THIS IS THE POWER OF THE NETWORK. NOW.

Fundamentals of Network Security (FNS)

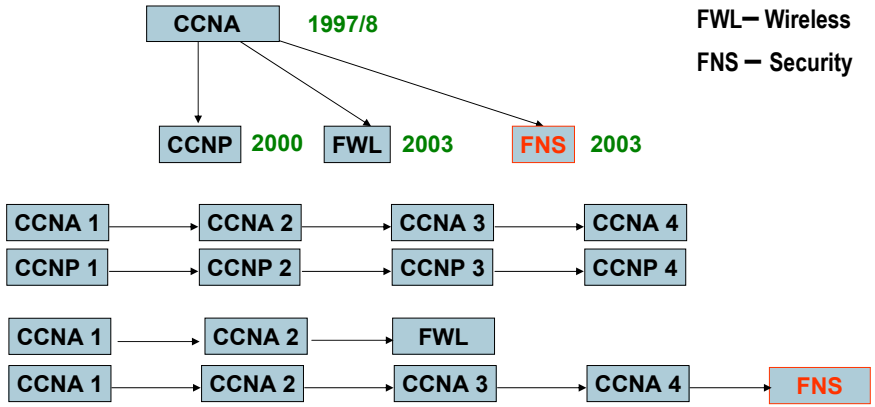
prezentacja programu

Krzysztof Szczypiorski
Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych
ITU Internet Training Centre
at Warsaw University of Technology
`http://itu-itc.elka.pw.edu.pl`

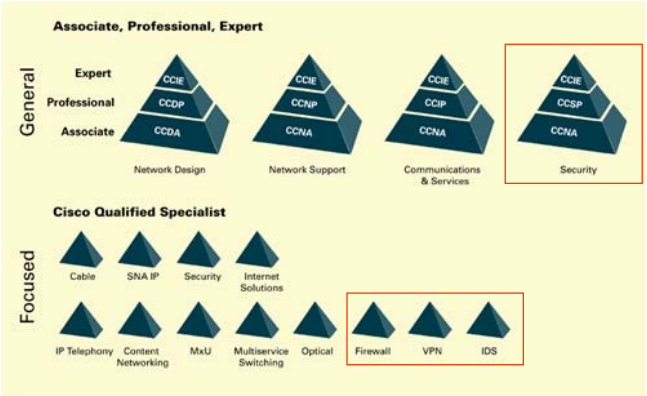
Plan prezentacji

- FNS w CNAP
- FNS a ścieżki certyfikacyjne
- Zakres FNS
- Zestaw laboratoryjny
- Implementacja na PW
- Konfiguracje laboratoryjne
- Zwartość modułów
- Najbliższa przyszłość programu

FNS a inne kursy sieciowe w CNAP



Ścieżka CCSP cz. 1/2



Ścieżka CCSP cz. 2/2

- ważny certyfikat CCNA lub CCIP

• 642-501 SECUR	Securing Cisco IOS Networks	FNS
• 642-521 CSPFA	Cisco Secure PIX Firewall Advanced	
• 642-531 CSIDS	Cisco Secure Intrusion Detection System	
• 642-511 CSVPN	Cisco Secure VPN	
• 642-541 CSI	Cisco SAFE Implementation	

Kwiecień 2003 – Information Systems Security (INFOSEC) Professional National Security Agency (NSA) i Committee on National Security Systems (CNSS) (cztery egzaminy – bez CSI)
`http://newsroom.cisco.com/dlls/prod_070103b.html`

Zakres programu FNS

- Tworzenie i zarządzanie polityką bezpieczeństwa w szczególności na poziomie urządzeń sieciowych
- Metody ochrony informacji, produkty i oprogramowanie
- Ściana przeciwogniowa i bezpieczny router – wybór urządzenia, instalacja, konfiguracja i utrzymanie
- Implementacja AAA na routerach i ścianach przeciwogniowych
- Implementacja VPN na routerach i ścianach przeciwogniowych

