CITINET 2005

http://www.ciscopoland.pl/citinet2005

Kontrola dostępu i identyfikacja tożsamości oraz ochrona dostępu do zasobów

(od wewnątrz)

Michał Kraut
Systems Engineer
Maj 2005

Agenda

- Zintegrowana Ochrona w sieci WAN
  - -Zintegrowane bezpieczeństwo w Cisco IOS
  - -Rozwiązabua dla małych placówek i oddziałów
- Uwierzytelnienie i kontrola dostępu
  - -NAC
  - -IBNS
- Zintegrowana Ochrona w sieci LAN
  - - Bezpieczenstwo w przelacznikach
- Pytania…?

Zintegrowana Ochrona w sieci WAN

Zintegrowane bezpieczeństwo w Cisco IOS

rozwiązanie ALL-in-ONE

Cisco.com

Identyfikacja zasobów

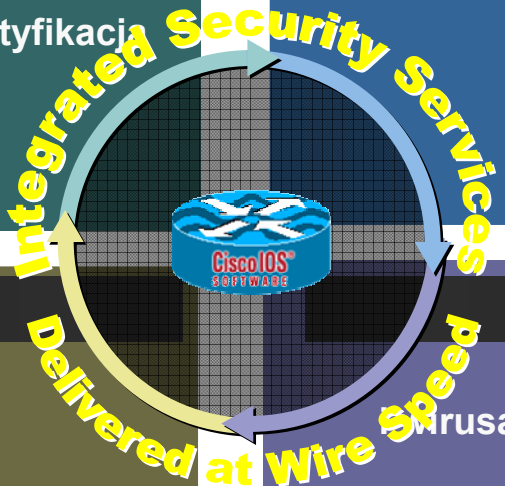
Ochrona sieci przed stacją oraz identyfikacja użytkowników i urządzeń

Network Admission Control, 802.1x

Bezpieczne połączenia

Bezpieczne i skalowalne połączenia , poufność danych

VPN, DMVPN, V3PN, Secure Voice



Ochrona infrastruktury

Wymuszanie określonej polityki bezpieczeństwa

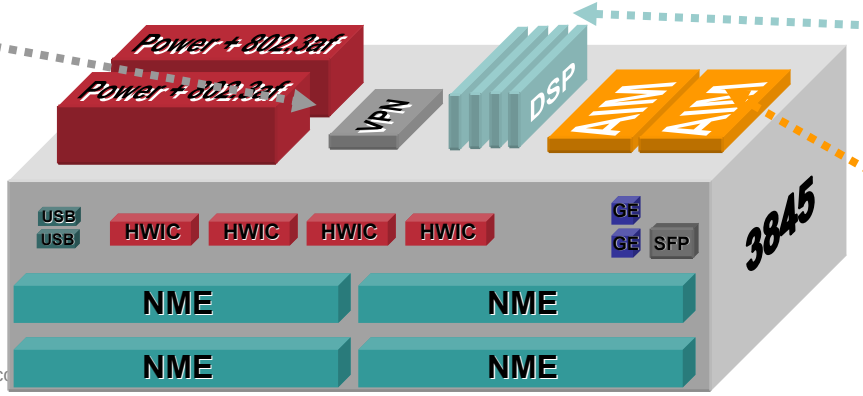
Control Plane Policing

Ochrona przed zagrożeniami

Ochrona przed atakami, robakami i wirusami. Wymuszanie określonej polityki bezpieczeństwa

Intrusion Prevention, Firewall with NAT

Wbudowane szyfrowanie sprzętowe



Bezpieczna transmisja głosu

Wysoka wydajność szyfrowania

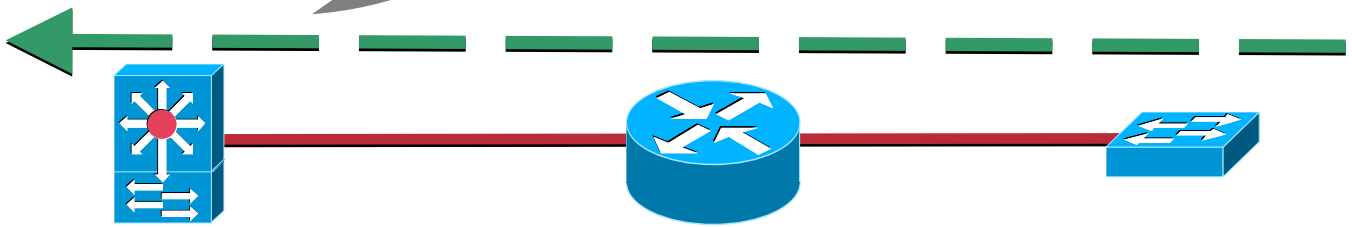
Cisco Network Foundation Protection

Bezpieczne sieci muszą być budowane na bezpiecznych urządzeniach

Cisco.com

Kontrola infrastruktury
Ochrona wydajności
Network Lockdown

Cisco Network Foundation Protection



Ochrona urządzenia

"zablokowanie urządzenia" I ochrona usług

Łatwe "blokowanie" konfiguracji urządzenia

Odporność na ataki DDOS

Separacja zarządzania - role

Bezpieczny dostęp zarządzania

Ochrona dla funkcji

Ochrona przesyłanych danych

Black hole DDoS

Ochrona przed spoofingiem

Rate limit dla kwestionowanego ruchu

Wykrywanie anomalii i dokładne info o nich

Uwierzytelnienie protokołów routingu

Cisco IOS Firewall

Zaawansowana inspekcja aplikacyjna

App Sec

Cisco.com

HTTP Inspection Engine

- Zapewnienie kontroli aplikacyjnej dla ruchu kierowanego na port 80
  - Spójność Cisco IOS Firewall i technologii Inline IPS
- Kontrolowania nadużyć związanych w przesyłaniem informacji z niektórych aplikacji wewnątrz ruchu HTTP
  - Przykład: Instant messaging i aplikacje peer-to-peer jak np. Kazaa

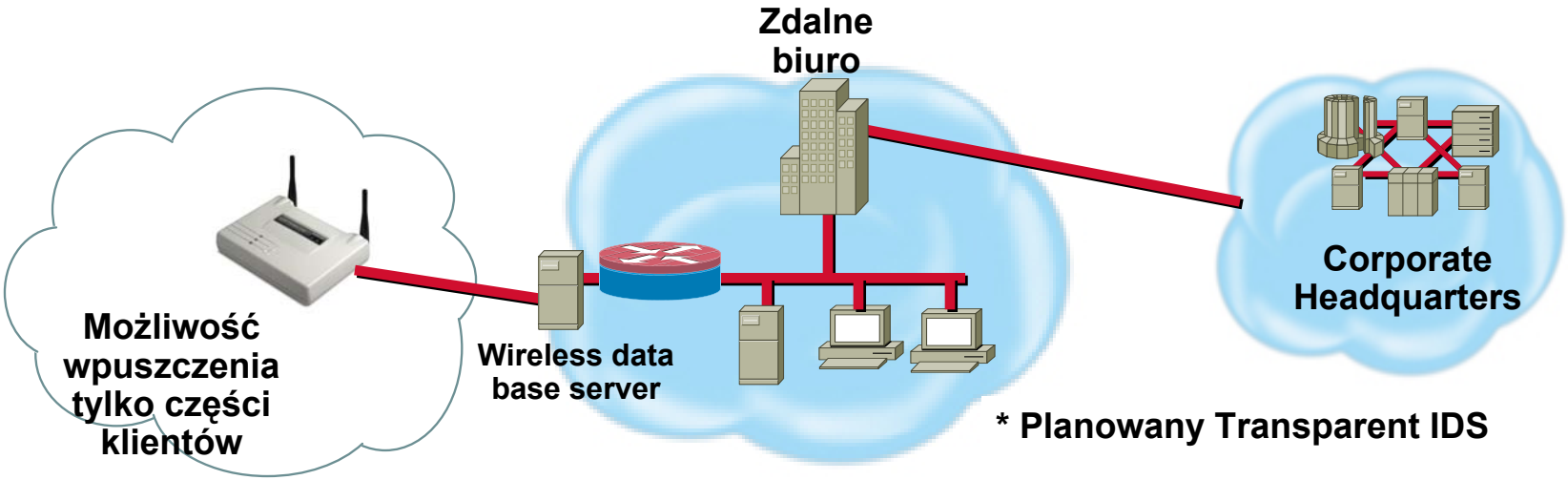
Email Inspection Engine

- Kontrola nadużyć w protokołach email
- SMTP, ESMTP, IMAP, POP inspection engines

Inspection Engines Zapewniają także wykrywanie anomalii związanych z protokołami

Transparent IOS Firewall

- Wykorzystanie narzędzi CBAC
- Minimalna konfiguracja IOS Firewall
- Wsparcie dla Layer 2 Layer 3
- Praca z uwzględnieniem Spanning Tree Protocol (STP)
- Możliwość określenia konkretnych urządzeń, które mogą przesylac dane
- Wsparcie DHCP pass through dla przypisania adresów z DHCP po drugiej stronie FW (bi directional)



Cisco IOS IPS

Anti-X

Cisco.com

- IPS wprowadzony jako funkcja routera umożliwia ochronę przed robakami i zagrożeniami sieciowymi – również w lokalizacjach zdalnych
- String Engines pozwalają na wychwytywanie dowolnego ciągu znaków w pakiecie
  - *możliwość własnej konfiguracji sygnatur dla szybszego wykrywania potencjalnych I realnych zagrożeń*
  - TCP String, UDP String, ICMP String, Trend Micro
- Dodanych zostało ponad 400 nowych sygnatur ataków I robaków – w sumie IOS IPS posiada 1200 sygnatur
- *Wsparcie dla sygnatur Trend Micro*

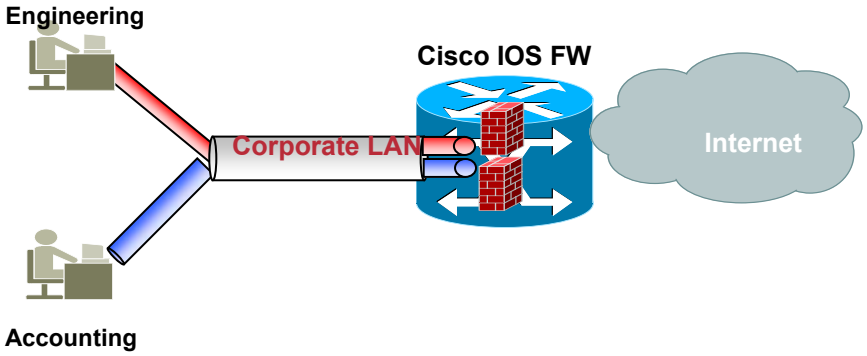
NCC

Cisco IOS Virtualized Services

VRF-Aware "Virtual" Firewall & IP Sec "Virtual" Interface

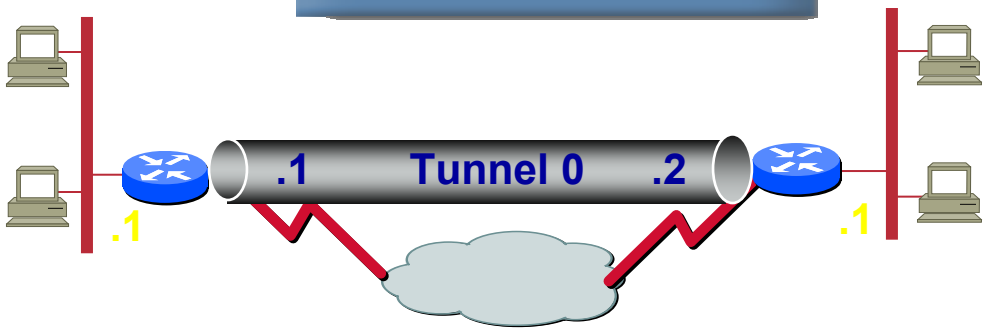
Cisco.com

VRF-Aware "Virtual" Firewall



- VRF pozwala na obsługę wielu niezależnych kontekstów (adresy, routing, interfejsy) w lokalizacji dostępowej dla odseparowania departamentów, kiosków, bankomatów, etc.
- VRF-Aware FW pozwala na dodanie do wymienionych funkcjonalności niezależnych firewalli, dostępnych dla każdego z kontekstów

IPsec "Virtual" Interface



- Uproszczenie konfiguracji i projektowania IPsec VPN (Network-aware IPsec)
- Prostsze i bardziej skalowalne zarządzanie
- Szybsze wdrożenia sieci IPSec
- Wsparcie dla aplikacji V3PN - Multicast, QoS i routing

