# Virus protection for NAStorage 8200

2003.6.13 Henry Ho

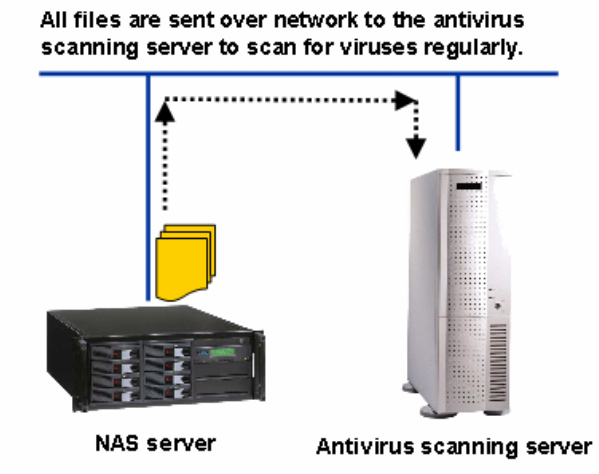
## 1. Abstract

As companies are deploying enterprise-wide anti-virus protection to prevent from losses caused by rapidly spreading deadly viruses, NAS servers are usually the most vulnerable systems because most of them do not include antivirus capabilities, nor can an antivirus software run on them. Data on NAS servers are often unprotected against virus threats. To address this issue, Ingrasys Technology and Trend Micro worked together to offer integrated antivirus solutions for our NAStorage servers. Running Trend Micro's best-of-class antivirus software, our NAStorage servers have now fast, economic and easily deployed virus protection.

## 2. Different approaches of protecting NAS servers from viruses

- Set up antivirus scanning servers to scan NAS servers on predefined schedules:

  For NAS servers with no antivirus capability, MIS people usually set up a Windows server running some antivirus software and set schedules for scanning the NAS servers regularly.

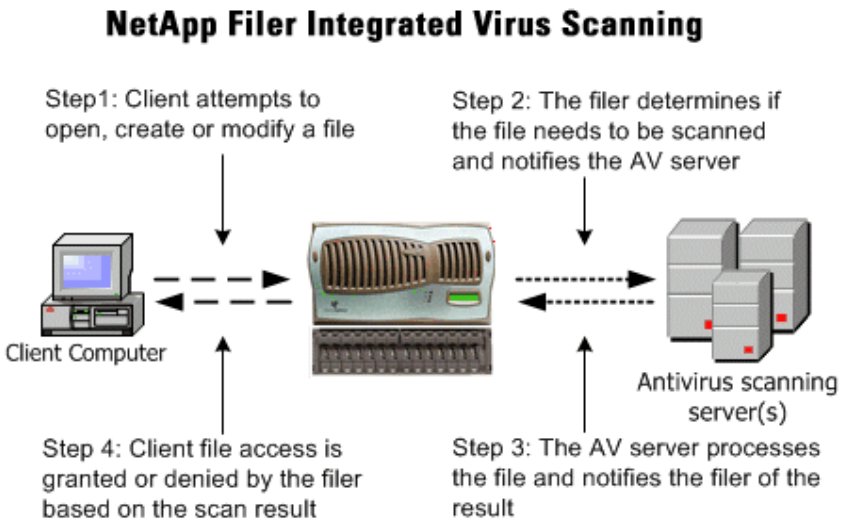



  There are some disadvantages as it causes heavy network traffic and the antivirus scanning servers must read all the files on the NAS servers in

order to scan them. Moreover, the NAS servers are heavily accessed during scanning which forces scanning tasks to be started in off-hours so that normal operations are not affected. Most importantly, there are chances that, by the time of scanning, all files on the NAS servers have already been infected or damaged by viruses.

- Set up antivirus scanning servers to scan NAS servers on file access

  Some NAS vendors take this approach. Network Appliance is an example. MIS people must also set up an antivirus scanning server. The difference is that, they can not only scan NAS servers on predefined schedules, but also scan files on access. See the diagram below.




  Same as the first approach, the file being scanned must be sent to the antivirus scanning server over the network. Clients will experience some lags in network performance but the NAS server can get real-time virus protection.

- Manually install an anti-virus software on the NAS servers

  For NAS servers running Windows SAK operating systems, MIS people can choose to install any Windows-compatible antivirus software on these NAS servers.

  The disadvantages are that companies must purchase extra licenses for those

NAS servers and deployment costs are high since MIS people must manually install the antivirus software on each NAS server. The advantage is that companies can deploy the same antivirus solutions from one antivirus vendor for both Windows PCs and NAS servers.

- Running built-in antivirus software directly on NAS servers

  This approach is to integrate the antivirus software into the NAS OS and run it natively. An example is the Snap Appliance's Guardian OS. It integrates CA's eTrust antivirus software to provide manual and scheduled virus scanning capability. However, it lacks the most important real-time virus protection due to some integration difficulties.

