Дәріс №14: NAT мүмкіндіктері бар желіаралық экрандар

1) **NAT** сипаттамасы**;**
2) Open-Source NG FW **Untangle 16.1.1;**

1) **NAT** сипаттамасы**;**

NAT (Network Address Translation) - TCP-IP желілерінде IP мекенжайларын сақтауға және түрлендіруге арналған технология.

NAT IPv4 IP мекенжайларының жетіспеушілігін шешу үшін ойлап табылды. Бірнеше жыл бұрын IPv4 протоколының негізін қалаушылар интернетке қосылған барлық құрылғылар үшін 4,3 миллиард IP мекен-жайы жеткілікті болады деп сенді. Бірақ әлемде 7 миллиардтан астам адам бар екенін және көпшілігімізде бірнеше құрылғы бар екенін ескерсек, олардың жеткіліксіз болғаны анық.

Интернетке қосылған маршрутизаторға бір жалпы IP мекенжайы беріледі. Ол ғаламдық желіде көрінеді және серверлермен байланыс үшін қажет. Маршрутизаторға жергілікті түрде қосылған кез-келген құрылғыда жеке IP мекенжайлары бар, олар серверлермен тікелей "байланысуға" мүмкіндік бермейді. Бұл жерде NAT пайда болады - ол трафикті бағыттайды.

NAT қалай жұмыс істейді:

- Сіздің құрылғыңыз деректер пакеттерін жіберу арқылы серверге сұрау жібереді. Бұл пакеттерде жіберуші мен алушының IP, порт нөмірлері және қандай ақпарат сұралады;
- Трафик Nat брандмауэрімен маршрутизатор арқылы өтеді. NAT деректер пакетінің жеке IP мекенжайын жалпыға қол жетімді IP маршрутизаторына өзгертеді. Ол бұл өзгерісті атап өтеді және оны NAT бағыттау кестесіне қосады;
- Деректер пакеттері серверге жетіп, қажетті ақпаратты алады;
- Ақпарат маршрутизаторға қайтарылады. Енді Nat міндеті-ақпаратты сұраған құрылғыға қайта жіберу;
- NAT деректер пакетінің жалпы IP-ін алдыңғы жеке IP-ге өзгертеді және оны сұралған құрылғыға жібереді.

NAT қалай қорғайды?

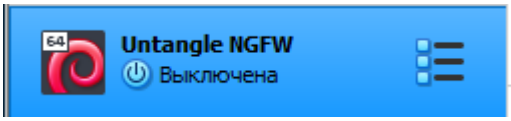
- Сіздің желіңіздегі кез-келген құрылғылардың IP-мекен-жайларын сыртқы әлемнен жасырады, олардың барлығына бір мекен-жай береді;
- Ол әрбір кіріс ақпарат пакетін құрылғыдан сұрауды талап етеді. Күтілетін хабарлар тізімінде жоқ кез келген зиянды деректер пакеті қабылданбайды;
- Кейбір брандмауэрлер рұқсат етілмеген трафикті бұғаттау үшін ақ тізімдерді қолдануы мүмкін.

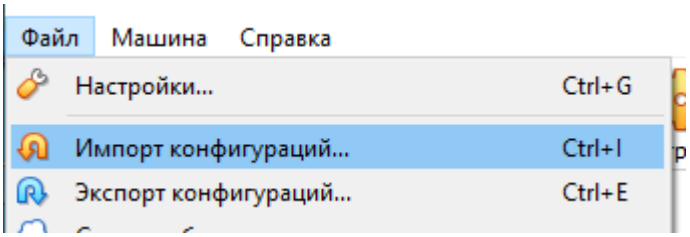
Неғұрлым күрделі шабуылдар әлі де NAT қорғанысын, әсіресе фишинг немесе әлеуметтік инженерия әдістерін қолдана алады. Алайда, бұл сіз оны пайдаланбауыңыз керек дегенді білдірмейді. NAT болмаса, кез-келген әуесқой хакерге компьютерге кіру оңай болар еді.

