STABLENET®

AUTOMATED NETWORK & SERVICE MANAGEMENT

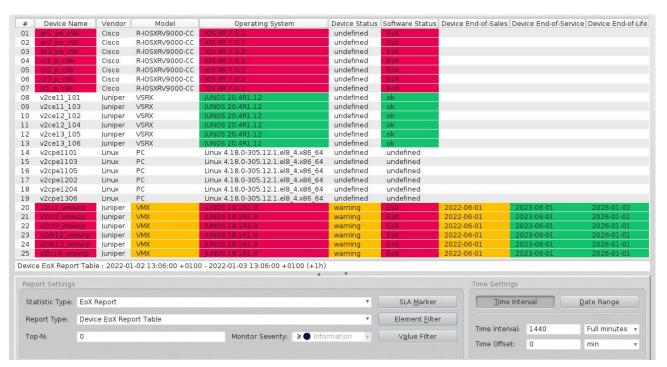## ⚙️ Network Configuration & Change

Making Security Simple: An automated and scalable approach to Vulnerability and Lifecycle Management that works for you

Let StableNet® help ensure that your ever-changing network infrastructure stays secure by managing vulnerability and product lifecycle updates (e.g. EOL/EOS)

Background & Motivation

Maintaining a secure, healthy network is the goal of every network operator. It is, however, a moving target and one that requires constant supervision. With the incessant introduction of new network technologies and IoT, the proliferation and scope of cyber-attacks and security breaches continues to grow exponentially. This diversification and increased complexity in network infrastructure requires a powerful, automated tool that can facilitate management across multiple vendors and technologies so that you can proactively identify known vulnerabilities before they hurt you.

Network hardware and software vendors periodically release updated lists of devices and software versions that are affected by End-of-Sales, End-of-Support, and End-of-Life (together referred to as EoX) announcements along with new vulnerabilities. While it is possible to manually run checks of each device and software installation in your infrastructure (from each of a multitude of vendors), this can quickly become a huge waste of resources for telecommunications and large enterprise networks. Firms not only have a personal vested interested in ensuring that their networks are safe and secure, but also have to consider numerous compliancy agencies and their requirements as well. The need for an automated, scalable solution to EoX and Vulnerability Management has never been greater.

#	Device Name	Vendor	Model	Operating System	Device Status	Software Status	Device End-of-Sales	Device End-of-Service	Device End-of-Life
01	ar1_pe_c9k	Cisco	R-IOSXRV9000-CC	iOS XR 7.0.2	undefined	EoX			
02	ar2_pe_c9k	Cisco	R-IOSXRV9000-CC	iOS XR 7.0.2	undefined	EoX			
03	ar3_pe_c9k	Cisco	R-IOSXRV9000-CC	iOS XR 7.0.2	undefined	EoX			
04	cr1_p_c9k	Cisco	R-IOSXRV9000-CC	iOS XR 7.0.2	undefined	EoX			
05	cr2_p_c9k	Cisco	R-IOSXRV9000-CC	iOS XR 7.0.2	undefined	EoX			
06	cr3_p_c9k	Cisco	R-IOSXRV9000-CC	iOS XR 7.0.2	undefined	EoX			
07	tr1_p_c9k	Cisco	R-IOSXRV9000-CC	iOS XR 7.0.2	undefined	EoX			
08	v2ce11_101	Juniper	VSRX	JUNOS 20.4R1.12	undefined	ok			
09	v2ce11_103	Juniper	VSRX	JUNOS 20.4R1.12	undefined	ok			
10	v2ce12_102	Juniper	VSRX	JUNOS 20.4R1.12	undefined	ok			
11	v2ce12_104	Juniper	VSRX	JUNOS 20.4R1.12	undefined	ok			
12	v2ce13_105	Juniper	VSRX	JUNOS 20.4R1.12	undefined	ok			
13	v2ce13_106	Juniper	VSRX	JUNOS 20.4R1.12	undefined	ok			
14	v2cpe1101	Linux	PC	Linux 4.18.0-305.12.1.el8_4.x86_64	undefined	undefined			
15	v2cpe1103	Linux	PC	Linux 4.18.0-305.12.1.el8_4.x86_64	undefined	undefined			
16	v2cpe1105	Linux	PC	Linux 4.18.0-305.12.1.el8_4.x86_64	undefined	undefined			
17	v2cpe1202	Linux	PC	Linux 4.18.0-305.12.1.el8_4.x86_64	undefined	undefined			
18	v2cpe1204	Linux	PC	Linux 4.18.0-305.12.1.el8_4.x86_64	undefined	undefined			
19	v2cpe1306	Linux	PC	Linux 4.18.0-305.12.1.el8_4.x86_64	undefined	undefined			
20	v2cr1_vmxvcp	Juniper	VMX	JUNOS 18.1R1.9	warning	EoX	2022-06-01	2023-06-01	2026-01-01
21	v2cr2_vmxvcp	Juniper	VMX	JUNOS 18.1R1.9	warning	EoX	2022-06-01	2023-06-01	2026-01-01
22	v2cr3_vmxvcp	Juniper	VMX	JUNOS 18.1R1.9	warning	EoX	2022-06-01	2023-06-01	2026-01-01
23	v2dr12_vmxvcp	Juniper	VMX	JUNOS 18.1R1.9	warning	EoX	2022-06-01	2023-06-01	2026-01-01
24	v2dr13_vmxvcp	Juniper	VMX	JUNOS 18.1R1.9	warning	EoX	2022-06-01	2023-06-01	2026-01-01
25	v2tr14_vmxvcp	Juniper	VMX	JUNOS 18.1R1.9	warning	EoX	2022-06-01	2023-06-01	2026-01-01