Główne cechy programu FNS

- jeden semestr – nominalnie 70 godzin zajęć
- 15 (!) modułów
  - **moduły 1-7:** SECUR (Securing Cisco IOS Networks)
  - **moduły: 8-15:** CSPFA (Cisco Secure PIX Firewall Advanced)
- Zestawy laboratoryjne
  - **opcja 1:** samodzielny zestaw, niezależny od zestawów CCNA/CCNP
  - **opcja 2:** dwa PIXy + możliwość wykorzystania trzech routerów i switcha (lub dwóch routerów i switcha L3) z zestawów CCNA/CCNP
- W przypadku opcji 1 zyskujemy jedno stanowisko laboratoryjne dla CCNA

Zestaw laboratoryjny FNS 1.1 - STANDARD BUNDLE v 1.3

CISCO2611XM-ADSL - 1 szt.	2611XM ADSL Bundle, WIC-1ADSL, 2FE, IP Plus, 32FLASH, 128MB DRAM
C2611XM-2FE/VPN/K9 – 2 szt.	Cisco 2611XM VPN Bundle, AIM-VPN-EP/2FE/IOS FW/IPSec 3DES, 32MB Flash, 128MB DRAM
PIX-515E-R-DMZ-BUN – 2 szt.	PIX-515E-DMZ Bundle (Chassis, Restricted SW, 3 FE ports) SF-PIX-6.3; PIX-515-VPN-3DES
WS-C2950T-24 - 1 szt.	24 10/100 ports w/ 2 10/100/1000BASE-T ports, Enhanced Image

FNS 1.1 - PIX POD Version 1.3

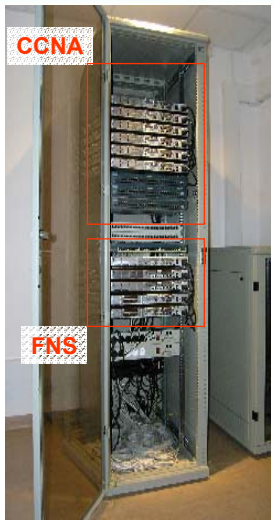
W co należy jeszcze się wyposażyć?

- Oprogramowanie
  - SuperServer wymaga Windows 2000 Server z SP3
  - Dla każdego Student Pod PC zalecany jest Windows 2000 Server z SP3 (do Standard Bundle potrzebne są 2 Student Pod PC)
  - Cisco Secure ACS v3.2 lub nowszy (aktualny 3.3)
  - Serwer Syslog (np. *Kiwi*)
  - Klient SSH (np. *Putty)*
  - Serwer TFTP (np. *SolarWinds TFTP, Cisco TFTP Server*)
  - Aplikacja SNMP (np. *SNMP Trap watcher*)
- Karta sieciowa (1 szt.) ze wsparciem dla VLAN (802.1q)
  - **PILA8470C3 Intel PRO/100 Server Adapter**
  - LNE100M Linksys Managed Network Adapter

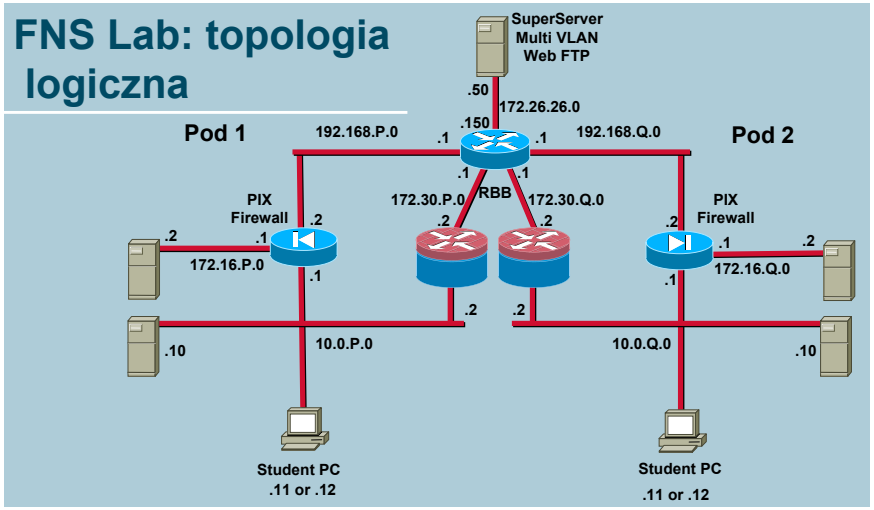
Implementacja laboratorium na PW cz.1/2

- 15 stanowisk dla studentów + 1 dla wykładowcy
- 3 logiczne sieci UTP 5e
- każda maszyna wyposażona w dwie karty sieciowe FE i port szeregowy
- multisystemowe

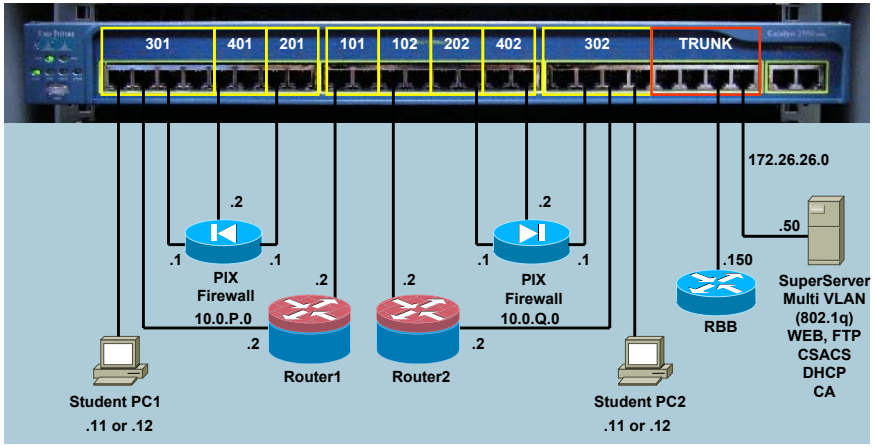
Implementacja… cz. 2/2



FNS Lab: topologia logiczna



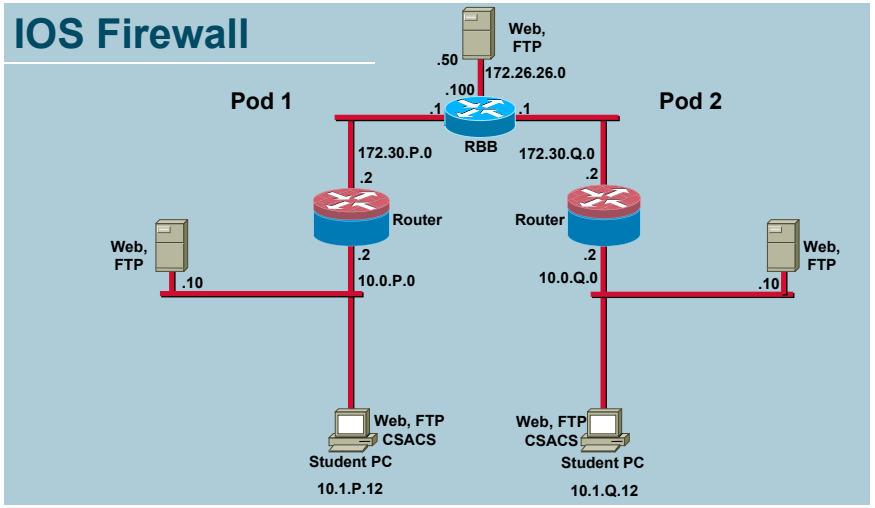
FNS lab: topologia fizyczna



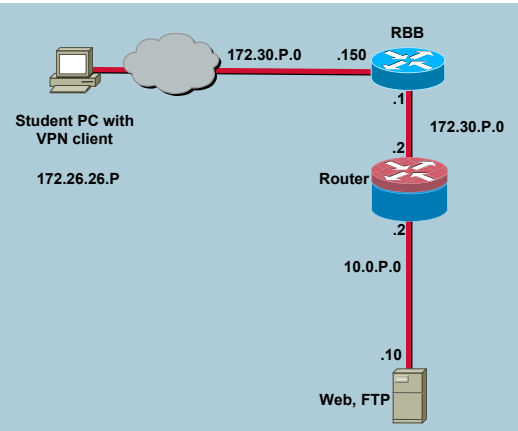
Moduły 1-7: SECUR

- Securing Cisco IOS Networks
- nominalnie ok. 8h30” zajęć laboratoryjnych
- zwiększenie komfortu pracy – co najmniej jeden dodatkowy bezpieczny router (+ wykorzystanie dodatkowego switcha)

