Internet, ale jaki?
Bezpieczne połączenia WAN i VPN

Andrzej Zając
Solidex

http://www.solidex.com.pl

Agenda

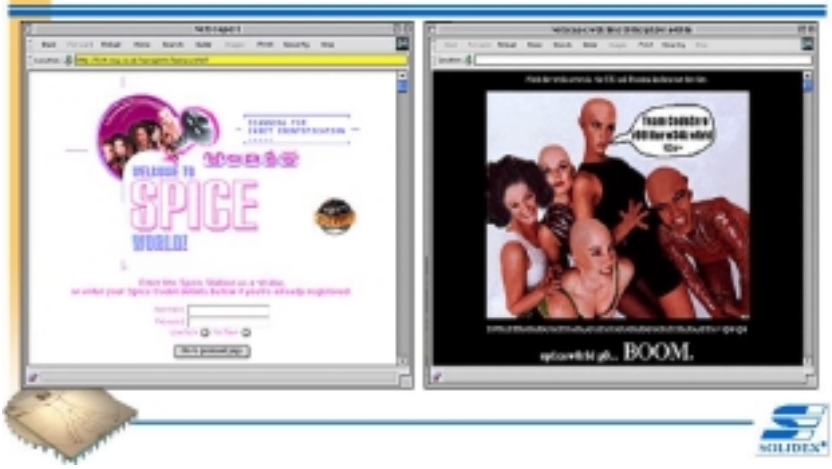
- Aspekty biznesowe
- Aspekty techniczne
- Firewall - co to takiego ?
  - Elementy składowe struktury ochrony styku
  - Modelowe rozwiązania

Taka jest rzeczywistość

YAHOO!
amazon.com
CNN.com
ebay
E*TRADE

Taka jest rzeczywistość c.d.

Taka jest rzeczywistość c.d.



Straty związane z przerwami w działaniu usługi e-Commerce

	Dzienne zyski z Internetu 1/16/99	
www.amazon.com	$2,700,000	$22,500
www.dell.com	$10,000,000	$91,320
www.cisco.com	$20,000,000	$182,640
www.intel.com (partner extranet site only)	$33,000,000	$274,980

Source: Forrester Research 1999

Ankieta dotycząca bezpieczństwa informacji - Ernst & Young

- 78% ankietowanych firm odnotowało w ciągu ostatnich dwóch lat stratę finansową związaną z bezpieczeństwem informacji
- Niektóre firmy odnotowały straty przekraczające milion USD
  - Straty były spowodowane:
  - 1. Wirusami komputerowymi
  - 2. Złośliwymi działaniami z wnętrza sieci
  - 3. Złośliwymi działaniami z zewnątrz (hacking)
  - 4. Niedopatrzeniami
  - 5. Szpiegostwem przemysłowym

Polityka bezpieczeństwa

- **Dokument definiujący poziom ryzyka, jakie dana organizacja zgadza się zaakceptować w zależności od wartości chronionej informacji i użytych do tego celu zasobów**
- **Zwykle określa:**
  - Co powinno być chronione ...
  - ... przed kim ...
  - ... i w jaki sposób,
  - a także sposób reakcji na zdarzenia.

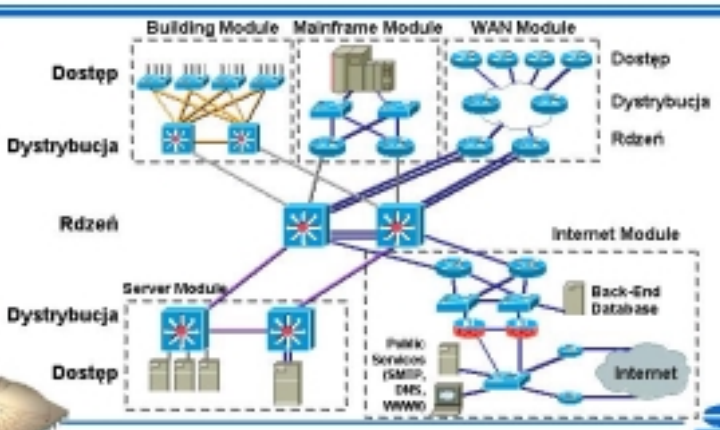
Polityka bezpieczeństwa sieciowego jest odbiciem polityki bezpieczeństwa Firmy. Nie można oddzielać polityki bezpieczeństwa sieciowego od polityki bezpieczeństwa Firmy.

Agenda

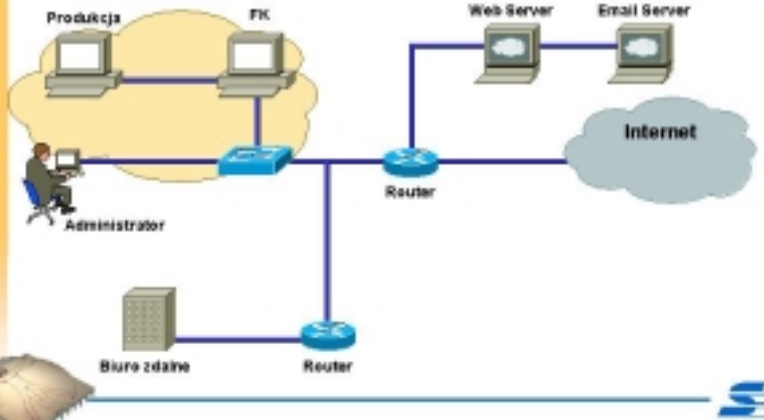
- **Aspekty biznesowe**
- **Aspekty techniczne**
- **Firewall - co to takiego ?**
  - Elementy składowe struktury ochrony styku
  - Modelowe rozwiązania

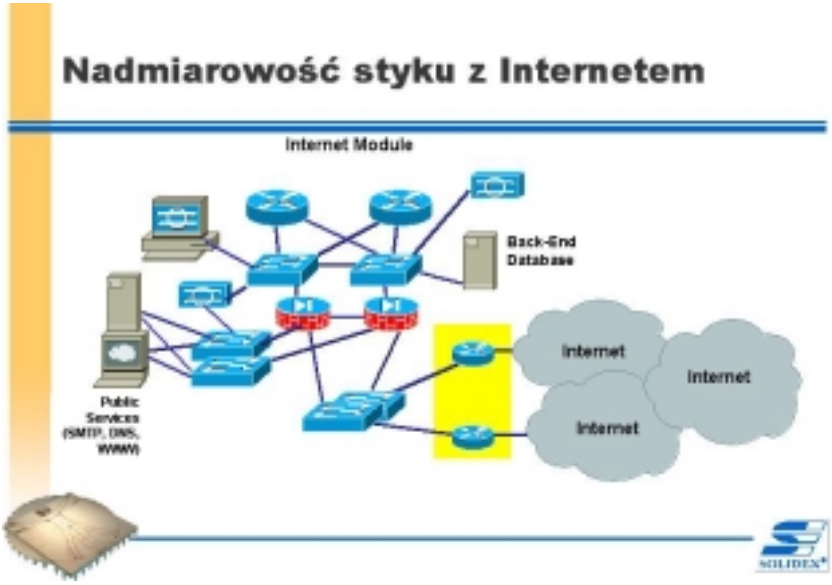
Wymagania stawiane systemowi ochrony styku

