

PCFJ

Parse Core Firewall Logs

Cisco ASA · Juniper SRX

User Manual

Version 1.0.3

TC Consulting

September 2026

Contents

- 1** Introduction
- 2** What the Tool Does
- 3** System Requirements
- 4** Installation and Building
- 5** Quick Start
- 6** The Main Window
- 7** Parsing Options Reference
- 8** The Four Result Tabs
- 9** How Log Lines Are Interpreted
- 10** Service Classification
- 11** Command-Line Test Harness
- 12** Troubleshooting and FAQ
- 13** Roadmap: Firewall Deployment
- A** Appendix A — Quick Reference Card

1 Introduction

PCFJ_GUI (Parse Core Firewall Logs — Juniper) is a Windows desktop utility that reads firewall syslog captures and turns them into a clear, sortable inventory of which network connections were blocked and which were allowed, grouped by the service they represent (DNS, DICOM, SMB, remote access, and so on).

It is the successor to PCF_GUI, which handled Cisco ASA logs only. PCFJ_GUI adds full support for Juniper SRX RT_FLOW session logs and automatically detects which format each line belongs to — so captures from either device, or a folder containing both, are parsed correctly without any manual switch.

The application is written in C# using Windows Forms and targets the version of the .NET Framework (4.x) that ships in-box with Windows 10 and Windows 11. There is no runtime to install, no Visual Studio requirement, and no external dependencies — the program is a single self-contained executable.

Who this manual is for. Network and system administrators who need to review firewall traffic, audit blocked connections, or generate ready-to-paste firewall configuration snippets from real observed traffic. No programming knowledge is required to use the tool.

2 What the Tool Does

At a glance, PCFJ_GUI takes one or more log files and produces four things:

- **Blocked connections** — every unique source/destination/port combination that the firewall denied, with a hit count and first/last-seen timestamps.
- **Allowed connections** — the same inventory for permitted traffic, so you can confirm expected flows and spot anything unexpected.
- **Firewall configuration snippets** — ready-to-paste Cisco ASA object-groups and/or Junos address-book commands for blocked DICOM, SMB, and remote-access traffic.
- **A grouped text report** — a plain-text summary organized by service, suitable for pasting into a ticket or an email.

Along the way it deduplicates repeated log lines into single entries with hit counts, sorts IP addresses numerically, and flags “obsolete” rules — connections that appear as both blocked and allowed, where the older side likely reflects a firewall rule that has since changed.

Everything runs locally. No data leaves your machine, and .zip archives are read entirely in memory — no temporary files are ever extracted to disk.

3 System Requirements

Item	Requirement
Operating system	Windows 10 or Windows 11 (64-bit or 32-bit)
Runtime	.NET Framework 4.x — present in-box on all supported Windows versions
Disk space	Under 1 MB for the executable
Privileges	Standard user; no administrator rights needed to run
To build from source	The in-box C# compiler (csc.exe); no Visual Studio required

4 Installation and Building

If you were given the compiled program, no installation is required. Copy PCFJ_GUI.exe to any folder and double-click it to run.

4.1 Building from source

The project includes a build script that uses the C# compiler already present on every Windows 10/11 machine. Open a Command Prompt in the project folder and run:

<code>build.bat</code>	builds PCFJ_GUI.exe
<code>build.bat test</code>	builds and runs the parser self-tests (79 checks)

The build script locates the framework compiler automatically, first trying the 64-bit path and falling back to 32-bit. On success it reports “Built PCFJ_GUI.exe”.

