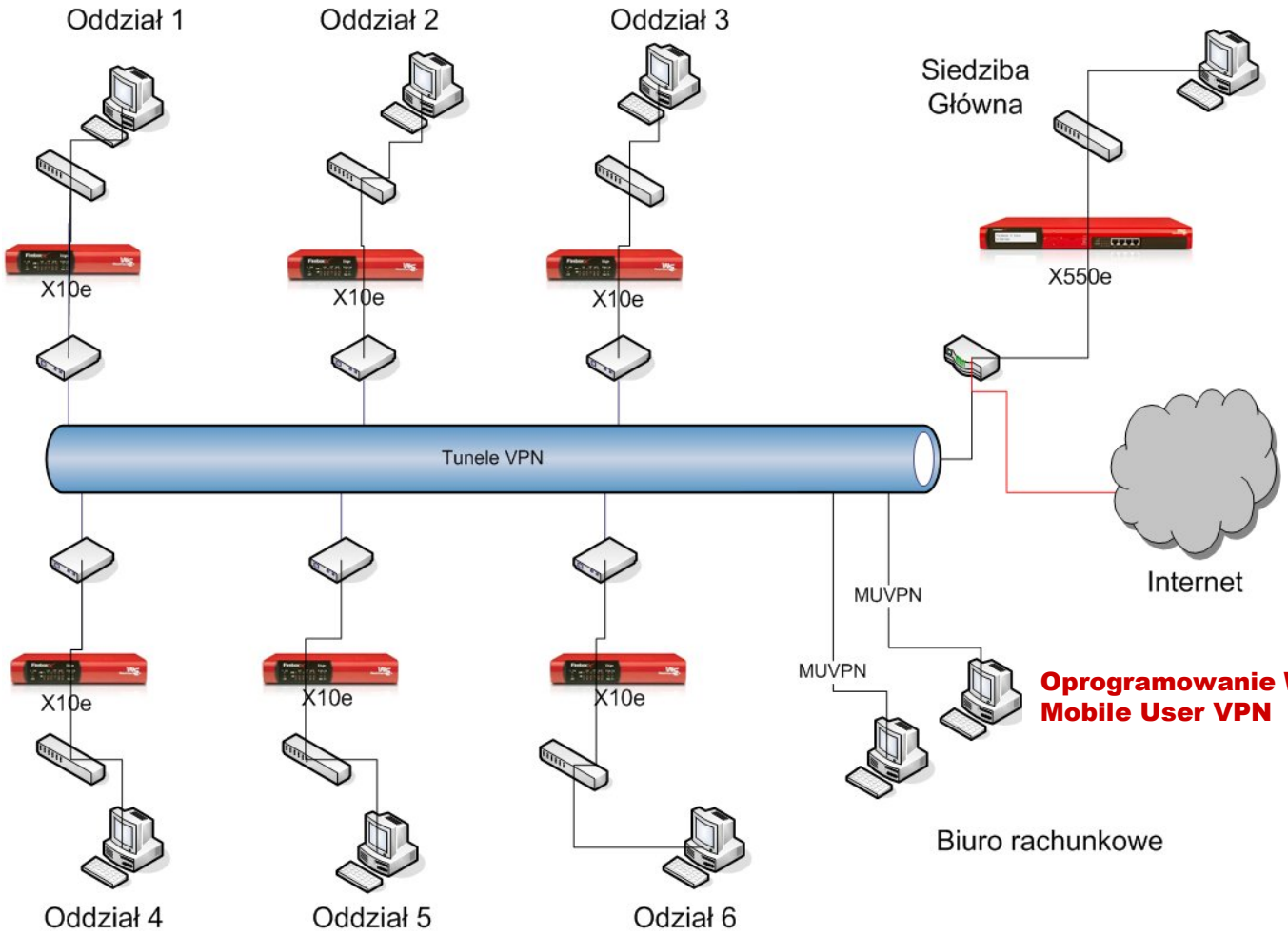
Firma z rozproszonymi oddziałami

Schemat rozwiązania



Firma z rozproszonymi oddziałami

Schemat rozwiązania



Oprogramowanie WatchGuard Mobile User VPN

Firma z rozproszonymi oddziałami

Oddziały firmy

- **Urządzenia Firebox® Edge X10e**
  - Najtańsze urządzenie w ofercie firmy WatchGuard
  - Obsługa do 5 statycznych tuneli VPN IPSec
  - Obsługa do 11 tuneli mobilnych IPSec
  - Separacja dwóch sieci fizycznych (tzw. DMZ)
  - Zaawansowane funkcje sieciowe (DNAT, 1:1 NAT, PAT)
  - Zarządzanie ruchem i QoS (np. ruch VoIP)
  - Wersja z interface'm bezprzewodowym 802.11b/g
  - Opcjonalna możliwość filtrowania antywirusowego i antyspamowego
  - Możliwość zarządzania poprzez WWW lub za pomocą centralnego systemu zarządzania.

