```
# may/04/2020 10:41:51 by RouterOS 6.45.8
# software id = 1AE5-CDD6
#
# model = 2011UiAS-2HnD
# serial number = B9070A896373
/interface l2tp-server
add comment="VPN L2TP STBLAN" name=l2tp-in1 user=
add comment="VPN L2TP HOME" name=l2tp-in2 user=
add comment="VPN for RDP" name=l2tp-in3 user=
add comment="VPN for RDP" name=l2tp-in4 user=
add comment="VPN for RDP" name=l2tp-in5 user=
/interface bridge
add name=INTERNET
add name=LAN
/interface ethernet
set [ find default-name=ether1 ] comment="I-TEAM INTERNET /1000Mb" \
    mac-address=**-**-**-**-**-**
set [ find default-name=ether3 ] comment=LAN
set [ find default-name=ether4 ] comment="HP DL360 G8"
set [ find default-name=ether6 ] comment="I-TEAM INTERNET /100Mb" \
    mac-address=**-**-**-**-**-**
set [ find default-name=ether9 ] comment="ILO HP DL360 G8"
/interface list
add exclude=all include=all name=list_guest_lan_wifi
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk eap-methods="" \
    management-protection=allowed mode=dynamic-keys name=security_lan \
    supplicant-identity="" wpa-pre-shared-key=****** wpa2-pre-shared-key=\
    ******
add authentication-types=wpa-psk,wpa2-psk eap-methods="" \
    management-protection=allowed mode=dynamic-keys name=secure_guest_lan
\
    supplicant-identity="" wpa-pre-shared-key******** wpa2-pre-shared-
key=\
    *******
/interface wireless
set [ find default-name=wlan1 ] antenna-gain=0 band=2ghz-b/g/n country=\
    no_country_set disabled=no frequency-mode=manual-txpower hide-ssid=yes
\
    mode=ap-bridge security-profile=security_lan ssid=LAN_L
add default-forwarding=no disabled=no keepalive-frames=disabled mac-
address=\
    **-**-**-**-**-** master-interface=wlan1 multicast-buffering=disabled
\
    name=lan_guest_wifi security-profile=secure_guest_lan ssid=LAN_G \
    wds-cost-range=0 wds-default-cost=0 wmm-support=enabled wps-
mode=disabled
/ip firewall layer7-protocol
add name=Drop_net regexp="^.+(HTTP\\/[0-2]).+\$"
add name=rambler regexp="^.+(rambler.ru).*\$"
/ip pool
add name=pool_lan ranges=10.12.3.101-10.12.3.150
add name=pool_vpn ranges=10.10.5.50-10.10.5.100
```

```
add name=pool_guest_wifi ranges=10.11.12.10-10.11.12.100
add name=pool_l2tp ranges=10.10.6.50-10.10.6.100
/ip dhcp-server
add address-pool=pool_lan disabled=no interface=LAN lease-time=2d name=\
    dhcp_lan
/ppp profile
add local-address=pool_vpn name=pptp only-one=no remote-address=pool_vpn \
    use-encryption=yes
add local-address=pool_l2tp name=l2tp only-one=no remote-address=pool_l2tp
/queue simple
add max-limit=3M/2M name=guest_wifi_limit target=10.11.12.0/24
/ip dhcp-server
add address-pool=pool_guest_wifi disabled=no insert-queue-before=\
    guest_wifi_limit interface=lan_guest_wifi lease-time=8h name=\
    dhcp_guest_wifi
/interface bridge port
add bridge=INTERNET interface=ether1
add bridge=LAN interface=ether2
add bridge=LAN interface=ether3
add bridge=LAN interface=ether4
add bridge=LAN interface=ether5
add bridge=INTERNET interface=ether6
add bridge=LAN interface=ether7
add bridge=LAN interface=ether8
add bridge=LAN interface=ether9
add bridge=LAN interface=ether10
add bridge=LAN interface=wlan1
/interface l2tp-server server
set authentication=mschap2 default-profile=l2tp enabled=yes ipsec-secret=\
    "************"
/interface list member
add interface=lan_guest_wifi list=list_guest_lan_wifi
