

Security Assessment Service for Firewall/DMZ (Standard)

United States

1. Scope

In this fixed-price service, Sun will review and assess Customer's security policies, processes, procedures, architecture, access control points and security of systems ("Environment") identified under this statement of work ("SOW") for exposures and risks as they apply to the Firewall/DMZ(s) being reviewed ("Service"). The Service entails Sun analyzing and measuring the level of security of Customer's Firewall/DMZ Environment, and identifying and detailing potential gaps in the Firewall/DMZ Environment. Sun will also compare the level of security with a set of industry standards and best practices.

This is a high-level evaluation to provide a representative list of vulnerabilities, risks, and requirements; the Service will not provide Customer with an exhaustive list. Moreover, the Service only entails a review of the current Environment; Sun will make no remedial changes to Customer's Environment as a part of the Service.

The scope of the Service is limited by groups of facilities located within a 2-km radius ("Campus"), number of live IP addresses on the network ("Nodes"), number of key selected hosts and gateways or access control points.

Based upon this information, this Service is identified as a Standard Firewall DMZ Security Assessment.

Standard

- Staff and systems located in two (2) single geographic Campus.
- p to three (3) gateways consisting of firewalls or access control point, or fail-over pairs.
- IP networks up to 150 Nodes.
- Key selected host audits limited up to 15 hosts. These hosts will be a combination of SunPS identified hosts and Customer identified hosts.
- One hour interviews, up to 6 key personnel.

The interviews performed during the Service are to be conducted in person within the campus area. The interviews are used to gather information related to the scorecard criteria. Customer-provided documentation will also be used to gather information related to the scorecard criteria. Customer documentation will be returned at the end of the engagement.

The service also includes the following:

- A review of the customer's Firewall/DMZ environment and how it relates to their line of business, with specific emphasis given to Focus Areas as defined in the Security Assessment.
- A review of how the customer's security policy, processes, and procedures apply to their Firewall/DMZ environment.
- A network-based assessment of accessible hosts and key selected hosts running

- Solaris or Linux.
- A review of Firewall/DMZ architecture, and access control rules used to enforce that architecture. Firewalls include Sunscreen, Cisco's PIX, and Checkpoint's Firewall-1.
- IP-based network protocol.

Service Scope Exclusion

Although the Firewall/DMZ service enables us, if warranted, to make a general recommendation that an architecture be deployed, say using access control mechanisms to separate trusted networks from non-trusted networks, Firewall/DMZ does NOT generate specific architecture design, product, or implementation recommendations. Firewall/DMZ is an assessment service, not an architecture or design service.

Firewall/DMZ will not address:

- denial of service attacks,
- war dialing or assessment of phone systems/PBX,
- actual exploits on or against production systems,
- hosts outside the scope of this service,
- firewalls outside the scope of this Service,
- non-IP based protocol or systems (such as DECNET, IPX, etc.), and
- physical security.

2. Approach, Tasks and Deliverables

2.1 Approach

Sun will complete the Service in the following Phases:

1. Phase 1: Firewall/DMZ Security Initiation
2. Phase 2: Firewall/DMZ Security Assessment
3. Phase 3: Firewall/DMZ Security Closure

2.2 Tasks and Deliverables

2.2.1 Phase 1: Firewall/DMZ Security Initiation

Sun will meet with Customer to review the status of their environment, and to review conditions and prerequisites for the Service delivery. Additionally, Sun will conduct a project kick-off meeting with key Customer contacts to finalize the project approach, discuss roles, responsibilities, and the work schedule. At the kick-off meeting, Sun and Customer will review resource matters such as available workspace, access to telephones, copiers, faxes, LAN connections, tape drives, conference rooms, and printing facilities required to deliver the Service. Additionally, Sun will gather customer information related to this Service via online data collection, documentation review, and interviews with Customer's staff. To facilitate the delivery of the Service, Sun and Customer will attend an additional meeting to discuss interview schedule coordination, and to complete a checklist in preparation for Service delivery.

2.2.2 Phase 2: Firewall/DMZ Security Assessment

Sun will collect data and documentation concerning the integrity of Customer's current Firewall/DMZ environment in the following focus areas *Focus Areas*:

1. Security policies and procedures.
2. Technical staff skills and training.
3. Management support and awareness.
4. Firewall/DMZ security architecture.
5. Firewall rulebase design and access control.
6. Authentication and authorization.
7. Auditing, accountability, and reporting.
8. Data privacy, integrity and security.
9. Host and system-based security.
10. Single points of failure.

