# Instytut Teleinformatyki

Wydział Fizyki, Matematyki i Informatyki
Politechnika Krakowska

## Bezpieczeństwo Systemów Komputerowych

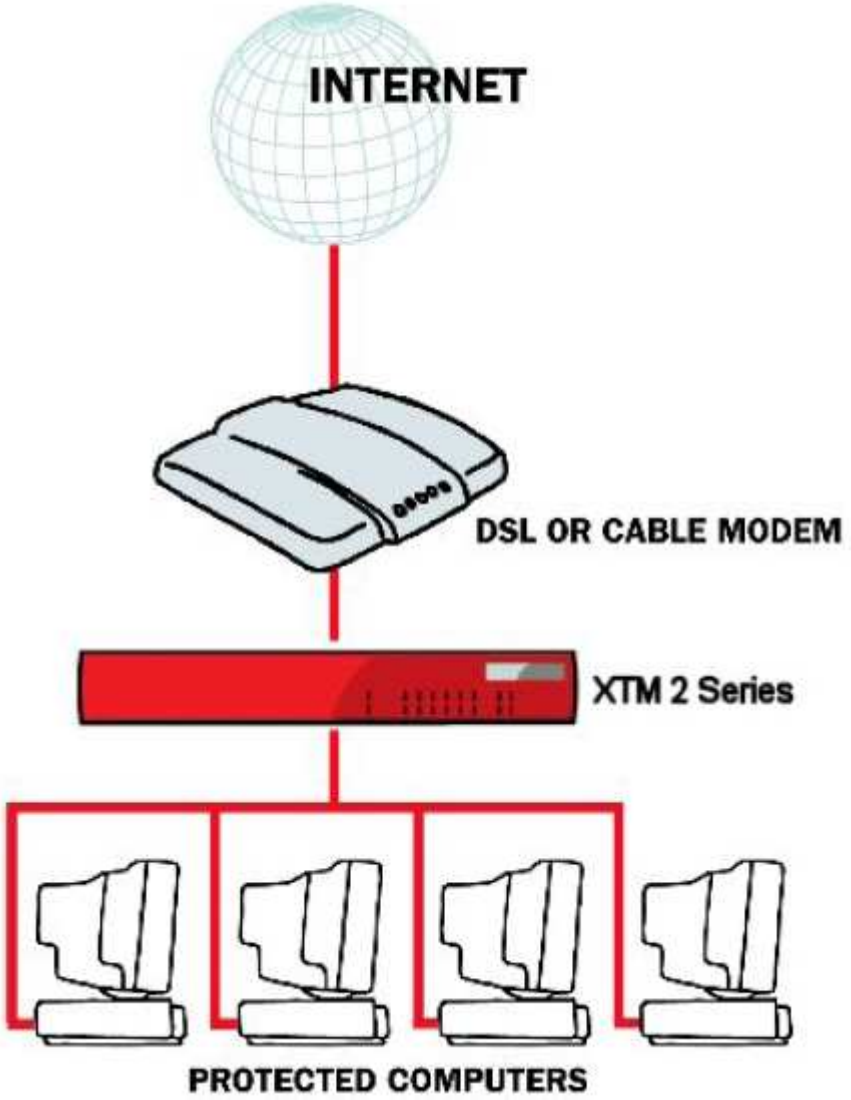
autor: mgr inż. Dariusz Żelasko

**Kraków, 2014**

# Bezpieczeństwo systemów komputerowych

Laboratorium 1

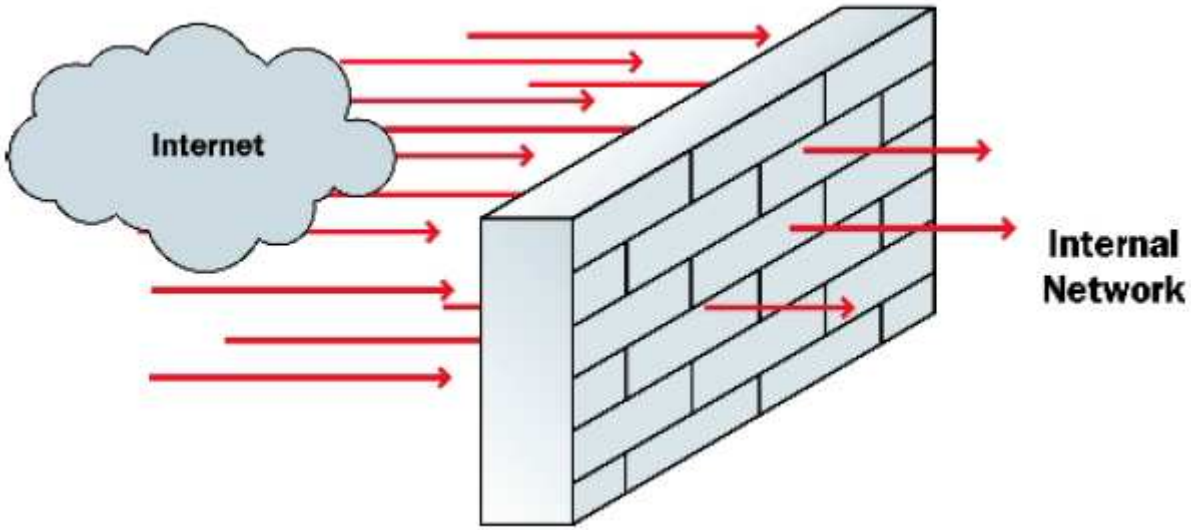
# Firewall


INTERNET
DSL OR CABLE MODEM
XTM 2 Series
PROTECTED COMPUTERS

# Firewall

- Służy do odseparowania sieci wewnętrznej od zewnętrznej
- Wykorzystuje reguły do identyfikowania i filtrowania ruchu
- Może filtrować zarówno ruch przychodzący jak i wychodzący
- Ruch niespełniający reguł bezpieczeństwa jest blokowany