Cisco AutoSecure Rollback i Logging

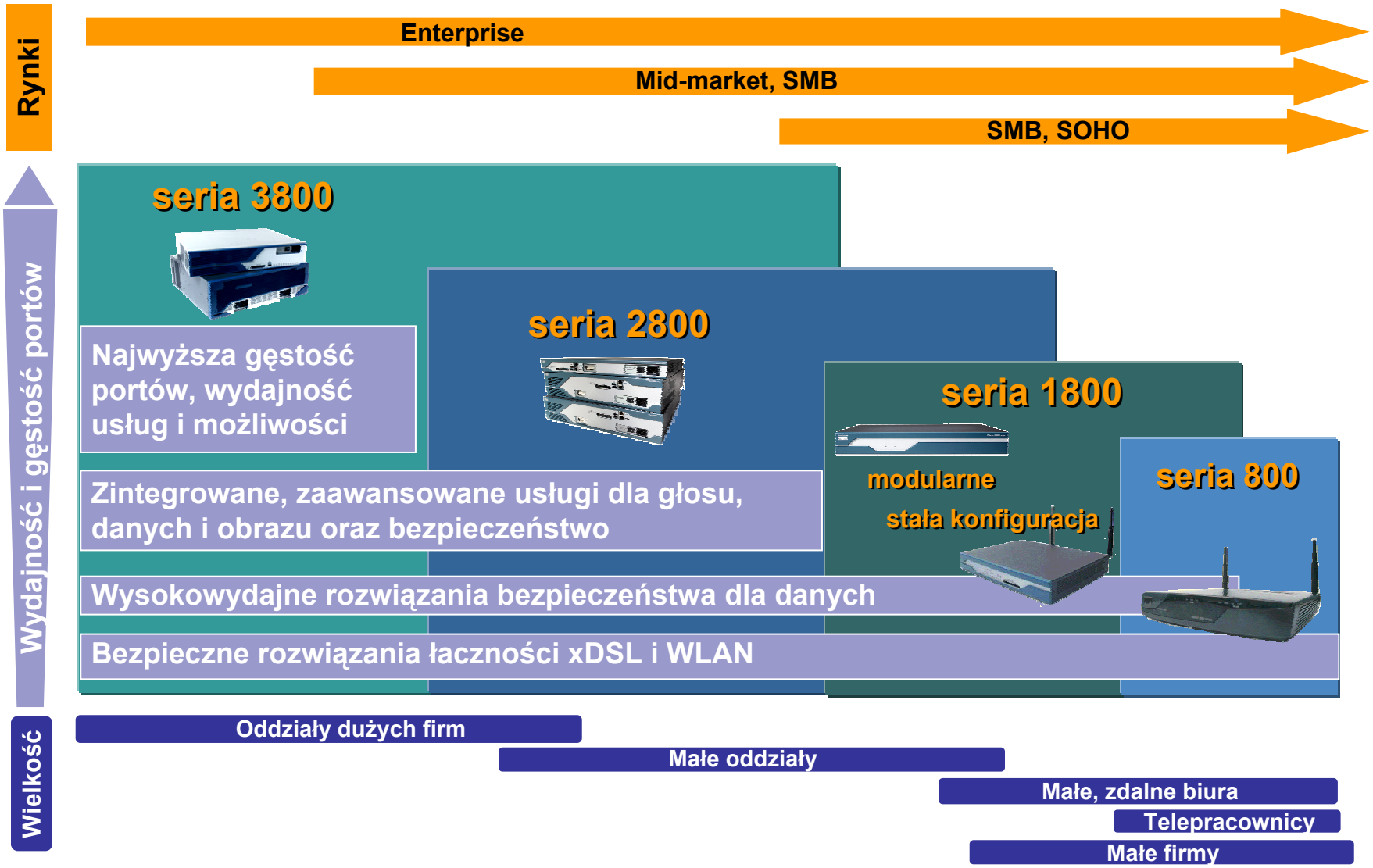
- Możliwość autozabezpieczenia routera – operacja “one-touch” z wykorzystaniem jednej komendy
- Możliwość odzyskania konfiguracji systemu do stanu sprzed uruchomienia zabezpieczeń

Zintegrowana Ochrona w sieci WAN

NOWE PRODUKTY DLA RYNKÓW SOHO/SMB

Pozycjonowanie urządzeń Cisco ISR

Cisco.com



Co nowego w serii 800?

- **Wysokowydajne rozwiązania dla pojedynczych pracowników oraz małych biur**
- **Pakiet funkcjonalności związanej z bezpieczeństwem, obejmujący:**
  - **Stateful firewall**
  - **IPSec VPN (algorytmy 3DES i AES)**
  - **Intrusion Prevention System (IPS)***
  - **wsparcie dla Network Admission Control (NAC)***
  - **Cisco Easy VPN & DMVPN* oraz AutoSecure**

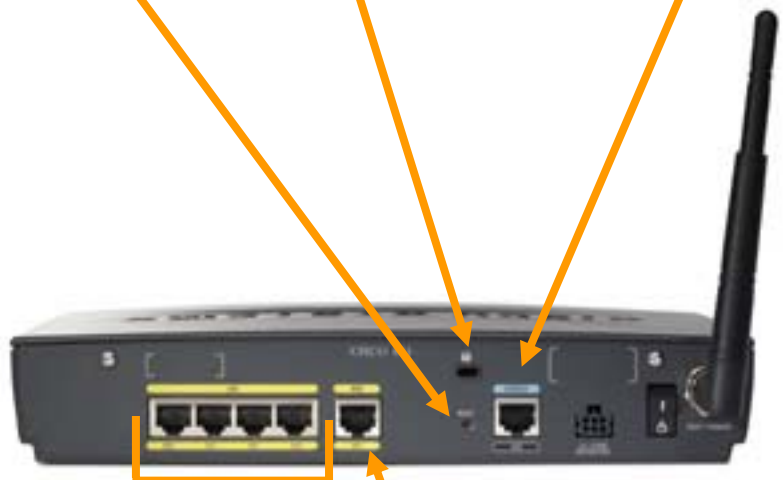
- **Opcja zintegrowanego punktu WLAN 802.11b/g**
- **Zarządzalny*, 4-portowy przełącznik 10/100 ze wsparciem dla 802.1Q oraz in-line power (zasilacz zewnętrzny)**
- **Dwa porty USB w Cisco 871**

***w serii 870**

Routery Cisco ISR 850

- **Dwa modele:**
  - **Cisco 851 – port WAN Ethernet**
  - **Cisco 857 – port WAN ADSL Annex A (POTS)**
  - **dodatkowo wersje Cisco 851W i 857W posiadają zabudowany WLAN AP 802.11b/g ze stałą anteną**
- **Funkcjonalność podstawowa:**
  - **routing statyczny i RIPv1/v2, NAT/PAT, PPPoA/PPPoE, serwer, klient i relay DHCP, STP, PBR**
- **Bezpieczeństwo:**
  - **IPsec 3DES/AES (do 8 tuneli), GRE, obsługa ACL**
- **Mechanizmy QoS:**
  - **WFQ, per-VC shaping i policing**
- **Ograniczenie do 10 użytkowników**

Routery Cisco ISR 851 i 857



Pamięć Flash:
Domyślnie: 20 MB
Maksymalnie: 32 MB

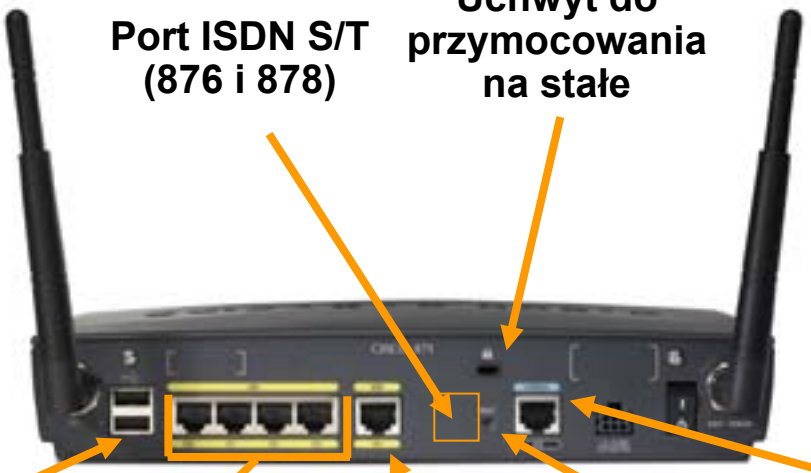
Pamięć RAM:
Domyślnie: 128 MB
Maksymalnie: 128 MB

Routery Cisco ISR 870

- **Cztery modele:**
  - **Cisco 871 – port WAN Ethernet**
  - **Cisco 876 – port WAN ADSL Annex B (ISDN)**
  - **Cisco 877 – port WAN ADSL Annex A (POTS)**
  - **Cisco 878 – port WAN G.SHDSL**
  - **dodatkowo wersje Cisco 871W, 876W, 877W i 878W posiadają zabudowany WLAN AP 802.11b/g z wymiennymi antenami**
- **Funkcjonalność podstawowa:**
  - **routing statyczny i RIPv1/v2, OSPF/EIGRP/BGP*, NAT/PAT, PPPoA/PPPoE, serwer, klient i relay DHCP, STP, PBR, wsparcie dla 3 VLANów na przełączniku*, VRRP/HSRP**
- **Bezpieczeństwo:**
  - **system IPS, integracja z NAC, IPsec 3DES/AES (do 10 tuneli), DMVPN, GRE, obsługa ACL**
- **Mechanizmy QoS:**
  - **CBWFQ, LLQ, NBAR, QoS pre-classify, LFI, WFQ, per-VC shaping i policing, RSVP, DiffServ**
- **Ograniczenie do 20 użytkowników**

- ***w oprogramowaniu Advanced IP Services**

Routery Cisco ISR 871, 876, 877, 878



podwójne, wymienne anteny

Port ISDN S/T (876 i 878)

Uchwyt do przymocowania na stałe

Pamięć Flash:
Domyślnie: 20 MB
Maksymalnie: 52 MB

Pamięć RAM:
Domyślnie: 128 MB
Maksymalnie: 198 MB

Porty USB 2.0 (871)

4-portowy przełącznik 10/100

WAN Port:
871 = 100BaseTX Ethernet
876 = ADSL Annex B (ISDN)
877 = ADSL Annex A (POTS)
878 = G.SHDSL

Przycisk Reset

Port konsoli i wirtualny AUX

Co nowego w serii 1800?

- Rozwiązania stworzone z myślą o obsłudze jednocześnie wielu usług z pełną wydajnością
- Pakiet funkcjonalności związanej z bezpieczeństwem, obejmujący:
  - Stateful firewall
  - IPSec VPN (algorytmy 3DES i AES)
  - Intrusion Prevention System (IPS)
  - wsparcie dla Network Admission Control (NAC)
  - Cisco Easy VPN & DMVPN oraz Autosecure

- Pełne funkcje routingu IP obecne w Cisco IOS
- Zintegrowane opcje zapewnienia połączeń zapasowych: ISDN BRI, modem analogowy lub Ethernet
- 8-portowy zarządzalny przełącznik 10/100 ze wsparciem dla 802.1Q i in-line power
- Opcja trójsystemowego WLAN AP 802.11a/b/g z wymiennymi antenami zewnętrznymi
- Sloty USB i CF, oraz zintegrowany zegar czasu rzeczywistego

Routery Cisco ISR 1800

- **Pięć modeli:**
  - **Cisco 1801 – 1x ADSL POTS, 1x FE, 8x 10/100 FE, ISDN BRI S/T**
  - **Cisco 1802 – 1x ADSL ISDN, 1x FE, 8x 10/100 FE, ISDN BRI S/T**
  - **Cisco 1803 – 1x G.SHDSL, 1x FE, 8x 10/100 FE, ISDN BRI S/T**
  - **Cisco 1811 – 2x FE, 8x 10/100FE, 1x modem V.92**
  - **Cisco 1812 – 2xFE, 8x 10/100FE, ISDN BRI S/T**
  - **osobne wersje 'W-AG-K9' zawierają zintegrowany AP WLAN**
- **Funkcjonalność podstawowa:**
  - **routing statyczny, RIPv1/v2, OSPF/EIGRP/BGP*, NAT/PAT, PPPoA/PPPoE, serwer, klient i relay DHCP, STP, PBR, wsparcie dla 8 VLANów na przełączniku, VRRP/HSRP**
- **Bezpieczeństwo:**
  - **system IPS, integracja z NAC, IPsec 3DES/AES (do 50 tuneli), DMVPN, GRE, obsługa ACL**
- **Mechanizmy QoS:**
  - **CBWFQ, LLQ, NBAR, QoS pre-classify, LFI, WFQ, per-VC shaping i policing, CAR, RSVP, DiffServ**
- **Ograniczenie do 50 użytkowników**

- ***w oprogramowaniu Advanced Enterprise Services**

Routery Cisco ISR 1800

Podwójne, wymienne anteny

Wewnętrzny zasilacz

Uchwyt do przymocowania na stałe

Przełącznik 8x 10/100 z opcjonalnym PoE

Pamięć Flash:
Domyślnie: 32 MB
Maksymalnie: 128 MB

Pamięć RAM:
Domyślnie: 128 MB
Maksymalnie: 512 MB

Port ISDN S/T (1801, 1802, 1803, 1812) lub modem analogowy (1811)

Wejście z zewnętrznego zasilacza PoE

Port konsoli

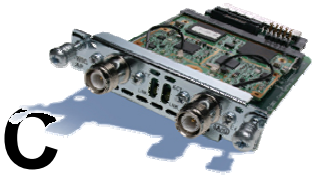
Port AUX

Podwójne porty 10/100 FE (1811, 1812)

Porty USB 2.0 (1811, 1812)

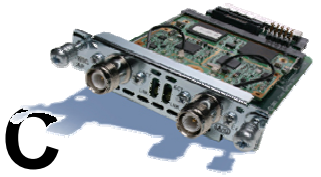
Port WAN xDSL:
- ADSL (1801)
- ADSL Annex B (1802)
- G.SHDSL (1803)

