

## Changing of the Guard...

### Migrating Check Point's set of rules to Astaro

Kings, queens and emperors rely on dedicated battalions of guards to shield them from intruders and outside dangers. In information technology, firewalls deployed at the computer gateway serve the same role, and changing of the guards requires precise choreography, even if ceremonies are less elaborate... Restructuring the network infrastructure, Germany-based POET AG replaced its Check Point FireWall-1 Version 4.1 with Astaro Security Gateway. Step by step, Check Point's set of rules was transferred to Astaro Security Gateway without negative effects on functionality and security. In the course of continuous improvements in performance, POET AG profited from a solution that preserved Check Point's set of rules at a lower price without neglecting security. In December 2003, the migration process was finalized and has been in effect until today.

IT-CUBE SYSTEMS GmbH ([www.it-cube.net](http://www.it-cube.net)), a systems integrator situated in Munich, helped as service partner when the search for a suitable firewall solution was under way. Checking the catalog of requirements, IT-CUBE's systems integration experts recommended Astaro Security Gateway. IT-CUBE SYSTEMS specializes in IT security systems, the team of technicians specifically focusing on questions of interoperability in regard to IPSec solutions. Together with Astaro's support staff, they set up a series of preliminary lab tests determining compatibility between the Check Point and Astaro Security Gateway systems. Test results clearly showed that a migration of all object and service definitions as well as packet filter rules was possible without difficulty. It became evident that IPSec VPNs between Astaro Security Gateway and Check Point supporting FeaturePacks 1 to 3 were viable due to implementations in line with standards and conformity requirements. POET even had the choice between authentication via PSK (PreShared Keys) and X.509v3 certificates. When generated on Astaro Security Gateway platforms, both X.509 and Root CA certificates could be imported into Check Point environments. Enabling their respective users to interact securely, it was even possible to issue cross-certificates between both Certification Authorities.

#### Installed Hardware:

- ProASL secuRACK Professional HA Bundle ([www.timenet.de](http://www.timenet.de))
- 19" 1 HU rack 42.6 x 37.9 x 4.3 cm (WxDxH)
- 250 W internal power supply unit
- 1024 MB DDR RAM
- 40 GB HDD
- 8 x 10/100 MBit/s Ports (Intel, Front Patch)
- 4 x 10/100/1000 MBit/s Ports (Intel, Front Patch)



Integrating VPN technology based on FreeS/WAN, Astaro's security solution achieves full compliance with the standard which results in excellent interoperability with third party vendors. In this way Astaro's platform allows high performance and extremely secure authentication and encryption concepts. The solution features a complete and fully implemented Public Key Infrastructure at no additional costs, enabling the deployment of a certificate authority to allow a company to issue their own digital certificates. Consequently, on both end-points of a VPN tunnel certificate-based authentication can be realized in a very secure way. Astaro Security Gateway adds additional value by supporting cryptographically strong encryption algorithms, including AES 256, Serpent, Blowfish or 3DES. Last but not least, this solution does not experience difficulties resulting from the use of dynamic IP addresses and Network Address Translation.

Before generating IPSec VPN connectivity between Astaro Security Gateway and a Check Point NG solution installed by one of POET's customers, a series of lab tests had to validate interoperability. A complex of problems was to be expected, because a single IPSec tunnel between PET's network with several Check Point Gateways and the customer enabled connections to four different target networks, all of which belonged to the same Check Point encryption domain. By generating individual VPN tunnels to the corresponding target network, the laboratory tests confirmed that the required results were feasible. So, for every target network an individual VPN tunnel was generated. The lab tests successfully showed that all of the services were available in this scenario.

In conjunction with the migration of filter rules, specific requirements concerning availability and performance had to be met. For one, web hosting of large customers still needed to be delivered via POET AG's 100 MBit/s internet connection. Additionally, access to a partner company's shipping and archive systems had to be guaranteed at all times. Hence, the security and NAT rules were transferred one-to-one. External partners did not notice the move from Check Point (Solaris 2.6) to Astaro. During this process, opportunity knocked to restructure and update the general set of rules.

### Redundant VPN Gateways

In larger networks it is quite common to have similar projects that require the full migration of a firewall's set of rules to a more cost-effective solution. As the availability of a central VPN gateway is mission-critical, companies need to consider all aspects of high availability solutions promising cost savings. In general, they have two options when realising such projects. Firstly, it is possible to work with firewall clusters by bringing in specialised systems. Alternatively, high availability can also be achieved by implementing master slave relationships between devices or processes.

In this case study, the second option was realised by deploying hot standby components. This allows for redundant system design at a significantly better price cost ratio, as Astaro Security Gateway protects against the most common reason of internet security system failure. Firewalls must be resilient to component and software

outages as failure of devices like the power supply unit, the hard disk drive, or even the processor are a frequent reason of system downtime. At POET, the installed high availability solution relies on two Astaro Security Gateway systems with identical hardware that run simultaneously to achieve system failover. The first firewall device has master control in normal mode, whereas the second box runs in hot standby mode (slave) supervising the primary device in real time over a direct network line via Link Beat. Periodically, the primary firewall system uses this connection to send heartbeat requests which are answered by the secondary firewall device. This network connection also serves as a means of updating the firewalls so that both systems contain identical information.

**POET AG**, based in Karlsruhe (Germany), is a globally active provider



of comprehensive catalog platforms for B2B eCommerce and Supplier Relationship Management. Organizations, suppliers and resellers rely on POET solutions to efficiently buy and sell their products online. Offering a unique self-service software for suppliers, the company is the leading provider of catalog management solutions for electronic marketplaces. POET software solutions optimize e-business processes, the company's list of customers including Fortune 500 companies such as ABB Inc., DaimlerChrysler AG, EADS, IBM, ThyssenKrupp AG, and Volkswagen AG.

## Conclusion

Migration from Check Point 4.1 to Astaro Security Gateway enabled POET AG to achieve a better price-performance ratio while maintaining the high level of functionality and security. Full compatibility between Astaro Security Gateway and the deployed Check Point firewall proved to be the main challenge and the decisive reason for success. It was essential to ensure continuous connectivity between remote networks and the main company network via IPSec VPN tunnelling. Apart from economic aspects, Astaro Security Gateway's high availability components and authentication options were additional reasons in favour of the unified threat management solution.

### Astaro AG

Astaro develops a complete line of network security products including the Astaro Security Gateway software and Astaro Security Gateway line of security appliances. All Astaro products offer nine critical security applications in three categories – Web Security, Email Security and Network Security – fully integrated on a single management platform. The company is co-headquartered in Burlington, Mass. and Karlsruhe, Germany. Astaro's software has won numerous industry awards, and is protecting over 30,000 networks in 60 countries. Astaro products are distributed by a worldwide network of 350 solutions partners who offer local support and services.

[www.astaro.eu](http://www.astaro.eu)