/interface pptp-server server
set authentication=mschap2 default-profile=pptp
/ip address
add address=10.12.0.1/20 comment=LAN interface=LAN network=10.12.0.0
add address=10.11.12.1/24 comment=LAN_GUEST_WIFI interface=lan_guest_wifi
\
    network=10.11.12.0
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=INTERNET
/ip dhcp-server lease
add address=10.12.3.101 address-lists=vi-backup client-
id=1:0:50:56:81:26:f \
    mac-address=00:50:56:81:26:0F server=dhcp_lan
add address=10.12.3.119 client-id=1:10:60:4b:b1:bf:44 comment=\
    "ILO HP DL360p G8" mac-address=10:60:4B:B1:BF:44 server=dhcp_lan
add address=10.12.3.113 mac-address=00:50:56:81:77:25 server=dhcp_lan
add address=10.12.3.129 client-id=1:0:50:56:81:cd:4f mac-address=\
    00:50:56:81:CD:4F server=dhcp_lan
add address=10.12.3.107 client-id=1:0:23:54:1d:1c:c0 mac-address=\
    00:23:54:1D:1C:C0 server=dhcp_lan
add address=10.12.3.122 client-id=1:48:5b:39:96:bd:27 mac-address=\
    48:5B:39:96:BD:27 server=dhcp_lan
```

```
add address=10.12.3.109 client-id=1:0:23:54:1d:1c:3c mac-address=\
    00:23:54:1D:1C:3C server=dhcp_lan
add address=10.12.3.108 client-id=1:c8:60:0:c7:79:86 mac-address=\
    C8:60:00:C7:79:86 server=dhcp_lan
add address=10.12.3.105 client-id=1:0:c:29:fc:2d:54 mac-address=\
    00:0C:29:FC:2D:54 server=dhcp_lan
add address=10.12.3.115 client-id=1:0:1d:60:65:f7:e3 mac-address=\
    00:1D:60:65:F7:E3 server=dhcp_lan
add address=10.12.3.128 client-id=1:90:2b:34:54:7f:9f mac-address=\
    90:2B:34:54:7F:9F server=dhcp_lan
add address=10.11.12.100 client-id=1:9c:2e:a1:9a:4:93 mac-address=\
    9C:2E:A1:9A:04:93 server=dhcp_guest_wifi
add address=10.11.12.98 client-id=1:3c:dc:bc:d8:63:49 mac-address=\
    3C:DC:BC:D8:63:49 server=dhcp_guest_wifi
add address=10.12.3.106 client-id=1:0:50:56:81:68:8b mac-address=\
    00:50:56:81:68:8B server=dhcp_lan
/ip dhcp-server network
add address=10.11.12.0/24 comment="GUEST WIFI" dns-server=10.11.12.1
domain=\
    8.8.8.8 gateway=10.11.12.1
add address=10.12.0.0/20 comment=LAN dns-server=10.12.0.101,10.12.0.5
domain=\
    zflan.loc gateway=10.12.0.1
/ip dns
set allow-remote-requests=yes
/ip firewall address-list
add address=**.**.**.**/24 comment="BLACK LIST VPN CLIENT" list=\
    black_list_vpn
add address=**.**.**.**/24 list=black_list_vpn
add address=10.11.12.100 list="allow to LAN of LAN_G"
add address=10.11.12.98 list="allow to LAN of LAN_G"
/ip firewall filter
add action=drop chain=forward comment="Deny guest wifi to lan work" \
    dst-address=10.12.0.0/24 src-address=10.11.12.0/24 src-address-list=\
    "!allow to LAN of LAN_G"
add action=drop chain=forward dst-address=10.11.12.0/24 src-address=\
    10.12.0.0/24 src-address-list="allow to LAN of LAN_G"
add action=drop chain=input comment="Drop vpn client (black_list_vpn)" \
    connection-state=new dst-port=1701,500,4500 protocol=udp \
    src-address-list=black_list_vpn
add action=drop chain=input comment="Bruteforce login
prevention(VPN_PPTP)" \
    dst-port=1701,500,4500 log=yes protocol=udp src-address-list=\
    vpn_blacklist
add action=add-src-to-address-list address-list=vpn_blacklist \
    address-list-timeout=4w2d chain=input connection-state=new dst-port=\
    1701,500,4500 log=yes protocol=udp src-address-list=vpn_stage_3
add action=add-src-to-address-list address-list=vpn_stage_3 \
