

# **GenieATM Helps LNEPC Address Network Attacking Threats Effectively**

The LNEPC (LiaoNing Electric Power Corporation) Information Network was planned and constructed since the end of 1997, and it has always been the pioneer in the arena of information technology infrastructure among the national state-owned large and middle enterprises ever since. At the present, the LNEPC information network had completed the cross-provincial, three-layered network architecture – backbone network, city territory network, and WAN. The network connects 102 key network nodes (including network nodes of State Power Corporation of China, Jilin Provincial Power Corporation and Heilongjiang Provincial Power Corporation) and hence forms a super large scale network system. Positioned as an enterprise network with an extra large scale, the LNEPC information network system has now been supporting a variety of network applications such as the teleconference system, the video conference system, the office automation system and so on.

## **The Emerging of Network Problems and Challenges**

In mid-August 2003, the LNEPC information network suffered from serious network congestions and the network users complained about the worse and worse network performance. After a preliminary inquiry, the network O&M engineers observed massive Worm.Welchia traffic on the network so that they tried to filter the ICMP traffic via firewalls and ACL configurations on core switches. However, the restriction measures did not appear to help to the congestion while the performance of the local area networks and the links to external networks continued to fall. In the meanwhile, the core network devices became overloaded and the CPU utilization reached 100%.

Further investigated the problem, the engineers found that once the computers in the internal networks were infected they started sending attacking traffic outwards randomly. Although the firewall and ACL functions could help to filter the traffic going to the external networks, it could not constrain the contagious traffic flowing everywhere inside the internal network. When more and more internal hosts got infected and sending out attacking traffic consuming the bandwidth, the network performance dropped tremendously and the network devices (switches, routers, firewalls) were overloaded by trying to deal with the egress traffic. Furthermore, even though the network engineers could vaguely know the cause of the worsen problem, without detailed information of contagious hosts, they could not take further counter measures to completely mitigate the problem.

With the understanding of the problem and the limitation of firewalls and other perimeter security solutions, the LNEPC network management team started to look for a solution which can better address the challenges they faced. After a survey and evaluation, LNEPC decided to adopt the GenieATM (Genie Advanced Traffic Management) solution for their network protection from the Worm/DoS/DDoS attacks and hence effectively fortify the whole network security.

## **Deployments and Operations of GenieATM**

After closely discussing with the LNEPC network management team to understand their network topology and the security challenges faced, GenieNRM put forward the GenieATM deployment proposal meeting LNEPC's needs. LNEPC then deployed the GenieATM system in its NOC (Network Operation Center) by receiving the traffic information exported from the core switches.



anomaly traffic signatures and location of attackers and victims, the O&M engineers could take the necessary counter actions immediately (e.g. isolate/unplug the attackers temporary) before infected computers could be fully cleaned and patched from the worm, so that the impacts and caused damages were effectively eliminated and the threat was removed thoroughly.

#### **Step IV → Continuous Monitor to Ensure Network Security**

In addition to the troubleshooting, LNEPC network O&M team also applied the 「Flow Monitor」 and 「Flow Analysis」 functions on important links, users, services for long-term traffic analysis. 「Flow Monitor」 provides continuous traffic monitoring and threshold settings of each monitored object. Once a threshold was violated, a real-time alarm was sent via SNMP trap or e-mail to notify management correspondents for timely reactions. 「Flow Analysis」 identifies up to Top-128 heavy network resource consumers, the remote-end they are connecting to, and the applications they are using. The information is essential to form the normal traffic usage behavior patterns and hence helps to anomaly activities timely.

### **GenieATM Unfolds the Real-time Analysis Power for Complete Security Protection**

#### **Beneficial Results :**

- **Proactive Network Security Protection** : via the traffic-based mechanism GenieATM can effectively address various network anomaly activities such as worms, DoS, and DDoS attacks. In addition to detect problems in the early stage, the comprehensive drill down information of anomaly traffic helps perform precise actions to completely resolve malicious anomalies. The used-to-be 30-mins-more troubleshooting process can now be shortened to 5 minutes in simple steps, and the security protection is no more passive waiting for the virus signature updates.
- **Make 24x7hrs, Global-scale Traffic Visibility Possible** : prior to the deployment of GenieATM, due to the giant scale of LNEPC network, the O&M staff had difficulties to gain the in-depth traffic visibility. Now with the capability of continuous traffic monitoring, drilled-down Top-N analysis, the O&M staff now can analyze user network behavior, detect illegal websites and servers, and plan for routing balance. The abundant trending analysis reports provided by GenieATM can also be generated in few clicks.
- **Low TCO & Painless Deployment** : GenieATM makes use of flow information exported from existing, dispersive network devices so that the low TCO (Total Cost of Ownership) can be realized by monitoring the whole scaled network without planting new traffic sensors. The appliance solution, transparent architecture of GenieATM contributes to an effortless, non-service-interrupting experience in LNEPC deployment.
- **Friendly Interface & Easy Management** : GenieATM's layered-administration design lets the LNEPC network management team easily delegate different management tasks to different members of the crew with different scopes of responsibilities. The remote access with friendly Web-based GUI and the support of Simplified Chinese language provides the network managers the superior manageability.

#### **Customer Profile**

Company Name: Liaoning Electric Power Corp. Ltd. (LNEPC)

Industry Sector: Electricity

Headquarter: Shenyang Liaoning, China

Employees: 86,504

Registered Capital: RMB 10 billion yuan