



# Główny Urząd Statystyczny

---

Odpowiedź na pytania do dialogu technicznego nr  
1/sisp-2/2014

# Zadanie 1 – sieć LAN w oddziałach

---

## *Wymiana przełączników dostępowych w Urzędach Statystycznych*

### **Podstawowe wymagania:**

- 48 portów o przepustowości 100/1000 Mbps
- 4 porty SFP
- Wsparcie technologii PoE
- Obsługa protokołów 802.1X, 802.1Q, 802.1p

## Propozycja - Enterasys B5 lub C5 Series

**B5G124-48P2** - B5 (48) 10/100/1000 AT-POE RJ45 ports, (4) combo SFP ports, (2) dedicated stacking ports and external RPS connector

**C5G124-48P2** - C5 (48) 10/100/1000 AT-PoE RJ45 ports , (4) combo SFP ports, (2) high speed dedicated stacking ports and external RPS connector

## Parametry techniczne

- Wsparcie dla PoE+ (802.3at) – możliwość zasilania urządzeń o zwiększonym poborze mocy
- Przepustowość switcha - 96 Gbps (praca z pełną prędkością łącza)
- Możliwość połączenia urządzeń w stos zarządzany i widziany jako jedno urządzenie
- Dożywotnia gwarancja i dostęp do aktualizacji oprogramowania
- Wsparcie dla 802.1p – klasyfikacja ruchu
- Możliwość uwierzytelnienia wielu użytkowników na porcie i przypisania im dedykowanych polityk (zasady dostępu, parametry QoS itd.)
- Możliwość klasyfikowania i znakowanie pakietów na podstawie informacji warstwy 2-4 (MAC, IP, TCP/UDP port, DSCP, ToS)
- Wsparcie dla mechanizmów QoS
  - Ograniczanie przepływności ruchu wchodzącego (COS Inbound Rate Limiting)
  - Różne mechanizmy kolejkowania (8 priorytetowych kolejek na port, mechanizmy SPQ, WRR itd.)
- Obsługuje 802.3ad Link Aggregation
- Możliwość podłączenia redundantnych źródeł zasilania
- Różne metody uwierzytelniania (802.1X, MAC, Web Authentication)
- Wspiera VLAN (802.1Q), dynamic VLAN Assignment (RFC 3580), GARP, GVRP

Tabela 1 – Zestawianie parametrów technicznych przełączników B5 i C5

	<b>C5</b>	<b>B5</b>
Redundant Power	External RPS	External RPS
Additive External PoE Power	Yes	No
802.3af Support	Yes	Yes
802.3at Support	Yes	Yes
Max Power for PoE - internal	850W	375W
Max Power for PoE	1500W	375W
Max PoE Power internal - 48 Ports	17.7W per port	7.8W per port
Max PoE Power - 48 Ports w RPS Supply	30W per port	7.8W per port
Class-based PoE Support	Yes	Yes
Processor Speed	8544 @ 1GHz	8347 @ 667MHz
ECC Memory	Yes	Yes
DRAM (MB)	512	512
Level 1 Cache	32KB	32KB
Level 2 Cache	256KB	None
PHYs	Octal	Octal
Blowers*	No	No
Stacking Bandwidth per Switch (Gbps)	128	48
Stacking Bandwidth per Stack (Gbps)	1024	384
# MAC Addresses	32K	32K
Buffering (per 24 ports)	4MB	2MB
Rules per Profile	250	250
Max Rules per Switch	3072	1536
Users per Port	8	4
Maximum # of Profiles	63	15
EtherType	512	256
DA SA Rules	512	256
L3 Rules	2048	1024
Policy	Included	Included
IP Interfaces	48	24
Number of Static Routes	128	64
Number of RIP Routes	5000	2500
OSPF Areas	8	N/A
Route Table Entries	5000	2500

DVMRP/# of Routes	512	N/A
Virtual Router ID per system	20	N/A
ARP Entries – Total	4048	2024
ARP Entries – Static	1024	512
Access Control Rules Total	400 (ingress only)	200 (ingress only)
Advanced Routing	Optional License	N/A
IPv6 Routing	Included in Adv Routing License	N/A

## Opis Produktu

### Przełączniki serii B/C

Wysoko wydajne przełączniki Gigabit Ethernet Enterasys B5/C5 z możliwością łączenia w stos zapewniają skalowalną wydajność z pełną prędkością łącza. Poza przepustowością przełączania na poziomie do 264 Gbps, przełącznik Enterasys B5/C5 zapewnia do 48 portów 10/100/1000 Ethernet, jak również opcje portów 1GbE i 10GbE typu *uplink*. Dzięki możliwościom łączenia przełączników w stos, 8 z nich (zarówno 24- jak i 48-portowych) może być połączonych ze sobą tworząc wirtualny przełącznik. Zapewnia on wówczas szybkość przełączania do 2.11 Tbps i do 384 portów Ethernet 10/100/1000, jak również możliwość obsługi 16 portów 10GE typu *uplink*. Wszystkie przełączniki pracujące w stosie zarządzane są przez jeden adres IP, a zarządzanie stosem jest redundantne. Połączenie między urządzeniami wykonane jest w formie zamkniętej pętli (*Closed Loop Stacking*) - w wypadku awarii kabla łączącego przełączniki lub jeden z nich, nie następuje utrata łączności pomiędzy urządzeniami w stosie. Przełącznik B5/C5 zapewnia także funkcje podnoszące niezawodność, takie jak rozproszone grupy LAG (*Distributed Link Aggregation Groups*). Realizując zaawansowane funkcje zarządzania politykami firmy Enterasys, przełącznik B5/C5 oferuje kontrolę pasma, QoS oraz polityki bezpieczeństwa dla maksymalnie ośmiu użytkowników na porcie, w oparciu o widoczność ruchu z warstw L2/L3/L4. Oprócz przełączania w warstwie L2 i obsługi standardu IPv4 RIPV1/v2, opcjonalne aktualizacje licencji zapewniają zaawansowany routing IPv4 i IPv6 (tylko C5).



Wysoce dostosowywalne funkcje klasyfikacji pakietów warstw L2/L3/L4 współdziałają z 8 sprzętowymi kolejkami priorytetowej obsługi przypisanymi do każdego portu Ethernet. Ma to na celu zapewnienie zbioru różnorodnych usług, na 8 odrębnych poziomach priorytetów, zapewniających gwarantowany poziom *Quality of Service* (QoS) dla krytycznego ruchu sieciowego. Duże możliwości konfiguracji klasyfikacji pakietów warstw L2/L3/L4 przez przełączniki i ich inteligentne mechanizmy kolejkowania gwarantują, że istotne dla danej organizacji aplikacje uzyskają nadrzędny dostęp do zasobów sieci. Wykorzystując możliwości polityk zapewniane przez Enterasys, administrator sieci może określić różne role lub profile, które reprezentują określone grupy operacyjne w ramach

organizacji. Każdej określonej roli przyznawany jest indywidualny dostęp do określonych usług i aplikacji sieciowych (np. administrator, dyrektor, technik, gość) i te przywileje dostępu pozostają związane z użytkownikami, którzy mogą się przemieszczać w obrębie całej sieci. Użytkownicy są uwierzytelniani przez IEEE 802.1X, adres MAC lub przy wykorzystaniu przeglądarki internetowej, a następnie przypisywani do określonej wcześniej roli operacyjnej, co daje pewność, że każdy użytkownik ma dostęp do odpowiednich dla niego informacji. Dzięki temu zasoby sieciowe są wykorzystywane zgodnie z celami i priorytetami organizacji.

## Parametry ofertowe

Parametr	Wartość netto
<b>\$ 5 995,00</b>	\$ 5 995,00
<b>\$ 8 995,00</b>	\$ 8 995,00
<b>28 dni</b>	28 dni
<b>15 dni roboczych</b>	15 dni roboczych

## Zadanie 2 – Segment Data Center

Zakup kart do Cisco 6500 oraz dwóch przełączników modułowych

### Moduły Cisco 6500

Model	Nazwa	Ilość	Cena za sztukę netto	Cena całkowita netto
<b><i>Dla nowego chassis 6500 (E – Series)</i></b>				
<b>VS-S2T-10G</b>	Cisco Catalyst 6500 Series Supervisor Engine 2T	2	28000 \$	\$56 000,00
<b>WS-X6848-TX-2T=</b>	Karta serii 6800, 48 portów RJ45	2	15000 \$	\$30 000,00
<b>WS-X6908-10G-2T=</b>	Karta serii 6900, 8 portów 10 Gbps SFP+	2	40000 \$	\$80 000,00
<b><i>Dla starego chassis 6500 (no E – Series) z wymienionymi wentylatorami</i></b>				
<b>VS-S720-10G-3C</b>	Cisco Catalyst 6500 Series Supervisor Engine 720	2	38000 \$	\$76 000,00
<b>WS-X6748-GE-TX=</b>	Karta serii 6700, 48 portów RJ45	2	15000 \$	\$30 000,00
<b>WS-X6708-10G-3C=</b>	Karta serii 6700, 8 portów 10 Gbps SFP+	2	37500 \$	\$75 000,00

### Nowe przełączniki - Enterasys S-Series

Zaproponowane zostały przełączniki do Data Center firmy Enterasys. Są to urządzenia modułowe z trzema slotami na karty liniowe. W chassis nie ma modułu supervisor – każda z trzech kart równocześnie odpowiada za logikę i przełączanie. Awarie dowolnej nie powoduje przerwy w pracy.

