NP-View User Manual

Network Perception
support@network-perception.com

Last updated
October 2017

Background

- NP-View is a firewall audit tool developed at Network Perception

- We are a team of software engineers, researchers, and industry experts from the University of Illinois

Mouna Bamba
Senior Developer

Robin Berthier
President

David Nicol
Technology Advisor

Edmond Rogers
Industry Advisor

Bill Sanders
Business Advisor

Feature Overview

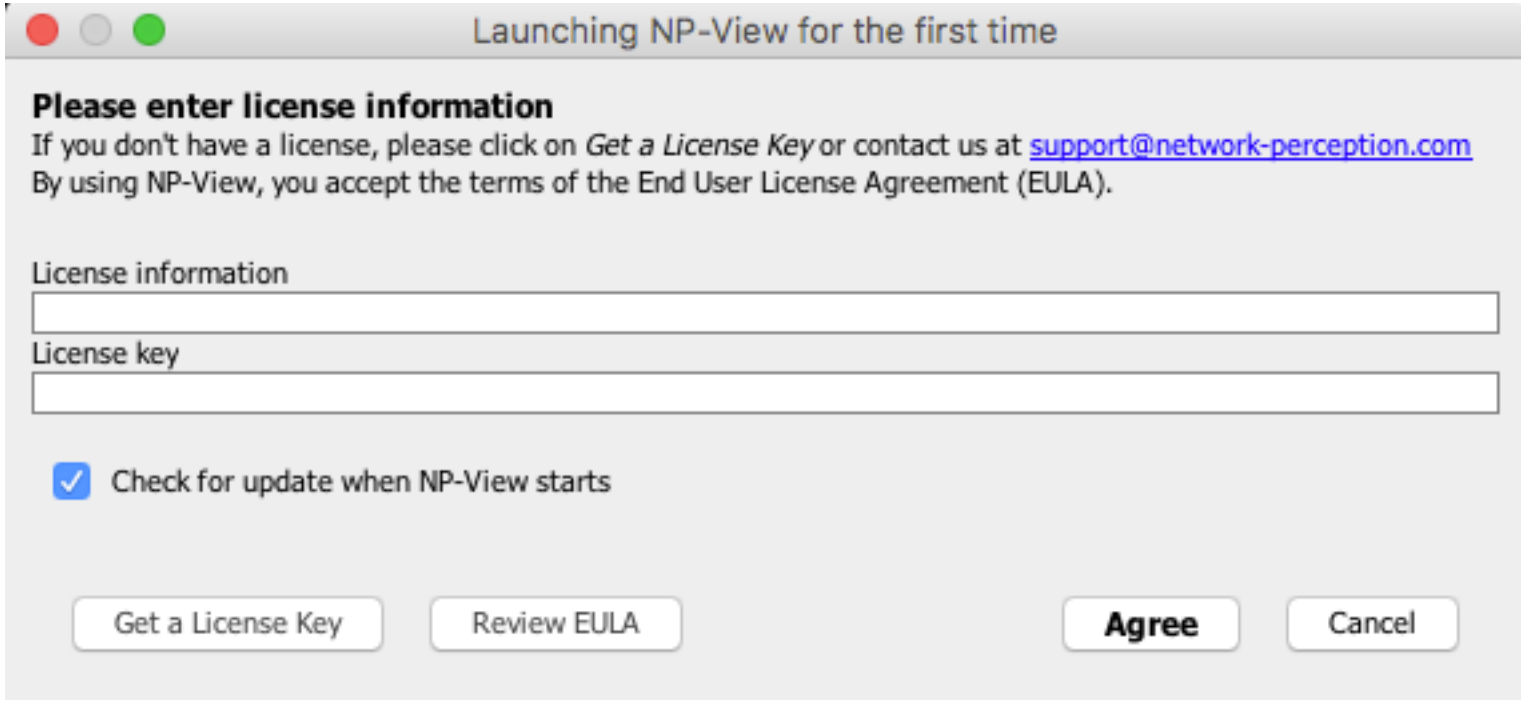
- Lightweight
  - Works offline and no installer needed
- Firewall audit
  - Health check filters automatically report issues
- Topology Map
  - Generate and export a network diagram
- Path Analysis
  - Detailed connectivity analysis and IP exposure
- Data Exports
  - Generate Excel spreadsheets of collected results

Installation

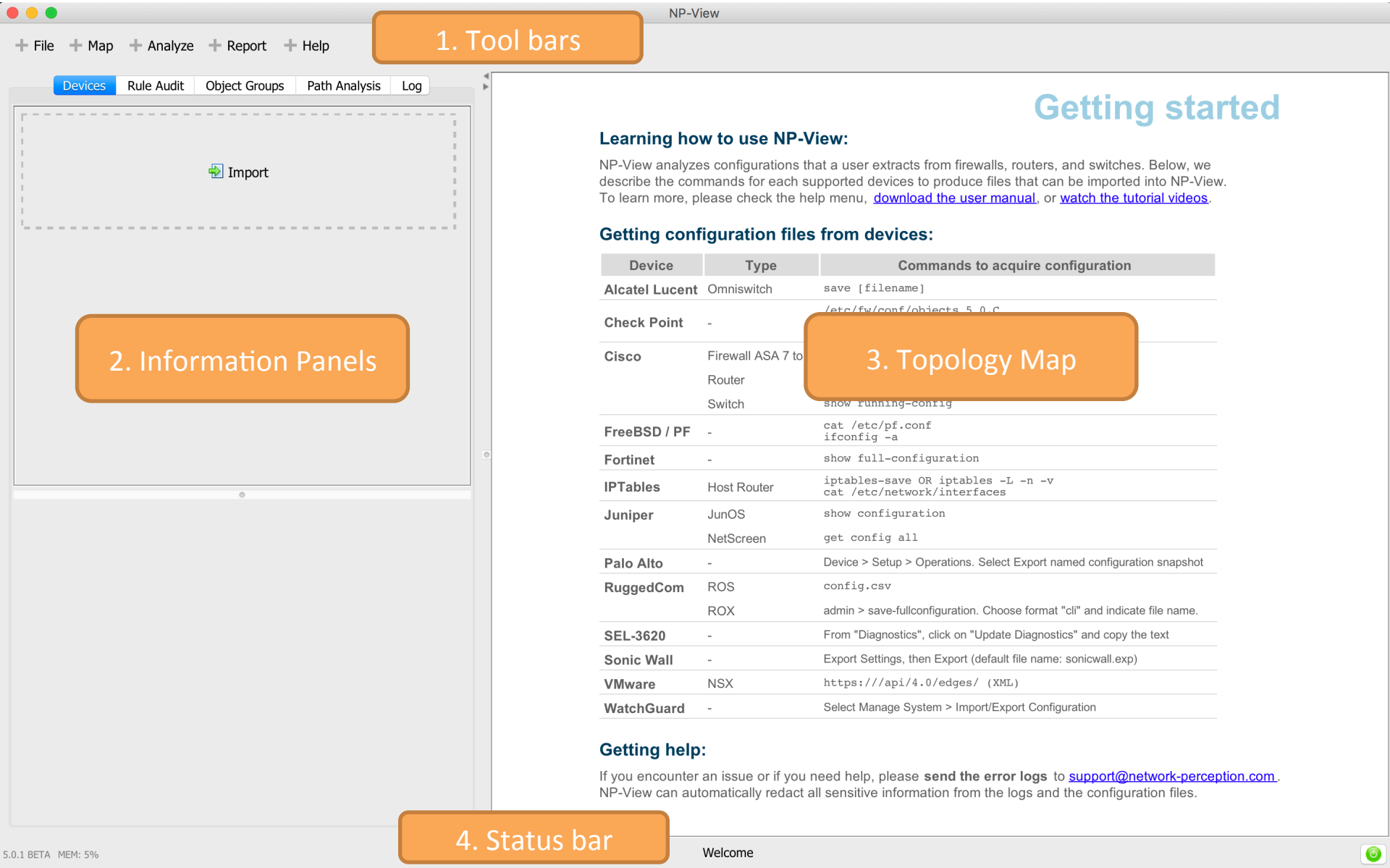
- Make sure the Java Runtime Environment is installed (version 7+)
  - Test by typing “java - version” in a terminal
- Sign up at https://portal.network-perception.com to download the latest version of NP-View and request a license
- Unarchive NP-View in a local folder
- Go to the unarchived folder and launch NP-View:
  - **Windows**: double click on NP-View.exe
  - **Linux**: run ./NP-View.sh
  - **Mac**: double click on NP-View.app

First Run

- Add license information
- Choose to check for updates or not



User Interface



Getting started

Learning how to use NP-View:

NP-View analyzes configurations that a user extracts from firewalls, routers, and switches. Below, we describe the commands for each supported devices to produce files that can be imported into NP-View. To learn more, please check the help menu, download the user manual, or watch the tutorial videos.

Getting configuration files from devices:

Device	Type	Commands to acquire configuration
Alcatel Lucent	Omniswitch	`save [filename]`
Check Point	-	`/etc/fw/conf/objects_5_0.C`
Cisco	Firewall ASA 7 to	
	Router	
	Switch	`show running-config`
FreeBSD / PF	-	`cat /etc/pf.conf` `ifconfig -a`
Fortinet	-	`show full-configuration`
IPTables	Host Router	`iptables-save OR iptables -L -n -v` `cat /etc/network/interfaces`
Juniper	JunOS	`show configuration`
	NetScreen	`get config all`
Palo Alto	-	Device > Setup > Operations. Select Export named configuration snapshot
RuggedCom	ROS	`config.csv`
	ROX	admin > save-fullconfiguration. Choose format "cli" and indicate file name.
SEL-3620	-	From "Diagnostics", click on "Update Diagnostics" and copy the text
Sonic Wall	-	Export Settings, then Export (default file name: sonicwall.exp)
VMware	NSX	`https:///api/4.0/edges/ (XML)`
WatchGuard	-	Select Manage System > Import/Export Configuration

Getting help:

If you encounter an issue or if you need help, please **send the error logs** to support@network-perception.com. NP-View can automatically redact all sensitive information from the logs and the configuration files.

Supported Rulesets

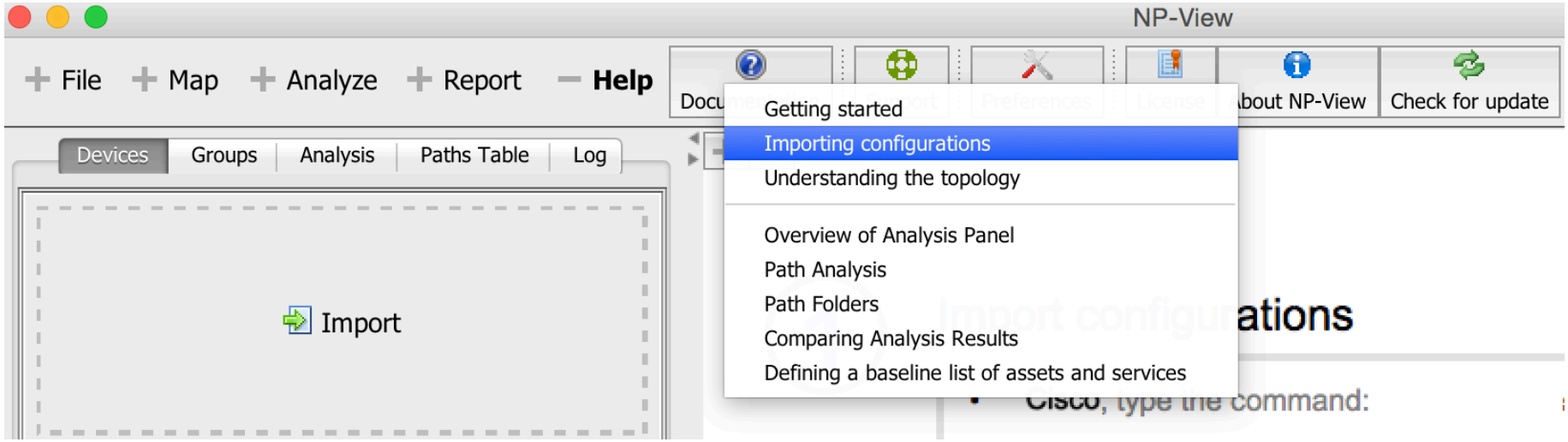
Device	Type	Commands to acquire configuration
Alcatel Lucent	Omniswitch	`save [filename]`

Check Point	-	`/etc/fw/conf/objects_5_0.C`
		`/etc/fw/conf/rulebases_5_0.fws`
		`identity_roles.C (optional)`

Cisco	Firewall ASA 7 to 9	`show running-config`
	Router	`show running-config`
	Switch	`show running-config`
FreeBSD / PF	-	`cat /etc/pf.conf` `ifconfig -a`
Fortinet	-	`show full-configuration`
IPTables	Host Router	`iptables-save OR iptables -L -n -v` `cat /etc/network/interfaces`
Juniper	JunOS	`show configuration`
	NetScreen	`get config all`
Palo Alto	-	Device > Setup > Operations. Select Export named configuration snapshot
RuggedCom	ROS	`config.csv`
	ROX	admin > save-fullconfiguration. Choose format "cli" and indicate file name.
SEL-3620	-	From "Diagnostics", click on "Update Diagnostics" and copy the text
Sonic Wall	-	Export Settings, then Export (default file name: sonicwall.exp)
VMware	NSX	`https:///api/4.0/edges/ (XML)`
WatchGuard	-	Select Manage System > Import/Export Configuration

Important note: the level of coverage for each individual parser depends on requests received from our users. Some parsers cover all the features of a device (for example: Cisco), while more recent parsers only covers a subset of the features available(for example: Check Point).
For a detailed table of supported features, please visit https://portal.network-perception.com
If you encounter issue importing your files, please contact support@network-perception.com

Getting Rulesets



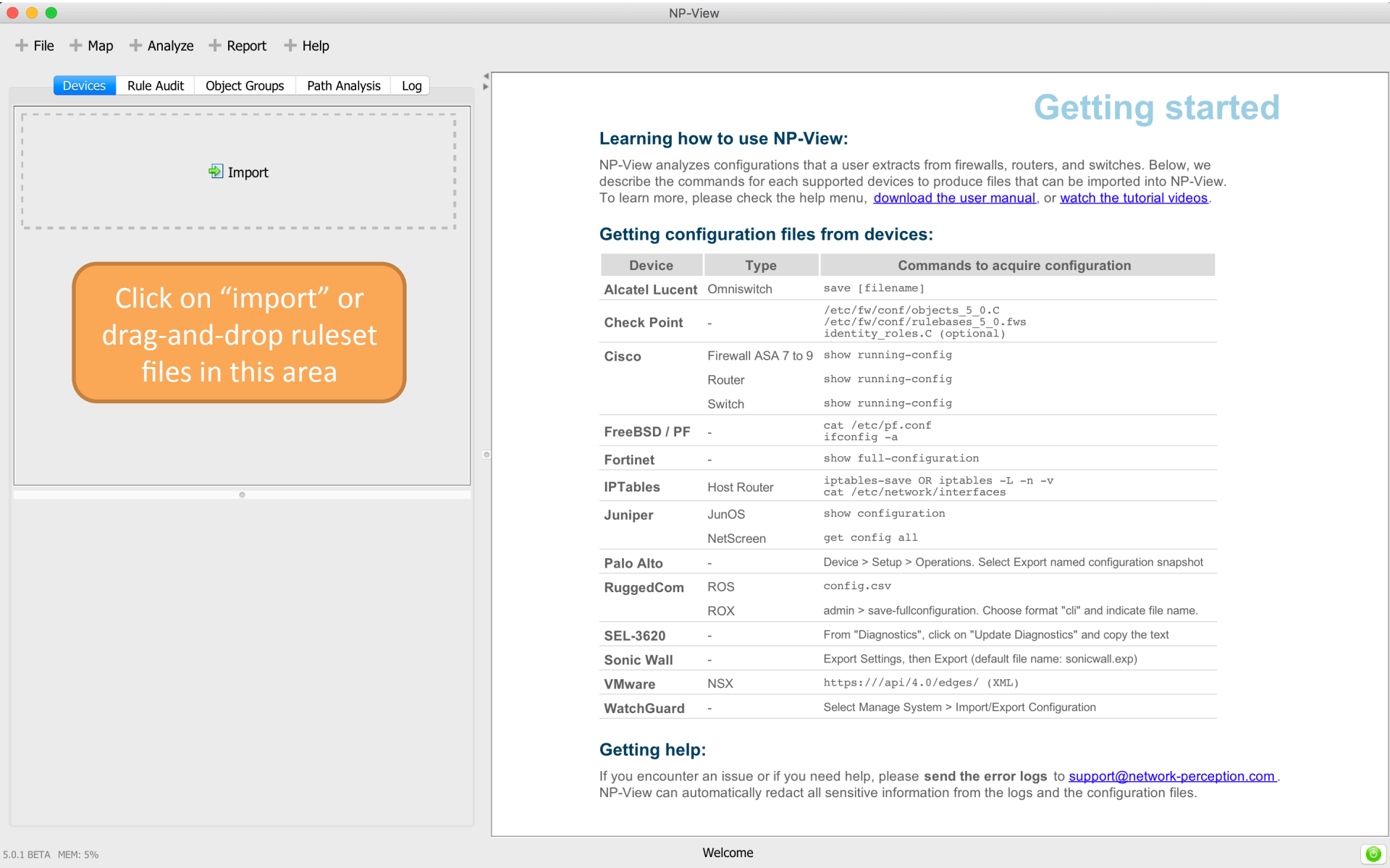
Example for Cisco:

- Using SSH, Telnet, or a direct console connection, you can login to your Cisco device and execute the command `show running-config`.