Sun will analyze each Focus Area with respect to its Security aspects.

- Gather this data via data collection, documentation review, and interviews with Customer's staff.
- Analyze the information to find potential gaps within the Firewall/DMZ environment in these focus areas.
- Then define high-level recommendations related in these focus areas as appropriate.

Based upon Sun's review of the Environment, Sun will provide Customer with a report and an optional presentation. The report will include a summary of findings, a scorecard which highlights areas to be addressed, and a set of recommendations. This report and an optional presentation is a high-level evaluation which provides a representative list of vulnerabilities, risks, and requirements: the report and optional presentation are not intended to be an exhaustive list.

In the course of this Service, should Sun identify any critical security risk that could result in immediate compromise, Sun will report the risk to Customer's Project Manager within one business day. This Service is a high-level assessment and therefore Sun makes no guarantees that such a risk will be discovered.

Activity Input(s)

- Firewall/DMZ Security Assessment Requirements Capture
Designated Customer personnel will gather and provide Sun with Firewall/DMZ Infrastructure Information, to include:
 - all infrastructure and network topology relevant to the systems identified in the Statement of Work;
 - all current computing platform, network device, and operating system software environment information for the systems set forth in the Statement of Work; and
 - any additional, applicable documentation of the Environment to be provided at the Customer's discretion.

Deliverable(s)

- Firewall/DMZ Security Assessment Report
One hardcopy or print-ready copy. The Report includes Sun's findings on:
 - security strengths and weaknesses,
 - vulnerabilities and risks,
 - high-level recommendations for the Focus Areas specified in the SOW, and
 - a security scorecard relating Customer's Firewall/DMZ security environment to a set of industry standards and best practices, to include analysis of the Focus Areas.

The recommendations will not include product, design, or implementation recommendations. The report is not intended to be a tutorial or a comprehensive reference manual.

- (One) Firewall/DMZ Security Assessment Report Revision (if necessary)
One hardcopy or print-ready copy, which may be used as set forth in the license provision in the Assumptions section of the SOW.
- Firewall/DMZ Security Assessment Presentation (optional)

2.2.3 Phase 3: Firewall/DMZ Security Closure

Sun will conduct a formal meeting with Customer to:

1. Review the tasks and deliverables for this Service which Sun completed; and
2. Obtain Customer sign-off on the delivery completion form *Completion Form*.
3. Review any outstanding issues at this time.

3. Customer Responsibilities

Customer shall provide Sun with the following:

1. Copies of relevant policy, architecture, configuration, and processes documentation.
2. Facilities access and access to relevant internal and external systems as required by Service
3. Adequate workspace for each of Sun's consultants, as well as access to telephones, copiers, faxes, conference rooms, and printing facilities as reasonably necessary
4. Customer relevant business requirements and service level agreements
5. Access to key Customer personnel, including management, IT, and operational staff.
6. Parking and access passes as required by Sun as necessary for Service delivery
7. A timely response (i.e. in a time period that does not affect Sun's scheduled delivery of the Service) to all requests for information by Sun
8. Timely delivery of information and support (i.e. in a time period that does not affect Sun's scheduled delivery of the Service) from suppliers of non-Sun equipment and services as requested
9. Any relevant operational performance standards in use by Customer related to Service delivery
10. An escalation procedure in the event that timely responses are not provided to

Sun to ensure that the Service can be completed within the established time-frames

11. Before work begins, Customer to provide a notification process should a severe or critical security vulnerability be discovered.

12. A timely response (i.e., in a time period that does not affect Sun's scheduled delivery of the Service) to the review of all Service-related documentation.

4. Change Control

The objectives of change control ("Change Control") are to:

1. Assess the impact of scope changes on project schedules, resources, and pricing.
2. Provide a formal vehicle for approval to proceed with any changes for this SOW.
3. Provide a project audit record of all material changes to the original SOW.

Should Customer want to change any deliverable, the Sun Project Manager will follow standard change control procedures described in this section. Sun will complete all work authorized under change control on a time-and-materials or fixed price basis, dependent upon which contract type is most appropriate. Time and Materials will be charged at Sun's then current rates.

