

ДИЗАЈН И ТЕСТИРАЊЕ НА ВИРТУЕЛНИ МРЕЖИ

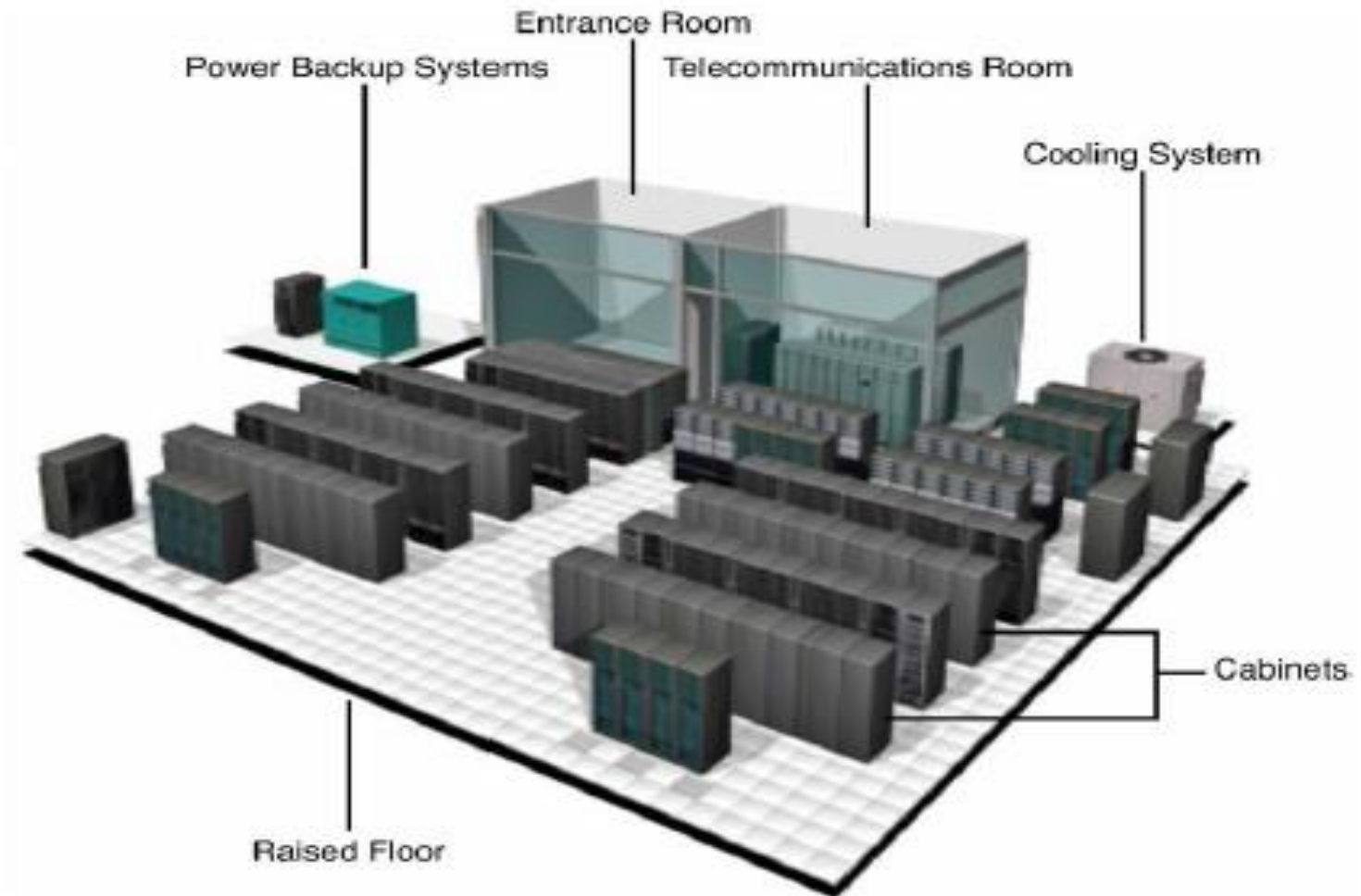
Дипл. инж. Дејан Чабуковски
S&T Macedonia, Скопје

cabuk_dejann@yahoo.com

12.11.2016

Семинар “Серверска и мрежна виртуелизација во
податочни центри”, ПМФ – УКИМ, Скопје