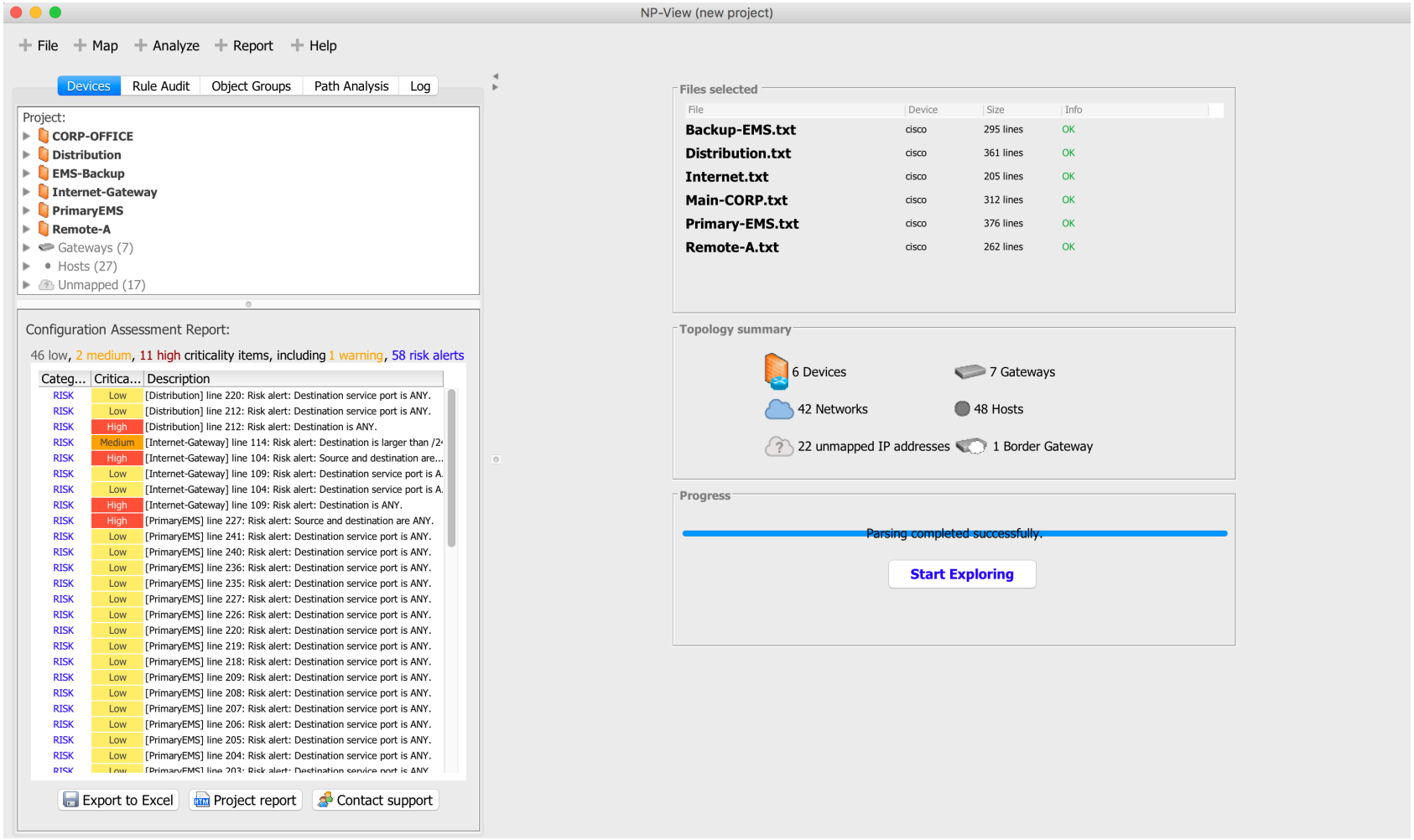
Example for Juniper:

- Login to the Web interface of your Juniper NetScreen device and go to Configuration, then Update, then Config File, and click on the *Save to file* button. Or,
- Connect to the device using SSH or Telnet or the console and type the command get config all. Save the captured output to a file and remove any visible page line.

Importing Rulesets

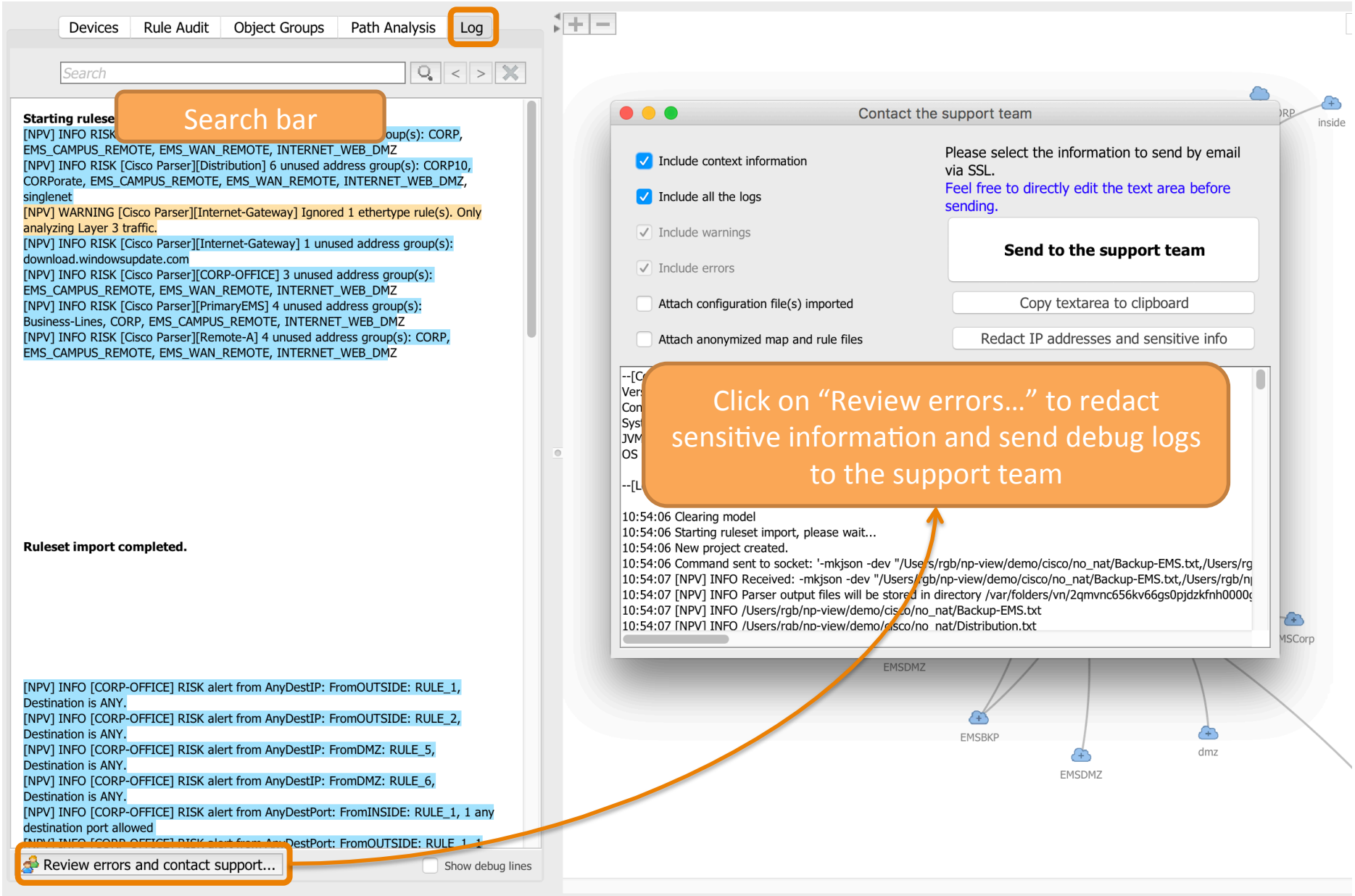


Reviewing Configuration Assessment Report

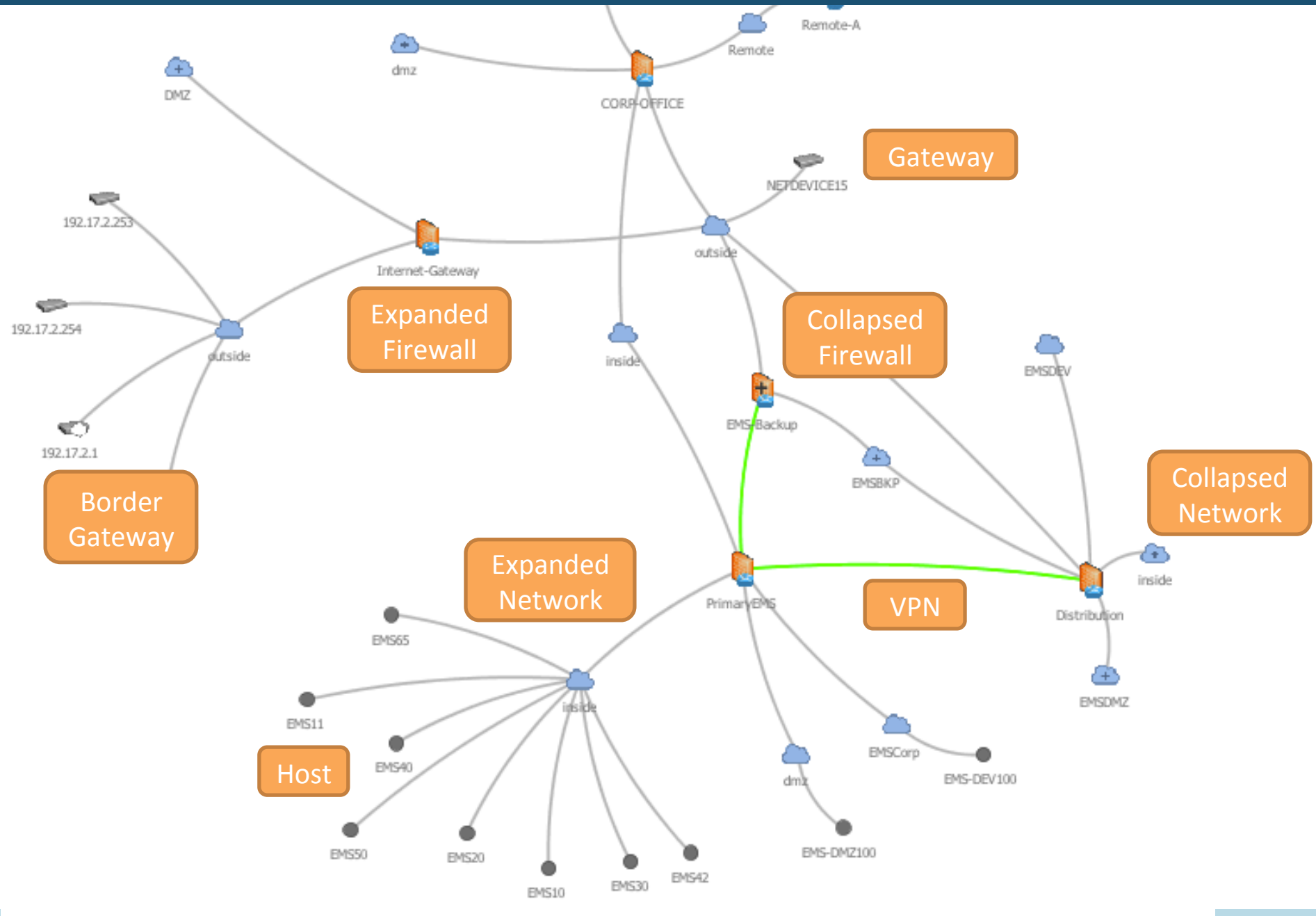


- Risk: rules allowing ‘any’ source, destination, or service. Unused groups. Vulnerabilities.
- Warnings: misconfigurations or unsupported configuration statements
- Error: parser issues or incompatible file format

Getting Assistance Through the Log Panel

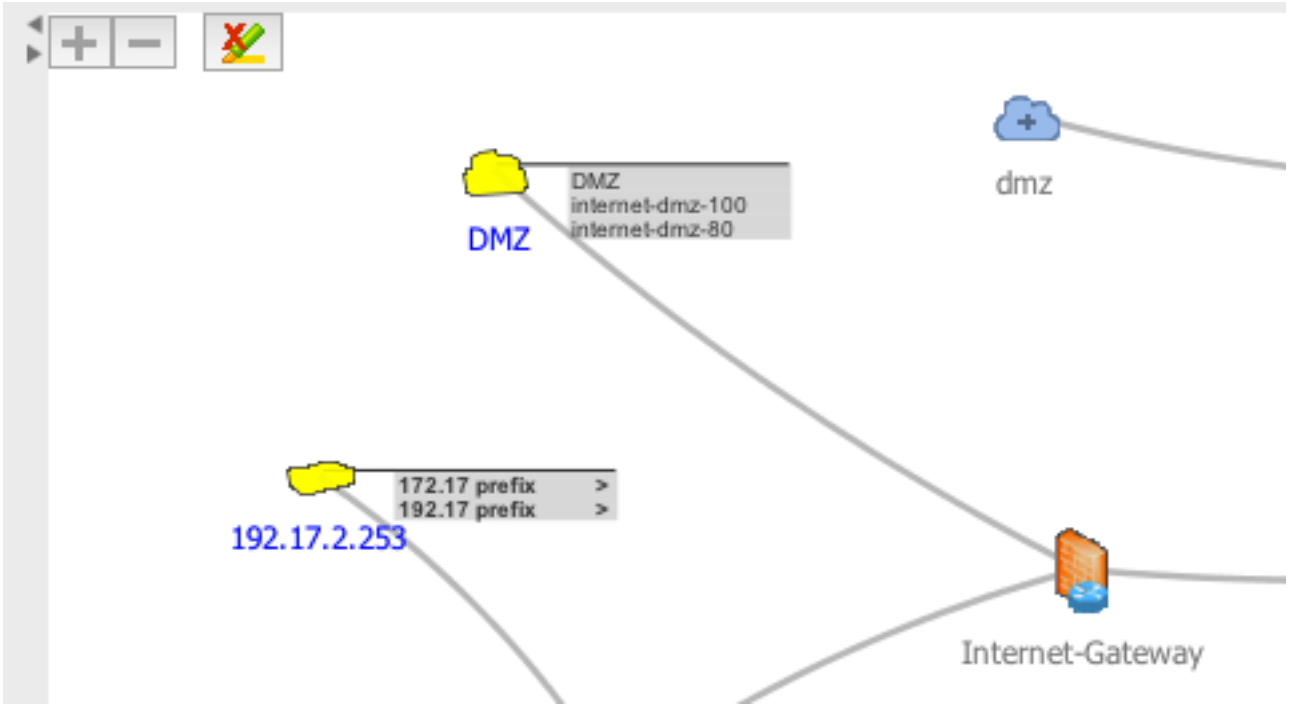


Topology Map

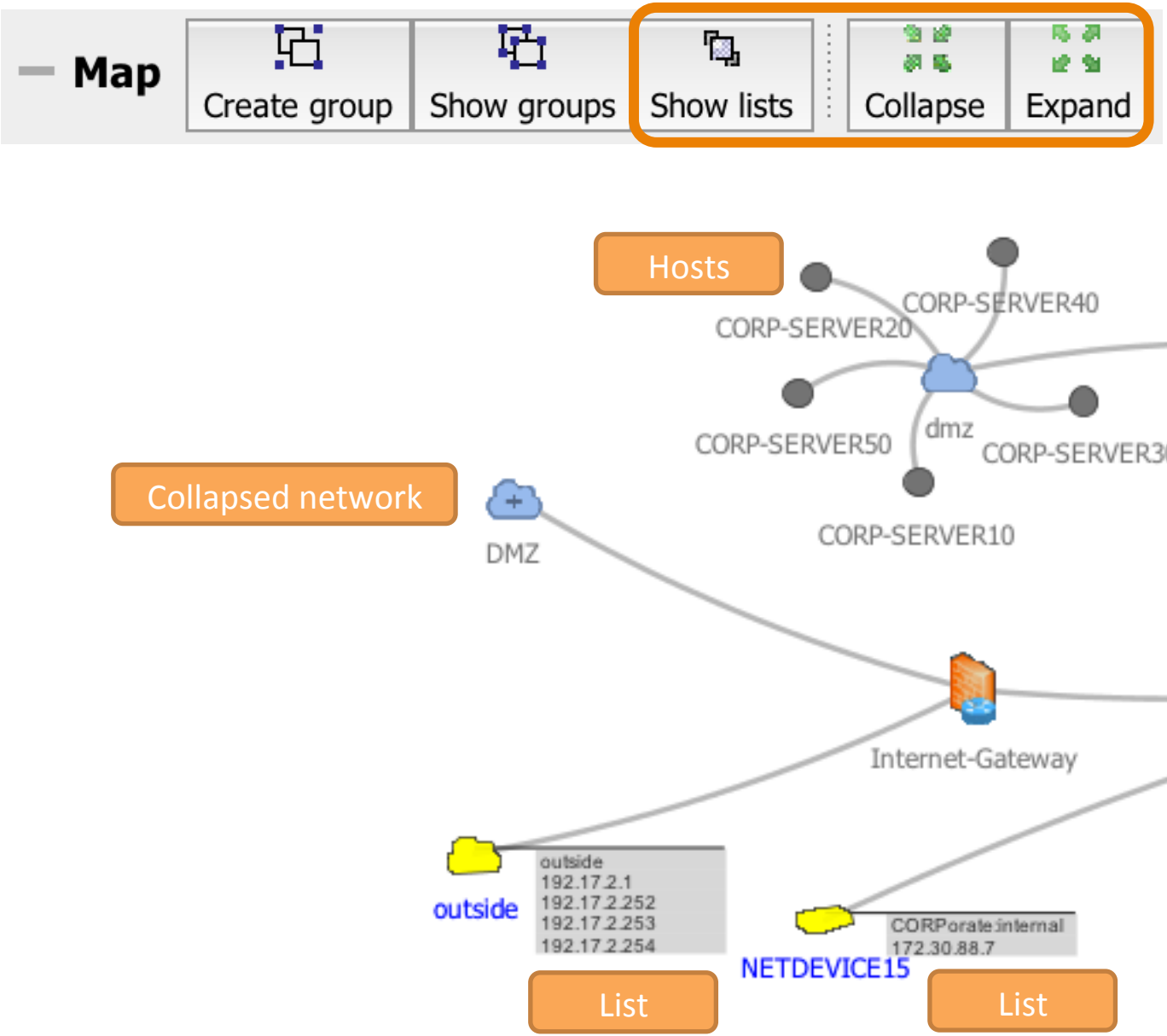


Selection

- Items colored in yellow are selected
- Press SHIFT to add items to your select
- Press SHIFT and drag the mouse to create a selection rectangle
- Press the “clear highlight” button to clear the selection (top left red cross icon)