Firma z rozproszonymi oddziałami
Siedziba główna firmy

- **Urządzenie Firebox® Core X550e**
  - Zintegrowana zapora sieciowa i koncentrator VPN
  - Obsługa do 45 statycznych tuneli VPN
  - Przepustowość VPN: 100Mb/s, firewall: 300Mb/s
  - Separacja do 4 sieci fizycznych
  - Intuicyjne oprogramowanie zarządzające
  - Dodatkowe usługi:
    - WebBlocker
    - spamBlocker
    - GAV/IPS
  - Opcjonalna obsługa VLAN, QoS, routing dynamiczny

Firma z rozproszonymi oddziałami
Siedziba główna firmy

- **Usługa WebBlocker**
  - Filtruje adresy URL niebezpiecznych stron WWW:
    - spyware, pharming, phishing etc.
  - Ułatwia egzekwowanie polityk bezpieczeństwa
  - Baza danych ponad 14 milionów adresów URL
  - Możliwość konfiguracji do 40 kategorii niedozwolonych treści
  - Możliwość nadania dostępu do stron WWW na podstawie zalogowanego użytkownika, grupy, godzin pracy etc.
  - Codzienne uaktualnienia bazy adresów
    - Baza danych przechowywana lokalnie na wydzielonym serwerze
  - Licencja na urządzenie a nie na użytkownika – efektywne kosztowo

Firma z rozproszonymi oddziałami
Siedziba główna firmy

- **Usługa spamBlocker**
  - Blokuje do 97% niechcianej poczty (spamu)
  - Blokowanie w czasie rzeczywistym
  - Wykorzystuje unikalną technologię firmy CommTouch
    - Rekurencyjna detekcja wzorców przez detektory rozsiane w Internecie pozwala na szybkie zauważenie wzmożonego ruchu mailowego.
  - Metoda niezależna od:
    - Zawartości listu
    - Użytego języka etc,
  - Licencja na urządzenie a nie na użytkownika – efektywne kosztowo

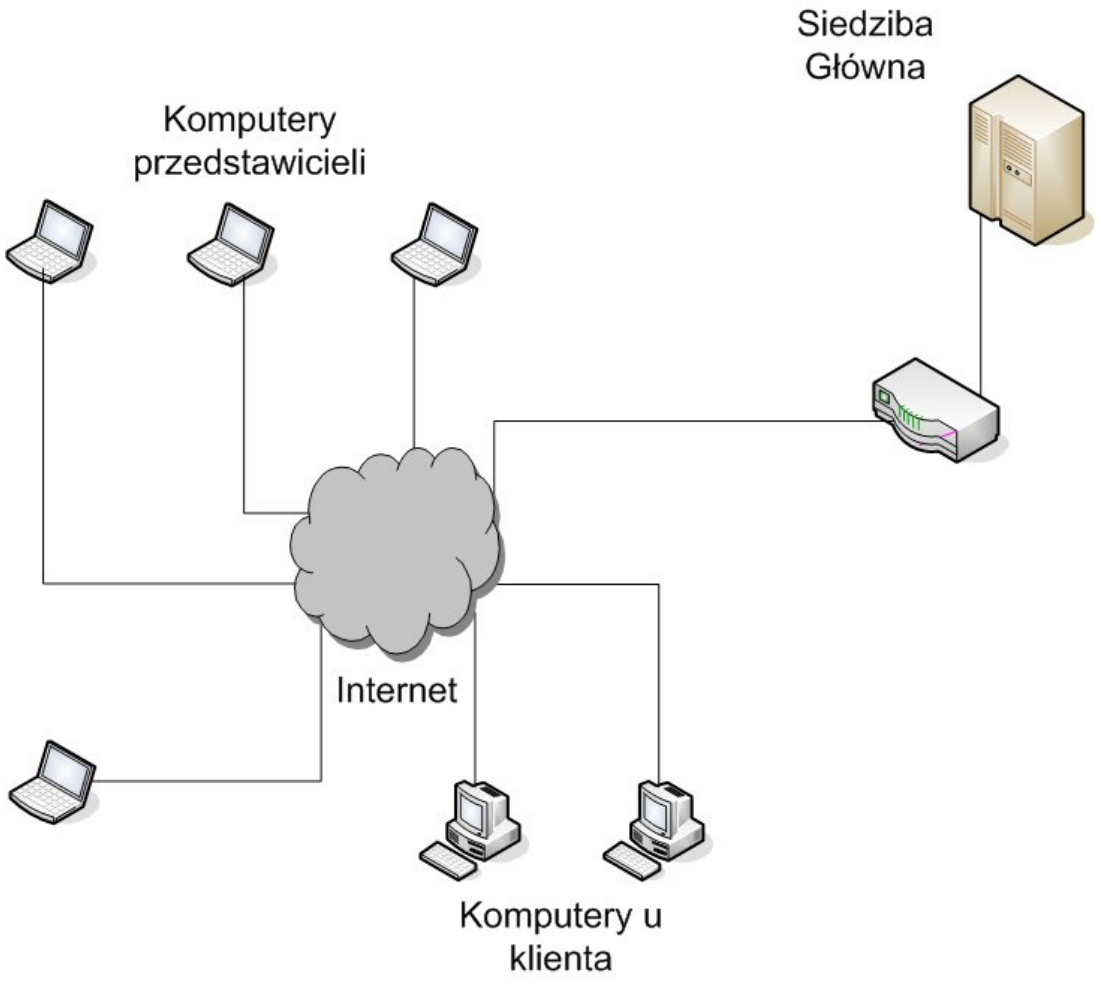
Firma z rozproszonymi oddziałami
Siedziba główna firmy

