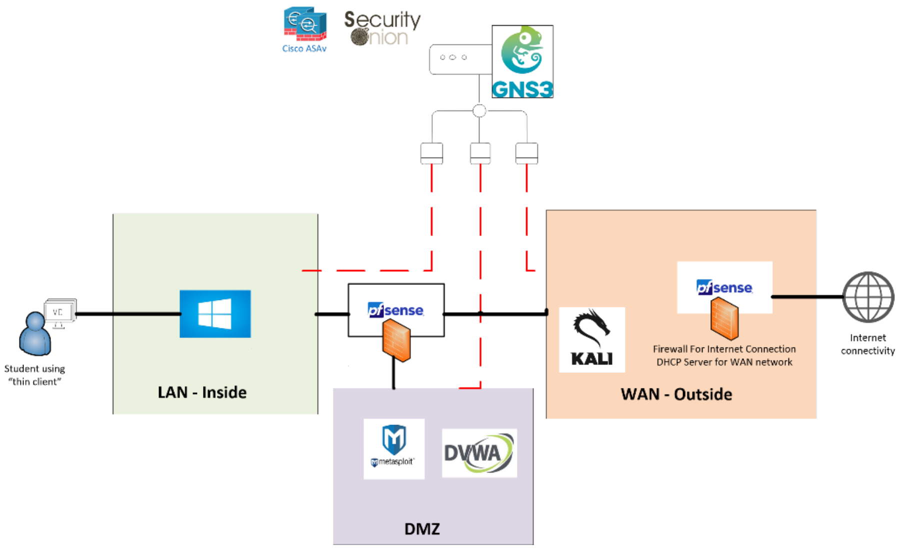
Titus Bălan

Network Security and Perimeter Defense

- Laboratory Guide -



EDITURA
UNIVERSITĂȚII
TRANSILVANIA
DIN BRAȘOV

2023

Contents

Introduction

This paper represents a laboratory guide dedicated for students of the “Cybersecurity” master program of “Transilvania” University of Brasov, Romania.

The laboratory guise is prepared for the “Network Security and Perimeter Defence” lab. However, the infrastructure can be used also for other topics.

The laboratory guide details different problematic of network security: it starts with the network monitoring methods: syslog, SNMP, Netflow, so relevant for incident management, continues with detailing Layer 2 vulnerabilities, and than goes into Firewall (next generation Firewall) functionality, different tunneling options (L2 and L3) and IDS/IPS functionality (Intrusion Detection System / Intrusion Prevention System).

Resources are different, including open source respurces like: Pfsense, Kali linux, Metasloptable, Security Onion, Snort, OpenVPN (.etc) and proprietary (like Cisco ASA and Cisco IOS, Solarwinds tools) and different testing host (Linux, Windows) and virual containers.

As prerequisites for students that will folow the laboratory guide we would like to mention the need for networking concepts know-how, cryptography concepts needed for the proper understanding of VPN settting-up, Linux know-how and GNS3 basic usage knowledge.

This is a second revision on the laboratory work, with most of the functionality migrated to GNS3 and with an upgrade to the software stack. The environment is extremly flexible and versatile, topologies and resources can be easily exchanges, virtual machines (e.g. Kali Linux) deployes in seconds, Internet connectivity can be established very fast in different methods, thus different realistic scenarious can be fastly emulated. The laboratory can be used as a Cyber Range and can be extended with other real, emulated and virtual resources.

I would like to thank Andreea Popescu and Mihai Matei for their support during the elaboration of this Network Security and Perimeter Defence laboratory guide (students of Cybersecurity master program at the time of the publishing).

I would like to thank Atos Romania as the initial sponsorship of the lab infrastructure (with effort support of Andrei Boghiu and Alex Rad) and the Fullbright Comission that provided a grant to support the effort of our laboratory modernisation.

Remote laboratory setup description

The laboratory is accesible online at citrix.unitbv.ro

The secure remote connectivity is assured via the Citrix Netscaler component from anywhere in the internet, while Citrix Xen Desktop is used as a robust VDI (Virtual desktop infrastructure) solution

On the client machine Citrix Receiver should be installed (you will be prompted at the first connecivity attempt) from your browser.

Via Citrix Xen Desktop you will have access to a Windows 10 machine that has all necessary software installed and will connect you to the other resourses.

Each laboratory will detail the setup and topology that should be created and the tools to be used.