Device EoX Report Table : 2022-01-02 13:06:00 +0100 - 2022-01-03 13:06:00 +0100 (+1h)

Report Settings

Statistic Type: EoX Report
Report Type: Device EoX Report Table
Top-N: 0
Monitor Severity: ≥ ● Information

SLA Marker | Element Filter | Value Filter

Time Settings

Time Interval | Date Range
Time Interval: 1440 — Full minutes
Time Offset: 0 — min

EoX & Vulnerability Reporting in StableNet®: Maintain oversight and react quickly by customizing your own succinct overview of End-of-Sales, End-of-Support, End-of-Life, and vulnerabilities. StableNet® is designed from the ground up to work across technologies and vendors to bring you the best all-in-one network and services management platform.

StableNet® Solution

While our optional Vulnerability & EoX service provides valuable information regarding new vulnerabilities and EoX announcements, the next step is figuring out a scalable solution to run automated checks of your entire network. With monitoring and inventory management by StableNet®, the XML Discovery Engine is regularly scanning your infrastructure. This data is fed into the centralized database repository that allows for an automated, up-to-date view of your landscape and is crucial in helping you ensure and maintain accurate and current vulnerability and EoX information. By having a dynamic overview of your hardware, software and configuration data all in one place, you know that each scan results in an accurate assessment of your current situation.

The StableNet® automated Vulnerability and EoX service is particularly powerful in its ability to provide a scalable solution. The vendor-supplied information is not just generically matched with the assets you have in your inventory. Sometimes, you may be using a software version that has been flagged for a vulnerability, but you are not using that specific software module (a false positive would typically have added to network operator overload). With StableNet®, customizable notifications and alarms are only triggered if they impact the actual device or software configurations that you use. StableNet's® unified database is truly unique in that it provides a holistic, in-depth aggregation containing all of the intricacies of your individual network.

Once dynamic vulnerability and on demand EoX scans are complete, the analysis and reporting engines provide highly-flexible, comprehensive tools to help you visualize and communicate the current state of your infrastructure via graphical dashboards. Vulnerability analyses include statistics on vulnerabilities broken down by their severity (e.g. minor, major, etc.). EoX analyses provide information on specific model/module/OS types and the number of affected instances. This can be further clarified in customizable Lifecycle or Vulnerability reports to help identify current vulnerabilities and EoX-triggered events. This not only helps in compliance reporting, but also to ensure visibility and comprehensibility to problem management teams.

Benefits & Results

Like an umbrella in a hurricane, vendor support for networking devices and software is simply not enough to help manage the torrential downpour of network infrastructure security issues that large corporations are constantly being bombarded with. With the powerful StableNet® Unified Network & Services Management platform, you have a solution that allows you to automate critical tasks and ensure that your multi-vendor and –technology network is safe from any sized storm. A customizable, scalable approach, StableNet® allows you to see your network for what it truly is, to receive notifications and alarms that matter, and to use this information to take appropriate actions. Whether you're concerned with compliancy, security, or resource management, StableNet® truly is an exceptional management platform for large networks in need of an automated solution to proactively identify problems before it's too late. StableNet®: one code base, one data source, one platform, and one GUI, for one holistic unified network & services management solution.

Key Benefits

- Centralized database repository with in-depth detail of actual network and services

- Automated scanning of hardware, software for Vulnerability and EoX

- Highly-scalable solution that minimizes false positives

- Detailed analysis of key security statistics and parameters

- Customizable dashboards for reporting on Vulnerability and EoX

- Simplified compliancy checks and violation report generation

powered by infosim®