- **Usługa Gateway Anti-Virus**
  - Ochrona przed:
    - Wirusami w poczcie elektronicznej
    - Zainfekowanymi plikami na stronach WWW
  - Baza sygnatur aktualizowana na bieżąco
- **Usługa Intrusion Prevention System**
  - Ochrona przed:
    - trojanami,
    - atakami buffer overflow,
    - SQL Injection, etc.
  - Zabezpieczenie ruchu Instant Messaging i P2P przed wirusami i spyware

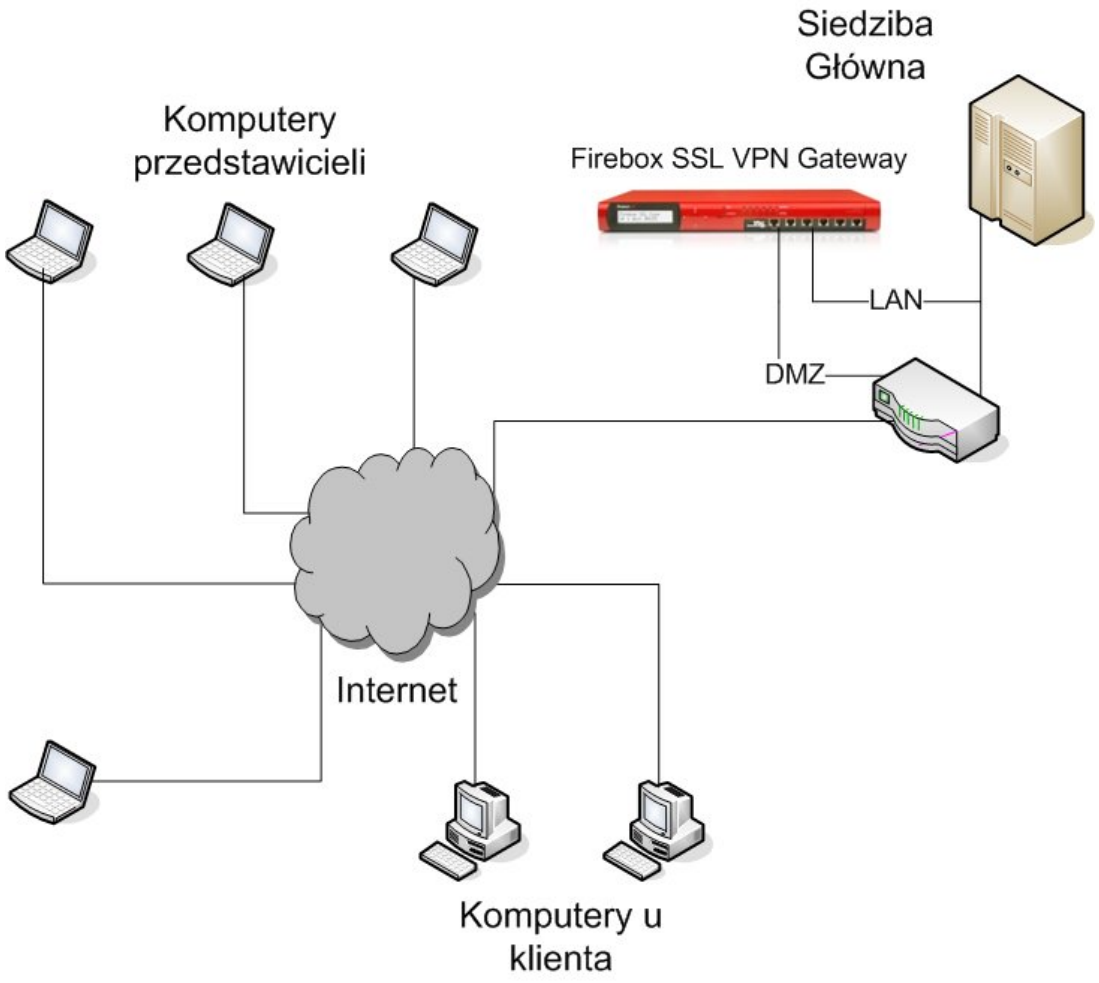
Przedstawiciele handlowi
Przykład #2

- **Opis przypadku**
  - Firma zatrudnia około 100 przedstawicieli handlowych, tzw. „wolnych strzelców”
  - Przedstawiciele korzystają z własnego sprzętu i własnych łączy, często ze sprzętu klienta
  - W siedzibie firmy znajdują się serwery aplikacji, z których aktywnie korzystają przedstawiciele
  - Firma posiada już infrastrukturę zabezpieczenia sieci (brak możliwości ingerencji w adresację etc.)
- **Opis potrzeb**
  - Należy zapewnić możliwość bezpiecznego korzystania z aplikacji na serwerach firmy przez przedstawicieli handlowych
  - Możliwość dostępu do informacji również bez konieczności instalowania dodatkowego oprogramowania (np. komputer kontrahenta)

Przedstawiciele handlowi
Schemat sieci



Przedstawiciele handlowi
Schemat sieci



Przedstawiciele handlowi
Rozwiązanie firmy CCNS S.A.

