**Pentesting Report**

Table of Contents

[1 Executive summary 1](#_Toc167105961)

[2 Customer contacts 1](#_Toc167105962)

[3 IPS contacts 2](#_Toc167105963)

[4 Method 2](#_Toc167105964)

[5 Scope 2](#_Toc167105965)

[6 Assessment 3](#_Toc167105966)

[6.1 Summary of findings 3](#_Toc167105967)

[6.2 Identified Devices 3](#_Toc167105968)

[6.3 Overview 3](#_Toc167105969)

[7 Technical findings details 4](#_Toc167105970)

[8 Recommendations 6](#_Toc167105971)

[8.1 Overview 6](#_Toc167105972)

[8.2 Remedies 6](#_Toc167105973)

# Executive summary

PacketFront Software Solutions AB (“PacketFront Software” herein) contracted IP-Solutions to perform a Network Penetration Test of the main firewall to identify security weaknesses, determine the impact to PacketFront Software, document all findings in a clear and repeatable manner, and provide remediation recommendations.

# Customer contacts

|  |  |  |
| --- | --- | --- |
| *Role* | *Name* | *Contact details* |
| CTO | Jonas Ohlsson | [jonas.ohlsson@pfsw.com](mailto:jonas.ohlsson@pfsw.com) |
| IT-Architect | Daniel Lundqvist | [daniel.lundqvist@pfsw.com](mailto:daniel.lundqvist@pfsw.com) |

# IPS contacts

|  |  |  |
| --- | --- | --- |
| *Role* | *Name* | *Contact details* |
| IT-Security Consultant | Aleksandar Milosavljevic | [aleksandar.milosavljevic@ip-solutions.se](mailto:aleksandar.milosavljevic@ip-solutions.se) |
| BDM-Security | Mattias Paajanen | [mattias.paajanen@ip-solutions.se](mailto:mattias.paajanen@ip-solutions.se) |

# Method

IP-Solutions performed a testing under “black box” approach during days between 2024-05-02 to 2024-05-03 with a limited knowledge of the internal network. Testing was conducted from a “non-evasive” point of view with the primary scope to identify as many vulnerabilities and misconfigurations as possible, without creating any possible disruptions since the product is used as main firewalling solution.

Testing was performed remotely from consultant’s laptop, without holding access to the local Wi-Fi network or VPN connection to simulate a possible attack scenario from an external threat actor. Each weakness identified was documented and manually investigated to determine the exploitation possibilities, and escalation potential. In the case of successful foothold IP-Solutions weren’t allowed for further testing as lateral movement and horizontal/vertical privilege escalation instead, the tester was asked to promptly inform the customer by documenting all the findings.

# Scope

The customer provided a list of owned public IPv4 addresses.

|  |  |
| --- | --- |
| *IP* | *Info* |
| 151.236.205.225 | Used by the firewall. |
| 151.236.205.226 | Used by the firewall. |
| 151.236.205.227 | Used by the firewall. |
| 151.236.205.228 | Used by the firewall. |
| 151.236.205.229 | Used by the firewall. |
| 151.236.205.230 | Used by the firewall. |
| 151.236.205.231 | Used by the firewall. |
| 151.236.205.232 | Used by the firewall. |

# Assessment

## Summary of findings

|  |  |  |
| --- | --- | --- |
| *Severity* | *ID* | *Details* |
| Informational | 1 | Weak Cypher/Diffie-Hellman group used in the IPSec service. |

## Identified Devices

|  |  |  |
| --- | --- | --- |
| *Hostname* | *IP* | *Details* |
| Pfswfw | 151.236.205.225 151.236.205.226 151.236.205.228 | Mikrotik firewall. |

## Overview

The tester found PacketFront Software’s network management to be well-maintained. No critical finding has been discovered that led to an actual breach of the environment from an “external” standpoint. In accordance with the customer, it is relevant to mention that invasive attacks like DOS (Denial of Service) and heavy brute-forcing haven’t been tested on the device.

The only documented finding shouldn’t be seen as a threat, instead as an opportunity for PacketFront Software to strengthen its internal network security. In addition, the customer should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

# Technical findings details

***Improper authorization on BECS frontend*** Severity: **INFORMATIONAL**

The tester used [Nmap](https://nmap.org/) network scanner to footprint the IP’s and identify that 3 of them had relevant services to a firewall.