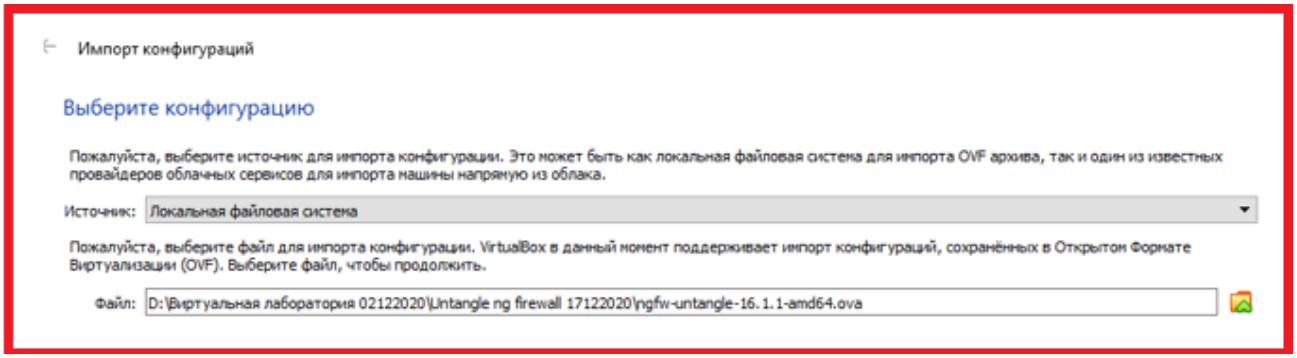
2) Open-Source NG FW **Untangle 16.1.1**

Untangle платформасы (**http://www.untangle.com)** 30-дан астам ашық бастапқы мәтін шешімдері негізінде жасалған (Metavize компаниясы ұсынған). Олардың арасында Knoppix, Snort, ClamAV, SpamAssasin, Squid және басқалары бар. Untangle жобасының мақсаты шағын және орта ұйымдарда Isa Server, SonicWall немесе WatchGuard сияқты коммерциялық шешімдерді ауыстыру болып табылады. Жаңа жобаның негізгі идеясы әкімшіге желі қауіпсіздігін нығайтуға мүмкіндік беретін бір компьютерге құралды орнату және оңай басқару. Барлық қорғаныс модульдері бар көптеген ұқсас шешімдерден айырмашылығы, Untangle-де **бастапқыда** ештеңе жоқ. Әкімші негізгі жүйені (**Untangle Gateway Platform**) орнатқаннан кейін орнатылатын өзіне қажетті қорғау модульдерін дербес таңдайды. Олардың ішінде бағыттауды, спамды сүзуді, вирусқа қарсы және spyware тексеруді, желіаралық экранды, антифишингті, шабуылдарды анықтауды, контентті қамтамасыз ететін компоненттер бар.

Орнату жолы:







Импорт конфигураций

Укажите параметры импорта

Далее перечислены виртуальные машины и их устройства, описанные в импортируемой конфигурации. Большинство из указанных параметров можно изменить двойным щелчком мыши на выбранном элементе, либо отключить используя соответствующие галочки.

Виртуальная система 1	
Имя	Untangle NGFW
Тип гостевой ОС	Debian (64-bit)
Процессор	1
ОЗУ	4096 МБ
DVD-привод	☑
USB-контроллер	☑
Сетевой адаптер	☑ Intel PRO/1000 MT Desktop (82540EM)
Сетевой адаптер	☑ Intel PRO/1000 MT Desktop (82540EM)
Контроллер (IDE)	PIIX4
Контроллер (IDE)	PIIX4
Контроллер (SATA)	AHCI
Контроллер (SCSI)	LsiLogic
Виртуальный образ диска	ngfw-untangle-16.1.1_buster_amd64_current-release161_2020-11-10t092338_affe360f2662.vmdk
Базовый каталог	C:\Users\Гульзинат\VirtualBox VMs
Основная группа	/

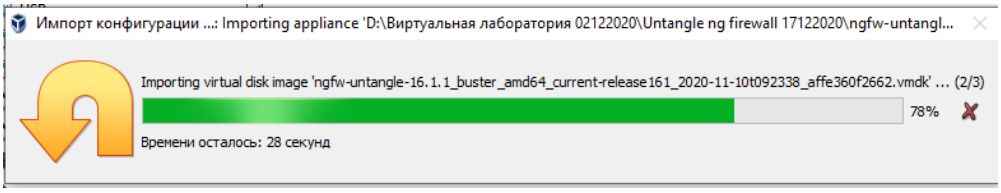
Папка машины: C:\Users\Гульзинат\VirtualBox VMs

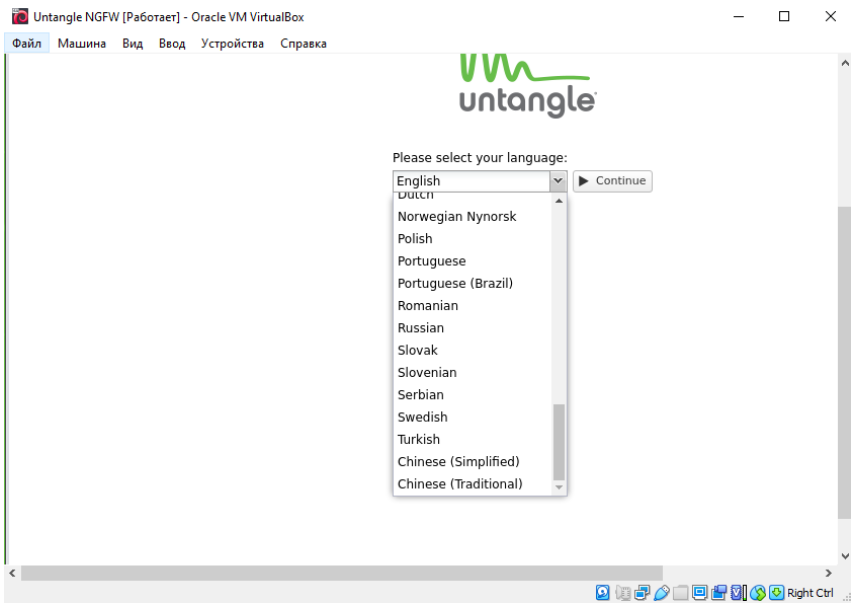
Политика MAC-адреса: Включать только MAC-адреса сетевого адаптера NAT

Дополнительные опции: ☑ Импортировать жёсткие диски как VDI

Конфигурация не заверена

По умолчанию | Импорт | Отмена





Thanks for choosing Untangle!

A wizard will guide you through the initial setup and configuration of the Untangle Server.

Run Setup Wizard

License

To continue installing and using this software, you must agree to the terms and conditions of the software license agreement. Please review the whole license agreement by scrolling through to the end of the agreement

Untangle Software License

UNTANGLE INC.

PROPRIETARY END USER LICENSE AGREEMENT

This End User License Agreement (this "Agreement") is entered into between Untangle, Inc. ("Untangle") and the person or entity ("you" or "Licensee") that purchases, receives, installs, or subscribes to the Software Product(s) (as defined below) accompanying this Agreement. If you do not agree to the terms and conditions of this Agreement, Untangle is unwilling to license the Software Product to you. Untangle reserves the right to refuse to sell subscriptions, or allow usage of, any Software

After installation, this license is available at https://www.untangle.com/legal

Disagree Agree

Configure the Server

Admin account

Choose a password for the **admin** account

Password: ••••••••••

Confirm Password: ••••••••••

Admin Email:

Administrators receive email alerts and report summaries.

Install Type

Install type determines the optimal default settings for this deployment.

Choose Type: Nonprofit

Timezone

(~UTC+06:00) Asia/Almaty

Identify Network Cards

This step identifies the external, internal, and other network cards.

Step 1: Plug an active cable into one network card to determine which network card it is.
Step 2: *Drag and drop* the network card to map it to the desired interface.
Step 3: Repeat steps 1 and 2 for each network card and then click *Next*.

Name	Device	Status	MAC Address
External	eth0	connected 1000 full-duplex Intel Corporation	08:00:27:b7:7c:8e
Internal	eth1	connected 1000 full-duplex Intel Corporation	08:00:27:a4:d3:06

Server Settings ●●○○○○○ Internet Connection

Configure the Internet Connection

Configuration Type

Auto (DHCP) **Static** **PPPoE**

Renew DHCP

Status

IP Address: 192.168.0.14

Netmask: /24 - 255.255.255.0

Gateway: 192.168.0.1

Primary DNS: 192.168.0.1

Secondary DNS:

Test Connectivity

Network Cards ●●●○○○○ Internal Network

Configure the Internal Network Interface

Router

This is recommended if the external port is plugged into the internet connection. This enables NAT and DHCP.

