

Virus protection for DataNAS XP

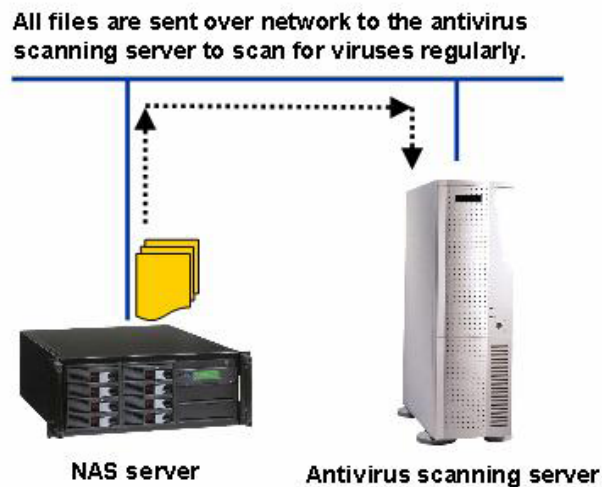
1. Abstract

As companies deploy enterprise-wide anti-virus protection to prevent losses caused by rapidly spreading viruses, NAS servers are often left vulnerable. Most NAS servers do not include anti-virus capabilities, leaving data unprotected against virus threats. To address this issue, Excel/Meridian Data introduces the DataNAS XP Filer, featuring integrated industry-leading Trend Micro anti-virus software.

2. Different approaches of protecting NAS servers from viruses

- Scenario 1: Set up anti-virus scanning servers to scan NAS servers on predefined schedules:

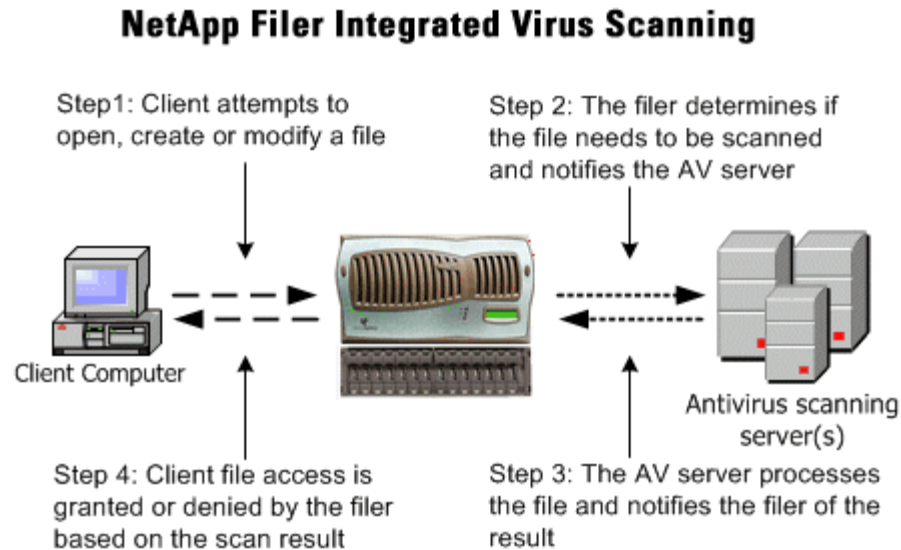
For NAS servers with no anti-virus capability, IT administrators usually set up a Windows server running some anti-virus software and set schedules for scanning the NAS servers regularly.



There are some disadvantages as it causes heavy network traffic and the anti-virus 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 during 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.

I Scenario 2: Set up anti-virus scanning servers to scan NAS servers on file access

Some NAS vendors take this approach, for example Network Appliance's NetApp. IT administrators must also set up an anti-virus scanning server separate from the NAS server. With this scenario and software support, the difference between this method and the first is that not only does software scan NAS servers on predefined schedules, but also scans files on access. See the diagram below.



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

I Scenario 3: Manually install an anti-virus software on the NAS servers

For NAS servers running Windows based operating systems, IT administrators can usually choose to install any Windows-compatible anti-virus software on the NAS server.

The disadvantages are that companies must purchase extra licenses for those NAS servers and deployment costs are high, as the IT administrators must manually install the anti-virus software on each NAS server and maintain them.