A screen shot of a computer

Description automatically generated

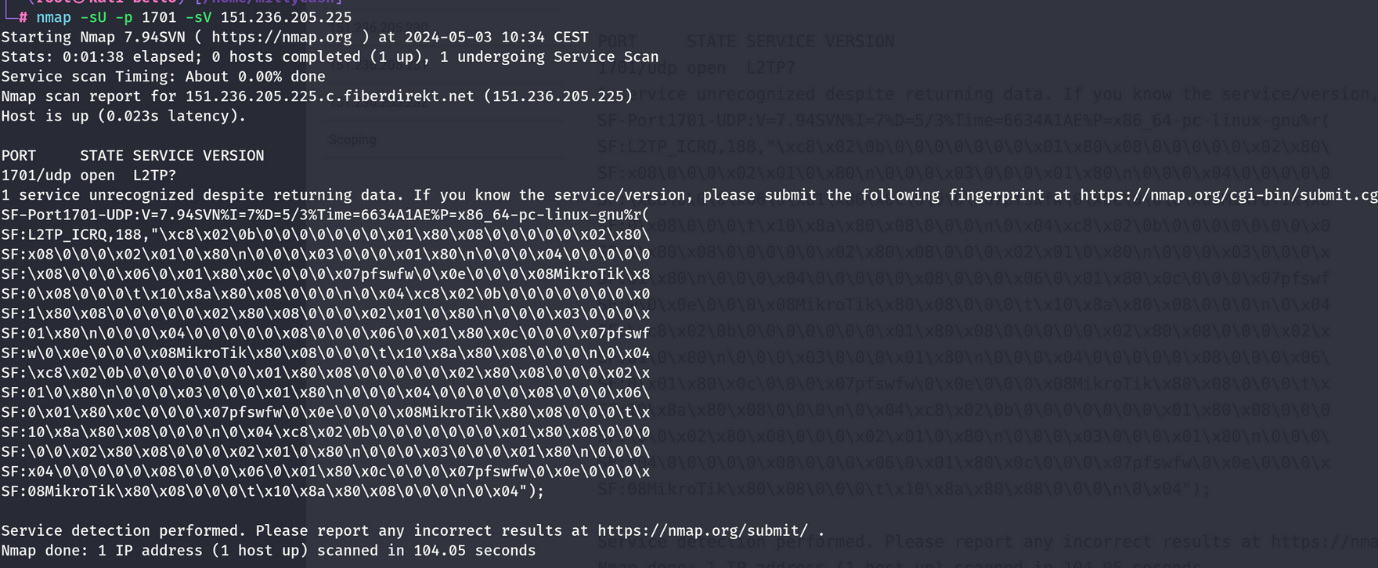
A computer screen with white text

Description automatically generated

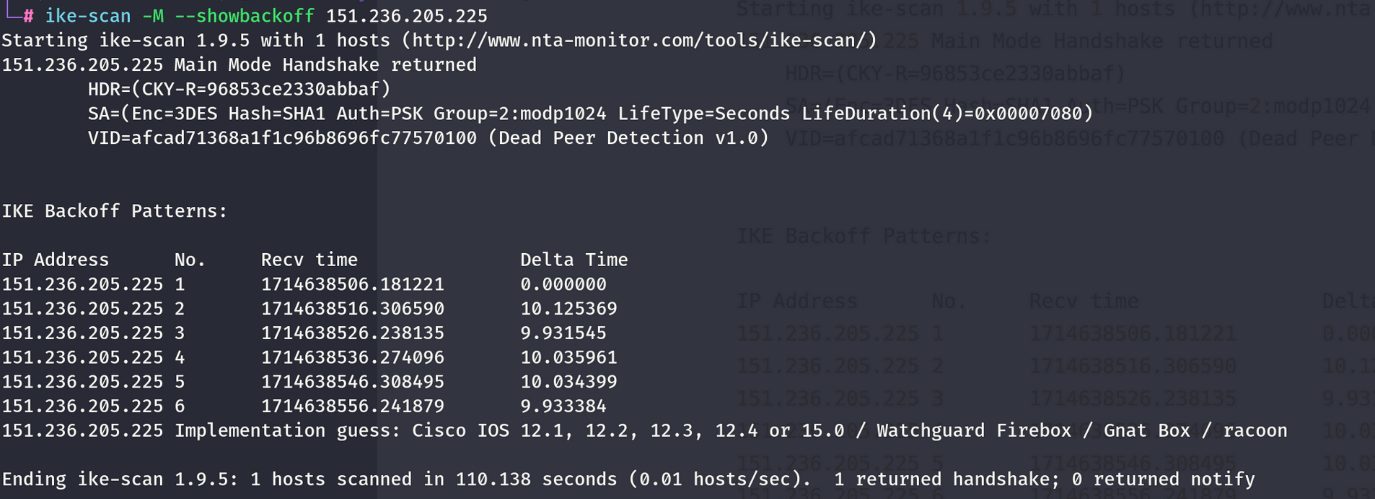
A screenshot of a computer

Description automatically generated

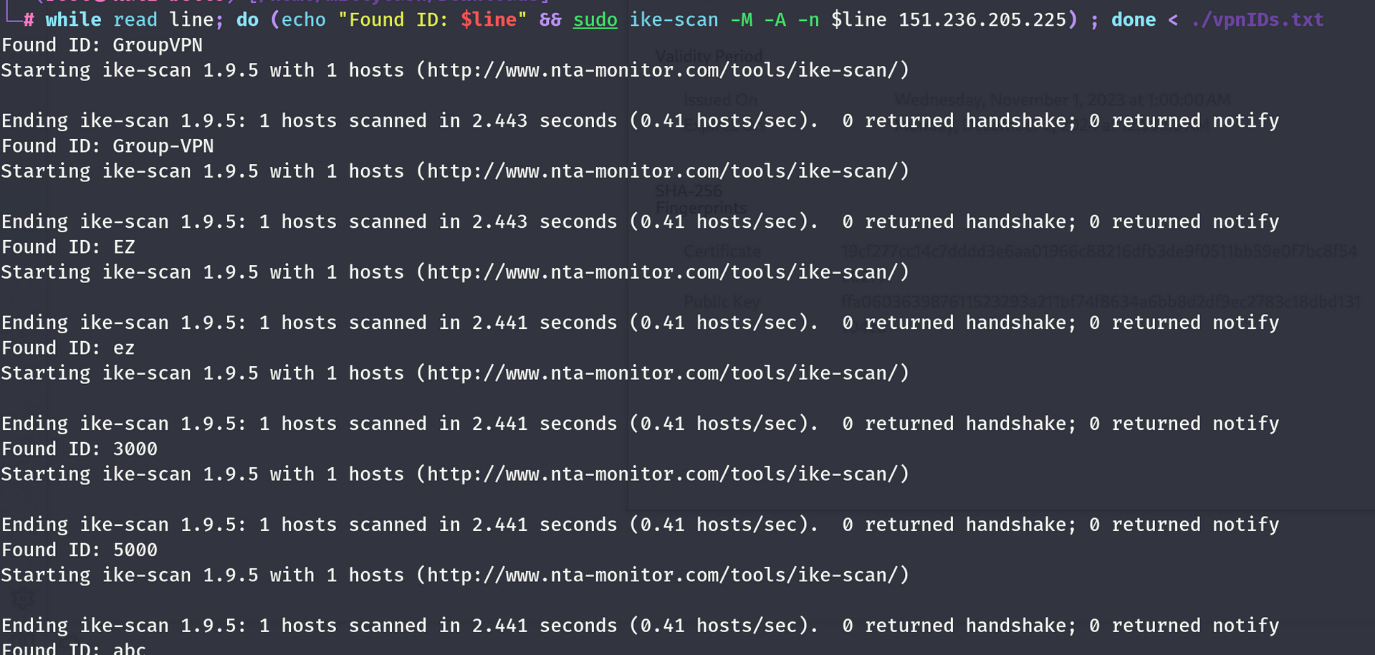
Foot printing the [L2TP](https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol) vpn service running on the port 1701/UPD identified the firewall with the hostname PFSWFW from the vendor [Mikrotik](https://mikrotik.com/). The tester didn’t manage to correctly identify the firewall model or OS version used on the running service.



Using the [Ike-Scan](https://github.com/royhills/ike-scan) tool the tester proceeded to footprint the ike service commonly used by [IPSec](https://en.wikipedia.org/wiki/IPsec) vpn connections. Specifically the tool identified that the service allowed a negotiation(handshake), the encryption method used was 3DES, the DH(Diffie-Hellman)group used was the 2 and the service uses a pre-shared key(AUTH-PSK).



In order to capture the hash used by the IPSec the group name is required and it needs to be brute-forced by using a custom [wordlist](https://github.com/danielmiessler/SecLists/blob/master/Miscellaneous/ike-groupid.txt) that contains common group names used in IPSec configurations. No handshakes have been returned, denoting the failure of the attack.



In case of returned handshake the group-name would be discovered. Holding a valid transformation and the correct group-name would allow to catch the hash used by the VPN service if the [aggressive mode](https://wiki.mikrotik.com/wiki/Manual:IP/IPsec) is allowed on the key exchange phase.

Lastly, managing to “crack” the hash hypothetically would allow the attacker to decrypt the VPN traffic in a MITM (Man in the Middle) attack. Unfortunately, these attacks are time consuming and relatively complicated resulting in rare success on modern infrastructure correctly secured.

# Recommendations

## Overview

As stated before in the Assessment Overview section these recommendation are informative and shouldn’t be seen as a threat instead as a possible improvement of the security posture.

## Remedies

Many networking providers recommend moving away from legacy encryption methods such as 3DES and do not using DH (Diffie-Hellman) keys exchange groups 1 & 2.

My suggestion is to change the encryption method used in the IPSec to AES-256bit and avoid using DH groups below 5(*DH=14 usually is the sweet spot*).

Please advise the manufacturer’s documentation for support and carefully plan and test all the remediation steps to prevent any service disruptions.

*\*DH(Diffie-Hellman) keys exchange: Diffie-Hellman key exchange is a method of digital encryption that securely exchanges cryptographic keys between two parties over a public channel without their conversation being transmitted over the internet. The two parties use symmetric cryptography to encrypt and decrypt their messages.*

*\*Encryption Method: is the process of concealing information by mathematically altering data so that it appears random. In simpler terms, encryption is the use of a "secret code" that only authorized parties can interpret.*