Model sieci korporacyjnej

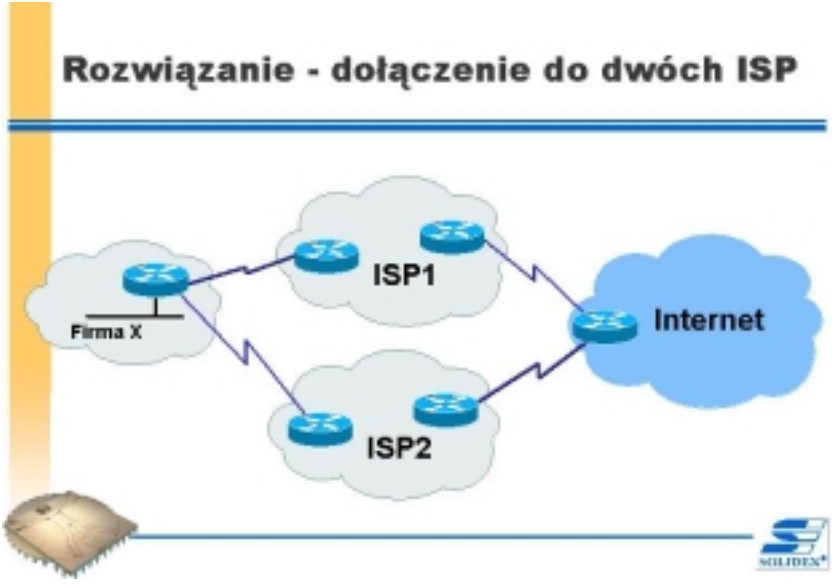


Styk z internetem




Nadmiarowość styku z Internetem
Internet Module
Back-End Database
Public Services (SMTP, DNS, WWW)
Internet
Internet
Internet


Pojedyncze dołączenie "firmy X" do sieci Internet
Internet
ISP
Firma X
"Punkty krytyczne" łączności przy pojedynczym dołączeniu sieci "firmy X" do sieci Internet:
bezpośrednie dołączenie do ISP
połączenie ISP z siecią Internet


Rozwiązanie - dołączenie do dwóch ISP
ISP1
ISP2
Internet
Firma X

Definicja „niezawodnego styku do sieci Internet"

Przez „niezawodny styk do sieci Internet" rozumiemy tutaj taką konfigurację sprzętową i programową sieci IP, która zapewni łączność do i z sieci Internet w przypadku:

- awarii bezpośredniego dołączenia danego przedsiębiorstwa do wybranego przezeń operatora internetowego (ISP)
- awarii dołączenia tego operatora internetowego (ISP) do ogólnoświatowej sieci Internet

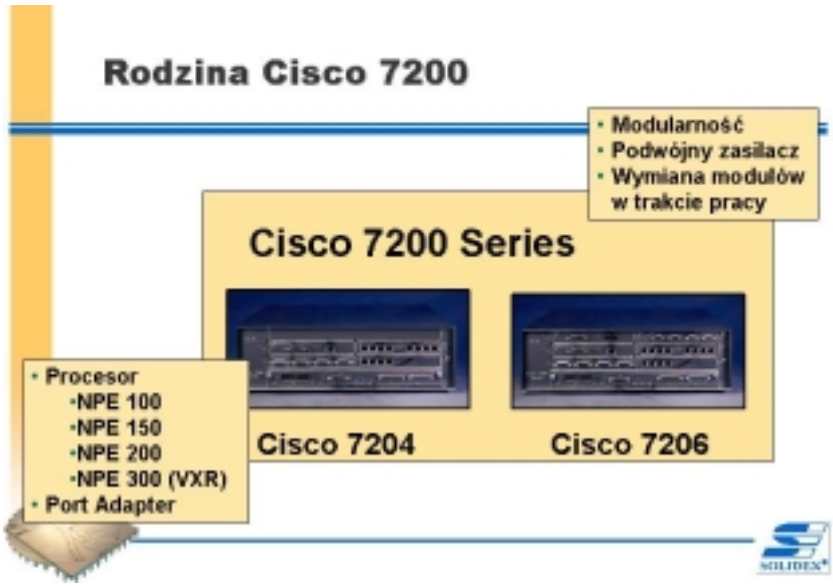
BGP - wymiana routingu z ISP

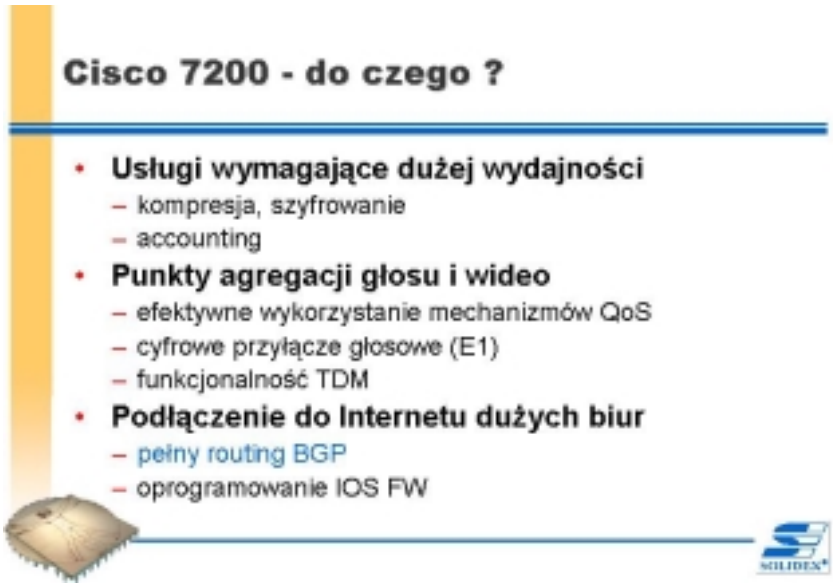
Routing BGP od ISP - trzy przypadki:

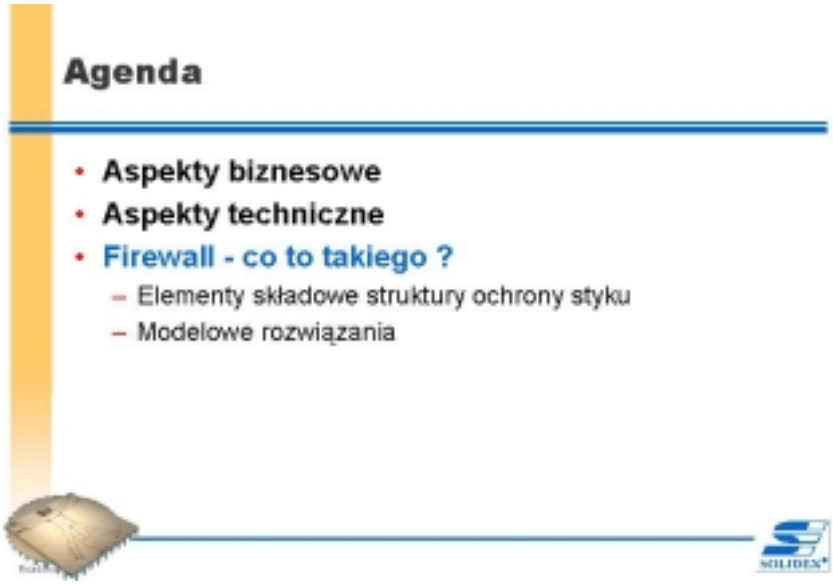
- Od obu ISP wyłącznie routing domyślny (default route)
  - statycznie na wybraną „stabilną sieć"
  - dynamicznie via BGP
- Od obu ISP routing domyślny oraz pewna cześć routingu Internetu
- Pełny routing Internetu od obu ISP

BGP - zalety

- W pełni automatyczna zmiana routingu w razie awarii łącza bezpośredniego lub łączy ISP do sieci Internet
- Możliwość kształtowania własnej polityki routingu do Internetu


Rodzina Cisco 7200
Modularność
Podwójny zasilacz
Wymiana modułów w trakcie pracy
Cisco 7200 Series
Procesor
NPE 100
NPE 150
NPE 200
NPE 300 (VXR)
Port Adapter
Cisco 7204
Cisco 7206


Cisco 7200 - do czego ?
Usługi wymagające dużej wydajności
kompresja, szyfrowanie
accounting
Punkty agregacji głosu i wideo
efektywne wykorzystanie mechanizmów QoS
cyfrowe przyłącze głosowe (E1)
funkcjonalność TDM
Podłączenie do Internetu dużych biur
pełny routing BGP
oprogramowanie IOS FW


Agenda
Aspekty biznesowe
Aspekty techniczne
Firewall - co to takiego ?
Elementy składowe struktury ochrony styku
Modelowe rozwiązania

Definicja zapory ogniowej

Zapora ogniowa „Firewall" to urządzenie przeznaczone do ochrony sieci przed intruzami. Zaporą ogniową może być specjalnie skonfigurowany komputer, router lub dedykowane urządzenie.