Moduł WLAN w postaci karty HWIC

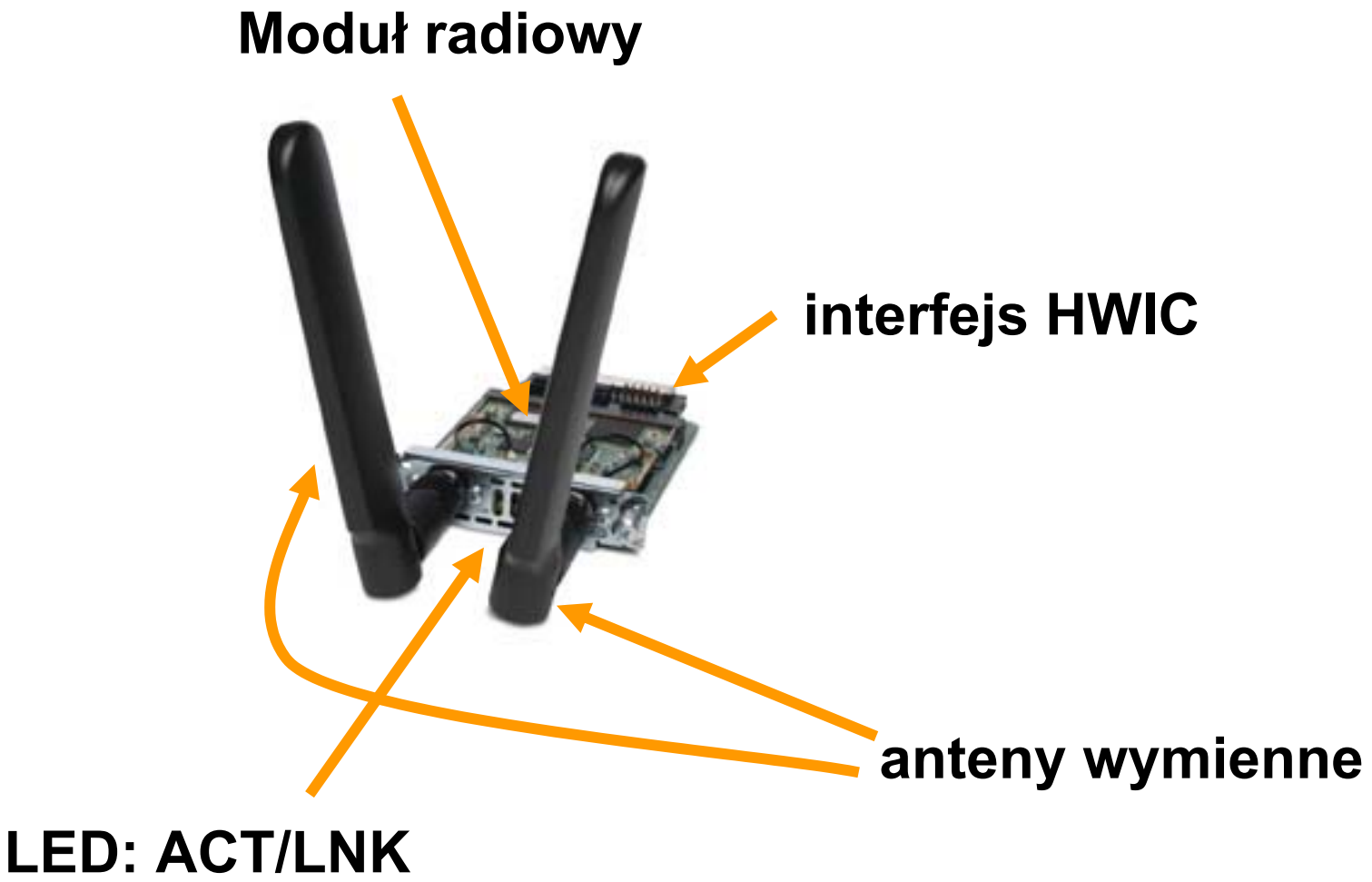


- **Karta HWIC zapewniająca funkcjonalność punktu dostępowego**
  - **wersja 802.11b/g i 802.11a/b/g**
  - **zewnętrzne, dołączalne anteny (RP-TNC)**
  - **moduły kompatybilne z 1841, 2800 i 3800**
- **Funkcjonalność:**
  - **statyczne i dynamiczne klucze WEP 802.1X, Cisco LEAP, PEAP-MSCHAPv2, EAP-TLS, WPA, uwierzytelnianie i filtrowanie po adresach MAC, uwierzytelnianie przy współpracy z serwerem RADIUS**
  - **802.1p i 802.11e (QoS)**
  - **mapowanie VLANów na SSID**

Moduł WLAN w postaci karty HWIC



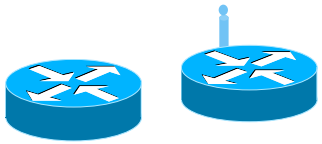
Cisco.com



Zestawienie nowych routerów 850/870/1800

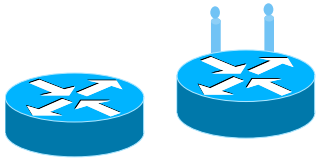
Cena

Seria Cisco 850



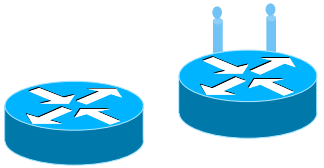
- Stateful firewall
- VPNy IPSec 3DES/AES
- Przełącznik 4x 10/100
- Opcja 802.11b/g WLAN, antena stała
- Zarządzanie przez CLI Cisco IOS oraz Cisco SDM

Seria Cisco 870



- Wyższa wydajność
- Stateful firewall
- VPNy IPSec 3DES/AES
- IPS, NAC/Antywirus
- Opcja 802.11b/g WLAN, wymienne anteny
- Zaawansowane mechanizmy QoS
- Zarządzalny przełącznik 4x 10/100
- Do 3 VLANów
- Zarządzanie przez CLI Cisco IOS oraz Cisco SDM

Seria Cisco 1800 (niemodularna)

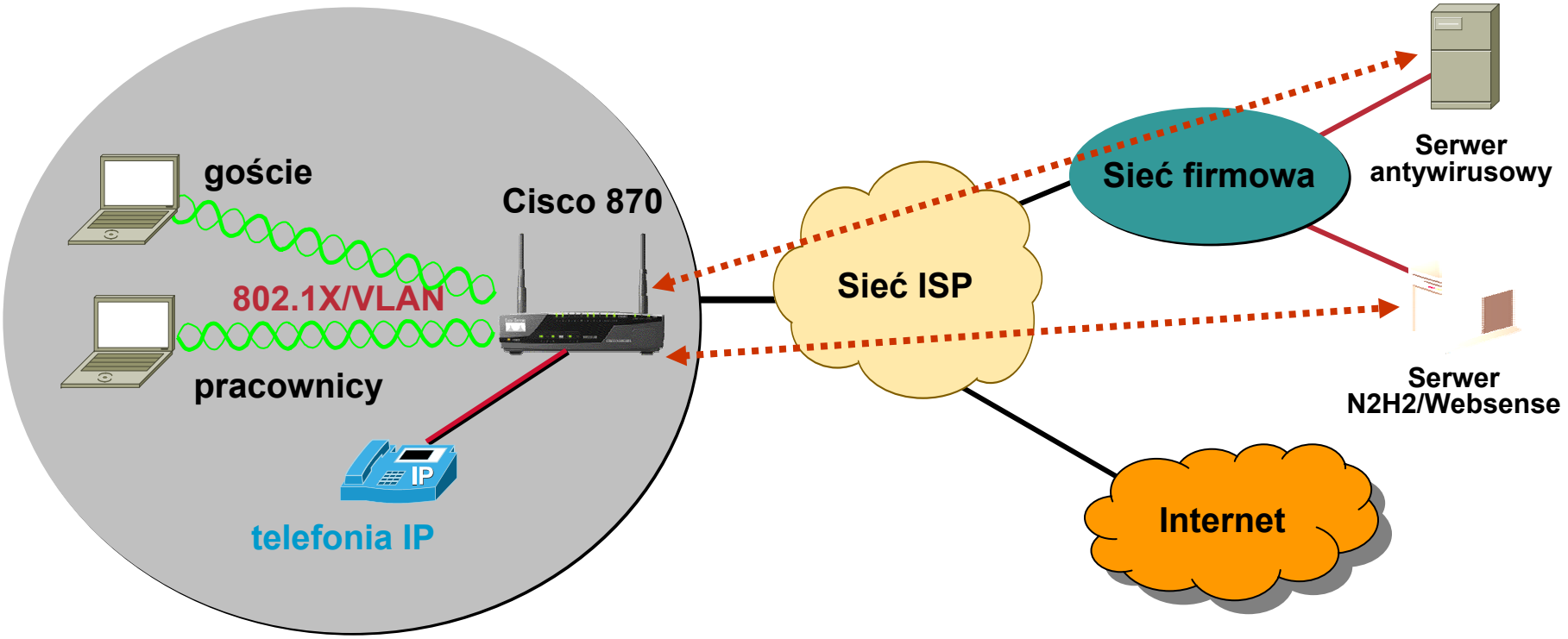


- Wydajność wire-speed
- Stateful firewall
- VPNy IPSec 3DES/AES
- IPS, NAC/Antywirus
- Zintegrowany port ISDN/modem analogowy lub port Ethernet jako backup i load-balancing
- Opcja 802.11b/g WLAN, wymienne anteny
- Zarządzalny przełącznik 8x 10/100, zasilacz wewnętrzny, opcjonalnie in-line power
- Do 8 VLANów
- Zarządzanie przez CLI Cisco IOS oraz Cisco SDM

Wartość (wydajność, funkcjonalność)