IOS Firewall



Client-to-IOS Firewall



Moduł 1

- **Module 1: Overview of Network Security**
  - **1.1** Overview of Network Security
  - **1.2** Vulnerabilities and Threats
  - **1.3** Security Framework and Policy
  - **1.4** Security Products and Solutions

Laboratorium (*65 min.*):
1.1.5 Student Lab Orientation
1.2.8 Vulnerabilities and Exploits
1.3.3 Designing a Security Plan

Moduł 2

- **Module 2: Basic Router and Switch Security**
  - **2.1** General Router and Switch Security
  - **2.2** Disable Unneeded Services
  - **2.3** Securing the Perimeter Router
  - **2.4** Router Management
  - **2.5** Securing LAN Access

Laboratorium (*110 min.*):
2.1.6 Configure General Router Security
2.2.1 Controlling TCP/IP Services
2.3.2 Configuring NAT/PAT
2.3.3 Configure Routing Authentication and Filtering
2.4.2 Configure Logging
2.4.3 Setting Time and NTP
2.4.5 Configure SSH

Moduł 3

- **Module 3: Router ACLs and CBAC**
  - **3.1** Access Control Lists
  - **3.2** Types of IP ACLs
  - **3.3** Context-based Access Control (CBAC)
  - **3.4** Configure CBAC (Task 1 and 2)
  - **3.5** Task 3: Port to Application Mapping (PAM)
  - **3.6** Task 4: Define Inspection Rules
  - **3.7** Task 5: Inspection Rules and ACLs Applied to Router Interfaces
  - **3.8** Task 6: Test and Verify CBAC

Laboratorium (*115 min.*):
3.2.4 Standard, Extended, Named and Context ACLs
3.2.5 Lock-and-Key ACLs
3.2.7 Time-Based ACLs
3.8.3 Configure Cisco IOS Firewall CBAC on a Cisco Router

Moduł 4

- **Module 4: Router AAA Security**
  - **4.1** AAA Secure Network Access
  - **4.2** Network Access Server (NAS) AAA Authentication Process
  - **4.3** Cisco Secure ACS
  - **4.4** AAA Servers Overview and Configuration
  - **4.5** The Cisco IOS Firewall Authentication Proxy

Laboratorium (*80 min.*):
4.2.3 Configure AAA on a Cisco Router
4.3.1 Install and Configure CSACS 3.0 for Windows
4.5.2 Configuring Authentication Proxy

Moduł 5

- **Module 5: Router Intrusion Detection, Monitoring, and Management**
  - **5.1** IOS Firewall IDS
  - **5.2** Setting Up the Cisco Firewall IDS
  - **5.3** Monitoring with Logging and Syslog
  - **5.4** SNMP
  - **5.5** Managing the Router
  - **5.6** Security Device Manager (SDM)

Laboratorium (*60 min.*):
5.2.5 Configure IOS Firewall IDS
5.3.8 Configure Syslog
5.4.5 Configure SNMP

Moduł 6

- **Module 6: Router Site-to-Site VPN**
  - **6.1** Virtual Private Networks
  - **6.2** IOS Cryptosystem
  - **6.3** IPSec
  - **6.4** Site-to-Site IPSec VPN Using Pre-shared Keys
  - **6.5** Digital Certificates
  - **6.6** Configure Site-to-Site IPSec VPN Using Digital Certificates

Laboratorium (*60 min.*):
6.4.5 Configuring Cisco IOS IPSec using Pre-Shared Keys
6.6.6 Configure IPSec using Digital Certificates