In order to access some resources please have these in mind:

GNS3 Resource:	Username:	Password:	IP Address:
KALI Linux	kali	kali	(GNS3)
Windows Server	administrator	Master01	

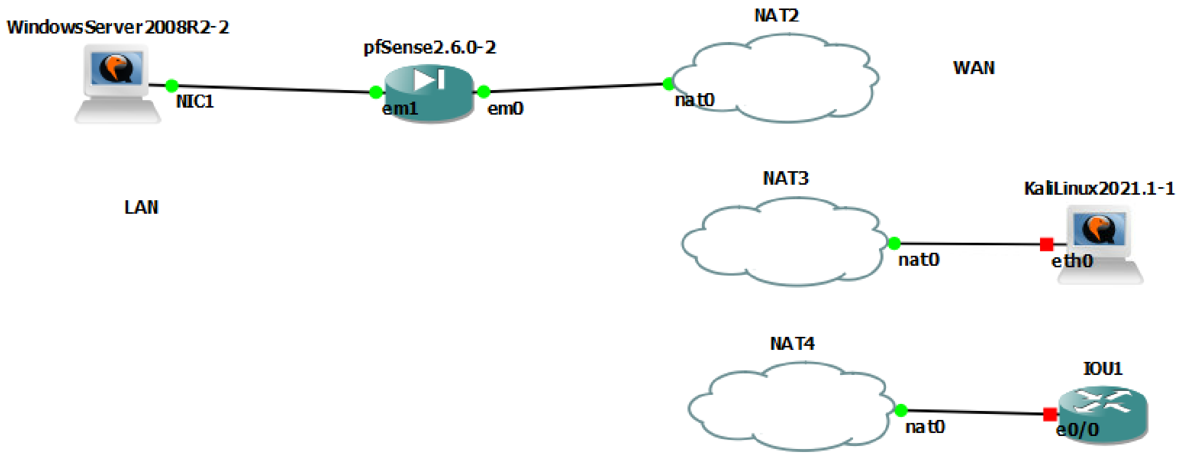
- In order to get internet access to resources inside GNS3 server, connect the "NAT" (cloud symbol) to the L3 device. Set the IP address to DHCP in order to get correct NAT IP and gateway.
- Caution! There are TWO types of clouds inside GNS3, one called "Cloud" and another called "NAT" - Do not connect any L2 devices (switches) to the "Cloud" (also a Cloud symbol inside GNS3) since this will create a bridge loop! The "Cloud" is basically a bridge device to the real network. If needed, ONLY connect L3 devices (routers/firewalls) to the "Cloud". Do this only with the approval and supervision of the your trainer/teacher.
- Devices MUST be configured with DHCP in order to receive an IP address when connected to the "Cloud" or "NAT"
- The GNS3 environment is persistent, but the Windows 10 VDI will reset to the initial configuration at any new login.