Zaproponowano rozwiązanie WatchGuard® Firebox ® SSL VPN Gateway, które zapewnia bezpieczne połączenie SSL VPN użytkownikom mobilnym. Działa w dwóch trybach:

- **Tryb bezpiecznego klienta,** gdzie uproszczona aplikacja dostępowa uruchamiana jest na komputerze użytkownika
- **Tryb Kiosk,** gdzie użytkownik, łącząc się za pomocą standardowej przeglądarki, ma dostęp do wybranych usług zdalnych

WatchGuard® SSL VPN Gateway

Tryb bezpiecznego klienta

- **Działanie**

  Użytkownik za pomocą zainstalowanego na komputerze programu łączy się z Firebox SSL. Cały ruch przeznaczony do sieci firmowej jest automatycznie szyfrowany i przesyłany tunelem.

- **Zalety**
  - Transparentny dla użytkownika
  - Dostęp do wszystkich aplikacji firmowych
  - Nie trzeba zmieniać konfiguracji systemu
    - DNS, WINS etc.
  - Tunel jest „zawsze dostępny”
  - Obsługa protokołu UDP
  - Optymalizacja pod kątem VoIP
- **Licencje**
  - Na podstawie ilości użytkowników (max 205 licencji)

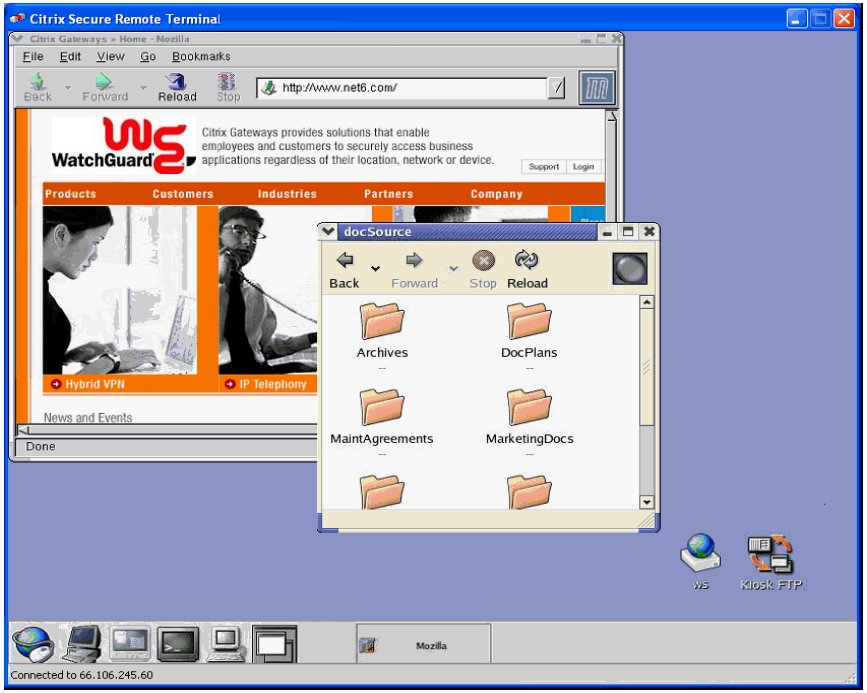
WatchGuard® SSL VPN Gateway
Tryb Kiosk

- **Działanie**

  Użytkownik za pomocą przeglądarki WWW łączy się z Firebox SSL. Otrzymuje dostęp do specjalnego pulpitu, z którego może nawiązywać połączenia z usługami dostępnymi w sieci.

- **Zalety**
  - Dostęp do określonych zasobów z publicznych punktów dostępu (kawiarenki)
  - Nie pozostawia żadnych informacji
  - Nie jest konieczne instalowanie dodatkowego oprogramowania (Java)

- **Obsługa aplikacji**
  - Zdalny Pulpit (Remote Desktop),
  - Połączenie SSH, Telnet
  - Dostęp do serwerów VNC
  - Szybki dostęp do współdzielonych dysków sieciowych.