**With the integrated antivirus software, the NAStorage servers can protect themselves from virus attacks.**

Using a similar approach, the NAStorage integrates the Trend Micro's antivirus software and takes advantage of Trend's services such as frequent virus pattern updates. In addition to a manual and scheduled virus-scanning, it also detects and protects from virus attacks on the fly when clients are accessing the NAS servers. Protection is around the clock and without interruption.

## 3. The advantages of integrating the antivirus software in the NAS

More and more NAS vendors are considering integrating and running the antivirus software natively on NAS servers. The advantages are obvious. Better integration. Less deployment time and costs. Less degrading of network performance.

With an antivirus software is integrated into the NAS servers, no extra licenses

are required. Moreover, MIS people do not have to install the software into each NAS server separately. The deployment costs are thus greatly reduced.

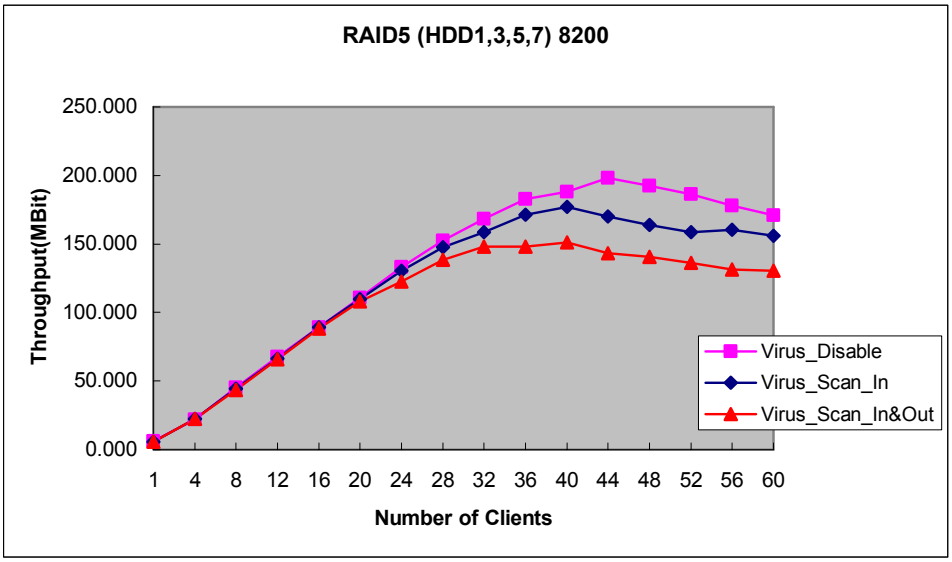
By running the antivirus software directly on NAS servers, performance impacts are minimized and network traffic is largely reduced since data are not sent to the antivirus scanning servers over the network.

## 4. Performance impacts when the real-time virus protection is activated

To protect the NAS servers from viruses at all times, it is necessary to have real-time virus protection, which scans for viruses when clients are accessing (writing to or reading from) the NAStorage servers. When clients are writing files, the data will be written to the NAS disks first and scanned for viruses. When clients are reading files, the data will not reach the clients until they are completely scanned. In both cases, NAS performance will be slowed down by a certain percentage.

Below are test results using the NetBench 7.02 software for the NAStorage 8200. There are three situations – the first is with the real-time virus protection turned off, the second is to scan the incoming files (i.e., during file writes), the third is to scan both incoming and outgoing files (i.e., during file writes and reads).

Let's check the performance differences:



Let us take 44 clients as an example.
The network throughputs are respectively 198Mbps, 170Mbps and 143Mbps.
As you see, the performance is reduced by ~ 14% when scanning incoming files.
The performance is down by ~ 28% when scanning in both directions.

## 5. Which network protocols are protected and which ones not?

The NAStorage server can be accessed through various network protocols – SMB, AppleShare, FTP, HTTP and NFS. Of those protocols, SMB, AppleShare, FTP and HTTP are well protected by the real-time virus scanning function. All file reads or writes from any of those protocols will trigger the virus-scanning. On the other hand, the NFS service running on the NAStorage servers is executed in the kernel mode and will not be able to trigger the virus-scanning during file reads/writes.

Although viruses written for the UNIX world are by far less than those for the Windows world, it is still suggested to set scanning schedules to regularly scan the NAStorage servers for viruses in order to screen out any infected files which could possibly enter through the NFS protocol.

## 6. Key features of the NAStorage virus protection software

- Real-time virus scanning protects the NAS server from virus attacks around the clock
- Features manual and scheduled virus scanning for screening out any infected files from your NAS sever
- Automatic virus pattern updates from the Trend Micro update server keeps your virus protection up to date
- Defines whether to quarantine, clean or delete the infected files when a virus is found
- Issue of email notifications, SNMP traps or web reminders when a virus is found using manual or scheduled scans
- Complete records of infected files and scan history