| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-5** | DENIAL OF SERVICE PROTECTION | |
| **SC-5.1**  **SC-5.1.1**  **SC-5.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and* 2. *the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Information system for protection against or limitation of the effects of denial of service attacks]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-7, SI-3, SI-4  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions**  **\*\*See “**[**Assessment Case Overview**](http://csrc.nist.gov/groups/SMA/fisma/assessment-cases-overview.html)**” for selecting, tailoring and executing action steps\*\*** |
|  | | *\*\*Assessment Case Assessor Note:* More convincing evidence (i.e., greater assurance) of correct implementation and operating as intended can be obtained through the assessment case actions by:   1. **Replacing bracketed values in action gathering statements to apply greater rigor in the assessment** (e.g, . replacing [“*reviewing*”] with “*studying*” or “*analyzing*”; replacing [“*observing*”] with “*inspecting*” or “*analyzing*”; replacing [“*basic*”] with “*focused*” or “*comprehensive*”); 2. **Replacing bracketed values in action gathering statements to apply greater sample coverage in the assessment** (e.g, . replacing [“*basic”*] sample with “*focused*” or “*sufficiently large”* sample); 3. **Defining additional action steps to the list of action steps suggested herein that exercise additional test methods** (i.e., Examine, Interview or Test) on additional assessment objects. |
| **SC-5.1.1.1** | | **Examine** system and communications protection policy, procedures addressing denial of service protection, security plan, or other relevant documents; [*reviewing*] for the types of denial of service attacks (or references to sources of current denial of service attacks) that can be addressed by the information system. |
|  | |  |
| **SC-5.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to protect against or limit the effects of the denial of service attacks identified in SC-5.1.1.1. |
| **SC-5.1.2.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-5.1.2.1;[*reviewing*] for evidence that these mechanisms are configured as identified in SC-5.1.2.1. |
| **SC-5.1.2.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-5.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **SC-5(1)** | | DENIAL OF SERVICE PROTECTION |
| **SC-5(1).1**  **SC-5(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Information system for protection against or limitation of the effects of denial of service attacks]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, AC-6, CM-6, SC-7, SI-4  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **SC-5(1).1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to restrict the ability of users to launch denial of service attacks against other information systems or networks. |
| **SC-5(1).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-5(1).1.1.1;[*reviewing*] for evidence that these mechanisms are configured as identified in SC-5(1).1.1.1. |
| **SC-5(1).1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-5(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-5(2)** | DENIAL OF SERVICE PROTECTION |
| **SC-5(2).1**  **SC-5(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information system bandwidth, capacity, and redundancy management]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-7, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-5(2).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks. |
| **SC-5(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-5(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-5(2).1.1.1. |
| **SC-5(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-5(2).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |