



## Statement of Work

### Provision of Firewall and Security Orchestration Solution to the International Atomic Energy Agency

#### 1. Scope

The Information Technology Division established within the Department of Management (MTIT) is responsible for the overall approach to information technology and security at the International Atomic Energy Agency (IAEA), and the operational security aspects of its hosted systems and applications.

The purpose of this Statement of Work (SOW) is to provide information pertaining to the provision of a Firewall and Security Orchestration solution, including related software components and post-implementation maintenance (herein after referred to as the “Solution”). The provision of the Solution includes the supply, delivery, configuration, installation, testing and commissioning, as well as technical and consultancy services (herein after referred to as the “Services”). Training will also be included as part of the Services for the purpose of managing the IAEA’s existing firewalls, network, vulnerability scanners and security systems.

The Solution will be installed at IAEA Headquarters in Vienna, Austria and will allow for integration with other (3) branch offices, as follows:

- IAEA Seibersdorf Laboratories, Seibersdorf, Austria;
- IAEA Environmental Laboratories Monaco; and
- Microsoft Azure Infrastructure as a Service (IaaS) data center

The Solution and Services shall include the following:

- 1.1. All required software and licenses;
- 1.2. Engineering and support services (including architecture and design and integration of the different network and security systems) for the roll-out phase of the Solution;
- 1.3. Post-implementation maintenance and warranty of the Solution;
- 1.4. Training of IAEA MTIT staff on the Solution; and
- 1.5. Post-implementation support services for any ad hoc requests on an “as and when required” basis for approximately eighty (80) hours per year.

#### 2. Applicable Documents

The following documents shall be applicable for this SOW to the extent specified hereinafter:

Annex I: Current System Specification

Annex II: Official IAEA Holidays

#### 3. Definitions, Acronyms, and Abbreviations

The following definitions, acronyms, and abbreviations shall apply throughout this Specification unless defined otherwise hereinafter:

SIEM – Security Information and Event Management

VPN – Virtual Private Network

L2 –Open Systems Interconnection Layer 2

L3 – Open Systems Interconnection Layer 3

#### 4. Technical and Functional Requirements

The Contractor shall ensure the Solution meets the following functional and performance requirements:

##### Mandatory Requirements

- 4.1 Provide firewall policy management, including the automation of firewall operations and policy push;
- 4.2 Provide auditing and compliance, change management, and risk analysis, across all leading vendors and devices, including at minimum Cisco, Palo Alto Networks and Tenable;
- 4.3 Provide actionable recommendations based on industry best practice to clean up, optimize, reorder and tighten the recommended security policy for enhancing firewall performance;
- 4.4 Allow for consolidation of redundant and over lapping rules, based on source, destination, service commonality;
- 4.5 Automatically generate a dynamic, real-time network topology of firewalls and routers, including all relevant interfaces, subnets and zones, to help visualize and analyse complex networks;
- 4.6 Provide and generate visualization of firewalls, network and visualization of on premise, hybrid and cloud environments;
- 4.7 Provide support for Microsoft Azure by allowing continuous monitoring and support of automatic implementation of rule addition and rule removal for Microsoft Azure Network Security Groups and Azure firewalls;
- 4.8 Support a flexible and customisable out-of-the-box baseline configuration compliance for all network devices; with an option to customise and to create custom security baselines;
- 4.9 Detect and notify, via channels such as email or dashboard, any compliance and firewall policy violations;
- 4.10 Provide support for both L2 & L3 devices with search capabilities by IP address, subnets, object names etc;
- 4.11 Allow creation of traffic simulation queries in order to check and verify whether the traffic flows are permitted or not;
- 4.12 Support clean up and optimization of firewall policy by detecting duplicated, unnecessary objects and overlapping and out-dated security rules;
- 4.13 Support Palo Alto and Cisco and other similar network hardware by managing firewall and network security policies across multi-vendor and hybrid environment;
- 4.14 Discover risky traffic flows, such as security breach or risk created by misconfigurations across different firewalls and Cloud security groups, based on firewall policy violation and detect them before the changes are implemented;



- 4.15 Identify network and security risks by auditing firewall policies and routing and configuring network devices on hourly/daily/monthly basis;
- 4.16 Identify network and system vulnerabilities;
- 4.17 Provide the option to look up all the potential traffic/connectivity to and from an IP address;
- 4.18 Support and integrate Nessus vulnerability scanners;
- 4.19 Allow integration with major SIEM solutions; and
- 4.20 Provide electronic report on business applications connectivity needs with respect to terms of firewall rules and security policy.