1. System logging and monitoring

Kiwi Syslog Laboratory

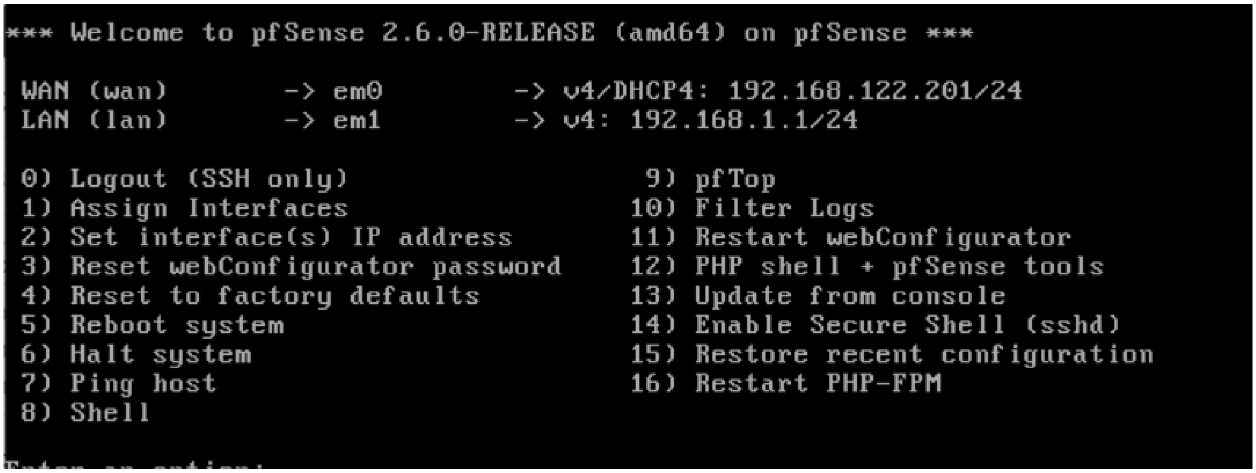
Step 1. Prepare the environment

1.1 Make in GNS3 the following topology



1.2. Prepare the setup. Start pfSense. In case you install pfSense for the first time follow these steps:

- For the initial setup of pfSense, choose the installation method with BIOS (not UEFI), second option. Do not enter Shell, but Reboot.
- Once it got installed, by default the IP address for the LAN Interface is 192.168.1.1.
- From the CLI menu of pfSense, using option 2, set the IP address for WAN via DHCP.
- You should get an IP address from subnet 192.168.122.0/24