    address-list-timeout=2h chain=input connection-state=new dst-port=\
    1701,500,4500 log=yes protocol=udp src-address-list=vpn_stage_2
add action=add-src-to-address-list address-list=vpn_stage_2 \
    address-list-timeout=30m chain=input connection-state=new dst-port=\
    1701,500,4500 log=yes protocol=udp src-address-list=vpn_stage_1
add action=add-src-to-address-list address-list=vpn_stage_1 \
```

```
    address-list-timeout=1m chain=input connection-state=new dst-port=\
    1701,500,4500 in-bridge-port-list=list_guest_lan_wifi log=yes
protocol=\
    udp
add action=accept chain=input comment="L2TP RULE" dst-port=1701,500,4500 \
    in-interface=INTERNET protocol=udp
add action=accept chain=forward comment=\
    "\C4\EE\F1\F2\F3\EF \EA srv.zflan.pp.ua \F7\E5\F0\E5\E7 https://" \
    dst-address=10.12.3.113 dst-port=443 protocol=tcp
add action=accept chain=forward disabled=yes dst-address=10.12.3.113 \
    dst-port=80 protocol=tcp
add action=accept chain=forward comment="Allow smtp for server (out)" \
    dst-address=10.12.3.113 dst-port=25 protocol=tcp
add action=accept chain=forward dst-address=10.12.3.113 dst-port=587 \
    protocol=tcp
add action=accept chain=forward comment="Allow smtp for server (in)" \
    dst-port=25 protocol=tcp src-address=10.12.3.113
add action=accept chain=forward dst-port=587 protocol=tcp src-address=\
    10.12.3.113
add action=accept chain=forward comment="Allow imap for server (out)" \
    dst-address=10.12.3.113 dst-port=143 protocol=tcp
add action=accept chain=forward dst-address=10.12.3.113 dst-port=993 \
    protocol=tcp
add action=accept chain=forward comment="Allow imap for server (in)" \
    dst-port=143 protocol=tcp src-address=10.12.3.113
add action=accept chain=forward dst-port=993 protocol=tcp src-address=\
    10.12.3.113
add action=accept chain=forward comment="\C1\EB\EE\EA\E8\F0\F3\E5\EC
\E8\ED\F2\
    \E5\F0\ED\E5\F2 \E4\EB\FF Backup-ws \EA\F0\EE\EC\E5
\EE\EF\F0\E5\E4\E5\EB\
    \B8\ED\ED\FB\F5 \F1\E0\E9\F2\EE\E2" disabled=yes dst-
address=10.12.0.0/20 \
    src-address=10.12.3.102
add action=accept chain=forward disabled=yes layer7-protocol=rambler \
    protocol=tcp src-address=10.12.3.102
add action=accept chain=forward disabled=yes dst-address-list=backup-ws \
    layer7-protocol=rambler protocol=tcp
add action=reject chain=forward disabled=yes layer7-protocol=Drop_net \
    protocol=tcp reject-with=tcp-reset src-address=10.12.3.102
add action=reject chain=forward disabled=yes dst-address-list=backup-ws \
    layer7-protocol=Drop_net protocol=tcp reject-with=tcp-reset
add action=accept chain=input comment="PING WAN \EF\EE\F0\F2\E0"
protocol=\
    icmp
add action=accept chain=input comment="VPN Network PPTP (GRE, TCP) " \
    disabled=yes in-interface=INTERNET port=1723 protocol=tcp
add action=accept chain=input disabled=yes in-interface=INTERNET
protocol=gre
add action=accept chain=input comment="local accept" in-interface=LAN
add action=accept chain=input comment="established&related accept" \
    connection-state=established,related
add action=drop chain=input comment="all input block" in-
interface=INTERNET
```

```
add action=fasttrack-connection chain=forward comment=fasttrack \
    connection-state=established,related disabled=yes
add action=accept chain=forward comment="established&related accept" \
    connection-state=established,related
add action=drop chain=forward comment="drop invalid" connection-
state=invalid
add action=drop chain=forward comment="drop WAN to LAN" in-
interface=INTERNET \
    out-interface=LAN
/ip firewall nat
add action=masquerade chain=srcnat out-interface=INTERNET
add action=netmap chain=dstnat comment="\CF\F0\EE\E1\F0\EE\F1
\EF\EE\F0\F2\EE\
    \E2 \EF\EE\F7\F2\EE\E2\EE\E3\EE \F1\E5\F0\E2\E5\F0\E0" dst-port=25 \
    in-interface=INTERNET protocol=tcp to-addresses=10.12.3.113 to-
ports=25
add action=netmap chain=dstnat dst-port=587 in-interface=INTERNET
protocol=\
    tcp to-addresses=10.12.3.113 to-ports=587
add action=netmap chain=dstnat dst-port=143 in-interface=INTERNET
protocol=\
    tcp to-addresses=10.12.3.113 to-ports=143
add action=netmap chain=dstnat dst-port=993 in-interface=INTERNET
protocol=\
    tcp to-addresses=10.12.3.113 to-ports=993
add action=netmap chain=dstnat dst-port=443 in-interface=INTERNET
protocol=\
    tcp to-addresses=10.12.3.113 to-ports=443
add action=netmap chain=dstnat disabled=yes dst-port=80 in-
interface=INTERNET \
    protocol=tcp to-addresses=10.12.3.113 to-ports=80
add action=dst-nat chain=dstnat disabled=yes dst-address=1.1.1.1 dst-
port=22 \
    protocol=tcp to-addresses=192.168.88.254
add action=dst-nat chain=dstnat comment="Hairpin NAT for MailServer" \
    dst-address=45.10.34.32 dst-port=443 protocol=tcp to-addresses=\
    10.12.3.113
add action=dst-nat chain=dstnat dst-address=45.10.34.32 dst-port=143 \
    protocol=tcp to-addresses=10.12.3.113
add action=dst-nat chain=dstnat dst-address=45.10.34.32 dst-port=587 \
    protocol=tcp to-addresses=10.12.3.113
add action=masquerade chain=srcnat dst-address=10.12.3.113 dst-port=443 \
    protocol=tcp src-address=10.12.3.128
add action=masquerade chain=srcnat dst-address=10.12.3.113 dst-port=143 \
    protocol=tcp src-address=10.12.3.128
add action=masquerade chain=srcnat dst-address=10.12.3.113 dst-port=587 \
    protocol=tcp src-address=10.12.3.128
add action=masquerade chain=srcnat comment=\
    "Hairpin NAT vi-Backup for send message to GMAIL" dst-
address=10.12.3.113 \
    dst-port=587 protocol=tcp src-address=10.12.0.102
/ip route
add distance=1 dst-address=192.168.1.0/24 gateway=l2tp-in2
add distance=1 dst-address=192.168.16.0/24 gateway=l2tp-in1
```

```
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set api-ssl disabled=yes
/ip ssh
set allow-none-crypto=yes forwarding-enabled=remote
/lcd
set default-screen=stats-all time-interval=hour
/lcd interface pages
set 0
interfaces="sfp1,ether1,ether2,ether3,ether4,ether5,ether6,ether7,ether8\
    ,ether9,ether10"
/ppp secret
add name=******** password********* profile=l2tp service=l2tp
add name******* password********* profile=l2tp service=l2tp
add name******** password********* profile=l2tp service=l2tp
add name********* password********* profile=l2tp service=l2tp
add name********* password="*********" profile=l2tp service=l2tp
add name******** password="**********" profile=l2tp service=l2tp
/system clock
set time-zone-name=Europe/Moscow
/system logging
add disabled=yes topics=l2tp
add disabled=yes topics=pptp
add disabled=yes prefix=ether6 topics=interface
/system ntp client
set enabled=yes primary-ntp=78.46.90.21 secondary-ntp=62.149.0.30
/system package update
set channel=long-term
/system scheduler