4.2 Project files

File	Purpose
<code>PcfjGui.cs</code>	The entire application — parser and user interface
<code>TestHarness.cs</code>	Console self-tests and a real-capture statistics mode
<code>build.bat</code>	Build script (uses the in-box compiler)
<code>README.md</code>	Short technical summary for developers

5 Quick Start

To produce a report in under a minute:

1. Launch PCFJ_GUI.exe.
2. Click **Add Files...** and choose one or more log files (.txt, .log, or .zip), or click **Folder...** to add every log in a folder.
3. Leave the default options as they are for a first pass.
4. Click **Parse Logs**. A progress bar tracks the work; the status bar reports the detected format and totals when finished.
5. Review the results in the **Blocked**, **Allowed**, **FW Rules**, and **Text Report** tabs.
6. Export any grid to CSV, or copy/save the text panels, using the buttons on each tab.

Tip. The file box accepts semicolon-separated entries, including wildcards such as Z:\logs\sys*.zip. You can type or paste paths directly instead of using the buttons.

6 The Main Window

The window is organized top to bottom into three areas:

- **The input bar** at the top holds the log-file path box and the **Add Files...** / **Folder...** buttons.
- **The options row** beneath it contains the parsing controls described in Section 7, followed by the **Parse Logs** button and a progress bar.
- **The results tabs** fill the rest of the window and are described in Section 8.

A status bar along the bottom edge shows readiness messages, live progress while parsing, and a summary line when parsing finishes — including how many lines were recognized as Cisco ASA versus Juniper, and any lines that were skipped.

7 Parsing Options Reference

These controls sit in the options row and take effect the next time you click Parse Logs.

Option	Default	What it does
Parse allowed connections too	On	When on, permitted traffic is inventoried in the Allowed tab. Turn off to focus only on blocked traffic and speed up large parses.
Include allowed UDP/ICMP	Off	By default only allowed TCP sessions are counted. Enable this to also include allowed UDP and ICMP sessions (for example DNS-over-UDP, which can dominate a capture).
Hide ports ≥	Off	When enabled, connections whose port is at or above the given threshold (default 20000) are dropped. Useful for hiding ephemeral high-numbered client ports.
Last N days	0 (all)	Restricts processing to the last N days. Input files whose last-modified date is older than N days are skipped entirely; the files that

		remain are then trimmed line-by-line using each line's own timestamp. Zero means no date filter (every file is read).
Include only IP	empty	When set, only connections whose source or destination equals this exact IP are kept.
Exclude IP	empty	When set, any connection whose source or destination equals this IP is dropped.
Local subnet prefixes	192.168.192. , 192.168.193.	Comma- or semicolon-separated address prefixes that identify your internal networks. Used only by the FW Rules tab to decide which end of a blocked connection is the 'foreign' address.

8 The Four Result Tabs

8.1 Blocked and Allowed

These two tabs share the same layout: a filter box, an Export CSV button, and a table with one row per unique connection. The columns are:

Column	Meaning
Source IP	The originating address of the connection.
Destination IP	The target address.
Port	The destination port, or "icmp" for ICMP traffic.
Service	The service category the port maps to (see Section 10).
Hits	How many log lines collapsed into this one entry.
First Seen / Last Seen	The earliest and latest timestamps observed for this connection.
Notes	Shows "obsolete" when a connection appears as both blocked and allowed and this is the older side.

Click any column header to sort by it. Source and destination addresses sort numerically (so 192.168.2.10 comes before 192.168.10.2), and ports and hit counts sort as numbers, not text. Type in the filter box to show only rows matching your text across the address, port, and service columns. Export CSV writes the currently displayed rows to a spreadsheet-friendly file.

8.2 FW Rules

This tab generates ready-to-paste firewall configuration for the blocked DICOM, SMB, and remote-access (VNC/RDP) traffic found in the logs. The format matches the device(s) actually detected:

- **Cisco ASA** — object-group network statements listing the foreign addresses.

- **Juniper SRX** — zone-based set security zones ... address-book commands defining address objects and address-sets, for example:

```
set security zones security-zone untrust address-book address 10.0.70.40 10.0.70.40/32
set security zones security-zone untrust address-book address-set DICOM_Server address
10.0.70.40
```

If a capture contains both formats, both sections are produced. The “foreign” address in each rule is chosen using the Local subnet prefixes option: when the source of a blocked connection is on a local subnet, the destination is treated as the address of interest, and vice versa. Duplicate addresses are removed and the list is sorted numerically.