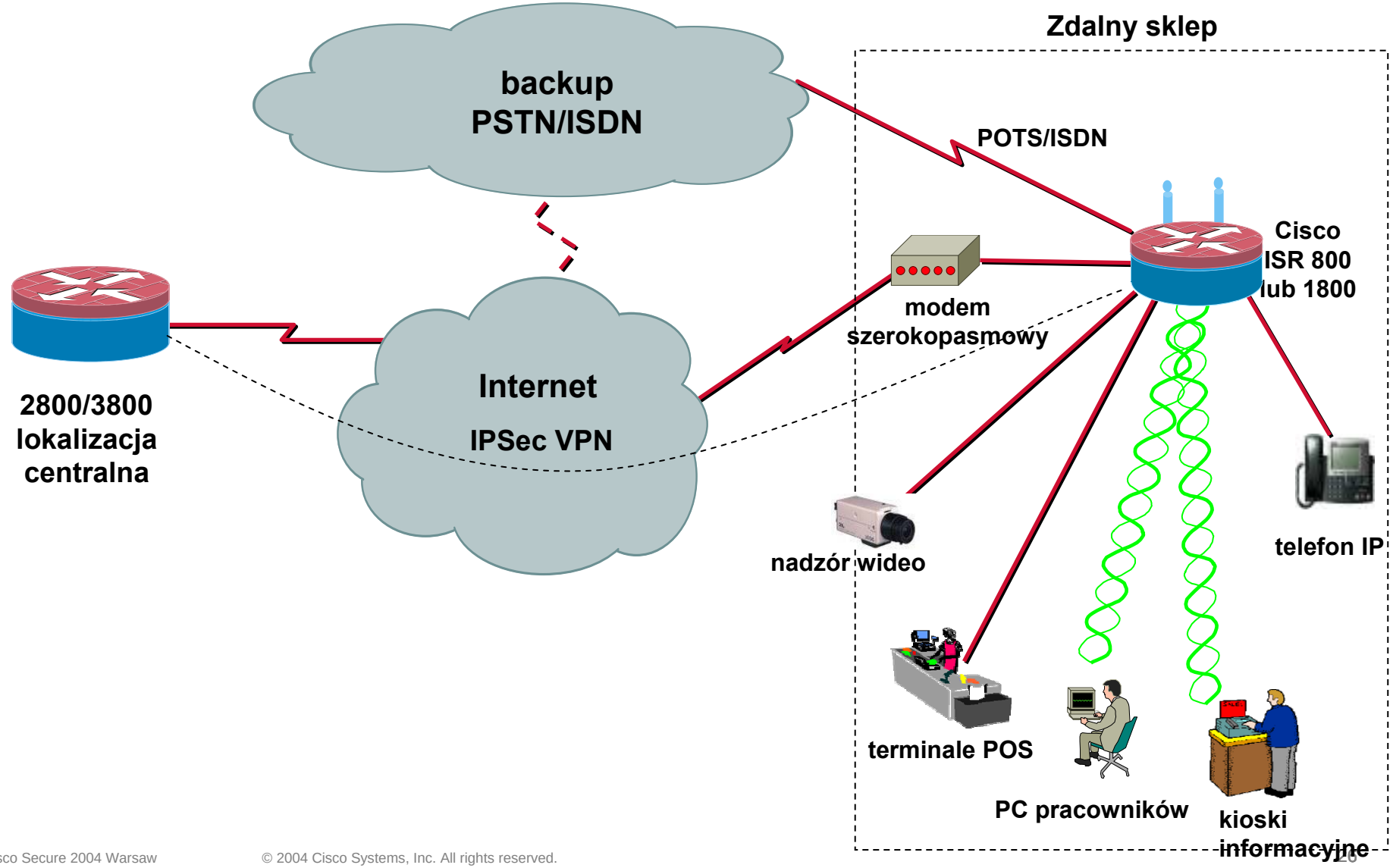
PRZYKŁADY ROZWIĄZAŃ

Bezpieczny dostęp ze zdalnych lokalizacji



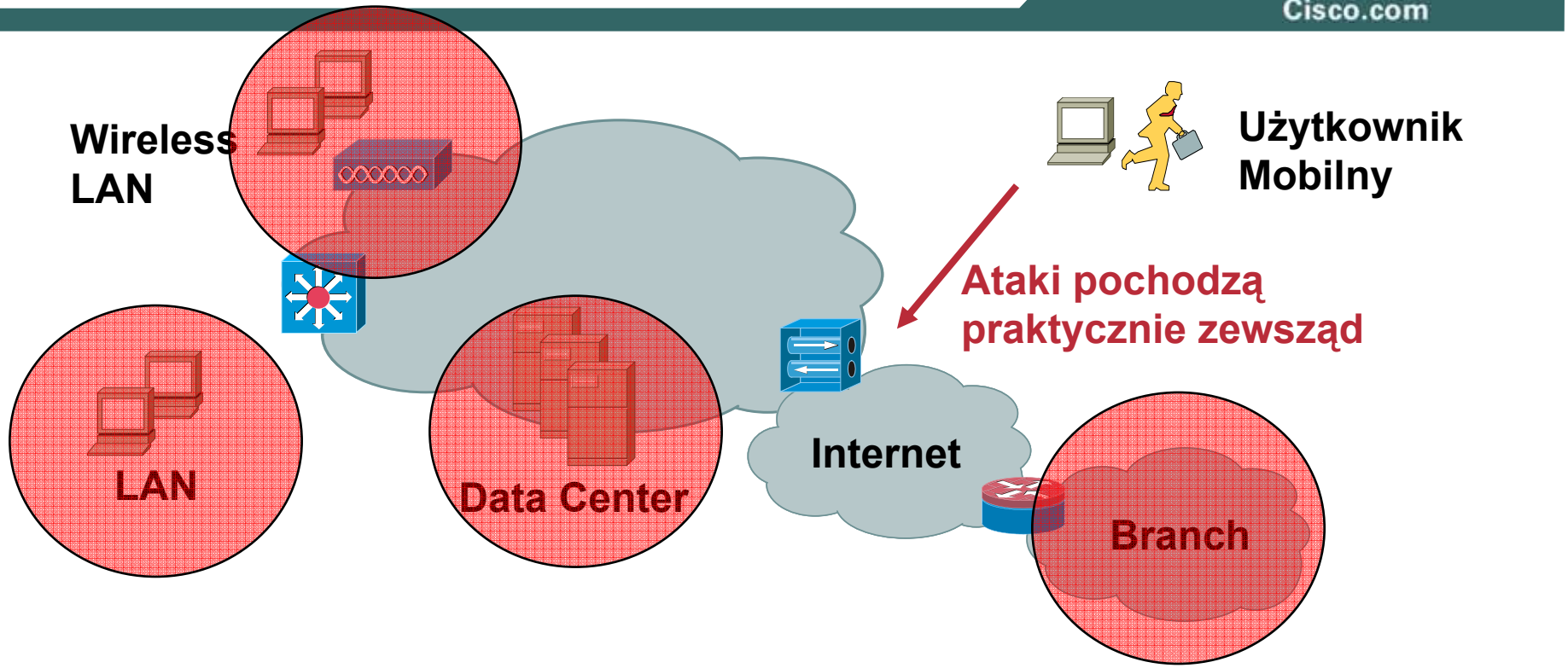
- Router zapewnia bezpieczny dostęp i ochronę zasobów, dzięki wykorzystaniu usług Stateful Firewall, NAC, URL filtering, IPsec VPN oraz zapewnia pełne portfolio usług, również WLAN dla lokalnych użytkowników

Bezpieczna sieć sprzedaży



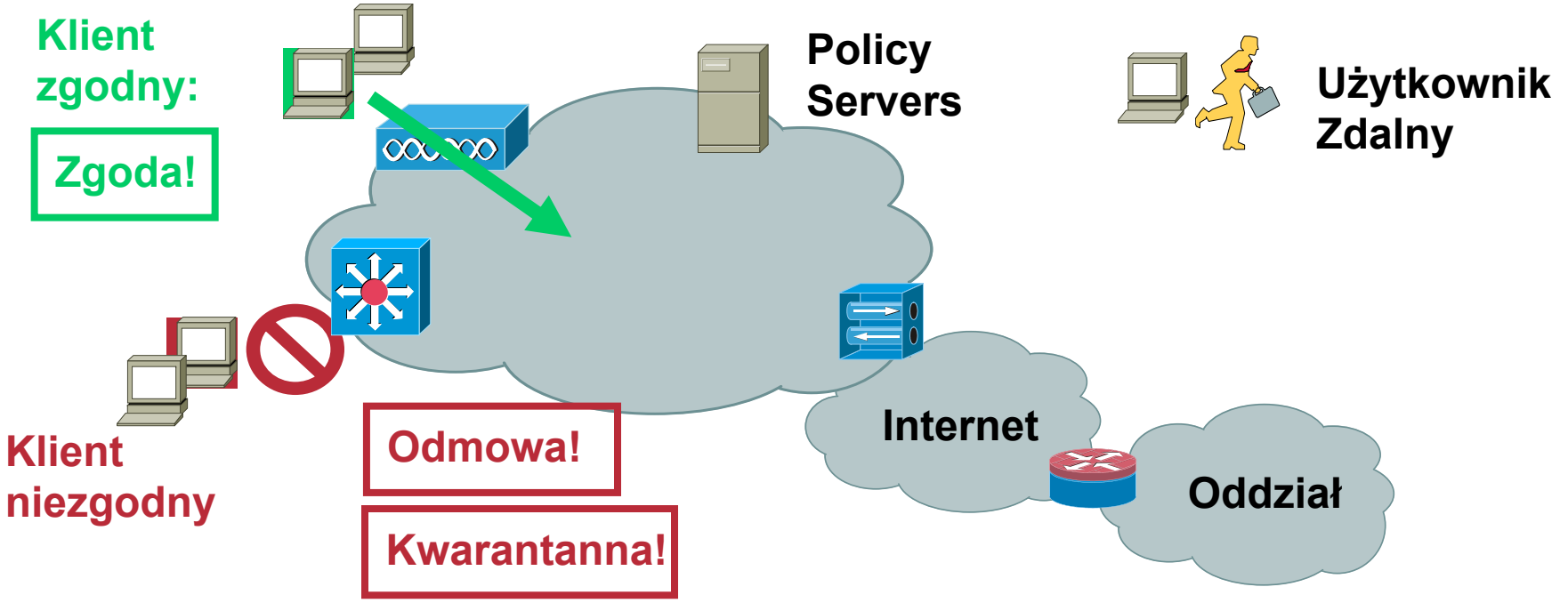
Uwierzytelnienie i kontrola dostępu

Infekcja – robak internetowy



- Samopropagujące się robaki w dalszym ciągu blokują działanie firm, powodują zaprzestanie działania sieci oraz wymuszają patchowanie
- Lokalizowanie i izolowanie zainfekowanych systemów I segmentów jest kosztowne I czasochłonne
- Wiele funkcji pracowniczych, metod i sposobów dostępu potęguje problem

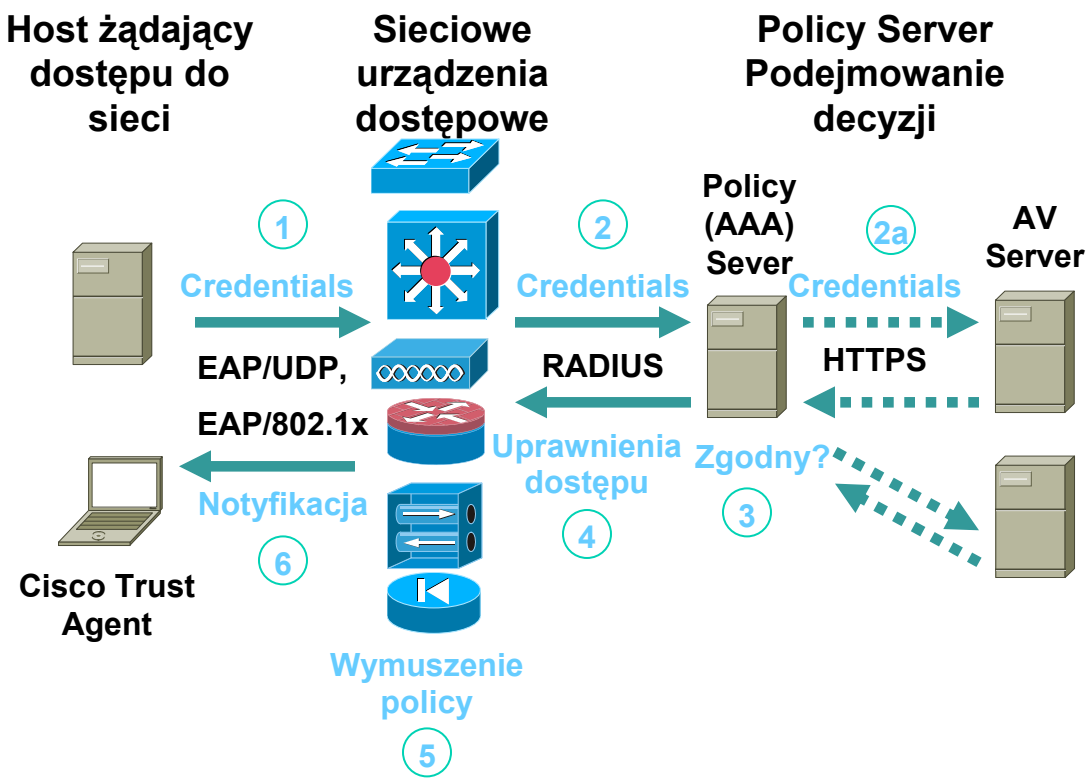
Idealne rozwiązanie: System Zintegrowany



- Rozwiązanie składa się z wielu komponentów
  - Rozwiązania instalowane na systemach końcowych znają warunki bezpieczeństwa
  - Policy Servers znaja zależność między zgodnością, a regułami dostępu
  - Urządzenia sieciowe (routery, przełączniki) wymuszają policy
- Ochrona przed wirusami/robakami wymaga współpracy między producentami

Rozwiązanie Network Admission Control oparte o CTA

NAC: Wykorzystanie sieci do inteligentnego narzucenia uprawnień dostępowych na bazie "security posture"urządzenia końcowego



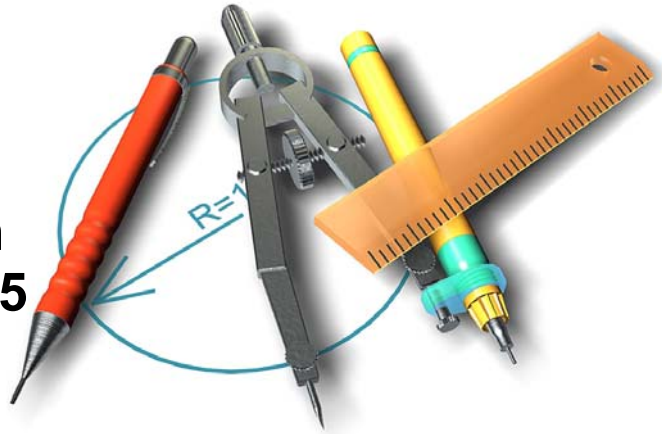
Charakterystyka NAC :

- Wszechobecne rozwiązanie dla *wszystkich metod* połaczeń
- Sprawdza *wszystkie* hosty
- Wykorzystuje inwestycje w sieć i oprogramowanie antywirusowe
- Usługi Quarantine & remediation
- Skalowalne rozwiązanie

…czyli co jest potrzebne dla wdrożenia rozwiązania NAC

Wymagania dla NAC:

- **Cisco IOS v.12.3(8)T lub nowszy**
- **IOS security (firewall feature set)**
- **Cisco Trust Agent zainstalowany na hostach (PC, laptop, etc.) lub Cisco Security Agent 4.5**
- **Cisco Secure Access Control Server (ACS) v3.3**
- **Znajomość konfiguracji list dostępowych (access control list - ACL)**
- **Znajomość konfiguracji: authentication, authorization and accounting (AAA) w Cisco ACS**

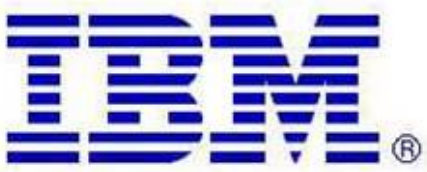


Aplikacje NAC-Enabled

- **McAfee**
  - VirusScan 7.0, 7.1, 8.0i

- **Symantec**
  - SAV 9.0 [AV] & SCS 2.0 [AV, FW, HIDS]

- **Trend Micro**
  - OfficeScan Corporate Edition & Trend Micro Control Manager integration - OfficeScan CE 6.5
  - CTA w komplecie z OfficeScan



- **IBM**
  - IBM/Tivoli (planowane)
- **Aplikacje tworzone niezależnie**

Kluczowe Elementy SDN

- **Wymuszenie Reguł Bezpieczeństwa**

  Network Admission Control, Identity Based Network Services, SSL Device Protection

- **Ochrona Urządzeń Sieciowych**

  Control Plane Policing, Auto-Secure, CPU Memory Thresholding

- **Elastyczne bezpieczne połączenia**

  Dynamic Multipoint VPN, VLAN

- **Automatyczne Reagowanie na Zagrożenia**

  Cisco Security Agent, Network Anomaly Detection (Riverhead), NIDS

Agent komunikacyjny

- **Cisco Trust Agent**

  Odpowiada na wywołania z urządzenia sieciowego (Network Access Device) z żądaniem przesłania “security credentials” dla hosta

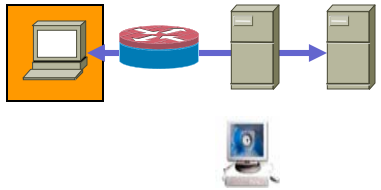
  Zbiera informacje o stanie bezpieczeństwa z oprogramowania NAC-enabled instalowanego na hostach, takiego jak antywirus i CSA

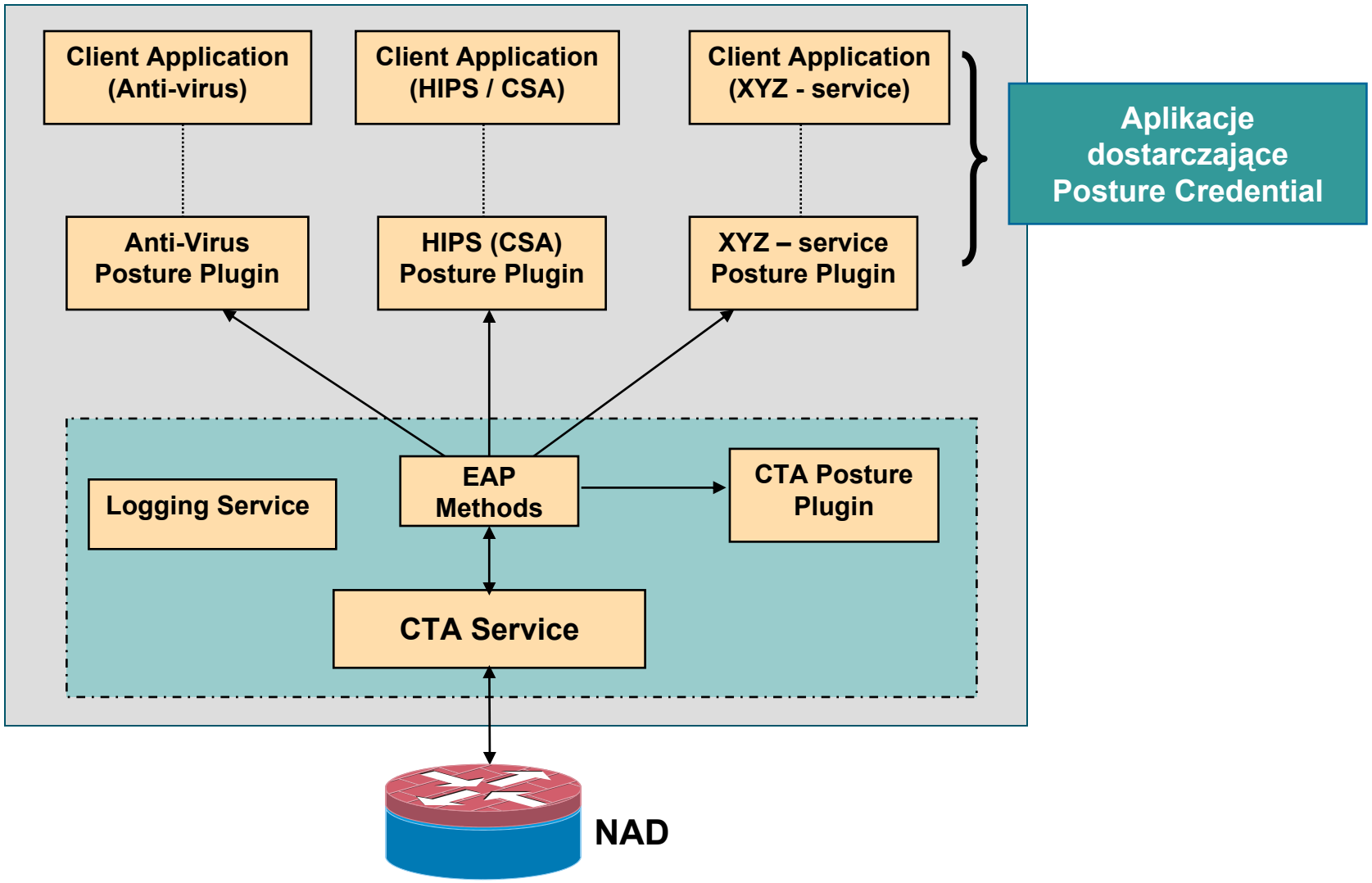
  Komunikuje “security credentials” hosta do urządzenia sieciowego (NAD)

  Cisco’s Trust Agent jest dołączane do oprogramowania Cisco i oprogramowania antywirusowego NAC-enabled

Cisco Trust Agent

Architektura





Systemy zarządzania NAC

- **CiscoWorks VPN/Security Management Solution (VMS)**

  Zarządzanie elementami NAC

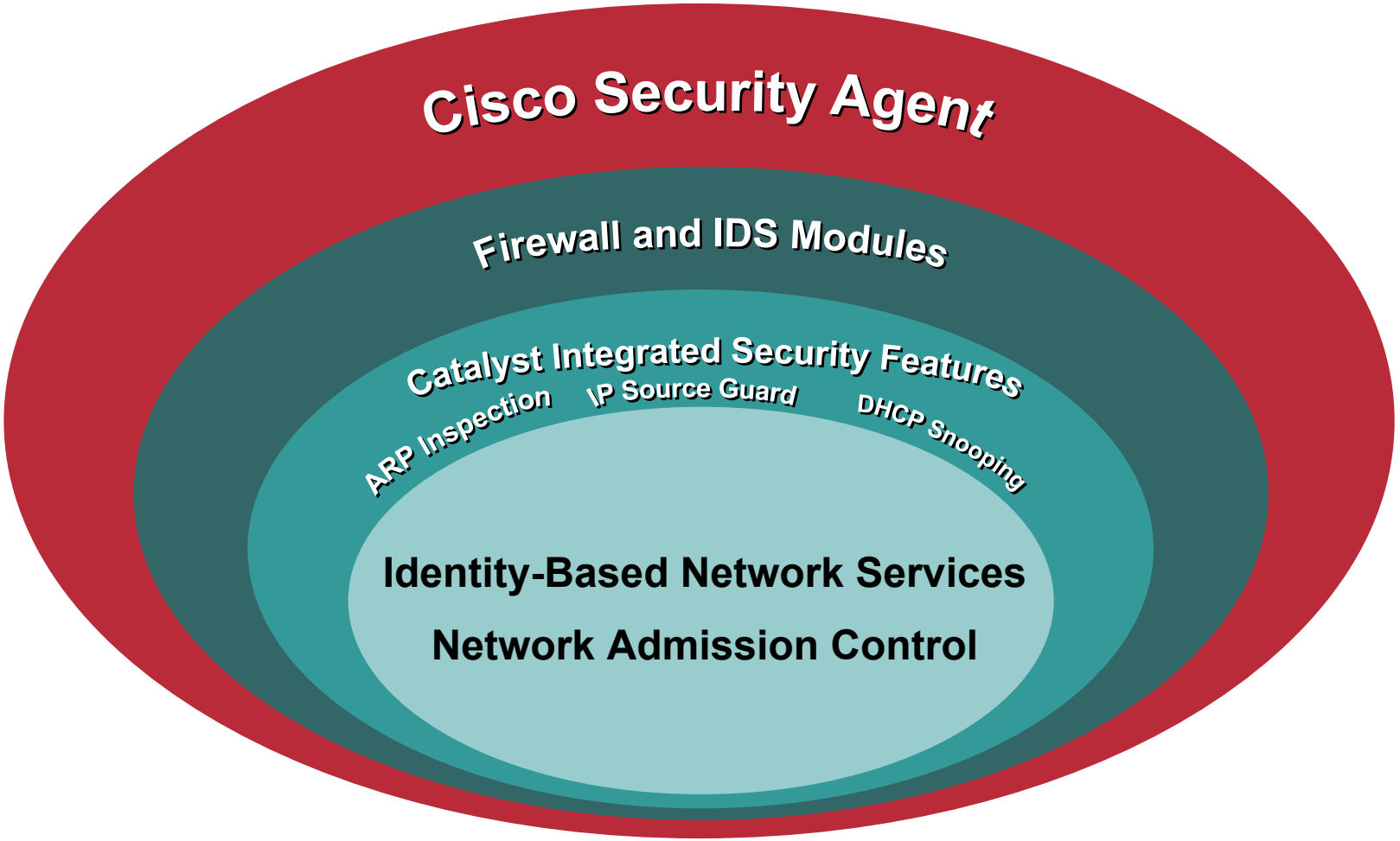
- **CiscoWorks Security Information Manager Solution (SIMS)**

  Zapewnia narzędzia monitoringu i raportowania

- **Producenci oprogramowania antywirusowego (oraz innych aplikacji NAC-enabled) również dostarczaja narzedzia zarzadzania – dla własnego oprogramowania (np.AV)**

Co to jest IBNS?

Bezpieczeństwo jest jak... cebula?



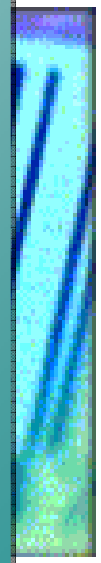
Co to jest IBNS?

- IBNS != IEEE 802.1x
- IBNS jest nadzbiorem funkcjonalności IEEE 802.1x
- IBNS jest podstawą autentykacji w sieciach LAN, której część stanowi 802.1x
- Dodatkowe rozszerzenia/technologie uzupełniają 802.1x tworząc IBNS.

Cisco Identity Based Network Services (IBNS) kontroluje kto i co jest w Twojej sieci
Funkcje IBNS w Catalyst 6500 IBNS (CatOS 8.4)

- Podstawowe funkcje IEEE 802.1X
- IBNS: rozszerzenia Cisco dla .1x
  - 802.1X + Dynamic VLANs
  - 802.1X + Port Security
  - 802.1X + VVID (IP Telephony)
  - 802.1X Guest VLANs
  - 802.1X + ARP Inspection
  - 802.1X + DHCP
  - 802.1X + Security Profile — Soon
  - 802.1x + QoS Profile — Soon

- Większa kontrola dostępu
- Większa elastyczność
- Większa produktywność użytkowników
- Niższe koszty operacyjne
- Większe bezpieczeństwo w sieciach konwergentnych



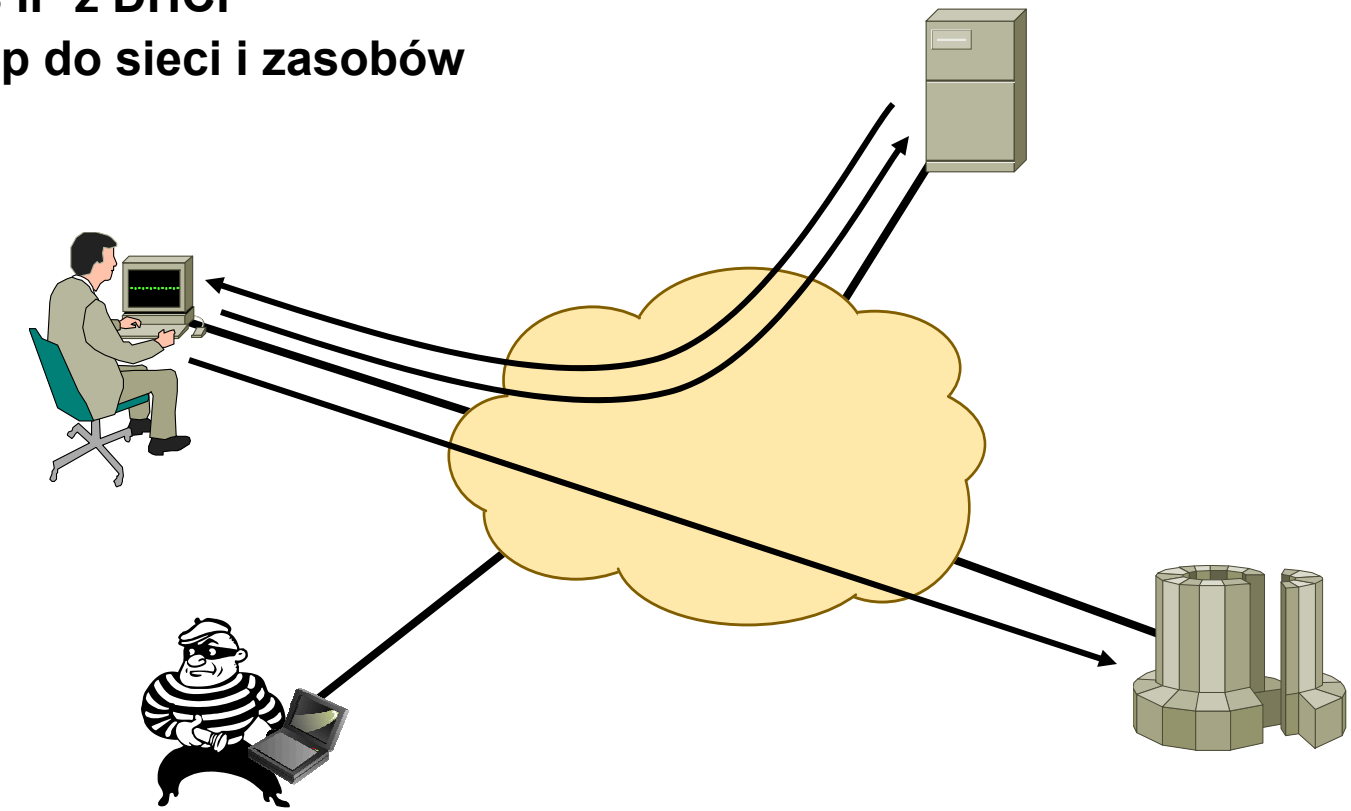
Bezpieczna mobilność i optymalizacja pracy = zwiększona produktywność

Mniejszy OpEx przy mniejszych nakładach pracy z MAC(Moves/Adds/Changes)

Łatwy nieautoryzowany dostęp

- Użytkownik dołącza sie do sieci
- Wysyła zapytanie o IP
- Adres IP z DHCP
- Dostęp do sieci i zasobów