Potencjalne cele ataków

- Zablokowanie zasobów sieciowych - ataki DoS
- Przechwycenie strategicznych danych
- Przejęcie sesji
- Penetracja sieci
- Zniszczenie zasobów sieciowych

Sposoby przeprowadzania ataków

- TCP hijacking, TCP SYN
- land, teardrop
- ping śmierci, SMURF
- spam, itp.
- spoofing
- sniffing
- wirusy

Mechanizm filtrowania w Cisco IOS

- Klasyczne filtry (access lists)
  - Standardowe - tylko adresy IP
  - Złożone - adresy IP oraz porty TCP/UDP
- Filtry typu „reflexive"
- Mechanizm „TCP intercept"
- Mechanizm „Lock and key"

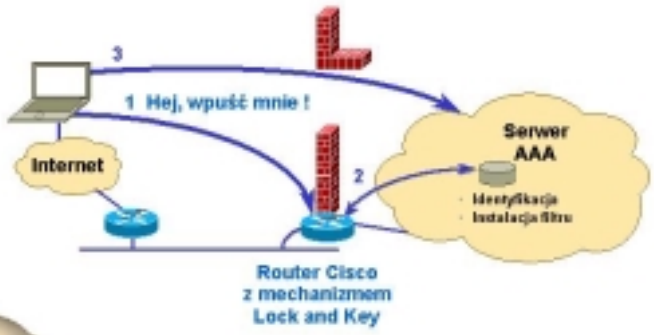
Filtry typu „reflexive"

- Stan filtru typu „reflexive" uzależniony jest od stanu ruchu przechodzącego przez urządzenie
- Alternatywa do parametru „established" w zwykłych filtrach
- Filtr typu „reflexive" jest zamknięty dopóki nie zostanie aktywowany przez dozwolony w nim typ ruchu
- Dostępne w Cisco IOS od wersji 11.3

Mechanizm „TCP Intercept" chroni przed atakiem typu „TCP SYN flooding"

- Atak „TCP SYN flooding" może całkowicie pozbawić serwer zasobów pamięci lub CPU, uniemożliwiając jego pracę
- Mechanizm „TCP Intercept" chroni sieć przed tego typu atakiem poprzez odnotowanie żądania otwarcia sesji TCP (A1) i jego przepuszczenie (A2) lub wydanie odpowiedzi negatywnej w przypadku wykrycia próby ataku „TCP SYN flooding"
- Może również zostać skonfigurowany w trybie pasywnego monitorowania (B) procesu zestawiania sesji TCP, gdzie odpowiada negatywnie jeśli sesja nie zostanie zestawiona w trakcie określonego czasu

Mechanizm "Lock-and-Key"



Cisco IOS Firewall

Rozszerzone mechanizmy zabezpieczeń dla sieci zbudowanych na routerach Cisco

- Context-Based Access Control (CBAC)
  - Operacja typu „stateful" na poziomie aplikacji
  - Obsługa złożonych protokołów (H.323, SQLnet, RealAudio, etc.)
- Wykrywanie i unieszkodliwianie ataków typu „Denial of Service"
- Kontrolowane ładowanie apletów Java
- Alarmy w czasie rzeczywistym
- Logi z transakcji TCP/UDP
- IOS = łatwa konfiguracja i zarządzanie

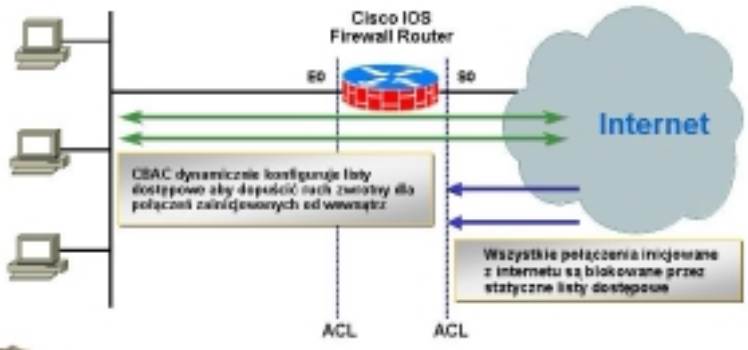
Co to jest „Context-Based Access Control" (CBAC)?

- Śledzenie stanu i kontekstu połączeń w sieci aby zapewnić bezpieczny przepływ informacji
- Dopuszczanie do otwierania połączeń (sesji) poprzez tymczasowe rekonfiguracje filtrów na podstawie informacji pobranych z danych przesyłanych przez aplikację
- Przeglądanie danych wchodzących i opuszczających router

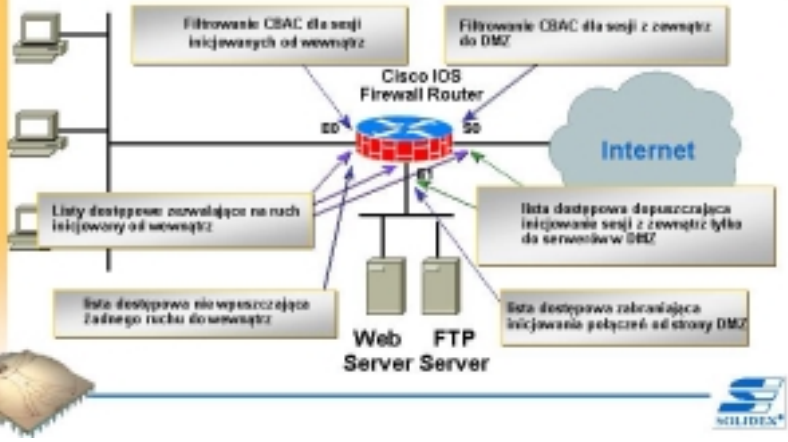
Cisco IOS Context-Based Access Control Obsługiwane aplikacje

- Przejrzystość dla zwykłych usług bazujących na TCP/UDP:
  - WWW, Telnet, SNMP, finger, etc.
- FTP
- TFTP
- SMTP
- BSD R-cmds
- Oracle SQL Net
- Remote Procedure Call (RPC)
- Aplikacje multimedialne
  - VDOnet's VDO Live
  - RealNetworks' RealAudio
  - Intel's InternetVideo Phone (H.323)
  - Microsoft's NetMeeting (H.323)
  - Xing Technologies' StreamWorks
  - Whitepine's CuSeeMe

Jak działa CBAC?