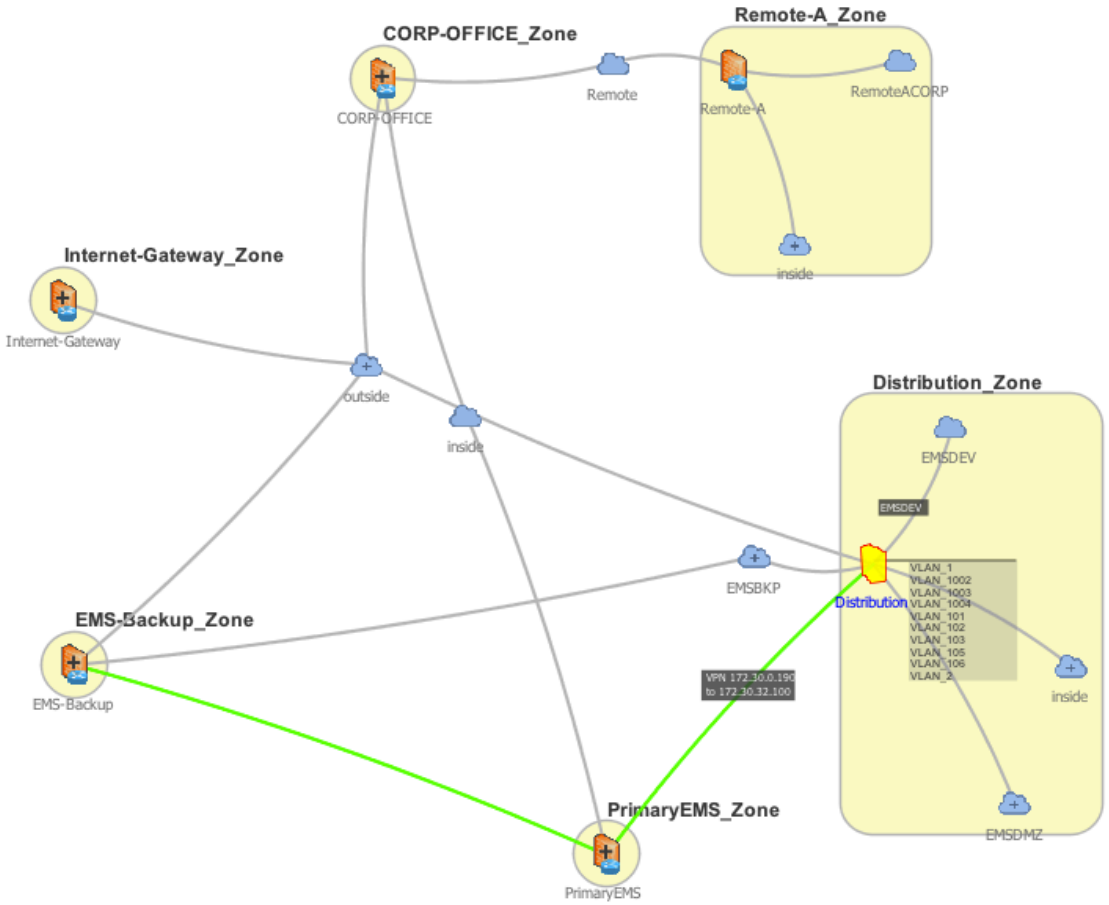


Expansion

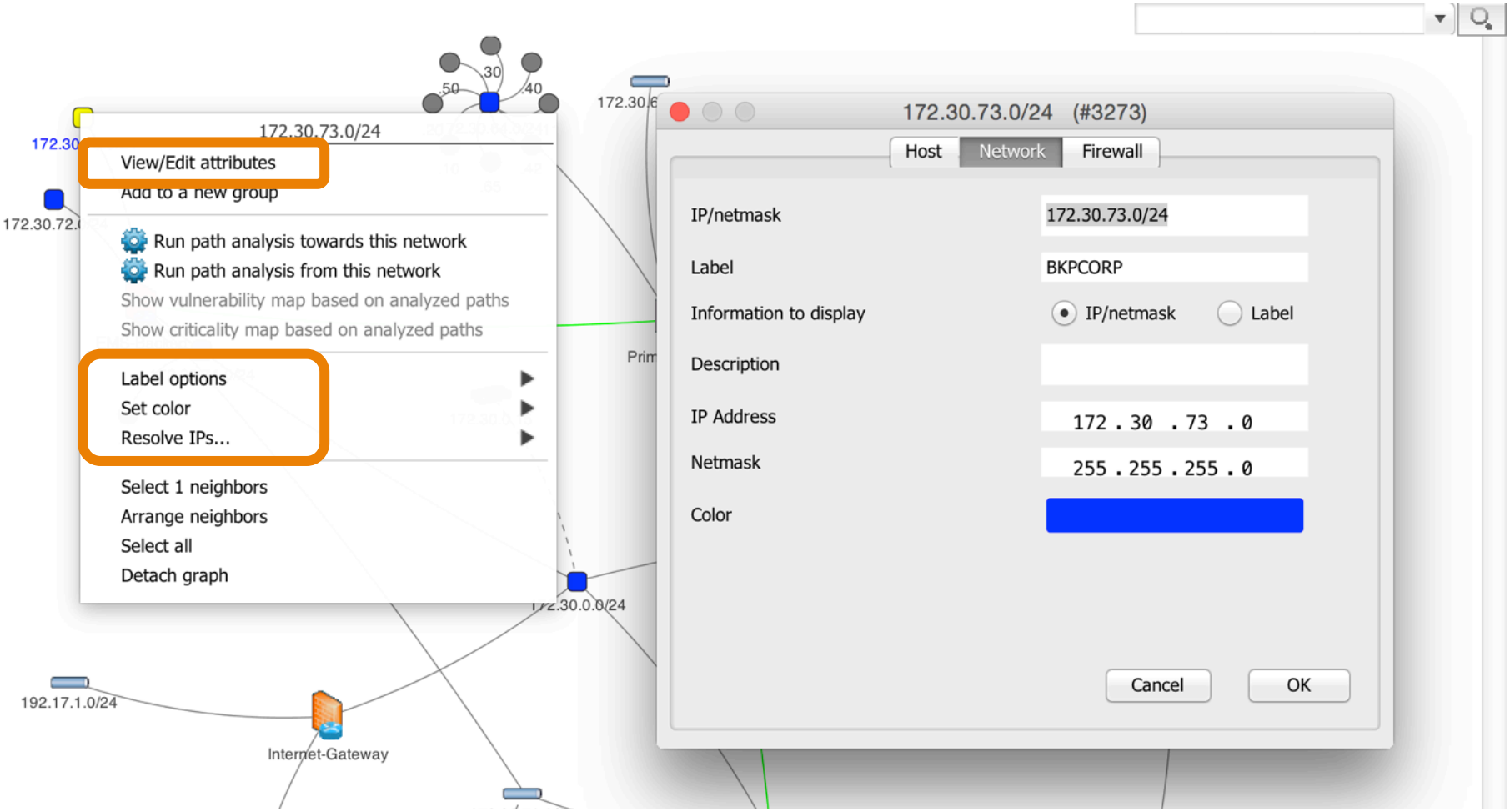

Map
Create group
Show groups
Show lists
Collapse
Expand
Hosts
CORP-SERVER20
CORP-SERVER40
CORP-SERVER50
dmz
CORP-SERVER30
CORP-SERVER10
Collapsed network
DMZ
Internet-Gateway
outside
outside
192.17.2.1
192.17.2.252
192.17.2.253
192.17.2.254
NETDEVICE15
CORPorate:internal
172.30.88.7
List
List

Groups

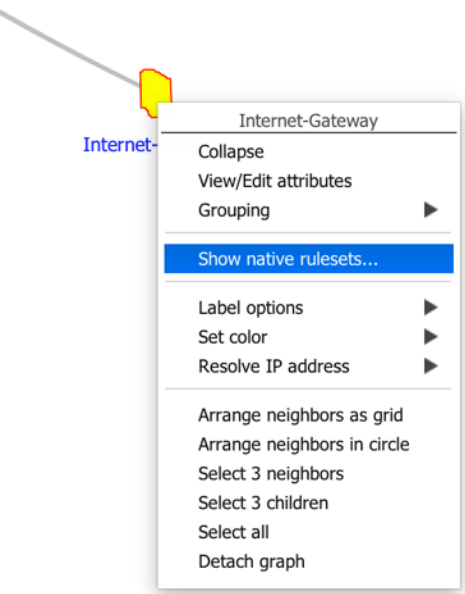
Map
Auto group
Create group
Hide groups

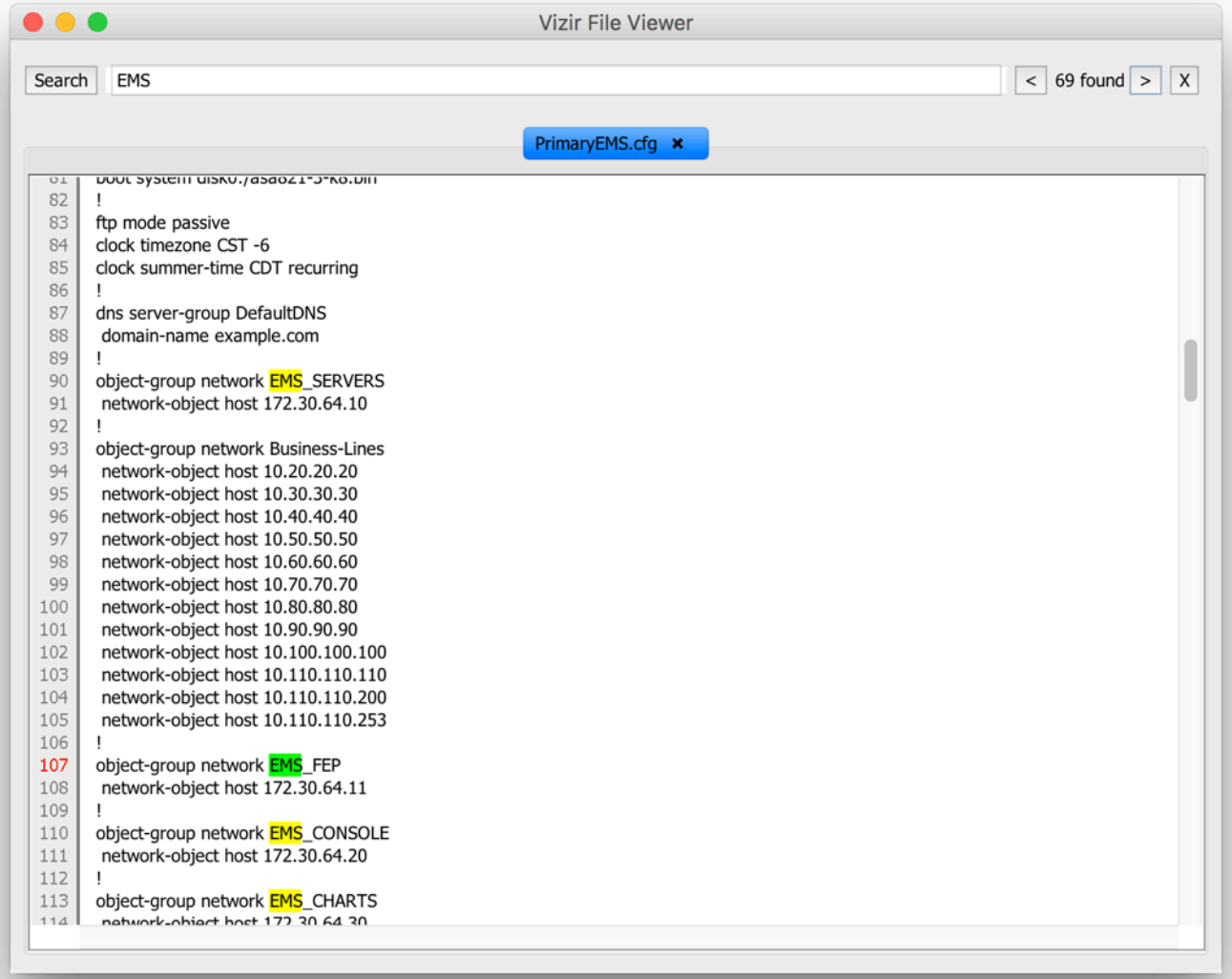

CORP-OFFICE_Zone
CORP-OFFICE
Remote
Remote-A_Zone
Remote-A
RemoteACORP
inside
Internet-Gateway_Zone
Internet-Gateway
outside
inside
Distribution_Zone
EMSDEV
EMSDEV
EMSBKP
Distribution
VLAN_1
VLAN_1002
VLAN_1003
VLAN_1004
VLAN_101
VLAN_102
VLAN_103
VLAN_105
VLAN_106
VLAN_2
inside
EMSDMZ
EMS-Backup_Zone
EMS-Backup
VPN 172.30.0.190
to 172.30.32.100
PrimaryEMS_Zone
PrimaryEMS

Contextual Menu



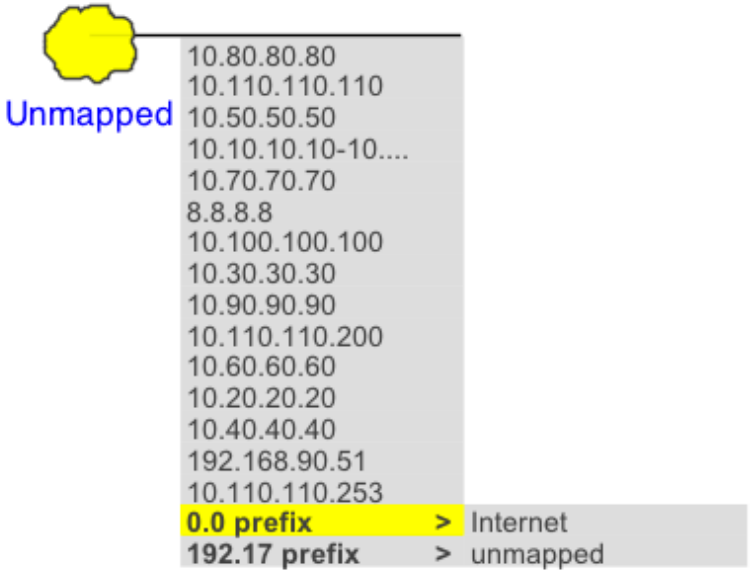
File Viewer


Internet-
Internet-Gateway
Collapse
View/Edit attributes
Grouping
Show native rulesets...
Label options
Set color
Resolve IP address
Arrange neighbors as grid
Arrange neighbors in circle
Select 3 neighbors
Select 3 children
Select all
Detach graph


Vizir File Viewer
Search
EMS
< 69 found >
X
PrimaryEMS.cfg
82 !
83 ftp mode passive
84 clock timezone CST -6
85 clock summer-time CDT recurring
86 !
87 dns server-group DefaultDNS
88 domain-name example.com
89 !
90 object-group network EMS_SERVERS
91 network-object host 172.30.64.10
92 !
93 object-group network Business-Lines
94 network-object host 10.20.20.20
95 network-object host 10.30.30.30
96 network-object host 10.40.40.40
97 network-object host 10.50.50.50
98 network-object host 10.60.60.60
99 network-object host 10.70.70.70
100 network-object host 10.80.80.80
101 network-object host 10.90.90.90
102 network-object host 10.100.100.100
103 network-object host 10.110.110.110
104 network-object host 10.110.110.200
105 network-object host 10.110.110.253
106 !
107 object-group network EMS_FEP
108 network-object host 172.30.64.11
109 !
110 object-group network EMS_CONSOLE
111 network-object host 172.30.64.20
112 !
113 object-group network EMS_CHARTS

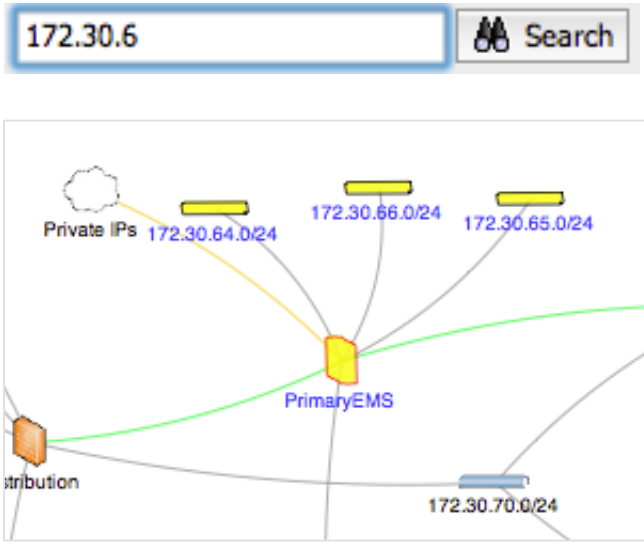
Unmapped Cloud

- IP addresses found in rules and object groups are attached to networks and gateways in the topology
- Unmapped has all the IP addresses that could not find a parent network.