Internal Address: 192.168.2.100

Internal Netmask: /24 - 255.255.255.0

Enable DHCP Server (default)

Transparent Bridge

This is recommended if the external port is plugged into a firewall/router. This bridges Internal and External and disables DHCP.

Internet Connection ●●●●○●● Auto Upgrades

Automatic Upgrades and Command Center Access

Automatically Install Upgrades

Automatically install new versions of the software when available.
This is the recommended choice for most sites.

Connect to Command Center

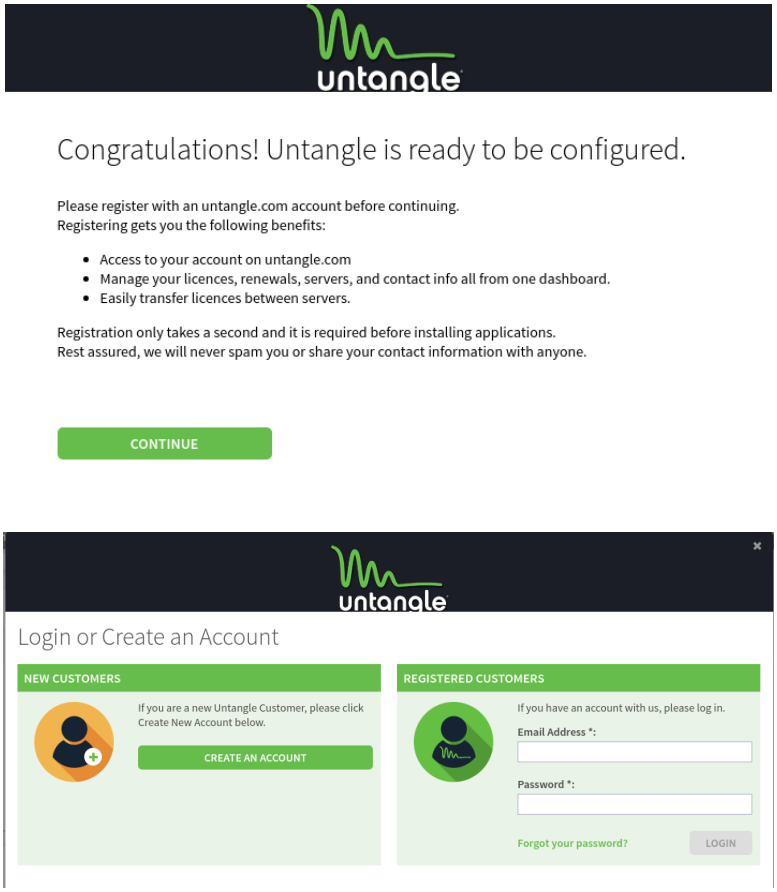
Remain securely connected to the Command Center for cloud management, hot fixes, and support access.
This is the recommended choice for most sites.