If Customer requests a material change in the scope of this SOW, as determined by Sun in its sole discretion ("Change"), Sun and Customer will review the Change through the change control process set forth in this Section ("Change Control Process"). When Sun determines a change is material, Sun will complete a change request form (the "Form") and provide the completed Form to Customer. Both Sun and Customer will have to provide written approval of the Change detailed in the Form, including the impact of the Change on the schedule, resources, and the price of the Service, before Sun will make the Change. When Customer accepts the Change set forth in the Form, Customer will modify its P.O. or other forms for payment as requested by Sun. If Customer does not accept the Change as set forth in the Form (including the impact on the schedule, resources, or price), the Parties will complete their obligations with respect to this Service as set forth in this SOW.

5. Assumptions and Dependencies

Sun will rely on the following assumptions, together with those stated elsewhere in this SOW, in performing the Service. Should any of these assumptions prove incorrect or incomplete or should Customer fail to comply with any of the Customer responsibilities set forth in this SOW, Sun reserves the right to modify the price, scope, or schedule of the Service.

1. Sun will assign a project manager to this engagement and will coordinate project management activities with Customer's Project Manager. Sun's project manager will have primary responsibility for coordinating all activities for this Service, including scheduling resources, confirming project activities and deliverables are within the scope of this SOW. Sun's project manager will serve as Sun's single point of contact for this Service. The Sun Consultant or Engagement Manager may perform the project manager function as appropriate.

2. Customer has valid licenses for all software covered by the Service, and all licenses will cover Sun's use of the software as well.
3. Customer will assign staff to support Sun that are properly trained in their area of responsibility (e.g., properly trained as a Solaris Systems Administrator).
4. Sun's provision of the Service presumes that Customer is performing backups on a regular basis at the proposed Name the location site prior to Sun providing the Service. Sun has no responsibility in any way with respect to Customer's data in providing the Service.
5. Meetings will take place at a mutually accepted location.
6. Sun reserves the right to use subcontractors in those roles it deems appropriate.
7. The engagement will begin on a mutually acceptable date.
8. The tasks and deliverables described in this SOW will be deemed accepted by Customer upon delivery.
9. The only tasks and deliverables Sun will undertake or deliver in providing the Service are those specifically set forth in this SOW.
10. Any Service schedule estimates represent Sun's best technical judgment based on information available. The actual duration of the Service may vary.
11. Unless otherwise specified by Sun, all Service-related documentation requested by Sun must be provided one week prior to Sun's onsite visit.
12. The implementation of any project recommendations resulting from the Service are beyond the scope of this SOW.
13. Sun is not responsible for design issues attributable to Customer's failure to provide any pertinent information.
14. Sun will make commercially reasonable efforts to meet those critical time frames identified by Customer and agreed to by Sun in writing.
15. Customer understands that Sun will take commercially reasonable precaution to avoid causing unexpected behavior or down time in Customer's environment.
16. Sun will conduct the Service during Sun's standard business hours and standard business days.
17. From the time Sun provides Customer the Report, Customer has five days to review the Report and provide comments and ask questions. In the case where the Report requires revision after it is reviewed, Sun will make one revision of the Report and deliver it to the Customer's Project Manager. The Service is considered finished upon delivery of the Report.

6. Fees and Expenses

This is a fixed-price engagement. This is a fixed-price engagement. The fee for this Service (including all expenses noted below) is as stated in Customer's most recent quote from Sun or as otherwise mutually agreed by Customer and Sun ("Fee").

Expenses incurred in connection with the Service, such as telephone toll-calls, photocopies, fax charges, messengers, travel, lodging, meals, and car rental are included in the Fee.

7. Contract Requirements

In the event that Customer purchases the above-described Services from Sun, this

Service Listing or SOW is incorporated by reference in and subject to the terms of the agreement which has been most recently entered into by the parties and under which Customer may order products and services from Sun ("Agreement"). Sun is not obligated to perform the Services described in this Service Listing or SOW unless Customer has an Agreement with Sun and has received an order confirmation from Sun accepting Customer's purchase order or electronic order for the Services. This Service Listing or SOW does not constitute an offer by or invitation to contract with Sun. The Services described above are subject to availability and unless otherwise stated, are only available within the above-referenced country. Any reference to "Customer" in this Service Listing refers to the party that enters into the Agreement with Sun. Such party may be referred to in the Agreement as "Company", "Customer" or other appropriate term.

Last Revised: March 2007