Przykład konfiguracji Cisco IOS Firewall

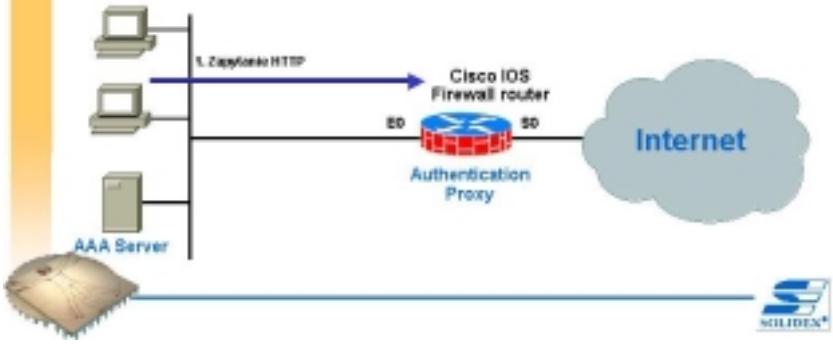


Cisco IOS Firewall Authentication Proxy

- Uwierzytelnienie użytkowników poprzez protokół HTTP (authentication proxy)
- Współpraca z zewnętrznymi serwerami uwierzytelniania (TACACS+, RADIUS)
- Współpracuje z filtrowaniem CBAC i z translacją adresów
- Wspiera hasła jednokrotne (OTP) i inne mechanizmy uwierzytelniania wykorzystujące protokoły TACACS+ i RADIUS

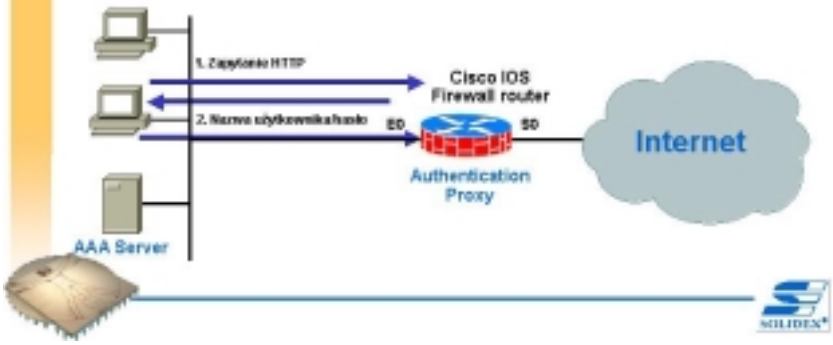
Jak działa authentication proxy?

- Proxy przechwytuje zapytanie HTTP i zapamiętuje docelowy URL



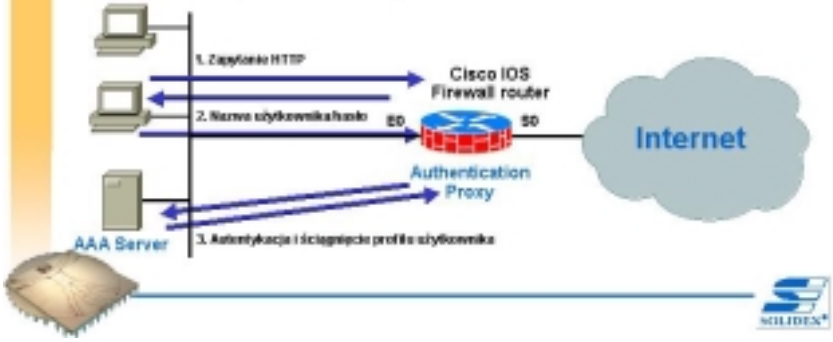
Jak działa authentication proxy?

- Proxy odpowiada użytkownikowi przez HTML: podaj nazwę użytkownika i hasło



Jak działa authentication proxy?

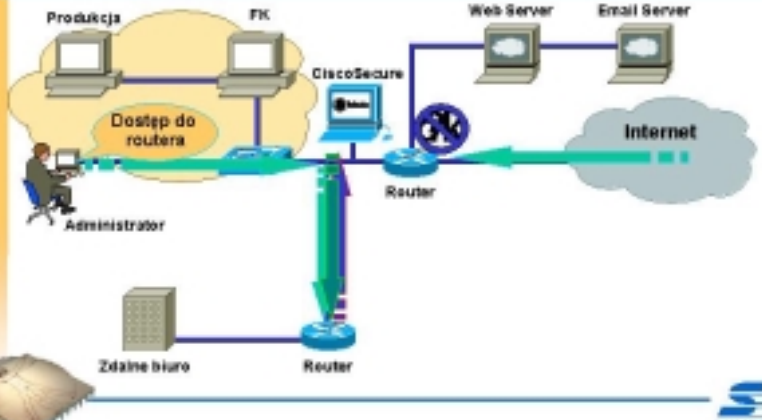
- Proxy uwierzytelnia użytkownika na serwerze AAA: ściągnięcie profilu użytkownika i zdefiniowanie dynamicznych list dostępu



Authentication Cache

- Uwierzytelnienie użytkownika traci ważność po przekroczeniu pewnego okresu nieaktywności - domyślnie jest to 60 minut

AAA



Model AAA

- **Uwierzytelnienie (ang. authentication)**
  - Kim jesteś?
- **Autoryzacja (ang. authorization)**
  - Co możesz zrobić?
- **Rozliczanie (ang. accounting)**
  - Co robiłeś?
  - Czy to co robiłeś jest dopuszczalne?

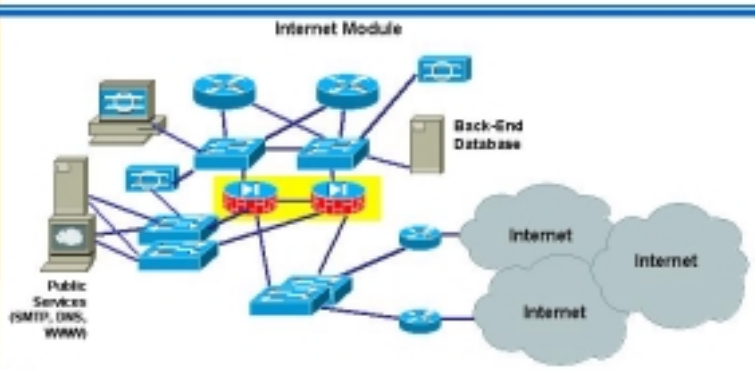
AAA - CiscoSecure

- **Serwer kontroli dostępu (Access Control Server - ACS) realizujący zadania AAA**
- **Autentykacja w oparciu o:**
  - Nazwę użytkownika i hasła z bazy domeny NT
  - Token
  - NDS
- **CiscoSecure NT może również wykorzystywać integralną bazę użytkowników**

Cisco Secure Server

- **CiscoSecure**
  - RADIUS and TACACS+
  - Uprawnienia w oparciu o:
    Time-of-day
    i day-of-week
  - Token server
  - CryptoCard Server

Firewall PIX



Co może zrobić firewall ?

- **Kontrola dostępu oparta na danych o:**
  - Źródle
  - Adresacie
  - Usłudze
  - Czasie, dacie, dniu tygodnia
  - Użytkowniku
- **Logowanie i notyfikacja zdarzeń**

Co może zrobić firewall ?

- **Uwierzytelnianie w oparciu o hasła wielokrotnego i jednokrotnego użytku z wykorzystaniem technologii:**
  - CiscoSecure
  - SecurID
  - CryptoCard
  - RADIUS, TACACS+, etc.

Co może zrobić firewall ?

- **Być platformą dla innych usług bezpieczeństwa takich jak:**
  - VPN (Virtual Private Networking)
  - Java, activeX blokowanie/skanowanie (Finjan)
  - URL blokowanie (Websense)
  - Wirusy - skanowanie (Trend Micro VirusWall)
  - Etc.