Model	Nazwa	Cena netto
<b>S3A-Chassis</b>	S-Series S3 Chassis and fan tray(Power supplies ordered separately)	\$8 495,00
<b>ST2206-0848</b>	S-Series S140 I/O Module - 48 Ports 10/100/1000BASE-TX via RJ45 with PoE (802.3at) and two Type2 option slot (Used in S3/S4/S6/S8)	\$26 995,00
<b>SK2008-0832</b>	S-Series S140 Class I/O Module -32 Ports 10GBASE-X via SFP+ (Used in S3/S4/S6/S8)	\$53 995,00
<b>SK2009-0824</b>	S-Series S140 Class I/O Module 24 Ports 10GBASE-T via RJ45 (Used in S3/S4/S6/S8)	\$53 995,00

## Parametry techniczne

### Porównanie Enterasys i Cisco

Parametr	Enterasys S-Series (S180)	Cisco 6500-E z 2T supervisor
<b>Switching performance</b>	120 Gbps / slot	80 Gbps / slot
<b>Routing performance</b>	Do 960 Mpps	Do 720 Mpps
<b>Bufor pakietów / port</b>	ponad 40 MB	poniżej 1 MB
<b>Uwierzytelnienie wielu użytkowników na porcie</b>	Pełne – tysiące użytkowników	Ograniczone
<b>Szczegółowa kontrola QoS per użytkownik</b>	Tak – domyślnie	Tylko z dedykowanym service module
<b>Wsparcie dla polityk</b>	Tak – zaawansowane reguły dostępu per użytkownik	Ograniczone – tylko ACL, VLAN

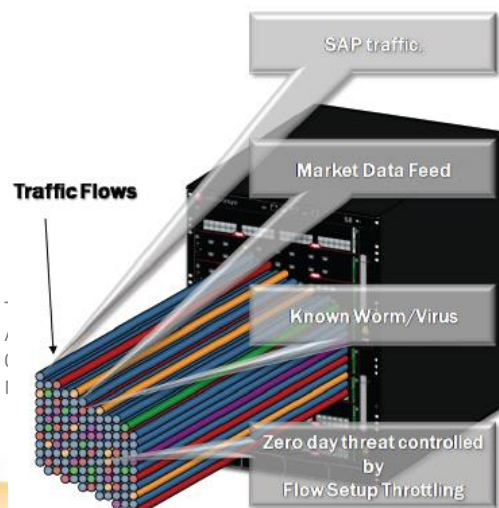
## Opis produktu

### Sprzęt sieci LAN

Enterasys oferuje szereg zarządzalnych przełączników dostarczając tym samym rozwiązania spełniające wymagania od obszarów dostępowych aż po rdzeń sieci. Produktami, które według nas są najlepiej dopasowane do celów i założeń klienta są przełączniki Enterasys Serii S z wbudowanym bezpieczeństwem. Wszystkie proponowane przełączniki obsługują najlepszą na rynku szczegółową kontrolę nad priorytetami i parametrami bezpieczeństwa poprzez role użytkowników i aplikacji zapewniając jednocześnie pełną mobilność użytkowników. Te środki kontroli mogą być egzekwowane statycznie oraz dynamicznie dla wielu użytkowników na pojedynczym porcie. Przełączniki Enterasys z obsługą polityk pozwalają Państwu na aktywną ochronę przed incydentami bezpieczeństwa i gwarantują odpowiedni poziom usług przez ograniczanie przepustowości ruchu sieciowego, nadawanie mu priorytetów, blokowanie go lub poddawanie kwarantannie w oparciu o przywileje użytkownika, priorytet aplikacji lub wymagane protokoły. W rezultacie uproszczone jest zarządzanie infrastrukturą sieci, bo jest ona traktowana jako zintegrowany system. Enterasys stosuje w swoich produktach standardy branżowe i otwartą architekturę zapewniając tym samym kompatybilność i współpracę z urządzeniami wielu różnych dostawców.

### Seria S

Proponowane urządzenia Enterasys Serii S są idealnie dopasowane do zastosowania w warstwie rdzeniowej infrastruktury sieci. Seria S posiada bardzo elastyczną rozproszoną architekturę przełączania i routingu z funkcjami kontroli i zarządzania wbudowanymi w każdy moduł, dostarczając w ten sposób niezrównaną niezawodność, skalowalność i odporność na błędy. Przełączniki serii S wprowadzają najlepszą na rynku, opartą na przepływie architekturę przełączania by inteligentnie zarządzać indywidualnymi połączeniami użytkowników lub aplikacji – wykracza to



poza standardowe możliwości przełączników ograniczonych do stosowania sieci VLAN i list ACL w celu realizacji opartych na rolach środkach kontroli dostępu. Architektura ta zapewnia, że gdy określony przepływ komunikacyjny zostanie ustanowiony pomiędzy dwoma punktami końcowymi, pierwsze pakiety tego przepływu będą przetwarzane przez mechanizmy wielowarstwowej klasyfikacji w modułach I/O przełącznika. Podczas tego procesu identyfikowana jest rola, określane są stosowane polityki, przeprowadzana jest inspekcja pakietów i wyznaczona jest odpowiednia akcja. Po zidentyfikowaniu przepływu, wszystkie kolejne związane z nim pakiety są automatycznie obsługiwane przez Enterasys ASIC bez konieczności dalszego przetwarzania. W ten sposób przełącznik Enterasys Serii S może zapewnić bardzo szczegółowy poziom kontroli każdego przepływu przy pełnej prędkości łącza. Identyfikacja użytkowników i przypisywanie ról są realizowane, aby zapewnić każdemu użytkownikowi oddzielnie możliwość uzyskania dostępu do krytycznych dla niego aplikacji niezależnie od miejsca, z którego łączy się z siecią. Reguły polityk Serii S połączone ze szczegółową inspekcją pakietów mogą inteligentnie wykrywać i automatycznie reagować na zagrożenia bezpieczeństwa, poprawiając tym samym niezawodność i jakość obsługi systemu przez użytkowników.

Na rodzinę produktów Serii S składają się płaszczyzny montażowe (*chassis*): S8 z 8 gniazdami, S4 z 4 gniazdami i S3 z 3 gniazdami oraz wolnostojący przełącznik o ustalonej konfiguracji SSA (*S-Series Stand Alone*). Płaszczyzna montażowa serii S wykorzystuje zarówno architekturę przekazywania opartą na strukturze (*Fabric-Based*) typu punkt-punkt oraz kratową architekturę niewykorzystującą struktury (*Fabric-Less*). *Chassis* S4 i S8 wykorzystują architekturę przekazywania opartą na strukturze, która zapewnia wiele ścieżek danych o dużej przepustowości pomiędzy modułami I/O, natomiast S3 posiada wysoce wydajną kratową architekturę przekazywania, która nie wykorzystuje struktury i jest idealnie dopasowana do wysoce dostępnych implementacji w szafach kablowych na skraju sieci. Wszystkie płaszczyzny montażowe (*chassis*) są zoptymalizowane dla realizacji redundantnego wysoce wydajnego przełączania i routingu, jak również zapewniania elastycznej łączności i możliwości dodawania nowych funkcji oraz zwiększania osiągnięć w miarę potrzeb i pojawiania się nowych technologii.

Moduły struktury I/O (*Fabric Module*) posiadają skalowane, wysoce wydajne ścieżki do przesyłania danych, jak również pełny zestaw interfejsów na przednim panelu wraz z opcjami elastycznych, modułowych interfejsów. Pojedynczy moduł struktury I/O może być stosowany zarówno w S4 jak i S8. Zastosowanie dwóch modułów struktury I/O tworzy parę struktury współdzielącą obciążenie, która zapewnia przepustowość przełączania do 1280 Gbps i dodaje funkcje wysokiej dostępności. *Chassis* S8 powiększa możliwości pary struktury współdzielącej obciążenie umożliwiając dodanie trzeciego modułu struktury I/O (*Fabric Module*), wzrasta dzięki temu niezawodność systemu na wypadek awarii modułu struktury I/O oraz dostępność i wydajność wymagane przez krytyczne dla działania organizacji sieci. Moduły struktury I/O (*Fabric Module*) oraz moduły I/O są dostępne z szeroką gamą interfejsów i wysoką gęstością portów (10/100/1000BASE-TX, 1000BASE-X SFP oraz 10GBASE-X SFP+) w celu spełniania różnorodnych wymagań stawianych przez daną sieć. Wszystkie oferowane moduły I/O z interfejsami miedzianymi obsługują funkcję PoE. Wiele modułów I/O wyposażonych jest również w jedno lub dwa gniazda do instalacji opcjonalnych modułów. W gnieździe tym można umieścić opcjonalne moduły 1GbE lub 10GbE zapewniając tym samym dodatkowe medium transmisyjne i szybszą transmisję. W konsekwencji projekt sieci ulega znacznemu uproszczeniu i zmniejszają się koszty budowy sieci.