### **Desirable Requirements**

The Solution should be able to:

- 4.21 Enable auto-matching and correlate change requests with current policy changes and ensure they are implemented in line with the requests and approvals;
- 4.22 Present vulnerabilities in an application context by integrating with leading vulnerabilities scanners;
- 4.23 Allow for customization with change management and workflow in ensuring it is completely modifiable to best match the business requirements;
- 4.24 Support role-based access for users; and
- 4.25 Integrate with a standard identity management solution for all management functions (such as RADIUS, LDAP and/or Microsoft Active Directory) with support for 2-factor authentication.

## **5. Maintenance, Support and Personnel**

The Contractor shall meet the Services and Personnel requirements listed below:

### **Mandatory Requirements**

- 5.1 Deploy the Solution in IAEA's environment and provide Services to integrate the Solution with IAEA's firewalls and other security and network equipment;
- 5.2 Provide regular Solution updates and schedule annual maintenance in coordination with MTIT;
- 5.3 Provide technical support on and off-line during IAEA working hours only (no support after IAEA working hours is required), Monday to Friday from 09:00 to 18:00 CET. The official holidays of IAEA and Austrian public holidays are not always the same. Services shall be available on Austrian public holidays, if this is a working day for IAEA. The list of the IAEA official holidays is provided under Annex II. Technical support shall include a mechanism available to log service requests and categorise them by severity levels and response times accordingly as follows:
  - Level 1 (High) – response time within 4 hours
  - Level 2 (Medium) – response time within 6 hours
  - Level 3 (Low) – response time within 12 hours

- 5.4 Provide support services for any ad hoc requirements on the Solution, separate from the annual maintenance, to be used on an “as and when required” basis. The estimated requirement is 80 (eighty) hours per year;
- 5.5. Provide a telephone number that can directly reach a service operator and provide an up-to-date e-mail address; and
- 5.6. Assign at least one (1) Senior IT Engineer with a minimum of three (3) years’ experience in the implementation of the Solution and one (1) Account Manager as focal points for IAEA’s operational and administrative matters.

## **6. Marking**

The Solution shall have all safety markings in English language.

## **7. Quality Requirements**

- 7.1. The Solution shall be manufactured, shipped and installed in accordance with the Contractor’s ISO quality assurance system or an equivalent quality assurance system; and
- 7.2. The Contractor shall document the compliance with this quality assurance system.

## **8. Testing and Acceptance**

- 8.1. The Solution shall be tested for the conformance with manufacturer’s performance specifications and the minimum requirements specified herein;
- 8.2. The Solution, after installation, shall be tested by the Contractor together with MTIT to demonstrate that the performance meets the manufacturer’s performance specifications and the minimum requirements specified herein as determined by the IAEA and MTIT; and
- 8.3 The results of the testing of the Solution shall be documented by the Contractor in an acceptance protocol that shall be signed by MTIT.

## **9. Installation and Training**

- 9.1. The Contractor shall install the Solution on site at IAEA Headquarters in Vienna, Austria and integrate it with the IAEA’s existing firewalls and network security infrastructure. Installation shall be done in person on site or remotely in a virtual environment; and
- 9.2 The Contractor shall provide training for up to eight (8) MTIT staff in the operation and maintenance of the Solution immediately after the installation of the Solution. The training should be delivered online or at IAEA Headquarters.

## **10. Deliverable Data Items**

- 10.1. The Contractor shall provide two (2) complete sets of operation and servicing manuals and technical drawings in the English language; and
- 10.2. The Contractor shall provide access to an online knowledge base containing reference material and a continuously updated database of common support issues and corresponding solutions.