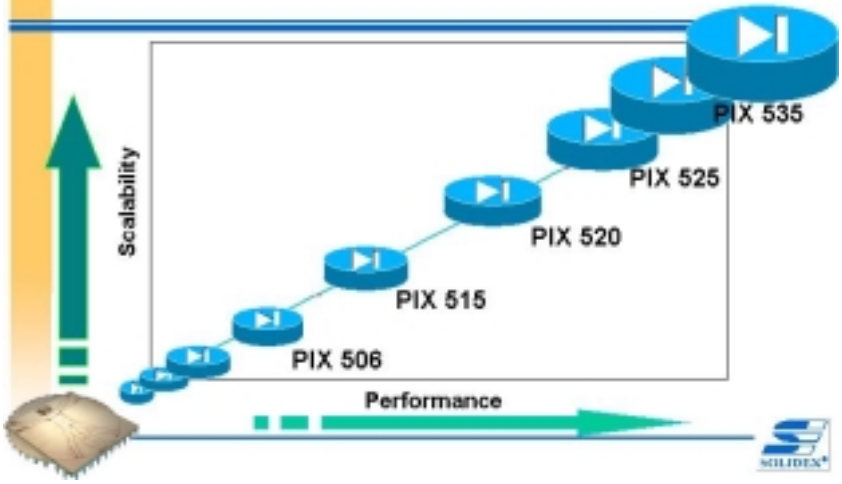
Cisco Firewall

- **PIX firewall**
  - Dedykowane urządzenie
  - Wsparcie aplikacji
  - Duża wydajność
  - Skalowalność
- **Cisco IOS firewall**
  - Opcja oprogramowania IOS
  - Wsparcie aplikacji
  - Cisco 800/1600/1700/2500/2600/3600/7200

PIX Firewall

- **Dedykowane urządzenia**
  - Specjalizowany OS, brak twardego dysku
- **Rozwiązania**
  - Adaptive Security Algorithm (ASA)
  - Cut-through proxy
- **Wydajność**
  - Do 256,000 jednoczesnych sesji
  - Do 370 Mbps przepustowości
  - Do 6500 połączeń na sekundę

Rodzina PIX Firewall



PIX 506 (ROBO)

- MSRP: $1,950
- Obsługa bardzo małych oddziałów firm
- „Prawdziwy" firewall w miejsce małego routera z dwoma interfejsami LAN (wymaga podstawowego urządzenia routującego)
- przepustowość 10Mbps

PIX 506 — Specyfikacja

- 200 MHz Intel Pentium MMX
- 32 MB RAM
- 8 MB Flash
- 2 zintegrowane porty 10Mbps
- Zewnętrzny zasilacz
- Urządzenie „biurowe" (8 x 12 x 1.7")

PIX 506 — restrykcje

- 4 peery VPN
- Zablokowane cut-through proxy
- Zablokowany mail guard
- Brak failover
- Zablokowane wsparcie dla serwerów AAA/Radius

PIX 506 — Wydajność

- 10 Mbps przepustowości
- 4 Mbps 3DES
- 4 peer'y VPN

PIX 515 (SMB)

- PIX 515-R ($5,000)
  - Ograniczenia: Brak failover, 64,000 połączeń,
  - 2 interfejsy Ethernet
- PIX 515-UR ($12,000)
  - 125,000 połączeń
  - do 6 interfejsów Ethernet
- Duża wydajność
  - do 170 Mbps przepustowości
  - do 6,500 połączeń na sekundę

PIX 520 (Enterprise)

- Licencje na użytkowników ($9,000-19,000)
- Do sześciu portów Ethernet 10/100, czterech TR lub dwóch FDDI
- 128MB RAM - 250,000 jednoczesnych połączeń
- Przepustowość 370 Mbps
- Przygotowane dla środowisk o dużych szybkościach pracy

Płyta:	Intel SE440BX-2
Procesor:	350MHz Pentium II
Pamięć:	128MB
Porty LAN:	Konfigurowalne
Flash:	16 MB

PIX 525 — Specyfikacja

- 600 MHz Pentium III
- 128-256 MB RAM
- 16 MB flash
- Dwa zintegrowane 10/100 FE
- 3 sloty PCI

PIX 525 — Licencje

- Restricted License - $16,000
  - 128 MB RAM - 250,000 równoczesnych połączeń
  - Do 6 interfejsów Ethernet
  - Brak Failover
- UnRestricted License - $22,000
  - 256 MB RAM - 500,000 równoczesnych połączeń
  - Do 8 interfejsów Ethernet
- Failover License - $5,000

PIX 525 — Wydajność

- 400 Mbps (2 porty Gigabit) przepustowości
- 6,500 nowych połączeń na sekundę
- 30 Mbps 3DES (software)

PIX 535

- Duże sieci „Enterprise":
  - agregacja VPN,
  - główne węzły w sieciach operatorskich
- Bardzo duża wydajność

PIX 535 — Specyfikacja

- Procesor(y) 800 MHz Pentium III
- 512MB-1GB RAM
- 7 slotów PCI
  - 4-64 bit/66 MHz
  - 3- 32 bit/33 MHz
- AC, Dual AC, DC, Dual DC

PIX 535 — Licencje

- **Restricted license - $60,000**
  - 8 interfejsów Ethernet
  - 512 MB RAM
- **Unrestricted license - $75,000**
  - 8 interfejsów Ethernet
  - 1GB RAM
- **Failover license - $20,000**

PIX Gigabit Ethernet Card

- Wykorzystywana do bezpiecznego odseparowania szybkich segmentów LAN
- $3,000
- Przepustowość 370 megabitów/sekundę (full duplex)
- Światłowód wielomodowy (62.5-50um), konektor SC.
- Wsparcie dla standardów LX i SX

Podsumowanie

- Produkty z rodziny „firewall" Firmy Cisco opierają swoje działanie na filtracji pakietów
- Pozwalają na efektywną filtrację pakietów z uwzględnieniem stanu połączenia
- Szeroki asortyment pozwala na dopasowanie sprzętu do potrzeb użytkownika
- Mogą wykorzystywać zewnętrzne serwery uwierzytelniające
- Integrują się z innymi produktami Cisco
- Umożliwiają bezpieczną komunikację przez Internet za pomocą mechanizmu VPN
- Oferują możliwość integracji z serwerami filtrującymi zawartość przesyłanych informacji
- Dobre wsparcie techniczne

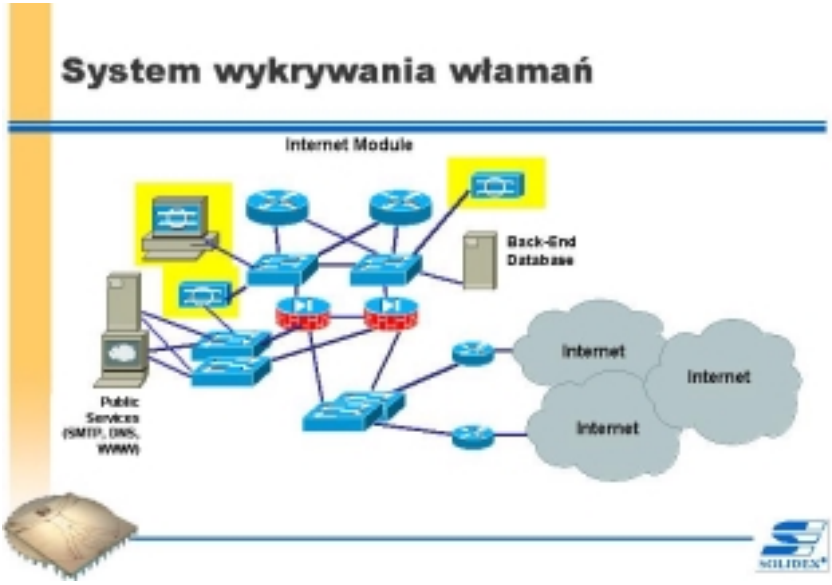
Typowe zalecenia polityki bezpieczeństwa