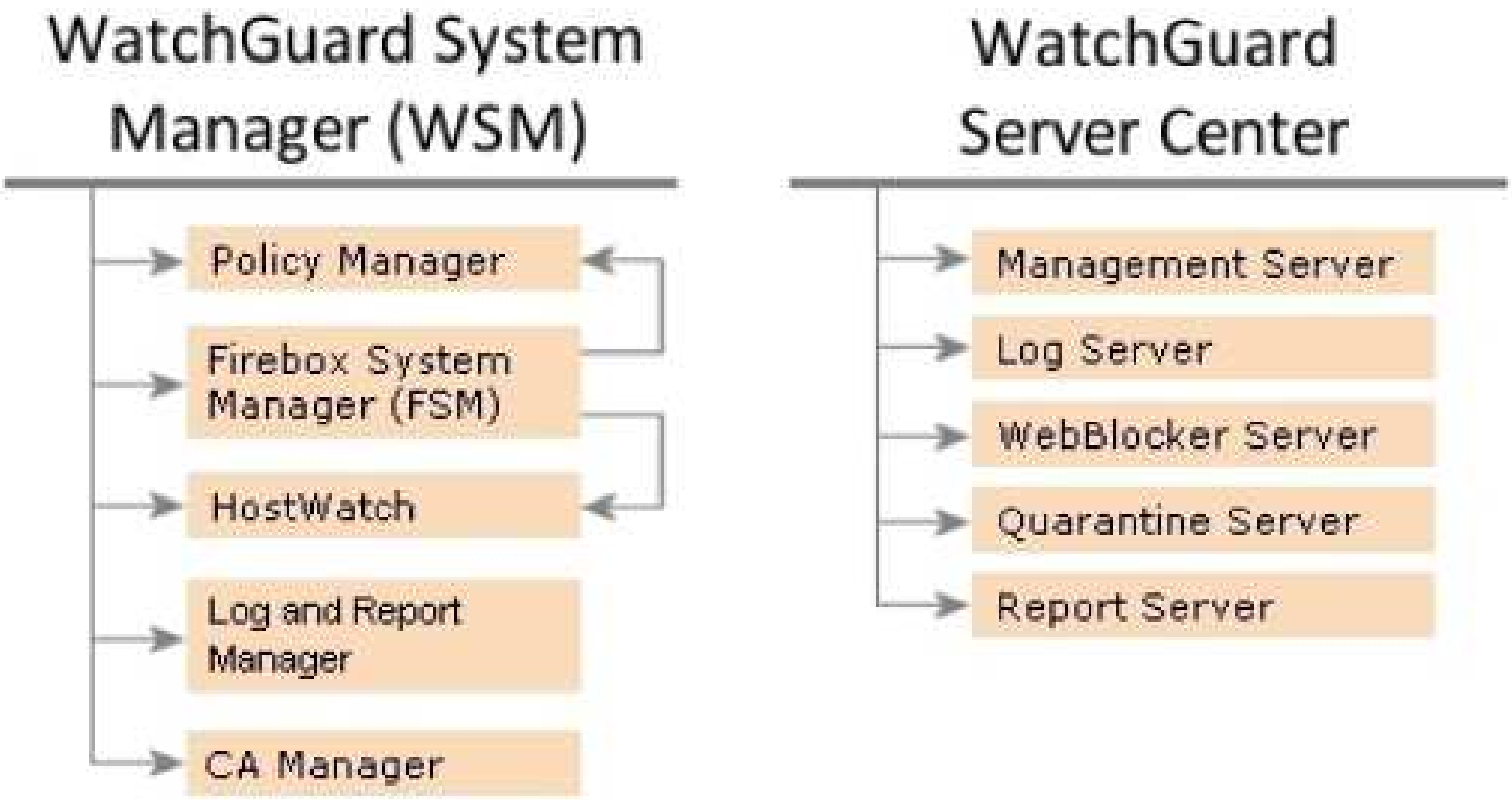
# Firewall



# Watchguard Firewire XTM

- WatchGuard System Manager (WSM)
- Fireware XTM Web UI
- Fireware XTM Command Line Interface (CLI)
- WatchGuard Server Center

# Watchguard Firewire XTM



# Firewire XTM2 i XTM5

# Laboratorium – zasady/wskazówki

- Na każdych zajęciach należy mieć pendrive – do przechowywania konfiguracji (z każdych zajęć) i klucza licencyjnego
- Na początku zajęć należy wziąć jedno urządzenie (XTM-2 lub XTM-5)
- Na zajęciach należy siedzieć zawsze na tym samym miejscu i należy brać zawsze to samo urządzenie (numer seryjny!!!)
- Należy odpiąć kabel sieciowy od gniazdka i podłączyć do portu 1 urządzenia
- Drugi kabel należy podłączyć do portu 0 urządzenia i gniazdka
- Następnie należy przeprowadzić wstępną konfigurację

# Laboratorium – zasady/wskazówki

- External addres – statyczny, 192.168.112.NR_STANOWISKA/24
- Internal address – 192.168.NR_STANOWISKA.1/24 (DHCP)
- Passphrase read-only: aaaaaaaa
- Passphrase read-write: bbbbbbbb
- Po każdych zajęciach należy zapisać swoją konfigurację i klucz licencyjny na pendrive
- Na koniec każdych zajęć należy przywrócić urządzenie do ustawień fabrycznych

## Laboratorium 2 – Quick Setup Wizard, zapoznanie z WSM i FSM (rozdziały 4, 5 i 22 WSM user guide)

**Zadanie 1**. Przeprowadź konfigurację przy użyciu Quick Setup Wizard. (1 pkt.)
**Zadanie 2.** Skonfiguruj serwery NTP i strefę czasową. (1 pkt.)
**Zadanie 3.** Uruchom FSM, sprawdź obciążenie poszczególnych łącz. Sprawdź logi – jakie alarmy widzisz? (1 pkt.)
**Zadanie 4.** Zapisz konfigurację urządzenia, a następnie przywróć urządzenie do ustawień fabrycznych. (1 pkt.)