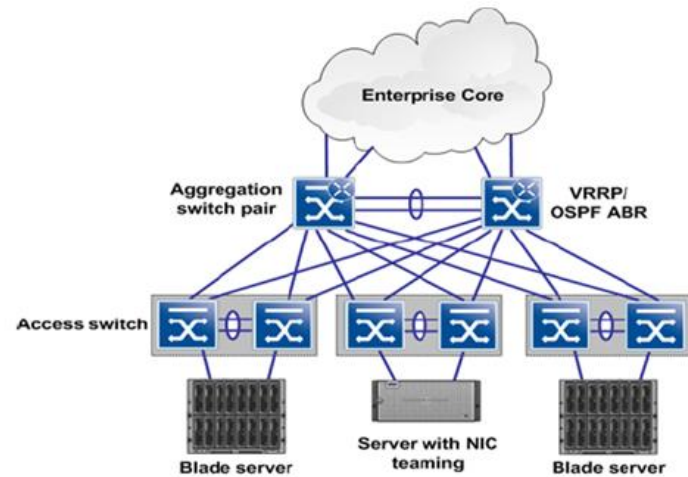
Податочен центар



Податочен центар

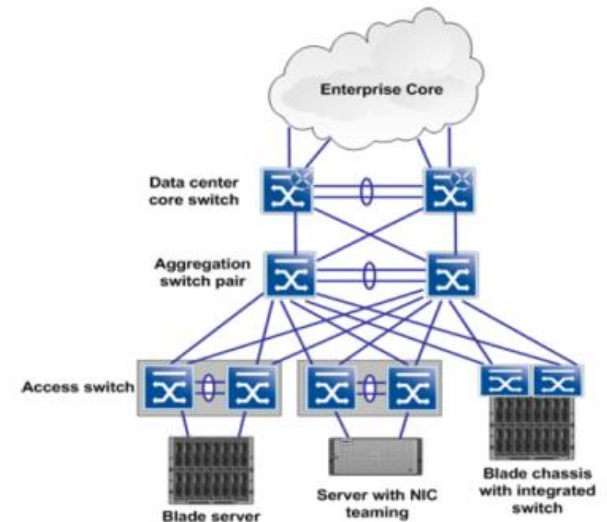
Компоненти на податочен центар:

- ✓ Сервери
- ✓ Складирање
- ✓ Вмрежување



Мрежни топологии на податочен центар:

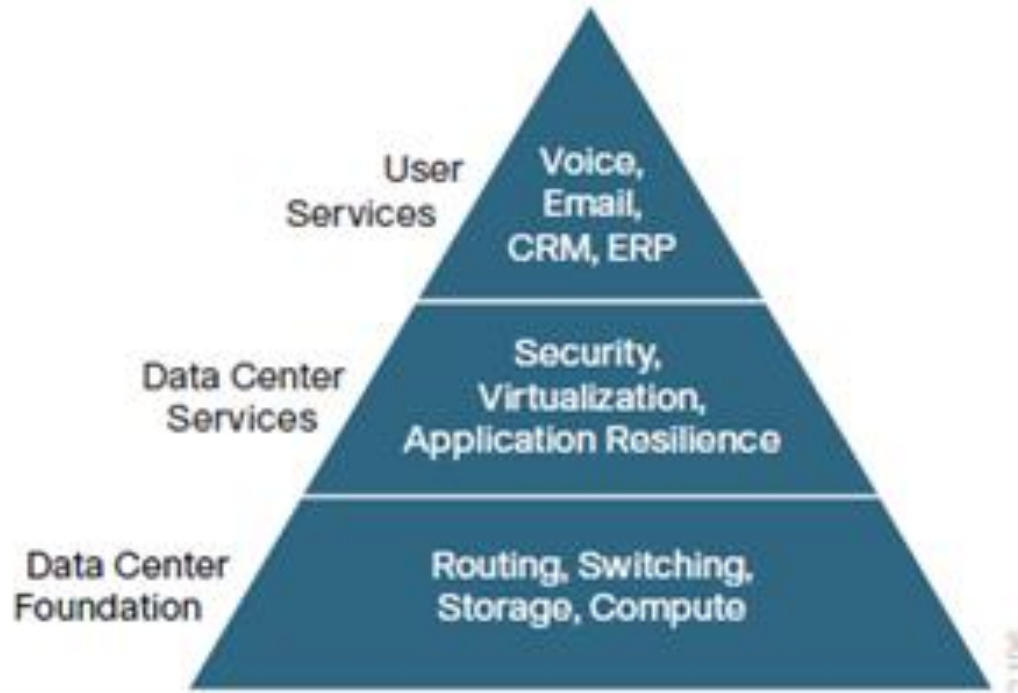
- ✓ Двослоен дизајн
- ✓ Трислоен дизајн



Податочен центар

Сервисна архитектура на податочен центар

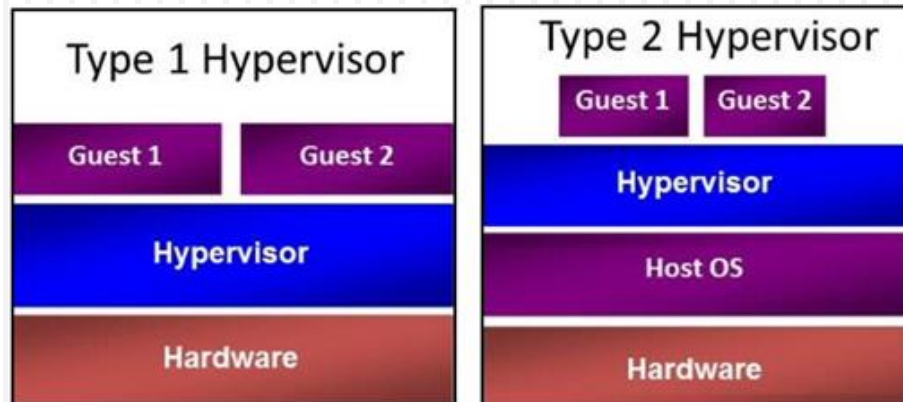
Figure 1 - Data center pyramid of service layers



Виртуелизација

Типови на виртуелизација

- ✓ Серверска виртуелизација
- ✓ Десктоп виртуелизација
- ✓ Виртуелизација на складиштето
- ✓ Виртуелизација на мрежата
- ✓ Виртуелизација на сервис