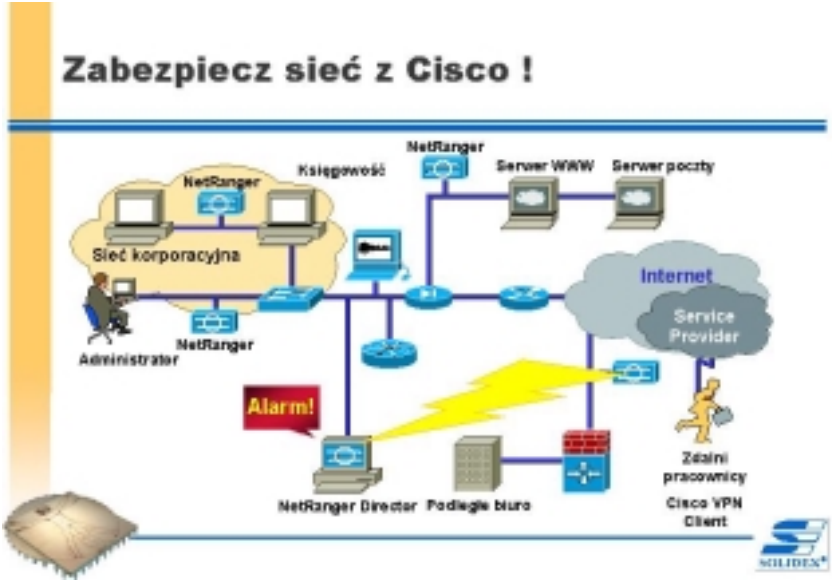
- Witalne zasoby Firmy powinny być chronione przez co najmniej dwa poziomy zapór ogniowych
- Zapory ogniowe powinny pochodzić od różnych producentów
- Często wymagania filtracji ruchu dotyczą konkretnych aplikacji

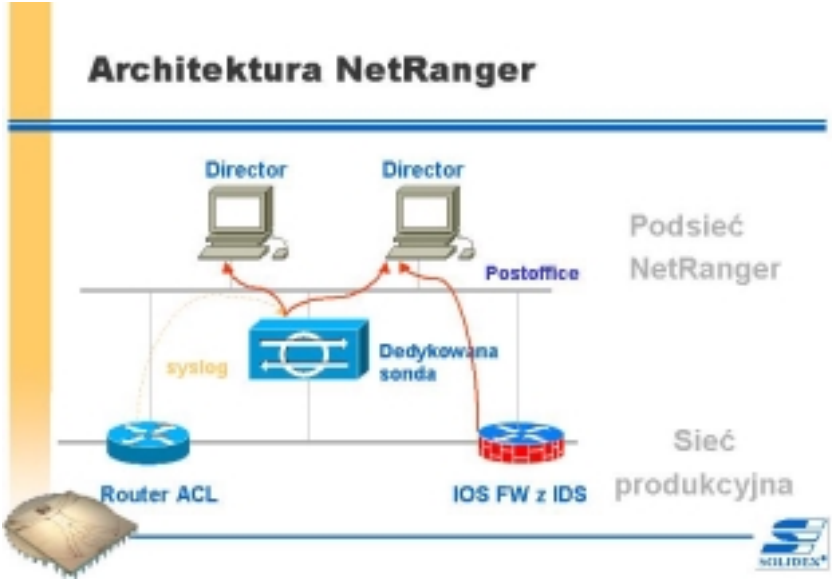
CheckPoint Firewall-1

- Zapora ogniowa oparta na patentowanej metodzie „inspekcji stanowej" pakietów
- Mechanizmy precyzyjnej filtracji pakietów
- Rozwiązanie typu programowego
- Wspiera popularne platformy takie jak SUN SOLARIS czy MS Windows NT
- Wspiera standard OPSEC
- Możliwość współpracy z serwerami filtrującymi URL i zawartość (CVP)
- Wsparcie dla VPN
- Znaczny udział w rynku zabezpieczeń
- Partner SOLIDEX

Systemy Wykrywania Włamań Intrusion Detection System


System wykrywania włamań
Internet Module
Back-End Database
Internet
Internet
Internet
Public Services (SMTP, DNS, WWW)


Zabezpiecz sieć z Cisco !
NetRanger
Księgowość
NetRanger
Server WWW
Serwer poczty
Sieć korporacyjna
Internet
Service Provider
NetRanger
Administrator
Alarm!
Zdalni pracownicy
NetRanger Director
Podległe biuro
Cisco VPN Client


Architektura NetRanger
Director
Director
Podsieć NetRanger
Postoffice
Dedykowana sonda
syslog
Router ACL
IOS FW z IDS
Sieć produkcyjna

Architektura NetRanger

- **Sensor (zawiera IOS FW w/ IDS)**
  - Analiza pakietów
  - Generowanie alarmów
  - Odpowiedzi/zapobieganie następstwom
- **Director**
  - Prezentacja alarmów w czasie rzeczywistym

Sensor

- **Jeden lub dwa procesory Pentium III 600MHz**
- **4 GB HDD**
- **Solaris x86 2.6**
- **Dwa interfejsy LAN**
  - Command & Control - 10/100BaseT
  - Sniffing/Monitoring - Ethernet, Fast Ethernet, Token Ring i FDDI

Sensor (c.d.)

- **300+ sygnatur ataków**
  - co m-c uaktualnienie sygnatur z CCO
- **Możliwa reakcja**
  - TCP Reset
  - Shun

IOS Firewall z IDS

- Wersja IOS 12.0(5)T na platformy routerów 2600, 3600, 7100, 7200
- Połączenie funkcji FW i IDS
- 59 sygnatur
- konfiguracja przez CLI
- wsparcie Postoffice & Syslog
- Akcje: TCP Reset i usuwanie pakietów

Sniffing Interface dedykowanej sondy

- Działa w trybie Promiscuous
- Nie wpływa na ruch sieciowy
  - Sonda nie jest urządzeniem pass-thru
- Ograniczone do interfejsów sieci LAN
- Reakcje TCP Reset wysyłane są przez Sniffing Interface

Podłączenie Sniffing Interface

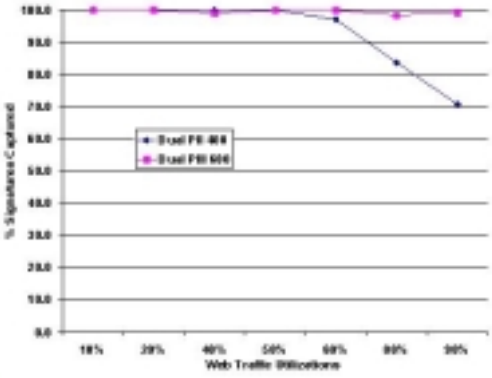
- Przyłączenie do współdzielonych mediów (hub) lub do portów SPAN przełączników
- Żelazna zasada: Jeżeli ruch który ma podlegać monitoringowi nie będzie widziany przez sondę to nie będzie ona działać!
  - `sensor# snoop -d spwr0`

Cisco Secure IDS - sondy

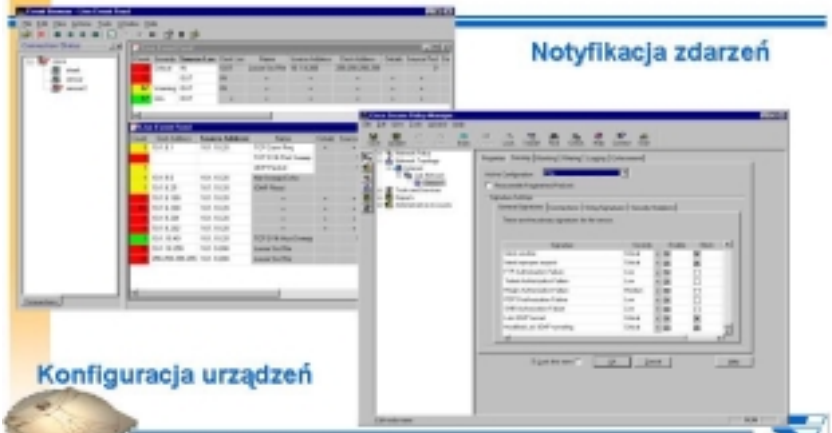
	Sondy IDS		
	4210	4220	4230
Wydajność (Mbps)	45	60	100
Procesor (MHz)	PIII 600	PIII 600	Dual PIII 600
Pamięć (MB)	256	256	512
Cena ($US)	8 000	12,500 (-E)	19,000 (-FE)
Dostepnosc	Juz	Juz	Juz