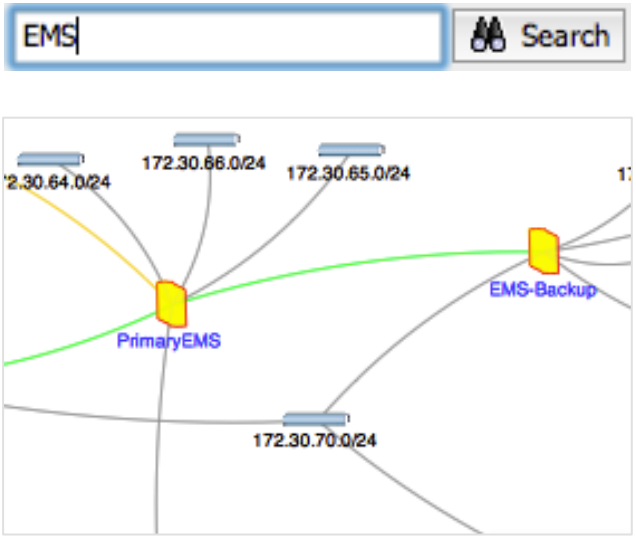


Search Bar

- Search by IP starting with 172.30.6*.*



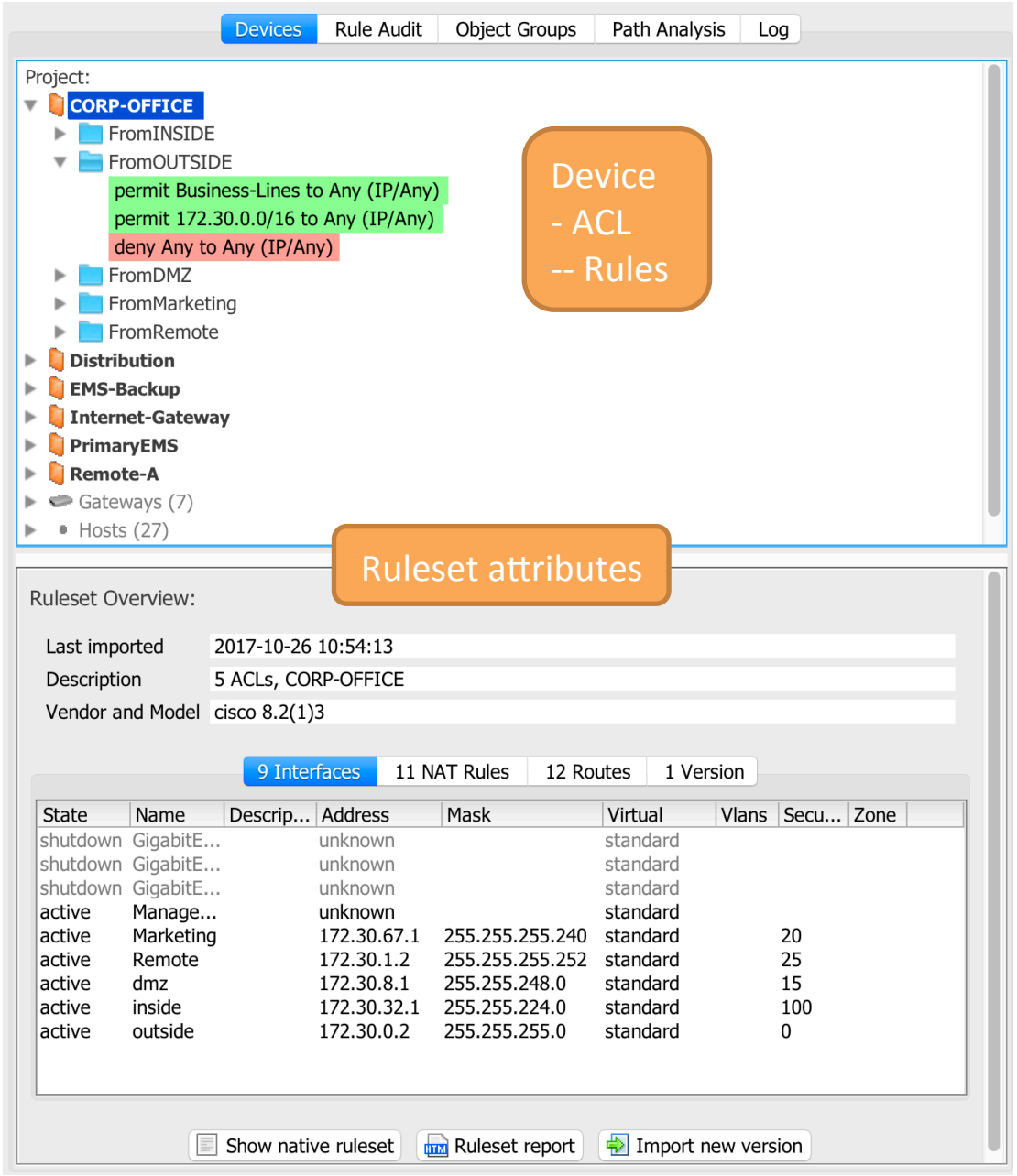
- Search by ID names



Saving the Project

- .npv file are zipped folder with XML files of the topology, the converted rulesets, and the analysis results.

Device Tab



Interfaces

Physical Ports

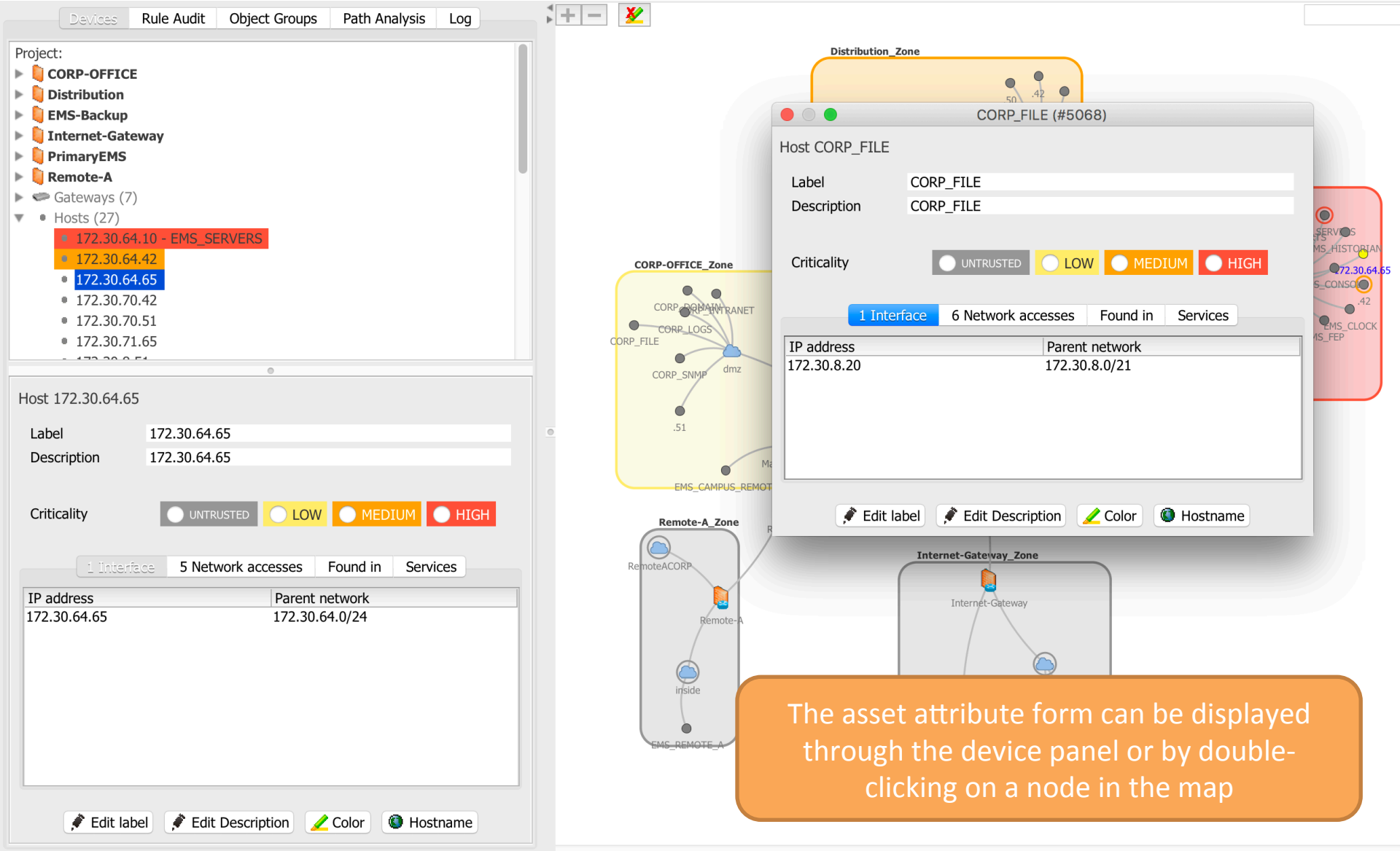
NAT Rules

Routes

Versions

Marking Asset Criticality

4 criticality levels: UNTRUSTED, LOW, MEDIUM, HIGH. Marking criticality will help highlight rules and paths



The asset attribute form can be displayed through the device panel or by double-clicking on a node in the map

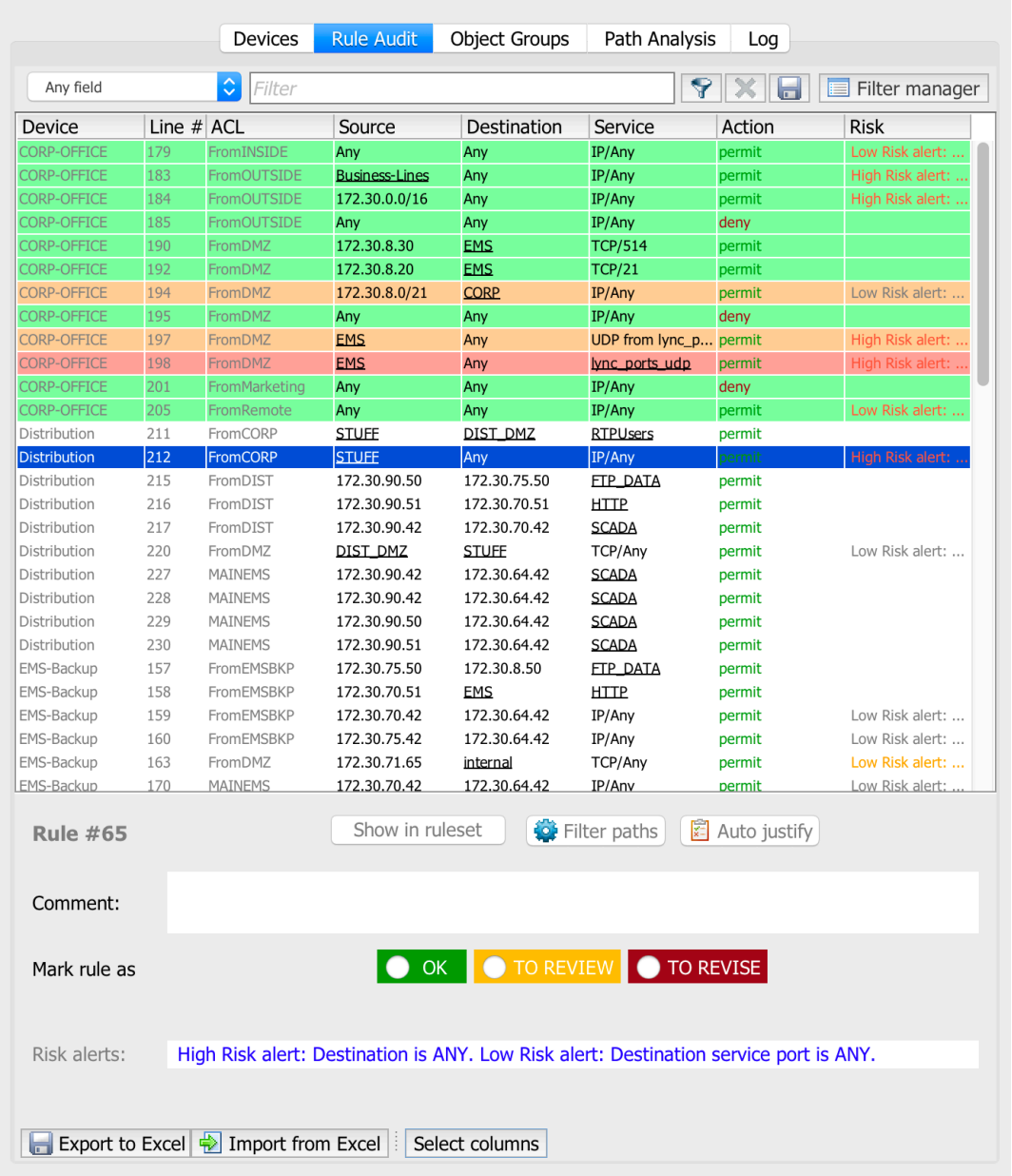
Rule Audit Tab

Search and Filter

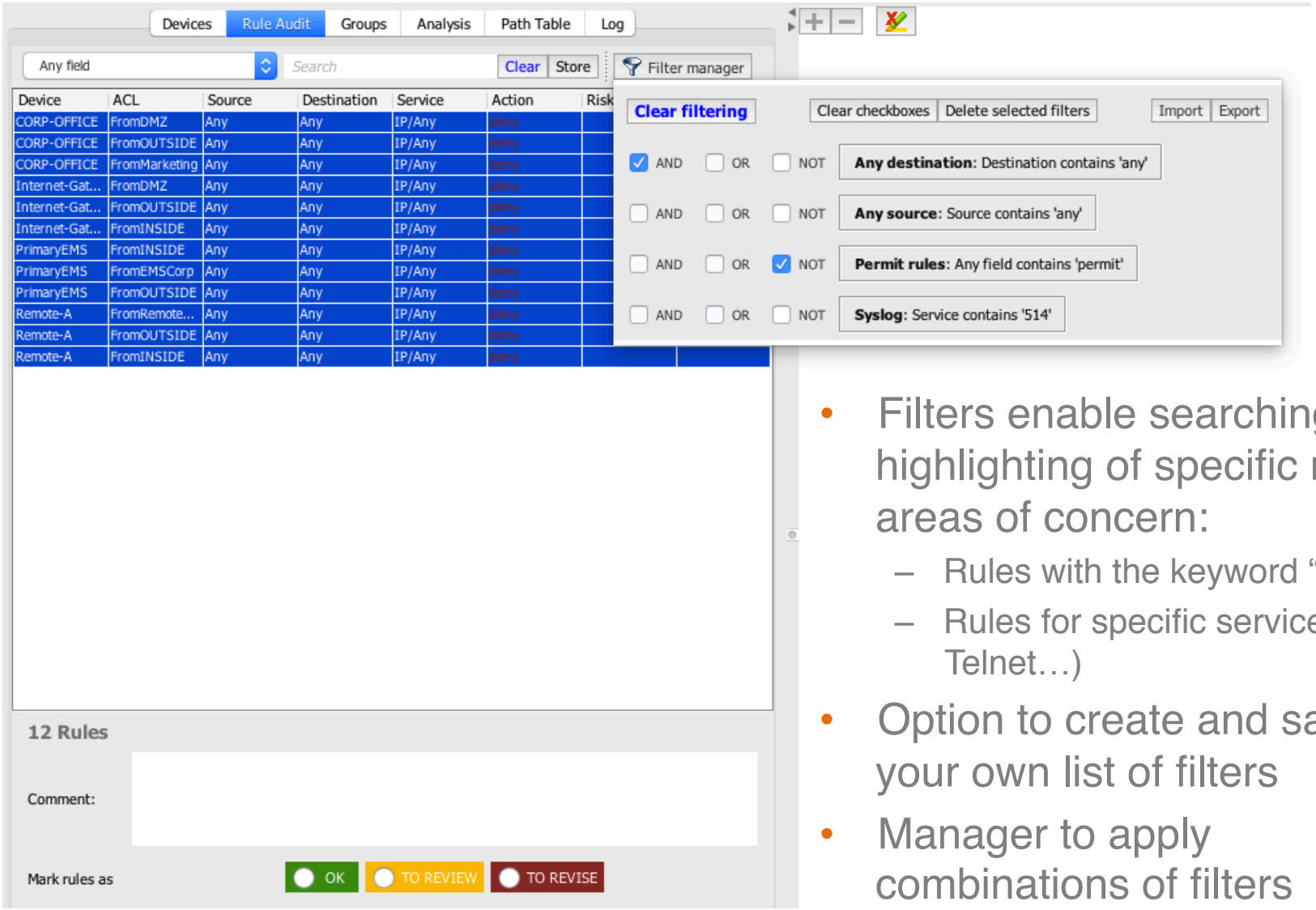
Add rule justifications

Select and annotate

Export to Excel



Rule Filter



- Filters enable searching and highlighting of specific rules or areas of concern:
  - Rules with the keyword “any”
  - Rules for specific services (HTTP, Telnet…)
- Option to create and save your own list of filters
- Manager to apply combinations of filters
- Form to annotate results

