Request for Proposals for Managed Security Services

Questions and Answers

Questions and Answers

№	Question	Answer
1	Please provide the details on the number of sites and their geographical locations in-scope.	Please refer to the UNDP public web site at http://www.undp.org/regions/ for complete list of regions (site groups) and at http://www.undp.org/countries/ for complete list of Countries
	Can the UN provide a country breakdown of where the devices will reside?	
2	Please provide the details on the number of group-sites and their geographical locations in-scope.	See answer to question 1
3	Please provide the details on the WAN connectivity between the sites in-scope	All UNDP offices are independently connected to the Internet, as described in section. Typical Internet connection bandwidth is stated in sections 2.2.1.1 (Small/Medium Office) and 2.2.1.2 (Large Office or Data Center)
4	Please provide the details on the number of Datacenters and their geographical locations in-scope.	Currently UNDP uses 4 Data Centers; two of them are commercial hosting Data Centers located in U.S.A., one located in Switzerland, and one in UNDP HQ in New York, U.S.A. However, respondents should not assume that this list is complete or final. UNDP may discontinue use of any listed Data Centers and/or establish new one.
5	Please provide the details on the in-scope Firewalls (Location, Count, Make, and Model).	Out of all managed firewall devices, the count per model is: Cisco PIX 515 – qty 55 Cisco PIX 515E – qty 15 Cisco PIX 525 – qty 2 Cisco ASA 5510 – qty 2 However, the Respondents should not consider this list final as UNDP is currently replacing some of Cisco PIX 515 with Cisco ASA5510
	Can you provide an itemized list of specific firewalls that you are currently running? For example 10 Cisco PIX 515E, 5 PIX 525, 20 Cisco ASA 5510, etc…	
6	Please provide the details on the in-scope IDS/IPS (Location, Count, Make, and Model).	UNDP currently not using any IDS/IPS devices. This is a service we may request in the future.
	Can you provide an itemized list of specific IDS devices that you are currently running? For example 10 ISS Proventia G400, 5 ISS Proventia G2000, etc…	
7	Please provide the details on the in-scope VPN concentrators (Location, Count, Make, and Model).	All existing IPSec VPN tunnels are terminated on the same firewall device that is installed at location. Please note that not all firewalls are configured for the IPSec VPN tunnels yet.

№	Question	Answer
8	Please clarify how many implementations to be done in Small/Medium Office?	Out of 74 sites, only 3 are Large Office/Data Center. Remaining 71 are Small/Medium Office sites.
9	Please clarify whether the currently in place Firewalls, IDS/IPS, VPN concentrator adhere to the specifications mentioned. If not what is their specification?	Please refer to answers to questions 5, 6 and 7 about specifications of existing devices. Cisco PIX 515, PIX 515E and ASA5510 are used in Small/Medium Offices, and PIX 525 and ASA5510 in Large Office and Data Centers.
10	Please clarify how many implementations to be done in Large Office or Data Center?	Please refer to the answer to question 8.
11	Please clarify whether the currently in place Firewalls, IDS/IPS, VPN concentrator adhere to the specifications mentioned. If not what is their specification?	Please refer to the answer to question 9.
12	Please clarify whether UNDP has a Log Management system already in place. Can it be leveraged for delivering the MSS?	The log management system for managed devices is provided by current MSSP, and respondents are expected to provide the same.
13	Please provide the details on how the Log management currently being performed (Architecture)?	Unknown, since it is part of the service. We have access to logs through the portal.
14	Please clarify whether we can transfer the logs to our SOC for performing Log Management?	Respondents are expected to provide solution to collect and analyze managed device logs, and provide access to UNDP through management portal.
15	Please provide the details on Security Information Management tool currently being used?	All information related to the Managed Security Services is provided by current MSSP through the proprietary portal. Respondents are expected to provide the same.
16	Please provide the details on the call volume for the in-scope devices?	On average, each Small/Medium Office submits about 2 policy change requests per month and about 5 for Large Office or Data Center. However, these numbers are only indicative, and there may be a significantly higher volume of requests during implementation of corporate-wide projects.
	How many changes occur within a monthly period per location? Per large office? Per small office?	
17	Please provide the details on the current MSS team strength?	Please refer to section 3.1.5 of the RFP for personnel requirements.
18	Please provide the details on the current ticketing system in place. Can we leverage the same?	Existing MSSP uses its own ticketing system. UNDP will not provide MSSP with access to our own ticketing system.
19	Please provide the details on the compliance regulations and standards being followed for the in-scope security devices.	UNDP follows the US Dept of Defense hardening guidelines as applicable to non classified information. It is anticipated that any recommended technology and/or device complies to FIPS199/FIPS200. If vendors do not comply or would wish to comply to a different standard they will have to provide clarification in their detail proposal.
20	Please clarify whether UNDP has defined process for implementation and management activities for the in-scope security devices?	Please refer to the RFP document for details on the implementation and management activities. Detailed processes and procedures will be negotiated with successful bidder prior to contact signing.
21	Please clarify whether UNDP can share the current SLA in place?	Existing SLA is confidential. The SLA for the requested service will be negotiated with successful bidder prior to contract signing.