Urządzenia Serii S oferują wiele standardowych funkcji wysokiej dostępności. Dzięki sprzętowym funkcjom wysokiej dostępności przełączniki Serii S mogą być instalowane w krytycznych



środowiskach, które wymagają dostępności 24/7. Seria S obsługuje następujące sprzętowe funkcje wysokiej dostępności:

- Pasywna płyta montażowa (*backplane*) w *chassis* S3, S4 i S8.
- Kratowa architektura płyty montażowej (*backplane*) w *chassis* S3.
- Półki wentylatorów z możliwością wymiany podczas pracy (*hot-swap*) i wieloma wentylatorami.
- Oddzielne zasilacze systemowe oraz PoE.
- Zasilacze z funkcją wymiany podczas pracy (*hot-swap*).
- Moduły struktury I/O (*Fabric Module*) dla realizacji podziału obciążenia i redundancji w *chassis* S4 i S8.
- Redundancja struktury typu N+1 w *chassis* S8.
- Moduły I/O i moduły struktury I/O z możliwością wymiany podczas pracy (*hot-swap*).
- Wiele procesorów hosta dla redundancji N+X.

## Parametry ofertowe

	Ceny netto
<b>Cena Katalogowa Moduły do Cisco 6500</b>	\$166 000,00
<b>Cena katalogowa netto – Enterasys</b>	\$143 480,00
<b>Czas dostawy urządzeń</b>	28 dni

## Zadanie 3 – Monitoring

*System do monitorowania sieci oraz aplikacji*

### Propozycja – Netscout nGenius

Model	Opis	Cena netto
<b>Oprogramowanie monitorujące (przetwarzanie i prezentacja danych)</b>		
<b>9600X-XX</b>	nGenius One (produkt najwyższy, integrujący większość funkcji i produktów, w tym poniższy Performance Manager)	od \$50,000.00 *
<b>9500X-XX</b>	Performance Manager (produkt o mniejszej funkcjonalności)	od \$20,000.00 *
<b>Urządzenia przechowujące pakiety – sondy</b>		
<b>1906/TS</b>	nGenius InfiniStream, 2-Port 10/100/1000Base-T, 1TB (najmniejsza wersja)	\$19,995.00
<b>6980/VS</b>	nGenius InfiniStream, 8-Port Gigabit Configurable, 16TB (prawie największa wersja)	\$125,000.00
<b>Pozostałe źródła danych</b>		
<b>VA1300</b>	nGenius Virtual Agent (4-Pack)	\$4,000.00
<b>IA1110</b>	nGenius Integrated Agent for Cisco UCSe (4-pack)	\$4,000.00
<b>3300/LS</b>	nGenius Collector, 10/100/1000Base-T Interface, 2TB	\$25,000.00

\* - licencjonowane w zależności od ilości monitorowanych elementów.

### Opis produktu

Rozwiązanie firmy Netscout pozwala na monitorowanie działania aplikacji i sieci. Głównym źródłem danych o wydajności działania tych elementów jest monitorowanie rzeczywistego ruchu sieciowego. Produkty takie jak: sondy, agenci dla maszyn wirtualnych czy moduły do routerów pozwalają analizować ruch na poziomie pakietów, wyodrębnić strumienie, sesje i aplikacje. Rozpoznawanie aplikacji i świadomość protokołów pozwala na zagłębienie w pakiety i analizowanie zdarzeń. Dzięki temu możliwe jest np. raportowanie błędów, retransmisji czy wysokich czasów odpowiedzi.

### nGenius ONE

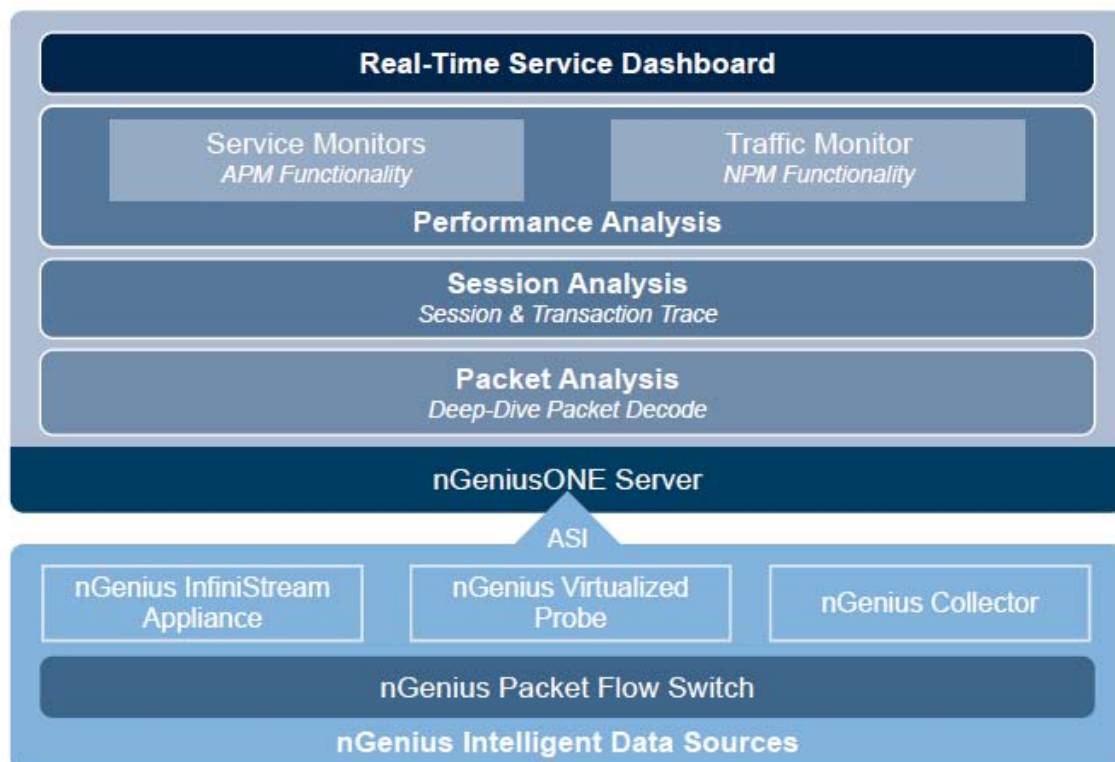
Oprogramowanie do monitorowania wydajności aplikacji, sieci i serwerów. Integruje dane otrzymywane z różnych źródeł opisanych poniżej (wyspecjalizowane sondy, agenci na serwerach wirtualnych, moduły w routerach Cisco, dane NetFlow). Jest to wygodny interfejs do całego systemu, pozwalający czuwać nad jakością dostarczania usług. System posiada rozbudowane możliwości badania jakości usług głosowych i video.

### Kluczowe aspekty produktu

- Jedna zunifikowana platforma łącząca zarządzanie wydajnością aplikacji i sieci, umożliwiającą kontrolowanie wszystkich elementów składających się na odczucie użytkownika końcowego.
- Wgląd w wydajność usług z poziomu makro jak i mikro, od strony całej korporacji, lokalizacji, grupy użytkowników , serwerów itd.
- Widoczność w złożone środowiska dostarczania usług typu „multi-tier” składające się z wielu współpracujących serwerów, interfejsów i użytkowników.
- Efektywne zarządzanie dostępnością i stanem różnorodnych usług
- Bogate widoki graficzne zarówno w czasie rzeczywistym jak i historycznym generowane na podstawie analiz ruchu na poziomie pakietów.
- Łatwe w użyciu scenariusze działania (workflows) pozwalają na szybkie wyszukiwanie przyczyn problemów.
- Skalowalne rozwiązanie klasy enterprise pozwalające na monitorowanie bardzo dużych sieci.

