# TSG Solution Review Description

1. **TSG Solution Introduction**

The Traffic Secure Gateway (TSG) aims to manage cyberspace and reduce security risks. TSG delivers high-performance traffic processing for its global customers, providing the network traffic visibility and manageability required by high-bandwidth network perimeters.

TSG performs deep packet and flow inspection on Internet protocol packets and classifies their content using a stream-based analysis engine. The proxy module of TSG utilizes MITM (Man-in-the-middle) technologies, enabling authorities to perform layer 4-7 advanced manipulation of application and user traffic for interception.

The TSG has the ability of monitoring and blocking internet traffic, popular Apps such as Facebook, Twitter, and YouTube and also some evasive tools. The TSG is deployed at multiple geolocations such as ISP IGW sites and Data Center. There will be a Data Center in YGN (YGN Center). The YGN Center is used for central management, log storage and analysis. All ISP sites which are deployed TSG will connect to the YGN Center for data transporting.

The core component of the solution is the TSG Appliance (TSG XM14220). It also includes following components:

* Ether Fabric for traffic access and steering
* External Optical Bypass Protector (OBP) for failover
* TSG Central Management (CM)
* TSG Online Analytical Processing (OLAP)
* Cyber Narrator for identifying evasive proxy serves.

1. **Technical Team Introduction**

The technical team is led by Prof. Fang Binxing and the senior staff members have more than 20 years’ experience of this area.

Professor Fang Binxing, Academician of Chinese Academy of Engineering. Fang Binxing was the leading designer of a key part of the Great Firewall (GFW) of the Chinese mainland network censorship system, and was therefore known as the "father of the Great Firewall of China".

1. **Proof of Concept**

Provider has been provided Test Procedure of the TSG solution, including firewall, proxy, network visibility and report functions as mentioned in the proposal to NCSC department. NCSC department do all test in Test Procedure, and pay more attention on their concerning requirements: VPN blocking and application control.

The POC lasted about 6 months, from June to November.

* POC Environment Survey

On 18th June, the Provider visited MPT and NCSC for environment survey. The Provider checked the internet topology, network interfaces and machine room. The Provider present the document of the hardware list, power requirements, and deployment requirements.

* Hardware and Software Deployment

On 26th June, the Provider installed TSG XM14220, Ether Fabric, Optical Bypass Protector (OBP) to MPT data center room and layer 3 switch, Central Management (CM) server and Online Analytical Processing (OLAP) server to NCSC server room. After system hardware integration, the Provider installed software and prepared POC environment in the pointed conference room of NCSC.

* Test and Present

On 27th June, The Provider introduced the system functions and presented 18 test cases，explained how to block VPN using TSG. Then NCSC presented all test cases in test procedure to head of MOTC.

On 1st July, the Provider introduced the process of TSG solution for VPN or application blocking. The Provider prepared 12 VPNs which were blocked by using customization signature or built-in signature. Based on NCSC requirements, the Provider presented how to capture the VPN traffic, extract signature and import the VPN signature to the TSG. After that the Provider blocked TSG OpenVPN node and Apple IOS built-in VPN node in different VPN protocols which are using built-in application of TSG. On 11th July, the Provider blocked online advertainments for an android game and subscriber paid VPN nodes, like Nord VPN and Proton VPN. On 26th July, the Provider presented how to rate limit YouTube website both on PC and Smartphone.

On August and September, NCSC has been tested all functions of TSG to head of MOTC department.

On October, the Provider presented how to control Psiphon, Outline VPN, VPN and Viber voice call based on the requirements of NCSC.

1. **Software and License Description**

The Provider provides software:

* TSG Centralized Management is for the central management such as GUI, Policy, Events and Records, Network Visibility and Report
* Network Zodiac is for the system operation and maintenance
* Cyber Narrator is for supporting hunting the IP addresses of evasive proxy.

The software all has long-term authorization.

1. **Hardware Description**

The Provider provides hardware and All hardware is made in China:

|  |  |  |
| --- | --- | --- |
| **Model** | **Specification** | **Functionality** |
| Optical Bypass Protector | 2U, Optical Bypass Protector Chassis; Support 8 OBP Subcards for 8 ISP links. | External Optical Link Bypass Protection |
| Ether Fabric | 7U Chassis. | Ether Fabric Chassis, for Link access, traffic steering and load balancing |
| TSG XM14220 | 2U  CPU: 2x Intel Xeon Scalable 3rd Gen;  MEM: 8x DDR4 3200 REG 32GB;  HD: 1x 480G 2.5 SATA 6Gb R SSD;  NIC: 1 piece 2x 100GE; 2 pieces 2x 25GE;  IPMI2.0  Power: 2\*800W Redundancy; C13-C14 Power Cable; | Active DPI  Support Firewall  Support Proxy  Support App Sketch |
| TSG Central Management | 2U  CPU: 2x Intel® Xeon® Gold 5220R;  MEM: 8x DDR4 2933 32G;  HD: 480G 2.5 SSD\*2; 10x 2TB 7.2k 3.5 SATA; 2x 3.84T 2.5 SATA SSD;  RAID (RAID0, RAID1, RAID01, RAID3, RAID5);  NIC: 2x 25GE (Mellanox CX6);  IPMI2.0  Power: 2\*550W Redundancy; C13-C14 Power Cable; | TSG Central Management  GUI |
| TSG OLAP (Server 1) | 2U  CPU: 2x Intel® Xeon® Gold 5220R;  MEM: 8x DDR4 2933 32G;  HD: 480G 2.5 SSD\*2; 10x 2TB 7.2k 3.5 SATA; 2x 3.84T 2.5 SATA SSD;  RAID (RAID0, RAID1, RAID01, RAID3, RAID5);  NIC: 2x 25GE (Mellanox CX6);  IPMI2.0  Power: 2\*550W Redundancy; C13-C14 Power Cable; | TSG OLAP Server1 |
| TSG OLAP (Server 2) | 4U  CPU: 2x Intel® Xeon® Gold 5220R;  MEM: 8x DDR4 2933 32GB;  HD: 2x 480G 2.5 SATA SSD; 36x 8T 3.5 7.2K SATA;  RAID (RAID0, RAID1, RAID01, RAID3, RAID5);  NIC: 2x 25GE (Mellanox CX6);  IPMI2.0  Power: 2\*1200W Redundancy; C13-C14 Power Cable; | TSG OLAP Server2 |
| ISP Traffic Aggregation Switch | 2U  64\*100GE | For Traffic Aggregation |
| Center Core Switch | 12U  Chassis  4\* 2400W AC Redundancy Power;  2\* Fans Modules  36\*100GE  48\*10GE | Data Transfer |
| ISP Core Switch | 2U  Chassis  4\* 650W AC Redundancy Power;  2\* Fans Modules  24\*25GE, 2\*100GE | Data Transfer |
| Network Management Switch | Support 48\*10/100/1000BASE-T,4\*10G/1G BASE-X SFP+;  2\*150W AC Redundancy Power Modules;  2\*Fans | For Network Management Access. |
| Clock synchronization | Atomic Clock Integration, 20000 Client User Support. | For Network Time Service |
| Cabinet | 2\*PDU (32A and 63A better), Each PDU has no less than 12\*C14 Power Connector and has no less than 4\*C20 Power Connector. |  |

1. **Spare Part Description**

The Provider will prepare local spare parts, and faulty parts express deliver service.

1. **Support Service (Including System Update) Description**

* During the contract execution

The solution provides 3-year free of cost warranty and technical support.

The 3-year free of cost warranty and technical support including:

1. Hardware Warranty, local spare parts, and express delivery from China.
2. App Sketch DB updates
3. System updates (the Provider releases new version monthly, which includes new features and enhancements);
4. Bug fixes
5. Technical support, initial response in 4 hours
6. Documentation

* After the contract

When the first 3-year contract is expired, the Purchaser should buy the Warranty and Technical Support service for the future.

1. 2 engineer on-site support, working shoulder to shoulder with customers
2. Hardware Warranty, local spare parts, and express delivery from China.
3. App Sketch DB updates
4. System updates (the Provider releases new version monthly, which includes new features and enhancements);
5. Bug fixes
6. Technical support, initial response in 4 hours
7. Documentation
8. **Training Service Description**

* Training during the POC

The Provider provides training service to the NCSC’s engineers in the POC for using of the TSG. So that engineers have acquired the necessary knowledge of the TSG not only to manage but also to do the daily operation of the TSG. The Provider provided two-day training for introducing the architecture of the TSG. The Provider also trained the NCSC’s engineers to use system such as policy enforcement, checking system logs and executing reports in a shoulder to shoulder way. The Provider also trained the NCSC’s engineers using customized application signature function. From traffic capture, traffic analysis, signature extract to import the signature to the TSG and finally the NCSC’s engineers could block the VPN. During the POC, the Provider and NCSC’s engineers troubleshoot together and maintain the system together.

* Training during the contract execution

The Provider provides training services including the field of operation, management and maintenance of all types of equipment and software that is supposed to be supplied.

The Provider will provide before training:

1. Training program;
2. Training schedule;
3. The duration of each course;
4. Place of training;
5. The number of trainees for each course, indicating the requirements to their qualifications and work experience required for the successful completion of each training course.
6. **Scalability**

The design capacity of current solution is 5990.6Gbps. If the peak traffic doesn’t exceed the capacity, the expansion only needs to add OBP and Ether Fabric to access the new ISP links.

If the peak traffic is close to or exceeds the capacity, the expansion of the system needs to add additional devices (OBP, Ether Fabric, TSG XM14220, TSG OLAP Server1, TSG OLAP Server2 and network elements), the provider will provide a formula to calculate the number of devices.

No new license is required.

1. **Future Suggestion**

NCSC has the requirement of identifying application behavior using machine learning technology, such as the application is downloading.