I Scenario 4: Running built-in anti-virus software directly on NAS server

This approach is to integrate the anti-virus software into the NAS OS and run it natively. An example is the Snap Appliance's Guardian OS. It integrates CA's eTrust anti-virus software to provide manual and scheduled virus scanning capability. However, it lacks critically important real-time virus protection, offering only anti-virus scanning on a scheduled basis. This could allow a virus to spread and infect data on the NAS without IT administrator knowledge until it is too late.



DataNAS XP, with integrated anti-virus software by Trend Micro, allows several levels of customizable virus protection, including real-time protection.

Using a similar approach, DataNAS XP integrates Trend Micro's anti-virus 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.

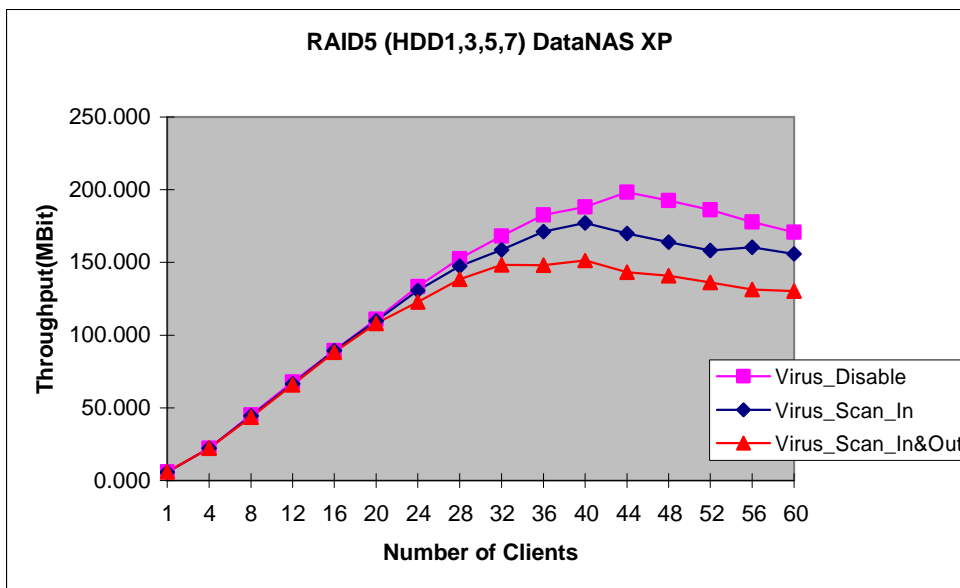
3. The advantages of integrating the anti-virus software in the NAS

The advantages are better anti-virus integration, less deployment time and costs, less degradation of network performance and bandwidth resulting in end-user lag. And from a cost standpoint, no additional anti-virus licenses are required for the new servers and users.

4. Performance impact of real-time virus scanning

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 NAS server. When clients are writing files, the data will be written to the NAS disks first and then immediately 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 marginally.

Below are test results using the NetBench 7.02 software for the DataNAS XP. 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).



Using 44 clients as an example:

The network throughputs are respectively 198Mbps, 170Mbps and 143Mbps.

As you see, the performance is marginally reduced by ~ 14% when scanning incoming files, and reduced an additional ~ 14% when scanning both directions.

5. Which network protocols are protected on DataNAS XP and which ones are not?

The DataNAS XP server can be accessed through various network protocols – SMB, AFP, FTP, HTTP/HTTPS and NFS. Of those protocols, SMB, AFP, FTP and HTTP/HTTPS are 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 DataNAS XP servers is not protected in real-time mode, so for this reason a scheduled anti-virus scan should still be run for Unix/Linux NFS uses.

6. Key features of the DataNAS XP 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, without any intervention
- | Options to choose whether to quarantine, clean or delete the infected files when a virus is found
- | Issue 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

Revision 06.18.03

Network Appliance is a trademark, registered trademark, or service mark of Network Appliance Inc in the US and other countries. NetApp is a trademark, registered trademark, or service mark of Network Appliance Inc in the US and other countries. Snap Appliance is a trademark, registered trademark, or service mark of Snap Appliance Inc in the US and other countries. Guardian OS is a trademark, registered trademark, or service mark of Snap Appliance Inc in the US and other countries. All other marks are held by their respective owners. Excel/Meridian Data believe this data to be accurate but are not to be held responsible for any inaccuracies.