Firma udostępniająca dane pomiarowe
Przykład #3

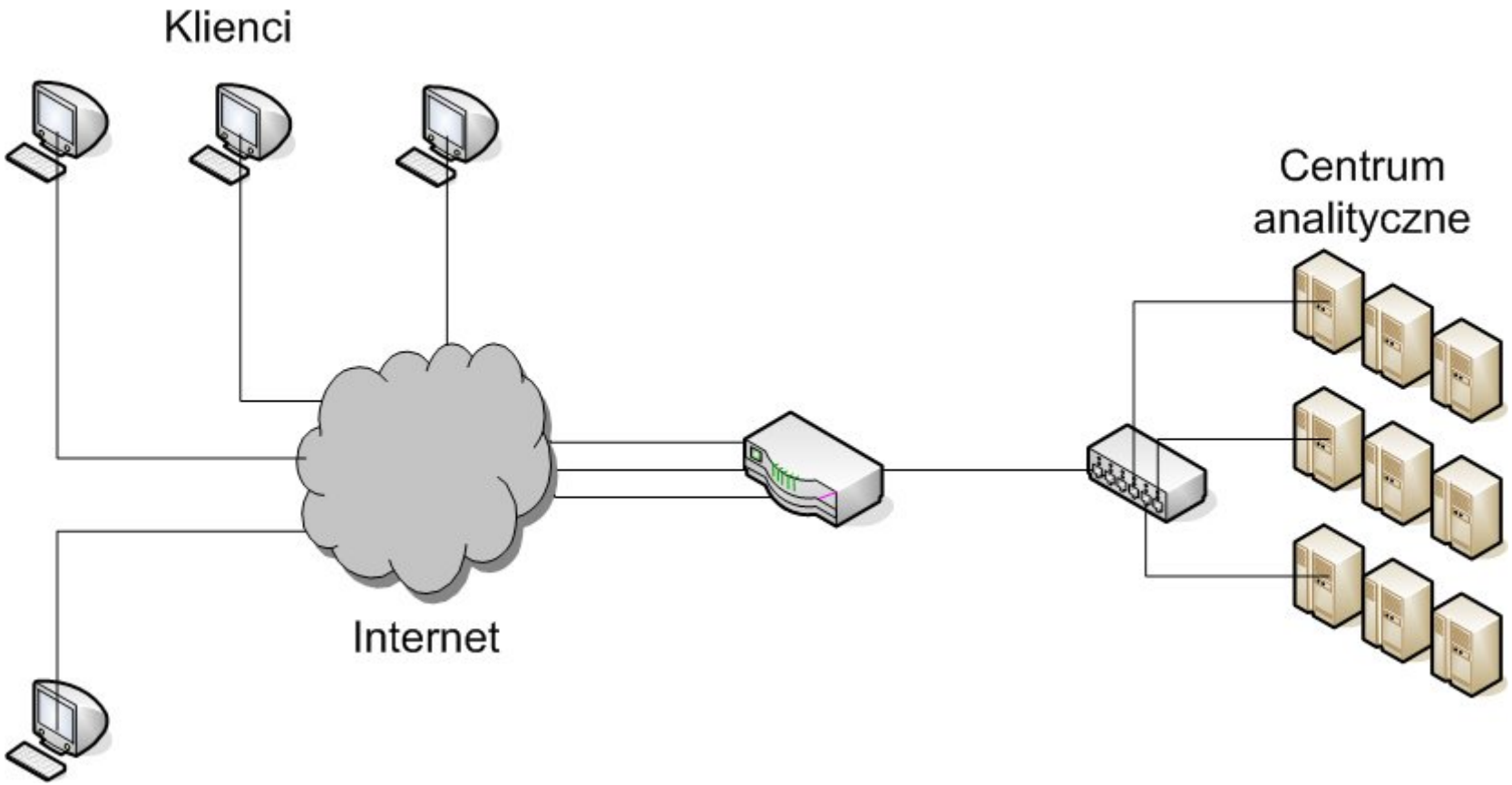
- **Opis przypadku**
  - Firma zajmująca się zbieraniem, analizą i udostępnianiem danych pomiarowych pochodzących z procesów automatyki
  - Centrum analityczne składa się z 30 odrębnych serwerów, na których przetwarzane są dane osobno dla każdego klienta
  - Dane te oraz wyniki analizy są udostępniane nieprzerwanie klientowi
  - Centrum analityczne posiada 3 niezależne łącza do sieci Internet.

- **Opis potrzeb**
  - Konieczne jest zapewnienie bezpieczeństwa danych pomiarowych
  - Priorytetem jest wysoka dostępność centrum analitycznego
  - Konieczne jest odseparowanie od siebie poszczególnych serwerów
  - Wymagana jest obsługa kilku łączy z siecią Internet

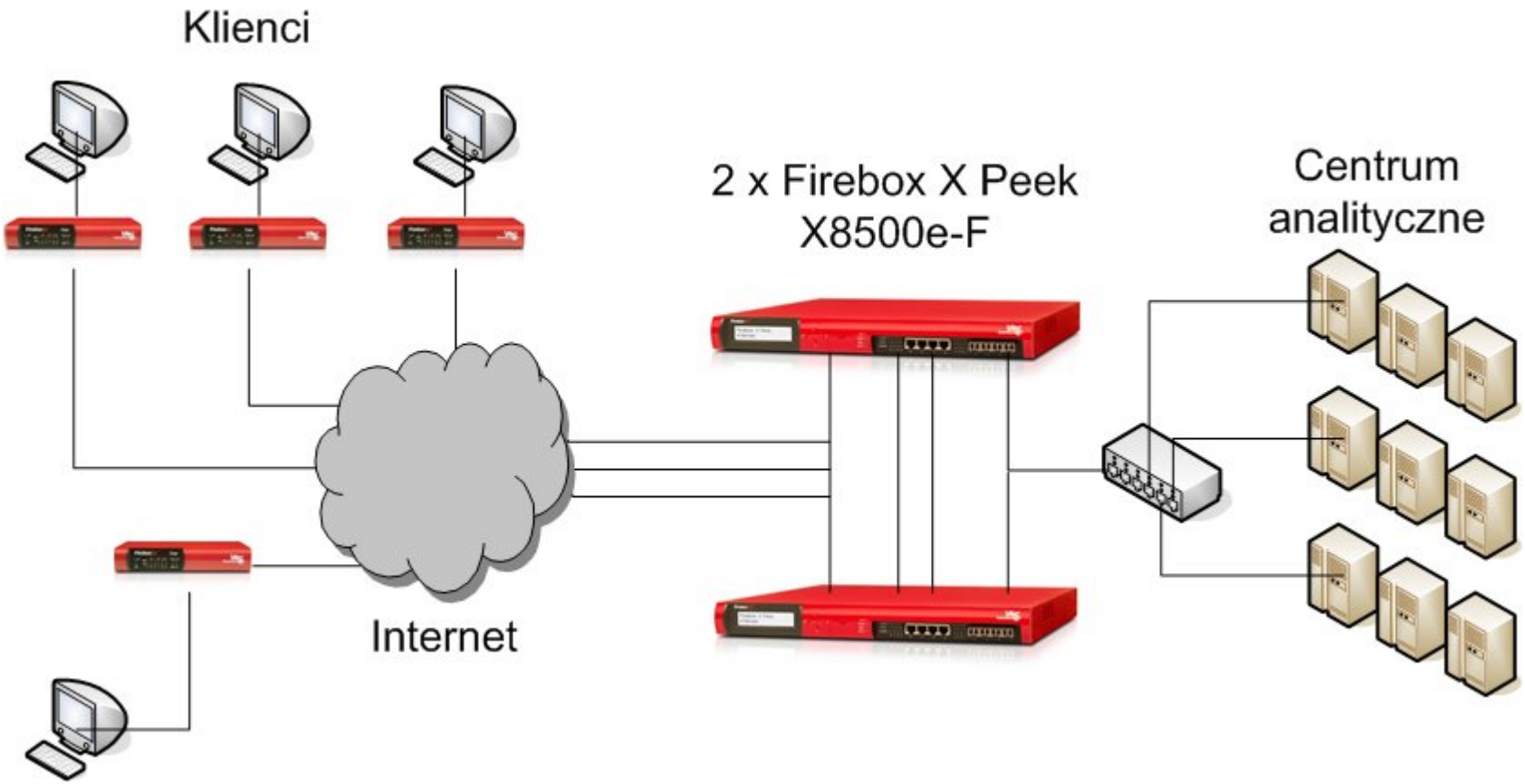
Firma udostępniająca dane pomiarowe
Rozwiązanie firmy CCNS S.A.

