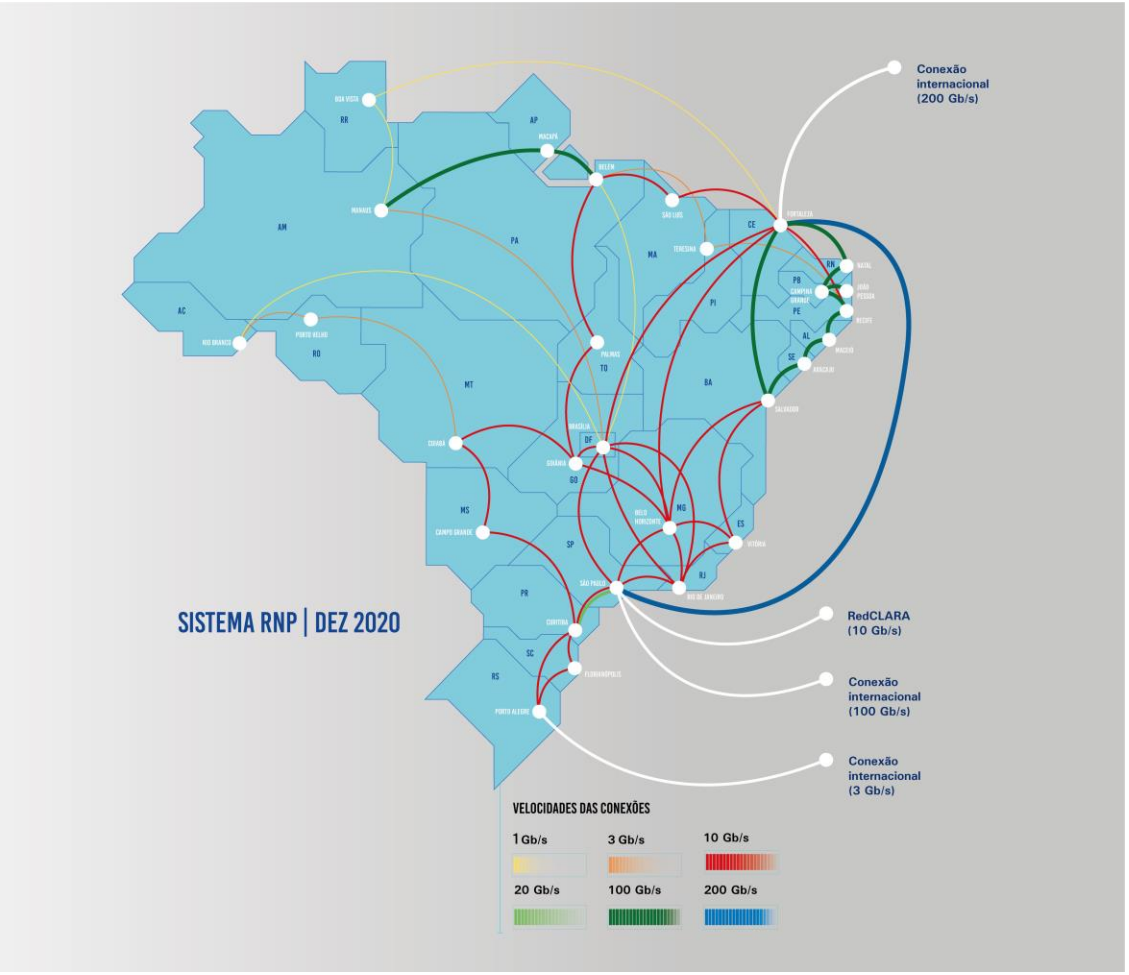
Guilherme Ladvocat

RNP

05/05/2022

Rede Nacional de Ensino e Pesquisa



- Brazilian NREN
- 27 PoPs
- ~ 1500 customers
  - Own infrastructure
  - Carriers
- Backbone
  - All states connected with high capacity circuits
  - Internacional connection to commercial networks and NRENs (Géant, I2, RedClara)

Scenario

- Multiple network device manufacturers;
- High density of devices on PoPs;
- Different support to automation technologies like Netconf, Restconf, yang, openconfig;
- Default configuration with gaps in security.

Scenario

- Multiple network device manufacturers;
- High density of devices on PoPs;
- Different support to automation technologies like Netconf, Restconf, yang, openconfig;
- Default configuration with gaps in security.

DevOps

Impact

- Routers and switches with considerable processing power can be targets of DDoS, botnets, DNS poisoning, etc.
- Ports open and unprotected can:
  - Affect network devices causing abnormal behavior and impacting on user's experience
  - Give an attacker access and control to the device
  - Create a man in the middle topology
  - Mirror traffic to eavesdrop
  - and so on...

