Troubleshooting

- After policy install: UDP packet that belongs to an old session drops
- How to copy a file from a Check Point firewall
- CPView Utility and High Load Traffic
- IPS Troubleshooting
- Limitation of 251 Inline Layers
- Packetpushers with SQLNet
- Show interface speed and duplex as a list
- VPN Troubleshooting
- Threat Extraction Troubleshooting

After policy install: UDP packet that belongs to an old session drops

Problem description

At the customer site we have a rule which allows a WLAN Controller to connect to the RADIUS Server in another network.
After installing the rules, the UDP connections were rematched because it is the needed global Setting on this Firewall.

image-1604935352454.png

With fw ctl zdebug drop we see the following:

```
;[vs_1];[tid_0];[fw4_0];fw_log_drop_ex: Packet proto=17 10.1.1.1:57056 -> 10.45.99.40:1812 dropped by fw_handle_old_conn_recovery Reason: UDP packet that belongs to an old session;
```

So the RADIUS Connection will not come up again.
It seems to be a virtual UDP session in the state table of the fw.
This UDP connection will never reach the timeout and will never be removed from the state table.

Troubleshooting

In the RADIUS service object "NEW-RADIUS" set "Keep connections open after the policy has been installed" but this does not help.

Problem is described here: https://www.cpug.org/forums/showthread.php/22042-ClusterXL-connection-drop-when-Policy-Push

Workaround

Disable the RADIUS server for 2 minutes and the Connections do work again.

Solution

Solution is described here:

Dropped UDP Server to Client packets refresh the connection timeout (sk121933)

> Fixed in Hotfix for current installed release or future Jumbo Hotfix from CP.

How to copy a file from a Check Point firewall

For troubleshooting you need sometime to transfer files from a Check Point firewal, as example tcpdump files etc.
With the admin user it is not possible to login with sftp, the shell for the user is set to /etc/cli.sh.

For a temporary access to the sftp feature you need to change the shell of the admin or other user which is used for the filetransfer with sftp.

Change the shell of the user

```
[Expert@fw]# chsh username
Changing shell for username.
New shell [/etc/cli.sh]: /bin/bash
Shell changed.
```

Then you can do the transfer.

Change it back again if needed

```
[Expert@fw]# chsh username
Changing shell for username.
New shell [/bin/bash]: /etc/cli.sh
Shell changed.
```

CPView Utility and High Load Traffic

If you have the situation and a fw has a high load on traffic sometimes you need tools to figure it out what causes the resulting high cpu load etc.

A great tool to use is Check Point's CPView:

https://community.checkpoint.com/videos/5977-the-cpview-utility

https://www.youtube.com/embed/OjsvuT2YxKs

How to use CPView to get History data

Start the cpview history daemon

```
# cpview history on
```

Check the status of the history daemon

```
# cpview history stat
```

history daemon is activated

Check the history data (use <+> or <-> to scroll the time)

```
# cpview -t
```

Jump directly to timestamp

Start cpview -t for the history mode.

Then press 't' to toggle the date mode and insert the date you want to start at.

IPS Troubleshooting

IPS Profile and Detect Mode

When you run the IPS recommended profile, most of the critical and high signatures are in inactive or detect mode.
But still there could be a high cpu performance impact even when you're only in detect mode.

> In prevent mode you kill the connection and you are done.
> In detect mode you have to keep the connection open and keep spending CPU cycles on tracking that traffic.

So detect mode maybe is using higher cpu cycles.

R80.x Performance Tuning Tip - DDOS

See: https://community.checkpoint.com/docs/DOC-3407-r80x-performance-tuning-tip-ddos-fw-sam-vs-fwaccel-dos

R80.10 IPS Best Practices

CP_R80.10_IPS_BestPractices_Guide.pdf

Limitation of 251 Inline Layers

Problem

> Policy push fails with the following error: Policy installation failed on gateway. If the problem persists contact Check Point support (Error code: 2000232)

Cause

The user has configured too many policy layers in the rulebase (a layer is either an Ordered layer or an Inline Layer).

> The Security Gateway has a limitation of 251 layers (in total there are 256, while 5 are reserved).

Solution

Verify that the number of layers is not exceeding 251.

Troubleshooting

Show Access Layers

```
mgmt_cli show access-layers limit 500 -s id.txt --format json | jq '."access-layers"[].name'
```

Count Access Layers

```
mgmt_cli show access-layers limit 500 --format json
```

Output:

```
.
.
 } ],
 "from" : 1,
 "to" : 260,
 "total" : 260
}
```


See here: Show Access Layers

Packetpushers with SQLNet

If you need to apply an ALG (Application level gateway) on SQLNet be careful and check the following:

SQL*Net (a.k.a Oracle TNS) and firewalls...

> Most vendor's firewalls have a SQL ALG that handles SQL*Net traffic.
> They listen on TCP port 1521.

> SQL*Net is based on Oracle's TNS protocol.
> The specification for this protocol is proprietary and inaccessible, but you can figure it out by reading Oracle's docs and looking at the Wireshark dissector source code.

> In Checkpoint firewalls, there are two ALGs for SQL*Net: "sqlnet1" and "sqlnet2."
> sqlnet1 should be used for non-redirected sessions and sqlnet2 should be used for redirected sessions.
> The implication is that non-redirected sessions evaluated against sqlnet2 could negatively impact the CPU of the firewall.

