Nokia Security Platform optimisation & fine-tuning strategy

To : Nokia Administrators	Date : 30-Dec-2002 Status : final
Author : Benoit Dee	

Version	Date	Nature of Change
V 1	30-Dec-2002	Proposal
V2	06-Jan-2003	Final

1. Automated management and monitoring

The purpose of automated management and external monitoring of the NSP is to minimise downtime and to offer a faster response to system failure and cyber attacks.

The newer IPSO versions offer various enhancements to make system administration easier and allow an enhanced resilience for business critical systems. The features of interest are:

- Transferring the syslog files to external systems, like Tivoli TEC and/or ITA manager
- Logging management activity in a separate log for Audit purposes.
- Automated backup possibilities (new since IPSO 3.5)
- Automated secure transfers of backup files and system logs to a central system using SCP and the schedule service CRON, which is a standard UNIX daemon. (new in IPSO 3.5)
- Activation of system failure notification to send alerts to a functional mailbox.
- Automated upgrade of modules through CP’s Secure Update allowing the deployment of new Checkpoint versions simultaneously and offering a fast back-out strategy. This way of migrating to newer versions will lower the system downtime considerably.

1.1. Transferring the syslog files to external systems.

The possibility to send the NSP’s Syslog files to an external system offers several operational and security advantages.

Degradation in performance or a partial failure can be discovered faster allowing TIVOLI’s TEC to create a ticket automatically. The generated tickets can have various severity levels, allowing the implementation of different response procedures. This kind of integration allows the Central Systems Control department to follow up day-to-day management in a more accurate way.

Sending some of the generated syslog files (security alerts) to the ITA architecture or in a later phase to a Centralised Event Management system (CEM), will allow a faster and more accurate detection of distributed or granular attacks. Currently the syslogs of the NSP’s are not checked due to the amount of resources needed to check the message file of every NSP. Merging all this logs by sending them to a central IDS or CEM system enhances efficiency.

1.2. Logging management activity in separate log.

IPSO offers the possibility to send administrator activity to a separate log instead of adding these entries to the standard *messages* file. This makes audit of the management activity more granular. Whenever 1 of the NSP boxes would be attacked, the use of a dedicated useractivity log makes it faster to search for possible security breaches.

1.3. Automated backup & restore possibilities.

Using the new automated back-up feature of IPSO makes it possible to daily back-up the configuration files of the NSP, the configuration of the CP firewall and even the NSP log files. These back-up files can then be send automatically and securely to an external server using the CRON feature integrated into Voyager. Whenever a system failure would occur, these back-up files can be used to restore the system in no time. The only criterion to meet is to obtain a NSP with the same IPSO version and software packages as the original one. This can be configured either using Voyager or CLISH.

1.4. Automated secure transfer of back-up files and system logs.

IPSO offers the possibility to transfer back up and logfiles automatically using 2 features:

- Transparent SCP (uses SSH) using client certificates associated to the different NSP.
- The possibility to schedule tasks using the Job Scheduler in Voyager. This corresponds to the UNIX cron service.

1.5. System failure notification.

IPSO offers the possibility to activate a mail relay to allow the system to automatically send mail messages when the NSP has serious problems. The mail account used should be that of a functional mailbox, which might be viewed by personal concerned by the NSP failure.

This should be done in co-operation with the mailhub team, since mail relaying is not allowed by default in the Fortisbank organisation. The current system notification configuration is not working for this reason, due to the sending of the mails to an internal SMTP server, which is not allowing relaying.

1.6. Automated upgrade of CP packages using Secure Update.

In Checkpoint NG a new central product and license manager was introduced: Secure Update (in FP2). This new integrated product offers the possibility to deploy new Checkpoint packages & licenses automatically, without manual intervention. When the upgrade doesn't succeed there is an automatic roll back procedure, minimising downtimes during upgrades.

Using this feature together with the IP clustering technology of IPSO will offer the possibility to migrate the Security architecture of the bank in a gradual way. (clustermember by clustermember)

This offers the possibility to migrate to new IPSO & Checkpoint versions, without impact on the active services.

2. Security fine-tuning

The IPSO operating system, which is a secured and optimised derivation of FreeBSD, offers the same user and usergroup granularity as any other UNIX system.

Using Voyager it is possible to create a dedicated group for FW administration (ex. *fwadmin*). This group is then associated to Checkpoint administration using the CP tool *cpconfig*. Every FW administrator should then be added to the *fwadmin* and the *other* group in the Voyager Groups tab. This will offer FW administrators the possibility to manage files in the $FWDIR and $CPDIR directories, while giving the possibility to access the MONITOR features of IPSO. The FW administrators should have the same UID & GID as the *Monitor* user.

The IPSO managers on the other hand should be added exclusively to the *wheel* group, which offer the full read/write access to the IPSO environment. The IPSO administrators should have the same UID & GID as the *Admin* user.

Another security enhancement is the creation of ACL to limit the client access to a predefined number of administration workstations.

3. Preparation of NSP for the IP clustering technology.

The new IPSO 3.6 offers a new *active/active* load-balancing feature borrowed from the now defunct Nokia Cryptocluster Series. This new features offers the possibility to create a dynamically loadbalanced clustering solution, where every cluster-member handles a part of the load.

In the current *active/passive* implementation offered by Nokia's Monitored Circuits, the back-up members are very often in an idle state. This overhead is only introduced for resilience.

The new clustering technology offers FREE additional scalability by sharing the load between the members. An additional feature of IP Clustering is the monitoring of daemons like *fwd, cpd, and ipsrd.*

Another big advantage of the clustering technology is the ease of administration, since any node can be removed from the cluster without disrupting the service. This results in "zero downtime and live upgrades" for the future migrations. When a NSP cluster needs to be upgraded (after the Management server upgrade) you remove 1 device at the time, upgrade it without stopping the service, and add it back to the cluster.

This technology can't be used together with CP's ClusterXL solution or any other 3rd party solution like Stonebeat or Rainwall.

To allow the configuration of IP clustering, some preparation is needed on the NSP's:

- Enable NTP to a central NTP server (the CP management stations in the Fortis Architecture). This is needed for the proper functioning of the CP synchronisation.
- Allow multicast ARP replies
- Define all the interfaces (physical & virtual) of each clustermember in the hosts tab of the NSP's. Define the addresses of the NAT pools for every member.
- Define all admin hosts which are used for SSH communication
- Define routing modifications for every host and switch in the perimeter environment.
- Add necessary static ARP entries (for virtual IP addresses and NAT pools) on the routers and SUN machines. NT server shouldn't have any problem.

Before implementing IP clustering it is recommended to first migrate the Checkpoint software to CP FP3 HF2.