ПОДОБРЯВАНЕ НА РАБОТОСПОСОБНОСТТА И НАДЕЖДНОСТТА НА АРХИВИРАНЕТО ЧРЕЗ ***MIKROTIK***

Mikrotik в помощ на GDPR в SOHO среда

MUM София 06.2019

Да се запознаем

инж. Георги Анастасов

За мен! *Сертифициран мрежов специалист и консултант за продукти на* ***Mikrotik*** *с опит в проектиране и изграждане на малки и средни компютърни мрежи, сървъри и системи за архивиране.*

WEB: www.steadypc.com
E-mail: office@steadypc.com
GSM: +359 878806291

MikroTik MTCNA | MikroTik MTCRE | MikroTik MTCWE | MikroTik MTCUME | MikroTik MTCTCE | MikroTik MTCINE

Mikrotik в помощ на GDPR в SOHO среда

В съвременното общество, използването на компютри, мобилни устройства и интернет е в основата на всеки бизнес процес.

Обемът на събираните данни, скоростта на тяхната обработка и важността на информацията са в мащаби, които налагат създаването на организация на контрола и нивата на достъпа и надеждното съхранение на данните.

Служителите на фирмите и тяхната добра информираност за възможните заплахи, са от първостепенна важност за защитата на данните и репутацията на фирмите.

GDPR

Прилагане на GDPR регламент на Европейския Съюз 2016/679

- Важи за територията на целия ЕС
- Дава нови права на гражданите на ЕС
- Нови отговорности за фирмите
  Съхраняване на архивите
  Работоспособност на архивите
  Описание на инфраструктурата
  Отговорни лица
  Обучение на служителите

Архивиране

Загубата, унищожаването или кражбата на данни от организациите и фирмите биха довели до спиране на дейността, **загуба на доверие и пари.**

01

Допълнителна защита при архивиране
Mikrotik защита при архивиране

Повишаване на защитата на архивирането, чрез ограничаване на достъпа до архивиращото устройство.

- Описание на задачите за архивиране и съставяне на време-диаграма.
- Ограничаване на достъпа чрез забраняване на интерфейса, към който е включено архивиращото устройство.
- Ограничаване на достъпа чрез адресни листи.

Методи за реализиране – Port Knock.

Допълнителна защита при архивиране
GDPR Описание на задачите за архивиране

Описание на задачите и обема за архивиране

SERVER		
Виртуални машини		
Виртуална машина	Капацитет GB	Криптиране при архивиране
VM1	65	да
VM2	45	не
VM3	53	не
VM4	50	не
Общо GB	213	

PC		
Папки в персоналният компютър		
Потребител	Капацитет GB	Криптиране при архивиране
USER1	20	да
USER2	30	да
USER3	17	не
Общо GB	67	

Допълнителна защита при архивиране
GDPR Описание на задачите за архивиране

Съставяне на време-диаграма за разпределяне на натоварването

	Архивиращо устройство NAS						
Час	Понеделник	Вторник	Сряда	Четвъртък	Петък	Събота	Неделя
6.00			VM3				
6.30					VM4		VM2
7.00	VM1	VM1	VM1	VM1	VM1	VM1	VM1
7.30	VM2	VM2	VM2	VM2	VM2		VM3
12.00							
	USER1			USER1			
13.00	USER2			USER2			
	USER3			USER3			
14.00							
15.00							
16.00							
17.00		USER1			USER2		
		USER3			USER4		

Допълнителна защита при архивиране
Mikrotik Port Knock реализация

Port Knock в Mikrotik към портове

Port Knock чрез непоследователно обръщане към TCP или UDP портове на рутера и добавяне в адресна листа.

Port Knock в Mikrotik с дължина на пакет

Port Knock чрез ICMP обръщане към интерфейс на рутера с различна дължина на пакета и добавяне в адресна листа.

Допълнителна защита при архивиране
Mikrotik Port Knock

Необходимост от ограничаване на достъпа до архивиращото устройство.

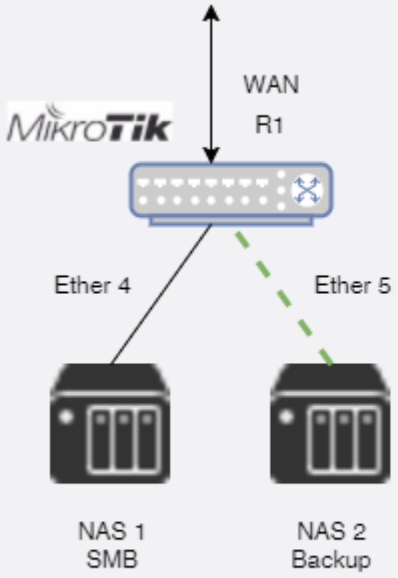


Fig 1

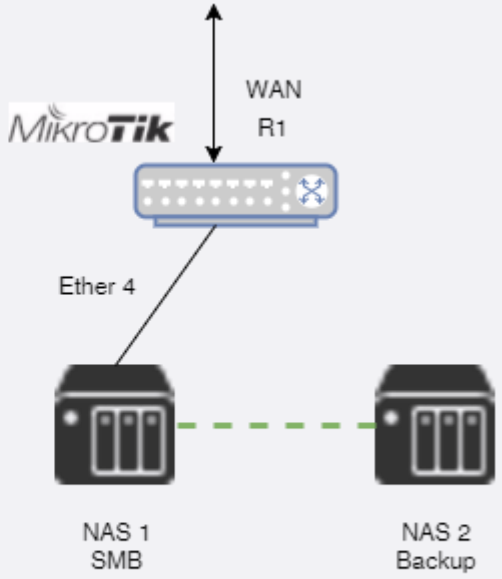
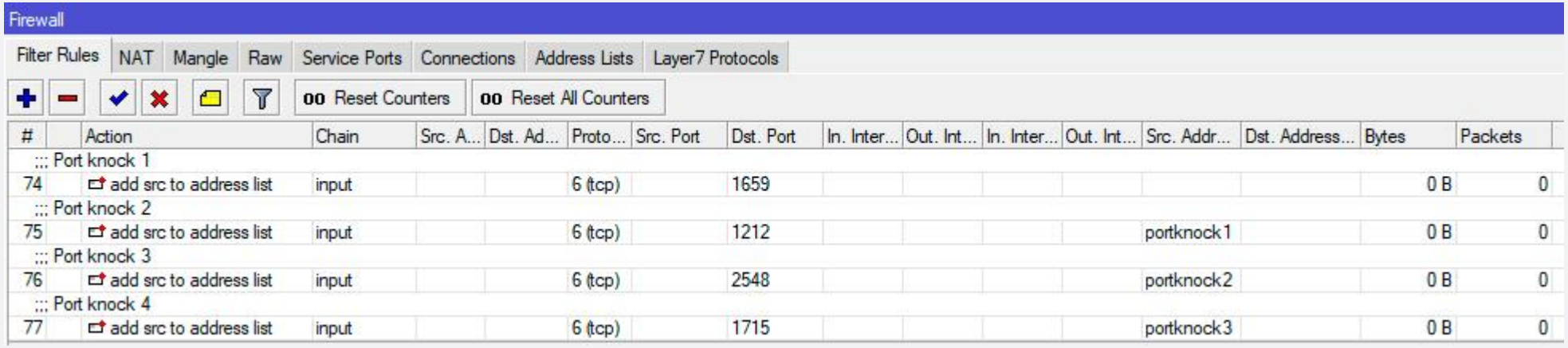


Fig 2

Допълнителна защита при архивиране
Mikrotik Port Knock

1. Port Knock чрез непоследователно обръщане към портове на рутера.

Проверката се извършва за TCP или UDP портове във веригата input на рутера.



#	Action	Chain	Src. A...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Addr...	Dst. Address...	Bytes	Packets
;;; Port knock 1															
74	add src to address list	input			6 (tcp)		1659							0 B	0
;;; Port knock 2															
75	add src to address list	input			6 (tcp)		1212					portknock1		0 B	0
;;; Port knock 3															
76	add src to address list	input			6 (tcp)		2548					portknock2		0 B	0
;;; Port knock 4															
77	add src to address list	input			6 (tcp)		1715					portknock3		0 B	0

Допълнителна защита при архивиране
Mikrotik Port Knock

Пример с добавяне в адресна листа NAS и защита от сканиране:

```
add action=accept chain=forward dst-address-list=Backup src-address-list=NAS
add action=drop chain=forward dst-address-list=Backup
add action=add-src-to-address-list address-list=portknock1 \
    address-list-timeout=1m chain=input comment="Port knock 1" dst-port=1659 protocol=tcp
add action=add-src-to-address-list address-list=portknock2 \
    address-list-timeout=1m chain=input comment="Port knock 2" dst-port=1212 \
    protocol=tcp src-address-list=portknock1
add action=add-src-to-address-list address-list=portknock3 \
    address-list-timeout=1m chain=input comment="Port knock 3" dst-port=2548 \
    protocol=tcp src-address-list=portknock2
add action=add-src-to-address-list address-list=NAS address-list-timeout=\
    1h chain=input comment="Port knock 4" dst-port=1715 protocol=tcp \
    src-address-list=portknock3
add action=add-src-to-address-list address-list=blacklist \
    address-list-timeout=1h chain=input comment=\
    "Add Router Port Scanners to blacklist" log=yes protocol=tcp psd=\
    29,3s,3,1
```

Допълнителна защита при архивиране
Mikrotik Port Knock

2. Port Knock чрез ICMP съобщение към рутера с различна дължина на пакета.

2.1 За IPV4 Проверяваме за протокол ICMP:
protocol=icmp
icmp-options=8:0

Към големината на ethernet пакета се добавя и хедъра от 28 байта(8 байта ICMP хедър и 20 байта IP хедър).
Тогава при пакет 400 байта (bytes) проверяваме за дължина 428 байта.
packet-size=428