### Możliwości

- Panel „Service Dashboard” zapewnia wgląd w czasie rzeczywistym w logiczną strukturę usług ułożoną w hierarchię odpowiadającą biznesowej rzeczywistości w przedsiębiorstwie.
- Analiza wydajności zorientowana na usługi
- Możliwość przechodzenia na coraz bardziej szczegółowe poziomy badania stanu sieci/aplikacji aż do wglądu w same pakiety.
- Identyfikacja ruchu widzianego w kilku punktach monitorowania i przypisywanie go do konkretnych sesji – możliwość monitorowania transakcji „hop-by-hop”
- Rozbudowane możliwości definiowania własnych usług i budowania hierarchii
- System na podstawie obserwowanego ruchu jest w stanie wyznaczyć wzorce zachowań i raportować odstępstwa i anomalie
- System integruje się z systemami zarządzania innych producentów, takimi jak: EMC Smarts, HP Network Node Manager czy IBM Tivoli. Wspierana jest dwustronna komunikacja. Alarmy generowane przez nGeniusONE przekazywane są do zewnętrznych systemów wraz z linkami do szczegółowych opisów.
- Bogate możliwości raportowania



**Figure 1: nGeniusONE unifies application performance management and network performance management in a single platform to deliver correlated metrics and simplified workflows that dramatically streamline service delivery management activities.**

## nGenius InfiniStream Appliance

Inteligentne urządzenie służące do zbierania pakietów i analizowania ruchu sieciowego. Zapewnia dedykowane, dostępne w sposób ciągły możliwości monitorowania i rozwiązywania problemów sieciowych. W czasie rzeczywistym generuje szczegółowe metadane, które pozwalają w łatwy sposób monitorować wydajność usług, sieci, aplikacji i serwerów w skomplikowanych środowiskach typu multi-tier i multi-domain.

Urządzenie interpretuje i analizuje pakiety nawet do warstwy 7, ponadto przechowuje je na własnych dyskach w celu późniejszej szczegółowej analizy. Sonda musi mieć dostęp do ruchu sieciowego na łączach zbiorczych (Span port lub TAP). Zapisywane pakiety można filtrować, przechowywać w całości lub tylko nagłówki. Ma to wpływ na długość okresu dla którego przechowywane są pakiety. Pojemność sondy w zależności od modelu mieści się między 1 a 96 TB.

Oprócz wykrywania aplikacji i monitorowania ruchu generowanego przez każdą z nich, sonda rozpoznaje ruch na poziomie sesji / transakcji, może raportować czasy odpowiedzi czy też kody błędów, anomalie działania, bądź też „session events” znanych protokołów.

## nGenius Virtual Agent

Jest to software agent do instalacji w środowiskach wirtualnych. Pozwala uzyskać wgląd w ruch generowany przez wirtualne serwery, nawet gdy zamyka się on wewnątrz szafy blade. Współpracuje on z oprogramowaniem monitorującym nGeniusONE. Pozwala na kontrolowanie: KPI (Key Performance Indicators), czyli wskaźników wydajności działania usług i sieci, zapewnia dostęp do pakietów, umożliwia generowanie alarmów. Wraz z innymi elementami systemu (Intelligent Data Sources) zapewnia wgląd w sposób dostarczania treści na zasadzie „end-to-end” czyli od serwera do klienta.

## nGenius Integrated Agent

Obecnie wyniesione oddziały potrzebują takiej samej gwarancji dostępu do usług biznesowych jak ich odpowiedniki w lokalizacji centralnej. Wymagany jest też taki sam poziom kontroli. Produkt nGenius Integrated Agent pozwala uzyskać dostęp do danych o wydajności sieci, aplikacji i serwerów już po stronie oddziału. Jest to fizyczny moduł dodawany do routerów Cisco ISR. Dzięki temu eliminowana jest konieczność instalacji kosztownych urządzeń InfiniStream Appliance. Agent posiada takie same możliwości jak sonda, za wyjątkiem własnych dysków, jednak jest możliwe uruchamianie zbierania pakietów na żądanie na zewnętrzny zasób – moduł posiada dedykowane interfejsy które mogą działać jak Span Porty.

### Możliwości monitorowania

- Pełne wsparcie dla strumieni (flow) na poziomie pakietów – wgląd w wydajność i obciążenie aplikacji, sieci i serwerów.
- Analiza czasów odpowiedzi, kluczowych wskaźników wydajności (KPI), stanu aplikacji i usług
- Integracja i raportowanie do systemu monitorującego nGeniusONE

### Zalety

- Wczesne, inteligentne powiadamianie o pojawiających się problemach w oddziałach
- Spójna widoczność stanu sieci i aplikacji w relacji ent-to-end (od Data Center do użytkownika końcowego)
- Szczegółowy wgląd w wykorzystanie aplikacji i zasobów sieciowych po stronie oddziału, możliwość badania jakości obsługi doświadczanej przez użytkowników w lokalizacji – narzędzia do planowania i efektywnego wykorzystywania zasobów.
- Lokalna widoczność wydajności i dostęp do pakietów skraca czas rozwiązywania problemów.

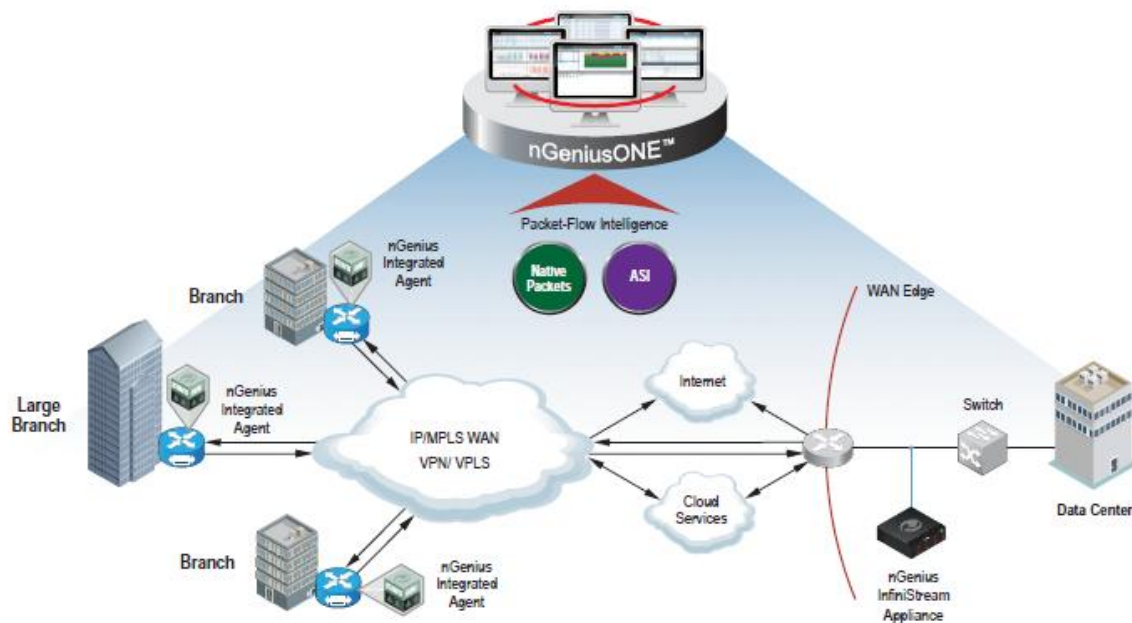


Figure 1: nGenius Integrated Agent enables traffic visibility between site to data center and site-to-site for decentralized networks.

## nGenius Collector

Jest to fizyczne urządzenie do zbierania statystyk NetFlow i podobnych oraz wykonywania testów Cisco IP SLA. Integruje się z oprogramowaniem monitorującym nGeniusONE.

### Możliwości:

- Mierzy szybkość działania usług w sieci wykorzystując do pięciuset syntetycznych testów transakcji Cisco IP SLA.
- Może zbierać dane Cisco NetFlow, Juniper J-Flow, Huawei NetStream i sFlow z wydajnością do dwóch milionów na minutę.
- Kolekcjonuje dane o strumieniach do późniejszej analizy. Do pięciu tysięcy routerów i switchów na urządzenie.
- Wspiera środowiska IPv4 i IPv6

## Parametry ofertowe

<b>Termin wdrożenia</b>	<b>2-8 tygodni *</b>
<b>koszt wdrożenia</b>	<b>15-50 tyś pln * netto</b>

\* - czas i koszt wdrożenia jest uzależniony od ilości źródeł danych, realizowanych integracji i struktury(ilości) monitorowanych usług.

## Zadanie 4 – Sieć WiFi

### Propozycja – Enterasys Wireless

Model	Nazwa	Cena netto
<b>WS-V2110-8-ROW</b>	V2110 Virtual Controller for Rest-of-World (verify country availability before ordering). Base of 8 APs, expandable to 250 APs in 1 or 16 AP increments	\$2 695,00
<b>WS-APCAP-16</b>	WLAN controller capacity upgrade for C25, and V2110. Increases capacity of WLAN controller by 16 access points.	\$2 295,00
<b>WS-AP3705i</b>	Dual radio 11abgn 2X2:2 MIMO indoor access point w/ integrated ceiling clips (wall and protruded drop ceiling brackets sold separate)	\$595,00
<b>WS-AP3710i</b>	DUAL RADIO 3X3:3 MIMO INTEGRATED ANTENNA	\$1 095,00

### Opis produktu

#### Szybki przegląd

IdentiFi to nagradzane urządzenia bezprzewodowe zapewniające wyjątkowe doświadczenia użytkownika, niezależnie od lokalizacji.