add comment="may/04/2020 09:03:46" interval=5s name=LogMikrotik on-
event="# BE\
    GIN SETUP\r\
    \n:local scheduleName \"LogMikrotik\"\r\
    \nlocal bot \"1162849918:AAE3-DpLYzuk2uYizJgSXf7LCyllGav0_mU\"\r\
    \nlocal ChatID \"-462570947\"\r\
    \n:local startBuf [:toarray [/log find message~\"logged in\" ||
message~\"\
    login failure\" || message~\"l2tp-in\" || message~\"link\"]]\r\
    \n:local removeThese {\"telnet\";\"whatever string you want\"}\r\
    \n# END SETUP\r\
    \n\r\
    \n# warn if schedule does not exist\r\
    \n:if ([:len [/system scheduler find name=\"\$scheduleName\"]] = 0)
do={\r\
    \n  /log warning \"[LOGMON] ERROR: Schedule does not exist. Create
schedul\
    e and edit script to match name\"\r\
    \n}\r\
    \n\r\
    \n# get last time\r\
```

```
    \n:local lastTime [/system scheduler get [find
name=\"\$scheduleName\"] co\
    mment]\r\
    \n# for checking time of each log entry\r\
    \n:local currentTime\r\
    \n# log message\r\
    \n:local message\r\
    \n \r\
    \n# final output\r\
    \n:local output\r\
    \n\r\
    \n:local keepOutput false\r\
    \n# if lastTime is empty, set keepOutput to true\r\
    \n:if ([:len \$lastTime] = 0) do={\r\
    \n  :set keepOutput true\r\
    \n}\r\
    \n\r\
    \n:local counter 0\r\
    \n# loop through all log entries that have been found\r\
    \n:foreach i in=\$startBuf do={\r\
    \n \r\
    \n# loop through all removeThese array items\r\
    \n  :local keepLog true\r\
    \n  :foreach j in=\$removeThese do={\r\
    \n#   if this log entry contains any of them, it will be ignored\r\
    \n    :if ([/log get \$i message] ~ \"\$j\") do={\r\
    \n      :set keepLog false\r\
    \n    }\r\
    \n  }\r\
    \n  :if (\$keepLog = true) do={\r\
    \n   \r\
    \n   :set message [/log get \$i message]\r\
    \n\r\
    \n#   LOG DATE\r\
    \n#   depending on log date/time, the format may be different. 3 known
for\
    mats\r\
    \n#   format of jan/01/2002 00:00:00 which shows up at unknown
date/time. \
    Using as default\r\
    \n    :set currentTime [ /log get \$i time ]\r\
    \n#   format of 00:00:00 which shows up on current day's logs\r\
    \n   :if ([:len \$currentTime] = 8 ) do={\r\
    \n     :set currentTime ([:pick [/system clock get date] 0 11].\"
\".\$cur\
    rentTime)\r\
    \n    } else={\r\
    \n#     format of jan/01 00:00:00 which shows up on previous day's
logs\r\
    \n     :if ([:len \$currentTime] = 15 ) do={\r\
    \n        :set currentTime ([:pick \$currentTime 0 6].\"/\".[:pick
[/syste\
    m clock get date] 7 11].\" \".[:pick \$currentTime 7 15])\r\
    \n      }\r\
```

```
    \n   }\r\
    \n    \r\
    \n#   if keepOutput is true, add this log entry to output\r\
    \n   :if (\$keepOutput = true) do={\r\
    \n     :set output (\$output.\$currentTime.\"
\".\$message.\"\\r\\n\")\r\
    \n   }\r\
    \n\r\
    \n    :if (\$currentTime = \$lastTime) do={\r\
    \n     :set keepOutput true\r\
    \n     :set output \"\"\r\
    \n   }\r\
    \n  }\r\
    \n  :if (\$counter = ([:len \$startBuf]-1)) do={\r\
    \n   :if (\$keepOutput = false) do={    \r\
    \n     :if ([:len \$message] > 0) do={\r\
    \n        :set output (\$output.\$currentTime.\"
\".\$message.\"\\r\\n\")\
    \r\
    \n      }\r\
    \n    }\r\
    \n  }\r\
    \n  :set counter (\$counter + 1)\r\