IP Header 20 - 60 bytes + ICMP Header 8 bytes + Ethernet Frame 18 bytes (14+4crc)

2.2 За IPV6 към проверката за големина на пакета добавяме хедъра добавяме 48 байта
8 байта ICMP Echo replay хедър и 40 байта IP хедър.
protocol=icmpv6
icmp-options=128:0
packet-size=448

Допълнителна защита при архивиране
Mikrotik Port Knock

2. Port Knock чрез обръщане към порт на рутера с различна дължина на пакета.

Пример:

```
add action=add-src-to-address-list address-list=ping1 address-list-timeout=1m \
    chain=input icmp-options=8:0 packet-size=428 protocol=icmp
add action=add-src-to-address-list address-list=ping2 address-list-timeout=1m \
    chain=input icmp-options=8:0 packet-size=128 protocol=icmp \
    src-address-list=ping1
add action=add-src-to-address-list address-list=NAS address-list-timeout=1m \
    chain=input icmp-options=8:0 packet-size=328 protocol=icmp \
    src-address-list=ping2
```

Допълнителна защита при архивиране
Mikrotik Port Knock от източника на данни

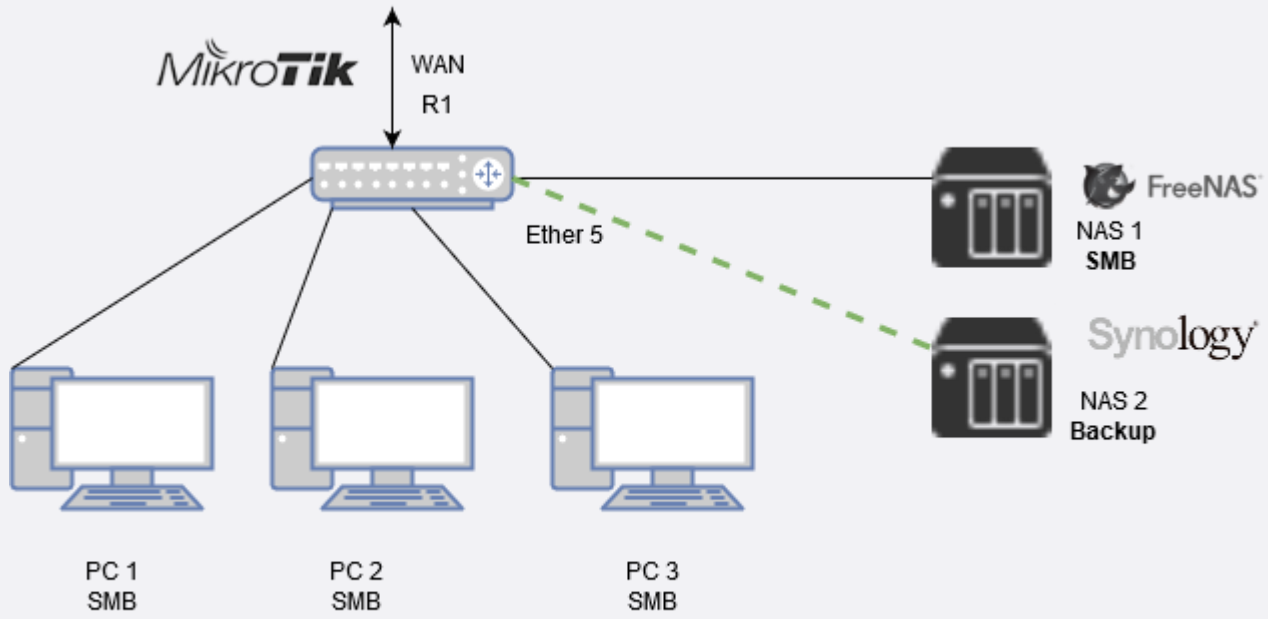


Fig 3

- SOHO мрежа със споделена папка в NAS1 и архивиране в NAS2.
- Port Knock скрипт на рутера.
- NAS port knock скрипт в NAS1.

Допълнителна защита при архивиране
Mikrotik Port Knock

Synology Port knock скрипт

1.Инсталираме допълнителни пакети.

Инсталираме Midnight Commander и SinoCli Network tools, в който се съдържа Nmap, като инсталираме SinoCommunity пакети.

Стъпка 1

Логнете се като администратор. Отворете **Main Menu** → **Package Center** → **Settings** и изберете Trust Level to *Synology Inc. and trusted publishers*.

Стъпка 2

В **Package Sources** tab, изберете Add **Name** *SynoCommunity*
Location *http://packages.synocommunity.com/* изберете **OK.**

Стъпка 3

Отворете **Package Center** и в **Community** tab инсталирайте Midnight Commander и SinoCli Network tools.

Допълнителна защита при архивиране
Mikrotik Port Knock

Synology Port knock скрипт

2.Създаваме скрипт файл с име knock.sc

- Създаваме папка */volume 1/scripts*
- Може да използваме Sinology File Station.
- Създаваме празен файл за скрипта nano */volume 1/scripts*/knock.sh

Поставяме командите във файла.

3. За Port knock използваме команди на Nmap, който е наличен за Windows, Linux, MacOS.

https://nmap.org/

Команди в Nmap:
nmap 192.168.0.1 -p1622;
nmap 192.168.0.1 -p1312;
nmap 192.168.0.1 -p2348;
nmap 192.168.0.1 -p1913

Допълнителна защита при архивиране
Mikrotik Port Knock

Synology Port knock скрипт

4.Поставяме командите в скрипта.
Ако работим в Windows, може да използваме Notepad++. За да работи правилно скрипта в меню Edit избираме EOL Conversion → Unix (LF)
Копираме командите. Поставяме във файла с Shift + Insert

5. Сменяме правата на файла.
chmod u+x /volume1/scripts/knock.sh

6. Стартирайте ръчно скрипта, за да проверите работоспособността му ./knock.sh

7. Добавяне на скрипта в Synology Task Scheduler custom script, като укажете времето за стартиране и пътя /volume1/scripts/knock.sh

Допълнителна защита при архивиране
Mikrotik Port Knock

FreeNAS Port knock скрипт

1.Създаваме скрипт файл с име knock.sc

- Създаваме папка */bin/sh*
  mkdir bin/sh
- Създаваме празен файл за скрипта - nano bin/sh/knock.sh

2. За Port knock използваме команди на Netcat, който е наличен за Windows, Linux, MacOS.
http://netcat.sourceforge.net/

Команди в Netcat:
nc -z 192.168.0.1 1659;
nc -z 192.168.0.1 1212;
nc -z 192.168.0.1 2548;
nc -z 192.168.0.1 1715
За сканиране на порт е използвана опцията -z, а -v , която дава детайлна информация за порта.

Допълнителна защита при архивиране
Mikrotik Port Knock

FreeNAS Port knock скрипт

3. Поставяме командите в скрипта.

- Ако работим в Windows, може да използваме Notepad++. За да работи правилно скрипта в меню Edit избираме EOL Conversion → Unix (LF)
- Поставяме във файла с Shift + Insert

4. Сменяме правата на файла.

chmod u+x /mnt/bin/sh/knock.sh

5. Стартирайте ръчно скрипта, за да проверите работоспособността му ./knock.sh

6. Добавяне на скрипта в FreeNAS Cron Jobs.

7. Ако не желаете да работите със скриптове , може да зададете във FreeNAS Cron Job. командата:

nc -z 192.168.0.1 1622;nc -z 192.168.0.1 1312;nc -z 192.168.0.1 2348;nc -z 192.168.0.1 1913

Допълнителна защита при архивиране
Mikrotik Port Knock

Windows Port Knock скрипт

1.Стартиране на скрипт в task scheduler.

Пример с ICMP ping с дължина на пакета 400 байта и адрес на рутера 192.168.0.1

Създаваме файл knock.bat и поставяме следните команди:

```
ping -f -n 1 -l 400 192.168.0.1
ping -f -n 1 -l 100 192.168.0.1
ping -f -n 1 -l 300 192.168.0.1
```

-f -Do not fragment packet (IPv4 only)
-n - number of echo requests to send
-l - send buffer size

