Centralized Antivirus Management

An Effective Approach for NICNET

In order to have a centrally managed antivirus solution for NICNET, National Informatics Centre has deployed three-tier architecture for Antivirus Management. One Antivirus Distribution/ Relay Server is deployed at each Bhawan/ State and a Central Antivirus Server is installed at NIC (HQ)

RAVI VIJAYVARGIYA
Sr. Technical Director
ravi.vijay@nic.in

D. H. KHAN
Technical Director
dhkhan@nic.in

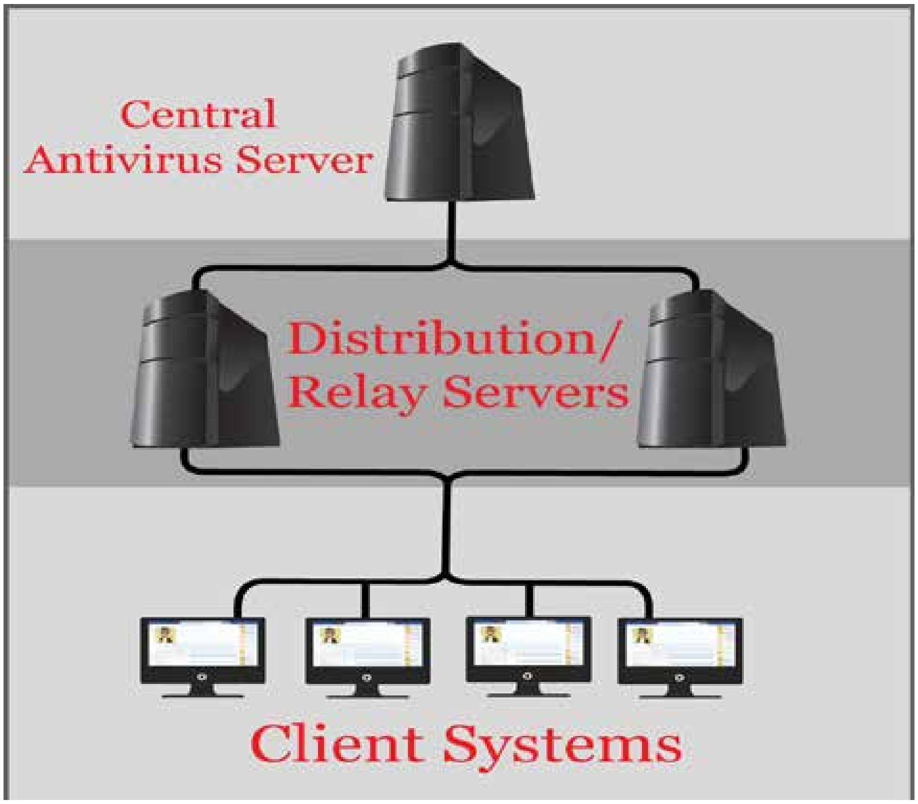
K.B. HARIHARAN
Scientist-D
kbh@nic.in

RAJESH KUMAR TRIPATHI
Scientist-D
rajesht@nic.in

Edited by
MOHAN DAS VISWAM

Centralized antivirus management technologies provide enterprises a bird's-eye view of antivirus defenses and establish applications that protect against unwanted malware and viruses. Contemporary distributed networking is a complex infrastructure of servers, gateways and workstations - in some enterprises, numbering thousands of nodes - all vulnerable to virus infections. The challenge to system administrator is keeping the antivirus applications on all of these systems updated and properly configured before the systems are infected with the next variant of viruses, worms, Trojans, bots and Ransomwares.

Centrally managed antivirus solution enables constant monitoring of the antivirus status on the client systems thereby ensuring latest antivirus signature pattern on the systems. Where the latest signature is not able to provide security, the infected system is analyzed further and new signatures are developed by taking up the matter with the antivirus Lab of the OEM (Original Equipment Manufacturer). This is a continuous process.



Architecture of NIC's Centralized Management of Antivirus

VISIBILITY OF ALL END POINTS

The basic feature set of all antivirus management suites is the ability to see all users on the network, know what antivirus application versions they're running, efficiently and expediently update virus signatures and policies, and receive threat alerts and other reports.

SIGNATURE UPDATES

In order to have a Centrally Managed Antivirus Solution for NICNET, NIC has deployed three-tier architecture for antivirus management. Antivirus client software is installed in each computer connected to NICNET, Antivirus Distribution/ Relay server is deployed in each Bhawan/ State and a Central Antivirus server is installed at NIC (HQ). The logs from the Bhawans/ State level antivirus server are sent to the Central server and are analyzed on a regular basis. These logs are further correlated with the logs of the other security devices (UTM and IPS). Based on this analysis, a report of defaulting IP addresses that either do not have the antivirus or have outdated antivirus signatures is generated and corrective action is taken/ recommended on such systems.