Source: Frost & Sullivan, 2000

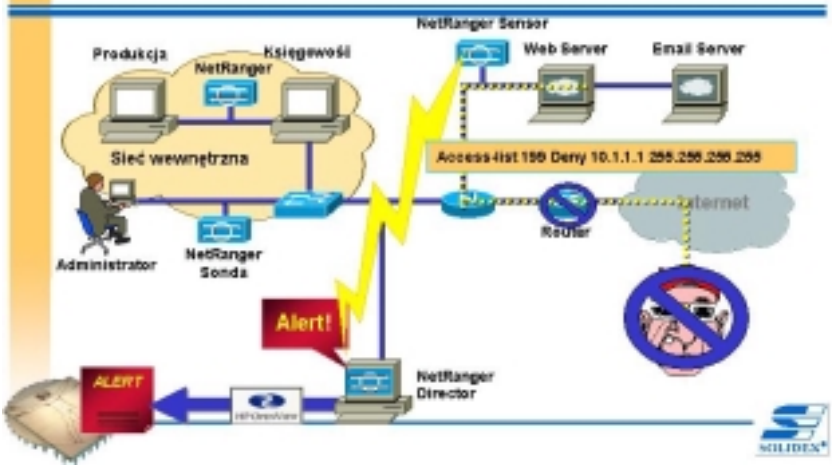
Testy wydajności z ruchem WWW



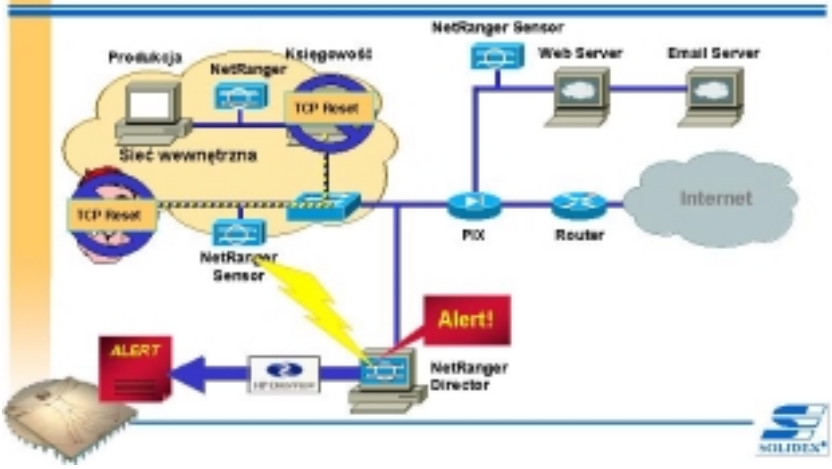
CSPM 2.3 (3.0) "- nowy Director



System Wykrywania Włamań c.d.

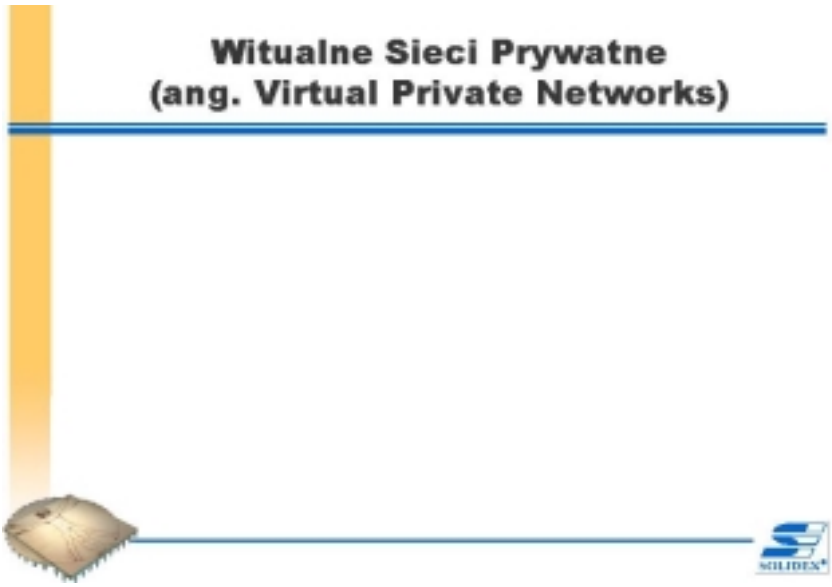


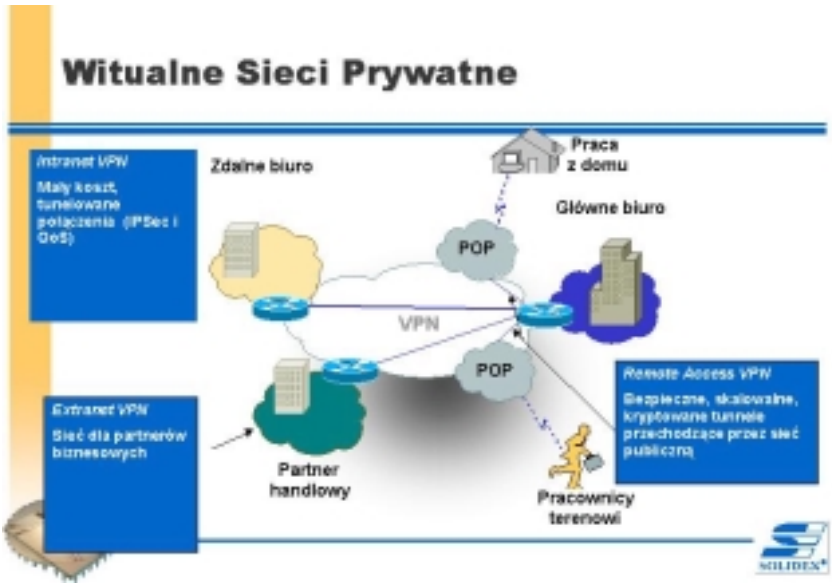
Atak od wewnątrz

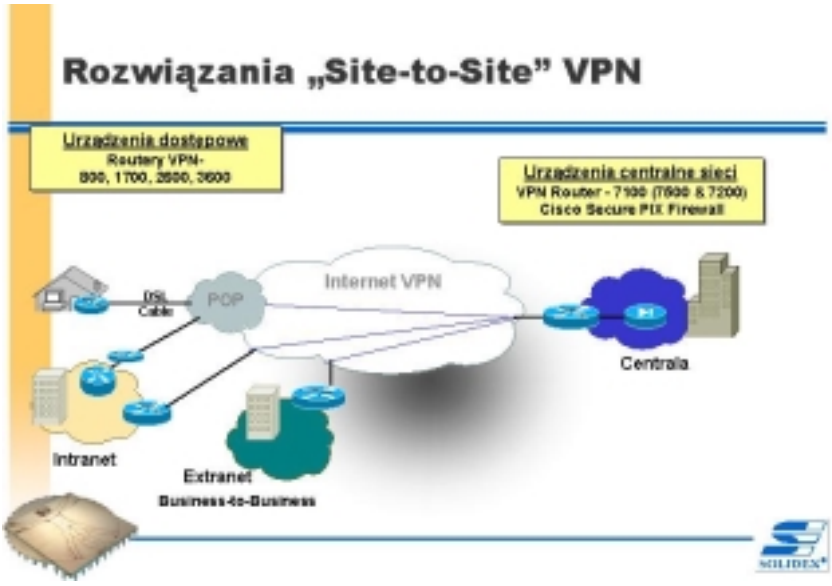


CheckPoint RealSecure

- Rozwiązania IDS Cisco współpracują z routerami Cisco utwardzając ich politykę bezpieczeństwa – nie współpracują z innymi urządzeniami
- Sondy IDS RealSecure integrują się z zaporą ogniową CP
- Rozwiązanie programowe na platformę MS Win NT
- Dobre wsparcie producenta