## Laboratorium 3 – Tworzenie polityk, logi (rozdziały 13 i 21)

**Zadanie 1.** Zablokuj wszystkim użytkownikom dostęp do szyfrowanych stron internetowych. Sprawdź działanie stworzonej reguły. (1 pkt.)
**Zadanie 2.** Zablokuj wszystkim użytkownikom dostęp do FTP w trakcie trwania laboratorium. Sprawdź działanie stworzonej reguły. (1 pkt.)
**Zadanie 3.** Zablokuj użytkownikowi 192.168.NR_KOMPUTERA.4 możliwość wysyłania pakietów ICMP typu 8 do sieci zewnętrznej. W przypadku wysłania pakietu powinien zostać zwrócony komunikat ICMP protocol unreachable. Sprawdź działanie stworzonej reguły. (2 pkt.)
**Zadanie 4.** Włącz zapisywanie logów dla którejś z powyższych reguł. Sprawdź działanie. (1 pkt.)

## Laboratorium 4 – Tworzenie polityk proxy (rozdział 14)

**Zadanie 1.** Usuń wszystkie niepotrzebne polityki. (1 pkt.)
**Zadanie 2.** Utwórz polityki dzięki którym możliwym będzie przeglądanie stron WWW. (1 pkt.)
**Zadanie 3.** Zablokuj możliwość pobierania plików pdf. (1 pkt.)
**Zadanie 4.** Zablokuj możliwość oglądania plików flash. (1 pkt.)
**Zadanie 5.** Zablokuj możliwość wchodzenia na stronę pk.edu.pl. (1 pkt.)
**Zadanie 6.** Zablokuj odwrotne zapytania DNS. (2 pkt.)

## Laboratorium 5 – Serwer zarządzania, serwer raportów, serwer kwarantanny, serwer WebBlocker (rozdziały 18, 19, 21, 30 i 36)

**Zadanie 1.** Dodaj swój firewall do serwera zarządzania. Czym różni się zarządzanie przez serwer manager? (1 pkt.)
**Zadanie 2.** Połącz się z serwerem raportów (Report Manager) i wygeneruj raporty. (1 pkt.)
**Zadanie 3.** Skonfiguruj spamBlocker dla POP3, antywirus dla POP3, HTTP i FTP. Następnie włącz Intrusion Prevention i sprawdź działanie wprowadzonej konfiguracji. (1 pkt.)
**Zadanie 4.** Wraz z osobą siedzącą obok zezwól na dostęp zdalny do swojego urządzenia. Przetestuj działanie. Następnie dodaj urządzenie kolegi/koleżanki do swojego serwera zarządzania. (2 pkt.)

## Laboratorium 6 – Autentykacja użytkowników (rozdział 12)

**Zadanie 1.** Utwórz użytkownika USER1 i USER2 należących do grupy BSK_USER. Użytkownik USER1 powinien mieć dostęp do strony onet.pl. USER2 ma dostęp do wszystkich stron WWW. Proszę zdefiniować domyślne przekierowanie (po poprawnej autoryzacji) na stronę pk.edu.pl. (2 pkt.)
**Zadanie 2.** Dla poprzedniego zadania proszę zabronić wielokrotnego logowania. Czym różnią się poszczególne opcje? (1 pkt.)
**Zadanie 3.** Zmień czas wygaśnięcia. Dobierz czas tak aby możliwym było przetestowanie działania. (1 pkt.)
**Zadanie 4.** Wraz z osobą obok stwórzcie takie reguły aby możliwym było zdalne zarządzanie waszymi firewallami (kolega/koleżanka może zarządzać twoim firewalla a ty jego/jej) za pośrednictwem Web UI przez zalogowanego użytkownika ADMIN_NRSTANOWISKA. (2 pkt.)