№	Question	Answer
22	Please clarify whether UNDP is looking for single device pricing?	UNDP would like to receive a service, and not interested in the individual device procurement or pricing. As stated in RFP section 2.2.1, UNDP would like MSSP to own managed devices.
23	Please clarify whether the billing should be raised separately for each UNDP ICT?	The exact billing arrangement will be negotiated with successful bidder.
24	We assume the WAN link for the Site-to-Site VPN will be provided by UNDP. Please clarify.	Please refer to the answer to question 3.
25	Please clarify whether the Vendor is Centralized/Decentralized for all UNDP.	UNDP has no preference on Centralized/Decentralized Vendor, as long as MSSP will be able to accommodate requirements stated in the RFP.
26	Please clarify whether all the in-scope Firewall, IDS/IPS, VPN concentrators has got the contract with the vendor.	All managed devices are under maintenance contract with the manufacturer, with the exception of “out of support” devices.
	Does the UNDP maintain current hardware and software agreements with Cisco and other manufactures on all devices or is it maintained by the incumbent MSSP or other vendor?	
27	Please provide the details on the contract with the vendor when it is expiring.	Contract with current MSSP will continue for additional 36 month to ensure smooth transition to the selected MSSP.
28	Please clarify whether the new devices (Firewall, IDS/IPS, VPN Concentrator) for UNDP will be procured by UNDP or by us?	Please refer to the answer to question 22.
29	Please clarify whether the current in-scope devices have the remote power management capabilities?	Please refer to the technical specifications of Cisco PIX 515, PIX 515E, PIX 525 and ASA5510.
30	Please clarify whether the account manager is expected to operate out of Onsite (UNDP) or Offshore (our premises)?If onsite please provide the location details	UNDP do not foresee a need to have MSSP account manager on site, except for the periodic status meetings.
31	Please provide details on the contract with the Vendors (Patch, L3 support,New Versions)	Each site maintains independent contracts for the Internet Access services and local ICT infrastructure support. The scope of this RFP is to provide Managed Security Services only, as described in chapter 2 of the RFP.
32	What are limits of insurance items mentioned in the RFP?	The insurance limits should be adequate. Exact amounts will be negotiated with successful bidder
	I would also request you to let me know the conformance on the limits of insurance items mentioned in the RFP, and what is the value for the Limits of Insurance, the text as per RFP is as follows: (Annex 5 Section 8).	

№	Question	Answer
33	Because analysis is not called out specifically in this RFP, it is unclear how much effort should be devoted to provide the UN an understanding of monitoring services. Would it be helpful for the UN to understand how the MSSP will be monitoring security devices from the following aspects? • Fault and Performance Monitoring of the devices that are to be managed • Monitoring & Analysis of Firewall Logs for malicious activity • Monitoring & Analysis of IDS Logs for malicious activity • Correlation of IDS & firewall logs with vulnerability scan data to provide additional context and validity to security events • Correlation of IDS & firewall logs with global intelligence to identify potential bots and mitigate against potential data loss • Process around classifying a security event, how incidents are handled, escalated, reported and tracked • Process around how analysts track IP and security event history and how this information is used in future analysis • The use of trending information in log analysis	UNDP expects respondents to provide as much details on the analysis as they see necessary for UNDP to understand respondent's services and how they differentiate from other bidders. References in the RFP are section 2.2.6 – Reporting, 3.1.6 – Services, and 3.1.8 – Differentiators.
34	Cisco lists the PIX 515 as end of life, is the UN still using PIX 515?	Yes, UNDP is still using Cisco PIX 515. Please note hardware/software ownership requirements in the section 2.2.1 of the RFP
35	What versions of Cisco firewall software are running on the firewalls today?	Current version of the Cisco firewall software is defined by our current MSSP, and for majority of the devices are running software version 6.
36	Does UNDP own the equipment currently deployed?	Yes, UNDP owns all currently deployed equipment.
	Does the UNDP currently own the firewall hardware and IDS or is it owned by the incumbent MSSP or other vendor?	
37	How many network segments are involved per office?	Standard UNDP network design includes at least 3 network segments: outsize between firewall and Internet router, DMZ and inside segment with internal users and servers. However, many of our offices are using additional network segments based on their needs and requirements.
38	What is the bandwidth per office?	Please refer to sections 2.2.1.1 and 2.2.1.2 for minimum bandwidth requirements.
39	What type of connections are required per office, ie. 10/100 or 10/100/1000?	Please refer to sections 2.2.1.1 and 2.2.1.2 for local area network connection requirements
40	How many ISP's are involved per office?	Each site connects to at least one Internet Service Provider