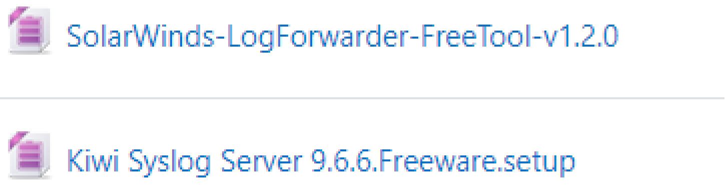
```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.122.201/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

- On the Windows Server machine by default the configuration of ip address is via DHCP. You should get an IP address from the subnet 192.168.1.0/24.
- In the browser, connect to the pfsense firewall at 192.168.1.1. Username: admin, password: pfsense.

- Go to Services / DHCP Server / LAN and set the following DNS servers:193.254.231.1 193.254.230.2
- Set the Same DNS Servers in menu System / General Setup.
- Go on the Windows Server Machine, Disable and Enable the interface so that DNS is also set via DHCP.

1.3. Start WindowsServer. Passord WindowsServer2008: Master01

1.4. Get from e-learning kiwi syslog and Solarwinds and install



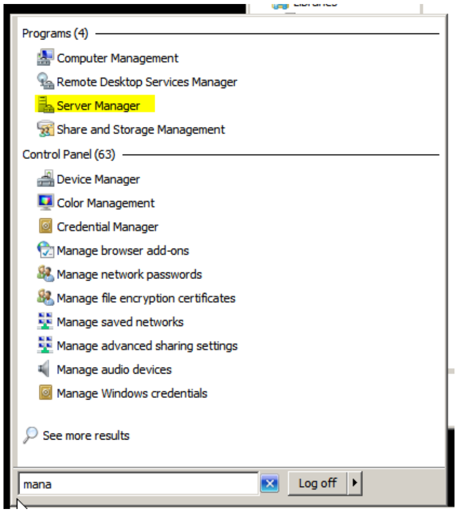
SolarWinds-LogForwarder-FreeTool-v1.2.0

Kiwi Syslog Server 9.6.6.Freeware.setup

Before installing SolarWinds, you might need to install microsoft .NET framework 4.0 (https://www.microsoft.com/en-us/download/details.aspx?id=17718)

Now you can install SolarWinds.

Before installing Kiwi Syslog, you might also need .NET framework 3.5. For this, perform the following steps.



Programs (4)

Computer Management

Remote Desktop Services Manager

Server Manager

Share and Storage Management

Control Panel (63)

Device Manager