Witualne Sieci Prywatne
(ang. Virtual Private Networks)

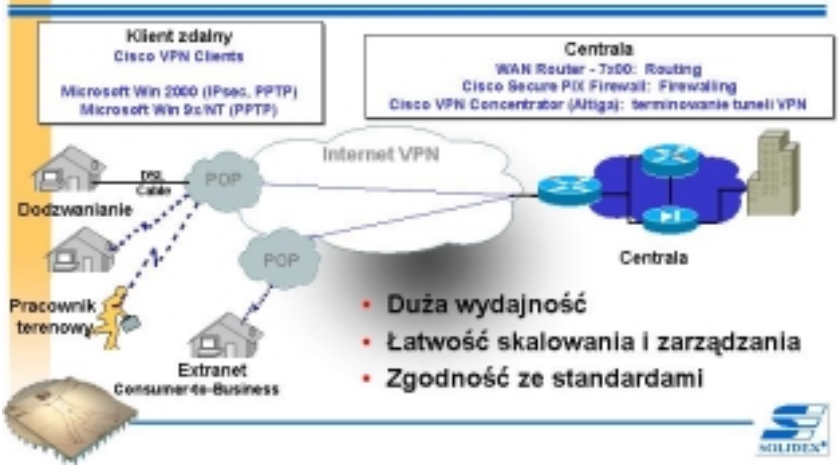

Witualne Sieci Prywatne
Intranet VPN
Mały koszt, tunelowane połączenia (IPSec i GeS)
Zdalne biuro
Praca z domu
Główne biuro
POP
VPN
POP
Remote Access VPN
Bezpieczne, skalowalne, kryptowane tunele przechodzące przez sieć publiczną
Extranet VPN
Sieć dla partnerów biznesowych
Partner handlowy
Pracownicy terenowi


Rozwiązania „Site-to-Site” VPN
Urządzenia dostępowe
Routery VPN-
800, 1700, 2600, 3600
Urządzenia centralne sieci
VPN Router - 7100 (7500 & 7200)
Cisco Secure PIX Firewall
Internet VPN
POP
Centrala
Intranet
Extranet
Business-to-Business

Wymagania sieci zdalnego dostępu Virtual Private Networks

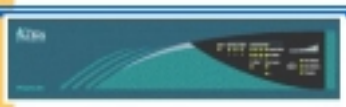
- Niepodważalne bezpieczeństwo
- Prosty, łatwy w użyciu klient VPN
- Skalowalność
- Stabilność/redundancja
- Zintegrowane zarządzanie
- Łatwość wdrożenia
- Zgodność ze standardami

Rozwiązania Remote Access VPN



- Duża wydajność
- Łatwość skalowania i zarządzania
- Zgodność ze standardami

Koncentrator Cisco VPN 3000 (Altiga)



- Duża wydajność
- Szyfracja
- Redundantne, moduły SEP hot swap z SEP failover
- Chassis failover
- Redundantne zasilacze

Scalable Encryption Processor (SEP)

Cisco VPN 3005

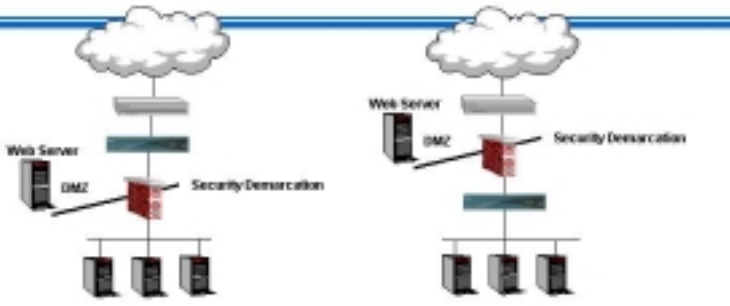
- Idealny dla małych biur, zdalnych lokalizacji dużych firm
- Do 100 jednoczesnych sesji, Ethernet,
- Oprogramowanie analogiczne do stosowanego w urządzeniach Cisco VPN 3015/30/60
- VPN Device Manager (VDM) dla serii Cisco VPN 3000 Concentrator

Cisco VPN 3000

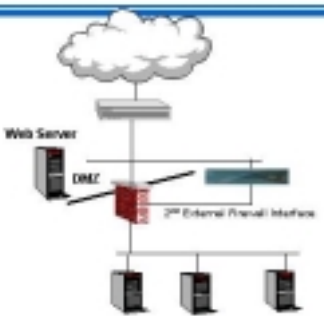
Network Computing
EDITOR'S CHOICE

	3005	3015	3030	3060	3080
Ilość użytkowników	100	100	1500	5000	10 000
Szyfrowanie	SW	SW	HW	HW	HW
WAN	Tak	Tak	Tak	Tak	Tak
Wydajność	4 Mb/s	4 Mb/s	50 Mb/s	100 Mb/s	100 Mb/s
Pamięć	32 MB	64 MB	128 MB	256 MB	256 MB
SEP	0	0	1	2	4
Skalowalność	Nie	Tak	Tak	Tak	N/A
Obsługa 2 zasilaczy	Nie	Tak	Tak	Tak	Tak
Redundancja	Nie	Tak	Tak	Tak	Tak

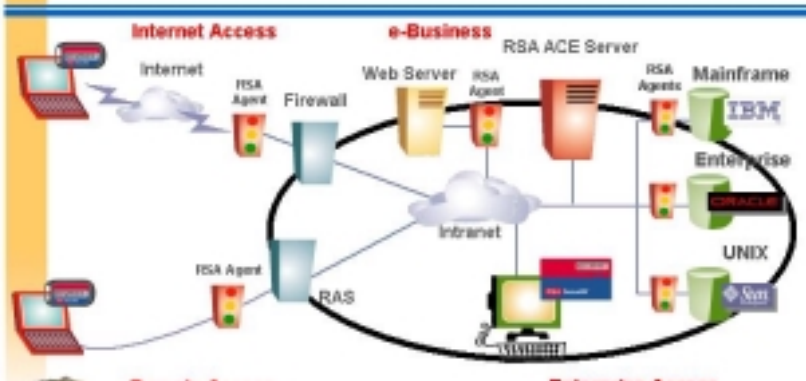
Gdzie umieścić VPN koncentrator?



Gdzie umieścić VPN koncentrator ?



Silna autentykacja użytkowników



Produkty RSA Inc.

Uwaga!!

Podane przykłady
miały na celu zapoznanie Państwa
z problematyką bezpieczeństwa.

Kopiowanie rozwiązań standardowych
bez ich indywidualnego dopasowania do potrzeb
otwiera drogę potencjalnym intruzom!

Podsumowanie

- Poruszone zagadnienia stanowią tylko niewielki fragment całości problematyki budowy bezpiecznego styku z Internetem
- Rozwiązania styku z Internetem muszą integrować produkty pochodzące od różnych producentów aby zapewnić właściwy poziom bezpieczeństwa
- Przez indywidualne podejście do potrzeb Klienta możemy zapewnić wyższy poziom bezpieczeństwa implementowanych rozwiązań
- SOLIDEX spełnia rolę SOLIDnego integratora technologii sieciowych

Podziękowanie

Do przygotowania niniejszej prezentacji wykorzystano
materiały Firm partnerskich Cisco, CheckPoint oraz
RSA Inc.


Dziękuję za uwagę
Pytania?