Show interface speed and duplex as a list

If you need a list of interfaces and the actual speed and duplex settings use this:

```
# ifconfig -a | grep encap | awk '{print $1}' | grep -v lo | grep -v bond | grep -v ":" \
| grep -v ^lo | xargs -I % sh -c 'ethtool %; ethtool -i %' | grep '^driver\|Speed\|Duplex\|Setting' \
| sed "s/^/ /g" | tr -d "\t" | tr -d "\n" | sed "s/Settings for/\nSettings for/g" \
| awk '{print $5 " "$7 "\t " $9 "\t" $3}' | grep -v "Unknown" | grep -v "\."
```

Found here: https://community.checkpoint.com/thread/7056-interface-speed-and-duplex-as-list

VPN Troubleshooting

VPN Problems

Links & Infos

IKEv2

Internet Key Exchange Protocol Version 2 (IKEv2)

https://tools.ietf.org/html/rfc5996

Check Point Probleme mit IKEv2

Site to Site using IKEv2 fails with "None of the traffic selectors match the conection"

https://support.checkpoint.com/results/sk/sk157473

How do I change the local id for an IKEv2 IPsec VPN?

https://community.checkpoint.com/t5/Remote-Access-VPN/How-do-I-change-the-local-id-for-an-IKEv2-IPsec-VPN/m-p/14786

Unauthorized VPN access to internal networks via IKEv2 tunnel (CVE-2019-8456)

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk149892

IKEv2 negotiation for Site-to-Site VPN tunnel with 3rd party peer fails if IKEv2 SA payload contains more than 8 proposals

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112139

When Check Point peer is initiator of IKEv2 negotiation, FQDN not being sent

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108817

Debugging IKEv2 on Check Point

Link

What is the IKEView Utility ?

https://support.checkpoint.com/results/sk/sk30994

How to collect a debug for VPN issues

https://support.checkpoint.com/results/sk/sk180488

Debugging Description

- Use Ike debug to validate and understand how both devices are negotiating the parameters

disable acceleration if you can:

```
fwaccel off
vpn debug trunc ALL=5
ike debug trunc
ike debug on TDERROR_ALL_ALL=5
```

Get the file ***$FWDIR/log/legacy_ikev2.xmll*** and check the proposal for both side.
Read the file ***$FWDIR/log/vpnd.elg*** and try to find any inconsistencies.

- IKE is the same for all players, the problem is configuration. Many times, the devices try to send parameters differently of what you expect they do.
- Check Point firewalls try to summarize the networks inside the encryption domain, this is called supernetting.
  It will try to summarize at maximum possible and will send that summarization in place of original one.
  If you have two subnets /24 it will try to send a /23.
- Route based VPN is more flexible than domain based and you can have both configured. Use it if you can.
- There's a new version for ikeview.exe capable to read *$FWDIR/log/ikev2.xmll*. (https://support.checkpoint.com/results/sk/sk30994)
  Check on support center and if possible use its the best tool to troubleshoot VPN problems on Check Point side.
- Disable debug after all

```
fwaccel on
vpn debug off
```

Threat Extraction Troubleshooting

Introduction

The following is a collection of troubleshooting I need to do with Check Point Threat Extraction R80.10.

I used the Technical Reference Guide (ATRG) here: sk114807

Workflow in MTA mode

1. A PostFix server receives and handles the emails.

2. Emails are forwarded to the *in.emaild.mta* daemon, which:
   1. Parses the emails (For example, Base64 decode)
   2. Passes the attachments to the *scrubd* process, if needed (based on the configuration of supported file types).

3. The *scrubd* process handles the file and sends it to the *scrub_cp_file_convertd* process with the relevant details (according to the policy).

4. *scrub_cp_file_convertd process*
   1. Converts the file / extracts potentialy malicious content from it.
   2. Returns a Safe copy of the file to *scrubd.*

5. The *scrubd* process returns the Safe copy to the *in.emaild.mta* daemon

6. The *in.emaild.mta* daemon:
   1. Replaces the original attachment with the Safe Copy version.

   2. Forwards the email to its destination.

Note: For environments with MTA bundle R80.10 jhf or R80.20, *in.emaild.mta* is replaced with *mtad* daemon

Check log of convert to PDF process

It seems that the path is wron documented in the sk114807

The path mentioned **/var/log/jail/$FWDIR/log/scrub_cp_file_convertd.elg*** is in real **/var/log/jail/$CPMDIR/log/scrub_cp_file_convertd.elg***

"This notification page has expired" error in UserCheck page when a user tries to download the original file that was blocked by Threat Extraction

According to: sk106249

Symptoms

"This notification page has expired. You can safely close the page or" error in UserCheck page when a user tries to download the original attachment 7 days after receiving the original e-mail, although the Threat Extraction is configured to keep the original attachments for more than 7 days.

image-1614413932202.png

- Attachment file still exists in /var/log/scrub/repository/ on Threat Extraction Gateway.
- The original mail can be retrieved by running the following command on the Security Gateway: scrub send_orig_email <email_id or reference_number> all.
- The Email ID or reference number can be retrieved from the incident log.

Solution

For more information about the sk106249 you need to login to CP support portal. There you will need to check more files if you have set the "Delete stored original files older than" to 30+ days. These files ave been patched if you have installed the latest R80.10 Jumbo hotfixes.

The next SK mentioned is the following:

Persistence of UserCheck incidents is not preserved when quarantine time is very high

sk122099

The solution for the SK above is to upgrade to R80.20