№	Question	Answer
41	Does UNDP expect us to manage ISP failover?	UNDP has its own solution for multiple Internet connections failover. However, ability of MSSP to provide such functionality is an advantage.
42	Does UNDP require ISP load balancing at the UNDP HQ as well as the remote offices?	Only as part of the Internet connection failover service, if provided.
43	Would these firewalls be deployed in High Availability?	Only one site under MSS is currently uses High Availability (HA) for the firewall deployment. Respondents are required to support HA, but only few sites will require it.
44	If not, what are the anticipated Hardware Replacement expectations?	Currently UNDP maintains spare devices in UNDP Regional Centers, and made arrangements to provide replacement devices to our offices for next business day. MSSP is expected to provide similar hardware replacement time, but exact details will be negotiated with successful bidder.
45	Is an all-in-one Firewall/IPS solution acceptable?	Yes. However, respondents should also provide a standalone IDS/IPS option.
46	If no, how many segments per office will be monitored by the IPS solution?	UNDP have not defined exact requirements for IDS/IPS.
47	How long must log data be available for access?	UNDP should have online access to the log files for at least past 7 days. Current MSSP provides access to 1 Gb of logs per site. Exact requirements will be negotiated with successful bidder.
48	How long must log data be stored?	Current MSSP provides 7 years of archived logs for each site. Exact requirements will be negotiated with successful bidder.
49	Will the switches be managed by UNDP staff?	Yes. MSSP will be responsible for the devices necessary to provide requested services only. This includes firewalls, IDS/IPS sensors, VPN concentrators, and Out-Of-Band Management devices, if required and provided by MSSP.
50	Who is responsible for the rule change requests in each region? If it's Respondent, how many people will be able to ask for changes?	Please review section 2.1. For each office, it would be local site contacts, as well as respective regional contacts, and HQ contacts. All contacts would be UNDP employees.
51	Who keeps track of the list of rule change requests?	MSSP. UNDP expects that MSSP ticketing system will provide records for all requests, including rule change requests.
52	Is the UNDP running the AIP functionality on the ASAs today or are they just leveraging the firewall functionality? If the UN is using the AIP is it AIP 10 or AIP 20?	UNDP is not using AIP functionality of the Cisco ASA appliances.
53	Does the UNDP have a preferred manufacturer or model of IDS/IPS and firewall devices that they would like to see the devices replaced?	UNDP does not have any preferences for proposed firewall, IDS/IPS and VPN devices.

№	Question	Answer
54	How many IDS/IPS does the UNDP intend to deploy in Small/Medium Office format? In Large Office?	UNDP may use single IDS/IPS sensor or integrated functionality of the firewall, if available, in Small/Medium Office, and few standalone IDS/IPS sensors in Large/Medium Office or Data Center. Please note that these numbers are indicative only, and do not constitute a commitment to subscribe to IDS/IPS service.
55	How many firewalls does the UN intend to deploy in Small/Medium Office format? In Large Office?	Most of the offices will have single firewall in standalone or High Availability configuration.
56	Regarding the client to site VPN connections, does the UNDP currently have a RADIUS, Active Directory or LDAP system in place that would integrate with the firewalls or is that something that the MSSP must build and maintain? Alternatively, is there a specific set of firewalls that these users should be maintained on? How many total users require client to site VPN access?	UNDP prefers to use RADIUS, and UNDP will be responsible for the maintenance of the RADIUS service, and its integration with LDAP and/or Active Directory.
57	Would the UNDP be open to the MSSP taking over management of the existing security devices initially with a transition plan to move off of the existing hardware and onto new hardware as the contract progresses to ensure there is no gap in service from the incumbent to a new MSSP?	Yes. UNDP is acceptable to such proposition.
58	In section 2.1, can you clarify the difference between the individual site contact and the group site contact? In the individual section it states that "They are also primary contacts for MSSP in case of security incidents, managed device outages or scheduled maintenance notifications." However in the group section it states "They are also the primary escalation contact for any of the sites within a group." Could you clarify this? I am trying to understand when which group is primary versus secondary.	Group site contacts are also referred as regional contacts. Group contacts are the escalation point in case local site contact is not responsive, or due to any other issue that requires escalation.
59	In section 2.1, it sounds like there are three tiers of site contacts. Individual site contacts, group site contacts and all site contacts, with all having the greatest view, group site having a "regional" view and individual site contacts having the narrowest view. Is that a correct assumption?	This is correct.

№	Question	Answer
60	In section 2.2.4, it sounds like the UNDP is looking for a two step approval process. A request is made for a firewall change, for example, and then the engineer, who responds to that request, after performing his review, then responds to another person to verify the request before making the change. Is that accurate?	This is correct understanding of the required process.
61	In section 2.2.4, it is noted that certain policy changes that are not permissive can be performed without additional approval. Can you provide some examples of what you see as a non-permissive policy change?	An example may be to block access from specific IP address on specific or any port/protocol to stop an attack.
62	In section 2.2.5, does the UNDP have a specific manner that is preferable to them on data destruction?	UNDP have not identified specific requirements for the data destruction.
63		