Два типа на хипервизори

Мрежна виртуелизација - факултетски ПЦ

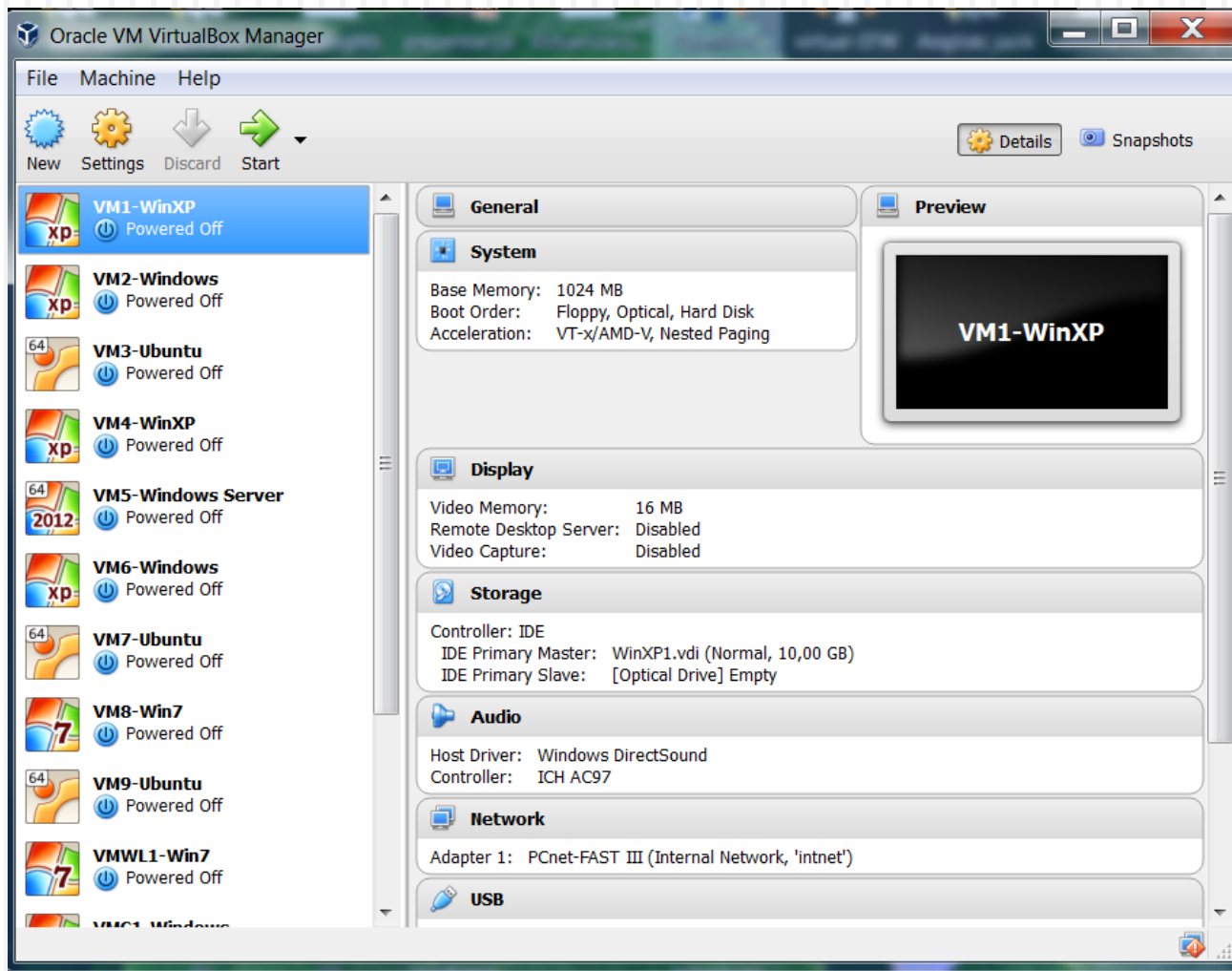
Oracle VirtualBox

VirtualBox за секоја виртуелна машина обезбедува до осум виртуелни PCI мрежни картички.

Секој од нив може посебно да се конфигурира да работи во еден од следните модови:

- ✓ Not attached
- ✓ Network Address Translation (NAT) / NAT Network
- ✓ Bridged networking
- ✓ Internal networking
- ✓ Host-only networking
- ✓ Generic networking

Мрежна виртуелизација - факултетски ПЦ



Основен екран на VirtualBox со креирани виртуелни машини

Мрежна виртуелизација - факултетски ПЦ

1. Приватни подмрежи (VLAN) – ограничен пристап (финансиско и материјално работење, архива, студентски систем, систем за поддршка на одлуки, персонална евиденција и др.)
2. Пошироко достапни подмрежи со излез на Интернет – влез преку VPN (предавални, училници, веб сервер, е-маил сервер, moodle сервер, SAKAI сервер)
3. Делумно пошироко достапни подмрежи – влез преку VPN (веб сервери, е-маил сервери, апликациски сервери)
4. Јавно достапни подмрежи со влез и излез на Интернет (moodle сервер, SAKAI сервер, апликациски сервери, веб сервери)

Мрежна виртуелизација - факултетски ПЦ

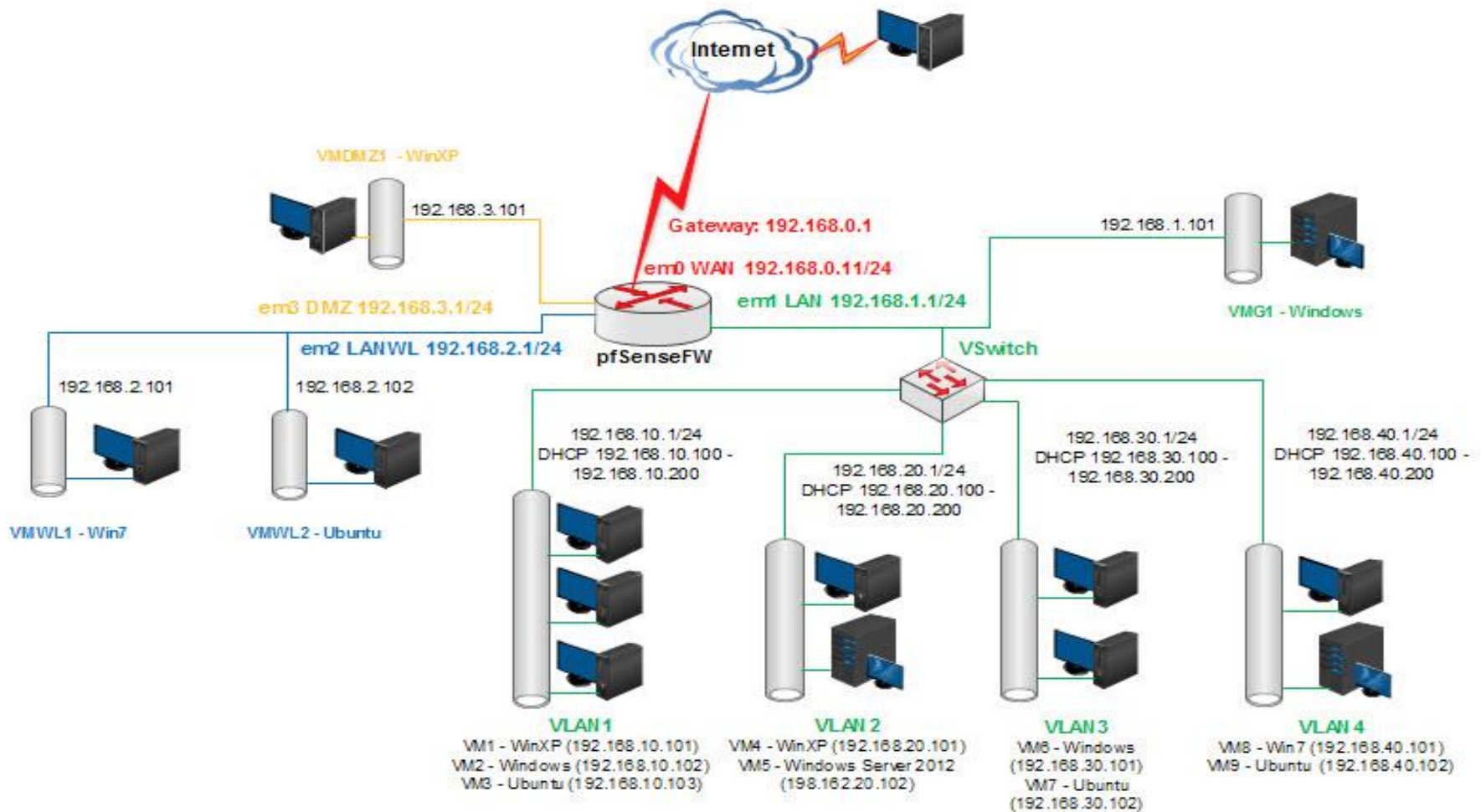
Безбедна мрежа (ВПМ – Виртуелна приватна мрежа)