CENTRALLY MANAGED ANTIVIRUS ARCHITECTURE

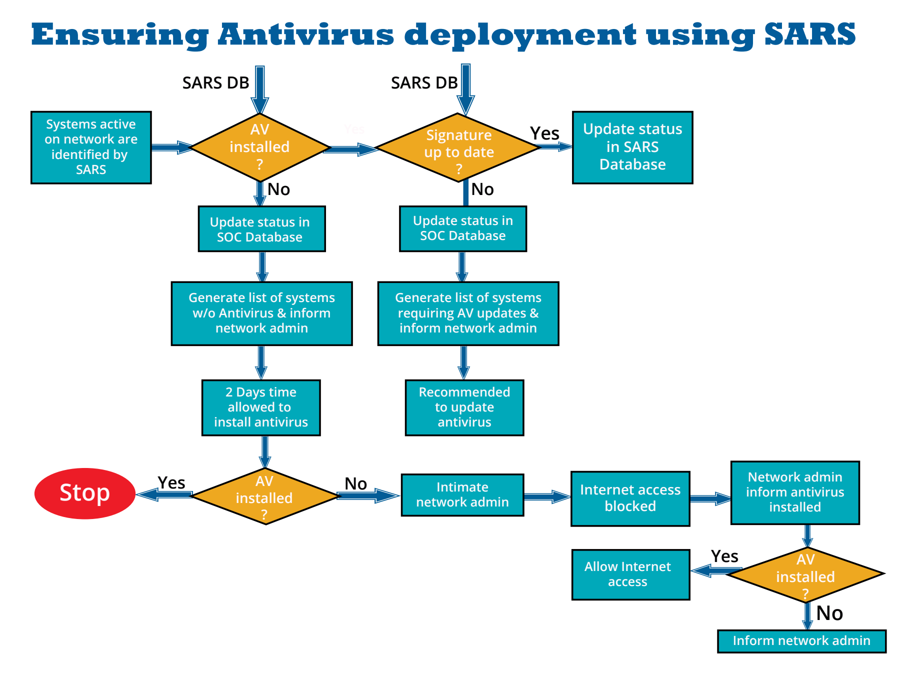
Besides the antivirus log correlation, the Security Monitoring Team on continuous basis also analyzes the network access behavior of the client systems. With this analysis, systems generating suspicious traffic on the network are identified. If antivirus is not installed or is not up-to-date on the identified systems, corrective action is taken/ recommended for the same. The analysis, at times, indicates that the systems depict suspicious behavior despite having up-to-date antivirus signatures. For such systems, where the signatures are up-to-date but still generating suspicious traffic, logs and system information is collected. Using this system information, logs and suspicious files the development of new signature pattern takes place with the help of Antivirus Lab of the OEM. It may be noted that NIC has an arrangement with the Antivirus OEMs (whose solutions are used in NICNET) under which the OEM has an obligation to analyze the logs and develop antivirus signatures.

LIMITATIONS OF USING THIRD PARTY ANTIVIRUS COMPARED TO CENTRALLY MANAGED ANTIVIRUS SOLUTION USED IN NICNET:

If systems do not have centrally managed antivirus, there is no way to ascertain if such systems are installed with any antivirus at all in the first place and even the support person would not be in a position to ascertain the antivirus status without physically going to each of the systems. If at all such a system is running with antivirus solution (other than the centrally managed antivirus solution), there is no mechanism to ensure that the signatures are kept up-to-date. In the absence of a service agreement with the antivirus OEM, it would not be possible to take up the matter with concerned antivirus OEM for the development of new antivirus signatures. NIC has deployed Centrally Managed Antivirus Solution of one OEM per Bhawan/ State/ Location for ease of management and monitoring.

POLICY ENFORCEMENT

Updating signatures is part of the challenge of managing antivirus defenses on large, distributed networks. If users disable their virus scanners - say, to install a new piece


Ensuring Antivirus deployment using SARS
SARS DB
SARS DB
Systems active on network are identified by SARS
AV installed ?
Yes
Signature up to date ?
Yes
Update status in SARS Database
No
No
Update status in SOC Database
Update status in SOC Database
Generate list of systems w/o Antivirus & inform network admin
Generate list of systems requiring AV updates & inform network admin
2 Days time allowed to install antivirus
Recommended to update antivirus
Stop
Yes
AV installed ?
No
Intimate network admin
Internet access blocked
Network admin inform antivirus installed
Allow Internet access
Yes
AV installed ?
No
Inform network admin

Process of ensuring antivirus deployment using SARS of (often unauthorized) software - they can create gaps in the antivirus protection.

Centralized Antivirus Management enables efficient enforcement of security policies by providing mechanisms for routinely applying product patches and upgrading software, scanning systems for malware, and configuring antivirus application settings.