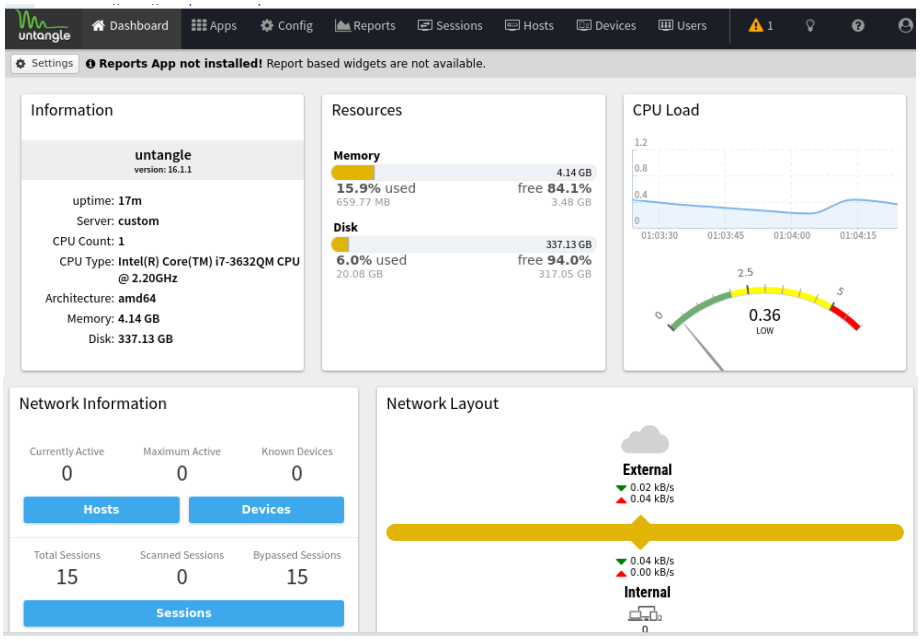
Internal Network ●●●●●●○● Finish

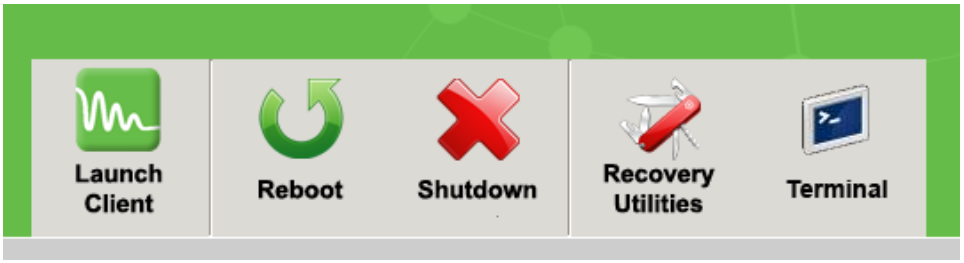
The Untangle Server is now configured.

You are now ready to configure the applications.