pfSense огнен ѕид (firewall) - максимум 4 виртуелни мрежни картички, vSwitch и можност за неограничен број на виртуелни подмрежи

базирана на протоколите:

- ✓✓ IPsec (Internet Protocol Security)
- ✓ SSL (Secure Sockets Layer)
- ✓ SSH (Secure Shell Tunneling)

Мрежна виртуелизација - факултетски ПЦ



Мрежна виртуелизација - факултетски ПЦ

Податоци за дизајнирана виртуелна мрежа на високо образовна институција

Виртуелна мрежа / мрежа	Зона	Ознака	Виртуелна машина	интерфејс	IP интерфејс (VirtualBox тип на интерфејс)	IP мрежа	Gateway	Инсталиран софтвер
WAN	red	pfSenseFW	pfSense Firewall (Open source)	Em0 – red	192.168.0.11 DHCP Bridged Adapter	192.168.0.0/24	192.168.0.1	FreeBSD базиран рутер, огнен ѕид, прокси, ... Пристап преку веб на адреса https://192.168.0.11
				Em1 – green	192.168.1.1 Internal network	192.168.1.0/24	192.168.1.0	
				Em2 – blue	192.168.2.1 Internal network (wireless)	192.168.2.0/24	192.168.2.1	
				Em3- orange	192.168.3.1 Internal Network	192.168.3.0/24	192.168.3.1	
	green	VMG1-Windows	Windows XP	Em1 – green	192.168.1.101	192.168.1.0/24	192.168.1.1	Web сервер (http) e-mail сервер
VLAN1	green	VM1-WinXP	Windows XP	Em1 – green	192.168.10.101	192.168.10.0/24	192.168.1.1	Апликациски сервер
VLAN1	green	VM2-Windows	Windows XP	Em1 – green	192.168.10.102	192.168.10.0/24	192.168.1.1	
VLAN1	green	VM3-Ubuntu	Ubuntu	Em1 – green	192.168.10.103	192.168.10.0/24	192.168.1.1	
VLAN2	green	VM4-WinXP	Windows XP	Em1 – green	192.168.20.101	192.168.20.0/24	192.168.1.1	
VLAN 2	green	VM5-Windows server	Windows Server 2012 R2	Em1 – green	192.168.20.102	192.168.20.0/24	192.168.1.1	Податочен сервер (SQL)
VLAN3	green	VM6-Windows	Windows XP	Em1 – green	192.168.30.101	192.168.30.0/24	192.168.1.1	
VLAN3	green	VM7-Ubuntu	Ubuntu	Em1 – green	192.68.30.102	192.168.30.0/24	192.168.1.1	
VLAN4	green	VM8-Win7	Windows 7	Em1 – green	192.168.40.101	192.168.40.0/24	192.168.1.1	
VLAN4	green	VM9-Ubuntu	Ubuntu	Em1 – green	192.168.40.102	192.168.40.0/24	192.168.1.1	
DMZ	orange	VMDMZ1-WinXP	WindowsXP	Em3- orange	192.168.3.101	192.168.3.0/24	192.168.3.1	Апликациски сервер SAKAI, Web сервер (http)
	blue	VMWL1-Win7	Windows 7	Em2 – blue	192.168.2.101	192.168.2.0/24	192.168.2.1	e-mail сервер, Web сервер (http)
	blue	vMWL2-Ubuntu	Ubuntu	Em2 – blue	192.168.2.102	192.168.2.0/24	192.168.2.1	