Color Management

Credential Manager

Manage browser add-ons

Manage network passwords

Manage file encryption certificates

Manage saved networks

Manage advanced sharing settings

Manage audio devices

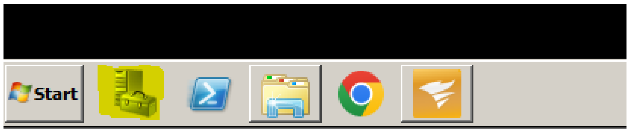
Manage Windows credentials

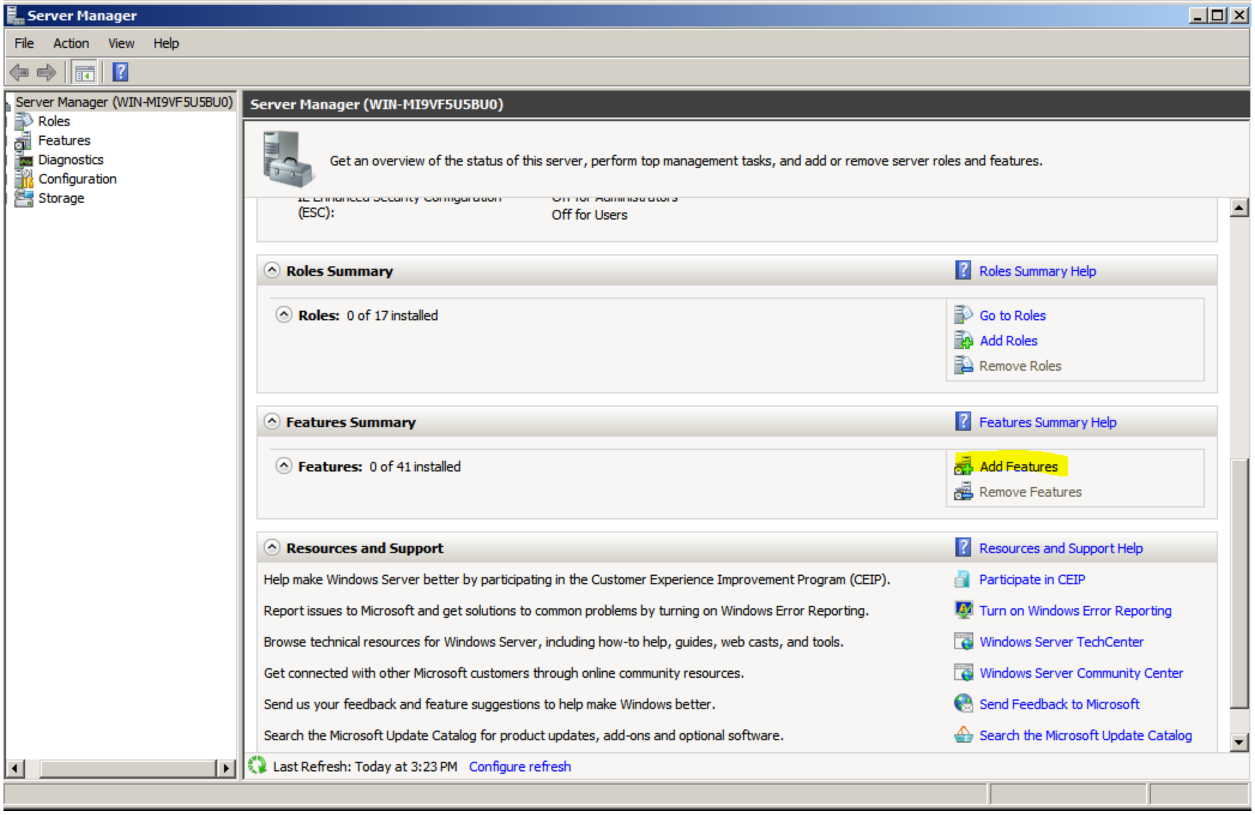
See more results

mana

Log off

or





Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

IE Enhanced Security Configuration (ESC): Off for Administrators
Off for Users

Roles: 0 of 17 installed

Features: 0 of 41 installed

Help make Windows Server better by participating in the Customer Experience Improvement Program (CEIP).

Report issues to Microsoft and get solutions to common problems by turning on Windows Error Reporting.

Browse technical resources for Windows Server, including how-to help, guides, web casts, and tools.

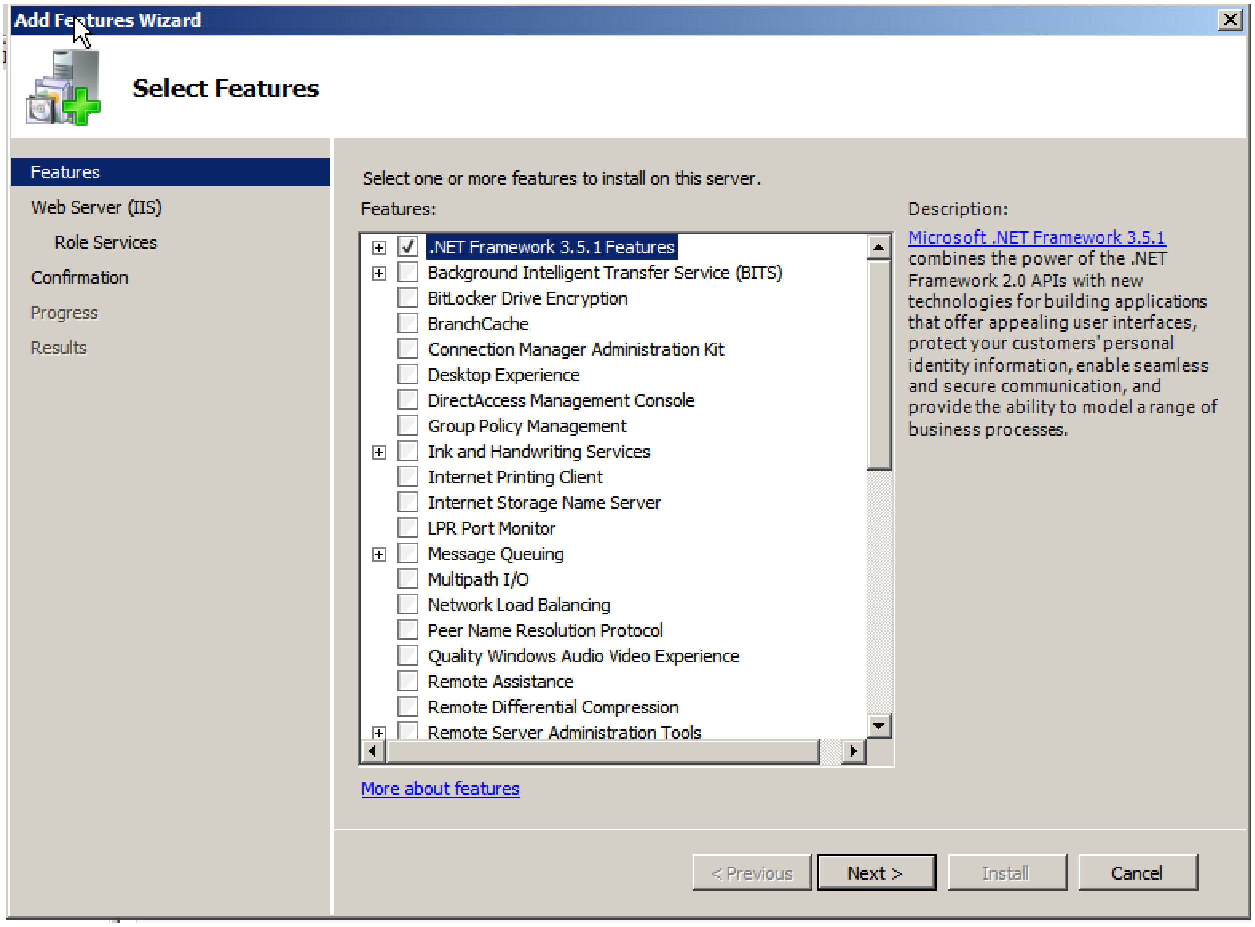
Get connected with other Microsoft customers through online community resources.

Send us your feedback and feature suggestions to help make Windows better.

Search the Microsoft Update Catalog for product updates, add-ons and optional software.

Participate in CEIP
Turn on Windows Error Reporting
Windows Server TechCenter
Windows Server Community Center
Send Feedback to Microsoft
Search the Microsoft Update Catalog

Last Refresh: Today at 3:23 PM



Add Features Wizard

Select Features