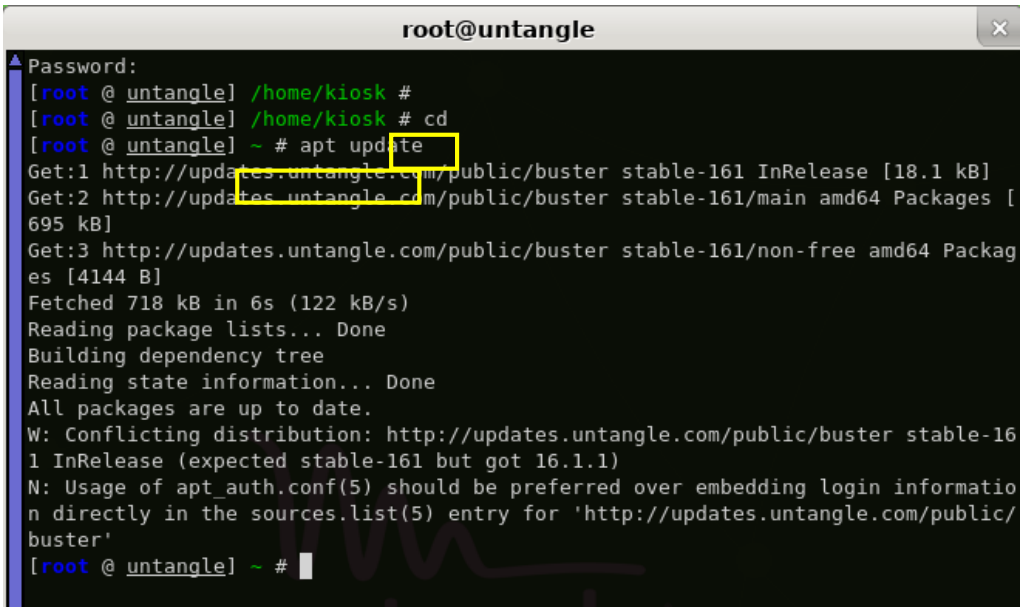
Go to Dashboard

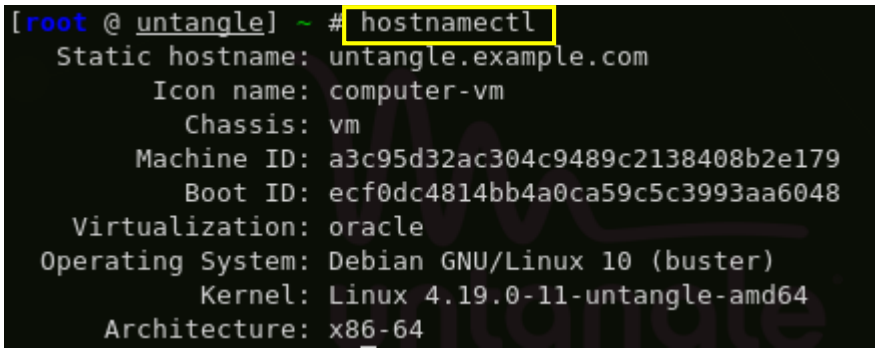

untangle
Congratulations! Untangle is ready to be configured.
Please register with an untangle.com account before continuing.
Registering gets you the following benefits:
Access to your account on untangle.com
Manage your licences, renewals, servers, and contact info all from one dashboard.
Easily transfer licences between servers.
Registration only takes a second and it is required before installing applications.
Rest assured, we will never spam you or share your contact information with anyone.
CONTINUE
Login or Create an Account
NEW CUSTOMERS
If you are a new Untangle Customer, please click Create New Account below.
CREATE AN ACCOUNT
REGISTERED CUSTOMERS
If you have an account with us, please log in.
Email Address *:
Password *:
Forgot your password?
LOGIN

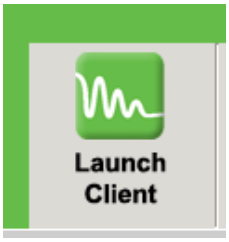

untangle
Dashboard
Apps
Config
Reports
Sessions
Hosts
Devices
Users
Settings
Reports App not installed! Report based widgets are not available.
Information
untangle
version: 16.1.1
uptime: 17m
Server: custom
CPU Count: 1
CPU Type: Intel(R) Core(TM) i7-3632QM CPU @ 2.20GHz
Architecture: amd64
Memory: 4.14 GB
Disk: 337.13 GB
Resources
Memory
4.14 GB
15.9% used
659.77 MB
free 84.1%
3.48 GB
Disk
337.13 GB
6.0% used
20.08 GB
free 94.0%
317.05 GB
CPU Load
0.36
LOW
Network Information
Currently Active
0
Maximum Active
0
Known Devices
0
Hosts
Devices
Total Sessions
15
Scanned Sessions
0
Bypassed Sessions
15
Sessions
Network Layout
External
0.02 kB/s
0.04 kB/s
0.04 kB/s
0.00 kB/s
Internal


Launch Client
Reboot
Shutdown
Recovery Utilities
Terminal


Terminal Use Warning
You will be prompted to enter the admin/root password to proceed.
WARNING:
Changes made via the command line are NOT supported and can seriously interfere with the proper operation of Untangle.
Changes made via the command line are NOT supported by Untangle and can severely limit your support options.
It is recommended to disable upgrades if any changes are made.
This feature is for advanced users only.
OK


root@untangle
Password:
[root @ untangle] /home/kiosk #
[root @ untangle] /home/kiosk # cd
[root @ untangle] ~ # apt update
Get:1 http://updates.untangle.com/public/buster stable-161 InRelease [18.1 kB]
Get:2 http://updates.untangle.com/public/buster stable-161/main amd64 Packages [695 kB]
Get:3 http://updates.untangle.com/public/buster stable-161/non-free amd64 Packages [4144 B]
Fetched 718 kB in 6s (122 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
W: Conflicting distribution: http://updates.untangle.com/public/buster stable-161 InRelease (expected stable-161 but got 16.1.1)
N: Usage of apt_auth.conf(5) should be preferred over embedding login information directly in the sources.list(5) entry for 'http://updates.untangle.com/public/buster'
[root @ untangle] ~ #


[root @ untangle] ~ # hostnamectl
Static hostname: untangle.example.com
Icon name: computer-vm
Chassis: vm
Machine ID: a3c95d32ac304c9489c2138408b2e179
Boot ID: ecf0dc4814bb4a0ca59c5c3993aa6048
Virtualization: oracle
Operating System: Debian GNU/Linux 10 (buster)
Kernel: Linux 4.19.0-11-untangle-amd64
Architecture: x86-64



