Best Practice for Networker® Legato and Firewalls

EMC Proven™ Professional Knowledge Sharing 2008

Pascal De Cock
Storage Engineer
Belgacom (BE)
pascal.de.cock@belgacom.be

Table of Contents

Disclaimer: The views, processes or methodologies published in this compilation are those of the authors. They do not necessarily reflect EMC Corporation's views, processes, or methodologies.

1 Summary

This article outlines how we implemented our environment to configure Networker Servers, Networker Clients, Networker Management Console, Networker Backup Advisor and communication to our Virtual tape library CentricStor over our private backup LAN(‘s) with defined access control lists.

This is not a new document, “How to configure Networker in a Firewall environment”, but an add-on with best practices in a mixed Networker environment.

The rules we present can be used as standards when adding new components in the environment.

2 Overview of the environment

Our security team decided to have separate LAN-traffic for management, applications and backups to ensure that no intrusion would be possible via the network between the several clients in one datazone or via the backup server. We defined that access control lists (ACL’s) should be defined, particularly for the backup LAN.

This triggered us to define the Service Ports Range for the communications between backup server and clients.

Also, we decided to create separate datazones depending upon what service they deliver.

In the middle of all datazones we have:

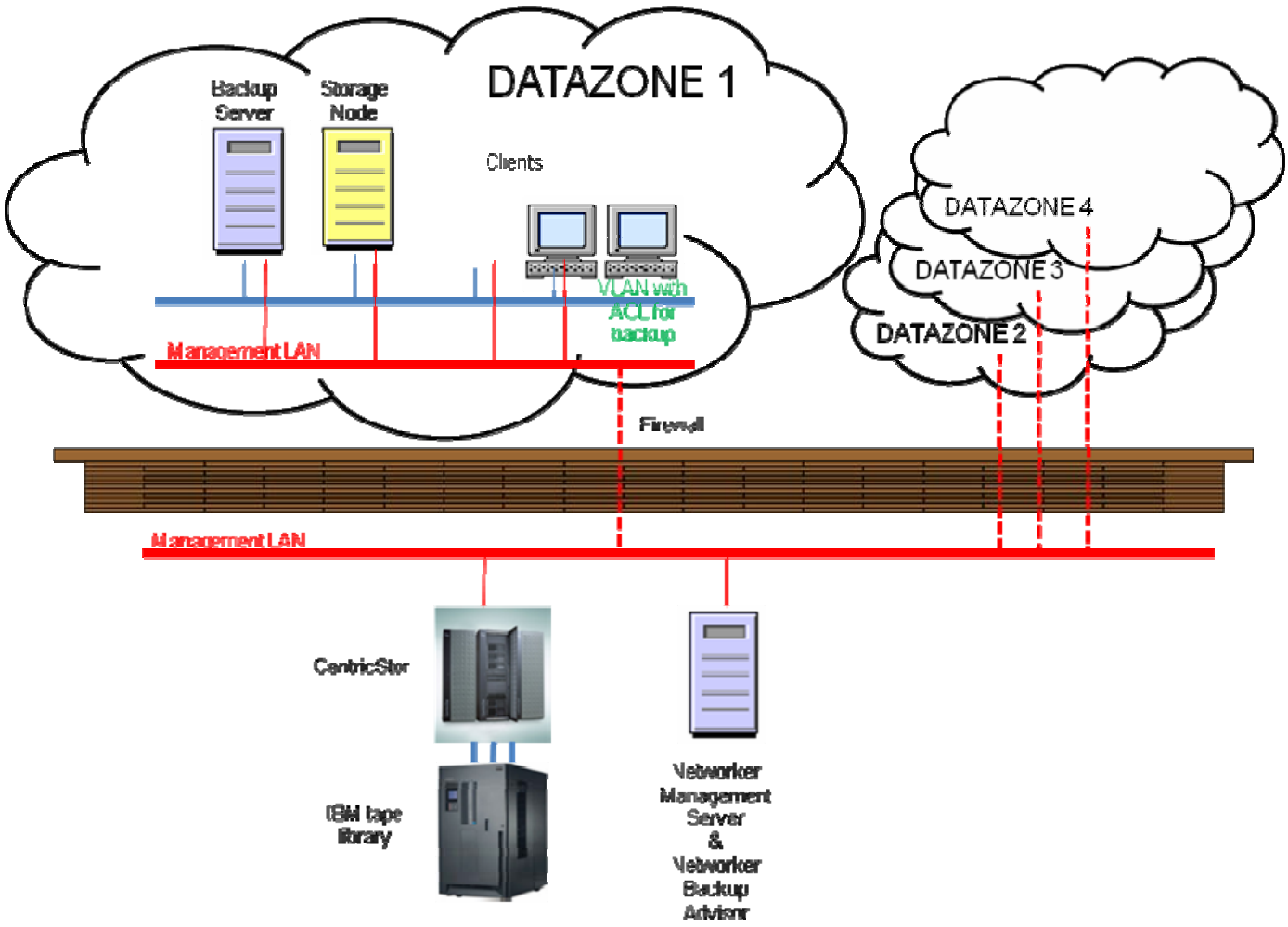
- our shared virtual tape library CentricStor
- our Networker Management Server
- our Networker Backup Advisor
- our Networker License Manager (is under construction)

The shared environment is protected with several firewalls toward the different datazones.