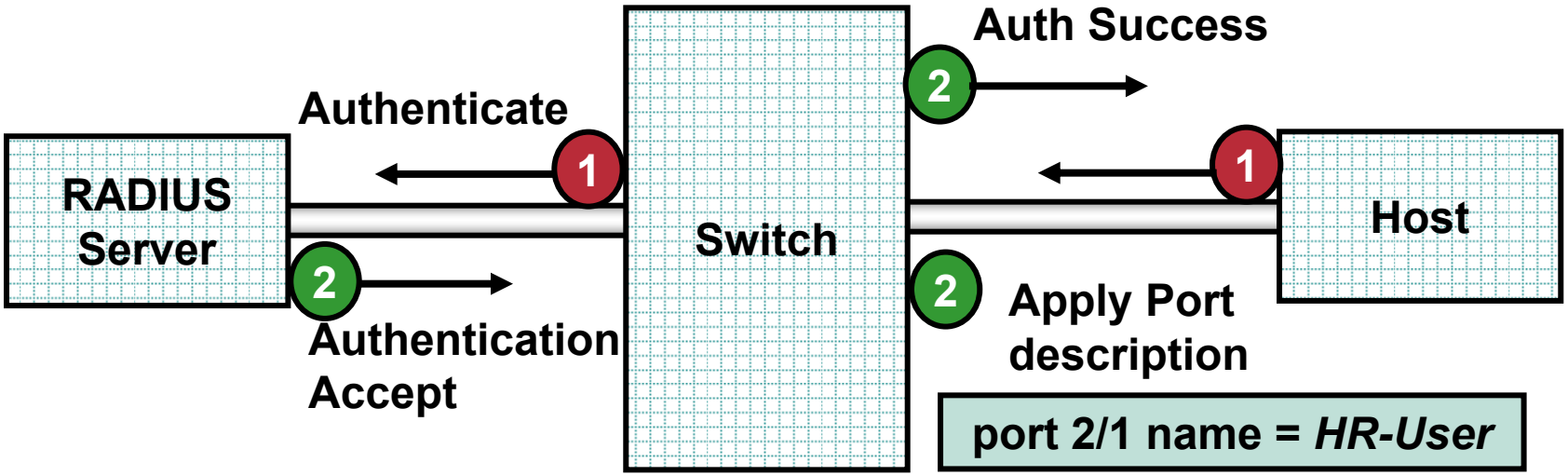
Łatwe i elastyczne; dobra mobilność



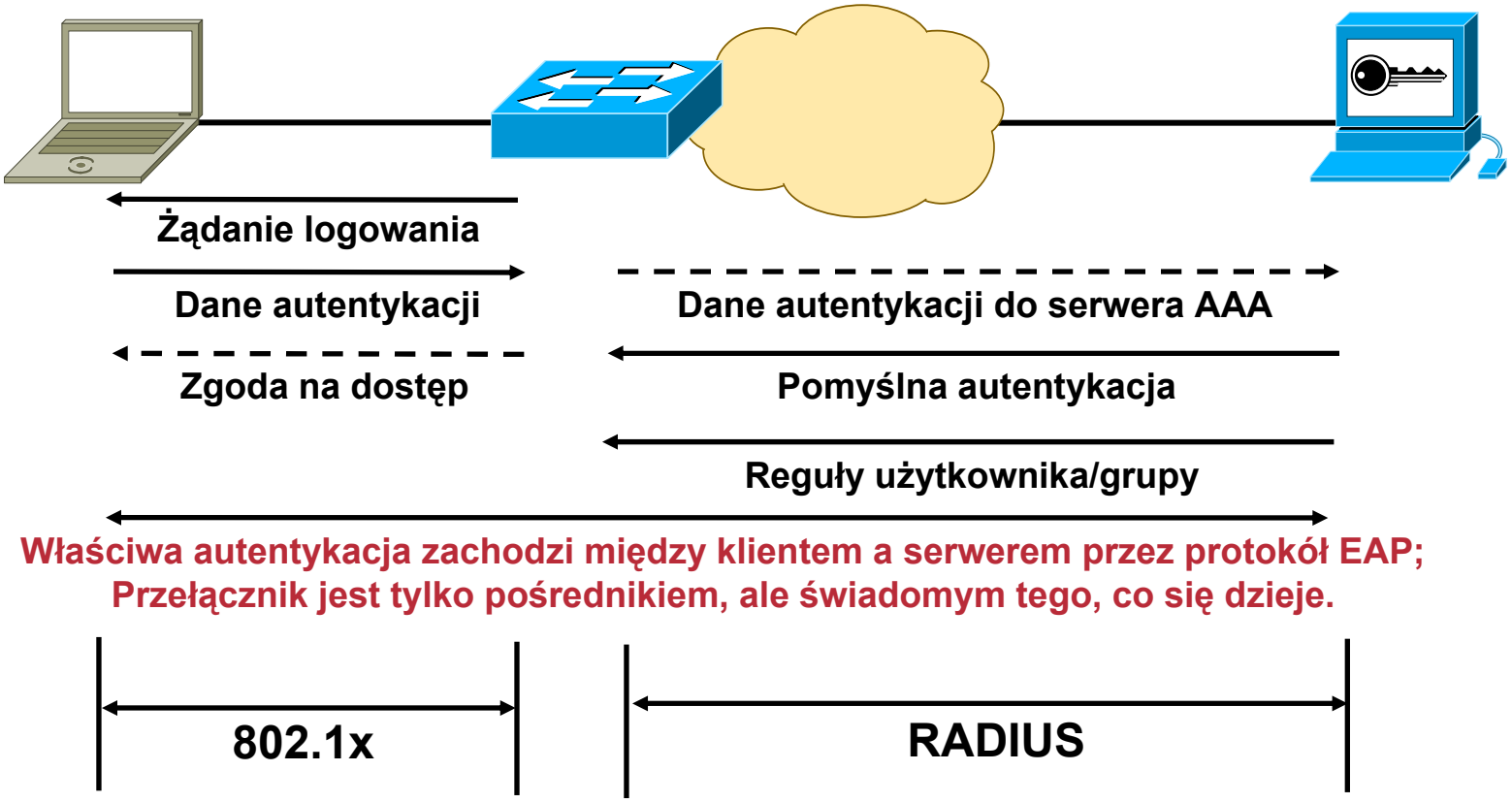
Niestety to działa dla KAŻDEGO

Trzy prawdy o IBNS

1. Trzyma intruzów na zewnątrz
2. Zapewnia uczciwość użytkowników wewnątrz sieci
3. Zwiększa „widzialność” sieci (np. 802.1x + port naming, RADIUS Accounting)



Bliższe spojrzenie…



Metody Autentykacji

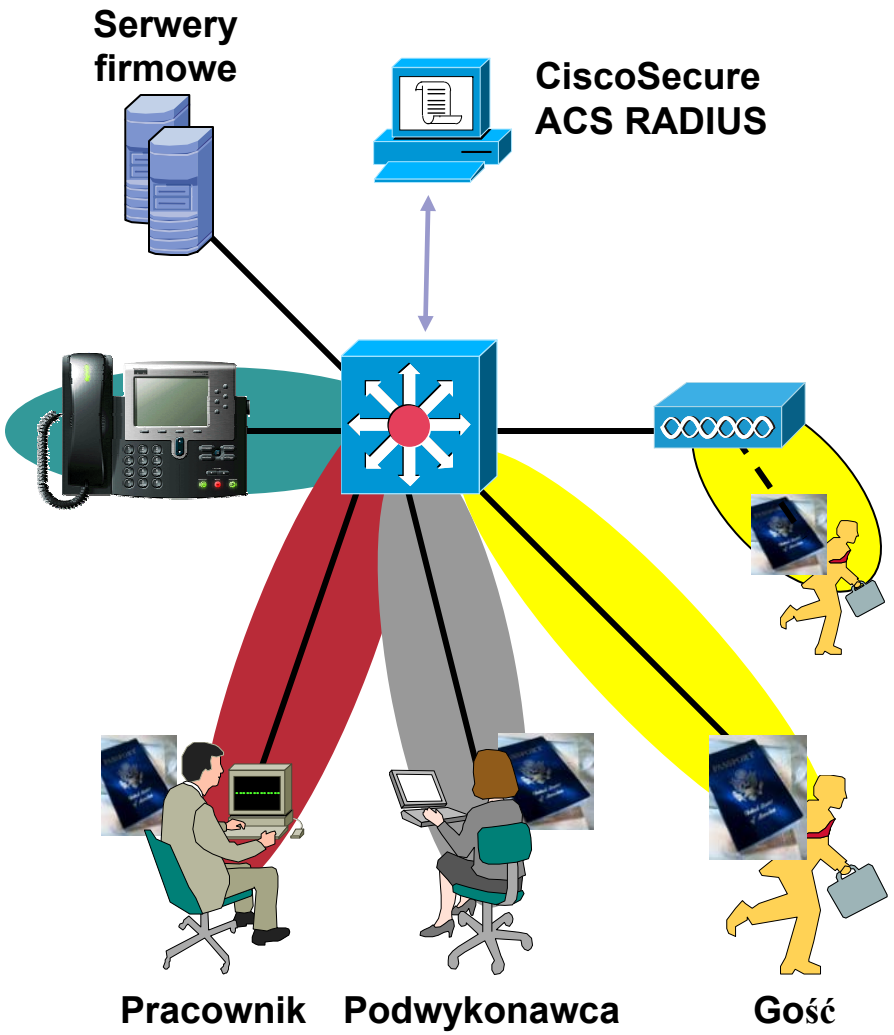
Cisco.com

- **Korzystające z Challenge-Response**
  - **EAP-MD5: challenge-response metodą MD5**
  - **LEAP: autentykacja „username/password”**
  - **EAP-MSCHAPv2: autentykacja „username/password” z MSCHAPv2 challenge-response**
- **Kryptograficzne**
  - **EAP-TLS: korzysta z certyfikatów x.509 v3 PKI oraz mechanizmu TLS**
- **Tunelowe**
  - **PEAP: Protected EA; tuneluje inne metody EAP w zaszyfrowanym tunelu; analogia do Web SSL**
  - **EAP-FAST: nowa metoda tunelowa, która nie wymaga certyfikatów**
- **Inne**
  - **EAP-GTC: Generic Token Card – obsługa haseł jednorazowych/tokenów**

Cisco IBNS — rozszerzenia RADIUS

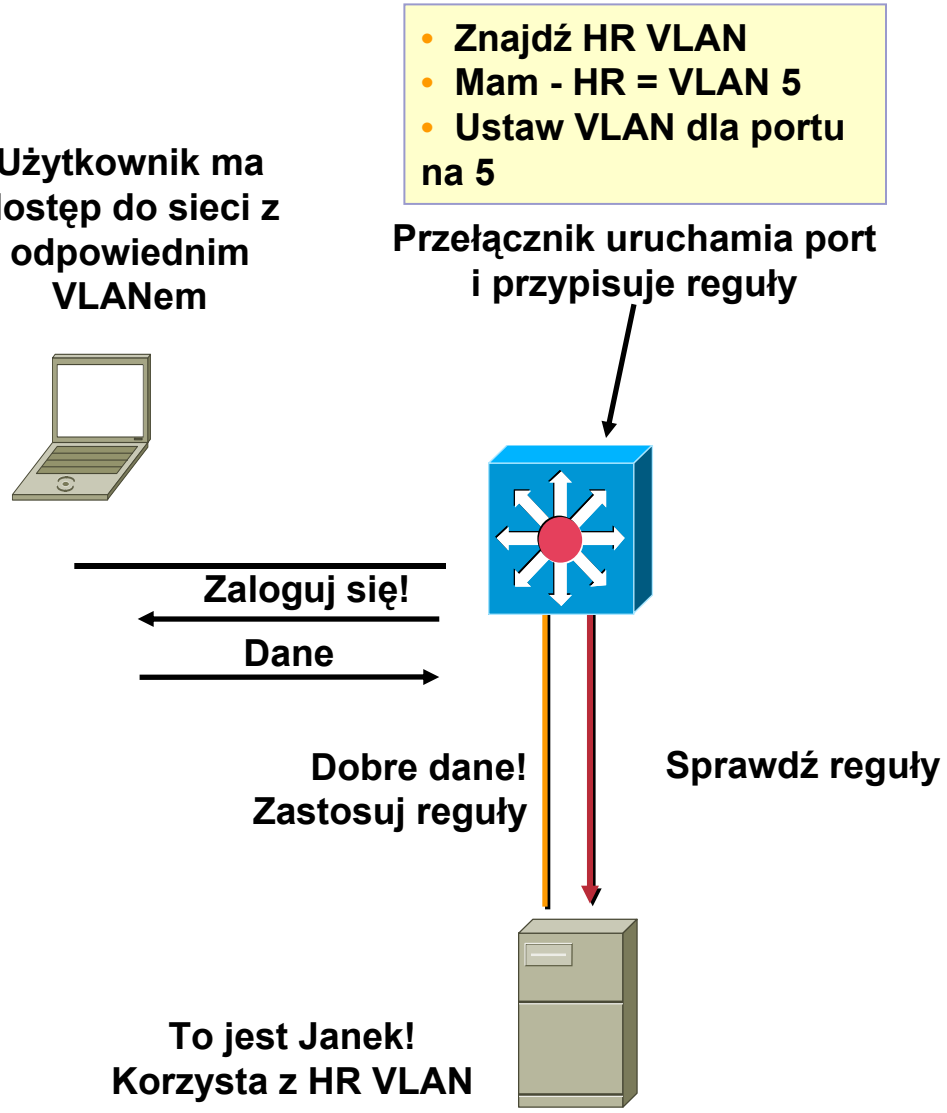
Nowe możliwości

- Dynamiczne przypisanie reguł bezpieczeństwa z wykorzystaniem ACL
- Dynamiczne przypisanie reguł QoS wykorzystując ACL per-port/per-user
- Rozliczanie w oparciu o IBNS