Moduł 7

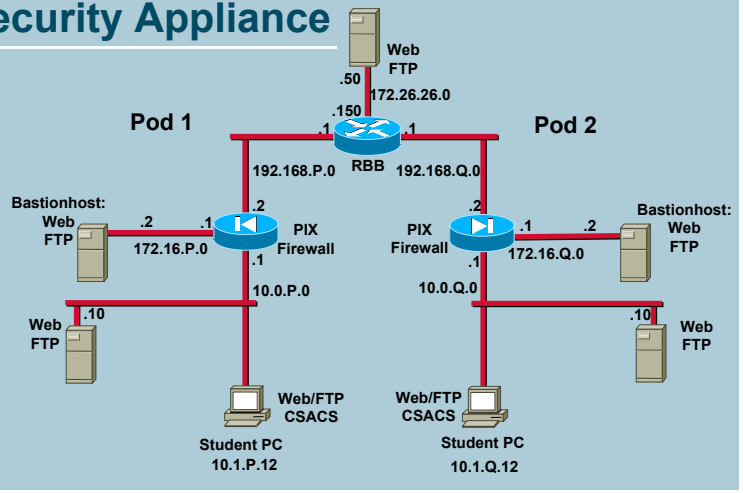
- **Module 7: Router Remote Access VPN**
  - **7.1** Remote Access VPN
  - **7.2** Cisco Easy VPN
  - **7.3** Cisco VPN 3.5 Client
  - **7.4** VPN Enterprise Management

Laboratorium (*20 min.*):
7.3.6 Configure Remote Access Using Cisco Easy VPN

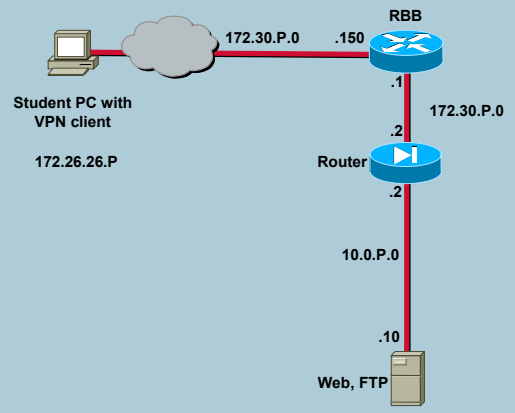
Moduły 8-15: CSPFA

- Cisco Secure PIX Firewall Advanced
- nominalnie ok. 8h30” zajęć laboratoryjnych
- zwiększenie komfortu pracy – co najmniej jeden dodatkowy PIX (+ wykorzystanie dodatkowego switcha)

PIX Security Appliance



Client-to-PIX Security Appliance



Moduł 8

- **Module 8: PIX Firewall**
  - **8.1** Introduction to Firewalls
  - **8.2** The Cisco PIX Security Appliance
  - **8.3** Getting Started
  - **8.4** Routing and Multicast Configuration
  - **8.5** PIX Dynamic Host Configuration Protocol (DHCP)

Laboratorium (*40 min.*):
8.3.3 Configure the PIX Firewall
8.5.3 Configure the PIX Firewall as a DHCP Server

Moduł 9

- **Module 9: PIX Security Appliance Translations and Connections**
  - **9.1** Transport Protocols
  - **9.2** Network Address Translations
  - **9.3** Configuring DNS Support
  - **9.4** Connections
  - **9.5** Port Address Translation (PAT)
  - **9.6** Multiple Interfaces on a PIX Security Appliance

Laboratorium (*65 min.*):
9.5.6 Configure PAT
9.6.3.1 Configure Access Through the PIX Security Appliance
9.6.3.2 Configure Multiple Interfaces

Moduł 10

- **Module 10: PIX Security Appliance ACLs**
  - **10.1** Access Control Lists and the PIX Security Appliance
  - **10.2** Using ACLs
  - **10.3** Filtering
  - **10.4** Object Grouping
  - **10.5** Nested Object Groups

Laboratorium (*75 min.*):
10.1.2 Configure ACLs in the PIX Security Appliance
10.4.4 Configure Object Groups

Moduł 11

- **Module 11: PIX Security Appliance AAA**
  - **11.1** AAA
  - **11.2** Authentication Configuration
  - **11.3** Authorization and Accounting Configuration
  - **11.4** PPPoE and the PIX Security Appliance

Laboratorium (*40 min.*):
11.3.5 Configure AAA on the PIX Security Appliance Using Cisco Secure ACS for Windows 2000

Moduł 12

- **Module 12: PIX Advanced Protocols and Intrusion Detection**
  - **12.1** Advanced Protocols
  - **12.2** Multimedia Support
  - **12.3** Attack Guards
  - **12.4** Intrusion Detection
  - **12.5** Shunning
  - **12.6** Syslog Configuration on the PIX
  - **12.7** SNMP