Допълнителна защита при архивиране
Mikrotik Port Knock и Hypervisor

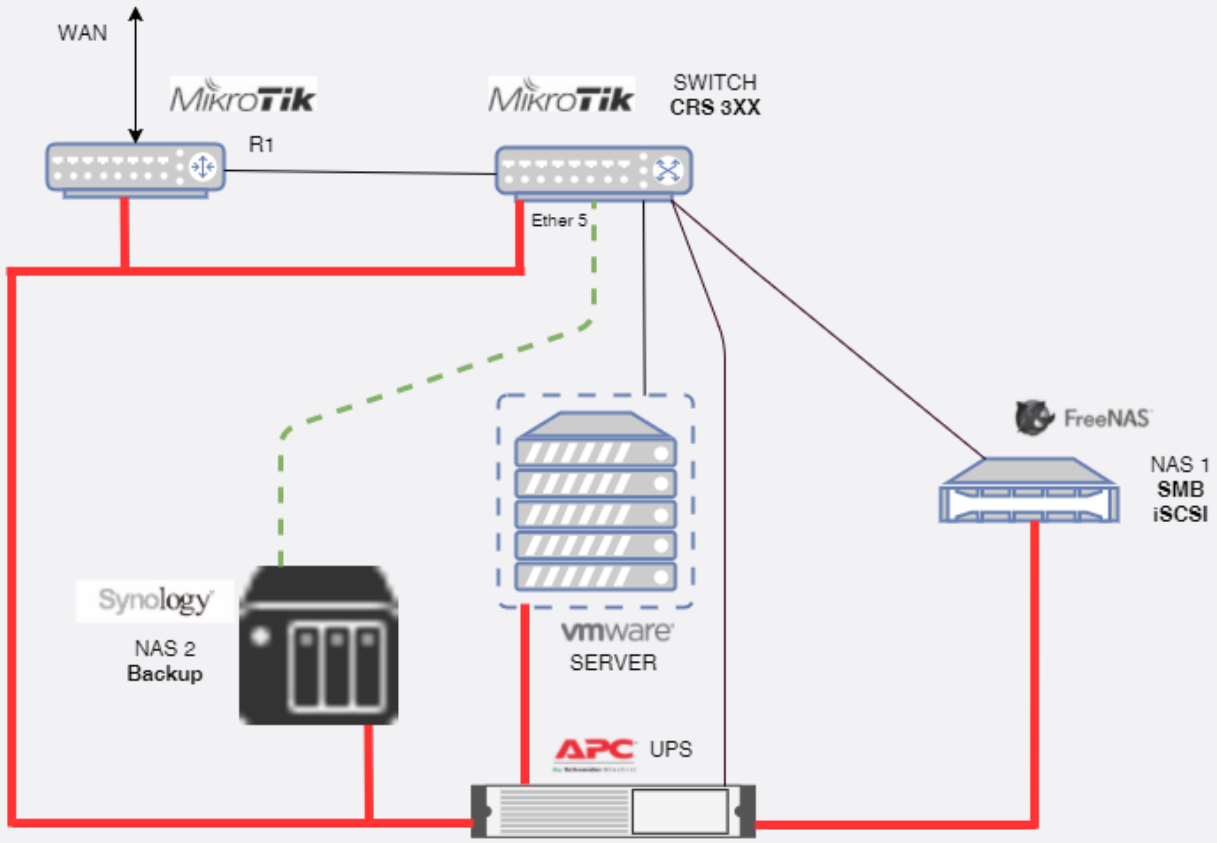


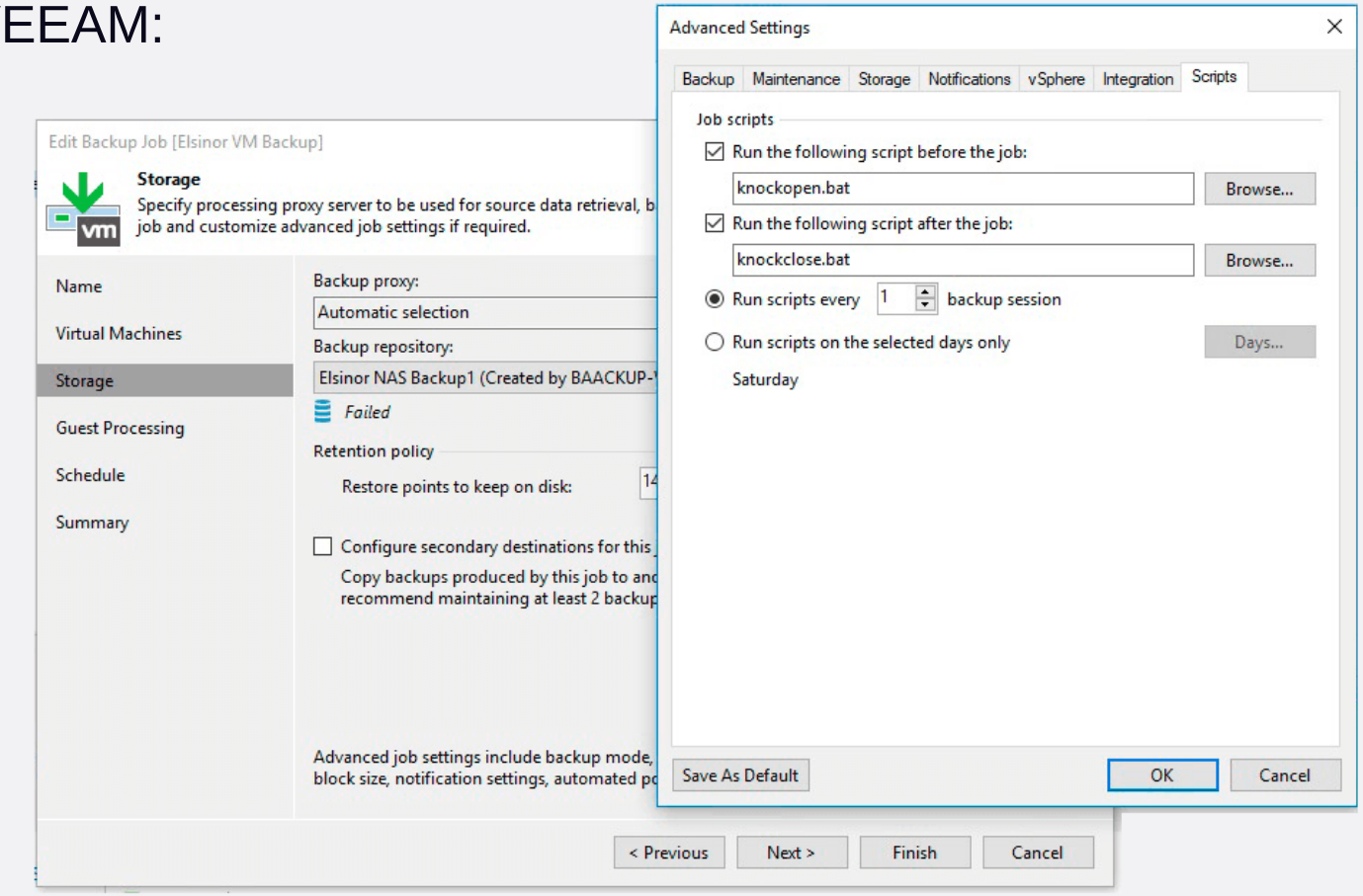
Fig 4

- SOHO мрежа със споделена папка в NAS1 и архивиране в NAS2.
- Port Knock скрипт на рутера.
- NAS port knock скрипт в NAS1.
- Port Knock скрипт в приложения.

Допълнителна защита при архивиране
Mikrotik Port Knock в приложения за архивиране

2. Стартиране на скрипт в приложението за архивиране.

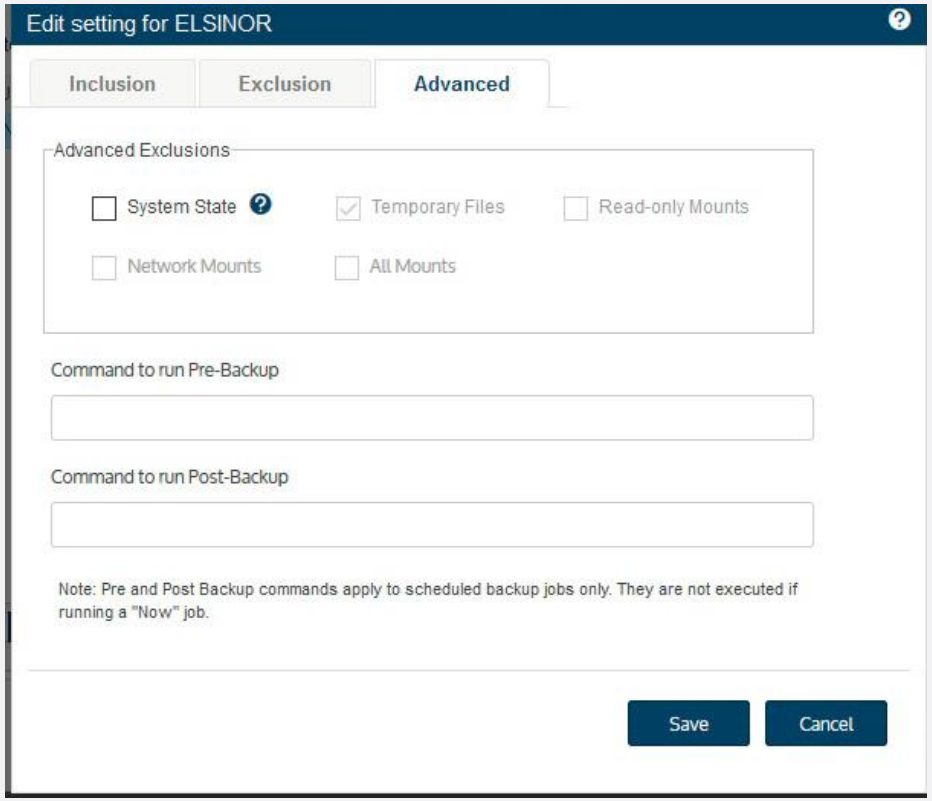
2.1 Пример VEEAM:



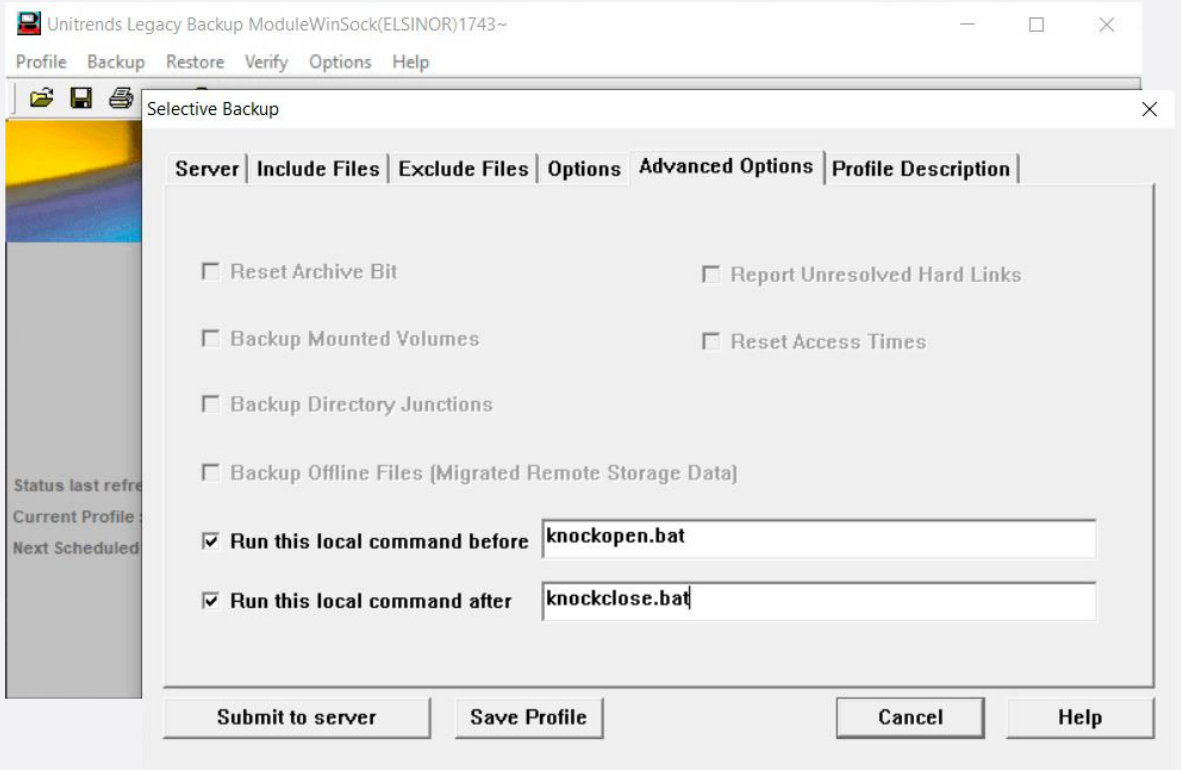
Допълнителна защита при архивиране
Mikrotik PortKnock

2.2 UNITRENDS

Virtual Appliance 1TB Free:



Windows Client:



Допълнителна защита при архивиране
Mikrotik стартиране на скриптове

Стартиране на скриптове с Port Knock

Цел: Разрешаване и забраняване на интерфейси към NAS.

- Създаване на bridge loopback – винаги е стартиран!
- Създаване на firewall правило за блокиране на адрес от адресна листа “turn-on”.
- Firewall port knock правила за добавяне в адресна листа “turn-on” на loopback dst адреса.
- Следене на loopback адреса чрез инструмента netwatch.
- Стартиране на скрипт от netwatch при отпадане на loopback.

Посредством скрипта, можете да забраните или разрешите интерфейса, към който е свързано архивиращото устройство.

Допълнителна защита при архивиране
Mikrotik стартиране на скриптове

```
# Creating loopback address
/interface bridge add name=loopback
/ip address add address=10.10.100.1 interface=loopback network=10.10.100.1

# Firewall rule to block addresses in “turn-on” address list
/ip firewall filter
add action=drop chain=input comment="turn-on" dst-address=10.10.100.1 src-address-list=turn-on

# port knock to start script
add action=add-src-to-address-list address-list=portknock1 \
    address-list-timeout=1m chain=input comment="Port knock 1" dst-port=1622 \
    protocol=tcp
add action=add-src-to-address-list address-list=portknock2 \
    address-list-timeout=1m chain=input comment="Port knock 2" dst-port=1312 \
    protocol=tcp src-address-list=portknock1
add action=add-src-to-address-list address-list=portknock3 \
    address-list-timeout=1m chain=input comment="Port knock 3" dst-port=2348 \
    protocol=tcp src-address-list=portknock2
add action=add-dst-to-address-list address-list=turn-on address-list-timeout=6s \
    chain=input comment="Port knock turn on script" dst-port=4444 protocol=tcp \
    src-address-list=portknock3 dst-address=10.10.100.1

# Creating loopback address
/tool netwatch add comment="turn-on" down-script=":log warning ("SCRIPT IS STARTED");" host=10.10.100.1 interval=5s
```

Допълнителна защита при архивиране
Mikrotik стартиране на скриптове

Стартиране на скриптове по SNMP

- Стартираме snmpwalk от компютър.

```
# snmp walk that return oid of scripts
snmpwalk -v2c -cpublic 192.168.0.1 1.3.6.1.4.1.14988.1.1.8
```

- Стартираме snmpget от компютър.

```
# Starting scripts without authentication and security
snmpget -v2c -cpublic 192.168.0.1 1.3.6.1.4.1.14988.1.1.18.1.1.2.1
```

- Стартираме snmp-get от RouterOS.

```
# Starting scripts without authentication and security
tool snmp-get community=public oid=1.3.6.1.4.1.14988.1.1.18.1.1.2.1 version=1 address=192.168.0.1
```

*snmp-get все още не може да се използва в скриптове!

Не се препоръчва стартирането на скриптове чрез SNMP без автентикация и криптиране!

Управление на работоспособността на сървърно оборудване

02

Автоматичното спиране и стартиране
Предотвратява загуба на данни и гарантира работоспособност на конфигурациите.

Управление на работоспособността
Методи за изключване на оборудването

Управление чрез USB

Мониторинга и изключването се осъществяват с USB кабел между UPS и сървъра или NAS устройството.

Управление по LAN

Изисква комуникационна карта инсталирана в UPS и софтуер за управление на изключването на сървъри и NAS.

Управление на работоспособността
Методи за изключване на оборудването

- Софтуер за управление на изключването на виртуални машини Powerchute network shutdown За UPS APC .

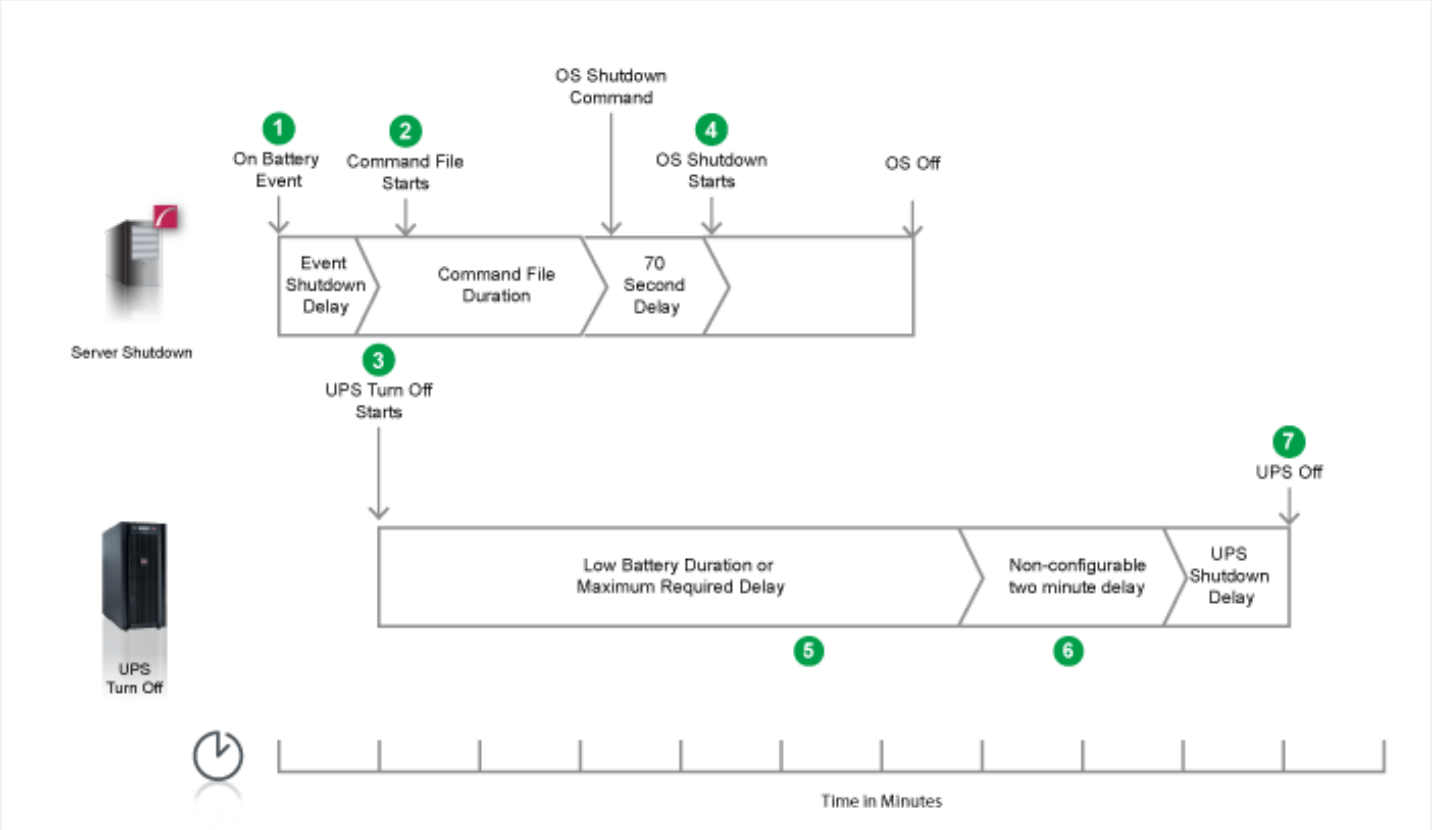
- Настройваме хипервайзора за автоматично включване и изключване на виртуалните машини.

- Задаване на закъснение в последователността при изключване на виртуалните машини от хипервайзора.

- Съставяне на време-диаграма на изключването.