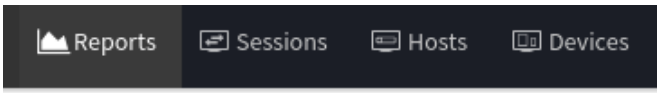
Untangle Administrator Login

localhost

admin

••••••••••

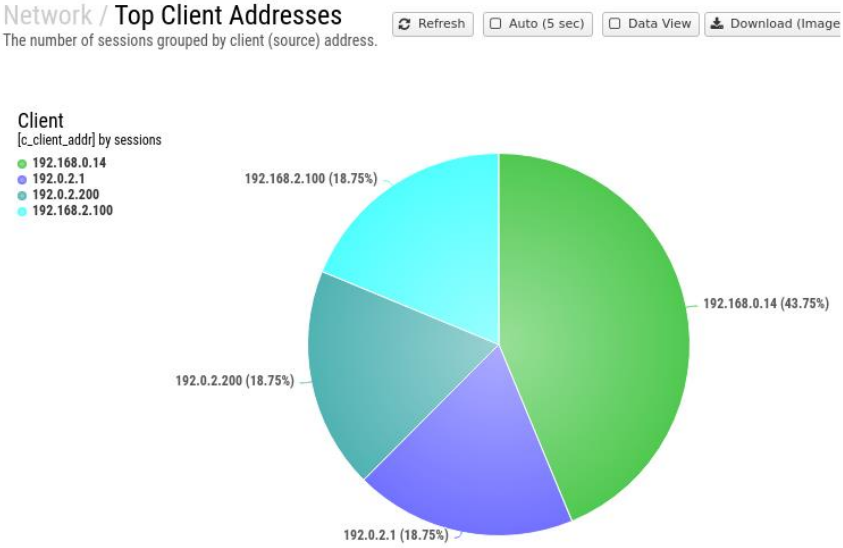
Login

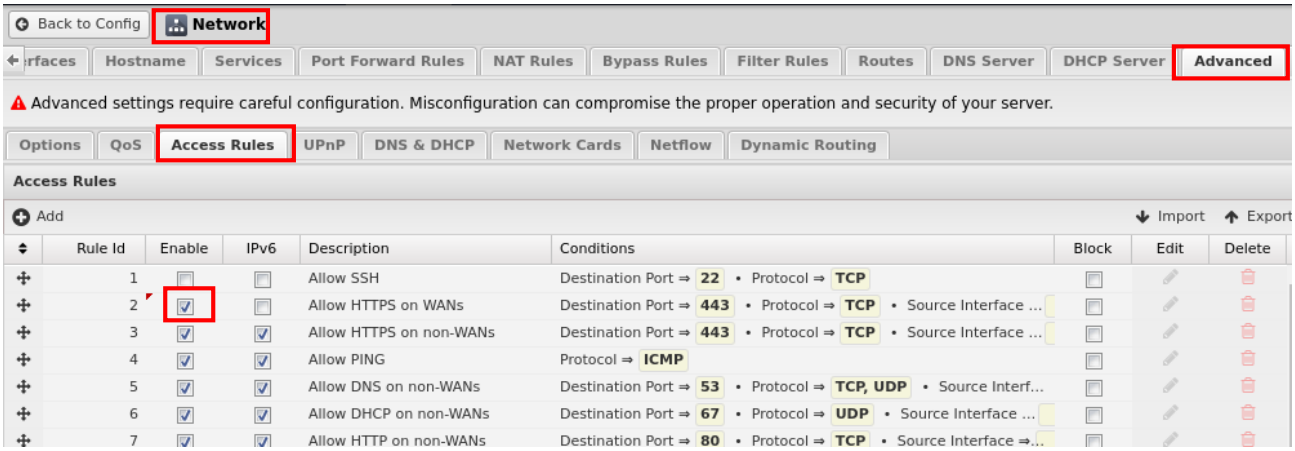


Reports App is not installed!

Please wait ...

Untangle мүмкін талдаулары





Небезопасно | ~~https~~://192.168.0.14

Ваше подключение не является закрытым

Злоумышленники могут попытаться украсть ваши данные с **192.168.0.14** (например, пароли, сообщения или кредитные карты).

NET::ERR_CERT_AUTHORITY_INVALID

Скрыть дополнительные сведения

Назад

Этому серверу не удалось доказать, что он является **192.168.0.14**. Его сертификат безопасности не является доверенным для операционной системы вашего компьютера. Причиной может быть неправильная настройка или попытка злоумышленника перехватить ваше подключение.

Перейти на 192.168.0.14 (небезопасно)