Nasze urządzenia bezprzewodowe są proste we wdrożeniu oraz zarządzaniu, zapewniają zaawansowane funkcjonalności pozwalające organizacjom na dokładne definiowanie jak ruch bezprzewodowy (w tym głos/video/data) ma być przesyłany, niezależnie od architektury oraz zgodnie z wymaganiami biznesowymi.

Wirtualne i fizyczne urządzenia IdentiFi cechuje budowa odporną na awarie, bez konieczności instalowania bądź kupowania dodatkowego oprogramowania. Urządzenia pracują jako pary active-active. W sytuacji awarii drugie urządzenie z pary jest w stanie przejąć całe obciążenie utrzymując połączenie między punktami dostępowymi. Przejęcie następuje w przeciągu milisekund; punkty dostępowe utrzymują pracę bez żadnych przerw czy też wpływu na obecnych lub nowych klientów.

- Skalowalne rozwiązania do 2000 punktów dostępowych na jedno urządzenie z jednolitym systemem zarządzania wykorzystującym standard 802.11n oraz 802.11a/b/g.
- Niezauważalne przełączenia pomiędzy punktami dostępowymi.
- Zintegrowane bezprzewodowe IPS zapewniające proaktywną ochronę przed zagrożeniami bezpieczeństwa.
- Rozwiązanie dla architektury o wysokiej dostępności dla ruchu czasu rzeczywistego (aplikacje głosu/video/data).

### Korzyści

Ujęcie biznesowe:

- Wsparcie dla aplikacji głosowych/video/data, pozwala na zwiększenie produktywności i komfortu pracowników mobilnych.
- Grupowanie użytkowników, urządzeń i aplikacji na podstawie ich ról umożliwia gwarancję jakości usług (QoS) oraz wysoki poziom bezpieczeństwa w zależności od potrzeb biznesowych.
- Zintegrowanie mechanizmów zarządzania, bezpieczeństwa oraz gwarancji jakości usług pozwala na zredukowanie kosztów operacyjnych i zapewnia użytkownikowi takie same możliwości niezależnie od lokalizacji.
- Kluczowe elementy rozwiązań mobilnych to funkcje VoWLAN oraz Dual-Mode Devices.

Wydajność operacyjna:

- Scentralizowanie kontroli i przeglądu sieci upraszcza zarządzanie, przyspiesza rozwiązywanie problemów, optymalizuje wykorzystanie zasobów sieciowych oraz umożliwia automatyczne reakcje na zagrożenia pochodzące ze strony sieci bezprzewodowej.
- Zintegrowane zarządzanie siecią przewodową i bezprzewodową oraz kontrola dostępu oparta na przypisanych rolach znacząco zmniejszają czas i nakład pracy administracyjnej.
- Adaptacyjna architektura redukuje złożoność oraz optymalizuje przepływ informacji pomiędzy aplikacjami.

Bezpieczeństwo:

- Funkcje uwierzytelnienia i autoryzacji zawarte w kontroli dostępu opartej na przypisanych rolach wykorzystują techniki: 802.1X, uwierzytelnienie poprzez MAC, *captive portal*.
- Wykorzystanie szeregu standardów szyfrujących – WEP, TKIP, WPA, WPA2, WPA-PSK, WPA2-PSK, AES.
- Wykorzystanie zewnętrznego *captive portal* pozwala na pełną dowolność ustawień konta gościa.
- Integracja sieci przewodowej i bezprzewodowej zwiększa bezpieczeństwo przeciwko włamaniom.
- Ochrona ruchu zarządzającego, sterującego oraz informacyjnego przed atakiem typu odmowa dostępu do usługi (DoS).

Wsparcie i usługi:

- Wiodące w branży wyniki uzyskane w kategorii *Satysfakcja klienta* oraz *Analiza problemu przy pierwszym połączeniu z serwisem*.
- Personalizacja usług, m.in. analiza u klienta, zaprojektowanie sieci, instalacja, szkolenia.
- Dożywotnia gwarancja na wybrane urządzenia bezprzewodowe.



## IdentiFi™ - Całościowe rozwiązanie Wi-Fi

Dystrybucja inteligencji na punkty dostępowe, kontrolery i narzędzia do zarządzania



### Punkty dostępowe

- Półautonomiczne punkty dostępu
- Własny projekt/ specjalnie opracowane
- Silne bezpieczeństwo – WPA2, WIDS/WIPS, AAA, narzędzia dochodzeniowe
- Osiągi 2x HD Video
- Zoptymalizowane anteny dla lepszego pokrycia łącznością radiową – lepsze wrażenia użytkowników
- Porty Gigabit Ethernet – brak wąskich gardeł
- Efektywność energetyczna – niski pobór mocy

### Kontrolery

- Fizyczne i wirtualne kontrolery
- Wysoka dostępność (brak zakłóceń)
- Elastyczność SFP+ (1G/10G)
- Sprzętowe przyspieszenie szyfrowania
- Obsługa do 2000 punktów dostępu i 32000 użytkowników na kontroler
- Gotowość do obsługi 802.11ac

### Zarządzanie

- Ujednolicona widoczność, kontrola i automatyzacja
- Zautomatyzowany, sterowany politykami system dla sieci przewodowej i Wi-Fi, zapewnia spójne wrażenia użytkowników, niezależnie od metody połączenia z siecią
- Wbudowane analizy widma i kontrola łączności radiowej
- Automatyczne zarządzanie łącznością radiową
- Wiele dróg przesyłania danych/ ról dla każdego pojedynczego SSID

25



now part of



## Punkty dostępowe **IdentiFi™**

*Całkowicie nowa, zaawansowana technologia*

Atrakcyjna cena	Wydajność	Wysoka dostępność	Zewnętrzne
<b>3705i</b> <ul style="list-style-type: none"> <li>❖ 11abgn, 2x2:2 MIMO</li> <li>❖ Dwuzakresowy</li> <li>❖ 802.3af PoE</li> <li>❖ Mesh, polityki, QoS</li> <li>❖ Opcjonalny WIDS, WIPS, analizy widma</li> <li>❖ Zaawansowane funkcje 11n (formowanie wiązki, LDPC, STBC)</li> <li>❖ 40.000 pps</li> <li>❖ Obudowa przypominająca detektor dymu</li> </ul> 	<b>3710i/e</b> <ul style="list-style-type: none"> <li>❖ 11abgn, 3x3:3 MIMO</li> <li>❖ Dwuzakresowy</li> <li>❖ 802.3af PoE</li> <li>❖ Mesh, polityki, QoS</li> <li>❖ Opcjonalny WIDS, WIPS, analizy widma</li> <li>❖ Zaawansowane funkcje 11n (formowanie wiązki, LDPC, STBC)</li> <li>❖ 60.000 pps</li> </ul> 	<b>3715i/e</b> <ul style="list-style-type: none"> <li>❖ 11abgn, 3x3:3 MIMO</li> <li>❖ Dwuzakresowy</li> <li>❖ 802.3af PoE</li> <li>❖ Mesh, polityki, QoS</li> <li>❖ Opcjonalny WIDS, WIPS, analizy widma</li> <li>❖ Zaawansowane funkcje 11n (formowanie wiązki, LDPC, STBC)</li> <li>❖ 60.000 pps</li> <li>❖ 2 x porty E/N dla redundancji zasilania i danych w sieci przewodowej</li> <li>❖ Małe wymiary obudowy/ praktycznie niewidoczny na ścianie</li> </ul> 	<b>3765i/e – Przemysłowy</b> <ul style="list-style-type: none"> <li>❖ 11abgn, 3x3:3 MIMO</li> <li>❖ Dwuzakresowy</li> <li>❖ 802.3af PoE</li> <li>❖ Mesh, polityki, QoS</li> <li>❖ Opcjonalny WIDS, WIPS, analizy widma</li> <li>❖ Zaawansowane funkcje 11n (LDPC, STBC)</li> <li>❖ 60.000 pps</li> <li>❖ Zintegrowane i zewnętrzne anteny</li> <li>❖ IP65/NEMA4</li> </ul> <b>3767e – Przemysłowy</b> <ul style="list-style-type: none"> <li>❖ To samo co 3765e +</li> <li>❖ 2x porty SFP E/N</li> </ul> 

### Najciekawsze funkcje

- Funkcja automatycznej kontroli mocy zapewnia ciągłość pokrycia obszaru
- Automatyczne zarządzanie łącznością radiową pomiędzy punktami dostępu
- Identyfikacja częstych źródeł zakłóceń, takich jak Bluetooth (37xx)
- Równoważenie obciążenia i sterowanie pasmem zapewnia równą dystrybucję do klientów
- Kod LDPC (low-density parity-check) i STBC (Space-time block coding)
- Proxy ARP @ AP – zmniejsza liczbę transmisji multicast
- Dynamiczna konwersja ruchu multicast do unicast w punkcie dostępowym przy mniejszej liczbie klientów
- Adaptowalne przesyłanie ruchu multicast przy najniższym poziomie ruchu dla dużej liczby klientów
- Filtrowanie ruchu multicast w punkcie dostępowym (lub kontrolerze)
- Funkcja Radar – Guardian („strażnik“) WIDS/WIPS (3710/3715)
- Reguły warstwy 2
- Ograniczanie do określonych reguł VLAN

### Przegląd proponowanego rozwiązania bezprzewodowej sieci LAN

Enterasys ma przyjemność przedstawić możliwości proponowanego przez siebie rozwiązania infrastruktury sieci bezprzewodowej (Enterasys Wireless). Zestaw produktów składających się na Enterasys Wireless zapewnia kompleksowe, opłacalne rozwiązanie bezprzewodowej sieci lokalnej,

które spełnia również wszystkie wymagania związane z niezawodnym, szerokopasmowym dostępem bezprzewodowym, zasięgiem, bezpieczeństwem WLAN, dostępem gości i zarządzaniem.