Управление на работоспособността
Методи за изключване на оборудването

- Време-диаграма за управление на изключването на виртуални машини при APC Powerchute network shutdown.



Управление на работоспособността
Методи за стартиране на оборудването

Събуждане със закъснение с цел стабилност на мрежовото напрежение, след спиране на захранването или токови удари.

- Наличие на UPS защитаващ оборудването и Mikrotik рутер.
- Допълнителен рутер без UPS захранване.
- Архивиращи устройства и сървъри с мрежови карти, поддържащи Wake On Lan (WOL).
- Списък с MAC адреси.
- Предварителен план за поредността на стартиране на устройствата и времевите интервали на изчакване.

Управление на работоспособността
Методи за стартиране на оборудването

Пример:
Server1 - сървър с VMWare хост и VEEAM.
NAS1 - iSCSI за Server1 и SMB за споделяне на файлове.
NAS2 – за архивиране на NAS1 и Server1.

Стъпки
- Първо изчакваме 15 минути, за да сме сигурни, че няма да има допълнителни спирания на тока.
- Проверяваме работоспособността чрез ping на Layer3 устройство, което не е свързано към UPS.
- Може да проверим и OID на UPS по SNMP за входното напрежение.

Стартираме NAS2, изчакваме 2минути, стартираме NAS1, изчакваме 5 минути и стартираме Server1.

Управление на работоспособността
Методи за стартиране на оборудването

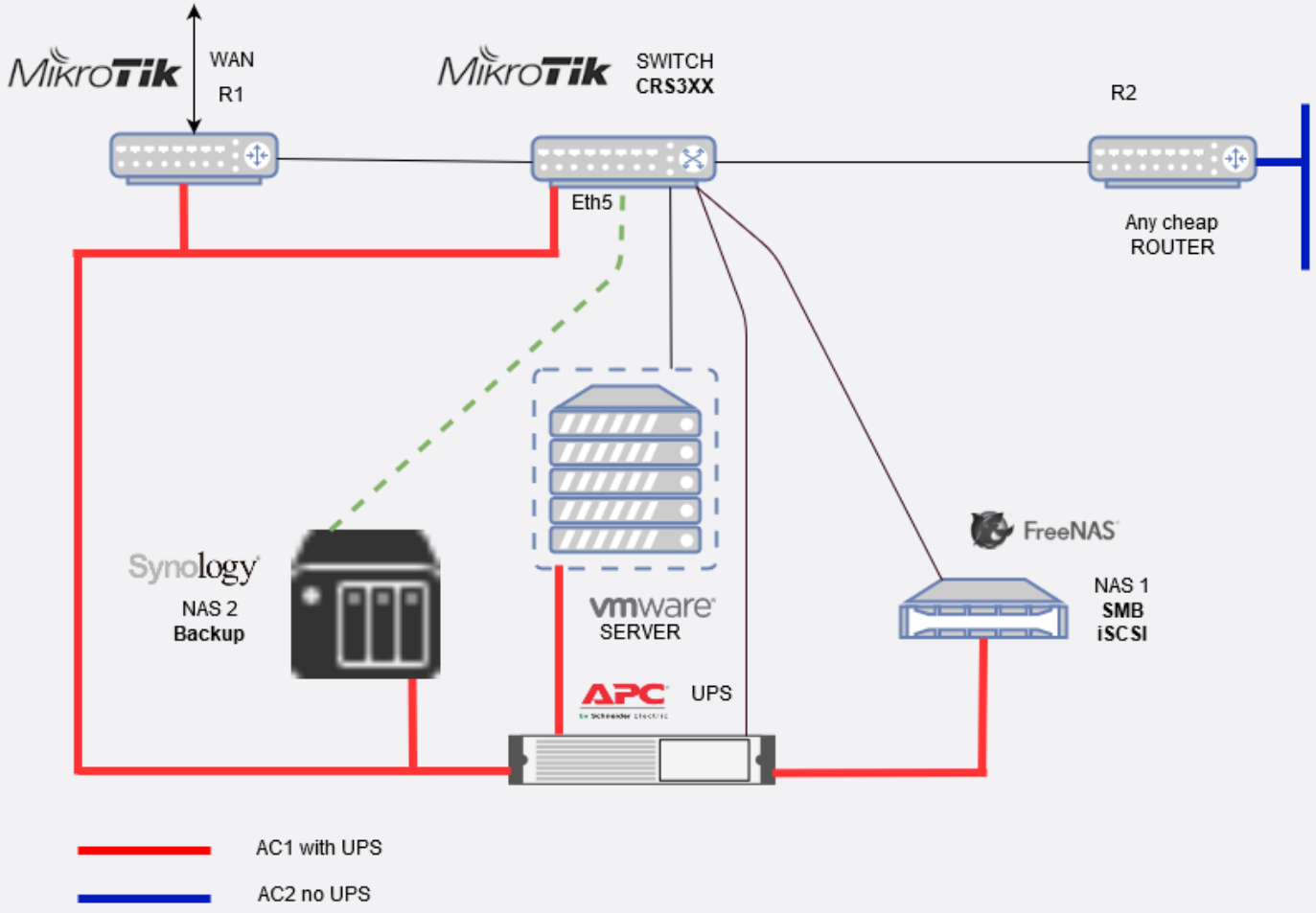


Fig 5

Управление на работоспособността
Методи за стартиране на оборудването

Примерен скрипт за проверка за стабилно захранващо напрежение 15 минути след възстановяване на захранването и единична загуба на ping:

```
# WOL for configuration with server, UPS and router2 without UPS 192.168.0.210

# ------------Declaration of variables--------------
#Interface from which you will ping
:global InterfaceR2 bridge1;
# IP address of router which is not connected to UPS
:global PingTarget 192.168.0.210;
#Maximum Pings in short test
:global ShortTest 20;
# Maximum failed pings in short test
:global PingResult 0;
:global ON 1;
# Number of pings with good AC input
:global PowerGood 1000;
:global PingShort 0;
# wait 20sec until router2 boot
:delay 20;
```

Управление на работоспособността
Методи за стартиране на оборудването

```
# -------------Wait 15 Min steady AC Power supply--------------
while ($ON<$PowerGood) do={
# wait 1 sec for steady ping
:delay 1;
#send ping command to router which is not connected to UPS
:set PingResult [/ping $PingTarget count=1 interface=$InterfaceR2];
#If ping is misses then start mini cycle  with ShortTest cycles
:put $PingResult;
:if ($PingResult=0) do={
:set PingShort [/ping $PingTarget count=$ShortTest interface=$InterfaceR2];
:put $PingShort;
:if ($PingShort<16) do={:set $ON 0}
}
:set $ON ($ON+1);
:put $ON;
}
```

Управление на работоспособността
Методи за стартиране на оборудването

Чрез SNMP следене на входното напрежение на UPS.

Скрипт „upsapc” с OID на UPS по SNMP. UPS IP адрес 192.168.0.220 SNMPv3

UPS APC OID за входно напрежение 1.3.6.1.4.1.318.1.1.1.3.3.1.0
* За да получим правилното напрежение, трябва да разделим на 10

1. При изключване на NAS1 On Shutdown стартираме knock скрипт, който от своя страна стартира скрипта “upsapc” на Mikrotik рутера.

tool snmp-get community=public oid= 1.3.6.1.4.1.318.1.1.1.3.3.1.0 version=1 address=192.168.0.220

2. Проверяване на входното напрежение на UPS на 1 секунда

3. При наличие на правилно входно напрежение за 1000s , стартираме събуждането на устройствата.

*snmp-get работи в CLI, но все още не може да се използва в скриптове!

Методи за стартиране на оборудването

Събуждане на оборудването

Събуждане по мрежата чрез Mikrotik рутер чрез “Wake on LAN”.

```
tool wol mac=XX:XX:XX:XX:XX:XX

tool wol interface=ether1 mac=XX:XX:XX:XX:XX:XX
```

Поставяйте коментари на редовете с MAC адреси за събуждане!

Методи за стартиране на оборудването

Изисквания събуждане по мрежата чрез “Wake on LAN”

Разрешаване на WoL.

- Jumper на дънната платка.
- В BIOS на компютъра.
- В операционната система на NAS или сървъра.

За Sinology NAS, трябва да разрешите в DSM Control Panel → Hardware & Power → Power recovery → Enable WOL on LAN

Управление на работоспособността
Методи за стартиране на оборудването

Последователно събуждане на оборудването с добавена пауза 120 и 180 sec.

```
# ------------Start Wake on LAN of Servers and NAS--------------
#Start NAS2
tool wol mac=00:11:32:99:76:ce
:delay 120;
#Start NAS1 with iSCSI and SMB
tool wol mac=00:fd:45:fd:4e:50
:delay 180;
#Start Server1
tool wol mac=08:9e:01:87:f3:88
```

Методи за стартиране на оборудването

Събуждане на оборудването чрез SSH в IPMI* сървърен интерфейс.

1. Изисквания

- Mikrotik pakages: *system* и *security* трябва да бъдат инсталирани.
- Създаване на потребител в рутера специално за SSH събуждането.
- Създаване на IPMI потребител за SSH събуждането.

*IPMI, ILO, iDRAC, BMC……

Методи за стартиране на оборудването

2. Генериране на SSH ключове – чрез Linux компютър

- ssh-keygen -t dsa
- Ключовете се записват в /home/user/.ssh/id_dsa

*Не забравяйте да оставите passphrase непопълнена, защото ключовете ще се използват в скрипт.

*Linux добавя името на потребителя, който създава ключа в края на публичния ключ. Поради това потребителя в ключа, трябва да се промени с този създаден в рутера!