Centralized management solutions can also push policy and configuration changes to the client, restart disabled scanners and deploy new antivirus software. In some cases, the management console can remotely install new software and reboot the client.

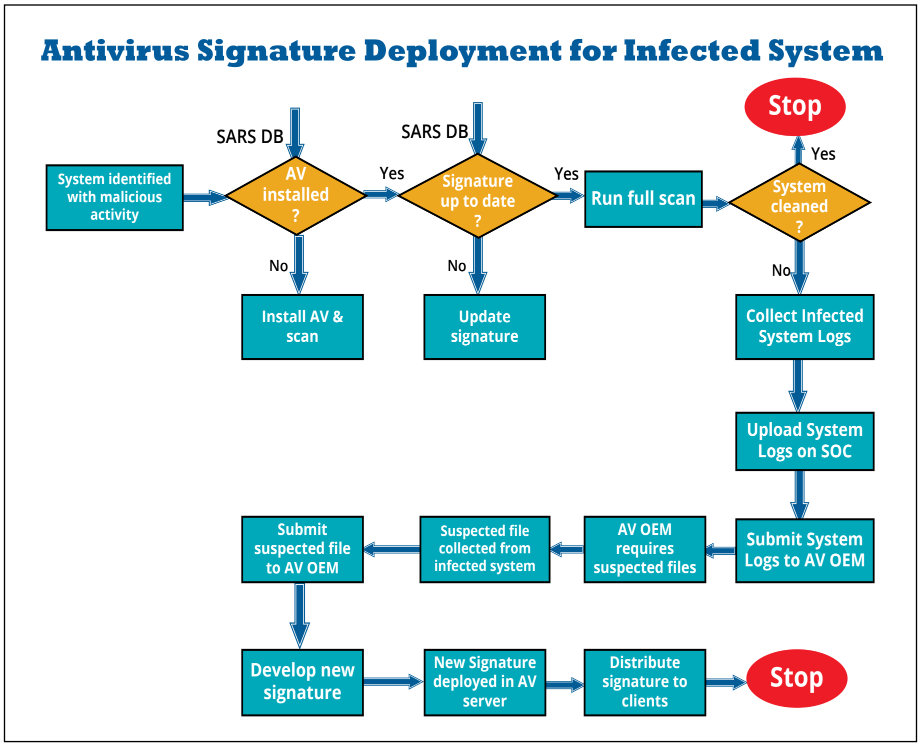
ALERTING FUNCTIONS

Time is of essence when new viruses are discovered in the wild. Administrators must implement mitigations and update signatures before the virus or worm enters the network. Most management consoles come with alerting mechanisms that tell administrators when their antivirus devices encounter a threat.

If new signatures are available, they can push the signatures out to the antivirus clients. If signatures aren't available, they can quarantine the point of infection to keep the malware from spreading to the rest of the network.

REPORTING AND ANALYSIS

Antivirus solutions deliver statistics on the number of viruses they detected, deleted and quarantined. Antivirus management consoles can collect and aggregate those statistics, as well as other operational information, for analysis.


Antivirus Signature Deployment for Infected System
System identified with malicious activity
SARS DB
AV installed ?
Yes
No
Install AV & scan
SARS DB
Signature up to date ?
Yes
No
Update signature
Run full scan
System cleaned ?
Yes
Stop
No
Collect Infected System Logs
Upload System Logs on SOC
Submit System Logs to AV OEM
AV OEM requires suspected files
Suspected file collected from infected system
Submit suspected file to AV OEM
Develop new signature
New Signature deployed in AV server
Distribute signature to clients
Stop

Process of Antivirus Signature Development for infected system

Antivirus logs and reports can show the devices and network segments most often targeted, and how well the antivirus defenses perform. Such information can help administrators identify and correct soft spots in their security infrastructure. And policy compliance reports show which users are opening gaps in the antivirus defenses.

SECURITY ALERTING AND REPORTING SYSTEM (SARS)

NIC has developed in-house software i.e. Security Alerting and Reporting System whose primary function is collecting, compiling and analyzing the IP addresses passing through various security devices and correlate with their antivirus status observed in the respective antivirus solutions.

This application also sends alert messages to the security administrators positioned at Bhawans and States for problems rectification such as installing the antivirus on endpoints, updating the signatures where signatures are not updated, collection of logs of the endpoints etc.

CONCLUSION/ SUMMARY/ WAY FORWARD/

Thus it is clear from the above discussion that running standalone antivirus solution on the endpoints does not assure security. Hence, in a nation-wide network like NICNET, centralized antivirus solution is the best option to protect the endpoints from viruses, worms, bots and malwares.

For further information, please contact:
RAVI VIJAYVARGIYA
Sr. Technical Director
Network Security Division
NIC HQ, A1B3, CGO Complex
Lodhi Road, New Delhi-110003
Email: ravi.vijay@nic.in
Phone: 24305122