- **Klienci**
  - Wyposażone w niewielkie urządzenia spełniające rolę końcówki VPN
  - Wymiana danych analitycznych poprzez tunel VPN
- **Centrum analityczne**
  - Sieć chroniona za pomocą zintegrowanej zapory i koncentratora VPN
  - Zastosowano technologię High Availability,
    - Drugie identyczne urządzenie pełni rolę zamiennika
    - Oba urządzenia są zsynchronizowane
    - W przypadku awarii pierwszego urządzenia jego rolę przejmuje zamiennik
  - W celu odseparowania poszczególnych serwerów zastosowano technologię VLAN

Firma udostępniająca dane pomiarowe
Rozwiązanie firmy CCNS S.A.



Firma udostępniająca dane pomiarowe
Rozwiązanie firmy CCNS S.A.



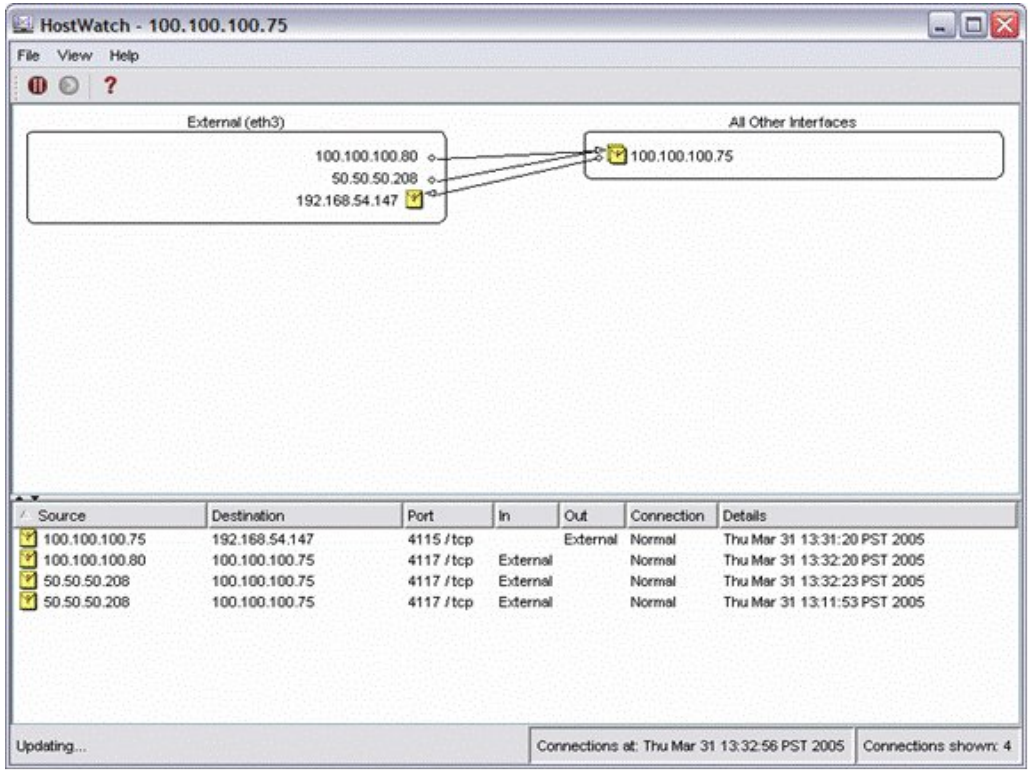
Firma udostępniająca dane pomiarowe

Rozwiązanie firmy CCNS S.A.