Goals

- Automate checkings efficiently
- Support multiple vendors
- Vulnerabilities and inconsistencies follow-up, providing reports.
- Standardize configurations (base-line)
- Improve network security, ensuring best-practice configurations are applied.

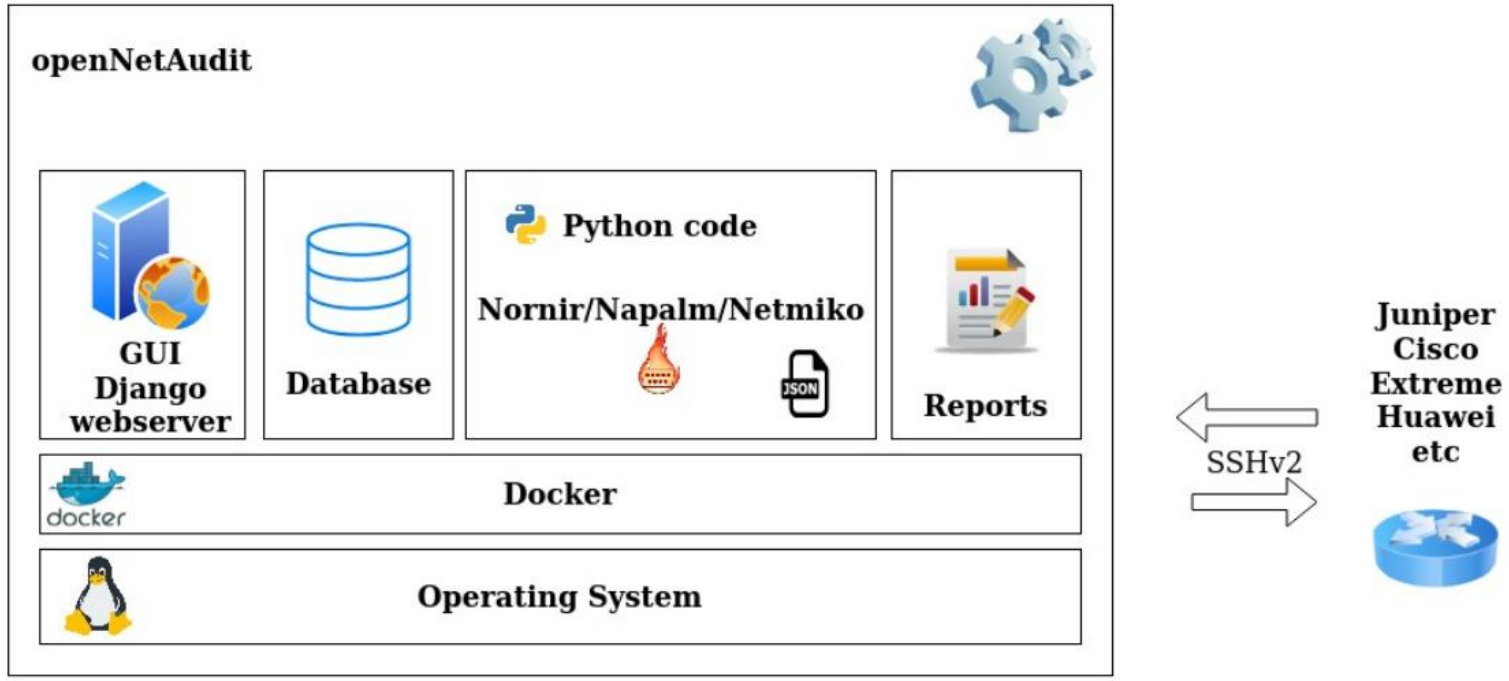
Historic

- 2019: MVP;
- 2020: Roadmap with sponsorship of Programa Frida; lacnic frida
- 2021: Release of v1.0.

- Developed by the RNP Network Operations team
  - Devs:
    - Guilherme Ladvocat
    - Thiago Siqueira
- Supported by Corporate Systems, CAIS and PoPs

Architecture

Django framework
Python code
Nornir/Napalm/Netmiko
SSHv2



openNetAudit - MVP

- Support to Juniper e Extreme;
- Checks based on internal best-practices guide;
- Minimal web interface;
- Simple database;
- Simple reports and results saved in csv files.

openNetAudit - MVP


Página Inicial
Devices PoP
Executar auditoria
Relatórios
Logout
Selecione o PoP para cadastro de device
PoP
AC
Cadastro
Upload csv
Lista de devices dos PoPs
PoP
AC
Listar
Selecione o PoP para commit de configuração
PoP
AC
Commit


