# NVCNet for Terminal Servers

## *a unique approach to the WTS challenges*

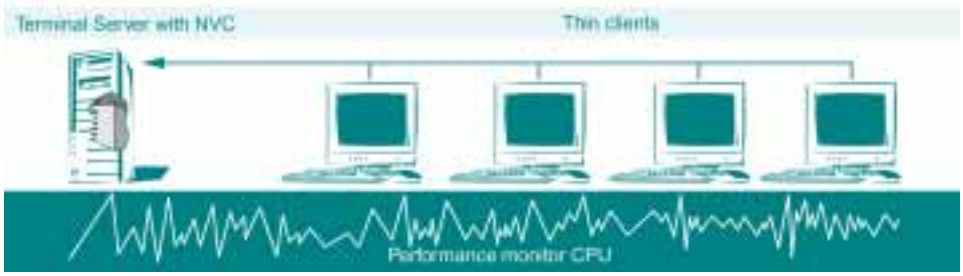
The use of Windows Terminal Services (WTS) is becoming more and more common in the small/medium enterprise sector. This is mainly due to the increasing bandwidth capacity of modern networks and the need for centralized management to reduce the risk of security breaches in the network. Terminal Servers reduce the total cost of ownership (TCO) in an organization.
Companies using WTS solutions have a need for antivirus software that is designed for this environment, different from traditional antivirus software for servers and workstations.

### The Terminal Server AV scanning challenge

A problem with On-access virus scanning on Terminal Servers is unpredictable peaks in CPU usage for the scanning. Some files take a lot of CPU power to determine if they are infected or not, and there are also situations when many users copy or save files to the Terminal Server at the same time, e.g. at start of the workday. These situations can unpredictably slow down the server, interrupting normal workflow on all terminals.

Testing has proved that this is a problem common to all virus scanners, so moving to other antivirus products will not help. One solution has been to invest in additional servers, to spread the heavy load on more CPUs.

(Fig: Show traditional On-access scanning on server)




### The NVCNet solution

In a Terminal Server environment, NVCNet adds flexibility and predictability to the environment. By adding dedicated NVCNet servers to the network, this moves the scanning load from the Terminal Server itself, to a separate virus scanning NVCNet Server. Consequently, most of the Terminal Servers' resources can be used to manage files and users, without interruptions caused by virus scanning.

By combining on-access scanning with the NVCNet technology, it is possible for a network administrator to more accurately predict both the resources needed to scan for viruses and the resources needed for the terminal services. When CPU load on the Terminal Server passes a set limit, the virus scanning is transferred to the dedicated NVCNet server. The CPU load on the Terminal Server will be lower, more stable, and not dependent on the type of files handled by the scanner.

(Fig: Show On Access scanning in combination with NVCNet)

**Load balancing and failover solution**
It is also possible to have several NVCnet servers connected to the Terminal Server. Then even more flexibility is added to the system by letting the next NVCNet server in the range take over if the first NVCNet server is already under heavy load.

Using at least two NVCNet servers also gives a failover solution, ensuring that OnAccess virus scanning will continue, even if one NVCNet server fails. This solution also give the possibility of updating the servers with patches etc. without the need for stopping AV scanning and thereby risk a potential virus infection.

## NVCNet concept

NVCNet -designed to remove CPU load and thereby avoid CPU load peeks on servers hosting files that are scanned by antivirus applications. The NVCNet solution has two parts – NVCNet server where the actual scanning of files are done and NVCNet client, placed on the Terminal Server where the files that are to be scanned reside. The NVCNet client communicates with the NVCNet server and passes files or fragments of the file over to the NVCNet server which scans the file for virus. Due to the logic and advanced design of NVCNet and our scanner engine we will in most cases need only fragments of a file to detect if it is infected. As a result, speed is increased and bandwidth usage is reduced.

There is no limit to the number of NVCNet servers in the network, and with two NVCNet servers you also get at system with fail-over and load balancing functionality. For load balancing the main server can be set to pass new scanning task over to another NVCNet server when the load reach certain threshold limits. And if one NVCNet server for some reason goes down or needs to be stopped for maintenance, the other will take over the scanning tasks.

In performance, the speed of a scanning session is restricted by the network speed. But unlike other scanners that transfer complete file across the network for scanning, NVCNet transfers relatively small amounts of data between client and server, thus maximizing the efficiency of the scanning session.

## Additional features for detection of viruses

**Norman SandBox v2**
Norman's SandBox technology detects new and unknown, binary computer viruses. Today, an email worm can infect tens of thousand workstations in a matter of seconds. The antivirus vendors are expected to find a cure, update the virus definition files, and distribute these to its customers immediately. The need for speed is paramount.

Norman's SandBox is a virtual world of computers in a network, simulated inside the virus control program. An emulator provides an environment where possible virus infected executables «run» just as they would do on a real system. The SandBox is particularly tuned to find new email-, network- and peer-to-peer worms.

**Decompression library**
A new advanced decompression module has been developed to scan files that have been compressed in different archive formats. This module now scan more than 30 archive types and variants like ZIP, TAR, RAR, ARJ, UUENCODE, ARC etc. If malware is found within an archived file, NVC will in most cases be able to clean the infection and repack the file.

## Updating virus definition files

A running version of NVC for servers have to be installed on the NVCNet server, and the updates of virus definition files will be handled by the standard NVC update module - Norman Internet Update (NIU). Norman Internet Update can be configured to regularly check for new and updated files on Norman's product servers. NIU offers complete updating and upgrading of the NVC software to ensure that virus definitions are kept up to date and that you are always running the latest version of the software. Norman Internet Update uses incremental updates of definition files to keep the size of the updates as small as possible, thereby reducing the network load and increase the speed in distributing updates.

## Prerequisites

Native Norman Virus Control for Terminal Servers installed on each Terminal Server that NVCNet for Terminal Server is installed (controls the virus scanning together with the NVCNet for Terminal Server client). Native Norman Virus Control for servers installed on each NVCNet server (this will handle all updates of virus definition files, engine, Norman SandBox, etc.)

## System requirements

For Windows NT, version 4 with SP4 (or higher) and Internet Explorer 4.0 (or higher) are required.
Windows 2000 and 2003 servers
For OS/2 we recommend Warp 4 fp 15 (or higher) and Java 1.1.8.