- Запишете ключовете в Mikrotik рутера – по FTP
- Инсталирайте частния и публичния ключ в рутера за потребителя „ssh-wol“

user=ssh-wol

/user ssh-keys private import private-key-file=id_dsa public-key-file=id_dsa.pub user=ssh-wol

Методи за стартиране на оборудването

2. Инсталирайте публичния SSH ключ в IPMI на сървъра.

В повечето случаи, ключът се добавя чрез посочване в графичния интерфейс.

3. Създайте скрипт за събуждане на сървъра.

/system ssh 192.168.0.202 user=ssh-wol command="power on“

SSH командата работи в CLI, но не работи в скрипт!

SSH тунели

Удобни за тестване и работа с отдалечени бази данни, chatbot и cloud приложения

SSH тунелите могат да се реализират успешно с Mikrotik Router OS.

Basic SSH

ssh user@remote-server.com

remote-server.com – SSH сървър или IP адрес

user – потребител в сървъра

SSH тунели

SSH local port forwarding

ssh -L <LocalPort>:<RemoteHost>:<RemotePort> user@<RemoteServer>

Пример:
ssh **-L 6000:restricted-domain.com:443** user@remote-server.com

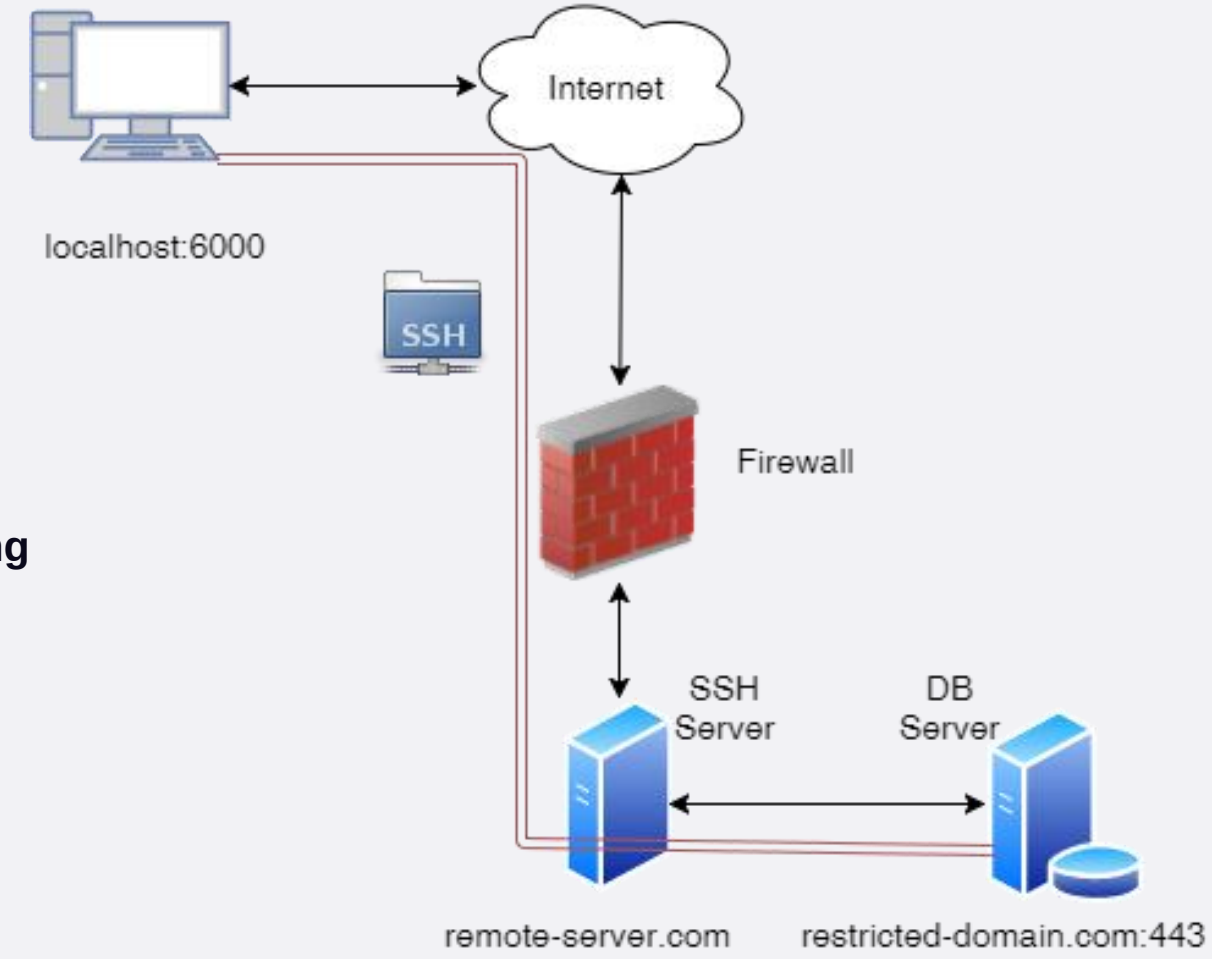
Този тунел позволява препращането на SSH заявки:
От **localhost:6000**
Към **restricted-domain.com:443** през **remote-server.com**

Този метод позволява свързването към отдалечена база данни, която има рестрикции за достъп само от локалната си мрежа. Това може да стане като се изгради SSH тунел до друг сървър от локалната мрежа, който има достъп до сървъра с базата данни.

Управление на работоспособността
Методи за защита на оборудването

SSH тунели

SSH local port forwarding



SSH тунели

SSH Remote port forwarding

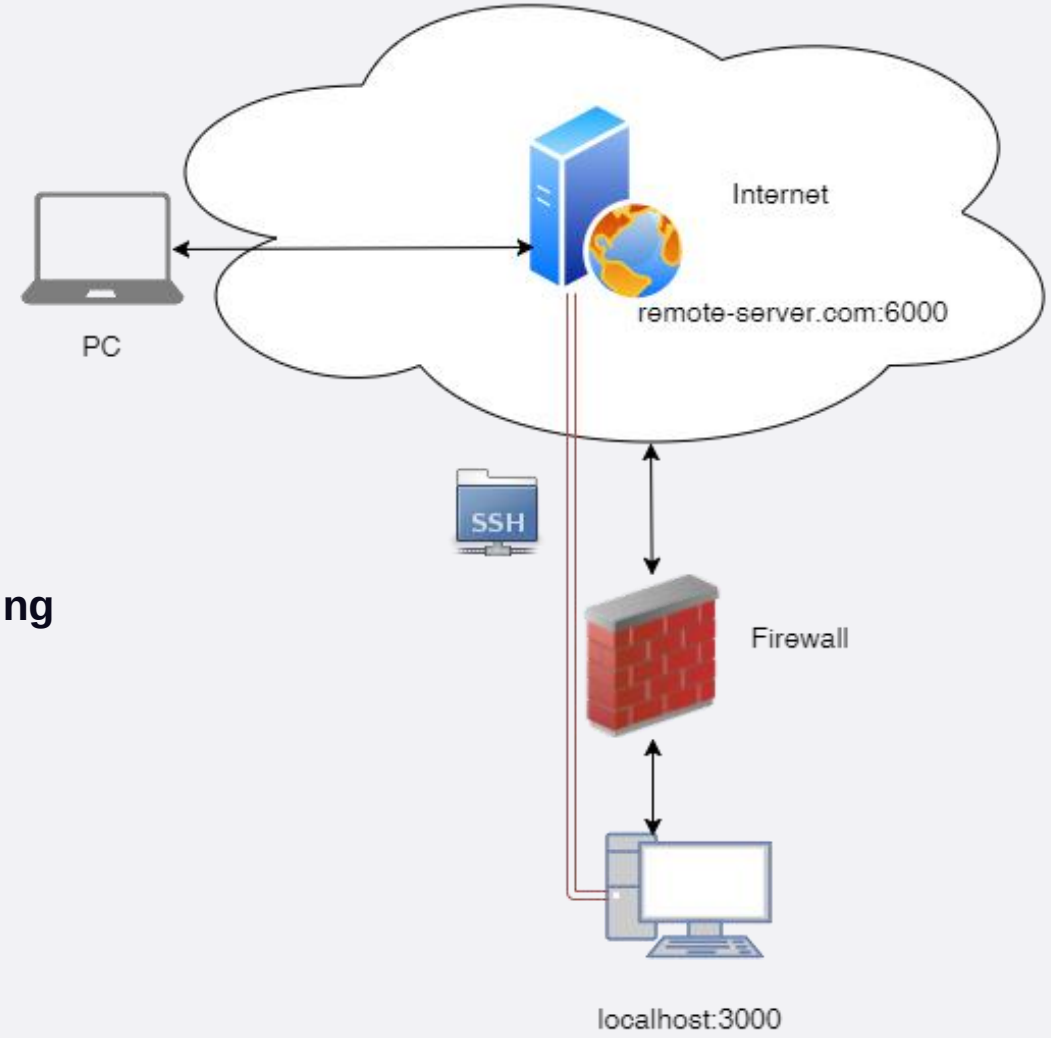
ssh -R <RemotePort>:<LocalHost>:<LocalPort> user@<RemoteServer>

Пример:
ssh **-R 6000:localhost:3000** user@remote-server.com

Този тунел позволява препращането на SSH заявки:
От **remote-server.com:6000**
Към **localhost:3000**

Този тунел позволява изграждане на SSH връзка към Cloud server или VPS, която да пренасочи трафика към локалната машина. По този начин заявките към публичен website или услуга с реален адрес, се пренасочват към локалната машина криптирано през NAT и Firewall.

Управление на работоспособността
Методи за защита на оборудването



SSH тунели

SSH Remote port forwarding

Методи за защита на оборудването

SSH сигурност при Mikrotik

1. Забраняване на услугата SSH.