## Laboratorium 7 - MOVPN z PPTP (rozdział 27)

**Zadanie 1.** (2 pkt.)

a) Utworzyć w Policy Manager tunel mobilny typu PPTP ustawiając przydział adresów od 192.168.112.xx0 do 192.168.112.xx9 gdzie xx to nr stanowiska + 2. Czyli dla stanowiska nr 1 będzie to od .30 do .39 a dla stanowiska 20 będzie to od .220 do .229.
b) Utworzyć konto użytkownika "kolega" nadając mu hasło aaaaaaaa (8*'a') i dodać go do grupy dla użytkowników VPN.
**Zadanie 2.** Proszę skonfigurować firewall tak, żeby użytkownicy VPN mogli pingować router i komputery w F-112 oraz wchodzić na strony WWW. (1 pkt.)
**Zadanie 3.** Pod Windows 7 skonfigurować połączenie VPN do routera kolegi/koleżanki i nawiązać połączenie używając loginu i hasła kolega/aaaaaaaa oraz metody uwierzytelniania CHAP. (1 pkt.)
**Zadanie 4.** Udowodnij, że połączenie ze stroną wp.pl odbywa się za pośrednictwem zestawionego połączenia VPN (tracert). (1 pkt.)

## Laboratorium 8 - MOVPN z IPSec (rozdział 28)

**Zadanie 1.** Utwórz tunel mobilny IPSec. Przydziel adresy z następującego zakresu: od 192.168.112.xx0 do 192.168.112.xx9 gdzie xx to nr stanowiska + 2. Utwórz konto VPN_NRStanowiska z hasłem aaaaaaaa. Dodaj użytkownika do grupy użytkowników VPN. Skonfiguruj VPN tak aby cały ruch płynął przez stworzony tunel. (2 pkt.)
**Zadanie 2.** Skonfiguruj firewall tak aby użytkownicy VPN mogli korzystać ze stron internetowych i ping. (1 pkt.)
**Zadanie 3.** Wygeneruj plik konfiguracyjny VPN. (1 pkt.)
**Zadanie 4.** Sprawdź czy na komputerze zainstalowany jest klient VPN - jeśli nie to zainstaluj. Zaimportuj wygenerowany przez kolegę/koleżankę plik. Nawiąż połączenie z VPN kolegi/koleżanki i przetestuj poprawność działania. (1 pkt.)

## Laboratorium 9 - MOVPN z SSL (rozdział 29)

**Zadanie 1.** (2 pkt.)
a) Utwórz w Policy Manager tunel mobilny typu SSL ustawiając pule adresów 192.168.NR_STANOWISKA+100.0/24. Czyli dla stanowiska nr 1 będzie to sieć 192.168.101.0, a dla stanowiska 20 192.168.120.0.
b) Utworzyć konto użytkownika "kolega" nadając mu hasło aaaaaaaa (8*'a') i dodać go do grupy użytkowników VPN.
**Zadanie 2.** Proszę skonfigurować firewall tak, żeby użytkownicy VPN mogli wykonać ping i wchodzić na strony WWW oraz łączyć się z FTP. (1 pkt.)
**Zadanie 3.** Zainstaluj oprogramowanie klienckie. Nawiąż połączenie. Następnie zaprezentuj ustawienia programu. (1 pkt.)
**Zadanie 4.** Udowodnij, że połączenie ze stroną wp.pl odbywa się za pośrednictwem zestawionego połączenia VPN (tracert). (1 pkt.)

## Laboratorium 10 - BOVPN (rozdziały 25 i 26)

**Zadanie 1.** Przy użyciu Policy manager'a zestaw dwukierunkowy tunel BOVPN z siecią kolegi/koleżanki. (2 pkt.)
**Zadanie 2.** Zmień konfigurację na jednokierunkową. Sprawdź działanie. Jaka jest różnica między tunelem dwukierunkowym i jednokierunkowym (ping)? (1 pkt.)
**Zadanie 3.** Przekieruj sieć kolegi/koleżanki do swojego komputera. Sprawdź poprawność działania. (1 pkt.)
Po ukończeniu zadania 1, 2 i 3 przedstaw je prowadzącemu.
**Zadanie 4.** Usuń tunel stworzony w zadaniu 1. Za pomocą serwera zarządzania utwórz tunel automatycznie. Sprawdź poprawność działania. (1 pkt.)

## Laboratorium 11 - MultiWAN (rozdział 7)

**Zadanie 1.** Skonfiguruj port 2 jako external. Nadaj mu adres IP 192.168.133.NR_STANOWISKA (brama 192.168.133.254). (1 pkt.)