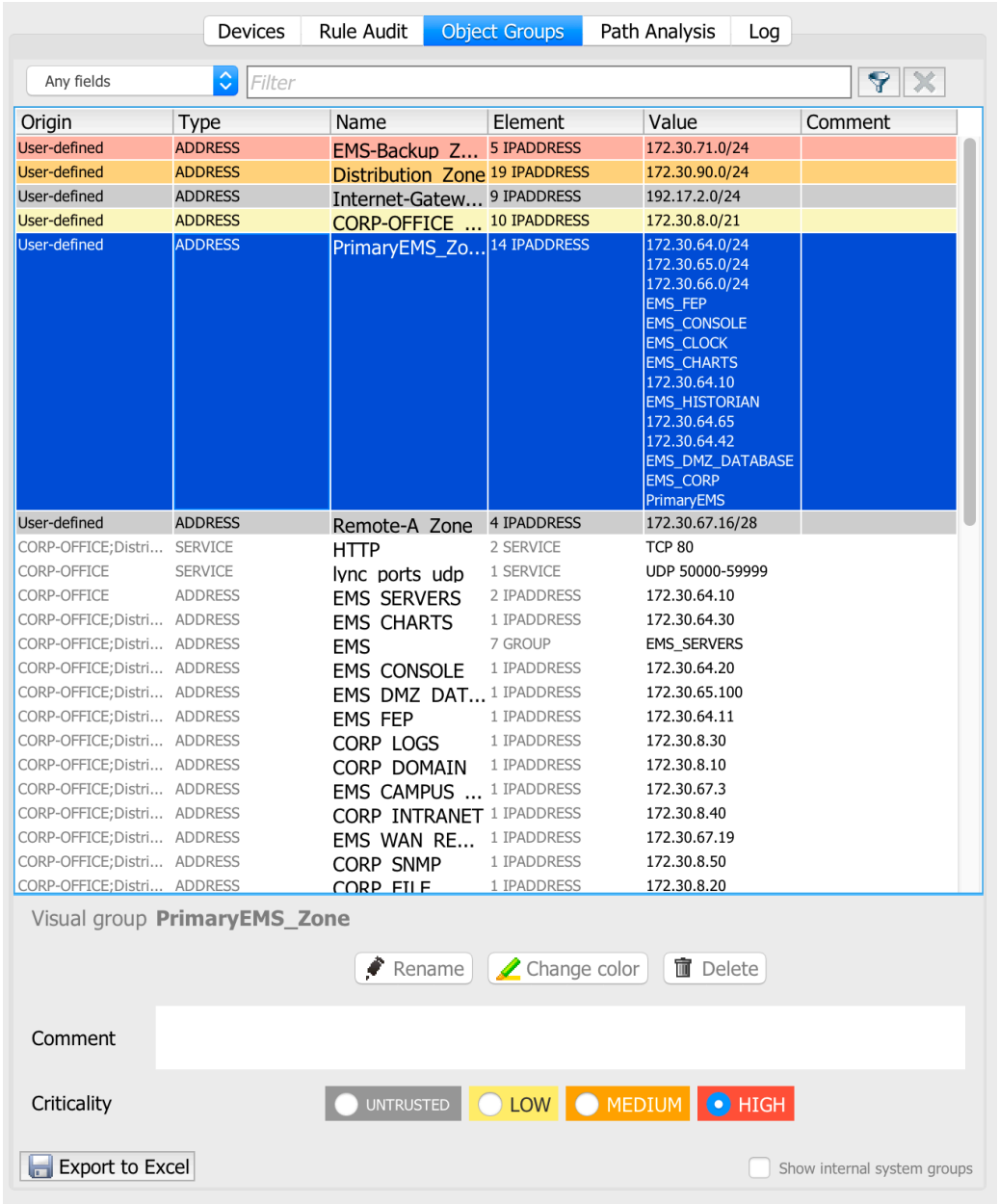
Group Tab

Search

Select to expand and highlight nodes in the map

Add comments and mark criticality

Export to Excel

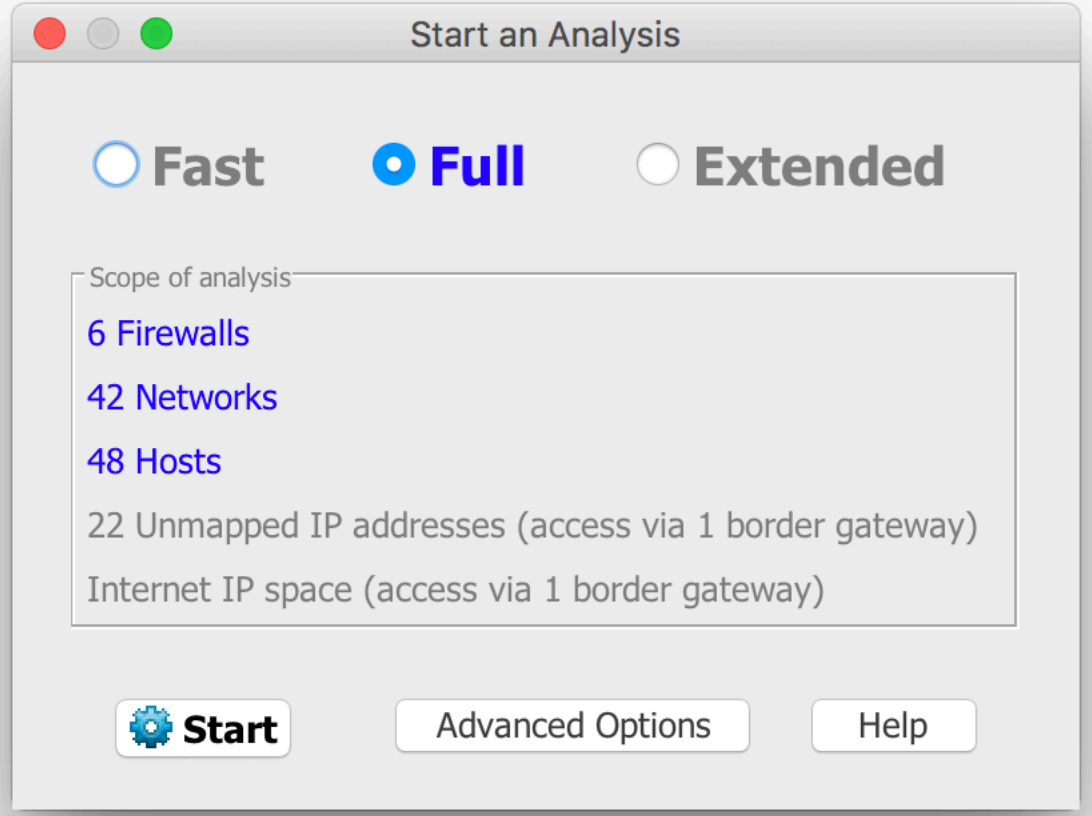


Path Analysis

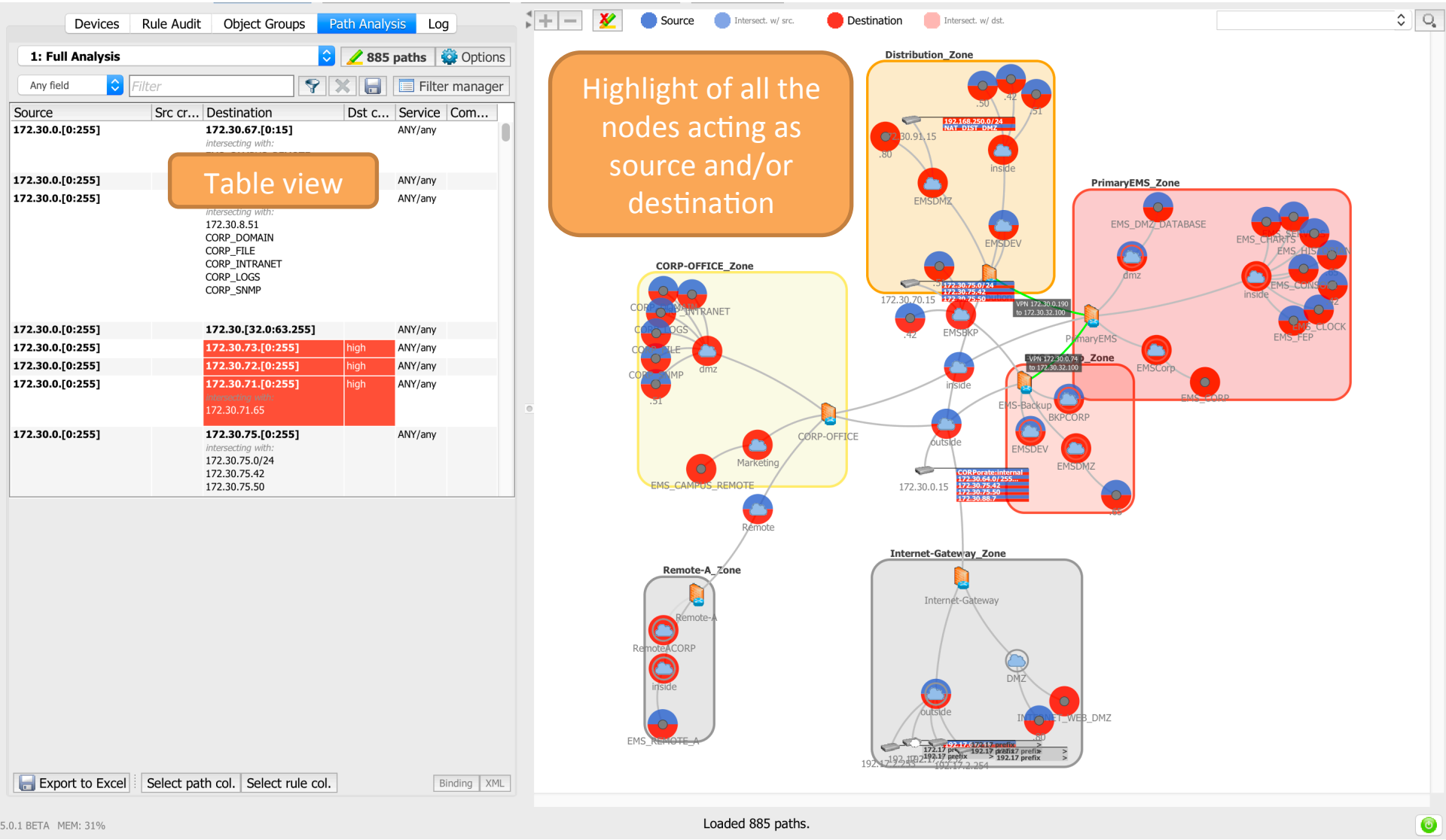
Fast: Analyze only network-to-network paths

Full: Analyze paths among nodes in the map

Extended: Include unmapped nodes and the Internet



Path Analysis Overview

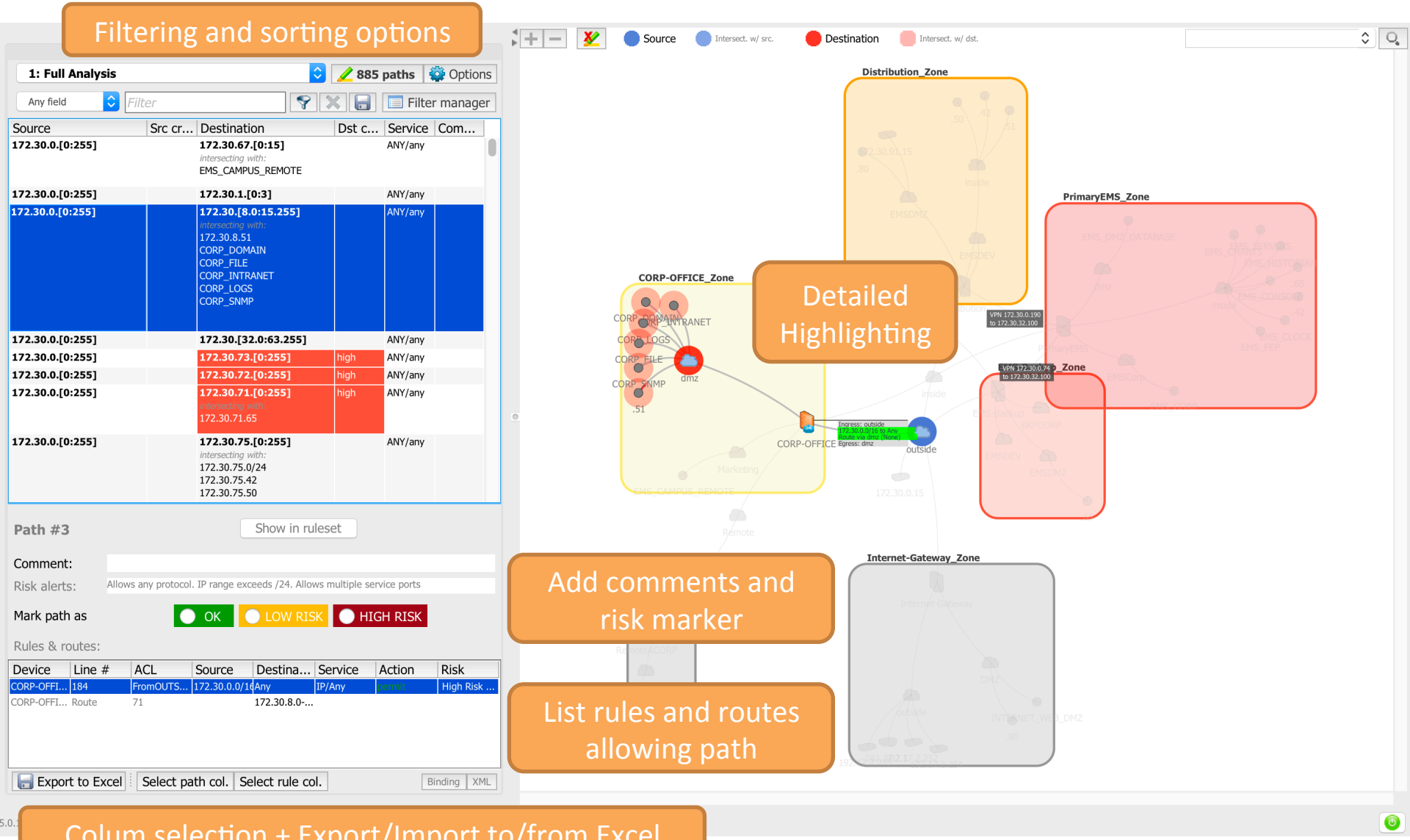


5.0.1 BETA MEM: 31%

Loaded 885 paths.

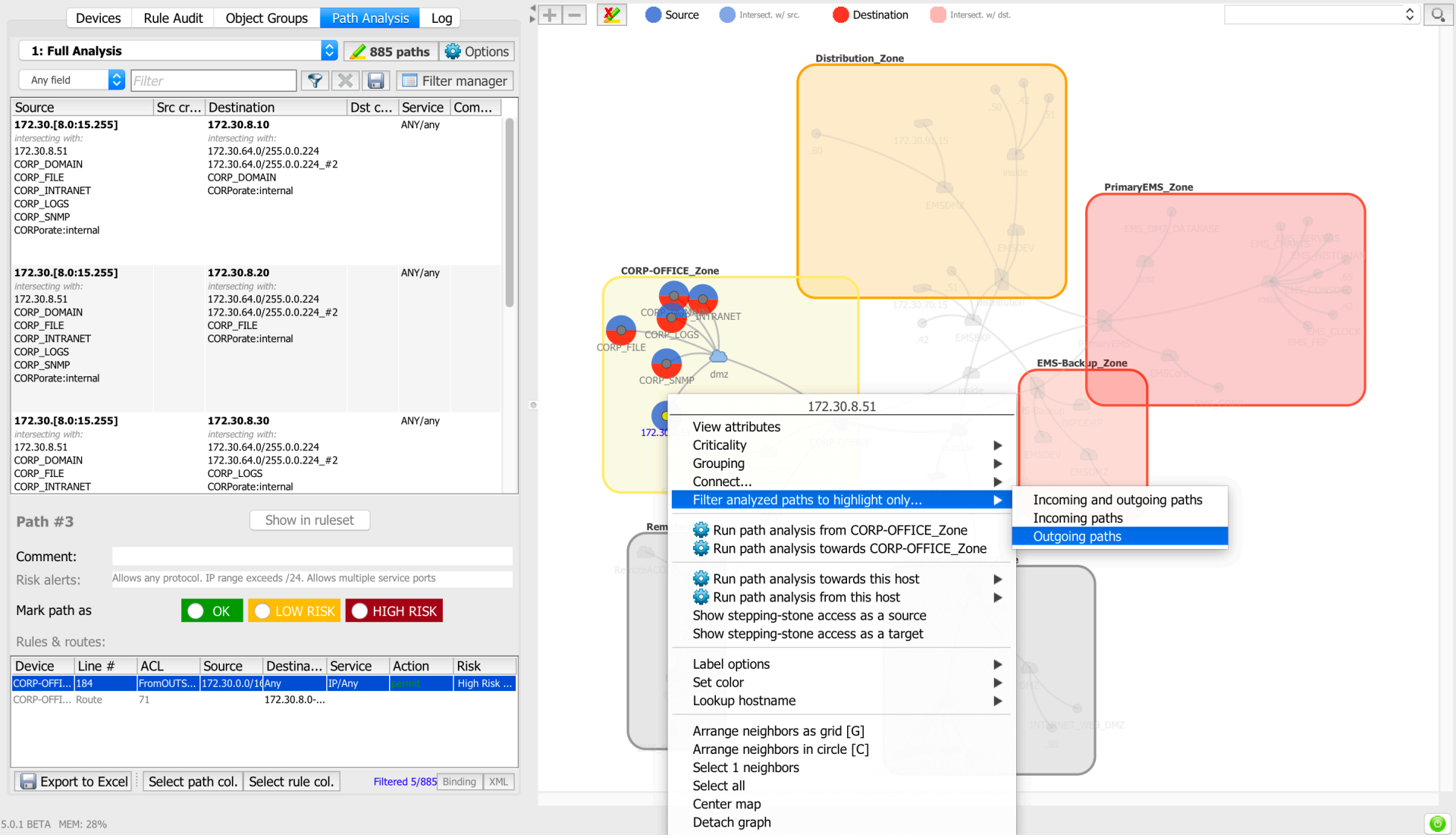
Path Analysis Detail

Filtering and sorting options



Path Filtering

Paths can be filtered using the Filter Toolbar at the top of the path table, or using the map by right-clicking on a node and selecting “Filter analyzed paths to highlight only…”



Path Data Structure

- Path #
- Protocol
- **Source information:**
  - Source Range
  - Source Hosts
  - Source Network
  - Source Firewall
  - Source Port
  - Source Criticality
- **Destination information:**
  - Destination Range
  - Destination Hosts
  - Destination Network
  - Destination Firewall
  - Destination Port
  - Destination Criticality
- Service
- Note
- Rules

Ranges are mathematically computed by the engine

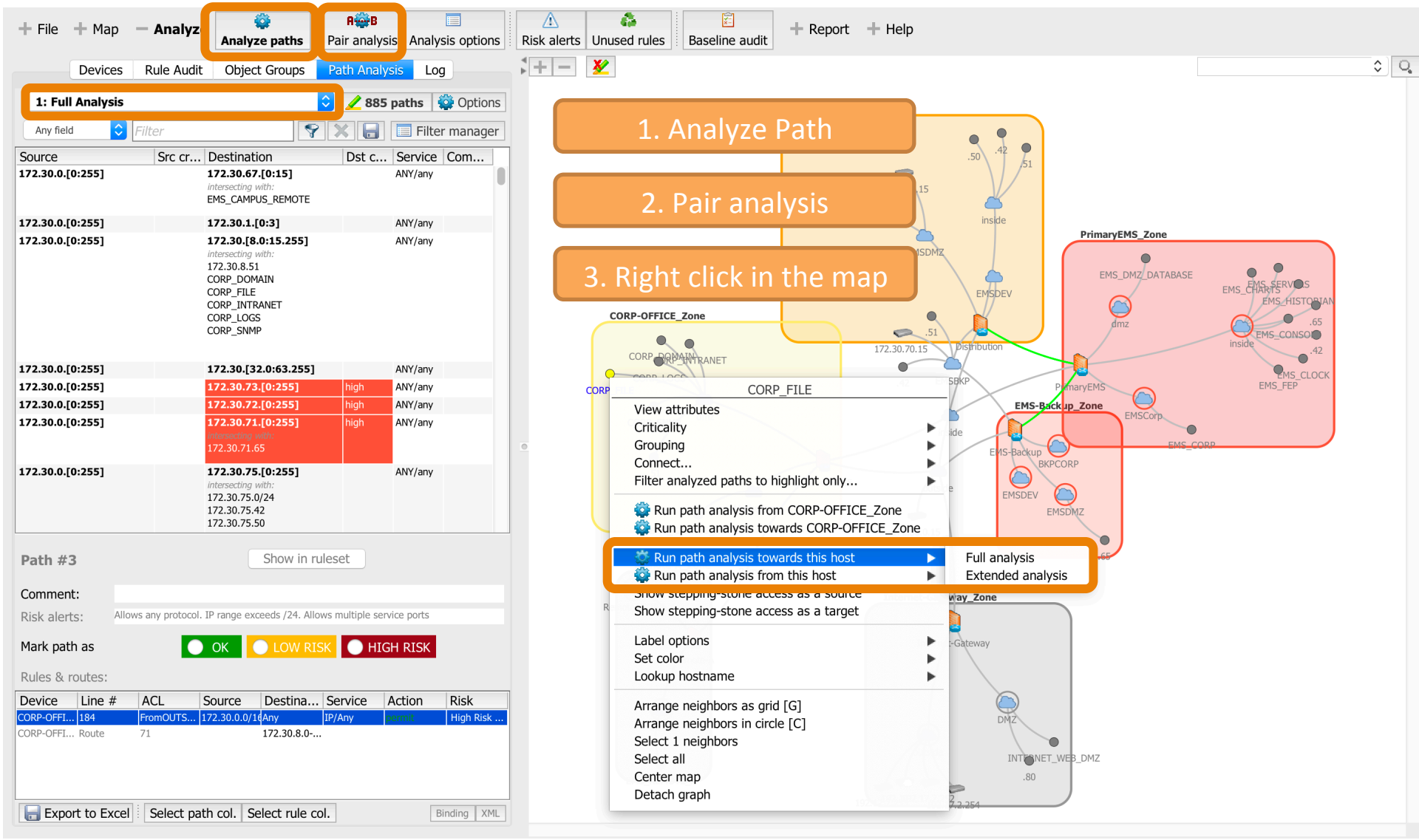
Hosts are IP found in the map from the range

