SCOP NET

NAC Solution Requirement

Cyber security is the cornerstone of a world connected over the Internet. In the years to come, a significant increase in the number of Internet users, devices and data across the globe will result in great opportunities as well as equally intimidating challenges. Cyber security covers many different concepts, from information security to operational security and the security of computer systems, network access control security (NAC), security information and event management (SIEM) and monitoring of network and system devices. Cyber security has different meanings for different people. In terms of individuals, this concept is to feel safe, to protect personal data and privacy. For institutions, cyber security means ensuring that
business-critical information is available, and that confidential data is protected by operation and information security. Cyber security refers to common activities and resources that enable individuals and institutions to reach computing objectives in a safe, private and reliable manner. Dependence on information technology brings with it a number of risks. Assailants can attack secure networks using various methods, anonymously and in secret (a keystroke takes around one hundred and fifty milliseconds to travel around the world). Mobile devices are rapidly spreading and even taking over from traditional personal computers. The increase in the number of internet users worldwide can lead to new vulnerabilities. In order for corporate networks to remain secure, devices that are connected to the network or will be connected must be subject to specific checks. Today, the types of devices and connection types necessary on a network vary. The connection requirements of the personnel of the institution, the guest personnel coming to the institution or the company personnel who support the institution all put network security at risk. Network Access Control Systems (NAC) are used to minimize these risks.

What is expected of the NAC System?

As the use of technology increases, the damage caused by cyber attacks is increasing rapidly. In May 2017, a large cyber attack was carried out that affected more than 57,000 computers in hospitals, companies and government departments of 100 countries, files on the targeted computers were encrypted and ransoms were requested from the victims to decrypt the files. In the 2017 Verizon Data Violation research report, it is stated that 81% of the breaches were facilitated by stolen or weak passwords and in 51% of them malicious software was used. Today, it is important to protect corporate networks from the increasing security threats, to monitor devices and circumstances in the corporate network, to set policies for devices to be connected to the corporate network and to prevent or limit access to devices that do not comply with these policies. For this purpose, it is necessary to install the Network Access Control System (NAC), to check that any devices wishing to access the corporate network comply with the determined security policies, providing access to those that comply and blocking access from unsuitable devices.

What is ScopNET?

ScopNET is a NAC solution that prevents unauthorized access to data networks and identifies malware with advanced threat analysis.

Why is ScopNET Different?

Scopnet is a solution capable of working with all independent brand and model network devices in order to prevent unauthorized devices from being incorporated into the corporate network. The auditor can perform his/her duties without using the 802.1x protocol and can manage 802.1x operations using the ScopNET Radius architecture.

A New Dimension in Threat Management;
- Makes various analyses on ScopNET systems.
- Major analyses performed
- Outbound programs
- Connection of devices with each other
- Network traffic created by applications
- Port scanning operations
- Detection of weak SNMP passwords, detection of weak operating system passwords
- Detection of malware
- Malicious system drive analysis
- Malicious service analysis, malicious automated employee analysis
- Malicious scheduled work analysis

Gains After Using ScopNET

- It is important to identify the behavior-based security breaches that may occur after users are authorized and included in the network. In this way, any security breaches that may occur after accessing the network can be detected with minimal operational costs.
- ScopNET can monitor key security incidents, such as password change, account lockout, event logging, change of account groups, and can prevent access to devices or accounts that are found to have security flaws during this process.
- ScopNET allows direct command execution on network devices. This structure increases efficiency in large systems. This provides easy integration with all devices that support SSH/Telnet/SNMP protocol.
- ScopNET can detect and block using multiple methods without requiring any structural changes on the network.
- Low operational costs with the advantage of being a domestic and national product,
- Application and service inventories,
- Microsoft WSUS status and Antivirus update status and analysis
- USB usage tracking, Windows AutoRun records
- General WMI Inventory, Windows Registry Inventory
- Incorrect User Entries, Port Scans
- Important Windows Event Logs
- Network Connection Settings, Virtual Host NAT Analysis
- File Analysis and BitLocker usage detection
- Windows Security Center Analysis
- Weak SNMP password analysis, weak Windows password analysis
- Bandwidth usage, TCP Connection Analysis
- Application Analysis for Listening Port, Scheduled Tasks Analysis
- Windows Driver Analysis

802.1x Support

scopNET Radius Key Features

- Active Directory Dynamic VLAN assignment
- Prioritize dynamic VLAN assignments
- Dynamic VLAN assignment according to NAS Port Type (Be able to assign different VLANs to users connecting wirelessly and users connecting through a cable)
- MAC Bypass
- Wildcard MAC Bypass and Dynamic VLAN assignment
- Time dependent MAC Bypass operations (integrated with NAC, Discard Device and Discard with Date)
- User-Computer and Certificate-based authentication
- Identify and assign a MYSQL-based user
- Assign different VLANs for mobile devices