

# #toxicframe

Der mysteriöse Hardware-Bug

der Dateitransfers bei genau 49% stoppen lässt

*Netgate SG-2100 / Marvell 6000*

Wim Bonis · Stylite AG · 39C3 Lightning Talk

# Der Kundenfall



**Problem: Dateitransfer stoppt immer bei 49%**

**Situation:**

- SMB-Dateiübertragung über **IPsec VPN**
- Ziel: Samba-Server im Firmennetzwerk
- **Neue Hardware:** Netgate SG-2100 (pfSense)

**Symptom:** 100% reproduzierbarer Abbruch bei exakt 49% einer bestimmten Datei.  
(stdww2.cab = 195MB)

# Erste Diagnose

✗ Was alles **NICHT** die Ursache war:

- **Netzwerk-Konfiguration:** MTU/MSS/Fragmentierung
- **VPN-Protokolle:** IPsec ↔ OpenVPN
- **Security:** Virenscanner / DPI
- **Hardware-Offloading:** Checksum, TSO, LSO

TargetException Fazit: **NICHT VPN/SMB - etwas viel Tieferes!**

# Paketanalyse



## Durchbruch: Das Problem isoliert!

- Abbruch bei 49% auf **einen einzigen 1-KB-Block** eingrenzbar
- Aus Originaldatei `stdww2.cab` bei 49% isoliert
- **"Toxisches Paket"** identifiziert!

```
000001E0 48 44 22 12 89 48 24 22 91 89 44 24 24 12 91 48 44 H D " . . H $ " . . D $ . . H D
000001F0 22 12 89 48 24 22 91 89 44 24 12 91 48 44 22 12 " . . H $ " . . D $ . . H D "
00000200 89 48 24 22 91 89 44 24 12 91 48 44 22 12 89 48 . H $ " . . D $ . . H D " . . H
00000210 24 22 91 89 44 24 12 91 48 44 22 12 89 48 24 22 $ " . . D $ . . H D " . . H $ "
00000220 91 89 44 24 12 91 48 44 22 12 89 4A 24 4A 4A 4A . . D $ . . H D " . . J $ J J J
00000230 4A J J J J J J J J J J J J J J J J J
00000240 4A J J J J J J J J J J J J J J J J J J
00000250 4A J J J J J J J J J J J J J J J J J J
00000260 4A J J J J J J J J J J J J J J J J J J
```

## Reproduktion:

```
dd if=stdww2.cab bs=1024 skip=99989 count=1 of=toxic.bin
```

# Labor-Analyse



**Protokoll-unabhängiger Hardware-Bug, nicht nur SMB, auch HTTP**

Protokoll/Testpfad	Ergebnis
<b>Reines Forwarding</b> (LAN ↔ Switch)	✗ Abbruch
<b>SMB</b> (Dateitransfer)	✗ Abbruch
<b>HTTP</b> (Web-Download)	✗ Abbruch



**Schlussfolgerung: Hardware/Switch-Pfad betroffen!**

**Einfachster Test: Download der toxische Datei:**

```
# nur über HTTP , den über HTTPS werden andere Daten übertragen  
curl http://toxicframe.stylite-live.net/toxic.bin
```

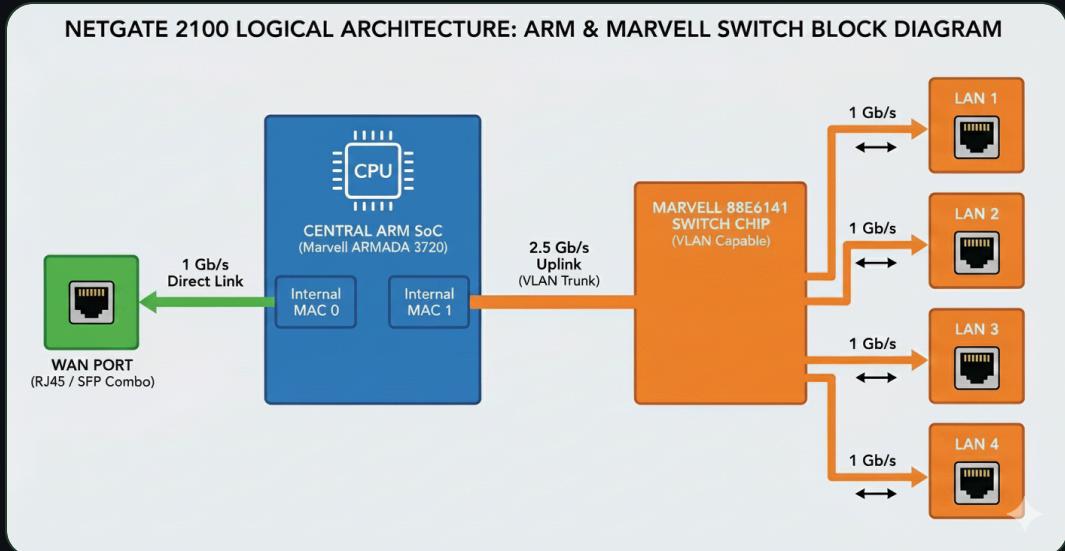
# Hardware-Architektur

## Netgate SG-2100 Aufbau:

- **CPU:** Marvell Armada 3720 (ARM64 Cortex-A53)
- **Switch:** interner Marvell 6000 Switch (88E6141)
- **Uplink:** CPU  Switch mit **2.5 GbE**

