Wise-Mon
MONITORING SOLUTIONS

SWAT

SWAT 4.3

Network Access Control & Compliance Manager

Network Access Control

Security management and access control to the organization LAN is a critical domain in the IT organization of every organization. Along the years many efforts and resources were invested in avoiding external resources from accessing the LAN, products such as Firewall and Authentication Servers developed in order to avoid unauthorized access to the organization network but these products can't avoid accessing of unauthorized people and devices from the LAN itself.

During the last years, security organizations and managers awareness to the threat of accessing the LAN by unauthorized resources from the organization network were increased. Network devices provide control tools that enable the system administrator to enforce basic controlling mechanism, some protocols try to answer to the threat but usually require agent installation on each device and endpoint and it supports Windows OS only. There is no response to many types of devices such as printers, embedded and Linux devices, etc.

Solving the threat require a product that support a vary device types and vendors including all sorts of end points.

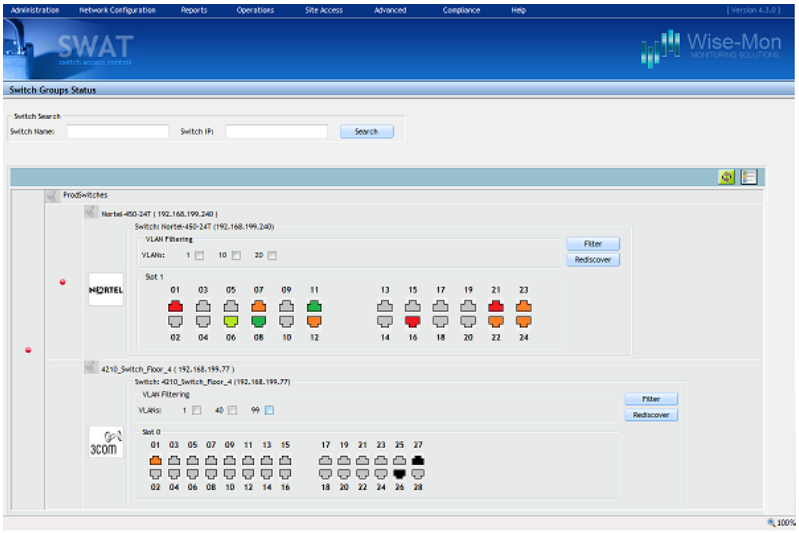
SWAT that was developed by Wise-Mon gives the total solution for such threats and support the information security approaches.

SWAT

SWAT is a Software product that gives overall solution for network access control (NAC) based on checking the devices that require network services.
SWAT enables the system administrator and security departments to define and enforce a clear policy of LAN accessing authorization based on the connected device type.

SWAT is developed since 2004 and today it helps many organizations to protect their LAN from internal threats. The latest version, 4.3, which was released at September 2010, provides innovative approach in avoiding access to the LAN based on vary protocols and techniques such as: Finger Print checking, Port grabbing, WMI, HTTP, SNMP.

SWAT has an easy to use web based management interface that enables policy definitions and an event console that provides information about all the events in the network. Using SWAT the organization can control and monitor the devices that connected to the organization network independently of the device type and vendor.
SWAT enables integration to SIEM/SOC systems based on SYSLOG and SNMP Traps



Main Features

- SWAT as a software product eliminates the need of adding a new device to the servers room.
- SWAT interface enable defining characteristics of authorized devices based on a vary number of protocols such as: WMI. Telnet / SSH, TCP based protocols, SNMP, Etc.
- Policy definition based on the above characteristics enables the organization to enforce pre defined policies when an unauthorized device is detected:
    - Alert – send alert to the alerts console, send alert to organizational SOC, send SMS, e-mail, etc.
    - Disconnect the unauthorized device from the network
    - Move the unauthorized device to a dedicate VLAN
- Decentralized management of the organization network – SWAT supports Federated Management that enables defining different policy for each zone or region.
- MAC spoofing support.
- IP Phone support.
- Fast and easy deployment that not require agent installation.

Compliance

Organizational compliance management system enables the policy decision makers to define policy for each device type that connected to the LAN. SWAT architecture give the network administrator the option to define which device types are entitled to connect the LAN and what characteristics are needed from every device type in order to enable its network connection.

Contact:
Cell: +972-54-5636818
Fax: +972-3-5059474
swat@wise-mon.com

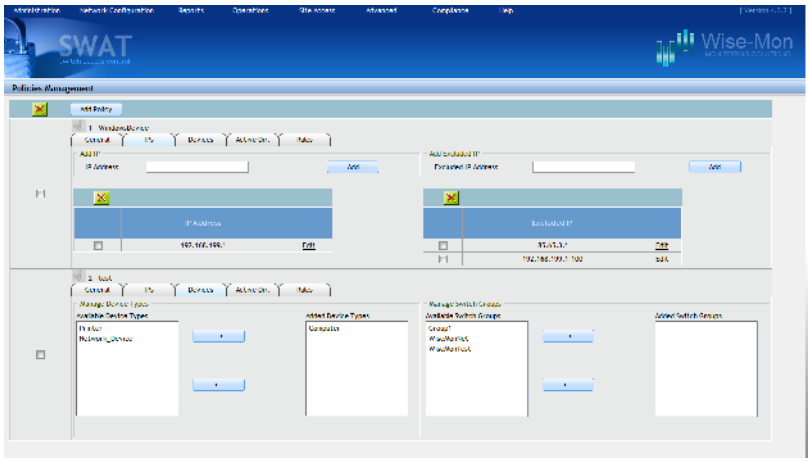
The validation process is based on identify and label the device (based on FP) and open ports monitoring. This process is done by structured NMAP interface.
Compliance tests are based on:

- WMI based compliance tests
  - Check if defined service is active or not-active
  - Check disk space and free disk space
  - Check the existence of defined process
  - Check a defined registry key value
  - Check Domain authorization
  - Check a defined NIC status
  - Check the number of active NICs
  - Check if a defined file existing in the disk
  - General WMI check for receiving a defined value from the Database
- Telnet based compliance tests
  - Welcome note / Banner check
  - Prompt check
  - Run a defined script
- HTTP based compliance tests
  - Checking a device WEB interface and strings
  - Checking HTTP based login
- TCP based compliance tests
  - Monitor open ports
  - Monitor TCP grabbing

Compliance Management

The compliance status interface enables receiving information about each device that was connected to the LAN in order to get the device status in terms of compliancy.

This interface helps the security administrator to receive information about the approved device and based on which policy it got the approval to be connected to the LAN.



SWAT & Active Directory

SWAT has full integration with AD and can provide AD based policy enforcement for LAN switches
The system may enable connection for a specific port only for a certain users/computers from a specific OU or Group

Device Analyze

Device Analyze interface create a detailed report of a defined IP address

Enforcement

Wise-Mon
MONITORING SOLUTIONS

Contact:
Cell: +972-54-5636818
Fax: +972-3-5059474
swat@wise-mon.com

In case of compliancy failure the system administrator can define the following automatic actions:

- Move the detected device to VLAN Remediation
- Disconnect the device from the LAN
- Sending alert using: E-mail, SMS, Trap, Syslog

IP phone support

SWAT knows to separate Voice VLANs from Data VLANs in supported switches, additionally SWAT supports:

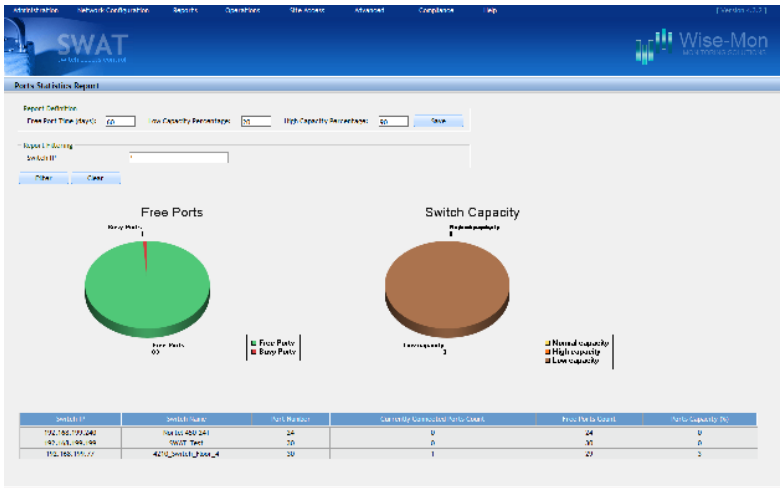
- The ability to study defined addresses on Voice and Data VLANs
- Showing Voice VLAN ports separately from Data VLAN ports
- Moving Voice VLANs and Data VLANs separately

Reports

SWAT has a very set of reports for trend analysis, these reports enable the organization to follow the threats and alerts and irregular behavior along time.

Sites management system enable the organization receiving a clear geographical view based on site, building, room, port. Activity report shoes the activities that were done by users, i.e. who did each activity and when each report can be sent by mail to the relevant people according to some levels (Switch and Switch group)

SWAT also support Safe VLAN for removing ports automatically' policy can be defined based on each parameter including SNMP OIDs



Wise-Mon
MONITORING SOLUTIONS

Contact:
Cell: +972-54-5636818
Fax: +972-3-5059474
swat@wise-mon.com

Wise-Mon
MONITORING SOLUTIONS

Integration with organizational systems

SWAT has a WS based API for enabling enforce policies with 3rd party tools; SWAT also provides integration with major anti-virus systems in order to identify detected devices and to disconnect them from the network or moving them to another VLAN.

SWAT has the following NMAP interface:

- Management interface for certain IP address analysis
- Finger Print tests
- Open ports monitoring

Installation

SWAT installation doesn't require any infrastructure changes. Installation procedure is simple and has no effect on network performance

System requirements

SWAT has is a Software product that installed on Windows servers.

Software:

- Operating system :Windows 2003 server
- Database: Microsoft SQL 2005
- Web Server: Internet Information Server
- .NET 2

Hardware:

- Pentium 4 2.6 GHZ Processor
- 2 GB Memory
- 80 GB Storage SATA/SCSI

Contact:
Cell: +972-54-5636818
Fax: +972-3-5059474
swat@wise-mon.com