Tuning the Junos output. An options row on this tab shapes the Juniper commands (the ASA object-groups are unaffected). Change any field and click **Regenerate** — no re-parse is needed. The controls are:

- **Junos zone** (default untrust) — objects are created in this zone's address book, matching the zone-based style the device uses. Unknown hosts land here.
- **DICOM set / SMB set / RDP-VNC set** — the address-set names to add the blocked foreign IPs to. The defaults DICOM_Server and File_Servers match the device's real group names. Clear a field to skip that service.
- **Reuse names from config (optional)** — point this at a Junos running-config text file and the generator reuses existing address-book object names (such as Elekta or GW) for any foreign IP already named in the target zone, instead of creating a new object. Harvesting is zone-aware and uses host (/32) addresses only.

Unknown foreign hosts are defined using the address itself as the object name (for example “address 10.0.70.40 10.0.70.40/32”), matching the device's own convention. Use the Copy or Save As buttons to capture the output.

8.3 Text Report

The text report reproduces the classic grouped-by-service summary of the original command-line tool. Blocked traffic is listed first, then allowed traffic if that option is enabled, each broken into service sections with a running total. Individual lines take the form:

```
192.168.193.20 ==> 8.8.4.4/53 (2)
```

meaning source, destination, destination port, and — in parentheses — the hit count. Entries flagged as obsolete are marked with “*obsolete”. Copy or Save As are available here as well.

9 How Log Lines Are Interpreted

PCFJ_GUI inspects each line and decides whether it comes from a Cisco ASA or a Juniper SRX, then extracts the connection details. The table below summarizes how each message type is handled.

Log message	Treated as	Notes
ASA Deny ...	Blocked	Direction (inside→outside or the reverse) determines source and destination orientation.
ASA TCP access denied	Blocked	Traffic denied to the firewall itself; uses the 'from' address as source.
ASA Built inbound/outbound TCP	Allowed	UDP equivalents are counted only when Include allowed UDP/ICMP is on.
SRX RT_FLOW_SESSION_DENY	Blocked	Source, destination, and destination port come from the original flow. ICMP (protocol 1) normalizes the port to "icmp".
SRX RT_FLOW_SESSION_CREATE	Allowed	Uses the pre-NAT source and destination so real endpoints are shown. TCP is always counted; UDP (17) and ICMP (1) only when the checkbox is on.
SRX RT_FLOW_SESSION_CLOSE	Ignored	Every close pairs with a create; counting both would double the hit counts.

Both formats retain the syslog-collector line prefix (for example "Sun Jun 28 23:00:09 2026;10.96.247.2; <14>..."). The leading 24-character timestamp on each line drives the per-line date filter and the first/last-seen columns.

Obsolete-rule detection. When the same source, destination, and port appear in both the blocked and allowed inventories, the firewall's handling of that flow changed at some point. The side with the older last-seen timestamp is flagged as obsolete, highlighting rules that may no longer reflect reality.

10 Service Classification

Each connection is tagged with a service category based on its destination port. This drives the grouping in the text report and the Service column in the grids.

Service	Ports / rule
DNS / Active Directory	53, 88, 135, 389, 464, 3268, 3269
HTTP	80
HTTPS	443
DICOM	104–109, 10401, 11112, 11113, 57200/57201, 57345/57347, 50505/50506
SMB / NetBIOS	137, 138, 139, 445

GotoMyPC	8200
ICMP	Traffic with no numeric port
IDMS	4000–4099
VNC / RDP	3389–3415, 5900
WSUS	8530, 8531
MIM / Precise ART	13913, 17190–17198
PTC Axeda/ThingWorx	17001, 17002
Misc. services	20, 21, 22, 23, 37, 123, 161, 990, 8080, 9100
Unknown / other	Anything not matched above

11 Command-Line Test Harness

A companion console program verifies the parser and doubles as a quick command-line report generator.