Мрежна виртуелизација - факултетски ПЦ



The screenshot shows the pfSense web interface in a browser window. The browser's address bar displays the URL `https://192.168.1.1/interfaces_assign.php`. The navigation menu includes links for Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main heading is "Interfaces: Assign network ports". Below this, there are tabs for "Interface assignments", "Interface Groups", "Wireless", "VLANs", "QinQs", "PPPs", "GRE", "GIF", "Bridges", and "LAGG". The "Interface assignments" tab is active, showing a table with the following data:

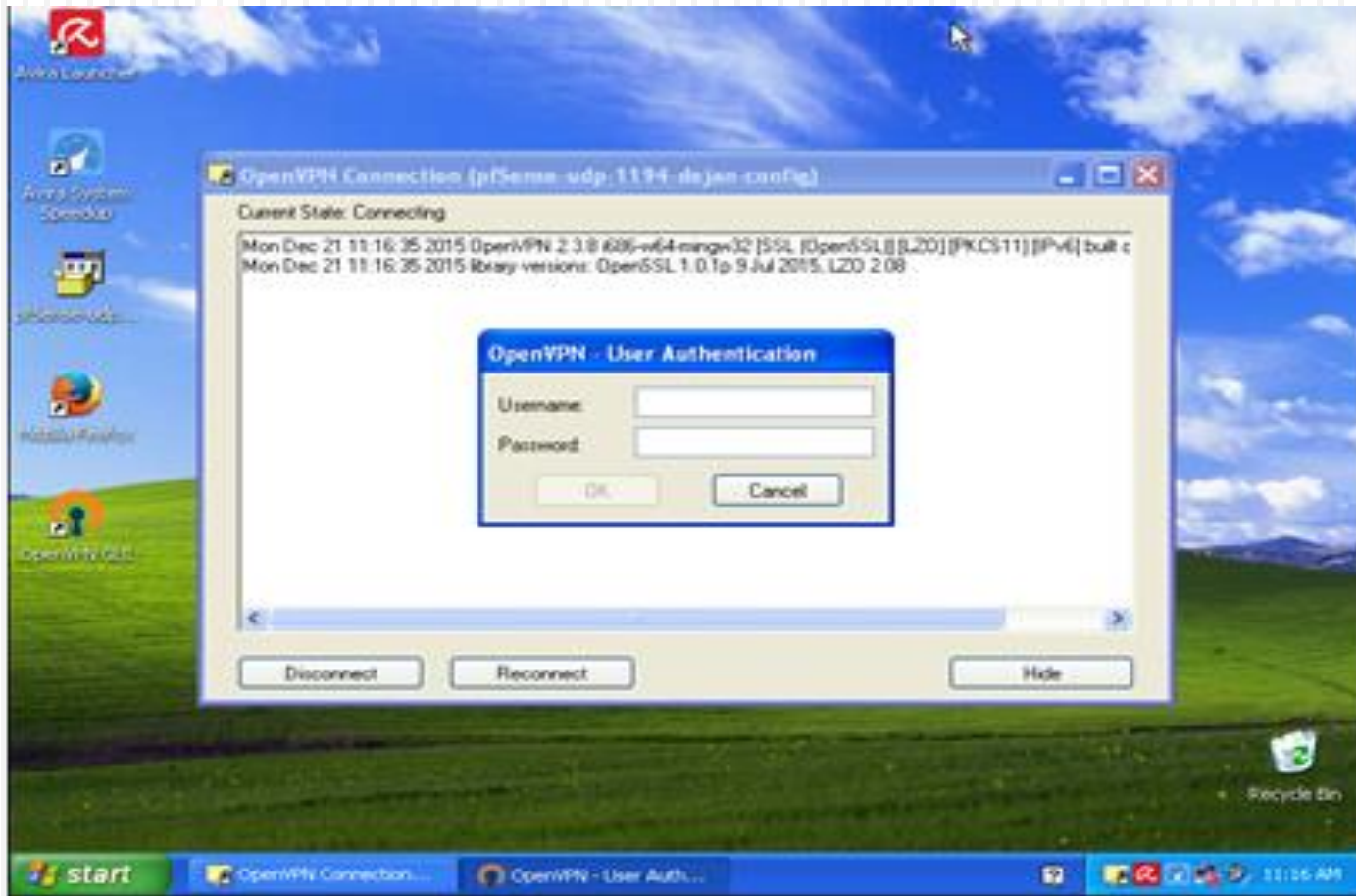
Interface	Network port
<u>WAN</u>	em0 (08:00:27:96:f3:6f)
<u>LAN</u>	em1 (08:00:27:76:8f:c8)
<u>LANWL</u>	em2 (08:00:27:1e:5d:b0)
<u>DMZORANGE</u>	em3 (08:00:27:4f:3d:0d)
<u>VLAN1GREEN</u>	VLAN 10 on em1 (VLAN1-GREEN)
<u>VLAN2GREEN</u>	VLAN 20 on em1 (VLAN2-GREEN)
<u>VLAN3GREEN</u>	VLAN 30 on em1 (VLAN3-GREEN)
<u>VLAN4GREEN</u>	VLAN 40 on em1 (VLAN4-GREEN)
Available network ports:	ovpns1 (MyOpen VPN Server LAN)