Poniższe informacje opisują zaawansowane możliwości naszych wiodących na rynku produktów i późniejsze korzyści, które klient będzie mógł wykorzystać dzięki wdrożeniu infrastruktury bezprzewodowej Enterasys. Opierając się na przeglądzie proponowanego rozwiązania, które obejmuje punkty dostępowe, kontrolery i oprogramowanie do zarządzania.

### **Najbardziej wydajne i energooszczędne rozwiązanie 802.11n**

Enterasys jest jedynym dostawcą zapewniającym pełną funkcjonalność standardu 802.11n (3x3 MIMO, 2 strumienie przestrzenne, łączenie kanałów, dwie częstotliwości jednocześnie) przy mocy źródła zasilania wynoszącej 11W lub zastosowaniu standardu PoE 802.3af.

Bezprzewodowe punkty dostępowe Enterasys 802.11n zostały specjalnie tak zaprojektowane by pobierać mniej niż 12W mocy przy wykorzystaniu wszystkich możliwych funkcji (dwie częstotliwości, 3x3 MIMO i łączenie kanałów), dzięki temu można korzystać ze standardu zasilania 802.3af PoE. Wiele konkurencyjnych rozwiązań 802.11n wymaga większej ilości mocy niż zapewnia powszechnie stosowany standard Power over Ethernet - 802.3af. W związku z tym muszą one ograniczać możliwości swoich punktów dostępowych 802.11n lub konieczne są kosztowne modernizacje sieci polegające na prowadzeniu dodatkowego okablowania Ethernet, ewentualnie na wymianie przełączników na takie, które obsługują wyższy standard PoE - 802.11at. Wielu dostawców próbuje ominąć te ograniczenia poprzez oferowanie wyłącznie konfiguracji 2x3 MIMO. W tym wypadku zmniejsza się zużycie energii, ale wydajność również znacznie spada. Enterasys oferuje najbardziej opłacalne rozwiązanie 802.11n zapewniające pełną funkcjonalność technologii 802.11n, bez konieczności wprowadzania kosztowych zmian w infrastrukturze PoE sieci i zużywające mniej energii, co dodatkowo obniża koszty operacyjne.

### **Elastyczna, zorientowana na rozwiązaniach architektura**

Rozwiązania bezprzewodowe Enterasys posiadają najbardziej elastyczną architekturę – umożliwiającą jednoczesną obsługę scentralizowanego i rozproszonego przekazywania ruchu (ewentualnie połączenie obu), która łatwo i opłacalnie dostosowuje się do różnych implementacji sieci, bez konieczności podejmowania przez klienta znaczących modyfikacji w istniejącej infrastrukturze sieci przewodowej. Architekturalne podejście Enterasys zapobiega powstawaniu wąskich gardeł w sieci, w wyniku przesyłania całego ruchu sieciowego przez centralny kontroler. Zamiast tego ruch może być przełączany i dystrybuowany w każdym punkcie dostępowym i kontrolowany centralnie w hybrydowych trybach działania, zależnie od oczekiwanego zachowania, które jest najlepiej dopasowane do indywidualnych potrzeb organizacji. Rezultatem jest skalowalna i adaptowalna infrastruktura bezprzewodowa zapewniająca wyjątkową wydajność i niezawodność, i która może być łatwo wykorzystana do wdrożenia nowych wysokowydajnych konwergentnych rozwiązań, takich jak głos czy przesyłanie video w jakości HD.

### **Elastyczna architektura Enterasys zapewnia:**

- Jednoczesną obsługę scentralizowanego i rozproszonego przekazywania ruchu (ewentualnie połączenie obu) oraz łatwe i opłacalne dostosowanie do różnych implementacji sieci.
- Łączący najlepsze elementy obu technik model postępowania, który zapobiega powstawianiu wąskich gardeł w sieci spowodowanych kierowaniem całego ruchu z powrotem do centralnego kontrolera.
- Możliwość przełączania i dystrybuowania ruchu w każdym punkcie dostępowym i kontrolowania go centralnie w hybrydowych trybach działania optymalnie dopasowanych do potrzeb organizacji.
- Polityki, które mogą być egzekwowane w punkcie dostępowym, w związku z tym niepożądany ruch nie jest przesyłany przez sieć WAN i nie blokuje przełączników agregujących.
- Zoptymalizowane opcje wdrożenia wykorzystujące rozwiązanie Virtual Network Services (VNS) do podziału sieci, przypisując użytkowników i dedykowane zasoby do specyficznych usług mobilnych (np. dedykowane SSID dla głosu, video, itp.)
- Współpracę z rozwiązaniami innych dostawców dzięki architekturze opartej na standardach.

### **Technologia Flexible Client Access poprawiająca przepustowość**

Rozwiązania sieci bezprzewodowych Enterasys oferują technologię Flexible Client Access (FCA). FCA to technologia dostępu, która znacząco poprawia przepustowość połączenia dla klientów korzystających z urządzeń 802.11n w środowisku a/b/g/n. FCA działa na zasadzie zapewniania równego czasu antenowego dla wszystkich klientów w środowisku, w którym występują urządzenia różnych standardów 802.11a/b/g/n. Administratorzy sieci mogą w prosty sposób wprowadzić tą funkcjonalność w oparciu o usługę WLAN, by polepszyć czas odpowiedzi dla wszystkich użytkowników i zmaksymalizować ogólną przepustowość połączenia bezprzewodowego.

### **Ujednolicone bezpieczeństwo i zarządzanie środowiskami przewodowymi i bezprzewodowymi**

Enterasys prowadzi w integracji technik bezprzewodowych i przewodowych, ujednolicając zarządzanie i bezpieczeństwo dla całej infrastruktury sieci, zwiększając tym samym efektywność działania i obniżając koszty. Enterasys jako jedynym dostawcą oferuje zintegrowane dla obu środowisk rozwiązanie NAC. Integracja pomiędzy zestawem oprogramowania zarządzającego Enterasys NMS i urządzeniami bezprzewodowymi Enterasys zapewnia kompleksową widoczność punktów dostępowych, kontrolerów i klientów bezprzewodowych z poziomu NMS Console – jak również możliwość centralnego zarządzania kopiami zapasowymi i przywracaniem danych konfiguracyjnych oraz pobieraniem oprogramowania. Ta innowacyjna integracja poprawia efektywność zarządzania siecią, umożliwia mapowanie topologii całej sieci oraz zapewnia pełną widoczność dla administratorów.

Rozwiązania bezprzewodowe Enterasys obsługują konfigurowanie polityk użytkownika z poziomu kontrolera lub centralnej aplikacji Enterasys Policy Manager NMS poprzez SNMP. Z poziomu Enterasys NMS Policy Manager administratorzy IT mogą określać globalne polityki, które są powszechnie stosowane do użytkowników sieci bezprzewodowej i przewodowej. Centralnie zdefiniowane polityki są dystrybuowane w całym środowisku sieci (niezależnie od medium transmisyjnego), na wielu przełącznikach, kontrolerach i punktach dostępowych by zapewnić ich egzekwowanie na skraju sieci. Integracja zarządzania politykami znacząco ulepsza możliwości

zarządzania i bezpieczeństwa ujednoczonych sieci przewodowych i bezprzewodowych. Zaawansowana możliwość centralnego definiowania i dystrybuowania jednolitych polityk dla obu środowisk pracy użytkowników ma znaczący wpływ na obniżenie kosztów operacyjnych, poprzez późniejszą ochronę i zachowanie integralności usług sieciowych.

Poniższa tabela podsumowuje zaawansowane, ujednoczone możliwości zarządzania i bezpieczeństwa dostępne w całej infrastrukturze sieci Enterasys (niezależnie od medium transmisyjnego).