Networks are the parent subnet containing the range

Firewalls are the first or last device crossed

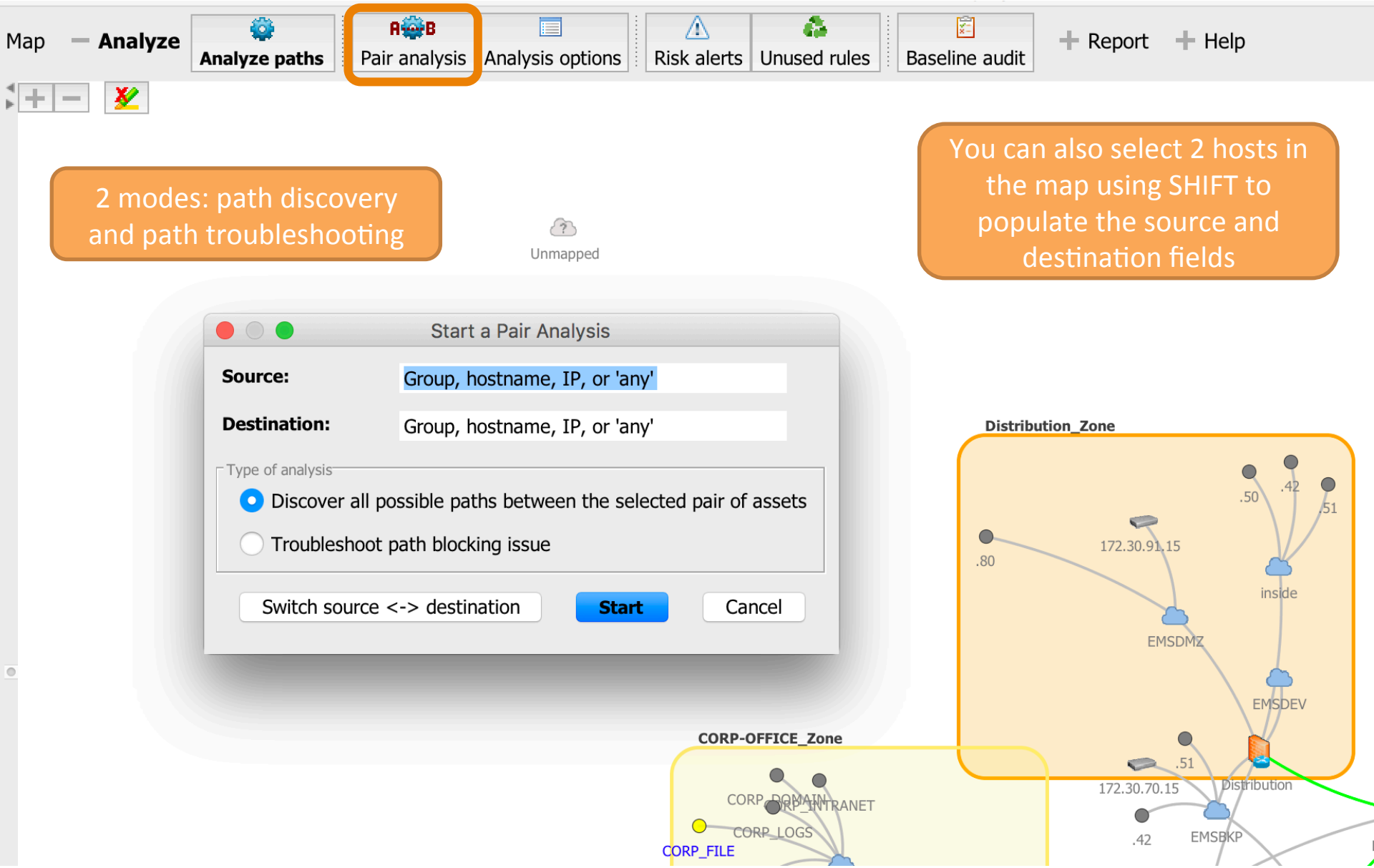
Criticality is set based on the node(s) criticality marker

Ways to Launch Path Analysis

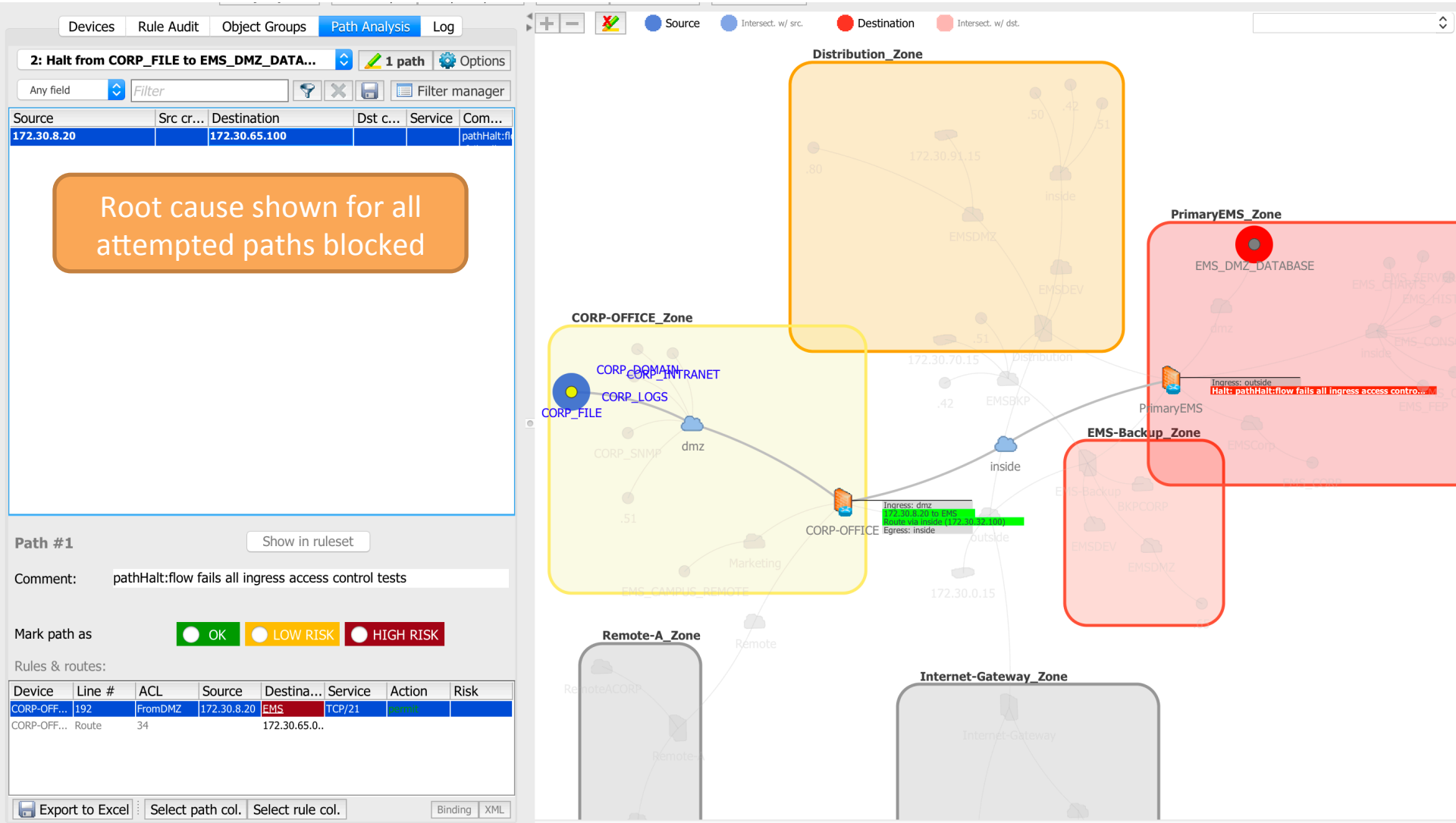


Every path analysis is automatically saved and can be re-loaded through the drop-down list (top left)

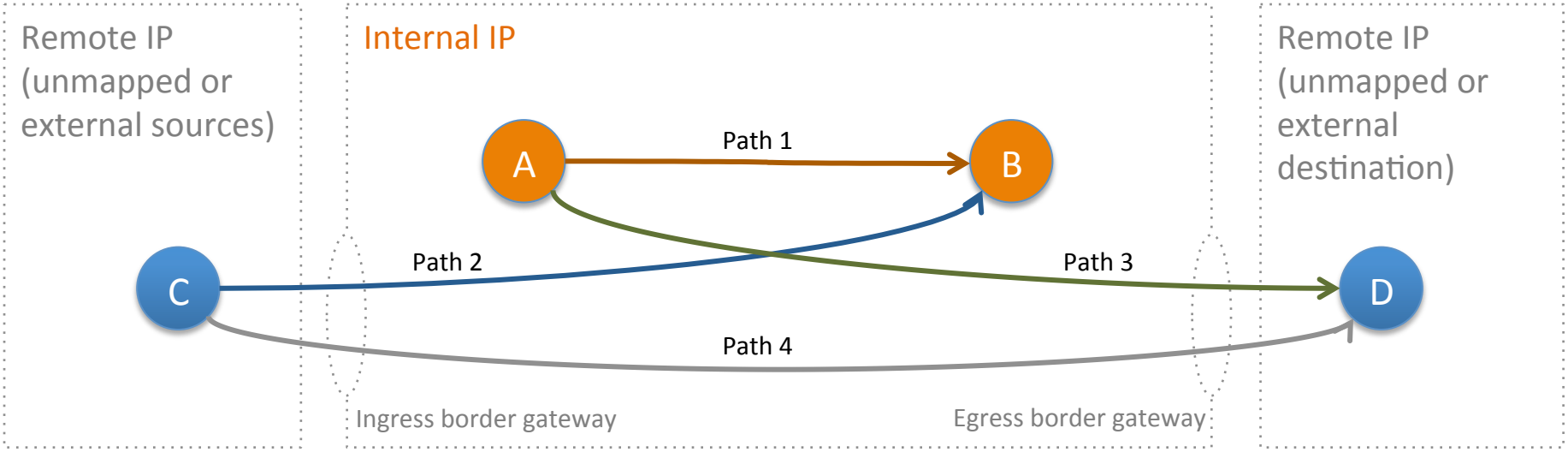
Pair Analysis

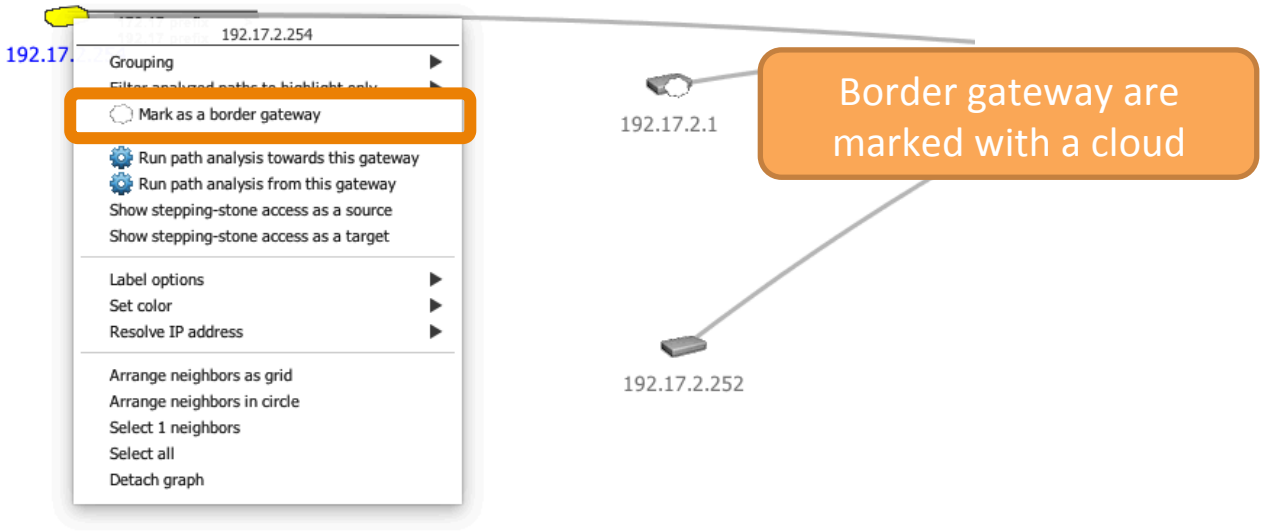


Path Troubleshooting Analysis

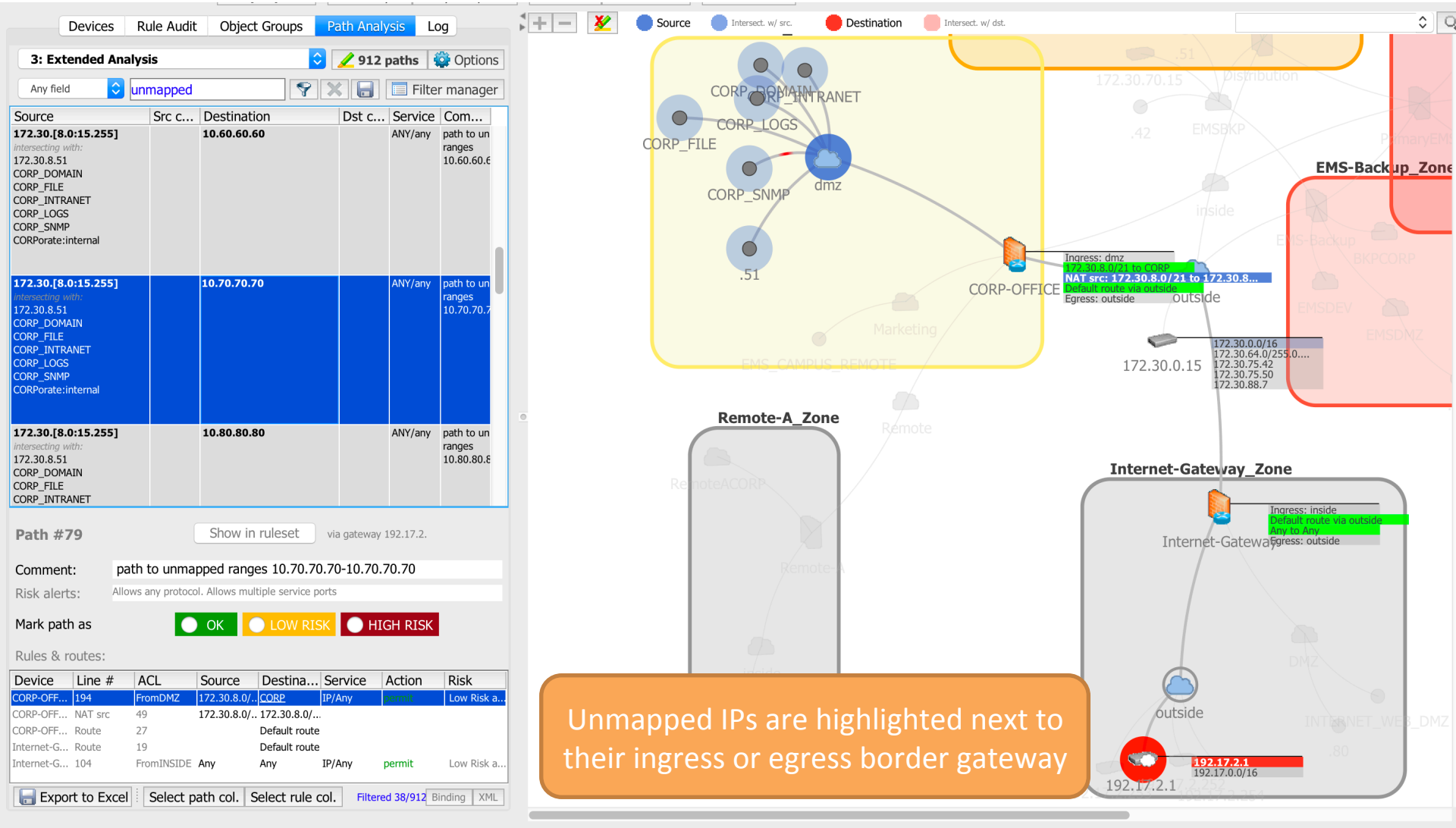


Extended Analysis

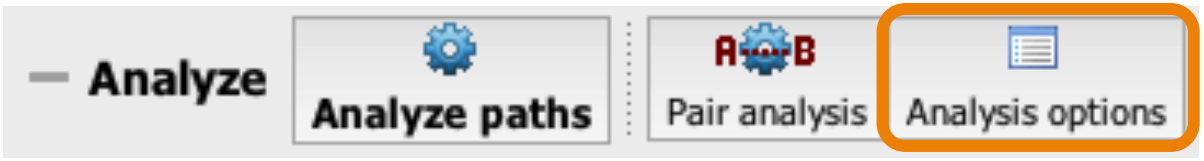




Extended Analysis (cont.)