Below the table, a note states: "Interfaces that are configured as members of a lagg(4) interface will not be shown." The Windows taskbar at the bottom shows the Start button, the pfSense local domain, and the system clock at 10:42 AM.

Приказ на екран на pfSense со креирани виртуелни мрежи

Мрежна виртуелизација - факултетски ПЦ

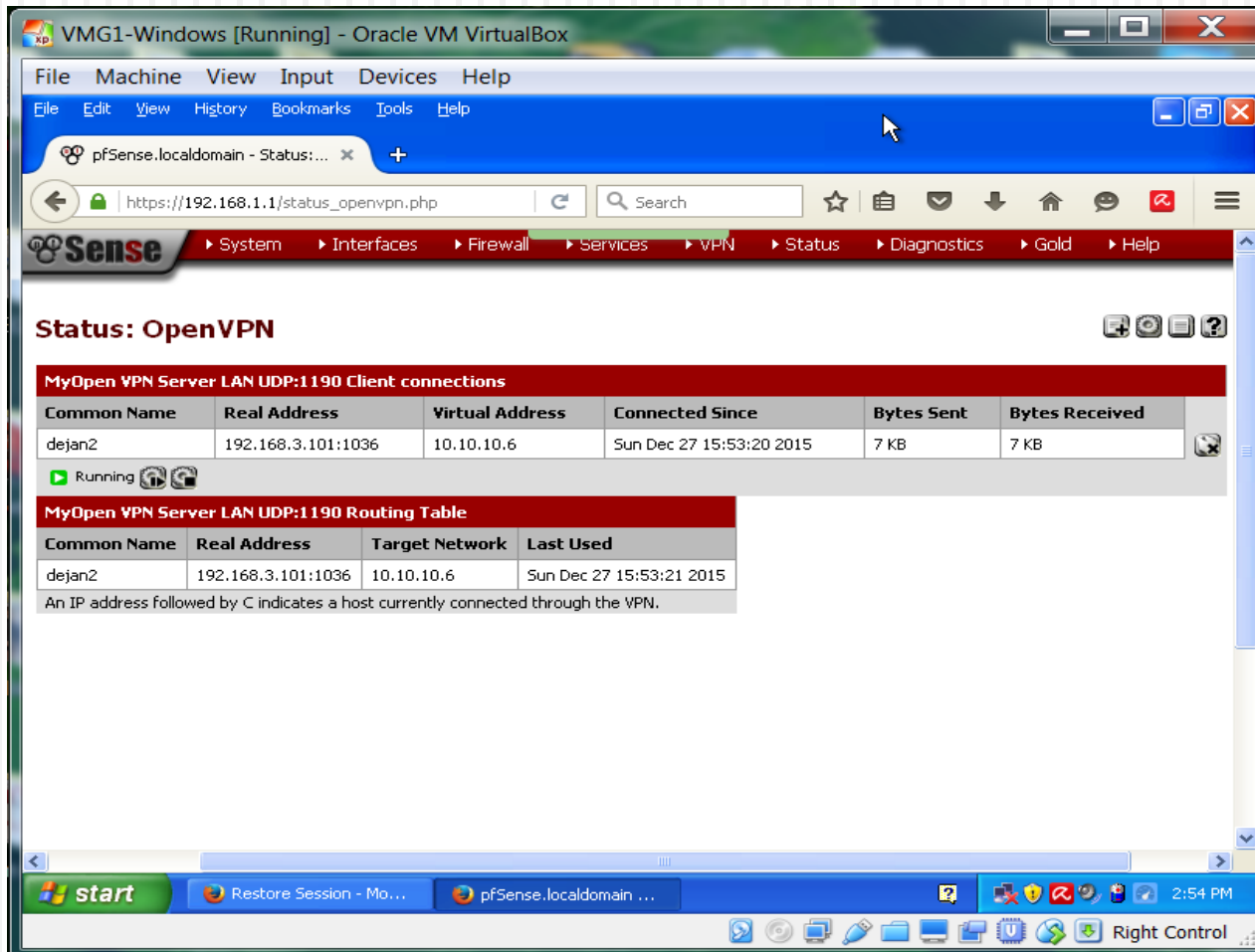
Поставување на ВПМ – постапка на креирање на приватен канал (тунел) во pfSense