/ip service set ssh disabled=yes
/ip ssh set forwarding-enabled=no

2. Проверка на L7 за SSH връзки.

/ip firewall layer7-protocol add name=SSH regexp="^ssh-[12]\\\\.[0-9]"
/ip firewall filter add action=drop chain=forward comment="Drop SSH Traffic" disabled=no layer7-protocol=SSH protocol=tcp

SSH портовете могат да бъдат произволни в обхвата от 1 до 65535 с изключение на резервираните според IANA.

L7 Позволява проверка независимо от използваният порт за връзка.

Ограничаването на SSL връзките е едно от основните изисквания при стандарт за сигурност PCI DSS.

03

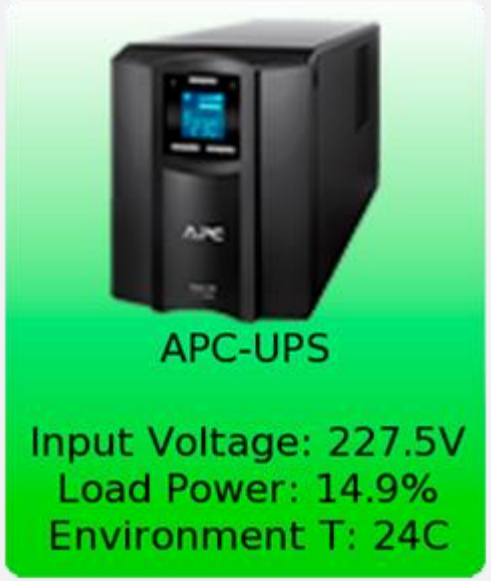
Управление на работоспособността

SNMP мониторинг на захранването.
Уведомления.

Управление на работоспособността
Методи за мониторинг на оборудването

- DUDE за следене по SNMP на параметрите на UPS.

[Device.Name]
[device_performance()][Device.ServicesDown]
Input Voltage: [oid("1.3.6.1.4.1.318.1.1.1.3.3.1.0")/10]V
Load Power: [oid("1.3.6.1.4.1.318.1.1.1.4.3.3.0")/10]%
Environment T: [oid("1.3.6.1.4.1.318.1.1.10.2.3.2.1.4.1")]C



Управление на работоспособността
Мониторинг на UPS с DUDE

Полезни SNMP OID за мониторинг на APC UPS.

1.3.6.1.4.1.318.1.1.1.4.3.4.0	Load current A	* Да се дели на 10
1.3.6.1.4.1.318.1.1.1.4.3.3.0	Load Power %	* Да се дели на 10
1.3.6.1.4.1.318.1.1.1.2.2.3.0	Runtaim remaining	02:52:00.00 = 2h.52.min
1.3.6.1.4.1.318.1.1.1.3.3.1.0	Input Voltage V	* Да се дели на 10
1.3.6.1.4.1.318.1.1.1.4.3.1.0	Output Voltage V	* Да се дели на 10
1.3.6.1.4.1.318.1.1.1.2.3.2.0	Internal Temperature C	* Да се дели на 10
1.3.6.1.4.1.318.1.1.1.2.3.4.0	Batteries Voltage V	* Да се дели на 10
1.3.6.1.4.1.318.1.1.1.2.3.1.0	Batteries Capacity %	* Да се дели на 10
1.3.6.1.4.1.318.1.1.10.2.3.2.1.4.1	Environment T Sensor C	Стойността е в цели градуси

Управление на работоспособността
Мониторинг на UPS с DUDE

Изпращане на уведомления, при отпадане на захранването по SMS, e-mail или Telegram messenger.

Създаване на Telegram BOT – 5 Минути.

- Инсталирайте Telegram Desktop.

- Използвайте Telegram BotFather, за да създадете нов bot.

https://telegram.me/botfather
/newbot

- Параметри на бота : bot name, bot username, API key, chat_id

Името на бота, трябва да съдържа “bot”

- Адрес на бота http://t.me/<bot username>
- За да намерите chat_id напишете в браузера

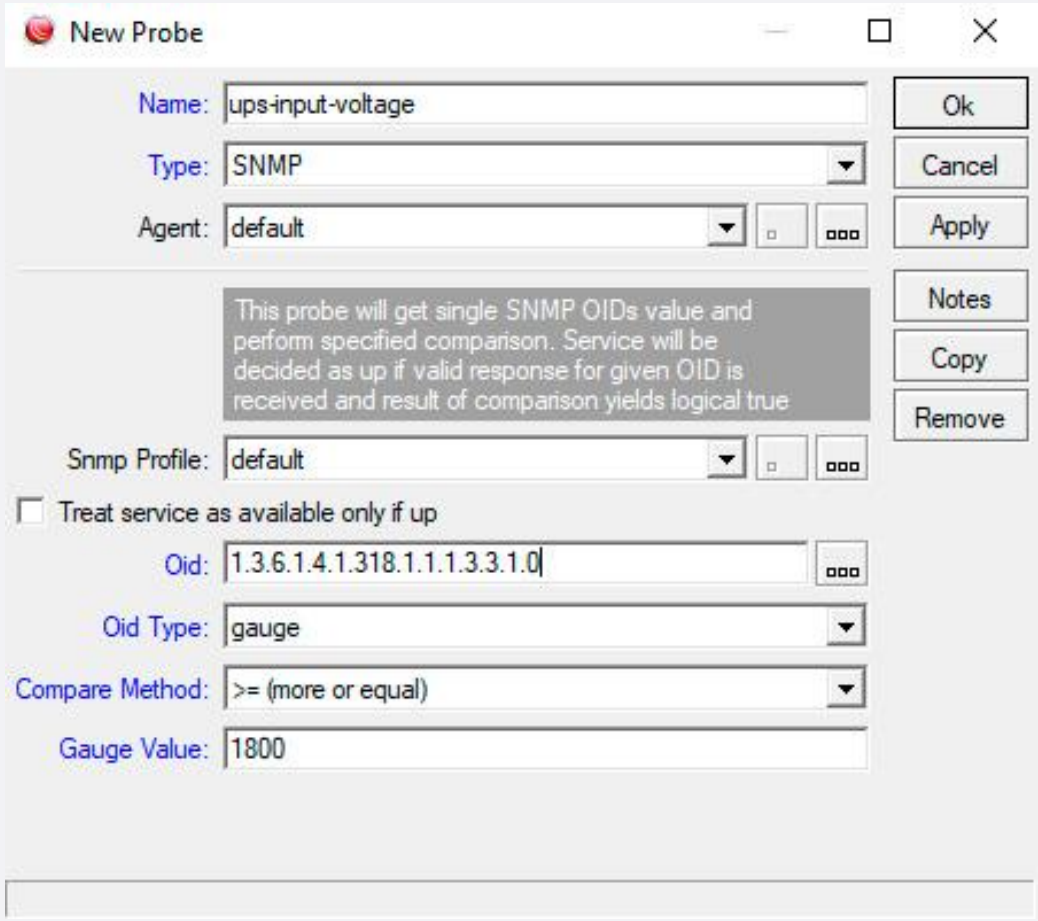
https://api.telegram.org/bot< API key >/getUpdates
Браузерът ще върне chat_id

Сигурност – не предоставяйте параметрите на бота на други лица!

Управление на работоспособността
Мониторинг на UPS с DUDE

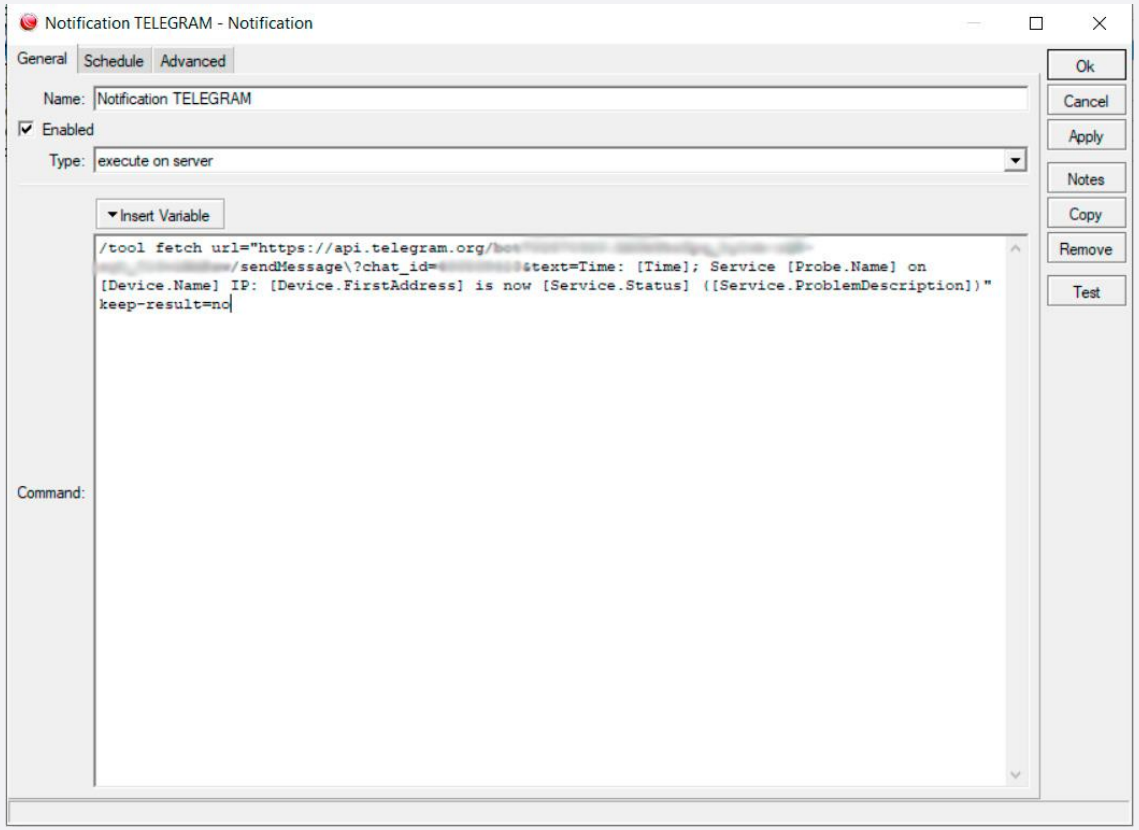
Изпращане на уведомления, при отпадане на захранването чрез Telegram bot.