11.1 Running the self-tests

From the project folder:

```
build.bat test
```

This builds and runs 79 checks covering both log formats, the option switches, orientation of source/destination, deduplication, obsolete-rule detection, service classification, the generated firewall rules, and the Junos config-name harvesting. Each check prints PASS or FAIL, ending with an overall result.

11.2 Parsing a real capture from the command line

Pass a log file to the test executable to print statistics and the full text report without opening the GUI:

```
PCFJ_Tests.exe Z:\logs\somecapture.txt
```

The output lists total lines, how many were recognized as ASA versus Juniper, the count of unrecognized timestamps, the number of unique blocked and allowed connections, and then the grouped report. This mode enables allowed UDP/ICMP so nothing is hidden. It is a fast way to sanity-check a new capture or confirm that every line in a file is recognized.

12 Troubleshooting and FAQ

Q. I clicked Parse Logs but nothing appeared.

A. Confirm the file box points at real files. It accepts semicolon-separated paths, folders, and wildcards; the tool looks for .txt, .log, and .zip files. If you added a folder, only those three extensions are picked up.

Q. The status bar says many lines were skipped as unreadable dates.

A. PCFJ_GUI expects each line to begin with a 24-character timestamp like Mon Dec 13 14:22:33 2021. If your collector writes a different prefix, those lines are counted as bad dates and skipped. Send a sample line and the parser can be extended.

Q. A capture parsed, but the Juniper line count looks far lower than the total.

A. That usually means the SRX is logging in *structured-data format* (fields such as source-address="..." in brackets) rather than the standard space-separated layout this version reads. Capture a sample line so support for that variant can be added.

Q. Why is allowed UDP traffic (like DNS) missing?

A. By design. Allowed UDP and ICMP are counted only when **Include allowed UDP/ICMP** is enabled, because on a busy network DNS-over-UDP can otherwise dominate the report. Enable the checkbox and parse again.

Q. What does “obsolete” in the Notes column mean?

A. The same connection was seen both blocked and allowed. The older of the two is flagged as obsolete, indicating the firewall's treatment of that flow changed and one side may reflect a stale rule.

Q. Are my logs uploaded anywhere?

A. No. All processing is local. ZIP archives are read in memory and never extracted to disk.

13 Roadmap: Firewall Deployment

A future version is planned that would push the generated rules directly to a firewall over a serial console or an SSH connection, letting the operator choose the device type (ASA or Juniper), the connection method, the port or address, and supply login, password, and enable credentials.

This capability is not present in version 1.0. It is documented here so users are aware of the intended direction. Any deployment feature will include safeguards such as Junos “commit confirmed” automatic rollback, an explicit opt-in before saving configuration on the ASA, and a full transcript of every command sent and received. Credentials would be held in memory only and masked in the transcript.

Appendix A — Quick Reference Card

Common tasks

To do this...	Do this
Add logs	Add Files... / Folder..., or type paths (semicolon-separated, wildcards allowed)
Run the analysis	Click Parse Logs
See only blocked traffic	Turn off "Parse allowed connections too"
Include DNS/UDP and ICMP	Turn on "Include allowed UDP/ICMP"
Focus on one host	Type its address in "Include only IP"
Sort a grid	Click the column header
Search a grid	Type in the Filter box
Get firewall config	Open the FW Rules tab; Copy or Save As
Target a Junos zone / rename sets	Edit the FW Rules options row, then Regenerate
Reuse existing Junos object names	Point "Reuse names from config" at a running-config file
Export to spreadsheet	Export CSV on the Blocked or Allowed tab

Build commands

Command	Result
<code>build.bat</code>	Builds PCFJ_GUI.exe
<code>build.bat test</code>	Builds and runs the 79 self-tests
<code>PCFJ_Tests.exe <file></code>	Prints stats and a full report for a capture