

## COMPLIANCE MATRIX FOR TECHNICAL PROPOSAL

<b>RFP 381314 - MV</b> <b>Provision of Firewall and Security Orchestration Solution to the IAEA</b>			
<b>Ref.</b>	<b>Statement of Work Requirements</b>	<b>Compliant Yes/No</b>	<b>Bidder's comments</b>
<b>4</b>	<b>The Contractor shall ensure the Solution meets the following functional and performance requirements:</b>		
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 auditing and compliance, change management, and risk analysis, across all leading vendors and devices, including at minimum Cisco, Palo Alto Networks and Tenable.		
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 polices 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.		
4.20	Provide electronic report on business applications connectivity needs with respect to terms of firewall rules and security policy.		
<b>Desirable Requirements</b>			
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.		
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.		
<b>5</b>	<b>The Contractor shall meet the Services and Personnel requirements listed below:</b>		
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		

	<p>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:</p> <ul style="list-style-type: none"> <li>• Level 1 (High) – response time within 4 hours</li> <li>• Level 2 (Medium) – response time within 6 hours</li> <li>• Level 3 (Low) – response time within 12 hours</li> </ul>		
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.		
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.		
<b>6</b>	<b>Marking</b>		
6	The Solution shall have all safety markings in English language.		
<b>7</b>	<b>Quality Requirements</b>		
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.		
7.2	The Contractor shall document the compliance with this quality assurance system.		
<b>8</b>	<b>Testing and Acceptance</b>		
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.		
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.		
<b>9</b>	<b>Installation and Training</b>		
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.		
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.		
<b>10</b>	<b>Deliverable Data Items</b>		
10.1.	The Solution shall have all operational and safety markings in English language.		
10.2.	The equipment required for the Solution shall be packed in accordance with the international standards, applicable for the shipment by air for the type of equipment described in this SOW.		