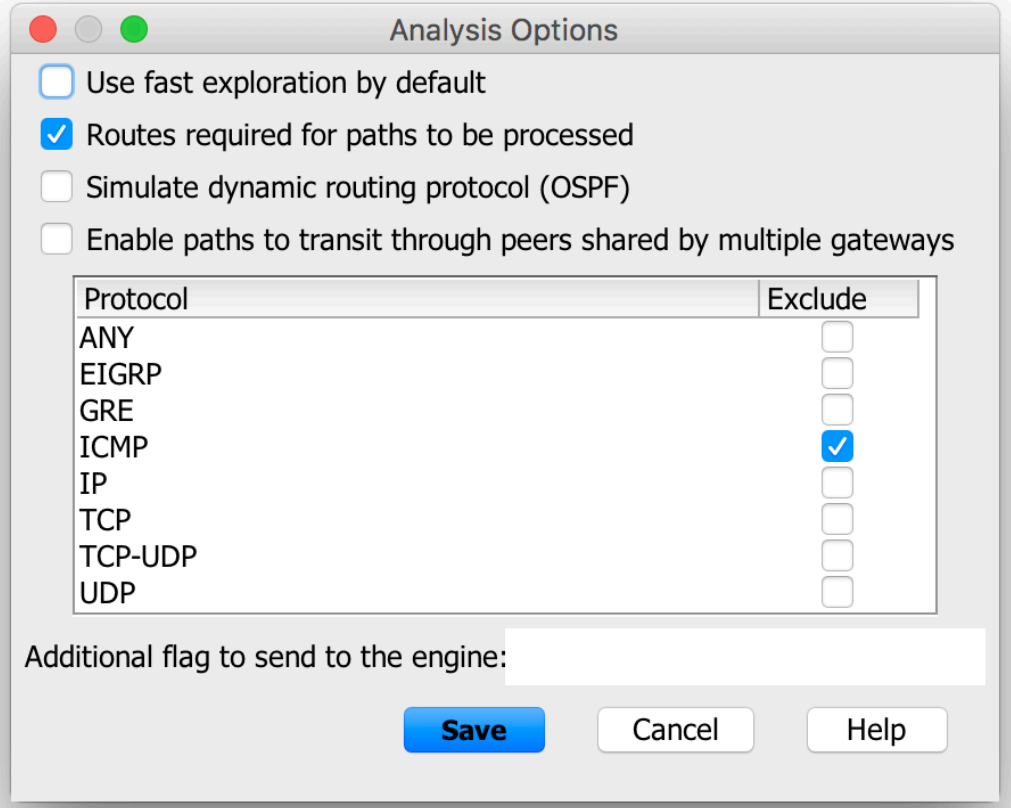


Path Analysis Options



Default analysis options

Default protocol Filtering



Exporting Results

- **Project report**: complete HTML page with all the information parsed by NP-View
- **Comments report**: subset of project report including assets, rules, groups, and paths that have been manually annotated or marked
- **Asset inventory**: Excel spreadsheet of all the nodes parsed
- **Rule table**: Excel spreadsheet of all the rules
- **Export groups**: Excel spreadsheet of all the object groups and user-defined groups
- **Export paths**: Excel spreadsheet of the path analysis currently loaded
- **Export map**: save the topology map into a JPG, Visio, SVG, or ICS-CSET format

If you need a new report or a different export format, please contact support@network-perception.com

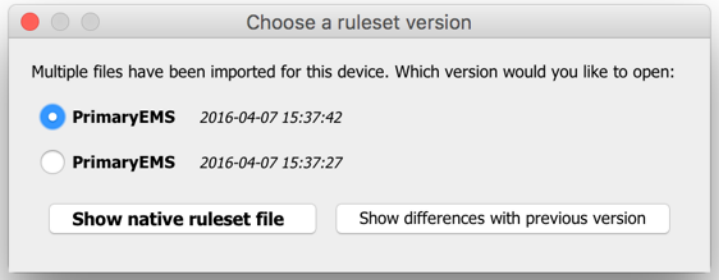
Advanced Features: Additional Data Import

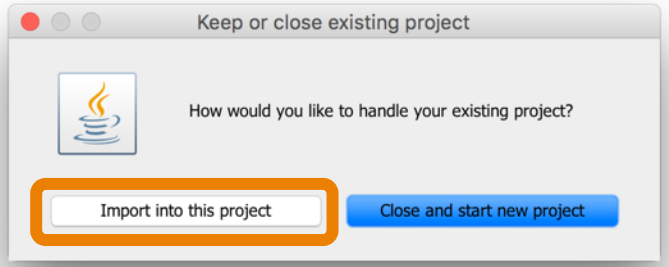
- **Import Nmap**: import a scan report from the Nmap tool in XML format (`-oX` flag). Nodes from the scan reports that are not part of the topology map will be added. OS information and opened ports/services from the scan reports will be added.

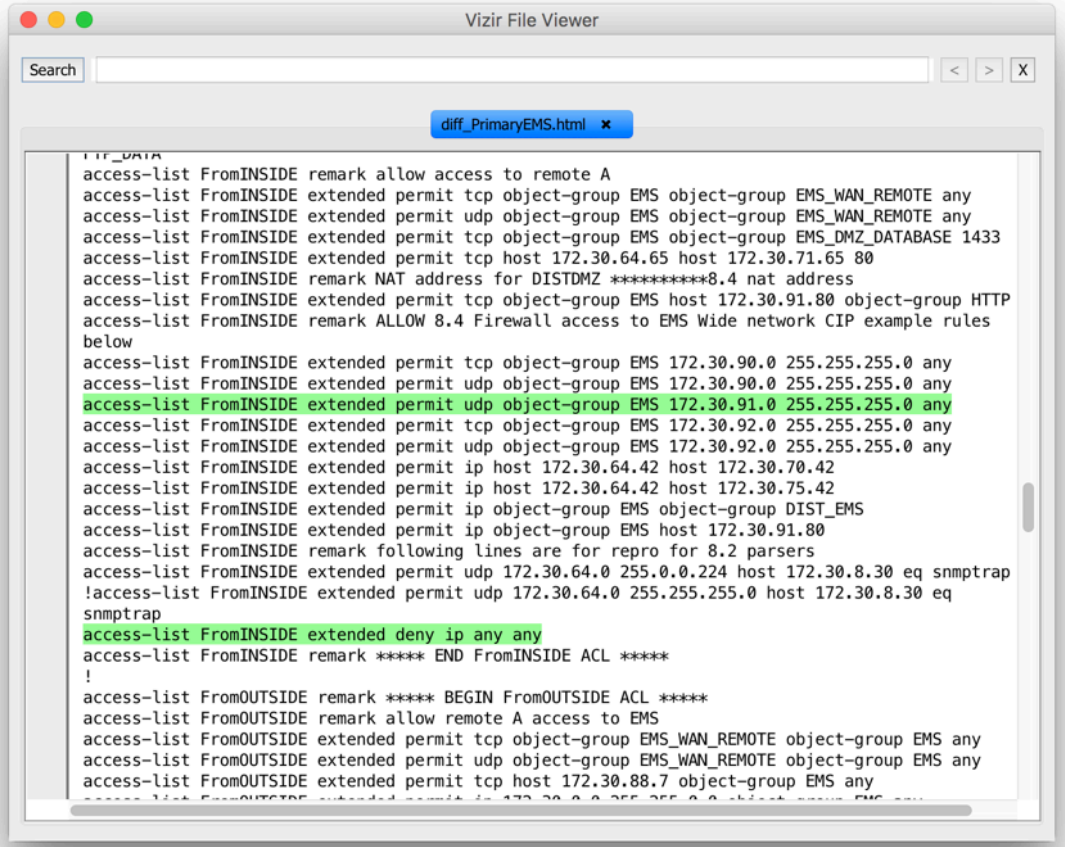
- **Import PCAP**: import a network trace file in PCAP format (Wireshark or tcpdump). Nodes from the trace file that are not part of the topology map will be added. A summary of network flows from the trace file will be saved in the path analysis tab.

- **Import netstat**: import opened ports/services information from the netstat command ran on a Windows (`-abon` flags) or Linux (`-atunp` flags) system.

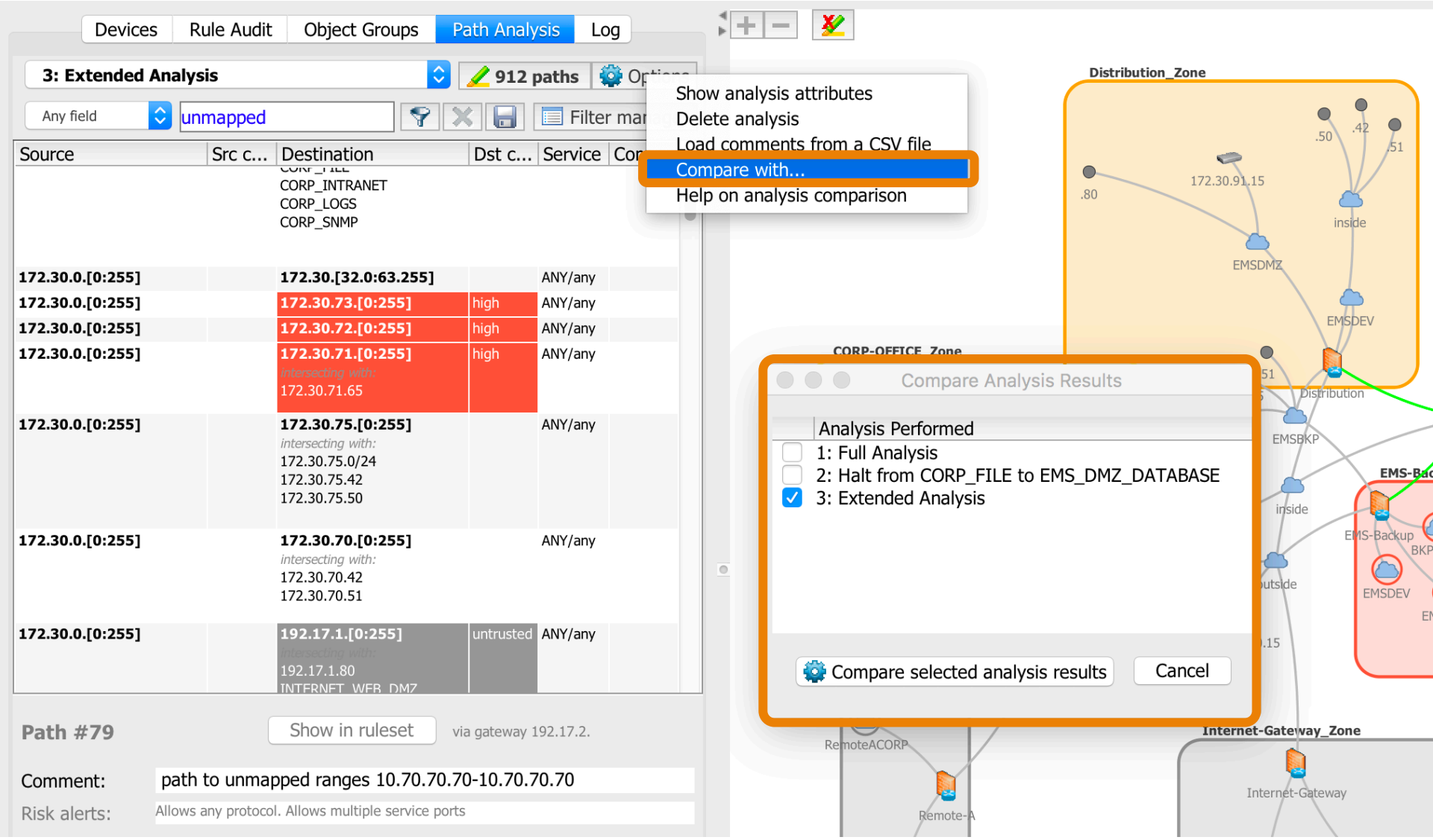
Advanced Features: Change Tracking



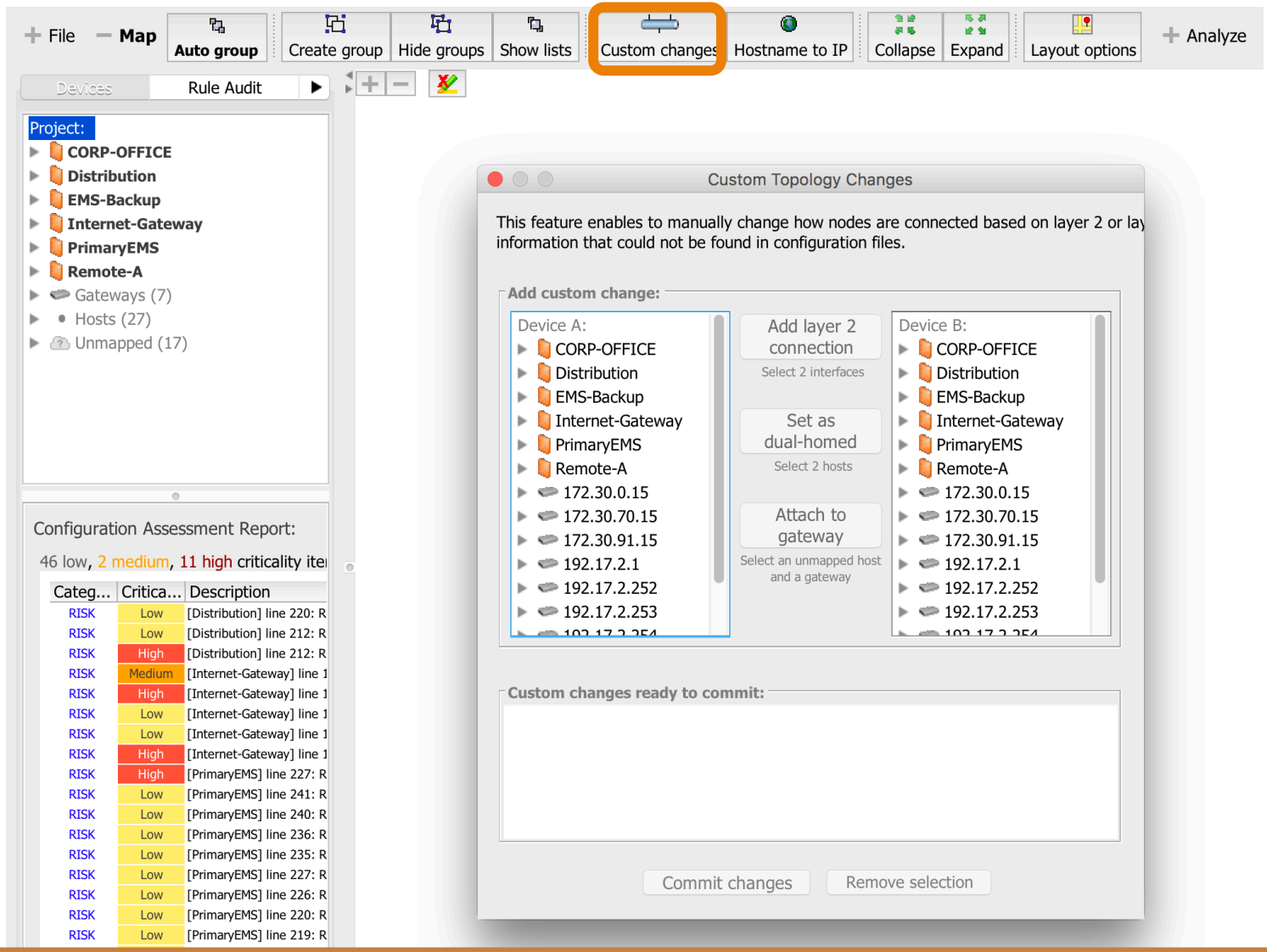




Advanced Feature: Analysis Comparison

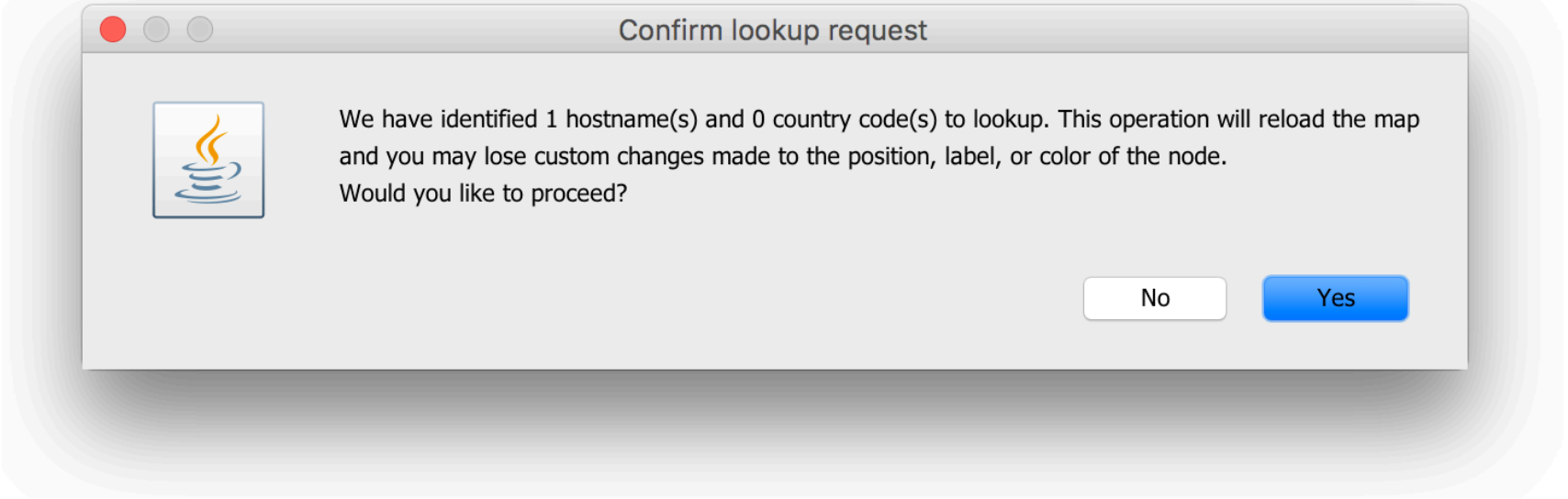


Advanced Feature: Custom Changes

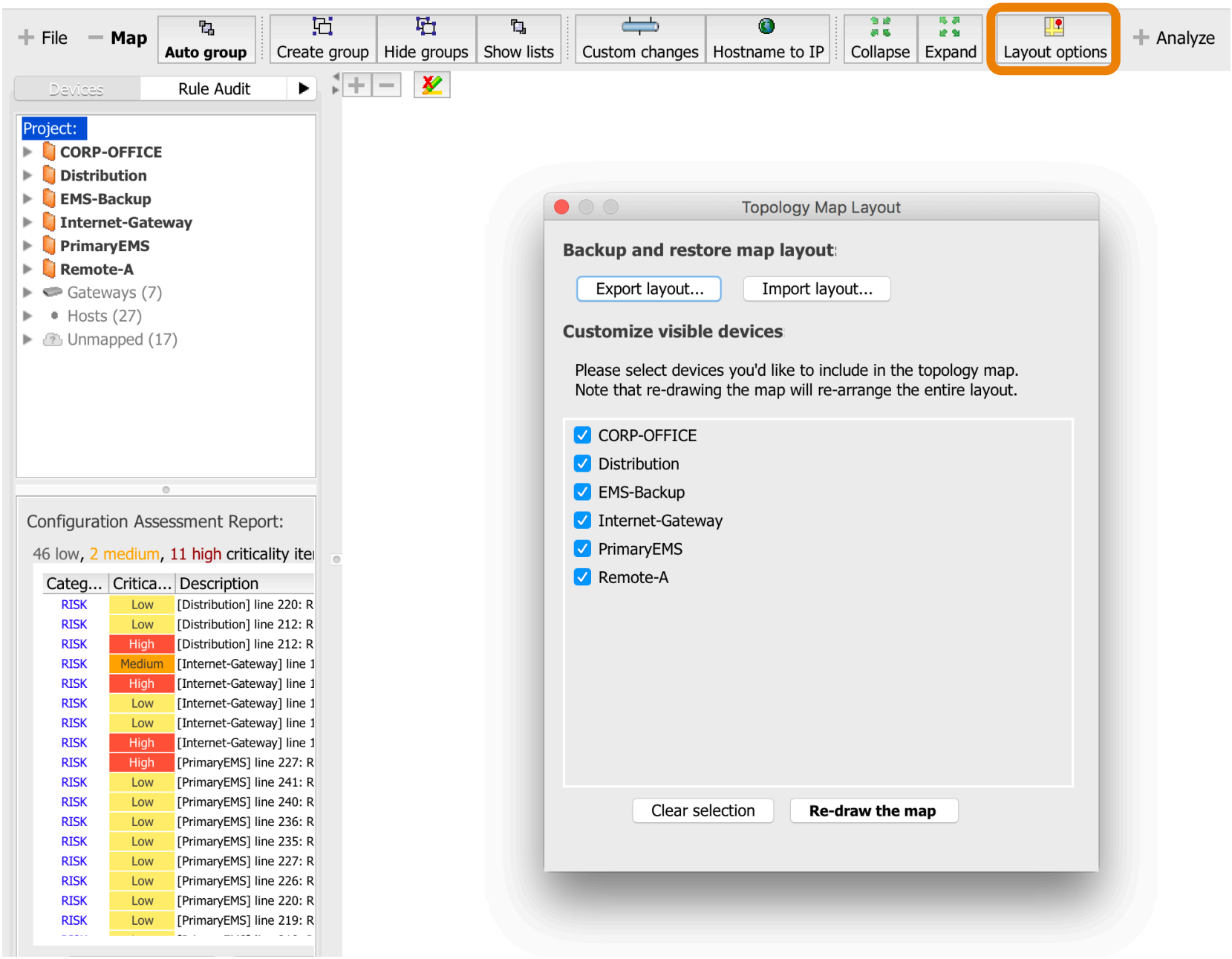


Custom Changes enable you to alter the topology map by: 1) adding layer 2 connections between interfaces, 2) merging nodes into dual-homed assets, 3) moving unmapped nodes to a gateway