OpenVPN клиентска програма и авторизација

Мрежна виртуелизација - факултетски ПЦ

Поставување на ВПМ – постапка на креирање на приватен канал (тунел) во pfSense



The screenshot shows the pfSense web interface in a browser window. The page title is "Status: OpenVPN". Below the title, there is a section for "MyOpen VPN Server LAN UDP:1190 Client connections" which contains a table with the following data:

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
dejan2	192.168.3.101:1036	10.10.10.6	Sun Dec 27 15:53:20 2015	7 KB	7 KB

Below this table, there is a "Running" status indicator. Underneath, there is a section for "MyOpen VPN Server LAN UDP:1190 Routing Table" with the following table:

Common Name	Real Address	Target Network	Last Used
dejan2	192.168.3.101:1036	10.10.10.6	Sun Dec 27 15:53:21 2015

A note at the bottom of the routing table states: "An IP address followed by C indicates a host currently connected through the VPN."

Активни VPN конекции во pfSense

Мрежна виртуелизација - факултетски ПЦ

Тестирање на виртуелната мрежа (прод.)

The screenshot displays the Wireshark 1.10.3 interface. The main pane shows a list of network packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 13445) is expanded to show its details: Ethernet II, Destination: CadmusCo_76:8f:c8, and Source: CadmusCo_6e:09:74. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
13445	393.686188	192.168.1.101	192.168.1.101	ICMP	74	Echo (ping) reply id=0x02
13446	393.775922	192.168.1.101	192.168.10.1	ICMP	74	Echo (ping) request id=0x02
13447	393.776157	192.168.10.1	192.168.1.101	ICMP	74	Echo (ping) reply id=0x02
13448	393.785985	192.168.1.101	192.168.40.1	ICMP	74	Echo (ping) request id=0x02
13449	393.786214	192.168.40.1	192.168.1.101	ICMP	74	Echo (ping) reply id=0x02
13450	394.049583	fe80::1:1	ff02::1	ICMPv6	110	Router Advertisement from 08
13451	394.275360	93.184.220.29	192.168.1.101	TCP	60	http > remote-as [FIN, ACK]
13452	394.275391	192.168.1.101	93.184.220.29	TCP	54	remote-as > http [ACK] Seq=4
13453	394.275584	192.168.1.101	93.184.220.29	TCP	54	remote-as > http [FIN, ACK]
13454	394.312180	93.184.220.29	192.168.1.101	TCP	60	http > remote-as [ACK] Seq=7
13455	394.345028	192.168.3.101	192.168.0.13	UDP	159	source port: nsstp Destination
13456	394.345032	192.168.0.13	192.168.3.101	UDP	159	source port: commlinux-av1 0
13457	394.475868	192.168.3.101	192.168.0.13	UDP	159	source port: nsstp Destination
13458	394.476450	10.10.10.6	192.168.1.101	ICMP	74	Echo (ping) request id=0x03
13459	394.476505	192.168.1.101	10.10.10.6	ICMP	74	Echo (ping) reply id=0x03

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 1

- Ethernet II, Src: CadmusCo_6e:09:74 (08:00:27:6e:09:74), Dst: CadmusCo_76:8f:c8 (08:00:27:76:8f:c8)
 - Destination: CadmusCo_76:8f:c8 (08:00:27:76:8f:c8)
 - Source: CadmusCo_6e:09:74 (08:00:27:6e:09:74)
 - Type: IP (0x0800)

```
0000  08 00 27 76 8f c8 08 00 27 6e 09 74 08 00 45 00  ..'v.... 'n.t..E.
0010  00 3c 5d 9f 00 00 80 01 07 05 c0 a8 01 65 0a 0a  .<].....e..
0020  0a 06 08 00 5c 1d 02 00 ef 3e 61 62 63 64 65 66  .....>abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefgh i
```

Пристап и анализирање на одредени сервиси со Wireshark