## Muster erkannt:

*Sobald der Switch-Pfad beteiligt ist, ist der Bug 100% reproduzierbar!*



5

# TCP Dump

🔍 **Das Paket verschwindet im Switch!**

**Netzwerk-Trace Ergebnis:**

- **Netgate → Switch:** ✓ Paket wird **gesendet**
- **Switch → Client:** ✗ Paket kommt **nie an**

❗ **Das "toxische" Paket verschwindet im Switch-Pfad!**

*(Paket-Filter, Switch-ASIC oder elektrischer Pfad CPU ↔ Switch)*

# Historie

JUL  
17

## Das Problem ist NICHT NEU!

- **Mindestens seit 2020** bekannt
- **Reddit-Thread:** "Weirdest Issue Ever?" - exakt gleiche Symptome



## Damals auch ohne Lösung.

The screenshot shows a Reddit post from the subreddit r/PFSENSE. The title is "Weirdest Issue Ever? - Experts Needed! SMB Hangs over Specific File". The post contains text describing a network issue where SMB shares hang when attempting to copy specific files from a network share on an EC2 instance in AWS. It includes sections for Infrastructure, Issue, and Troubleshooting, with several bullet points listed under Troubleshooting.

reddit /r/PFSENSE · vor 4 Jahren JamesObZ

Weirdest Issue Ever? - Experts Needed! SMB Hangs over Specific File

Apologies if the title is a little click-baity, I've just never seen anything like this. I'm really hoping someone can help me here as I have no idea what is causing this problem.

**Infrastructure:**

In short, a basic setup where office laptop > HP 3500 Switch (Latest firmware) > Fibre link to Aruba 6100 Switch (Latest firmware) > PfSense version: 22.01 (Latest) on a Netgate SG-2100 > IPSEC VPN to SMB Share location

**Issue:**

Connecting from a new Office/network I have recently setup, I am attempting to connect to a network share on an EC2 instance in AWS to copy down a bunch of files, explorer will hang half way through and the share temporarily will crash when I try to grab a specific file.

I have found out what file the process is hanging on, I go directly to where the file is located on the share and if I attempt to right click this file, I will not get the menu box appear to allow me to interact with it at all for 10+ mins. Eventually it will appear... I select copy for example, and if I attempt to paste this to my desktop, it will get say 60% of the way there, then hang for 15 mins until I get an error saying the network share cannot be found.

Now... 100% this file is not the issue. It can be accessed fine from multiple other networks in different sites and has been this way for years. The problem is specific to the new network I have recently configured, and I imagine likely a symptom of a larger problem. I am just seeing this behaviour manifest itself with this one file currently.

**Troubleshooting:**

- The file can be successfully copied to this new network via an RDP session.
- Initially, IPSEC fragmentation was looked into as the file needs to be accessed via an IPSEC tunnel, but can rule out IPSEC being an issue as having copied this file to the network via an RDP session I get the same problem when copying the file between different VLANs in the same office over SMB.
- If I rule PfSense out of the equation by performing a test coping the file from 2 addresses on the same VLAN it works. So it appears it's something to do with PfSense.
- This was also happening on PfSense version 21.05.2, I had hoped an upgrade would possibly resolve this, it didn't.

7

# Hersteller-Kontakt

## Netgate informiert:

- **am** 3.11.2025
- **Bug bestätigt** und reproduzierbar
- **Status:** Anerkannt, aber...
- **Kein klarer Fix** bisher verfügbar
- **Kein Rollout** eines Patches

## Was passiert als nächstes?

# Das Paketmuster:

🎯 Minimal reproduzierbar:

**Trigger-File:** `toxic.bin` (nur 1 KB!)

**Quelle:** Aus `stdww2.cab` isoliert

```
dd if=stdww2.cab bs=1024 skip=99989 count=1 of=toxic.bin
```

📊 Enthält wahrscheinlich:

- 14-Byte Pattern wiederholt sich 39-mal: 44 24 12 91 48 44 22 12 89 48 24 22 91 89
- Spezifisches Timing oder Bit-Muster

# Alternative Hardware



**Test mit ähnlicher Hardware:**

**GL-iNet Edge GL-MV1000 Brume:**

- Marvell 88E6141 Switch (gleicher Chip!)
- **Unterschied:** Nur 1GbE statt 2.5GbE Uplink
- **OpenWRT** statt pfSense
- **Ergebnis:** toxicframe → **nicht reproduzierbar** ✓

**Hypothese:** **2.5GbE Uplink könnte der Auslöser sein!**

# Folgerungen ?

## Status: Alles noch Vermutung

- **Hardware-Bug** - nicht wegkonfigurierbar!
- **Hersteller-Fix** nötig: Firmware/ASIC/Hardware-Revision
- **4+ Jahre** bekannt (Reddit 2020)

## Workaround:

### Nicht den integrierten Switch verwenden!

- Nur WAN-Port verwenden
- VLANs mit externem Switch realisieren

# Diskussion & Hilfe

## 👉 Wo bin ich?

Ihr findet mich beim OpenWRT Tisch in Halle H

**Habt ihr SG-2100 oder ähnliche Hardware?**

**Ideen für weitere Analyse:**

- Kann man aus dem Switch-ASIC herauslesen, ob das Paket gedroppt wird?
- Bekommt man OpenWRT o.ä. auf die SG-2100 installiert?

## 🔗 Ressourcen:

- **Artikel:** <https://stylite.io/toxic>