Rozwiązania zarządzania i bezpieczeństwa Enterasys	Główne korzyści
NMS Policy Manager	Zapewnia centralne zarządzanie politykami i ich rozproszone, dynamiczne egzekwowanie.
NMS Inventory Manager	Zapewnia centralne zarządzanie oprogramowaniem oraz kopie zapasowe konfiguracji kontrolerów
NMS Console	Zapewnia kompleksową widoczność bezprzewodowych punktów dostępowych, kontrolerów i mobilnych klientów
NMS Automated Security Manager	Zapewnia możliwość automatycznego tworzenia czarnych list użytkowników sieci w oparciu o zdarzenia bezpieczeństwa
Network Access Control (NAC)	Polityki kontroli dostępu oparte o tożsamość jednolicie stosowane do użytkowników z różnych środowisk.
Intrusion Prevention System (IPS)	Kompleksowy IPS przy wdrożeniu In-line w każdej sieci VNS VLAN wraz z wykrywaniem zagrożeń opartym o dopasowywanie wzorców
Security Information & Event Manager (SIEM)	Ochrona całej sieci za pomocą powiadomień i ostrzeżeń z kontrolerów sieci bezprzewodowych i systemu WIPS

Skuteczność operacyjna osiągnięta przez zintegrowane podejście oznacza, że przedsiębiorstwa potrzebują mniej pieniędzy, personelu i czasu by spełnić wymagania konwergentnej sieci przesyłającej głos, video i dane. Inaczej niż w przypadku konkurencji, wbudowana inteligencja i bezpieczeństwo rozwiązań sieciowych Enterasys automatyzują zarządzanie konfiguracją i ograniczają konieczność korzystania z pomocy działu HelpDesk i angażowania usług IT. Użytkownicy biznesowi uzyskują mobilny dostęp do swoich treści (głosu, video lub danych) z dowolnego urządzenia i miejsca

– ponieważ wbudowane funkcje bezpieczeństwa zapewniają, że tylko właściwi użytkownicy mają dostęp do właściwych usług w odpowiednim miejscu i czasie.

### **Wysoka dostępność – kontrolery sieci bezprzewodowej Enterasys połączone w pary**

Wysoka dostępność kontrolerów sieci bezprzewodowych Enterasys jest osiągnięta poprzez podział między nie obciążenia. Umożliwia to skonfigurowanie kontrolerów w pary zapewniające wsparcie dla wszystkich punktów dostępowych w sieci. Punkty dostępowe mogą być przypisane do dowolnego z połączonych w parę kontrolerów, równoważąc pomiędzy nimi obciążenie i zapewniając jednocześnie redundancje w trybie *fail-over*. Konfiguracja trybu wysokiej dostępności pozwala na przeniesienie punktów dostępowych zarejestrowanych do uszkodzonego kontrolera na sparowane urządzenie. To podejście do trybu *fail-over* wymaga mniejszych nakładów na oprogramowanie i sprzęt niż powszechnie stosowane modele dostępności N+1. Ponadto podejście opierające się na połączonych w parę kontrolerach, pozwala na ich geograficzne odseparowanie i umieszczenie w różnych centrach NOC (Network Operation Center), co dodatkowo zwiększa dostępność w przypadku nieprzewidzianych katastrof. W przeciwieństwie do większości produktów konkurencji, rozwiązania bezprzewodowe Enterasys **nie wymagają** stosowania licencji by uzyskać możliwość stosowania trybu *fail-over* dla punktów dostępowych.

### **Najlepsze na rynku rozwiązania bezpieczeństwa WLAN**

Rozwiązanie Enterasys Wireless Intrusion Prevention System (WIPS) poprawia bezpieczeństwo poprzez wbudowany system zapobiegania włamaniom (IPS – Intrusion Prevention System), oparte na lokalizacji usługi i trzywarstwowy model bezpieczeństwa WLAN. Na poziomie ramowym WPA2 (802.11i) gwarantuje poufność i integralność danych, natomiast na poziomie klientów i punktów dostępowych uwierzytelnianie 802.1X zapewnia, że tylko autoryzowani użytkownicy i punkty dostępowe mają dostęp do sieci. Ponadto proponowane rozwiązanie Enterasys Wireless Management Suite WIPS oferuje najlepsze możliwości WIPS/WIDS dla pełnej ochrony komunikacji bezprzewodowej, w tym wykrywanie i łagodzenie zagrożeń takich jak: nieuczciwe punkty dostępowe, *Honeypot*, ataki *Evil Twin*, MAC spoofing i wiele więcej. To rozwiązanie WIPS chroni również klientów WLAN, aby nie zostali podłączeni do niesprawdzonych lub sąsiednich SSID (polityki powinny temu zapobiegać).

Przy implementacji WIPS w połączeniu z tradycyjnym, przewodowym IPS użytkownicy obu środowisk mają zapewnione: pełną inspekcję pakietów, adaptacyjne dopasowywanie wzorów sygnatur, analizy protokołów i wykrywanie anomalii w zachowaniu sieci. Ponadto, przywileje polityk Enterasys NAC wykorzystujące tożsamości są jednolite w całej infrastrukturze sieci zapewniając opartą o rolę kontrolę dostępu – niezależnie od metody połączenia i medium transmisyjnego. Polityki NAC zapewniają, że tylko właściwi użytkownicy mają dostęp do właściwych usług, w odpowiednim czasie i miejscu.

### **Wysokiej jakości technologia Voice over WLAN (VoWLAN)**

Enterasys Wireless jest uznanym, wiodącym rozwiązaniem dla technologii VoWLAN i ma na swoim koncie wiele udanych implementacji. Rozbudowane funkcje QoS dla obu środowisk, połączone z najbardziej elastyczną na rynku architekturą zapewniają idealne warunki dla transmisji głosu. Szyfrowanie odbywa się lokalnie w bezprzewodowych punktach dostępowych Enterasys, natomiast QoS jest realizowane zarówno w punkcie dostępowym i kontrolerze. Dzięki temu wydajność dla ruchu głosowego jest znacznie lepsza niż u rozwiązań konkurencji - w których ruch kierowany jest do kontrolera i tam przetwarzany - i pozwala na stosowanie kompleksowej polityki QoS. Ponadto, najlepszy na rynku wybór wyrafinowanych funkcji, takich jak: QoS, CAC (Call Admission Control), spójny roaming i oszczędzanie energii powoduje, że rozwiązania Enterasys Wireless są najlepszą platformą technologiczną dla wprowadzenia VoWLAN.

### **Dożywotnia gwarancja na punkty dostępowe**

Bezprzewodowe punkty dostępowe Enterasys objęte są dożywotnią gwarancją. Obejmuje ona okres 5 lat od zakończenia sprzedaży i zapewnia wsparcie techniczne oraz zaawansowaną wymianę części zamiennych. Poprawki i aktualizacje oprogramowania są dostępne przez rok.

### **Usługi i wsparcie**

Enterasys posiada najlepsze na rynku wskaźniki zadowolenia klientów i problemów rozwiązanych przy pierwszym zgłoszeniu. Oferuje spersonalizowane usługi i posiada przedstawicieli legitymujących się średnio ponad 11 letnim doświadczeniem, którzy są wspierani przez dział inżynierii dla szybkiego rozwiązywania problemów. Motto Enterasys – „Nie ma niczego ważniejszego od naszych klientów” - jest najlepiej zilustrowane przez badanie zadowolenia klientów z roku 2009, w którym uzyskaliśmy ogólną ocenę 97% . Poza usługami wsparcia technicznego Enterasys oferuje również szeroki zestaw usług szkoleniowych i profesjonalnych.

### **Przegląd produktów Enterasys dla sieci bezprzewodowych**

#### **Kontrolery sieci bezprzewodowej Enterasys**

Enterasys oferuje kilka kontrolerów sieci bezprzewodowych możliwych do zastosowania w sieciach o różnych rozmiarach. Na gamę modelową składają się:

- C25 wspierające do 100 punktów dostępowych (AP).
- V2110 wspierające do 496 AP.
- C5210 wspierające do 2000 AP.

Redundantne kontrolery sieci bezprzewodowej Enterasys mogą być zainstalowane w dowolnym miejscu w sieci i pracować w trybie *fail-over* lub podziału obciążenia. Wiele kontrolerów może być połączonych ze sobą w celu zwiększania obszaru mobilności i obsługi tysięcy punktów dostępowych.

Kontroler sieci bezprzewodowej Enterasys jest wysoce wydajną platformą zapewniającą scentralizowaną inteligencję dla rozwiązań Enterasys Wireless. Kontrolery sieci bezprzewodowych Enterasys zapewniają oparte o role zarządzanie użytkownikami, urządzeniami i aplikacjami oraz zindywidualizowane usługi obejmujące Quality of Service (QoS), Call Admission Control, polityki bezpiecznego dostępu, Network Access Control (NAC), Captive Portal, ograniczanie przepustowości, multicast, filtrowanie i przekazywanie ruchu. Te usługi sieci WLAN są elementami unikalnej i elastycznej architektury Enterasys Wireless zorientowanej na rozwiązania, która pozwala na łatwe zarządzanie i świadczenie ich w oparciu o intuicyjny panel zarządzania, obsługiwany z poziomu przeglądarki internetowej.