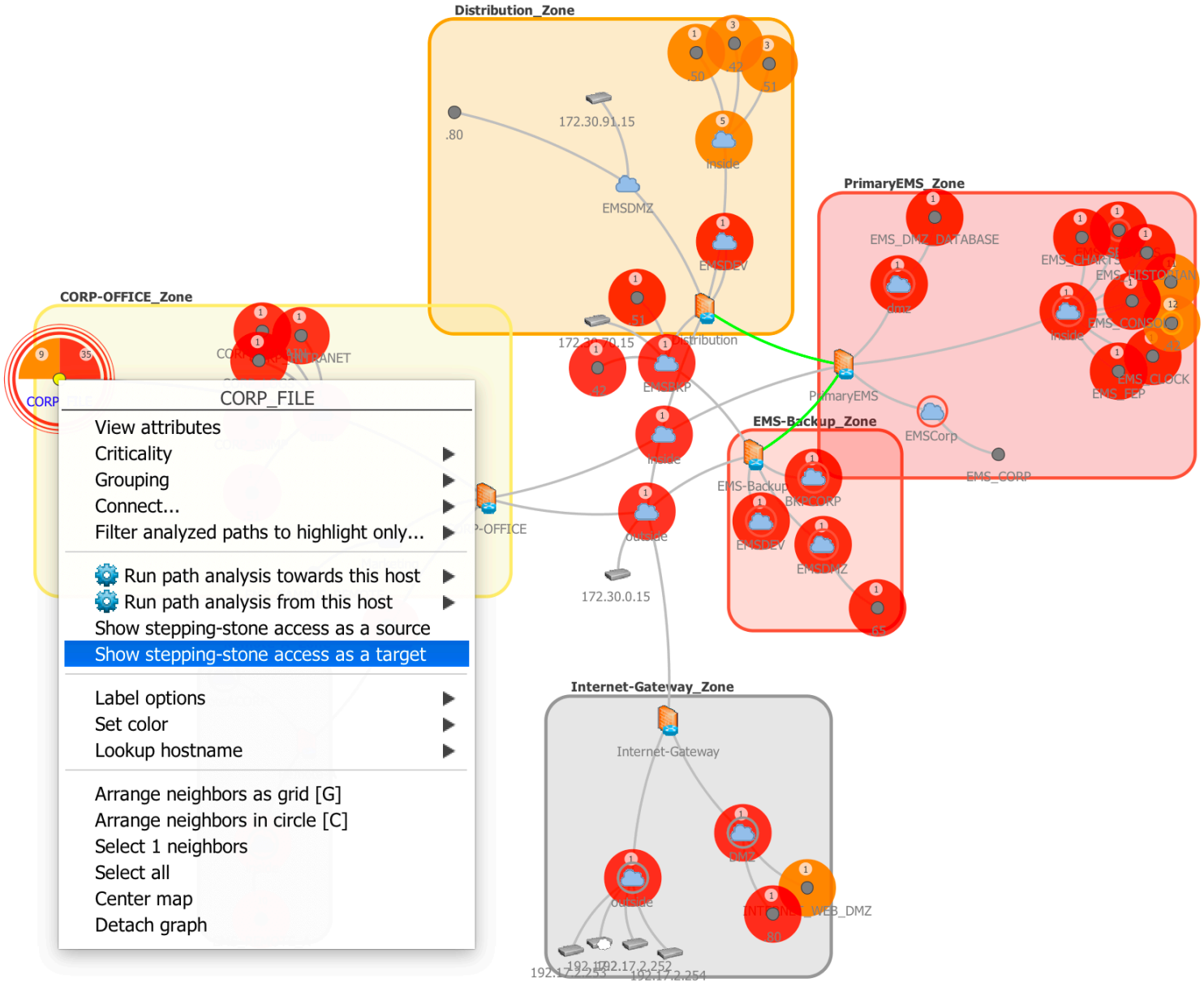
Advanced Feature: Hostname Lookup



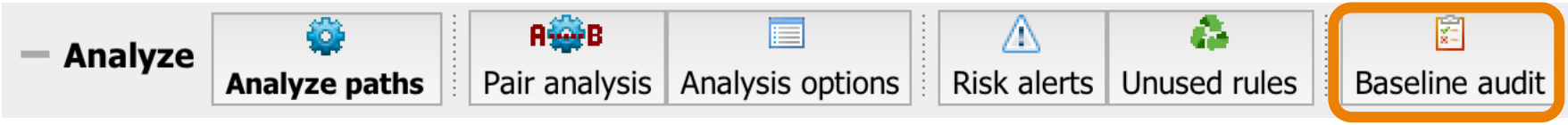
Advanced Feature: Save/Restore Layout



Advanced Features: Stepping-stone Access Map



Advanced Features: Baseline Analysis



Baseline audit

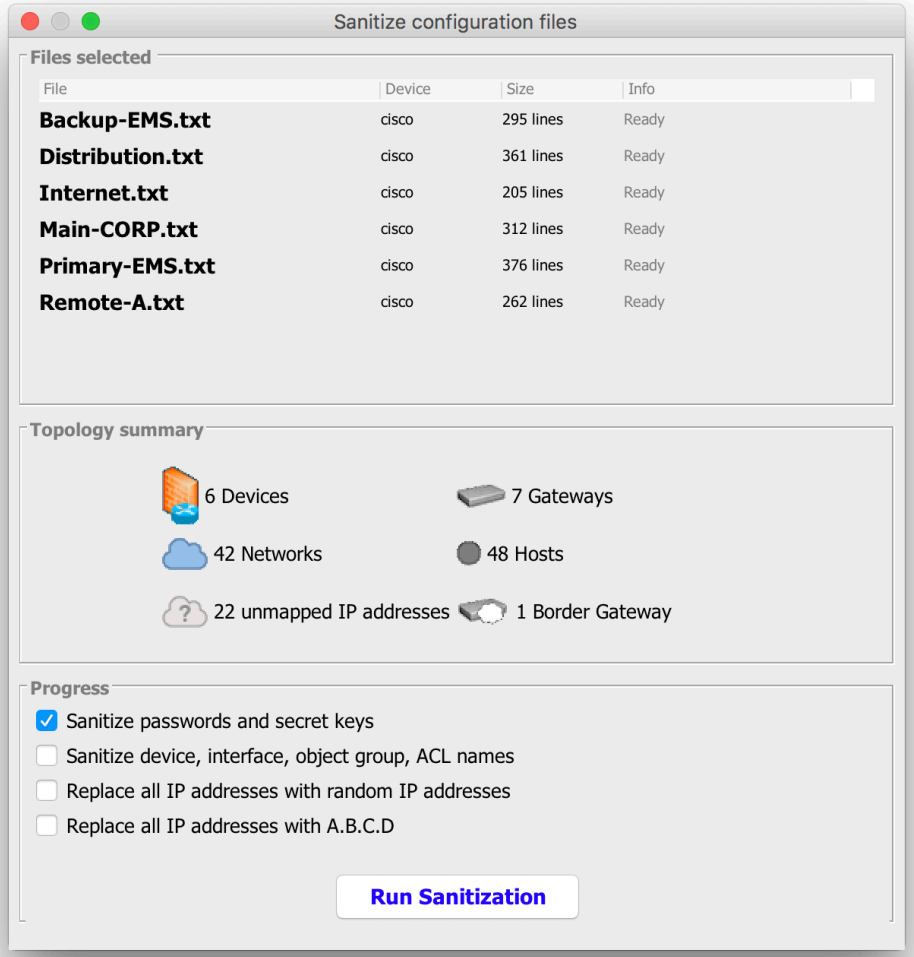
Baseline Analysis Results

The table shows the ports and services accessible through the network for each of the protected cyber assets that you selected. From the assets you selected, a total of 21 port and service access(es) were discovered through the path analysis

IP	Network	Protocol	Port	Direction	Documentation
10.35.1.101	10.35.1.101	tcp	22	in	2015-07-17 08:08:14
10.35.1.102	10.35.1.102	tcp	22	in	2015-07-17 08:08:14
10.35.1.103	10.35.1.103	tcp	22	in	2015-07-17 08:08:14
10.35.1.104	10.35.1.104	tcp	22	in	2015-07-17 08:08:14
10.35.1.201	10.35.1.201	tcp	22	in	2015-07-17 08:08:14
10.35.1.202	10.35.1.202	tcp	22	in	2015-07-17 08:08:14
10.35.1.203	10.35.1.203	tcp	22	in	2015-07-17 08:08:14
10.35.1.250	10.35.1.250	tcp	22	in	2015-07-17 08:08:14
10.36.1.101	10.36.1.101	tcp	22	in	2015-07-17 08:08:14
10.36.1.102	10.36.1.102	tcp	22	in	2015-07-17 08:08:14
10.36.1.103	10.36.1.103	tcp	22	in	2015-07-17 08:08:14
10.36.1.104	10.36.1.104	tcp	22	in	2015-07-17 08:08:14
10.36.1.105	10.36.1.105	tcp	22	in	2015-07-17 08:08:14
10.36.1.201	10.36.1.201	tcp	22	in	2015-07-17 08:08:14
10.36.1.202	10.36.1.202	tcp	22	in	2015-07-17 08:08:14
10.36.1.203	10.36.1.203	tcp	22	in	2015-07-17 08:08:14
10.36.1.250	10.36.1.250	tcp	22	in	2015-07-17 08:08:14
10.37.1.101	10.37.1.101	tcp	22	in	2015-07-17 08:08:14
10.37.1.102	10.37.1.102	tcp	22	in	2015-07-17 08:08:14
10.37.1.201	10.37.1.201	tcp	22	in	2015-07-17 08:08:14
10.37.1.250	10.37.1.250	tcp	22	in	2015-07-17 08:08:14

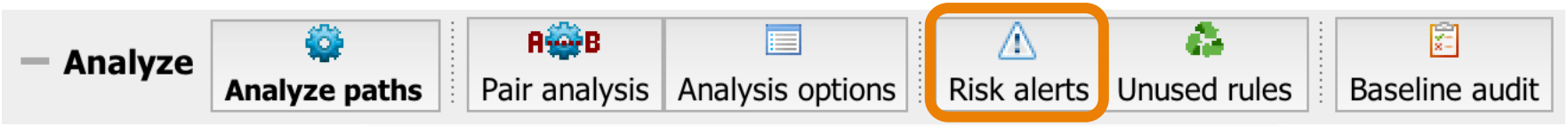
The Baseline Audit feature enables you to generate a summary of ports/services accessible for a set of nodes using the path analysis. This summary can be saved and reloaded at a later time to check if accesses to ports/services have been modified

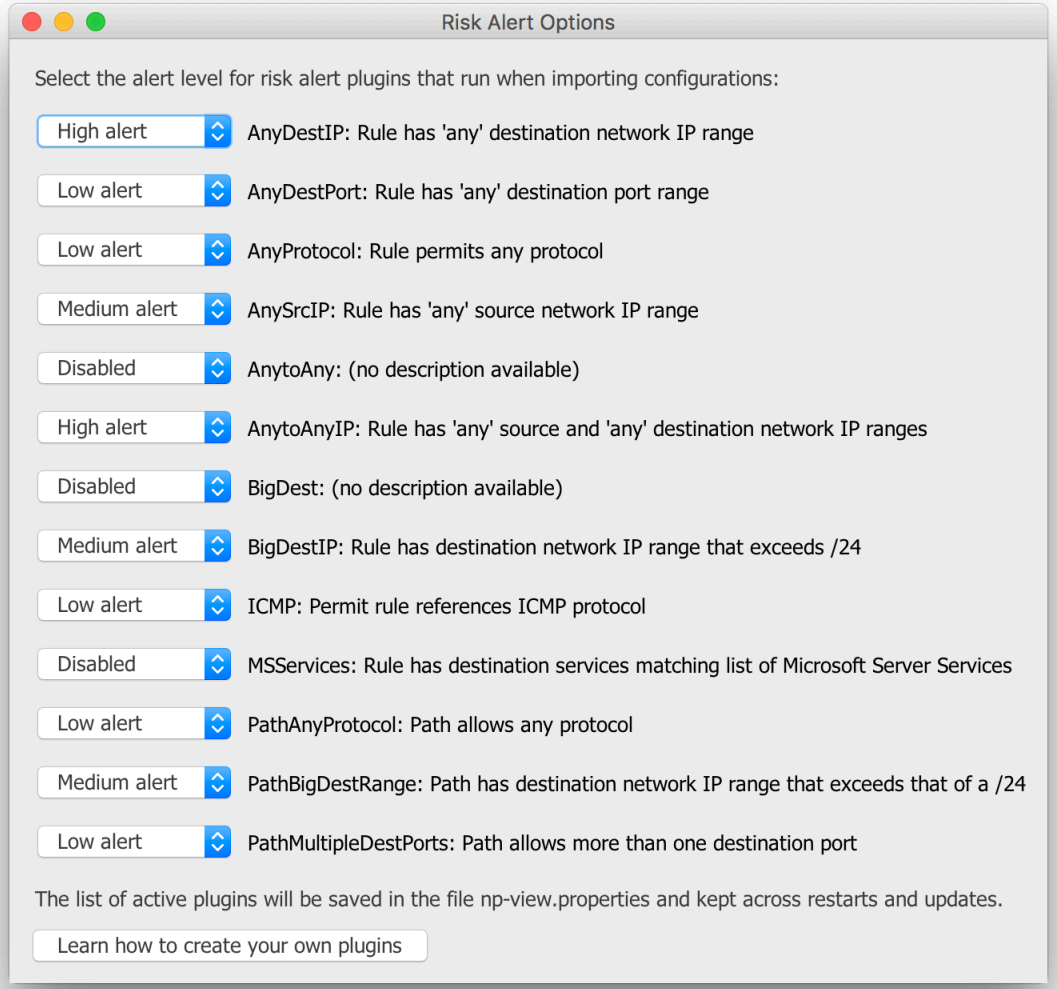
Advanced Features: Ruleset Sanitization



Sanitized files are saved next to the native files with the _sanitized extension

Advanced Features: Risk Alert Criticality





One can change the criticality level of each risk alert plugin and even disabled plugins that are not relevant

Advanced Features: Custom Plugins

- Python plugins stored in the folder `./plugins/rule`
- Enabled by default:
  - pluginAnyDestIP
  - pluginAnyDestPort
  - pluginAnyProtocol
  - pluginAnytoAny
  - pluginBigDest
  - pluginMSServices
- Disabled by default
  - pluginICMP
- Enabling/disabling plugins in the file `np-view.properties`

New risk alert plugins can be added by user through short Python script. Please refer to the documentation available at the bottom of the risk alert window (previous slide)

```
from yapsy.IPlugin import IPlugin
from filters.plugins.utils import AnyIP

# rule is dictionary with keys
#  bindings
#     - egress
#     - ingress
#
#  device
#  dstIP  (list of IPRanges)
#  srcIP  (list of IPRanges)
#
#  encrypted
#  permit
#  ruleName
#  service
#    'protocol'
#       dstRange
#       srcRange

class pluginAnytoAny(IPlugin):
    def applyFilter(self,rule):
        if not rule['permit']:
            return False

        dstFound = False
        srcFound = False
        self.comment = ''
        for ipr in rule['dstIP']:
            if AnyIP( ipr ):
                dstFound = True
                break

        for ipr in rule['srcIP']:
            if AnyIP( ipr ):
                srcFound = True
                break
        return srcFound and dstFound
```

Summary

Input → Process → Output

- Backup-EMS Firewall
- Main Corp. Firewall
- Distribution Firewall
- Primary EMS Firewall
- Internet Firewall
- Remote Access Firewall

- Project Report
- Rule table
- Path tables
- Network Maps

Workflow:

1. Import configuration files
2. Review and customize topology map
3. Mark asset criticality and define visual groups
4. Review rules and add justifications
5. Review object groups and mark criticality
6. Run path analysis and verify network accesses
7. Export findings

Questions?
We can help!

support@network-perception.com