Stosowanie reguł: przypisanie VLAN

- **Autentykacja użytkownika a następnie przypisanie do portu VLANu zdefinowanego w ACS**
- **RADIUS AV-Pair używane do przesyłania informacji o VLANie do autentykatora.**
- **Wykorzystanie AV-Pair do przypisania VLAN jest w specyfikacji IEEE 802.1x**
- **AV-Pairs:**
  - **[64] Tunnel-Type – "VLAN" (13)**
  - **[65] Tunnel-Medium-Type – "802" (6)**
  - **[81] Tunnel-Private-Group-ID -** *<VLAN name>*



Identity Based Networking Services (IBNS)

Cisco Aironet	Cisco ACS Server	Catalyst 3750/3550/2950	Catalyst 4000/4500	Catalyst 6500
				

Cisco Wireless Security Suite featuring:
• Multiple VLANs for employees, guests and application specific devices
• Cisco IOS
• Expanded 802.1X Authentication Support for: Cisco LEAP, EAP-TLS, EAP-TTLS, PEAP, EAP-SIM
• Expanded Encryption Support for 802.11i Pre-standard TKIP
  • Message Integrity Check
  • Per-packet Keying
  • Broadcast Key Rotation
	ACS v3.0 *Avail Now*
	• 802.1x Catalyst support
	• PKI Support
	• Password Aging
	• New PKI support for Wireless and Switches
	ACS v3.1 *Avail Now*
	• PEAP Support for Wireless
	• 802.1x & EAP
	• SSL Security
	ACS v3.2 *Avail Now*
	• PEAP support for Microsoft Windows and Cisco clients
	• EAP mixed configurations 802.1x & EAP
	• Support of Windows Server 2003 Enterprise Edition
	• **Machine Access Restrictions (MARs) of EAP-TLS.**
	• **EAP-FAST authentication support**
	• **Processing of multiple LDAP authentication requests**
	• **Support of machine auth**
	• **User-based accounting for Aironet Wireless Access Points**
		IOS 12.1(14)EA1
		Avail Now
		• 802.1x Authentication
		• 802.1x with Port Security
		• 802.1x with VVID
		• 802.1x with VLAN Assignment
		• 802.1x with ACLs (3750/3550)
		• 802.1x with Guest VLAN
			CatOS 7.2(1)
			Avail Now
			• 802.1x Authentication
			• 802.1x with VLAN Assignment
			IOS 12.1(19)EW (4500)
			Avail Now
			• 802.1x Authentication
			• 802.1x with VLAN Assignment
			• 802.1x with Guest VLAN
			• 802.1x with Dynamic ARP Inspection
			• 802.1x with IP Source Guard
			IOS 12.2(18)EW (4500)
			Avail Now
			• 802.1x with Port Security
			• 802.1x with RADIUS Accounting
				CatOS 7.6(1)
				Avail Now
				• 802.1x Authentication
				• 802.1x with Port Security
				• 802.1x with VVID
				• 802.1x with VLAN Assignment
				• 802.1x Guest VLAN
				• 802.1x with Static ARP Inspection
				• 802.1x with DHCP Relay
				• 802.1x with HA
				• 802.1x with Multiple Hosts Option
				IOS 12.2(13)E
				Avail Now
				• 802.1x Authentication
				• 802.1x with VLAN Assignment
				• 802.1x with VVID

Identity Based Networking Services (IBNS)
End-to-End Solution

Identity Based Networking Services (IBNS)

Cisco Aironet	Cisco ACS Server	Catalyst 3750/3550/2950	Catalyst 4000/4500	Catalyst 6500
				
	ACS v3.3 ***New*** • **Cisco Network Admission Control (NAC) support** • **EAP-FAST support for wireless authentication** • **Downloadable IP Access Control Lists (ACLs)** • **Certification Revocation List (CRL) comparison for EAP-TLS authentication** • **Network Access Filtering (NAF)** • **Cisco CSA integration on Cisco Secure ACS Solution engine** • **Replication enhancements (granular selection of users and group of users as separate replication components)**	**IOS 12.1(20)EA2** **IOS 12.2(20)SE** ***New*** • 802.1x with RADIUS Accounting • 802.1x MIB	**CatOS 8.4(1)GLX (4500)** ***New*** • 802.1x with Guest VLAN	**CatOS 8.3(1)** ***New*** • 802.1x with ACLs • 802.1x with QoS Policy • 802.1x with Dynamic ARP Inspection • 802.1x with IP Source Guard • 802.1x with WoL • 802.1x with RADIUS Accounting • 802.1x with DNS Resolution for RADIUS • 802.1x with One-to-Many VLAN Assignment • 802.1x with Authenticated Identity to Port Description Mapping

Identity Based Networking Services (IBNS)
End-to-End Solution

Zintegrowana Ochrona w sieci LAN

Zagrożenia w sieci LAN

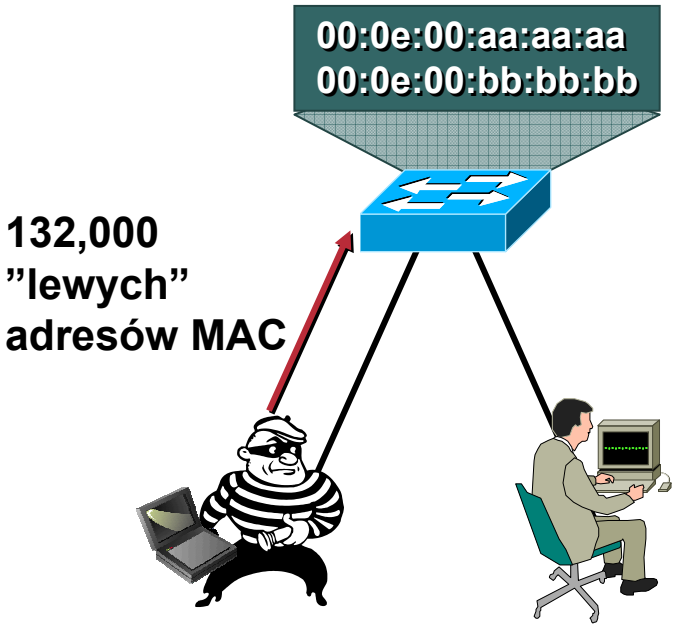
Eliminowane przez funkcje przełączników Catalyst

- **Zalewanie adresami MAC**
  - Narzędzia: macof (część pakietu of dsniff)
    - Zalanie pakietami SYN z losowymi src/dst MAC, losowymi src/dst IP
    - Po wypełnieniu tablicy CAM, ruch przesyłany na wszystkie porty
    - Losowe adresy IP zawierają również adresy m-cast i potencjalnie zmuszają przełączniki do intenswnej pracy
- **Podstawiony serwer DHCP**
  - Narzędzia: gobbler lub podstawiony serwer DHCP
    - Atak „Man in the middle” przez DNS lub IP GW
- **Wyniszczenie DHCP**
  - Narzędzia: gobbler
    - Wyczerpanie puli adresów DHCP
- **ARP Spoofing**
  - Narzędzia: ettercap, dsniff, arpspoof
    - Wykrywanie topologii sieci MAC
    - Ataki „Man in the middle” z przechwytywaniem pakietów, haseł etc.

Podnosimy poprzeczkę atakującym

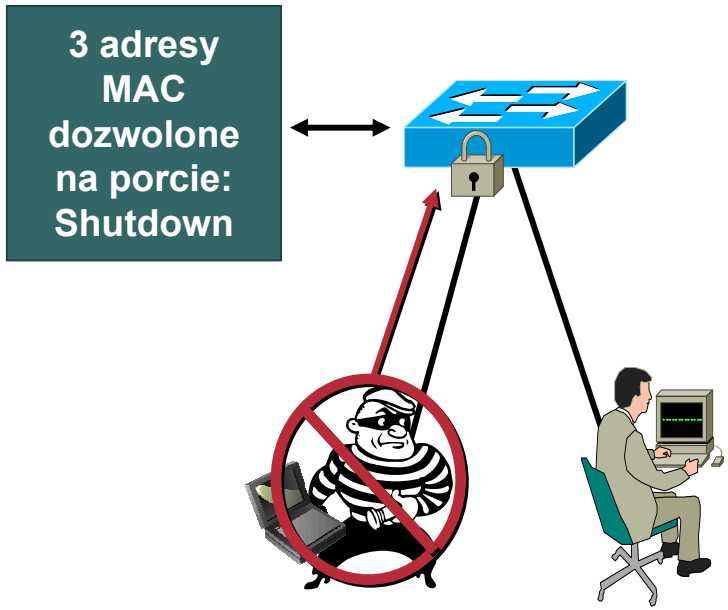
Ataki w warstwie MAC

Cisco.com



Problem:

Proste narzędzia pozwalają zalać tablicę CAM losowymi adresami MAC zmieniając przełącznik w hub



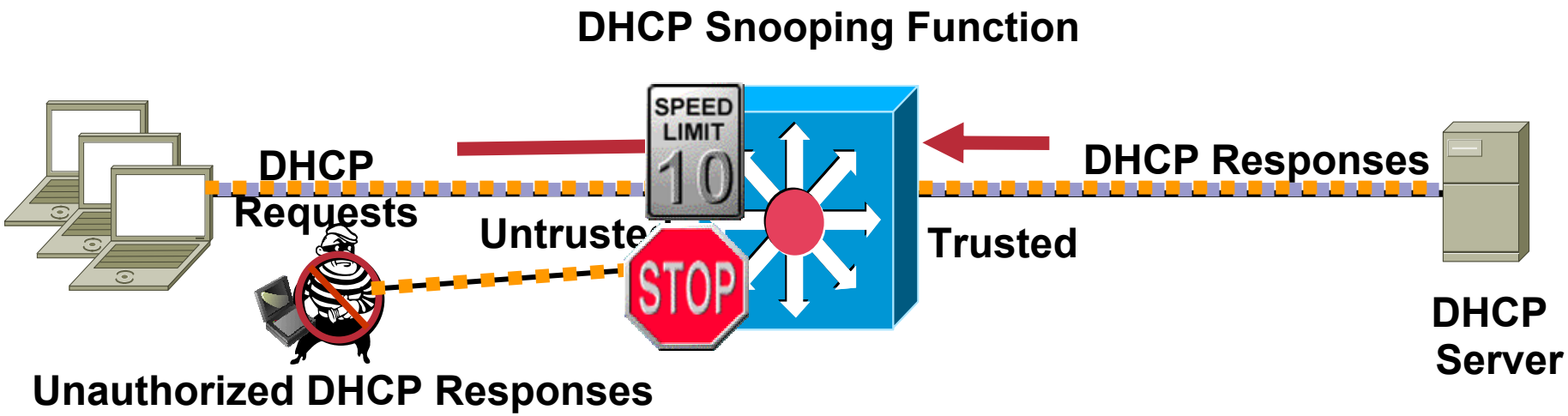
Rozwiązanie:

„Port Security” ogranicza ilość adresów MAC na porcie, wyłącza port i wysyła komunikat SNMP

Funkcja „DHCP Snooping”

Zabezpieczenie przeciw podstawionym serwerom DHCP

Cisco.com

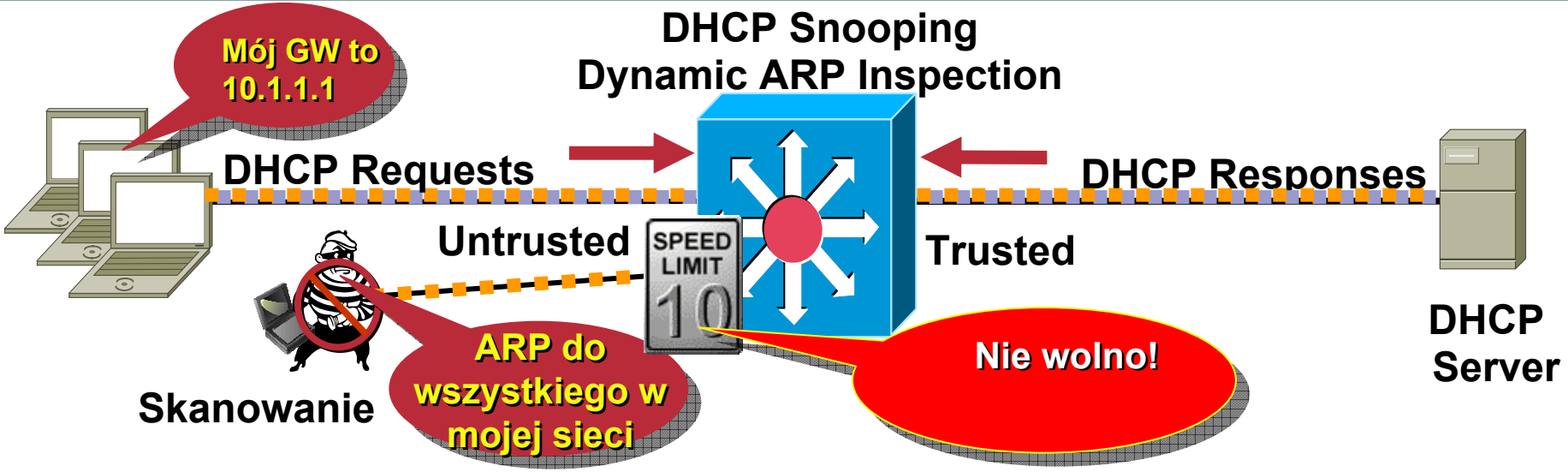


DHCP Snooping

1. Śledzenie zapytań (Discover)
2. Śledzenie odpowiedzi (Offer)
3. Ograniczenie pasma dla zapytań na portach Trusted. Eliminuje ataki DoS na serwer DHCP
4. Odrzuca odpowiwedzi (Offers) na portach Untrusted. Elimiuje podstawione serwery DHCP