Laboratorium (*50 min.*):
12.1.7 Configure and Test Advanced Protocol Handling on the Cisco PIX Security Appliance
12.4.3 Configure Intrusion Detection

Moduł 13

- **Module 13: PIX Failover and System Maintenance**
  - **13.1** Understanding Failover
  - **13.2** Serial Cable Failover Configuration
  - **13.3** LAN-Based Failover
  - **13.4** System Maintenance via Remote Access
  - **13.5** Command Authorization
  - **13.6** PIX Security Appliance Password Recovery and Upgrades

Laboratorium (*75 min*):
13.3.3 Configure LAN-Based Failover (OPTIONAL)
13.5.3 Configure SSH, Command Authorization, and Local User Authentication
13.6.1 Password Recovery

Moduł 14

- **Module 14: PIX VPN**
  - **14.1** The PIX Security Appliance Enables a Secure VPN
  - **14.2** Tasks to Configure VPN
  - **14.3** Task 1 - Prepare to Configure VPN Support
  - **14.4** Task 2 - Configure IKE Parameters
  - **14.5** Task 3 - Configure IPSec Parameters
  - **14.6** Task 4 - Test and Verify VPN Config.
  - **14.7** The Cisco VPN Client
  - **14.8** Scaling PIX Security Appliance VPNs

Laboratorium (*105 min.*):
14.6.6 Configure a Secure VPN Gateway Using IPSec Between Two Cisco Secure PIX Security Appliances
14.7.5 Configure a Secure VPN Using IPSec Between a PIX and a VPN Client
14.8.2 Configure IPSec between Two PIX Security Appliances with CA support

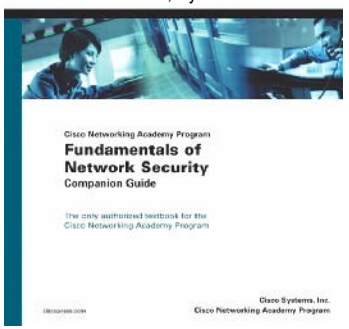
Moduł 15

- **Module 15: PIX Security Appliance Management**
  - **15.1** PIX Security Appliance Management Tools
  - **15.2** The Cisco PIX Device Manager
  - **15.3** Preparation for PDM
  - **15.4** Using PDM to Configure the PIX Security Appliance
  - **15.5** Using PDM to Create Site-to-Site VPNs
  - **15.6** Using PDM to Create Remote Access VPNs
  - **15.7** Enterprise PIX Management

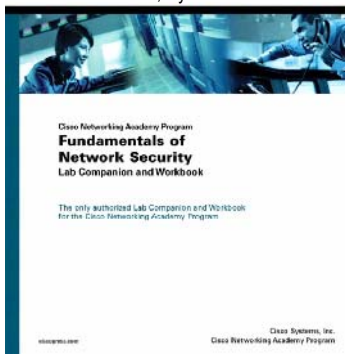
Laboratorium (*45 min.*):
15.6.3 Configuring the PIX Security Appliance with PDM

Literatura do FNS

ISBN: 1587131226; wydana 20-01-2004



ISBN: 1587131234; wydana: 24-02-2004



Najbliższa przyszłość programu

- Wersja 1.2 – korekta drobnych błędów i dynamiczne dostarczanie zawartości programu
- Dostosowanie do najnowszych wersji egzaminów SECUR i CSPFA
- Zestaw laboratoryjny bez zmian – jedynie ewentualnie upgrade oprogramowania urządzeń

Podsumowanie

- Nowy zaawansowany program szkoleń z bezpieczeństwa sieciowego w CNAP
- Wiedza o wysokiej przydatności praktycznej
- Szczegółowo omówione kwestie bezpieczeństwa routerów i ścian przeciwogniowych firmy Cisco Systems
- Problem: właściwe określenie czasu potrzebnego na FNS – standardowe 70 godzin wydaje się być nierealne
- Pytania: co dalej po FNS? czy CCSP będzie można skończyć w ramach CNAP?

Pytania?

Krzysztof Szczypiorski

`e-mail: krzysiek@tele.pw.edu.pl`
`http://krzysiek.tele.pw.edu.pl`