Página Inicial
Devices PoP
Executar auditoria
Relatórios
Logout
PoP
AC
Selecione o tipo de device
Device list
CPE Juniper
Username:
Password:
Executar

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	host	vendor	model	os_version	rec_os_version	os_is_equal_to_rec	loopback_fw_ipv4	fw_ipv4_last_term_discard	loopback_fw_ipv6	fw_ipv6_last_term_discard	rpf_check_enabled	telnet_enabled	ssh2_enabled	web_admin_enabled	root_login_enabled	route_passive
2	host	Juniper	J2320	12.1X44-D45.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
3	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
4	host	Juniper	SRX240H2	12.3X48-D30.7	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False
5	host	Juniper	SRX240H2	12.3X48-D85.1	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False
6	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
7	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False
8	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False
9	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False
10	host	Juniper	SRX240H2	12.3X48-D30.7	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False
11	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False
12	host	Juniper	J2350	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
13	host	Juniper	SRX240H2	12.1X46-D40.2	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False
14	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
15	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
16	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
17	host	Juniper	SRX240H2	12.3X48-D85.1	12.3X48-D101	False	True	True	True	True	False	False	True	False	False	False
18	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False
19	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
20	host	Juniper	J2350	10.2R4.10	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
21	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
22	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False
23	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False
24	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
25	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
26	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
27	host	Juniper	J2350	10.2R4.8	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
28	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False
29	host	Juniper	SRX340	15.1X49-D150.2	18.4R3-S2	False	True	True	True	True	False	False	True	False	False	False
30	host	Juniper	SRX220H	12.1X46-D67	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False
31	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
32	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False
33	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False
34	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False
35	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	False	True	False	False	False	True	False	False	False
36	host	Juniper	J2350	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
37	host	Juniper	SRX220H	12.1X46-D45.4	12.1X46-D86	False	True	True	True	True	False	False	True	False	False	False
38	host	Juniper	SRX220H	12.1X46-D86	12.1X46-D86	True	True	True	True	True	False	False	True	False	False	False
39	host	Juniper	J2320	12.1X46-D40.2	12.1X46-D66	False	True	True	True	True	False	False	True	False	False	False
40																
41	Legenda:															
42	os_is_equal_to_rec = True															
43	loopback_fw_ipv4 = True															
44	fw_ipv4_last_term_discard = True															
45	loopback_fw_ipv6 = True															
46	loopback_fw_ipv6 = True															
47	fw_ipv6_last_term_discard = True															
48	rpf_check_enabled = True															
49	telnet_enabled = False															
50	web_admin_enabled = False															

Roadmap – main features

- Refactor of the system;
- Hierarchical organization (Device -> Site -> Group);
- Audit core improvements
    - Custom checks;
    - Tests severity;
    - Multiple rules in one test.
- New vendors supported: Cisco, Huawei, Mikrotik;
- Results saved in JSON;
- Reports in web views;
- Vulnerabilities tracking.

Tests and rules

```
{
    "test_name": "telnet",
    "description": "Check if telnet service is enabled.",
    "rules": ["telnet_check"],
    "logic": "or",
    "severity": 9.8,
    "message_ok": "Telnet is disabled.",
    "message_nok": "Telnet is enabled. Prefer using SSHv2.",
    "solution": "delete system services telnet"
}
```

```
{
    "rule_name": "telnet_check",
    "description": "Check if telnet service is enabled.",
    "strings_match": ["set system services telnet"],
    "match_same_line": 1,
    "logic": "and",
    "string_present": 0,
    "exact_match": 1
}
```

openNetAudit

Home Devices Audit Reports Admin Profile Logout

[redacted]

Site Info

Number of Hosts: 26

Hosts Without Issues: 1

Hosts With Issues: 25

Number of Issues: 136

Top 5

Hosts with more issues

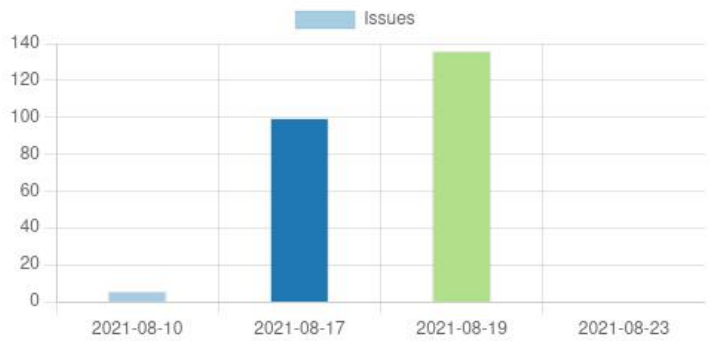
1. [redacted] 12
2. [redacted] 11
3. [redacted] 11
4. [redacted] 11
5. [redacted] 11

Docs

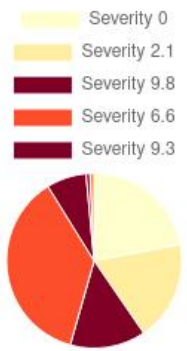
Documentation for OpenNetAudit, along with tutorials and guides, are available online.