Dynamic ARP Inspection

Zabezpieczenie przeciwko skanowaniu ARP/rozpoznaniu



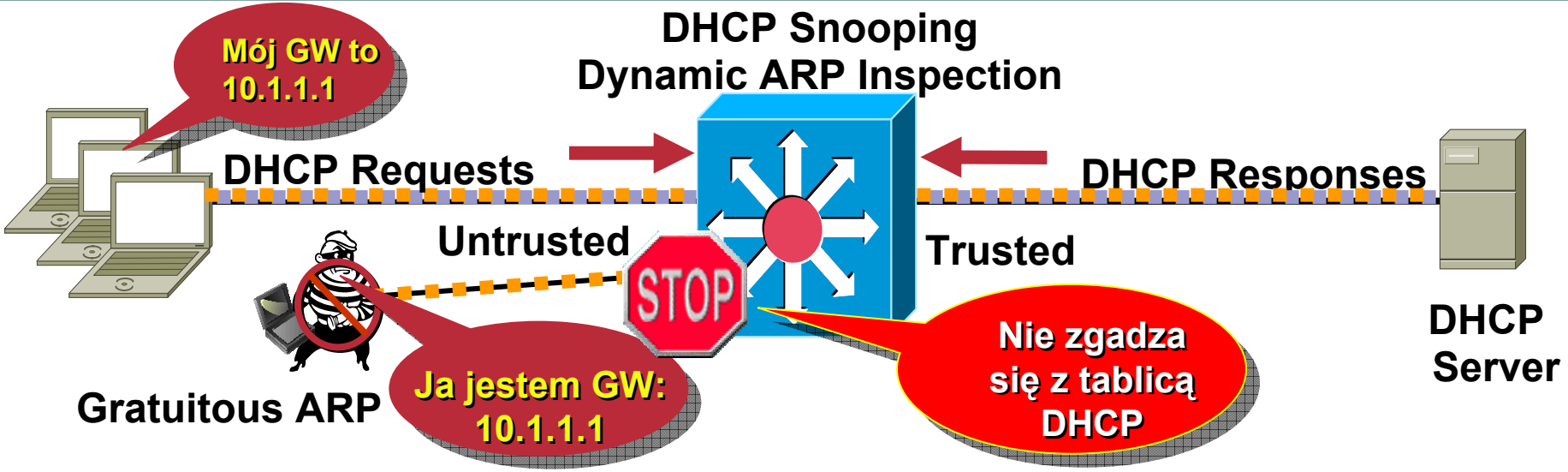
Dynamic ARP Inspection

1. Korzysta z tablicy przypisań DHCP Snooping
2. Śledzi pary MAC/IP z wymiany DHCP
3. Ogranicza zapytania ARP na portach klientów.

Dynamic ARP Inspection

Zabezpieczenie przeciwko „zatruwaniu” ARP (ettercap, dsnif, arpspoof)

Cisco.com



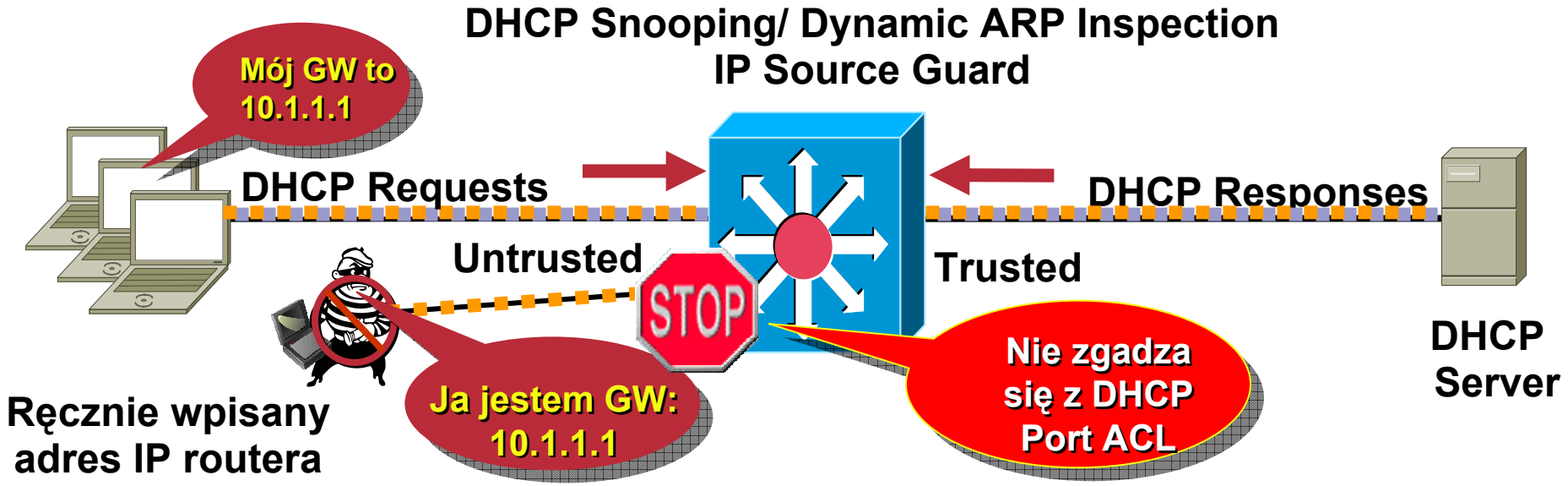
Dynamic ARP Inspection

1. Korzysta z tablicy przypisań DHCP Snooping
2. Śledzi pary MAC/IP z wymiany DHCP
3. Ogranicza zapytania ARP na portach klientów
4. Odrzuca podejrzane Gratuitous ARP

IP Source Guard

Zabezpieczenie przeciwko podejrzanym/podstawionym IP

Cisco.com

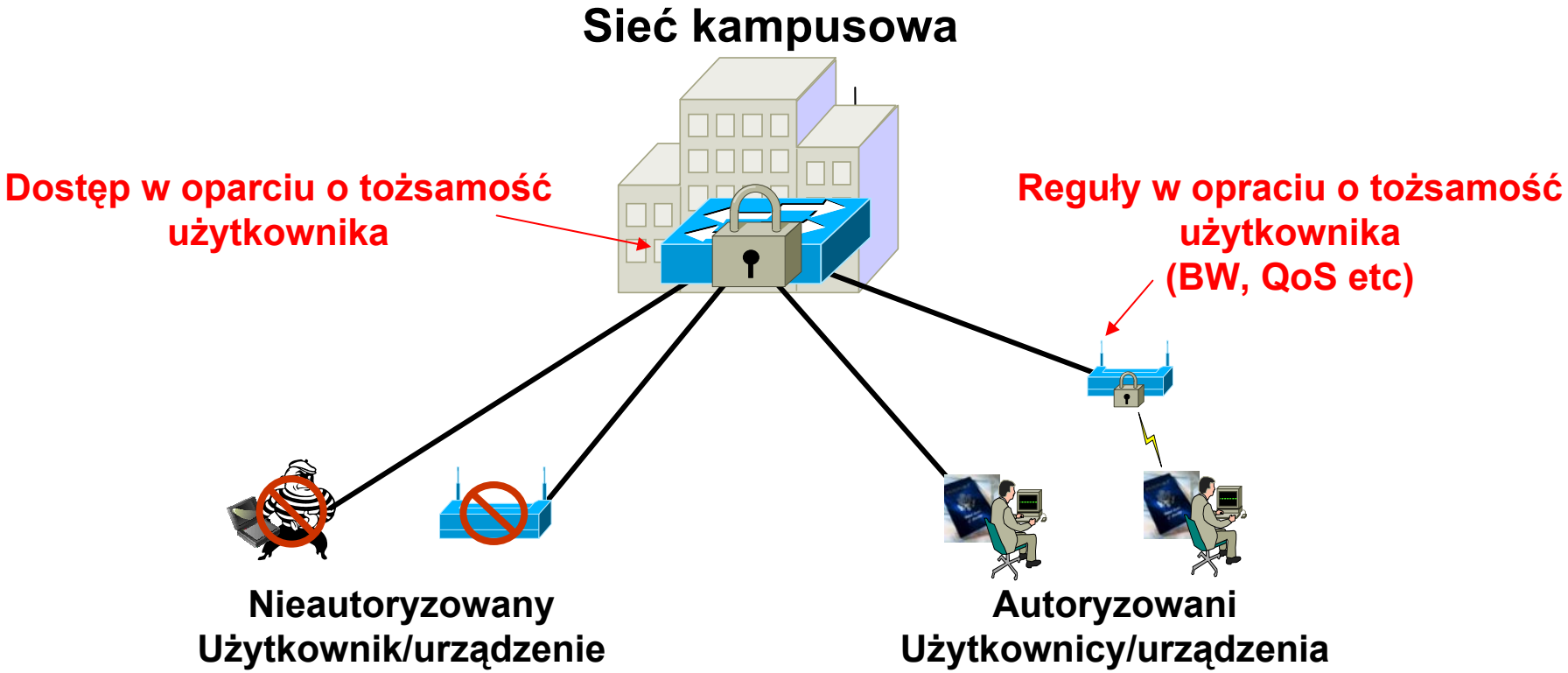


IP Source Guard

1. Korzysta z tbalicy przypisań DHCP Snooping
2. Śledzi przypisania IP do portu
3. Dynamicznie programuje Port ACL, aby odrzucać ruch z IP innego niż przydzielony przez DHCP

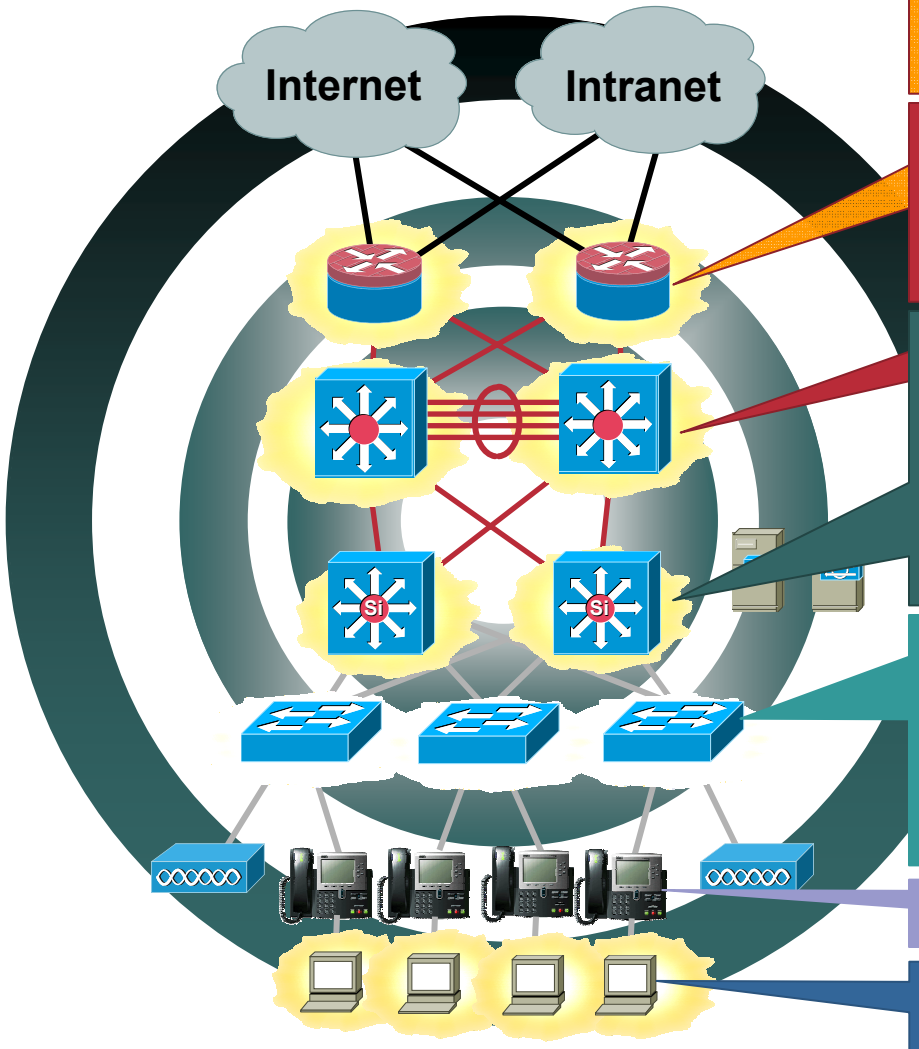
Bezpieczeństwo z IBNS

Określamy "kto" ma dostęp i "co" może zrobić



- Równoważne postawieniu strażnika przy każdym porcie
- Tylko autoryzowany użytkownik ma dostęp do sieci
- Nieautoryzowani użytkownicy mogą być umieszczeni w VLANie dla gości
- Zabezpiecza przed nieautoryzowanymi AP/koncentratorami etc.

Zintegrowane bezpieczeństwo Cisco
ZABEZPIECZANIE SIECI KAMPUSOWEJ



CEF Switching
QoS, CAR & Netflow
IOS FW, NIDS

Hardware CEF Switching
QoS & Netflow
Sup720 Rate Limiters & SPD
Segmentation – VRF & MPLS

HW CEF Switching
SUp720 Rate Limiters & Storm Control
HW Security and QoS ACL's
TCP Intercept, uRPF & Netflow
FWSM, NAM & NIDS
QoS Microflow Policing & CAR

DHCP Snooping, DAI, IP Source Guard
802.1x & Port Security
QoS Per Port/VLAN Policing and Marking
HW Security and QoS ACL's
Storm Control & Private VLAN's

Extended QoS Trust Boundary

Cisco Security Agent (CSA)
Network Admission Control

Pytania…
Pytania…
Pytania…