As a result, we had to include two communications channels in our environment.

- Communication between backup server and clients over private backup LAN
- Communication between the several datazones and the shared environment

2.1 Visualization



3 Determinations of service port ranges

When looking at the Networker administration guides concerning firewall support or when reviewing some other technical notes, we can narrow down the rules concerning Service port ranges.

From “Configuring Network Firewalls for a Networker Server,” a service port is:

> a port on which a server process listens for requests to provide a service. Service ports are also known as listen ports, or SYN ports. For example, an HTTP server typically uses port 80 as a service port and an SSH server typically uses port 22 as a service port. If a **2 Direct connect communication model** EMC® Networker® Release 7.3 or Later Configuring Network Firewalls for a Networker Server firewall is not configured to allow clients to make connections to a service port, the service will be blocked.

An overview of formulas that can be used to communicate between backup server and clients will be provided in the following chapters.

3.1 Service port ranges in 7.2.x

3.1.1 Backup server

5 is the minimum number of daemons registered on the Networker server.

- nsrexecd (uses two required ports, 7937 and 7938)
- nsrd (uses one port)
- nsrindexd (uses one port)
- nsrmmdbd (uses one port)

FORMULA : 5 + 2 * *#devices*

3.1.2 Storage Node

FORMULA : 2 + 2 * #devices

3.1.3 Client

FORMULA : 2

3.2 Service port ranges in 7.3.x and later

3.2.1 Backup server

11 is the minimum number of daemons registered on the Networker server

- nsrd (uses one port)
- nsrmmdbd (uses one port)
- nsrindexd (uses one port)
- nsrmmgd (uses one port)
- nsrjobd (uses one port)
- nsrexecd (uses 4 ports)
- nsrmmd (uses one port)
- nsrlcpd(uses one port)

FORMULA : 11 + 2 * #devices + #jukeboxes

3.2.2 Storage Node

FORMULA : 4 + 2 * #devices + #jukeboxes

3.2.3 Client

FORMULA : 4

4 How did we implement it?

4.1 Private backup LAN

We defined the following rule sets as standard in our environment to ensure the communication needed between Networker server, the clients and storage nodes. These rules are implemented as ACL's on the private backup LAN.

Implementation of these rules is done with following commands:

nsrports –S 7937-X, followed by a restart of the Networker services on the host.

We need to specify the server network interface correctly for each client because each private backup LAN is defined on another subnet of the LAN. No communication is possible via the management LAN.

4.1.1 Backup server rules

We defined a maximum of 300 ports as service port ranges. (7937-8236). This leaves enough room for jukeboxes and storage nodes defined on the backup server.

4.1.2 Storage node server rules

Here we use the standard formula: 4 + 2 * #devices + #jukeboxes, starting from 7937.

4.1.3 Client rules

Here we defined a service port range of 5 (7937-7941). This means that this is enough for the standard Networker communication and the client push that is available from Networker 7.4

4.2 Shared environment

We are using CentricStor, Networker Management Console and Networker Backup Advisor and, as much as possible, the standard firewall ports defined in the manuals for our shared environment.

4.2.1 Communication towards CentricStor

For the definition of the firewall, concerning communication between Networker backup Server and CentricStor (Virtual tape library), we are using the parameter:

SSI_BASE_SOCKET=50004; export SSI_BASE_SOCKET.

This parameter is defined in the startup of our backup server for communication via the SSI process towards the CentricStor. As extra with the definition of this parameter, the port+1 is used for returning communications.

This means for the firewall request we ask always:

- From backup server to CentricStor : TCP/UDP 50004
- From CentricStor to backup server : TCP/UDP 50005
- And the portmap process : rpc_prog : 111 in both direction

4.2.2 Communication towards Networker Management Console (NMC)

The following port has been opened on the firewall for one central point of management of all the different datazones.

- From backup server to NMC: 7937-7942

  Remark: we opened an extra port for License Manager on the NMC server already

- From NMC to backup server : 7937-8236

4.2.3 Communication towards Networker Backup Advisor (EBA)

We opened the following port on the firewall for one central point of reporting of all datazones.

- From backup server to EBA: TCP 3916 and TCP 4001
- From EBA to backup server : TCP 3741

5 What should the future bring?

To my humble way of thinking, Networker should offer a solution to reduce the number of required ports for communication between Networker Backup Server and Networker Clients.

Imagination could be only ONE PORT needed for the communication.

Between other products, like NMC and EBA, and the Networker Backup Servers there should be more flexibility in the definition of the ports that need to be used. Even the same use of port numbers would be helpful so it would be possible for the communications defined between Networker Backup Server and Networker Clients.

6 Authors Biography

Member of the Belgacom IT staff since 1994, first as UNIX Sysadmin, from 1999 as responsible for the central Monitoring team (24/7). In 2002, joined the team that was designing Belgacom's first shared Storage environment as expert in the backup area and participated in the design and implementation of Belgacom's shared storage infrastructure (SAN, NAS and backup) for Open Systems and mainframes. The knowledge and expertise gained in the design and implementation of this enterprise storage infrastructure has also led to several Storage consultancy assignments for external customers.