- Създайте Probe в DUDE.



Управление на работоспособността
Мониторинг на UPS с DUDE

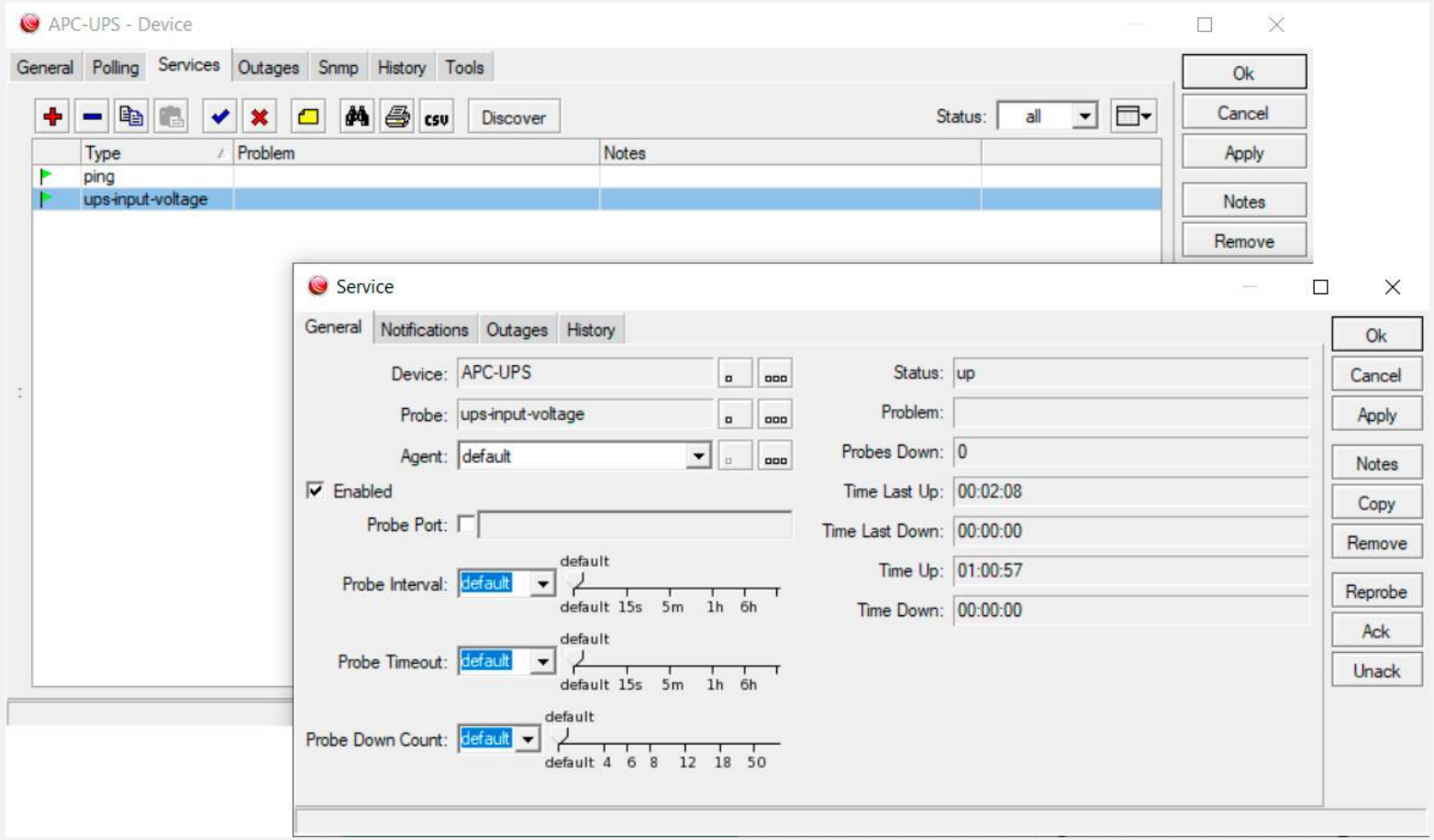
- Създайте Notification в DUDE.



/tool fetch url="https://api.telegram.org/bot<your API key>/sendMessage\?chat_id=<your chat_id>&text=Time: [Time]; Service [Probe.Name] on [Device.Name] IP: [Device.FirstAddress] is now [Service.Status] ([Service.ProblemDescription])" keep-result=no

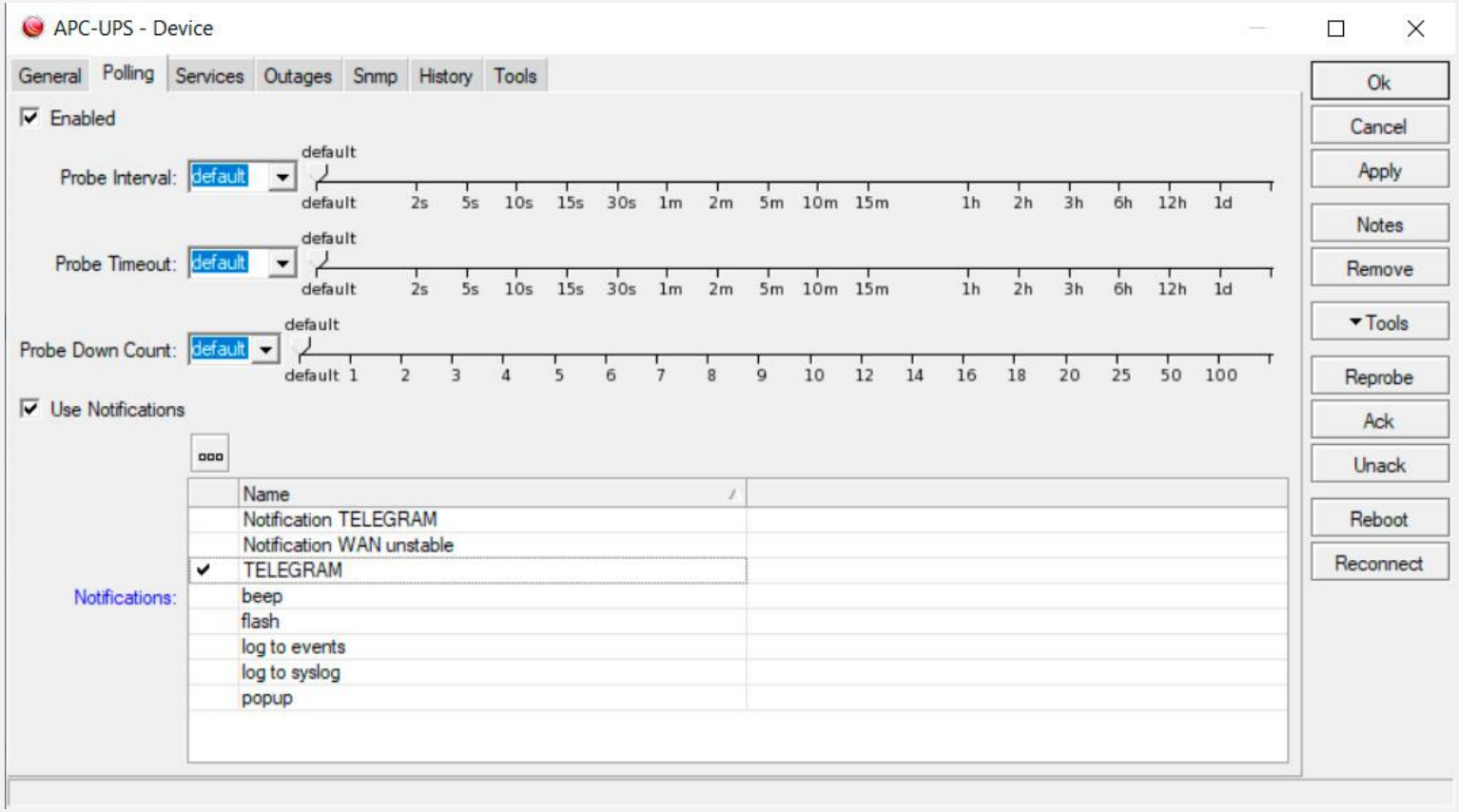
Управление на работоспособността
Мониторинг на UPS с DUDE

- Създайте нов Service на UPS в DUDE.



Управление на работоспособността
Мониторинг на UPS с DUDE

- Създайте нов Pooling на UPS в DUDE.



04

Използвайте **port knock,** за допълнително повишаване сигурността на достъпа.

Допълнителна информация

Portknock
Допълнителни материали

- Софтуер улесняващ Port Knock разработен от Greg Sowell
http://gregsowell.com/?p=2020

- Статия на Добри Бояджиев за Port Knock
https://mikrotik.unibit.bg/articles/port-knocking/

- Mikrotik Wiki Port Knocking
https://wiki.mikrotik.com/wiki/Port_Knocking

- Безплатен софтуер за диаграми
https://www.draw.io/

- Mikrotik Dude Telegram Example
https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6/Dude_Telegram_Example

- Layer 7 Filter supported protocols
http://l7-filter.sourceforge.net/protocols

ВЪПРОСИ?

Благодаря за вниманието!