**Zadanie 2.** Skonfiguruj funkcję Multi-WAN tak aby status poszczególnych łącz określany był na podstawie ping do bramy domyślnej i transmisji TCP na adres serwera www pk.edu.pl (oba warunki muszą być spełnione). (1 pkt.)

**Zadanie 3.** Ustaw czas pomiędzy kolejnymi testami łącz na 5 sekund. Łącze ma zostać uznane za niedziałające po 2 próbach. Ponowna aktywacja łącza ma nastąpić po 2 udanych próbach połączenia. (1 pkt.)

**Zadanie 4.** Proszę przetestować wszystkie opcje kierowania ruchu dostępne w ramach Multi-WAN. Jak działają poszczególne metody? (2 pkt.)

**Zadanie 5.** Skonfiguruj Multi-WAN w trybie failover. Ustaw kolejność interfejsów - najpierw 2 potem 0. Uruchom ping -t onet.pl na komputerze. Odepnij kabel od portu 2 firewalla. Jaki jest efekt? Co się stało z ping? (1 pkt.)

**Zadanie 6.** Ustaw polityki tak aby cały ruch http kierowany był przez interfejs 0. Z kolei cały ruch związany z ping należy kierować przez interfejs 2. Udowodnij, że wprowadzona konfiguracja działa prawidłowo (tracert). (1 pkt.)

## Laboratorium 12 - WebBlocker, AV/IPS, spamBlocker, RED, application control (rozdziały od 30 do 35)

**Zadanie 1.** Przy użyciu WebBlocker zablokuj strony o tematyce edukacyjnej i podróżniczej. (1 pkt.)

**Zadanie 2.** Zablokuj strony o reputacji >60. Przetestuj działanie wprowadzonej konfiguracji. (1 pkt.)

Komentarz: reputację można sprawdzić: http://www.watchguard.com/products/Reputation-authority.asp

Wszelkie adresy związane z ADSL mają zazwyczaj złą reputację. Pule adresów można sprawdzić: http://pl.wikipedia.org/wiki/Wikipedia:Lista_zakres%C3%B3w_IP

**Zadanie 3.** W przypadku podejrzanej wiadomo ci dodaj tag "TO MOŻE BYĆ SPAM". (1 pkt.)

**Zadanie 4.** Zablokuj możliwość korzystania z IRC, Winamp i eMule. (1 pkt.)

**Zadanie 5.** Wyłącz skanowanie AV dla stron o reputacji <20. (1 pkt.)

## Laboratorium 13 - Troubleshooting

**Zadanie 1.** Zmień adres IP na interfejsie 0 i 2 na zgodny ze swoim numerem stanowiska. (1 pkt.)

Int-0: 192.168.112.NR_STANOWISKA

Int-2: 192.168.133.NR_STANOWISKA

**Zadanie 2.** W oparciu o informacje dostarczone przez użytkowników znajdź problemy z konfiguracją. Nie wolno dodawać żadnych reguł, można tylko modyfikować te istniejące. (8 pkt.)

Informacje od użytkowników:

- Nie ma możliwości dostania się na żadną stronę internetową (http i https!!!).
- Administrator ma dostęp do firewalla przez Web UI, aby się dostać do strony https://192.168.19.1:8080 musi najpierw dokonać autoryzacji na stronie https://192.168.19.1:4100 (login: administrator, hasło: aaaaaaaa). Zgłoszono problem z dostępem do strony autoryzacji.
- Użytkownik ma konto do MOVPN PPTP, jego login to: uzytkownik_vpn, hasło: aaaaaaaa. Użytkownik nie może połączyć się z VPN.
- Cały ruch w sieci odbywa się przez łącze zapasowe (interfejs 2), a powinno przez łącze podstawowe (interfejs 0).
- Gdy działał jeszcze dostęp do stron WWW to nie można było się dostać na strony takie jak pk.edu.pl, pl.wikipedia.org.

Konfiguracja:

- XTM2 http://mars.iti.pk.edu.pl/~zelasko/BSK/XTM2.zip

- XTM5 http://mars.iti.pk.edu.pl/~zelasko/BSK/XTM5.zip