Documentation

Issues History



Issues



Device List

List of devices from site: LAB

Select All	Id	Name	Description	Type	IP : ssh_port	
☐	1	Huawei-Secure	Secure	huawei	10.1.0.80:22	Edit Delete
☐	2	Huawei-Insecure	Insecure	huawei	10.1.0.85:22	Edit Delete
☐	3	Juniper-vsrx	VSRX	juniper	10.1.0.107:22	Edit Delete
☐	4	Cisco	V1000	cisco_ios	10.1.0.250:22	Edit Delete
☐	5	Mikrotik-Secure	Secure	mikrotik	10.1.0.150:2222	Edit Delete
☐	6	Mikrotik-Insecure	Insecure	mikrotik	10.1.0.155:22	Edit Delete
☐	7	Extreme-Secure	Secure	extreme	10.1.0.100:22	Edit Delete
☐	8	Extreme-Insecure	Insecure	extreme	10.1.0.90:22	Edit Delete

Delete all Selected

Device Report

Info

Device: Cisco

IP: 10.1.0.250

Manufacturer: Cisco_ios

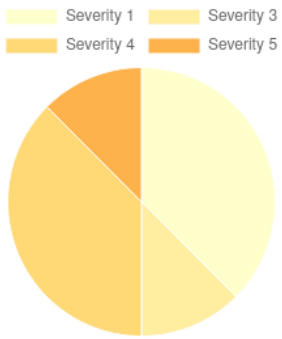
Last Audit: May 4, 2021

Status: Successful

Issues: 8

Recommended OS: True

Issues



Last Audit

Test	Description	Severity	Value
logging	OK	undefined	Logging service is enabled.
service.pad	OK	undefined	Service pad is disabled.
source_route	OK	undefined	IP Source Route service is disabled.
snmp_default_communities	NOK	5	SNMP default communities are present. Please delete them.
password_encryption	OK	undefined	Service password encryption disabled.
gratuitous_arp	NOK	3	Gratuitous ARP service is enabled
cdp	OK	undefined	CDP is disabled
http	OK	undefined	Web management is disabled
enable_secret	OK	undefined	Enable secret is applied. OK!
finger	NOK	4	IP Finger is enabled. Please disable it.
dhcp	NOK	1	DHCP service is enabled.
urpf	NOK	4	uRPF is disabled. Apply uRPF to the LAN interface.
telnet	OK	undefined	Telnet is disabled.
bootp	NOK	1	Bootp service is enabled.
ssh_parameters	NOK	4	SSH parameters like timeout and retries are not configured.

Audit Result

Number of hosts	Hosts with issues	Hosts without issues	Number of issues
1	1	0	8

Site	Host	Host Name	Ip	Model	OS	Os Recommended	SN	Status	Timestamp	Manufacturer
LAB	Cisco	Cisco-Lab	10.1.0.250	CSR1000V	16.6.5	True	91YV0PLMQW6	Successful	2021-05-04 13:58:05.281095	Cisco

Host	Test	Value	Severity	Description	Solution
Cisco	logging	OK	undefined	Logging service is enabled.	
Cisco	service.pad	OK	undefined	Service pad is disabled.	
Cisco	source_route	OK	undefined	IP Source Route service is disabled.	
Cisco	snmp_default_communities	NOK	5	SNMP default communities are present. Please delete them.	no snmp-server community private no snmp-server community public
Cisco	password_encryption	OK	undefined	Service password encryption disabled.	
Cisco	gratuitous_arp	NOK	3	Gratuitous ARP service is enabled	no ip gratuitous-arps
Cisco	cdp	OK	undefined	CDP is disabled	
Cisco	http	OK	undefined	Web management is disabled	
Cisco	enable_secret	OK	undefined	Enable secret is applied. OK!	
Cisco	finger	NOK	4	IP Finger is enabled. Please disable it.	no ip finger

Next steps

- Have new adoptants
- Receive feedback
- Improve the system and the best practices base

https://git.rnp.br/guilherme.ladvocat/opennetaudit

https://netaudit.rnp.br

guilherme.ladvocat@rnp.br

Gracias!