Select one or more features to install on this server.

Features:

- ☑ .NET Framework 3.5.1 Features
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BranchCache
- □ Connection Manager Administration Kit
- □ Desktop Experience
- □ DirectAccess Management Console
- □ Group Policy Management
- □ Ink and Handwriting Services
- □ Internet Printing Client
- □ Internet Storage Name Server
- □ LPR Port Monitor
- □ Message Queuing
- □ Multipath I/O
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ Remote Assistance
- □ Remote Differential Compression
- □ Remote Server Administration Tools

Description:

Microsoft .NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

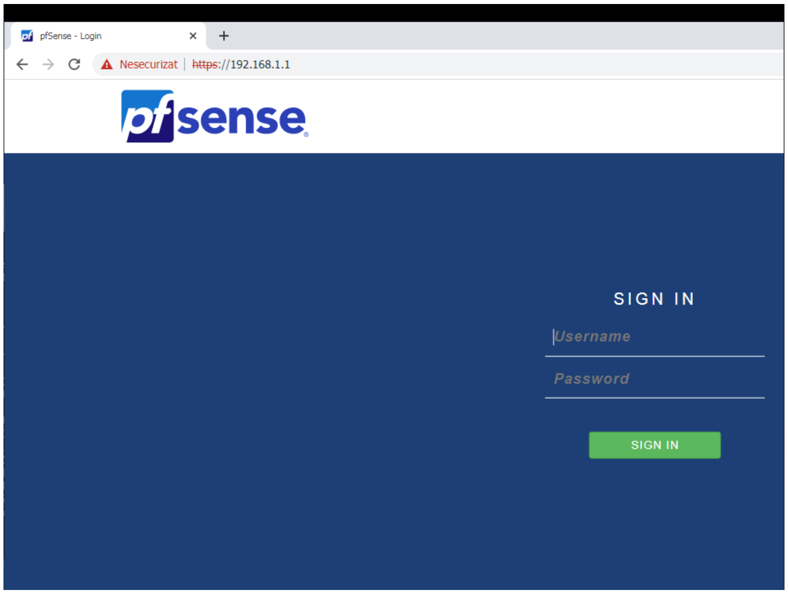
More about features

Click Next three times and the Install. After installation click Close.

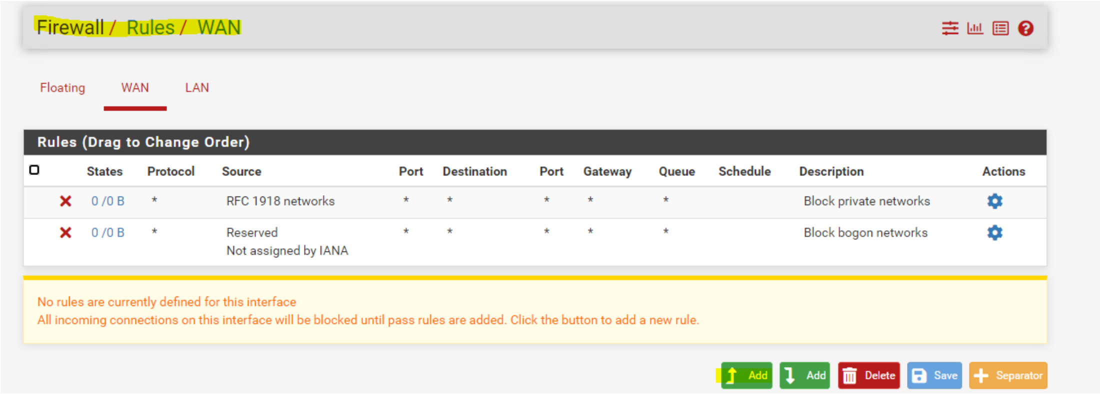
You can now install Kiwi Syslog. Select – install as an application when required.

Step 2. Make firewall settings for syslog

2.1. Connect to pfsense (Credentials pfsense: admin / pfsense)



2.2. Go to Firewall/Rules/WAN and click add to add a new rule.



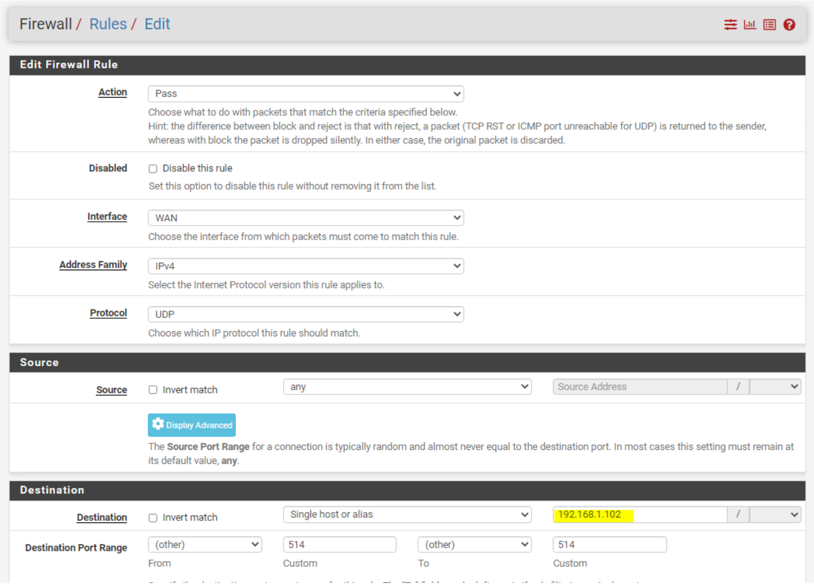
Firewall / Rules / WAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✕	0 /0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