- **Urządzenie Firebox® Peek X8500e-F**
  - Zintegrowana zapora sieciowa i koncentrator VPN
  - Obsługa do **400** statycznych tuneli VPN
  - **4 interface'y** Gigabit Ethernet oraz 4 Fiber Optic
  - Obsługa **VLAN**ów (max. 75)
  - Obsługa **High Availability** w trybie Active/Passive
  - Traffic Shaping oraz Quality of Service
  - Obsługa do 4 interface'ów zewnętrznych

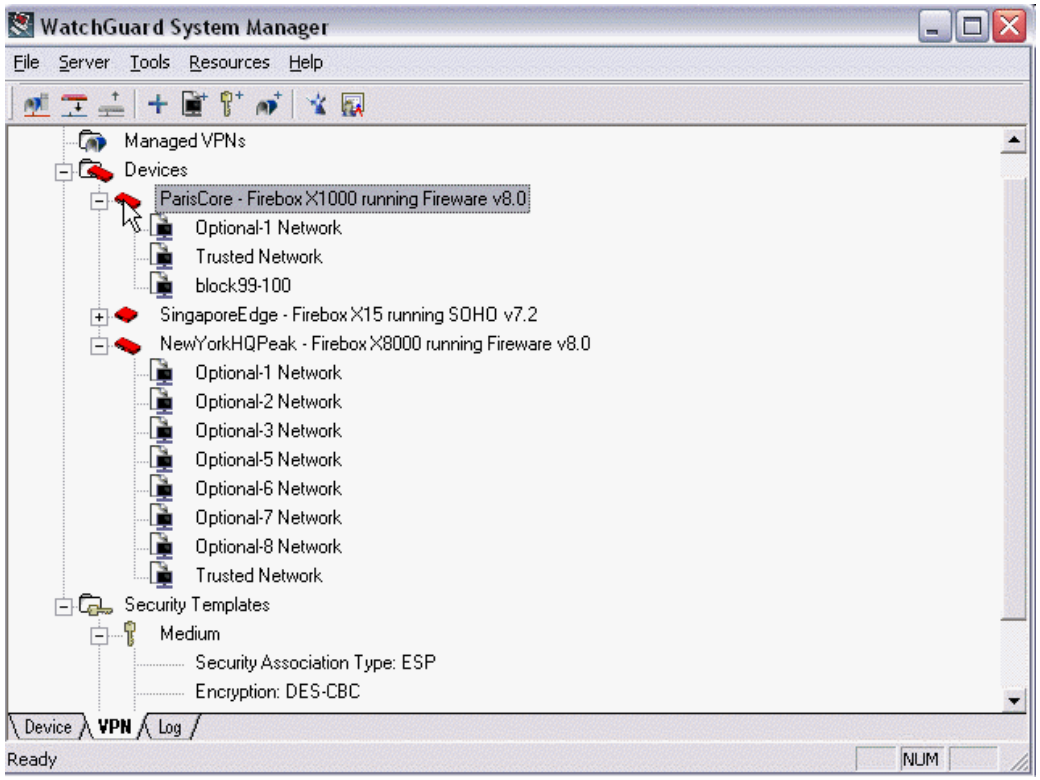
Ogólne cechy urządzeń Firebox
Centralne zarządzanie

- **WatchGuard System Manager**
  - Intuicyjny interface graficzny
  - Zunifikowana konsola zarządzania
  - **Interaktywny monitoring w czasie rzeczywistym**
  - Tworzenie tuneli VPN poprzez technologię Drag-and-drop
  - Bezpieczne logowanie
  - Wyczerpujące raporty o stanie sieci



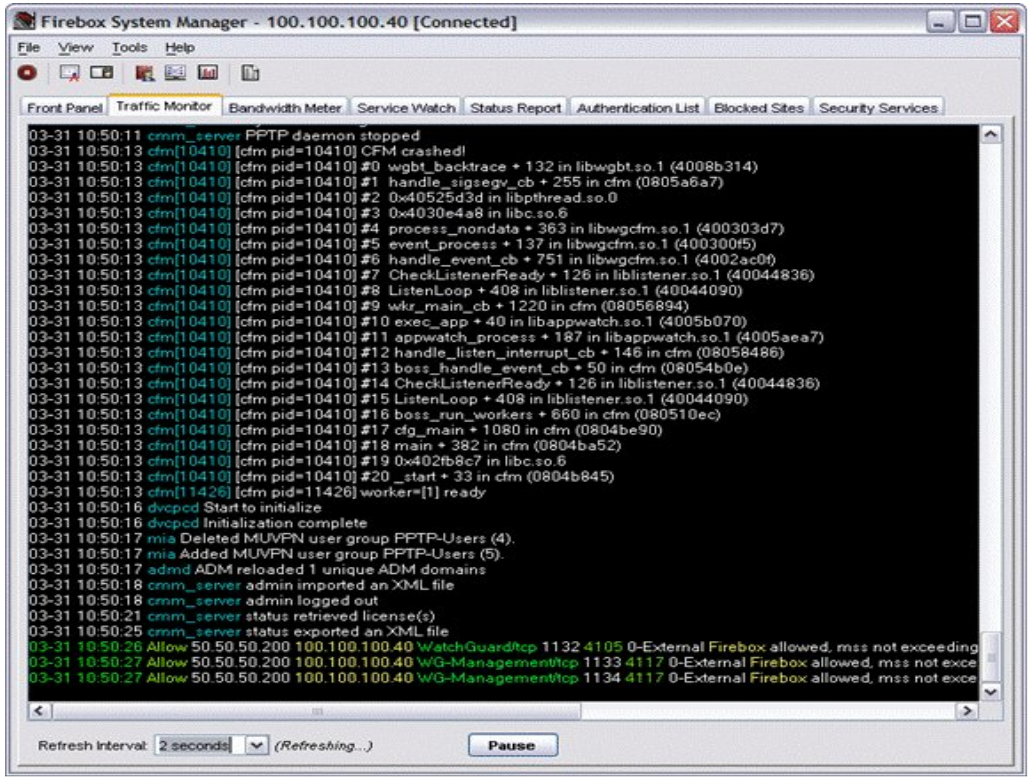
Ogólne cechy urządzeń Firebox
Centralne zarządzanie

- **WatchGuard System Manager**
  - Intuicyjny interface graficzny
  - Zunifikowana konsola zarządzania
  - Interaktywny monitoring w czasie rzeczywistym
  - **Tworzenie tuneli VPN poprzez technologię Drag-and-drop**
  - Bezpieczne logowanie
  - Wyczerpujące raporty o stanie sieci



Ogólne cechy urządzeń Firebox
Centralne zarządzanie

- **WatchGuard System Manager**
  - Intuicyjny interface graficzny
  - Zunifikowana konsola zarządzania
  - Interaktywny monitoring w czasie rzeczywistym
  - Tworzenie tuneli VPN poprzez technologię Drag-and-drop
  - **Bezpieczne logowanie**
  - Wyczerpujące raporty o stanie sieci

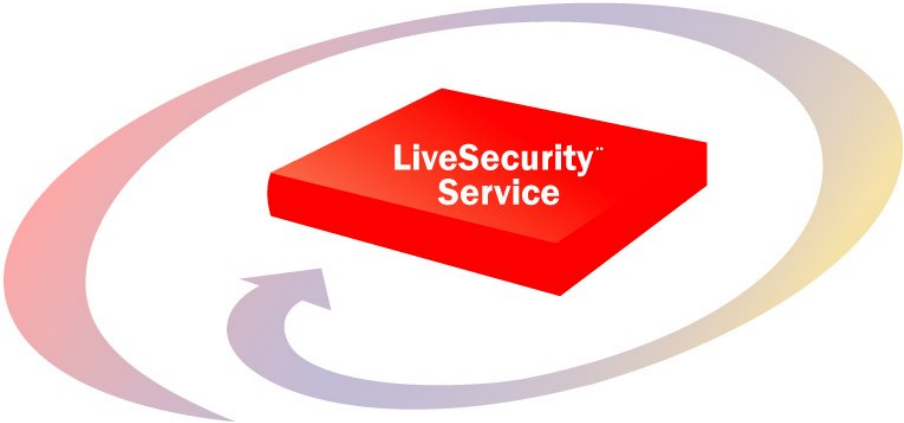


Ogólne cechy urządzeń Firebox
Licencje

- **Wykupienie odpowiedniej licencji daje:**
  - Możliwość rozszerzania funkcjonalności urządzeń
  - Możliwość upgrade'u modelu urządzenia w obrębie tej samej rodziny bez konieczności wymiany sprzętu.
  - Zwiększenie ilości jednoczesnych tuneli VPN
  - Upgrade oprogramowania do wersji Fireware Pro (dla rodziny X Core).
    - Obsługa VLAN
    - Traffic Shaping/QoS
    - Dynamiczny routing (BGP,OSPF)
- **Taka polityka pozwala na:**
  - Zapewnienie ochrony inwestycji
  - Skalowalność rozwiązań

Wsparcie techniczne WatchGuard®
USŁUGA LIVE SECURITY®

- Najbardziej kompleksowe wsparcie w całej branży
  - Specjaliści ds. bezpieczeństwa, konsultanci i inżynierowie stale monitorują sytuację pod kątem bezpieczeństwa
- Zapewnia stałą edukację w formie szkoleń, forum dla użytkowników, chatów w sieci oraz artykułów.
- Obejmuje:
  - Alarmy o zagrożeniach
  - Aktualizacje oprogramowania
  - Wsparcie techniczne
  - Gwarancję sprzętową
- Forma:
  - Płatna subskrypcja roczna



Wsparcie firmy CCNS S.A.
Usługi dodatkowe

- **Wdrażanie rozwiązań firmy WatchGuard**
  - Pomagamy przy projektowaniu i doborze zabezpieczeń sieci
  - Asystujemy podczas procesu konfiguracji urządzeń
  - Weryfikujemy poprawność konfiguracji klienta
- **Autoryzowane szkolenia**
  - Posiadamy tytuł „WatchGuard Certified Training Partner”
  - Prowadzimy szkolenia certyfikujące WCP

Dziękuję za uwagę !

Kontakt
Jakub Wojnarowicz
security@ccns.pl
http://www.ccns.pl