    \n}\r\
    \n\r\
    \nif ([:len \$output] > 0) do={\r\
    \n  /system scheduler set [find name=\"\$scheduleName\"]
comment=\$current\
    Time\r\
    \n  /tool fetch
url=\"https://api.telegram.org/bot\$bot/sendmessage\?chat_\
    id=\$ChatID&text=MikroTik alert \$currentTime : \$output\" keep-
result=no;\
    \r\
    \n}" policy=\
    ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon \
    start-time=startup
/system script
add dont-require-permissions=no name=backup_mail owner=dkorsachev policy=\
    ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon
source="{\
    \r\
    \n:log info \"Starting Backup Script...\";\r\
    \n:local sysname [/system identity get name];\r\
    \n:local sysver [/system package get system version];\r\
    \n:log info \"Flushing DNS cache...\";\r\
    \n/ip dns cache flush;\r\
    \n:delay 2;\r\
    \n:log info \"Deleting last Backups...\";\r\
    \n:foreach i in=[/file find] do={:if ([:typeof [:find [/file get \$i
name]\
    \_\\\r\
    \n\"\$sysname-backup-\"]]!=\"nil\") do={/file remove \$i}};\r\
    \n:delay 2;\r\
```

```
    \n:local smtpserv [:resolve \"10.12.3.113\"];\r\
    \n:local Eaccount \"it@zflan.pp.ua\";\r\
    \n:local pass \"*********\";\r\
    \n:local backupfile (\"\$sysname-backup-\" . \\\r\
    \n[:pick [/system clock get date] 7 11] . [:pick [/system \\\r\
    \nclock get date] 0 3] . [:pick [/system clock get date] 4 6] .
\".backup\
    \");\r\
    \n:log info \"Creating new Full Backup file...\";\r\
    \n/system backup save name=\$backupfile;\r\
    \n:delay 2;\r\
    \n:log info \"Sending Full Backup file via E-mail...\";\r\
    \n/tool e-mail send from=\"<\$Eaccount>\" to=\$Eaccount
server=\$smtpserv \
    \\\r\
    \nport=587 user=\$Eaccount password=\$pass start-tls=yes
file=\$backupfile\
    \_\\\r\
    \nsubject=(\"\$sysname Full Backup (\" . [/system clock get date] .
\")\")\
    \_\\\r\
    \nbody=(\"\$sysname full Backup file see in attachment.\\nRouterOS
version\
    : \\\r\
    \n\$sysver\\nTime and Date stamp: \" . [/system clock get time] . \"
\" . \
    \\\r\
    \n[/system clock get date]);\r\
    \n:delay 5;\r\
    \n:local exportfile (\"\$sysname-backup-\" . \\\r\
    \n[:pick [/system clock get date] 7 11] . [:pick [/system \\\r\
    \nclock get date] 0 3] . [:pick [/system clock get date] 4 6] .
\".rsc\");\
    \r\
    \n:log info \"Creating new Setup Script file...\";\r\
    \n/export verbose file=\$exportfile;\r\
    \n:delay 2;\r\
    \n:log info \"Sending Setup Script file via E-mail...\";\r\
    \n/tool e-mail send from=\"<\$Eaccount>\" to=\$Eaccount
server=\$smtpserv \
    \\\r\
    \nport=587 user=\$Eaccount password=\$pass start-tls=yes
file=\$exportfile\
    \_\\\r\
    \nsubject=(\"\$sysname Setup Script Backup (\" . [/system clock get
date] \
    . \\\r\
    \n\")\") body=(\"\$sysname Setup Script file see in
attachment.\\nRouterOS\
    \_\\\r\
    \nversion: \$sysver\\nTime and Date stamp: \" . [/system clock get
time] .\
    \_\" \\\r\
    \n\" . [/system clock get date]);\r\
```

```
    \n:delay 5;\r\
    \n:log info \"All System Backups emailed successfully.\\nBackuping
complet\
    ed.\";\r\
    \n}"
/tool e-mail
set address=10.12.3.113 from=IT@zflan.pp.ua password=********** user=\
    it@zflan.pp.ua
/tool graphing interface
add
/tool graphing resource
add
```