## Annex I

### IAEA Information and Information Technology Environment Description

- 1.1. Information and communication systems are central to the IAEA's mission and daily business activities, as they are utilised to routinely exchange information among management and staff, with member states and other third parties in the public and private sectors. This is accomplished through the normal enterprise business and communications systems, restricted access and public web and collaboration services and staff remote access systems that are hosted both internally and in cloud-based systems. In addition to the systems supporting daily business activities, the IAEA has information and communications systems supporting the highly sensitive Nuclear Security and Safeguards activities.
- 1.2. The information technology infrastructure supports ~3000 users (staff and consultants) located at one primary location (Vienna International Centre) with five additional permanent facilities located in Austria, Canada, Monaco and Japan.
- 1.3. The IAEA has a partially centralised IT management organizational structure. Centralised IT management provides network, server, endpoint and security operations planning and administration as well as software development and maintenance. Additionally, there are staff members within divisions throughout the Agency providing software development, server-based applications administration and local IT client support.
- 1.4. While all staff members have information security responsibilities, the IAEA has a number of staff positions dedicated to security functions. These include:
  - Central Security Coordinator (responsible for all aspects of security except for Information Security)
  - Chief Information Security Officer
  - Information Security Office
  - Safeguards Information Security Officer
  - Security operations groups, supporting:
    - Access control
    - Threat management
    - Incident response
    - IT security engineering
- 1.5. The IAEA has a formal information security policy; however, the elements that underlie the policy in terms of Agency-wide processes, procedures, standards and guidelines are limited. There are also Agency policies for various information security related activities. Additionally, each Department may also issue additional policies. For instance, the Department of Safeguards has policy and procedures focused on protecting the confidentiality and integrity of the sensitive information that is central to their mission. On an ongoing basis, both internal and external audits and security assessments are performed. The technology underlying these services that are administered by IAEA staff includes:

- 800+ Servers, physical and virtualised (highly virtualised), Windows and Linux (predominantly Windows);
- 3500+ Client computers (desktop and notebook, Windows, Macintosh and Linux, predominantly Windows);
- 500+ Mobile devices (phones and tablets);
- MS Active Directory, multiple forests/multiple domains and additional standalone domains (such as for the DMZ);
- IPv4 wired and wireless networks, supporting client and server environments and Internet access;
- Network security systems providing access control; threat identification and blocking; centralised logging and Security Event and Incident Management;
- Multiple inter-site network communications connections;
- Multiple remote access systems;
- On-site dedicated data centres and rooms;
- Cloud-based and outsourced resources;
- Centralised and local IT Service Desks;
- Commercial and bespoke applications (client, client-server and web-based);
- Specialised laboratory, remote monitoring and embedded systems;
- Disaster recovery infrastructure;



## Annex II – Official IAEA holidays

- **In 2020**

|                           |  |
|---------------------------|--|
| Wednesday, 1 January 2020 | New Year's Day                             |
| Friday, 10 April 2020     | Good Friday                                |
| Monday, 13 April 2020     | Easter Monday                              |
| Friday, 1 May 2020        | May Day                                    |
| Monday, 25 May 2020       | in lieu of 24 May (Eid al-Fitr)            |
| Friday, 31 July 2020      | Eid al-Adha                                |
| Monday, 26 October 2020   | Austrian National Day                      |
| Friday, 25 December 2020  | Christmas Day                              |
| Monday, 28 December 2020  | in lieu of 26 December (St. Stephen's Day) |

- **In 2021**

|                           |  |
|---------------------------|--|
| Friday, 1 January 2021    | New Year's Day                             |
| Friday, 2 April 2021      | Good Friday                                |
| Monday, 5 April 2021      | Easter Monday                              |
| Monday, 3 May 2021        | in lieu of 1 May (May Day)                 |
| Thursday, 13 May 2021     | Eid al Fitr                                |
| Tuesday, 20 July 2021     | Eid al-Adha                                |
| Tuesday, 26 October 2021  | Austrian National Day                      |
| Monday, 27 December 2021  | in lieu of 25 December (Christmas Day)     |
| Tuesday, 28 December 2021 | in lieu of 26 December (St. Stephen's Day) |