Każdy kontroler Enterasys obsługuje sieci, w których występują jednocześnie punkty dostępowe 802.11n i 802.11a/b/g oraz zapewnia jednolite przesyłanie danych do innych kontrolerów i punktów dostępowych. Wszystko to składa się na wysoką skalowalność i łatwość implementacji. W przypadku

dużych sieci technologia Enterasys upraszcza zarządzanie tysiącami punktów dostępowych przez tworzenie stref poruszania się, które rozszerzają usługi WLAN na wiele kontrolerów bezprzewodowych. Definicje i indywidualne polityki są utrzymywane w całym obszarze strefy poruszania się użytkowników i są przemieszczane wraz z użytkownikiem, niezależnie od jego fizycznej lokalizacji.

Większość rozwiązań WLAN zmusza administratorów sieci do wyboru pomiędzy scentralizowaną lub rozproszoną architekturą. Istotną zaletą kontrolerów sieci bezprzewodowej Enterasys jest możliwość obsługi obu modeli implementacji jednocześnie, co znacznie podnosi elastyczność w porównaniu do oferty konkurencji. Przy pomocy rozwiązań sieci bezprzewodowych Enterasys administratorzy sieci mogą tworzyć usługi WLAN i polityki, które razem mogą dynamicznie przypisywać reguły przekazywania ruchu do użytkowników i grup, ograniczać przepływy danych i kontrolować dostęp w oparciu o użytkowników i SSID. Dzięki elastyczności pozwalającej na świadczenie usług i egzekwowanie polityk w punkcie dostępowym bezprzewodowy ruch sieciowy może być obukierunkowo ograniczany do zdefiniowanych przez użytkownika progów, filtrowany i lokalnie przełączany, bez potrzeby tunelowania go z powrotem do kontrolera. W obu przypadkach niepożądany ruch nie jest przesyłany przez sieć WAN lub przełączniki agregujące zanim dotrze do kontrolera. Jest to możliwe dzięki unikalnym możliwościom przeprowadzania dokładnej inspekcji pakietów w punkcie dostępowym. W oparciu o identyfikację przeznaczenia i żądanej usługi dokonywane jest odpowiednie filtrowanie, przełączanie i ograniczanie pasma przesyłanych danych. Rezultatem jest optymalizacja czasu odpowiedzi i wydajności dla użytkowników i usług.

### **Oprogramowanie Enterasys Wireless Convergence Software**

Oprogramowanie Enterasys Wireless Convergence Software pracuje na platformie kontrolera i zapewnia scentralizowaną inteligencję rozwiązań bezprzewodowych Enterasys dla:

- Zarządzania i konfiguracji punktu dostępowego
- Zarządzania użytkownikami i polityk
- Quality of Service (QoS)
- Bezpieczeństwa



- Roamingu i płynnego działania usługi handover
- Proste zarządzania siecią

Oprogramowanie Enterasys Wireless Convergence Software automatycznie i centralnie zarządza punktami dostępowymi, ułatwiając instalacje i aktualizacje oprogramowania oraz upraszczając kontrolę sieci. Zarządza ono przypisywaniem klientów urządzeń bezprzewodowych w sieci, którzy są związani za pośrednictwem punktów dostępowych. Oprogramowanie Wireless Convergence Software jest wspólne dla wszystkich typów platform kontrolerów i zapewnia podobną funkcjonalność i sposób obsługi niezależnie od typu zastosowanych kontrolerów.

Kontroler monitoruje i zarządza powiązаныmi punktami dostępowymi za pomocą centralnego, obsługiwanego z poziomu przeglądarki internetowej interfejsu - Enterasys Wireless Assistant. Za jego pomocą możliwe jest globalne konfigurowanie oraz włączania lub wyłączania jednego lub wielu punktów dostępowych

Technologia Plug&Play stosowana w punktach dostępowych istotnie ułatwia wdrożenie rozwiązania WLAN. Bezprzewodowe punkty dostępowe Enterasys automatycznie i bezpiecznie rejestrują się w dostępnym kontrolerze sieci bezprzewodowej oraz pobierają z niego swoją konfigurację. Upraszcza to proces implementacji i wysiłek operacyjny. Punkty dostępowe od razu po podłączeniu do sieci mogą rozpocząć świadczenie usług dla użytkowników, bez konieczności przeprowadzania manualnej konfiguracji.

Bezprzewodowe punkty dostępowe Enterasys wykorzystują najbardziej zaawansowane standardy w celu zagwarantowania skutecznej ochrony i kompatybilności. Bezprzewodowe sieci LAN wykorzystujące standard 802.11i (WPA2) mogą stosować uwierzytelnianie 802.1X lub PSK oraz szyfrowanie AES, TKIP lub WEP. Możliwości te gwarantują bezpieczne uwierzytelnianie i bezproblemową integrację punktów dostępowych z pozostałą infrastrukturą sieci.

Bezprzewodowe punkty dostępowe Enterasys współpracują ze sobą w celu ochrony przed zakłóceniami i optymalizacji podziału częstotliwości radiowej. Każdy punkt dostępowy może inteligentnie i dynamicznie zmieniać moc transmitowanego sygnału i kanał, w oparciu o informacje z sąsiadujących punktów dostępowych, poziom zakłóceń zewnętrznych lub zajętość kanału. W ten sposób zapewniona jest optymalna wydajność dla wszystkich użytkowników sieci bezprzewodowej. Jeżeli punkt dostępowy ulegnie awarii, wówczas sąsiednie punkty dostępowe zwiększają swoją moc, by pokryć zasięgiem obsługiwany przez niego obszar. Punkty dostępowe wspierają również plan wyboru kanału częstotliwości radiowej, z opcją obsługi 3 kanałów, 4 kanałów, lub dowolnej konfiguracji.

### **Enterasys Wireless Management Suite**

Enterasys Wireless Management Suite (WMS) zapewnia kompleksowe zarządzanie wieloma kontrolerami pozwalające administratorom centralnie kontrolować duże sieci bezprzewodowe. Szeroki zbiór wykresów, statystyk i raportów zapewnia globalny obraz całej sieci bezprzewodowej niezbędny do analizy trendu jej rozwoju. Podczas, gdy szczegółowe dzienniki zdarzeń, zdefiniowane

przez użytkownika progi oraz ostrzeżenia ułatwiają zrozumienie i rozwiązywanie problemów. Możliwości systemu mogą być znacząco rozszerzone przez opcjonalne moduły dodatkowych usług Advanced Services, które integrują zaawansowane procesy i aplikacje mobilne organizacji. Opcjonalny moduł WMS WIPS dodaje najlepszy bezprzewodowy system IPS (Intrusion Prevention System) oraz optymalizacje położenia i wydajności, natomiast opcjonalny moduł WMS WIPS Reporting umożliwia testowanie zgodności ze standardami branżowymi.

### **Enterasys Wireless Management WIPS**

Moduł Wireless Management Suite WIPS jest w pełni zintegrowaną aplikacją, która zapewnia: szerokie możliwości zapobiegania włamaniom i wykrywania ich (IPS/IDS), ocenianie położenia, wizualizacje pokrycia obszaru częstotliwością radiową oraz narzędzia do rozwiązywania problemów.

WIPS tworzy mapy termiczne pokrycia obszaru częstotliwością radiową, które pozwalają administratorom sieci oceniać siłę sygnału i identyfikować niepokryte punkty. Ponadto wbudowane funkcje rozwiązywania problemów oferują szczegółowe instrukcje dotyczące wykrywania i zwalczania wąskich gardeł i błędów. Dzięki rozbudowanym funkcjom WIPS, za pomocą kontrolera można wyznaczać punkty dostępowe, które mają być dedykowanymi sensorami. To wszystko składa się na najbardziej zaawansowane i spójne rozwiązanie WIPS przy jednoczesnym zachowaniu kontroli nad pojedynczą, zintegrowaną infrastrukturą WLAN.

## Parametry ofertowe

	<b>Cena netto</b>
<b>Koszt elementów aktywnych 200 xAP( WS-AP3705i) + Kontroler + licencje</b>	\$ 151530 *
<b>Termin wdrożenia</b>	6-12 tygodni * **
<b>koszt wdrożenia</b>	50-100 tyś pln * **

\* - Założono instalacje składającą się z 200 AP w całej polsce . \*\* - koszt nie obejmuje wykonania okablowania, wykonanie okablowania i projektu rozmieszczenia AP wymaga wykonania wizji na miejscu i/lub dostępu do projektu budynków