	✕	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Perform the configurations as following. Optionally you can also add a description. When you are done click Save.



Firewall / Rules / Edit

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled □ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface WAN

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol UDP

Choose which IP protocol this rule should match.

Source

Source □ Invert match any Source Address /

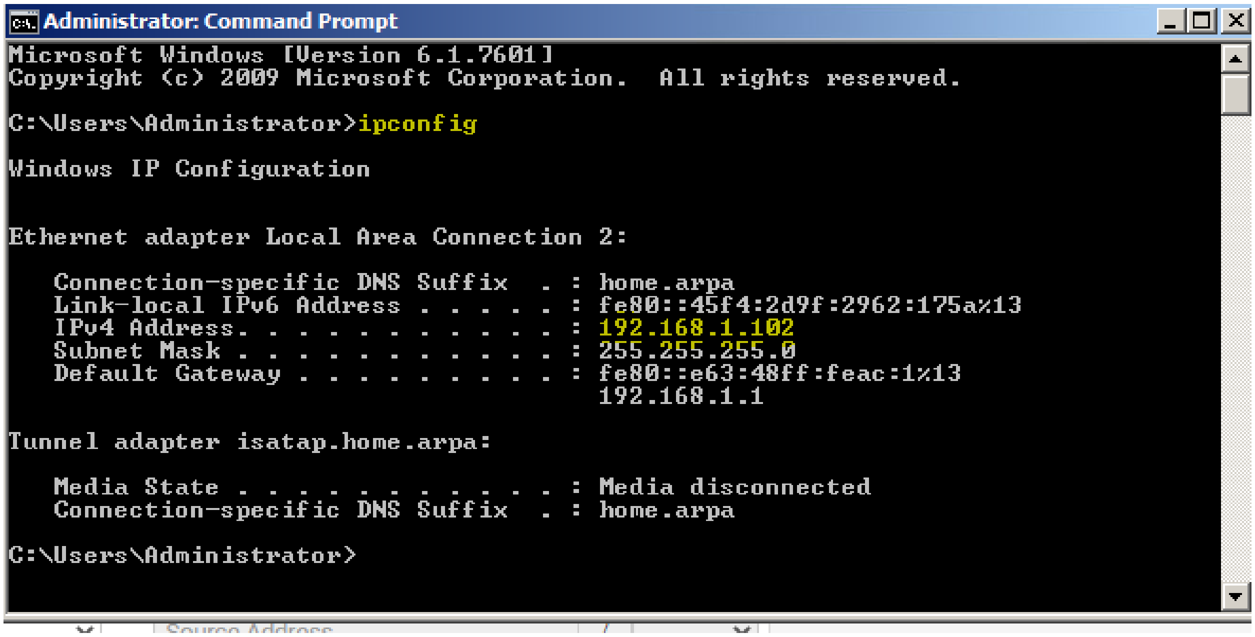
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination □ Invert match Single host or alias 192.168.1.102 /

Destination Port Range	(other)	514	(other)	514
	From	Custom	To	Custom

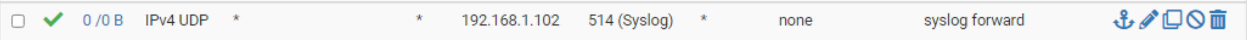
You can find the IP address of the WindowsServer using the ipconfig command:



Administrator: Command Prompt

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : home.arpa
   Link-local IPv6 Address . . . . . : fe80::45f4:2d9f:2962:175a%13
   IPv4 Address. . . . . . . . . . . : 192.168.1.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::e63:48ff:feac:1%13
                                       192.168.1.1

Tunnel adapter isatap.home.arpa:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : home.arpa

C:\Users\Administrator>
```

The new rule should look like this:



□	✓	0 /0 B	IPv4 UDP	*	*	192.168.1.102	514 (Syslog)	*	none		syslog forward

2.3. Go to Firewall / NAT / Port Forward and click add.